Islamic Azad University , Shiraz Branch
Journal of Circuits, Data and Systems Analysis

دانشگاه آزاد اسلامی
واحد شیراز

نشریه تحلیل مدارها، داده ها و سامانه ها

نشریه تحلیل مدارها، داده ها و سامانه ها

هیات تحریریه

نشریه تحلیل مدارها، داده ها و سامانه ها
Islamic Azad University , Shiraz Branch
Journal of Circuits, Data and Systems Analysis

نشریه تحلیل مدارها، داده ها و سامانه ها

سال دوم- شماره سوم - پاییز ۱۴۰۳

فهرست مقالات

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

Application of Machine Learning in Detection and Prevention of Money Laundering with Cryptocurrencies

Mojtaba Goodarzi[1] , Mahdi Khaghani Isfahani[2*], Mohammad Ali Kanani[3]

[1] Department of Humanities, Criminal Law and Criminology, Kish International Branch, Islamic Azad University, Kish Island, Iran
mgoodarzi359@gmail.com
[2] Department of Humanities, Criminal Law and Criminology, The Institute for Research and Development in Humanities (SAMT), Tehran, Iran khaghani@samt.ac.ir
[3] Department of Humanities, Criminal Law and Criminology, Roodhen Branch, Islamic Azad University, Tehran, Iran
dr.kanani110@gmail.com

Abstract: Money laundering, as a critical challenge for financial systems, has become increasingly complex with the advent of cryptocurrencies. Features such as anonymity and the ability for rapid, cross-border transfers have rendered cryptocurrencies attractive tools for illicit activities, including money laundering. Machine learning, as an advanced technological approach, offers promising capabilities for detecting suspicious patterns and preventing money laundering within decentralized financial systems. However, the efficacy of this approach hinges on the formulation of a sophisticated criminal policy framework that leverages the opportunities offered by cryptocurrencies while mitigating associated risks. This study, employing a descriptive-analytical methodology, examines legal challenges such as the absence of comprehensive and harmonized global regulations, regulatory issues like the lack of international standards for monitoring cryptocurrency transactions, and technical difficulties, including the complexity and volume of transaction data and user anonymity. The findings underscore the necessity of international legal cooperation and harmonized criminal policy strategies to combat money laundering in the cryptocurrency domain. Machine learning models, while holding significant potential for enhancing oversight and crime prevention, require a robust legal and regulatory framework to realize their full potential in addressing financial crimes within this emerging technological landscape.
Keywords: machine learning, cryptocurrency transactions, money laundering, criminal policy.

JCDSA, Vol. 2, No. 3, Autumn 2024	Online ISSN: 2981-1295	Journal Homepage: https://sanad.iau.ir/en/Journal/jcdsa
Received: 2024-08-24	Accepted: 2024-11-20	Published: 2024-12-20

CITATION

Goodarzi, M., et. al., *" Application of Machine Learning in Detection and Prevention of Money Laundering with Cryptocurrencies "*, Journal of Circuits, Data and Systems Analysis (JCDSA), Vol. 2, No. 3, pp. 1-15, 2024.

DOI: 00.00000/0000

* Corresponding author

Extended Abstract

1- Introduction

Money laundering has long been one of the most pressing challenges for global financial systems, and the advent of cryptocurrencies has introduced new layers of complexity. Due to features such as anonymity, decentralization, and rapid cross-border transfers, cryptocurrencies have become attractive tools for facilitating illegal financial activities, particularly money laundering. In traditional systems, money laundering involved complex schemes like using shell companies and fake identities, but cryptocurrencies have added new dimensions by leveraging blockchain technology and peer-to-peer transactions.

Machine learning (ML), as a subset of artificial intelligence, presents a promising solution for identifying and preventing money laundering activities within the cryptocurrency ecosystem. ML algorithms can detect suspicious patterns that might go unnoticed through traditional monitoring systems. However, the implementation of machine learning in financial regulation, particularly in cryptocurrency transactions, presents legal, regulatory, and technical challenges. These challenges are further compounded by the absence of comprehensive international legal frameworks governing cryptocurrency transactions, which makes cross-border enforcement and cooperation difficult. This paper investigates the potential of machine learning to combat money laundering in cryptocurrency transactions, while focusing on the regulatory, legal, and technical obstacles that hinder its effectiveness, particularly in the context of Iran's financial system.

2- Methodology

This study adopts a descriptive-analytical research methodology, utilizing both qualitative content analysis and a comparative approach. The analysis focuses on the intersection of cryptocurrency, machine learning, and anti-money laundering (AML) regulations. It examines legal texts, regulatory standards, and technical documentation to explore the challenges and solutions associated with the implementation of machine learning in monitoring cryptocurrency transactions. Furthermore, the paper compares international frameworks, such as those provided by the Financial Action Task Force (FATF), with Iran's legal and regulatory system, highlighting gaps and opportunities for improvement.

The research also investigates case studies of how ML algorithms such as Random Forests, XGBoost, Graph Convolutional Networks (GCNs), and Deep Neural Networks have been applied in real-world scenarios to detect money laundering activities. These case studies provide insight into the strengths and limitations of ML in the cryptocurrency space, especially in light of the vast amount of data and the anonymity provided by certain cryptocurrencies.

3- Results and discussion

The results show that machine learning models, when applied correctly, can significantly enhance the accuracy and efficiency of monitoring cryptocurrency transactions. Key advantages include:

- High accuracy: Algorithms like neural networks and GCNs detect hidden patterns in large datasets that manual or traditional rule-based systems miss.
- Real-time monitoring: ML allows for immediate detection of suspicious behaviors, which is essential given the fast-paced nature of cryptocurrency transactions.
- Adaptive learning: ML models continuously improve, which is vital for combating constantly evolving money laundering tactics.
- However, several challenges need to be addressed, particularly in Iran, including:
- Legal gaps: Iran's AML laws do not explicitly address ML or cryptocurrency-specific challenges, and the lack of global standards complicates cross-border enforcement.

Technical limitations: ML requires substantial computational resources and expertise, which are often limited in developing economies like Iran.

Regulatory barriers: Many Iranian cryptocurrency exchanges lack clear oversight, making it difficult to implement effective ML-based monitoring systems.

4- Conclusion

This study highlights the critical role machine learning can play in combating money laundering in cryptocurrencies. Technologies like Random Forests and GCNs show promise but require a supportive legal and regulatory framework to be effective. Key recommendations for Iran include:

- Developing clear legal frameworks: Policymakers must create regulations for using ML in financial monitoring and cryptocurrency transactions, aligned with global standards.
- Strengthening technical infrastructure: Investments in computational resources, expertise, and data quality are essential for implementing ML-based systems.
- Promoting international cooperation: Iran should engage in global discussions on AML regulations, especially related to cryptocurrencies, to align its policies with international norms.

In conclusion, while ML offers substantial promise in combating money laundering in cryptocurrency transactions, legal, technical, and regulatory reforms are essential for realizing its full potential in Iran's financial system. By addressing these challenges, Iran can harness the power of ML to enhance its AML capabilities and protect its financial system in the increasingly digital and decentralized global economy.

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

کاربست یادگیری ماشینی در کشف و پیشگیری از پولشویی با رمزارزها

مجتبی گودرزی[1]، مهدی خاقانی اصفهانی[2*]، محمدعلی کنعانی تیکمه داش[3]

۱- گروه علوم انسانی، حقوق جزا و جرم شناسی، واحد بین الملل کیش، دانشگاه آزاد اسلامی، جزیره کیش، ایران (mgoodarzi359@gmail.com)
۲- گروه علوم انسانی، حقوق جزا و جرم شناسی، پژوهشکده تحقیق و توسعه علوم انسانی (سمت)، تهران، ایران (khaghani@samt.ac.ir)
۳- گروه علوم انسانی، حقوق جزا و جرم شناسی، واحد رودهن، دانشگاه آزاد اسلامی، تهران، ایران (dr.kanani110@gmail.com)

چکیده: پولشویی، به‌عنوان یکی از چالش‌های کلیدی نظام‌های مالی، با ظهور رمزارزها ابعاد پیچیده‌تری یافته است. ویژگی‌هایی نظیر ناشناس بودن و انتقال سریع و فرامرزی رمزارزها، آن‌ها را به ابزاری جذاب برای جرایمی همچون پولشویی تبدیل کرده است. یادگیری ماشینی، به‌عنوان یک ابزار پیشرفته، قابلیت شناسایی الگوهای مشکوک و پیشگیری از پولشویی در سیستم‌های مالی غیرمتمرکز را دارد. با این حال، موفقیت این فناوری مستلزم تدوین سیاست جنایی هوشمندانه است که بتواند هم از مزایای رمزارز بهره‌برداری کند و هم مخاطرات آن را کاهش دهد. این پژوهش، با روش توصیفی-تحلیلی، به بررسی چالش‌های حقوقی نظیر نبود قوانین جامع و جهانی، چالش‌های مقرراتی مانند فقدان استانداردهای بین‌المللی برای نظارت بر تراکنش‌های رمزارزی، و چالش‌های فنی از جمله پیچیدگی و حجم بالای داده‌ها و ناشناس بودن کاربران می‌پردازد. تأکید بر همکاری بین‌المللی و هماهنگی سیاست‌های جنایی برای مقابله با پولشویی در حوزه رمزارزها ضروری است. یافته‌ها نشان می‌دهند که مدل‌های یادگیری ماشینی می‌توانند نقش مهمی در بهبود نظارت و پیشگیری از جرایم مالی مرتبط با رمزارزها ایفا کنند، اما این امر مستلزم چارچوب‌های قانونی و نظارتی مناسب است.

واژه های کلیدی: یادگیری ماشینی، تراکنش‌های رمزارزی ، پولشویی، سیاست جنایی

نوع مقاله: مروری
تاریخ ارسال مقاله: ۱۴۰۳/۰۶/۰۳ تاریخ پذیرش مقاله: ۱۴۰۳/۰۸/۳۰ تاریخ چاپ مقاله: ۱۴۰۳/۰۹/۳۰
DOI: 00.00000/0000

۱- مقدمه

با ظهور رمزارزها به‌عنوان یکی از نوآوری‌های مهم فناوری در دهه‌های اخیر، فرصت‌ها و چالش‌های جدیدی برای نظام‌های مالی جهانی به وجود آمده است. در حالی که رمزارزهایی مانند بیت‌کوین و اتریوم به‌عنوان ابزارهایی برای تسهیل تراکنش‌های مالی و بهبود سطح مبادلات اقتصادی مورد استقبال قرار گرفته‌اند؛ به دلیل ویژگی‌های خاص خود مانند ناشناس بودن، عدم وابستگی به نهادهای مرکزی و قابلیت انتقال سریع و فرامرزی، به‌طور هم‌زمان به ابزاری مطلوب برای فعالیت‌های غیرقانونی از جمله پولشویی تبدیل شده‌اند. تنها در اوایل سال ۱۳۹۹، ده‌ها پرونده سنگین در شعب مجتمع تخصصی رسیدگی به جرایم اقتصادی مفتوح شده که حجم قابل‌توجهی از آنها اتهامات پولشویی است [۱]. پولشویی در بستر رمزارزها با پیچیدگی بیشتری نسبت به پولشویی سنّتی مواجه است؛ چراکه رهگیری و شناسایی تراکنش‌های مالی در این حوزه به مراتب دشوارتر از سیستم‌های مالی سنتی است. از سوی دیگر، قدرت و گستردگی رمزارزها به‌طور بالقوه امکان توسعه و اجرای سیاست‌های مالی و جنایی هوشمندانه‌تری را فراهم می‌آورد که بتوانند هم‌زمان با تسهیل تجارت قانونی، از سوءاستفاده‌های مالی آن جلوگیری کنند. اهمیت موضوع در این است که در مواجهه با این چالش‌ها، سیاست‌گذاران، نهادهای نظارتی و مجریان قانون نیازمند ابزارها و رویکردهای نوینی برای شناسایی و پیشگیری از پولشویی در فضای رمزارزها هستند. یکی از این ابزارهای نوین، یادگیری ماشینی است که به‌عنوان بخشی از هوش مصنوعی، قابلیت‌های فراوانی در تحلیل حجم عظیمی از داده‌ها، تراکنش‌ها و شناسایی الگوهای مشکوک دارد. استفاده از یادگیری ماشینی می‌تواند به‌طور قابل‌توجهی فرآیند شناسایی و پیشگیری از پولشویی در تراکنش‌های رمزارزی را بهبود بخشد و به نهادهای نظارتی این امکان را بدهد که با دقت و سرعت بیشتری فعالیت‌های مشکوک را شناسایی کرده و ارتباط آن را با اتخاذ یک سیاست جنایی مطلوب در قبال جرایمی نظیر پولشویی در حوزه رمزارزها تحلیل کنند. فقدان سیاست جنایی در این زمینه، از این حیث ضرورت ویژه به چاره‌جویی می‌طلبد که به‌رغم نپیوستن ایران به کنوانسیون‌های پالرمو و تأمین مالی تروریسم و تبعاً عدم لزوم رعایت مقررات آنها در خصوص ارزهای رمزنگاری‌شده، در صورتی که ایران تمایلی به پیوستن به این نهادها در آینده هم نداشته باشد، باز باید مقررات مربوط به

* نویسنده مسئول

پولشویی از طریق ارزهای رمزنگاری‌شده را اجرا کند و مؤسسات ارائه‌دهنده خدمات این ارزها را ملزم به اجرای این قوانین سازد [۲].

ایران نمی‌تواند به‌تنهایی و بدون همکاری‌های بین‌المللی در راستای مبارزه با پولشویی گام بردارد. مبارزه با پولشویی در ایران داستان شگفت‌انگیز و غم‌باری است که هم اصل محرمانگی را نادیده می‌گیرد و هم اصل شفافیت را به قربانگاه می‌برد [۳]. ایران، نه دارای سیاست جنایی مدل زرد (احتیاطی) نسبت به رمزارزها است، نه پیرو سیاست جنایی مدل قرمز (تحریمیِ سزاگرا) و نه هم‌داستان با سیاست جنایی مدل سبز (روادار و موافق با رمزارزها و ناجرم‌انگار) می‌باشد [۴]. در واقع، سیاست جنایی خاصی در قبال رمزارزها و جرایم ناشی یا همبسته با آنها در کشور وجود ندارد. بخشنامه مورخ بهمن‌ماه سال ۱۳۹۷ از سوی معاونت فناوری‌های نوین اداره نظام‌های پرداخت بانک مرکزی با عنوان «الزامات و ضوابط حوزه رمزارزها»، در جهت اعتبارسنجی و بیان ویژگی‌های این ارزها مقرر شده است و به لحاظ تهی‌بودن از مقررات‌گذاری محتوایی و شکلی، به معنای دقیق تقنین، از مقررات خاص، صرفاً به‌سان گزارشی از ویژگی‌های این ارزها است. در این مقاله تلاش شده است تا نقش یادگیری ماشینی در شناسایی پولشویی در تراکنش‌های رمزارزی مورد بررسی قرار گیرد. این امر به‌ویژه از آن جهت اهمیت دارد که مقالات و تحقیقات قبلی عمدتاً به مباحث فنی و فناوری پرداخته‌اند و کمتر به تحلیل‌های حقوقی، سیاست‌گذاری و قانونی در این زمینه توجه کرده‌اند. بنابراین، این پژوهش تلاش دارد تا با ارائه دیدگاهی چندجانبه، گامی در جهت تکمیل ادبیات موجود در این حوزه بردارد و به تبیین ضرورت توجه به سیاست جنایی هوشمندانه‌ای که می‌تواند از سوءاستفاده‌های مالی در حوزه رمزارزها جلوگیری کند، کمک نماید. مسئله اصلی این پژوهش به چالش‌های حقوقی، مقرراتی و فنی استفاده از یادگیری ماشینی برای شناسایی پولشویی در تراکنش‌های رمزارزی بازمی‌گردد. از یک سو، نبود قوانین جامع و استانداردهای بین‌المللی مشخص برای مقابله با پولشویی در حوزه رمزارزها و، از سوی دیگر، پیچیدگی فنی تحلیل حجم بالای داده‌های ناشناس در این تراکنش‌ها، ضرورت تدوین سیاست‌های جنایی هوشمندانه و استفاده مؤثر از فناوری‌های نوین را پررنگ‌تر کرده است. این پژوهش به دنبال پاسخ‌گویی به این چالش‌ها و ارائه راهکارهایی برای بهره‌برداری از یادگیری ماشینی در شناسایی و پیشگیری از پولشویی است. ذیل پرسش اصلی مزبور، سؤالاتی قابل طرح است که این مقاله در کندوکاو پیرامون آن‌هاست:

۱ .چگونه می‌توان قوانین و مقررات حقوقی را برای استفاده از یادگیری ماشینی در شناسایی پولشویی در تراکنش‌های رمزارزی بهبود بخشید؟

۲ .چه راهکارهای فنی برای مقابله با چالش‌های تحلیل داده‌های رمزارزی از طریق یادگیری ماشینی وجود دارد؟

۳ .چگونه سیاست‌های جنایی هوشمندانه‌ای می‌توان تدوین کرد که از فناوری یادگیری ماشینی در مقابله با پولشویی در حوزه رمزارزها بهره ببرند؟

۲- پیشینه پژوهش

خلیلی پاجی در کتاب ارزهای مجازی؛ جهانی‌شدن بزهکاری و سیاست جنایی که در نشر میزان به چاپ دوم رسیده است، جهانی‌شدن بعضی جلوه‌های بزهکاریِ مالی ارتکابی توسط مرتکبان چندملیتی به‌طور سازمان‌یافته یا در قالب گروه‌های جنایی ساختارمند را تشریح کرده و تدابیر تقنینی، قضایی و اجرایی نظام‌های سیاست جنایی در پیشگیری و مجازات جرایم رمزارزها را تبیین کرده است. در مطالعه‌ای که در «مجله کنترل پولشویی» منتشر شد، به بررسی کاربرد یادگیری ماشینی[1] برای شناسایی و مقابله با پولشویی در صرافی‌های ارزهای دیجیتال پرداختند. این تحقیق نشان داد که روش‌های فعلی برای شناسایی پولشویی ناکارآمد بوده و نیاز به بهبود دارند؛ به‌ویژه در زمینه ارزهای دیجیتال. با مقایسه چهار الگوریتم یادگیری نظارت‌شده، این مطالعه تأکید کرد که الگوریتم درخت تصمیم به‌طور خاص برای شناسایی تراکنش‌های مشکوک در صرافی‌های رمزارزی مناسب‌تر است. نتایج این پژوهش همچنین بر اهمیت توسعه فناوری‌های نوین برای مبارزه مؤثرتر با پولشویی تأکید دارد.

در پژوهشی دیگر با عنوان «تجزیه و تحلیل کلان‌داده برای پیش‌بینی رفتارهای مالی بر اساس یادگیری ماشین» نشان دادند که استفاده از الگوریتم‌های یادگیری ماشین مانند الگوریتم گرگ خاکستری می‌تولند در پیش‌بینی بحران‌های مالی و تحلیل رفتارهای اقتصادی مؤثر باشد. این مطالعه با بهره‌گیری از داده‌های ۱۳۶ شرکت بین سال‌های ۱۳۹۴ تا ۱۳۹۷ نشان داد که مدل‌های یادگیری ماشین در ترکیب با کلان‌داده می‌توانند به پیش‌بینی دقیق‌تر و سریع‌تر ورشکستگی و بحران‌های مالی کمک کنند. در مطالعه‌ای دیگر به بررسی استفاده از تکنیک‌های یادگیری ماشین و یادگیری عمیق در شناسایی و مقابله با پولشویی پرداختند. این تحقیق بر ضرورت توسعه تکنیک‌های مؤثر برای شناسایی تراکنش‌های مشکوک، به‌ویژه در حوزه رمزارزها، تأکید دارد. در این پژوهش، از مدل‌های یادگیری عمیق و یادگیری ماشین شامل شبکه عصبی عمیق[2]، جنگل تصادفی[3]، الگوریتم K نزدیک ترین همسایه[4] و بیز ساده[5] با استفاده از مجموعه‌داده بیت کوین بیضوی[6] بهره گرفته شده است. در یکی از تحقیق‌ها، به بررسی چالش‌های قانونی و مقرراتی مرتبط با استفاده از یادگیری ماشینی در شناسایی پولشویی در تراکنش‌های رمزارزی پرداختند. این مطالعه نشان داد که اگرچه الگوریتم‌های یادگیری ماشینی پتانسیل بالایی در این زمینه دارند، اما همچنان نیاز به تدوین چارچوب‌های قانونی و مقرراتی مناسب برای حمایت از استفاده گسترده از این فناوری‌ها وجود

[1] MashineLearning
[2] Deep Neural Networks
[3] Random Forest
[4] K-Nearest Neighbors
[5] Naive Bayes Classifiers
[6] Elliptic Bitcoin

دارد. این تحقیق بر اهمیت همکاری بین‌المللی برای تدوین سیاست‌های جنایی مناسب در مقابله با پولشویی تأکید کرد.

در یک مطالعه دیگر، پیشرفت‌های اخیر در به‌کارگیری الگوریتم‌های یادگیری ماشینی و تکنیک‌های داده‌کاوی برای شناسایی ناهنجاری‌ها و پولشویی در تراکنش‌های رمزارزی بررسی شده است. این پژوهش بر نظارت بر تراکنش‌ها در شبکه‌های بلاک‌چین متمرکز است و نشان می‌دهد که ترکیب روش‌های یادگیری ماشینی با تکنیک‌های تحلیل گراف می‌تواند به بهبود دقت و کارایی سیستم‌های نظارتی منجر شود. در این مطالعه، اهمیت کیفیت داده‌ها برای آموزش مدل‌های یادگیری ماشینی به‌طور ویژه مورد تأکید قرار گرفته و چالش‌ها و مسیرهای تحقیقاتی آینده در این حوزه بررسی شده است. در مقاله‌ای با عنوان «واکاوی نقش هوش مصنوعی در چرخه سیاست‌گذاری عمومی؛ رویکرد فراترکیب»، به بررسی ابعاد مختلف کاربرد هوش مصنوعی در سیاست‌گذاری عمومی پرداختند. آن‌ها دریافتند که هوش مصنوعی می‌تواند با تحلیل کلان‌داده‌ها و شناسایی الگوهای موجود، به اولویت‌بندی مسائل و تدوین سیاست‌های مبتنی بر شواهد کمک کند. با این حال، چالش‌های اخلاقی و امنیتی، از جمله موانع اصلی در استفاده گسترده از این فناوری در این حوزه به شمار می‌روند.

تحقیقات گذشته نشان می‌دهد که استفاده از یادگیری ماشینی در شناسایی و پیشگیری از پولشویی توسط رمزارزها به سرعت در حال توسعه است و پیشرفت‌های فنی مهمی در این زمینه رخ داده است. اما این مطالعات بیشتر بر جنبه‌های فنی تمرکز داشته و کمتر به ابعاد حقوقی و سیاست‌گذاری مرتبط با این فناوری‌ها پرداخته‌اند. این مقاله با هدف پر کردن این خلأ، بر ارتباط میان سیاست جنایی و استفاده از یادگیری ماشینی در مقابله با پولشویی توسط رمزارزها تأکید دارد و نشان می‌دهد که رویکردی چندجانبه، شامل توجه به قوانین و سیاست‌گذاری، ضروری است. در این پژوهش، نقش یادگیری ماشینی در شناسایی پولشویی در تراکنش‌های رمزارزی و ارتباط آن با سیاست جنایی در پیشگیری از این جرم مورد بررسی قرار گرفته است. برای این منظور، از روش‌های پژوهش توصیفی و تحلیل محتوا استفاده شده است. این روش‌ها، با تکیه بر منابع کتابخانه‌ای و پایگاه‌های اطلاعاتی معتبر علمی، امکان تحلیل جامع و دقیق موضوع را فراهم می‌کنند. این پژوهش با اتخاذ رویکردی بین‌رشته‌ای، به ترکیب تحلیل‌های حقوقی و فنی پرداخته است. تأثیرات و کاربردهای فناوری یادگیری ماشینی در زمینه شناسایی پولشویی، نه‌تنها از منظر فنی بلکه از دیدگاه حقوقی و سیاست‌گذاری نیز مورد بررسی قرار گرفته است. کارایی و قابلیت‌های این فناوری در پیشگیری از پولشویی، چالش‌ها و فرصت‌های موجود در این زمینه و تأثیرات آن بر سیاست‌های جنایی نیز ارزیابی شده‌اند. در این بین، چارچوب‌های قانونی و سیاست‌های جنایی مرتبط با استفاده از فناوری‌های نوین در مبارزه با پولشویی تحلیل شده و خلأها و چالش‌های موجود در قوانین و مقررات جاری شناسایی و پیشنهاداتی برای بهبود و تقویت سیاست‌های جنایی ارائه شده است. با وجود تلاش برای انجام یک پژوهش جامع و دقیق، برخی محدودیت‌ها در این مطالعه وجود داشته است. محدودیت‌هایی همچون دسترسی محدود به برخی منابع، تغییرات سریع در حوزه رمزارزها و یادگیری ماشینی که ممکن است برخی از یافته‌ها را تحت تأثیر قرار دهد، و تنوع قوانین و مقررات در سطح بین‌المللی که تحلیل جامع و یکپارچه را دشوار می‌سازد، از جمله چالش‌های این پژوهش بوده است.

۳- فناوری‌های شناسایی و پیشگیری وضعی از پولشویی

فناوری‌های مختلفی، به‌ویژه در دهه‌های اخیر، به‌منظور شناسایی و جلوگیری از پولشویی به‌کار گرفته شده‌اند. این فناوری‌ها شامل ابزارهای تحلیل داده، تحلیل بلاکچین، و الگوریتم‌های یادگیری ماشینی هستند که به‌طور خاص برای شناسایی الگوهای پولشویی طراحی شده‌اند. با ظهور رمزارزها و پیچیدگی‌های جدیدی که این فناوری به‌وجود آورده است، استفاده از این فناوری‌ها ضروری شده است. در ایران، با توجه به اجرای قانون مبارزه با پولشویی مصوب ۱۳۸۶ و اصلاحات آن در سال ۱۳۹۷، استفاده از فناوری‌های پیشرفته مانند یادگیری ماشینی و تحلیل بلاکچین به‌عنوان بخشی از رویکردهای نظارتی جدید مورد توجه قرار گرفته است؛ اما نبود زیرساخت‌های فنی کافی و چارچوب‌های قانونی صریح در این زمینه همچنان چالش‌های زیادی برای اجرایی شدن کامل این فناوری‌ها به همراه دارد.

۳-۱- تحلیل داده‌ها

ابزارهای تحلیل داده‌ها، به‌ویژه در نهادهای مالی و نظارتی، به‌منظور شناسایی الگوهای غیرقانونی و فعالیت‌های مشکوک به پولشویی می‌توانند بسیار مؤثر باشند. این ابزارها با استفاده از تکنیک‌هایی مانند تحلیل روند، شبیه‌سازی، و ارزیابی ریسک، به شناسایی و پیشگیری از فعالیت‌های غیرقانونی کمک می‌کنند. این ابزارها قادر به پردازش و تحلیل حجم‌های وسیع از داده‌های تراکنش هستند و می‌توانند الگوهای غیرعادی و غیرقانونی را شناسایی کنند [۵]. در ایران، پیاده‌سازی این سیستم‌ها به زیرساخت‌های پیشرفته‌تر و آموزش پرسنل نظارتی نیاز دارد تا داده‌های تراکنش‌های مالی و رمزارزی را به‌طور دقیق‌تر تحلیل کرده و الگوهای مشکوک را به‌موقع شناسایی کرد. برای مثال، با بهره‌گیری از این فناوری‌ها در نهادهای نظارتی ایران، می‌توان به کشف و پیگیری تراکنش‌های مشکوک در بانک‌ها و صرافی‌های فعال در حوزه رمزارزها پرداخت که به‌طور فعالی در فضای دیجیتال کار می‌کنند و احتمال سوءاستفاده از آن‌ها برای پولشویی وجود دارد.

۳-۲- تحلیل بلاکچین

با توجه به ویژگی‌های خاص رمزارزها و استفاده از بلاکچین به‌عنوان یک دفترکل توزیع‌شده که تراکنش‌ها را به‌صورت غیرقابل تغییر ثبت می‌کند، تحلیل بلاکچین به یکی از ابزارهای کلیدی در مبارزه با پولشویی تبدیل شده است. با استفاده از ابزارهای تحلیل بلاکچین، نهادهای نظارتی می‌توانند به‌طور دقیق‌تر تراکنش‌های مالی را نظارت کرده و مسیر پولشویی را ردیابی کنند [۶]. در ایران، با توجه به رشد سریع بازار

رمزارزها و فعالیت‌های اقتصادی که به‌طور رسمی و غیررسمی در این حوزه انجام می‌شود، استفاده از فناوری تحلیل بلاکچین می‌تواند به شناسایی تغییرات غیرعادی در تراکنش‌ها و ردیابی وجوه مشکوک کمک شایانی کند. با توجه به تأکید قوانین مبارزه با پولشویی ایران بر استفاده از فناوری‌های نوین، تحلیل بلاکچین می‌تواند به ایجاد شفافیت بیشتر و مقابله با فعالیت‌های غیرقانونی مرتبط با پولشویی در حوزه رمزارزها کمک کند.

۳-۳- الگوریتم‌های یادگیری ماشینی

یادگیری ماشینی یکی از پیشرفته‌ترین فناوری‌ها در شناسایی و پیشگیری از پولشویی است که در ایران نیز قابلیت بهره‌برداری بالایی دارد. الگوریتم‌های یادگیری ماشینی قادر به شناسایی الگوهای پیچیده و پیش‌بینی فعالیت‌های غیرقانونی بر اساس داده‌های تاریخی و تحلیل‌های پیشرفته هستند. در ایران، نهادهای نظارتی و مالی با به‌کارگیری این الگوریتم‌ها می‌توانند تراکنش‌های مشکوک را به‌طور خودکار شناسایی کرده و از پولشویی در مراحل اولیه جلوگیری کنند. با وجود این، به‌کارگیری این فناوری‌ها نیازمند توسعه زیرساخت‌های فنی و آموزشی است که تاکنون به‌طور کامل محقق نشده است. به‌طور خاص، الگوریتم‌های پیشرفته‌ای مانند «جنگل تصادفی»[1] و «ایکس‌جی‌بوست»[2] می‌توانند به شناسایی الگوهای پنهان در تراکنش‌های مالی کمک کنند؛ در بسیاری از موارد، این تراکنش‌ها مربوط به پولشویی از طریق رمزارزها هستند[۷]. در ایران، با توجه به محدودیت‌های قانونی و نظارتی، استفاده از این فناوری‌ها می‌تواند نقش مهمی در تقویت سیستم‌های نظارتی کشور ایفا کند و شناسایی دقیق‌تر و سریع‌تری از فعالیت‌های مشکوک را امکان‌پذیر کند.

۴- ارتباط یادگیری ماشینی با هوش مصنوعی

یادگیری ماشینی به‌عنوان یکی از زیرشاخه‌های کلیدی هوش مصنوعی، نقش بسیار مهمی در پیشرفت و توسعه این حوزه ایفا می‌کند. هوش مصنوعی به‌طور کلی به تلاش‌های علمی و مهندسی اطلاق می‌شود که هدف آن ساخت سیستم‌هایی است که قادر به انجام وظایف انسانی مانند تفکر، یادگیری و تصمیم‌گیری باشند. یادگیری ماشینی به‌عنوان یکی از ابزارهای اصلی برای دستیابی به اهداف هوش مصنوعی شناخته می‌شود. این فناوری به‌ویژه در زمینه‌های مختلفی از جمله "پردازش زبان طبیعی"[3]، "بینایی کامپیوتری"[4] و رباتیک به طور گسترده‌ای استفاده می‌شود [۸]. در ایران، توسعه یادگیری ماشینی به‌عنوان بخشی از فناوری‌های هوش مصنوعی برای شناسایی و پیشگیری از جرایمی نظیر پولشویی از طریق رمزارزها به‌ویژه در نهادهای نظارتی و مالی کشور، مورد نیاز است. اما چالش‌هایی چون کمبود زیرساخت‌های فنی، نبود قوانین جامع و مشکلات آموزش نیروی انسانی همچنان مانعی برای بهره‌برداری کامل از این فناوری‌ها به شمار می‌روند.

۴-۱- پردازش زبان طبیعی

پردازش زبان طبیعی یکی از زیرمجموعه‌های هوش مصنوعی است که به تحلیل و درک زبان انسانی می‌پردازد. به‌عنوان مثال، تحلیل متون مبادلات و چت‌ها در پلتفرم‌های رمزارزی می‌تواند به شناسایی فعالیت‌های مشکوک و الگوهای پولشویی کمک کند [۹]. در ایران، با توجه به توسعه روزافزون پلتفرم‌های رمزارزی و استفاده از زبان فارسی در تراکنش‌ها و مکالمات مرتبط، بهره‌گیری از پردازش زبان طبیعی می‌تواند به تحلیل متون و مکالمات مربوط به تراکنش‌های مالی کمک کند. این فناوری، به‌ویژه در شناسایی فعالیت‌های مشکوک و پولشویی در پیام‌ها و مکالمات مرتبط با تراکنش‌های رمزارزی، برای نهادهای نظارتی ایران ارزش زیادی دارد؛ به‌خصوص در شرایطی که تحلیل و رصد مکالمات و متون رمزارزی با چالش‌هایی همراه است.

۴-۲- بینایی کامپیوتری

بینایی کامپیوتری به پردازش و تحلیل تصاویر و ویدئوها می‌پردازد. هرچند کاربرد مستقیم آن در پولشویی ممکن است کمتر باشد، در ایران می‌تواند در شناسایی و تحلیل مستندات و مدارک مرتبط با تراکنش‌های رمزارزی مفید باشد [۱۰]. استفاده از این فناوری در تحلیل اسناد و مدارکی که در تراکنش‌های مشکوک ارائه می‌شود، می‌تواند برای نهادهای اجرایی و قضایی ایران کارآمد باشد و به بهبود شفافیت و دقت در ردیابی پولشویی کمک کند.

۴-۳- یادگیری عمیق

یادگیری عمیق[5]، یکی از تکنیک‌های پیشرفته یادگیری ماشینی، به‌ویژه در تحلیل داده‌های پیچیده و حجیم به‌کار می‌رود. این فناوری می‌تواند به‌طور مؤثری به بهبود دقت و کارایی سیستم‌های نظارتی کمک کند و به شناسایی سریع‌تر و مؤثرتر فعالیت‌های غیرقانونی در تراکنش‌های مالی دیجیتال منجر شود [۱۱]. در ایران، با توجه به رشد سریع تراکنش‌های رمزارزی و نبود شفافیت در برخی تراکنش‌ها، استفاده از یادگیری عمیق می‌تواند به شناسایی الگوهای غیرمعمول در تراکنش‌ها و پیش‌بینی فعالیت‌های مشکوک کمک کند. مدل‌های شبکه عصبی عمیق، به‌ویژه شبکه‌های پیچشی و بازگشتی، قادر به تحلیل داده‌های پیچیده و بزرگ‌مقیاس هستند و می‌توانند به‌طور دقیق‌تری به شناسایی پولشویی در ایران بپردازند. در شرایطی که تراکنش‌های مشکوک در

---

[1] Random Forest

[2] XGBoost (Extreme Gradient Boosting) یک الگوریتم یادگیری ماشینی است که برای شناسایی و پیشگیری از فعالیت‌های پولشویی در تراکنش‌های رمزارزی کاربرد دارد. این الگوریتم با ایجاد مدل‌های تقویتی قدرتمند و دقیق، می‌تواند الگوهای پیچیده و مخفی در داده‌ها را شناسایی کرده و به تحلیل‌های دقیق‌تر و مؤثرتری در حوزه سیاست جنایی و مبارزه با جرایم مالی کمک کند. XGBoost به‌ویژه در تحلیل داده‌های بزرگ و پیچیده مفید است و بهبود عملکرد نظارتی و اجرایی را در این زمینه ممکن می‌سازد.

[3] Natural Language Processing

[4] Computer Vision

[5] Deep Learning

بستر رمزارزها به دلیل ناشناس بودن و پیچیدگی بالایی که دارند، شناسایی آن‌ها دشوار است، یادگیری عمیق می‌تواند به حل این مشکلات کمک کند.

۴-۴- انواع الگوریتم‌های یادگیری ماشینی و کاربردهای آن‌ها

در ایران، استفاده از انواع مختلف الگوریتم‌های یادگیری ماشینی برای مقابله با جرایم مالی، نظیر پولشویی، می‌تواند بسیار مؤثر باشد. با توجه به اینکه سیستم‌های مالی و نظارتی کشور با حجم بالای تراکنش‌ها روبه‌رو هستند و بخشی از آن‌ها ممکن است به فعالیت‌های مشکوک و غیرقانونی مرتبط باشند، الگوریتم‌های یادگیری ماشینی، مانند الگوریتم‌های یادگیری تحت نظارت و بدون نظارت، می‌توانند به شناسایی الگوهای مشکوک و پیشگیری از وقوع جرایم مالی کمک کنند. این الگوریتم‌ها به‌طور کلی به سه دسته اصلی تقسیم می‌شوند:

۴-۴-۱- الگوریتم‌های یادگیری تحت نظارت

الگوریتم‌های یادگیری تحت نظارت[1] یکی از اصلی‌ترین تکنیک‌های یادگیری ماشینی هستند که برای تحلیل داده‌های برچسب‌خورده مورد استفاده قرار می‌گیرند. این الگوریتم‌ها بر اساس داده‌هایی که شامل ورودی‌ها و خروجی‌های مشخص هستند، آموزش می‌بینند تا قادر به پیش‌بینی یا طبقه‌بندی داده‌های جدید شوند [۱۲]. الگوریتم‌های یادگیری تحت نظارت می‌توانند به تحلیل داده‌های تراکنش‌های رمزارزی در ایران کمک کنند. این الگوریتم‌ها با استفاده از داده‌های تاریخی و آموزش بر روی آن‌ها، قادرند تراکنش‌های جدید را تحلیل کرده و تراکنش‌های مشکوک را شناسایی کنند. به‌ویژه در شرایطی که ایران به دنبال ارتقای سیستم‌های نظارتی مالی است، این الگوریتم‌ها می‌توانند در شناسایی و گزارش‌دهی تراکنش‌های غیرقانونی به مقامات نظارتی نقش مهمی ایفا کنند.

۴-۴-۲- الگوریتم‌های یادگیری بدون نظارت

الگوریتم‌های یادگیری بدون نظارت[2] یکی از مهم‌ترین ابزارهای یادگیری ماشینی هستند که برای تحلیل داده‌های بدون برچسب و کشف ساختارهای پنهان در داده‌ها طراحی شده‌اند. برخلاف الگوریتم‌های یادگیری تحت نظارت که با داده‌های برچسب‌خورده کار می‌کنند، این الگوریتم‌ها به دنبال شناسایی الگوها و ساختارهای داخلی داده‌ها بدون نیاز به اطلاعات قبلی در مورد دسته‌بندی داده‌ها هستند. در زمینه پولشویی از طریق رمزارزها، این الگوریتم‌ها می‌توانند به شناسایی الگوهای غیرمعمول و فعالیت‌های مشکوک کمک کنند. برخی از مهم‌ترین الگوریتم‌های یادگیری بدون نظارت به شرح زیر است:

۴-۴-۳- تحلیل مؤلفه‌های اصلی

تحلیل مؤلفه‌های اصلی[3] یکی از تکنیک‌های کاهش ابعاد داده است که به شناسایی ویژگی‌های اصلی و مهم در داده‌های چندبعدی کمک می‌کند. این تکنیک می‌تواند در ایران برای شناسایی الگوهای غیرمعمول و کاهش پیچیدگی داده‌های تراکنش‌های رمزارزی مؤثر باشد. این ابزار با فشرده‌سازی داده‌ها و استخراج ویژگی‌های اصلی، به مقامات نظارتی کمک می‌کند تا با دقت بیشتری تراکنش‌های مشکوک را شناسایی کنند. با توجه به حجم بالای داده‌های مالی و تراکنش‌های انجام‌شده در ایران، استفاده از تحلیل مؤلفه‌های اصلی می‌تواند به شناسایی دقیق‌تر در زمینه پولشویی از طریق رمزارزها کمک شایانی کند.

۵- بسترمندی رمزارزها برای ارتکاب پولشویی

پولشویی به مجموعه‌ای از فرایندها و اقداماتی اطلاق می‌شود که به‌منظور تبدیل درآمدهای حاصل از فعالیت‌های غیرقانونی به منابع مالی که به نظر قانونی و مشروع می‌آیند، به‌کار گرفته می‌شود. این فرایند معمولاً شامل چندین مرحله است که هر یک به نوعی به پنهان‌سازی و توجیه منشأ واقعی وجوه کمک می‌کند. با ظهور فناوری‌های جدید و رمزارزها، این فرایند پیچیده‌تر و متنوع‌تر شده است. در پولشویی دیجیتال، رمزارزها و فناوری بلاکچین به‌ویژه به دلیل ویژگی‌هایی نظیر ناشناسی نسبی و عدم نیاز به واسطه‌های سنتی، زمینه‌های جدیدی برای پولشویی فراهم کرده‌اند. این شامل استفاده از صرافی‌های رمزارز، انتقال وجوه بین کیف‌پول‌های دیجیتال و استفاده از فناوری‌های مخفی‌کننده تراکنش‌ها مانند میکسرها و توکن‌های ناشناس است. پولشویی از طریق رمزارزها به‌ویژه به دلیل ویژگی‌های خاص این فناوری‌ها، نیازمند تکنیک‌های پیچیده و نوآورانه است که به بررسی و تحلیل دقیق الگوهای تراکنش‌ها و فعالیت‌های مشکوک در شبکه‌های غیرمتمرکز می‌پردازد. در ایران، با توجه به رشد سریع استفاده از رمزارزها و نبود قوانین جامع در این زمینه، استفاده از این فناوری برای پولشویی به یکی از نگرانی‌های اصلی نهادهای نظارتی تبدیل شده است. نهادهای نظارتی کشور باید زیرساخت‌ها و چارچوب‌های قانونی جدیدی را برای مقابله با پولشویی از طریق رمزارزها تدوین کنند.

۵-۱- ویژگی‌های رمزارزها و سختی‌های پیشگیری وضعی از آنها در مهار پولشویی

رمزارزها ویژگی‌های خاصی دارند که آن‌ها را به ابزارهایی جذاب برای پول‌شویان تبدیل می‌کند. در ایران، چالش‌های خاصی برای مقابله با پولشویی از طریق رمزارزها وجود دارد که شامل ضعف زیرساخت‌های نظارتی، نبود چارچوب قانونی صریح و همچنین مشکلات بین‌المللی مرتبط با تحریم‌ها و محدودیت‌های جهانی است. ویژگی‌هایی مانند

[1] Supervised Learning Algorithms.
[2] Unsupervised Learning Algorithms.
[3] Principal Component Analysis

ناشناس بودن، غیرمتمرکز بودن و حجم بالای تراکنش‌ها، شناسایی هویت کاربران و ردیابی منشأ وجوه غیرقانونی را دشوار و نظارت بر تراکنش‌ها را پیچیده‌تر می‌سازند. به‌ویژه، ناشناس بودن تراکنش‌ها و عدم وجود نهاد مرکزی، غیرمتمرکز بودن بلاکچین و امکان انجام تراکنش‌های جهانی بدون واسطه‌های بانکی سنتی، مشکلات زیادی برای نهادهای نظارتی به‌وجود آورده است. حجم بالای تراکنش‌ها نیز به پول‌شویان کمک می‌کند تا به‌سرعت و در مقیاس بزرگ وجوه را جابجا کنند. این چالش‌ها نیاز به سیاست‌گذاری‌ها، رهیافت‌های جدید و فناوری‌های نوین مانند الگوریتم‌های یادگیری ماشینی و ابزارهای تحلیل بلاکچین را ضروری می‌کند. در حالی که قانون مبارزه با پولشویی ایران مصوب ۱۳۸۶ و اصلاحات آن در سال ۱۳۹۷ بر اهمیت استفاده از فناوری‌های نوین تأکید کرده‌اند، اما همچنان چالش‌های فنی و نظارتی برای مقابله با پولشویی از طریق رمزارزها وجود دارد. نهادهای نظارتی ایران باید از فناوری‌های پیشرفته مانند یادگیری ماشینی و تحلیل بلاکچین برای افزایش دقت در نظارت بر تراکنش‌های رمزارزی استفاده کنند و با تقویت همکاری‌های بین‌المللی، به شناسایی بهتر جرایم مالی بپردازند.

۵-۲- روش‌های متداول پولشویی در فضای رمزارز

پولشویی در فضای رمزارز از تکنیک‌ها و روش‌های متنوعی بهره می‌برد که برای پنهان‌سازی منشأ وجوه غیرقانونی طراحی شده‌اند. در ایران، عدم وجود زیرساخت‌های نظارتی کافی و ضعف در اجرای دقیق قوانین ضد پولشویی[1] و شناخت مشتری[2] در برخی صرافی‌های داخلی، این مشکل را تشدید می‌کند. روش‌هایی که پول‌شویان از آن‌ها بهره می‌برند، شامل تراکنش‌های پیچیده و استفاده از رمزارزهای با حریم خصوصی بالاست برخی از این روش‌ها عبارتند از:

۵-۲-۱- تراکنش‌های پیچیده

پول‌شویان از تراکنش‌های پیچیده برای پنهان‌سازی منشأ پول‌های غیرقانونی استفاده می‌کنند. در ایران، با توجه به رشد استفاده از رمزارزها و نبود نهادهای نظارتی تخصصی در این زمینه، تراکنش‌های مکرر و پیچیده رمزارزها بین صرافی‌های داخلی و خارجی می‌تواند به راحتی وجوه غیرقانونی را در شبکه رمزارزی پنهان کند. نهادهای نظارتی کشور باید با بهره‌گیری از فناوری‌های نوین مانند الگوریتم‌های یادگیری ماشینی و همکاری با نهادهای بین‌المللی، تراکنش‌های پیچیده را به‌طور دقیق‌تر شناسایی کنند و مانع از گسترش فعالیت‌های پولشویی شوند [۱۳].

۵-۲-۲- صرافی‌های رمزارز با ضوابط ضعیف

در ایران، صرافی‌های رمزارز با ضوابط ضعیف، به یکی از چالش‌های اصلی در مقابله با پولشویی تبدیل شده‌اند. برخی از این صرافی‌ها به‌دلیل عدم تمایل یا توانایی در اجرای دقیق قوانین ضد پولشویی و شناخت مشتری، به محلی جذاب برای پول‌شویان تبدیل شده‌اند. این صرافی‌ها امکان انجام تراکنش‌های ناشناس و غیرقانونی را فراهم می‌کنند و می‌توانند به‌راحتی وجوه غیرقانونی را تبدیل و انتقال دهند. برای مقابله با این چالش، نهادهای نظارتی ایران باید مقررات جدیدی را برای نظارت دقیق‌تر بر صرافی‌های رمزارز داخلی وضع کنند و از فناوری‌هایی مانند یادگیری ماشینی برای شناسایی فعالیت‌های مشکوک استفاده کنند.

۵-۲-۳- استفاده از رمزارزهای با حریم خصوصی بالا

استفاده از رمزارزهای با حریم خصوصی بالا یکی از روش‌های پیشرفته پولشویی در فضای رمزارزها محسوب می‌شود. برخی رمزارزها به دلیل ویژگی‌های قوی در حفظ حریم خصوصی، جذابیت ویژه‌ای برای پول‌شویان دارند. این رمزارزها از تکنیک‌های پیچیده‌ای مانند «امضای حلقوی»[3]، «آدرس‌های مخفی»[4] و پروتکل‌های «اثبات بدون افشا»[5] استفاده می‌کنند تا اطلاعات مربوط به تراکنش‌ها، از جمله هویت فرستنده و گیرنده و میزان تراکنش‌ها، را به‌طور کامل مخفی نگه دارند. این قابلیت‌ها شناسایی و ردیابی تراکنش‌ها را برای نهادهای نظارتی و اجرای قانون به‌مراتب دشوارتر می‌کند [۱۴]. پرونده«Alpha Bay» ، که یکی از بزرگ‌ترین بازارهای غیرقانونی در دارک وب بود و در سال ۲۰۱۷ توسط نیروهای اجرای قانون تعطیل شد، نمونه‌ای بارز از استفاده گسترده از مونرو برای پولشویی است «Alpha Bay» .ابتدا از بیت‌کوین به‌عنوان ارز اصلی استفاده می‌کرد، اما با افزایش آگاهی از قابلیت‌های ردیابی بیت‌کوین، بسیاری از کاربران به رمزارز مونرو روی آوردند تا تراکنش‌های خود را به‌صورت کاملاً ناشناس انجام دهند. تحقیقات نشان داد که حجم قابل‌توجهی از تراکنش‌های مرتبط با مواد مخدر و سایر فعالیت‌های غیرقانونی در «Alpha Bay» از طریق مونرو انجام می‌شد. این امر تلاش‌های نهادهای اجرای قانون برای شناسایی و پیگیری مجرمان را به‌شدت پیچیده کرد[۱۵]. در ایران، عدم وجود زیرساخت‌های فنی کافی برای شناسایی و ردیابی این نوع رمزارزها، به پول‌شویان اجازه می‌دهد تا از رمزارزهایی مانند مونرو و زی‌کش برای پنهان‌سازی وجوه خود استفاده کنند. پرونده‌هایی نظیر «Alpha Bay» نشان داده‌اند که چگونه این نوع رمزارزها می‌توانند به‌طور مؤثر برای پولشویی مورد استفاده قرار گیرند. نهادهای نظارتی ایران باید از ابزارهای پیشرفته‌تری

---

[1] Anti-Money Laundering
[2] Know Your Customer
۳ - امضاهای حلقه (Ring Signatures) تکنیکی برای حفظ ناشناسی در تراکنش‌ها است که در رمزارزهایی مانند مونرو استفاده می‌شود. این روش به کاربران اجازه می‌دهد تا بدون فاش کردن هویت خود، تراکنش‌ها را امضا کنند، که این امر شناسایی منشأ وجوه غیرقانونی را دشوارتر کرده و چالش‌هایی برای نظارت و پیشگیری از پولشویی ایجاد می‌کند.

[4] Stealth Addresses
۵ - مدل‌های اثبات بدون افشا (Zero-Knowledge Proofs) تکنیکی است که به کاربران این امکان را می‌دهد که صحت اطلاعات را بدون فاش کردن جزئیات آن‌ها اثبات کنند. در زمینه رمزارزها، این روش می‌تواند برای پنهان‌سازی جزئیات تراکنش‌ها و محافظت از حریم خصوصی استفاده شود، اما همچنین می‌تواند مشکلاتی را برای نهادهای نظارتی در شناسایی و پیشگیری از پولشویی به همراه داشته باشد.

برای تحلیل و شناسایی این نوع تراکنش‌ها استفاده کنند و از همکاری‌های بین‌المللی برای مقابله با استفاده از رمزارزهای با حریم خصوصی بالا بهره‌برداری کنند.

۶- نقش یادگیری ماشینی در مبارزه با پولشویی

یادگیری ماشینی، مانند بسیاری از فناوری‌های نوین، می‌تواند به‌عنوان یک تیغ دولبه عمل کند؛ هم در تسهیل ارتکاب جرایم مالی نظیر پولشویی و هم در شناسایی و مبارزه با این جرایم. در ایران، با توجه به گسترش استفاده از رمزارزها و فقدان چارچوب‌های قانونی صریح در این زمینه، یادگیری ماشینی به‌عنوان ابزاری قدرتمند می‌تواند به نهادهای نظارتی کشور در شناسایی و پیشگیری از پولشویی کمک کند. اما در این مسیر، چالش‌هایی مانند نبود زیرساخت‌های فنی و آموزشی و همچنین نیاز به تدوین قوانین جدید باید برطرف شوند. در ادامه به برخی از مدل‌های پرکاربرد یادگیری ماشینی در این زمینه و نقش آن‌ها در شناسایی پولشویی پرداخته می‌شود:

۶-۱- رگرسیون لجستیک

رگرسیون لجستیک[1] یکی از مدل‌های پرکاربرد در یادگیری ماشینی است که برای پیش‌بینی احتمال وقوع رویدادهایی مانند پولشویی استفاده می‌شود. این مدل با تحلیل داده‌ها و ویژگی‌های تراکنش‌ها و رفتار کاربران، به شناسایی و پیش‌بینی پولشویی کمک می‌کند [۷]. در پرونده «بیتفینکس»[2] در سال ۲۰۱۶، که طی یک حمله هکری ۱۲۰،۰۰۰ رمزارز از نوع بیت‌کوین به سرقت رفت، از رگرسیون لجستیک برای شناسایی تراکنش‌های مشکوک استفاده شد [۱۶]. این مدل با تحلیل ویژگی‌هایی مانند حجم و فرکانس تراکنش‌ها و الگوهای رفتاری کاربران، توانست تراکنش‌های مشکوک مرتبط با پولشویی را شناسایی کند. در ایران، با وجود اصلاحات قانون مبارزه با پولشویی در سال ۱۳۹۷، نهادهای مالی و نظارتی همچنان نیازمند استفاده از مدل‌های یادگیری ماشینی نظیر رگرسیون لجستیک برای شناسایی و تحلیل تراکنش‌های مشکوک در سیستم‌های مالی کشور هستند.

۶-۲- درختان تصمیم

درختان تصمیم[3] در یادگیری ماشینی به‌عنوان یکی از ابزارهای قدرتمند برای طبقه‌بندی و تصمیم‌گیری شناخته می‌شوند. این مدل‌ها بر اساس ویژگی‌های داده‌ها، تصمیمات و پیش‌بینی‌هایی را به‌طور سیستماتیک و بصری انجام می‌دهند. درختان تصمیم به‌ویژه در شناسایی الگوهای پیچیده و قوانینی که ممکن است به پولشویی مربوط شوند، بسیار مؤثرند. در ایران، با توجه به اینکه رمزارزها به‌عنوان ابزاری برای پولشویی مورد استفاده قرار می‌گیرند، استفاده از درختان تصمیم در نهادهای نظارتی کشور می‌تواند به تحلیل دقیق‌تر داده‌های مالی و ردیابی تراکنش‌های مشکوک کمک کند. نهادهای نظارتی در ایران باید با بهره‌گیری از این مدل‌ها، توانایی خود را در شناسایی و پیشگیری از پولشویی تقویت کنند.

۶-۳- کاربرد درختان تصمیم در شناسایی پولشویی

درختان تصمیم با تقسیم داده‌ها به زیرمجموعه‌های کوچک‌تر و تحلیل ویژگی‌های مختلف مانند مقدار تراکنش‌ها، زمان و فرکانس، به شناسایی الگوهای غیرعادی و رفتارهای مشکوک کمک می‌کنند. در پرونده «کوین‌چک»[4]، یکی از بزرگ‌ترین صرافی‌های رمزارز ژاپن که در سال ۲۰۱۸ مورد حمله هکری قرار گرفت و ۵۰۰ میلیون دلار از رمزارز «نم» به سرقت رفت، از درختان تصمیم برای شناسایی الگوهای مشکوک استفاده شد. این مدل‌ها تراکنش‌هایی با مقادیر غیرمعمول بالا و از آدرس‌های ناشناخته را شناسایی کردند که به نهادهای نظارتی در بهبود توانایی شناسایی پولشویی کمک کرد. استفاده از درختان تصمیم در تحلیل داده‌های رمزارزها، نقش مهمی در تقویت امنیت و شفافیت دارد و به نهادهای نظارتی در اقدامات پیشگیرانه و واکنش سریع به فعالیت‌های مشکوک کمک می‌کند.

۶-۴- جنگل تصادفی

جنگل تصادفی تکنیکی پیشرفته در یادگیری ماشینی است که برای تحلیل داده‌های پیچیده و شناسایی الگوهای ناهنجار، از جمله در زمینه پیشگیری از پولشویی، کاربرد دارد. این مدل با استفاده از مجموعه‌ای از درختان تصمیم، توانایی پیش‌بینی و تحلیل را با ترکیب نتایج درختان تصادفی افزایش داده و خطر «اورفیتینگ» را کاهش می‌دهد. در حوزه پیشگیری از جرایم مالی نظیر پولشویی توسط رمزارزها، جنگل تصادفی به‌ویژه در شناسایی تراکنش‌های مشکوک بسیار مفید است. برای مثال، «بایننس»، یکی از بزرگ‌ترین صرافی‌های رمزارز، در سال ۲۰۱۸ از جنگل تصادفی برای تحلیل تراکنش‌های کاربران استفاده کرد. این تکنیک به شناسایی الگوهای غیرعادی و مشکوک، مانند تراکنش‌های مکرر و حجم بالای مبالغ که ممکن است به پولشویی توسط رمزارزها مرتبط باشند، کمک کرد [۱۱]. در ایران، با توجه به رشد تراکنش‌های رمزارزی و چالش‌های ناشی از نبود زیرساخت‌های نظارتی قوی، استفاده از جنگل تصادفی می‌تواند به شناسایی تراکنش‌های مشکوک در صرافی‌ها و دیگر نهادهای مالی کمک کند. این تکنیک به نهادهای مالی ایران امکان می‌دهد تا تراکنش‌های غیرعادی را به‌طور دقیق‌تر شناسایی کنند و از پیشرفت فعالیت‌های پولشویی جلوگیری کنند. در مقام تبیین مزایای استفاده از جنگل تصادفی باید گفت این شیوه

---

[1] Categorical Data

۲ - صرافی Bitfinex کی از بزرگ‌ترین و شناخته‌شده‌ترین صرافی‌های رمزارز در جهان است که در سال ۲۰۱۲ تأسیس شد و به‌طور ویژه به دلیل حجم بالای معاملات و امکانات پیشرفته‌اش برای معامله‌گران حرفه‌ای شهرت دارد. این صرافی در مدت زمان فعالیت خود با برخی چالش‌ها و مسائل امنیتی مواجه شده است که توجهات زیادی را جلب کرده است.

[3] Decision Trees

[4] Coin check

شـــامل دقت بـالا، پیشـــگیری از «اورفیتینـگ»[1] و توانـایی تحلیـل ناهنجاری‌ها اســت. با توجه به این ویژگی‌ها، جنگل تصـــادفی به‌عنوان یک ابزار مؤثر در شـــناســـایی پولشـــویی و تحلیل داده‌های پیچیده در زمینه رمزارزها شناخته می‌شود. این تکنیک با قابلیت‌های خود، به‌طور مؤثری در نظارت و مبارزه با پولشـــویی در صـــرافی‌های رمزارز و دیگر نهادهای مالی دیجیتال به کار گرفته می‌شـود و به شـناسـایی الگوهای غیرعادی و پیش‌بینی فعالیت‌های مشکوک کمک می‌کند.

۶-۵- ماشین‌های بردار پشتیبان

ماشـــین‌های بردار پشـــتیبان[2] ابزارهای مؤثری در یادگیری ماشـــینی هســـتند که برای طبقه‌بندی داده‌ها و تحلیل الگوهای پیچیده به کار می‌روند. این مـدل‌هـا بـا ایجـاد مرزهـای تصـــمیم‌گیری برای تفکیـک کلاس‌ها، قادر به شناسایی ناهنجاری‌ها و الگوهای پیچیده در داده‌ها، از جمله تراکنش‌های مشـکوک و پولشـویی هسـتند. در پرونده مرتبط با صـــرافی رمزارز «BTC-e»، این ماشـــین‌ها به‌عنوان ابزار کلیدی برای شناسایی و تحلیل تراکنش‌های غیرقانونی استفاده شدند. در سال‌های ۲۰۱۷ و ۲۰۱۸، صـــرافی «BTC-e» به دلیل ارتباط با فعالیت‌های پولشـــویی تحت تحقیق قرار گرفت و تحلیلگران بـا بهره‌گیری از ماشـــین‌های بردار پشـــتیبان توانســـتند تراکنش‌های غیرعادی، از جمله تراکنش‌هـای بزرگ و مکرر کـه ممکن بود نشـــانـه‌هـایی از عملیـات پولشـویی باشـند، شـناسـایی کنند [۱۷]. مزایای این تکنیک شامل دقت بالا، توانایی تحلیل داده‌های با ابعاد بالا و شـــناســـایی الگوهای پیچیده اسـت. این ویژگی‌ها ماشـین‌های بردار پشـتیبان را به ابزاری ارزشـمند برای نهادهای نظارتی تبدیل کرده اســـت، به‌ویژه در پیشـــگیری از پولشـــویی و تحلیل فعالیت‌های مالی غیرقانونی در فضـــای رمزارزها. در ایران، نهادهای نظارتی می‌توانند از ماشـــین‌های بردار پشـــتیبان برای شـــنـاســـایی تراکنش‌های غیرعادی اســـتفاده کنند و از آن در تحلیل تراکنش‌های مشـــکوک در فضـــای رمزارزها بهره ببرند. با توجه به پیچیدگی‌های موجود در فضـای مالی ایران و اسـتفاده‌های غیرقانونی از رمزارزها، این مدل می‌تواند به پیشگیری از پولشویی کمک کند.

۶-۶- شبکه‌های پیچشی گراف

شبکه‌های پیچشی گراف[3] مدل‌های پیشرفته در یادگیری ماشینی هستند که به‌ویژه برای تحلیل داده‌های گراف و شبکه‌های پیچیده، نظیر تراکنش‌های رمزارز و روابط بین کاربران، کاربرد دارند. این مدل‌ها با استفاده از تکنیک‌های پیچشی برای داده‌های گراف، قادرند الگوهای مخفی و ساختارهای پیچیده را شبیه‌سازی و تحلیل کنند. به‌عبارت دیگر، این شبکه‌های پیچشی گراف برای پردازش داده‌های ساختاریافته به شکل گراف طراحی شده‌اند و می‌توانند روابط بین نودها (کاربران، تراکنش‌ها و غیره) را به‌طور دقیق بررسی کنند. یکی از ویژگی‌های مهم این شبکه‌ها توانایی در شناسایی الگوهای پیچیده و روابط پنهان است که به شناسایی فعالیت‌های غیرعادی و پولشویی کمک می‌کند. در ایران، استفاده از شبکه‌های پیچشی گراف می‌تواند به نهادهای نظارتی کمک کند تا الگوهای مخفی و روابط پیچیده بین تراکنش‌های رمزارزی و کاربران را شناسایی کنند. این مدل‌ها به نهادهای امنیتی ایران امکان می‌دهند که فعالیت‌های غیرعادی و پولشویی را با دقت بیشتری شناسایی و پیگیری کنند.

۷- تحلیل مزایا و معایب استفاده از یادگیری ماشینی در مهار پولشویی با رمزارزها

۷-۱- مزایا

در تحلیل پولشویی از طریق رمزارزها، استفاده از یادگیری ماشینی، به‌ویژه به‌دلیل مزایای متعدد آن در دقت و کارایی، توانایی یادگیری از داده‌های جدید و کاهش نیاز به نظارت سنتی و دستی، به ابزاری قدرتمند در این زمینه تبدیل شده است. این تکنیک‌ها می‌توانند در شناسایی فعالیت‌های غیرقانونی پیچیده و الگوهای مخفی، به‌ویژه در زمینه وقوع جرم پولشویی توسط رمزارزها که دارای حجم بالای داده‌ها و پیچیدگی‌های ساختاری هستند، به‌طور مؤثری عمل کنند. یکی از مزایای بارز یادگیری ماشینی، دقت و کارایی بالای آن در تحلیل داده‌های پیچیده است. مدل‌های پیشرفته‌ای مانند شبکه‌های عصبی و شبکه‌های پیچشی گراف به‌طور ویژه برای شناسایی الگوهای پیچیده و ناهنجاری‌های پنهان طراحی شده‌اند. این مدل‌ها به تحلیل دقیق‌تر روابط پیچیده بین ویژگی‌های تراکنش‌ها و شبیه‌سازی فعالیت‌های غیرقانونی نظیر پولشویی کمک کردند. توانایی یادگیری از داده‌های جدید، مزیت دیگر یادگیری ماشینی است. مدل‌های یادگیری ماشینی می‌توانند با دریافت داده‌های تازه و به‌روز، به‌طور مداوم بهبود یابند و نتایج دقیق‌تری ارائه دهند. این ویژگی، به‌ویژه در دنیای رمزارزها که الگوهای فعالیت ممکن است به‌سرعت تغییر کنند، بسیار ارزشمند است. برای مثال، در مورد تحلیل تراکنش‌های مرتبط با صرافی‌های بزرگ مانند «Binance»، مدل‌های یادگیری ماشینی قادر بودند با پردازش داده‌های جدید و تحلیل الگوهای به‌روز، به شناسایی فعالیت‌های مشکوک و پولشویی کمک کنند. علاوه بر این، استفاده از یادگیری ماشینی می‌تواند نیاز به نظارت دستی و تحلیل‌های انسانی را کاهش دهد. در پردازش داده‌های بزرگ و پیچیده، این تکنیک‌ها به‌طور خودکار قادر به شناسایی ناهنجاری‌ها و فعالیت‌های غیرقانونی هستند، به‌ویژه در مواقعی که حجم داده‌ها بسیار زیاد است، می‌تواند مفید واقع شود. این قابلیت باعث می‌شود که تحلیلگران بتوانند بر روی بررسی‌های استراتژیک و

---

[1] خطر اورفیتینگ (Overfitting) زمانی رخ می‌دهد که یک مدل یادگیری ماشینی به حدی به داده‌های آموزشی خود تطابق پیدا می‌کند که قادر به تعمیم خوب به داده‌های جدید نباشد. به عبارت دیگر، مدل به جزئیات و نویزهای خاص داده‌های آموزشی به شدت وابسته می‌شود و از الگوهای عمومی و واقعی که در داده‌های جدید نیز وجود دارد، غفلت می‌کند.

[2] Support vector machines

[3] Convolutional Neural Network

تصمیم‌گیری‌های کلیدی تمرکز کنند، در حالی که مدل‌های یادگیری ماشینی به‌طور خودکار داده‌ها را تحلیل و گزارش‌های مورد نیاز را تولید می‌کنند [۱۲]. به‌طور کلی، استفاده از یادگیری ماشینی در شناسایی پولشویی از طریق رمزارزها، با بهره‌گیری از دقت بالا، توانایی یادگیری از داده‌های جدید و کاهش نیاز به نظارت دستی، توانسته است به‌طور قابل توجهی در بهبود فرآیندهای تحلیل و شناسایی فعالیت‌های غیرقانونی کمک کند. این تکنیک‌ها، اگرچه به همراه چالش‌هایی هستند، اما همچنان به‌عنوان ابزارهای مؤثری در مبارزه با پولشویی و فعالیت‌های غیرقانونی در دنیای دیجیتال شناخته می‌شوند.

۷-۲- معایب و چالش‌های فنی-حقوقی

توسعه و پیاده‌سازی مدل‌های یادگیری ماشینی برای شناسایی پولشویی از طریق رمزارزها، علی‌رغم مزایای زیادی که دارد، با چالش‌های قابل‌توجهی نیز همراه است. این چالش‌ها شامل پیچیدگی و هزینه، احتمال اورفیتینگ و مسائل مربوط به تفسیرپذیری می‌شود که در ادامه به تفصیل مورد بررسی قرار می‌گیرد. یکی از مشکلات اصلی در استفاده از مدل‌های یادگیری ماشینی در زمینه شناسایی عملیات جرم پولشویی، پیچیدگی و هزینه‌های بالای آن است. توسعه و پیاده‌سازی این مدل‌ها نیازمند منابع محاسباتی گسترده و تخصص در زمینه‌های مربوط به یادگیری ماشینی و تحلیل داده‌ها است. دیگر چالش مهم در این زمینه، احتمال اورفیتینگ مدل‌های موجود در یادگیری ماشینی است. اورفیتینگ به وضعیتی اشاره دارد که در آن مدل یادگیری ماشینی به‌طور بیش از حد به داده‌های آموزشی تطبیق می‌یابد و در نتیجه عملکرد آن در مواجهه با داده‌های جدید کاهش می‌یابد [۹]. در ایران، هزینه‌های بالای پیاده‌سازی این فناوری یکی از موانع اصلی است. در زمینه شناسایی جرم پولشویی، این موضوع می‌تواند به‌ویژه مشکل‌ساز باشد. به‌عنوان مثال، در استفاده از شبکه‌های عصبی عمیق برای تحلیل الگوهای پولشویی، این مدل‌ها ممکن است به‌طور خاص با داده‌های آموزشی خود تطبیق یابند و نتایج نادرستی در داده‌های واقعی ارائه دهند. این موضوع می‌تواند بر دقت و قابلیت اعتماد مدل‌ها تأثیر بگذارد و نیازمند استراتژی‌های مناسب برای تنظیم و ارزیابی مدل‌ها باشد.

علاوه بر این، مسائل مربوط به تفسیرپذیری نیز یکی از چالش‌های بزرگ در استفاده از مدل‌های یادگیری ماشینی است. بسیاری از مدل‌های پیچیده مانند شبکه‌های عصبی عمیق، به‌دلیل ساختار پیچیده و تعداد بالای پارامترها، به‌سختی قابل تفسیر هستند. این مسئله می‌تواند در تحلیل و توضیح نتایج به نهادهای نظارتی مشکل‌ساز باشد. برای مثال، در پرونده مربوط به استفاده از مدل‌های یادگیری ماشینی برای شناسایی پولشویی در صرافی«Bitfinex» ، تحلیلگران با مشکل توضیح و تفسیر دقیق نتایج مدل‌های پیچیده مواجه شدند. این مسئله، به‌ویژه زمانی که نتایج مدل باید به مقامات نظارتی ارائه شود و نیاز به توضیحات شفاف و قابل‌فهم دارد، می‌تواند چالش‌برانگیز باشد [۹]. در نتیجه، استفاده از یادگیری ماشینی در شناسایی پولشویی از طریق رمزارزها، با وجود مزایای چشمگیر آن، نیازمند توجه به چالش‌های مرتبط با پیچیدگی و هزینه‌های توسعه، احتمال اورفیتینگ و مسائل تفسیرپذیری است. این چالش‌ها باید به‌دقت مدیریت شوند تا بتوان از این تکنیک‌های پیشرفته به‌طور مؤثر در مبارزه با پولشویی و فعالیت‌های غیرقانونی در حوزه رمزارزها بهره‌برداری کرد. پیاده‌سازی الگوریتم‌های یادگیری ماشینی در حوزه مبارزه با پولشویی، با وجود پتانسیل‌های بالا، با چالش‌های فنی و اجرایی متعددی روبه‌روست:

۱. پیاده‌سازی الگوریتم‌های یادگیری ماشینی به‌عنوان یکی از ابزارهای نوین در مقابله با پولشویی در تراکنش‌های رمزارزی، با چالش‌های فنی و اجرایی مختلفی مواجه است. یکی از مهم‌ترین این چالش‌ها، نیاز به داده‌های با حجم و کیفیت بالاست. کیفیت داده‌ها به‌طور مستقیم بر دقت مدل‌های یادگیری ماشینی تأثیر می‌گذارد. داده‌های ناقص یا نادرست می‌توانند منجر به نتایج غیرقابل‌اعتماد شوند، چنان‌که در پرونده صرافی «BTC-e» مشاهده شد [۱۸]. در ایران، یکی از بزرگ‌ترین چالش‌ها، کیفیت داده‌ها است. برای پیاده‌سازی یادگیری ماشینی به داده‌های با کیفیت و جامع نیاز است، اما داده‌های موجود در نهادهای مالی و نظارتی کشور ممکن است ناقص یا نادرست باشند. برای مثال، در پرونده‌های مرتبط با صرافی‌های رمزارز در کشور، نقص در داده‌های مربوط به تراکنش‌ها می‌تواند به شناسایی نادرست فعالیت‌های مشکوک منجر شود و باعث سردرگمی نهادهای نظارتی گردد. این امر بر ضرورت ارتقای کیفیت داده‌ها و زیرساخت‌های داده‌ای در کشورهایی چون ایران تأکید دارد. از سوی دیگر، یکی از چالش‌های عمده در حوزه استفاده از یادگیری ماشینی برای شناسایی پولشویی، نیاز به انطباق مداوم مدل‌ها با تغییرات مستمر در روش‌های پولشویی است. پول‌شویان همواره تکنیک‌های جدید و پیچیده‌تری را به‌کار می‌گیرند تا از سیستم‌های نظارتی عبور کنند [۱۲].

۲. علاوه بر این، الگوریتم‌های یادگیری ماشینی، به‌ویژه مدل‌های یادگیری عمیق، نیازمند منابع محاسباتی گسترده‌ای هستند. این مدل‌ها با ساختار پیچیده و تعداد زیاد پارامترهای قابل آموزش، به پردازنده‌های پیشرفته، حافظه زیاد و واحدهای پردازش گرافیکی[1] برای تحلیل حجم زیادی از داده‌ها نیاز دارند. اجرای این مدل‌ها، به‌ویژه در سازمان‌های کوچک با منابع محدود، چالش‌برانگیز است و می‌تواند هزینه‌های عملیاتی را افزایش دهد. بنابراین، سازمان‌ها باید در ارتقای توانایی‌های محاسباتی خود سرمایه‌گذاری کنند و زیرساخت‌های مناسبی را برای بهره‌برداری مؤثر از این تکنیک‌ها فراهم آورند.

در مجموع، استفاده از الگوریتم‌های یادگیری ماشینی در شناسایی و پیشگیری از پولشویی در تراکنش‌های رمزارزی به‌عنوان یک ابزار پیشرفته و ضروری، با چالش‌های فنی و اجرایی مختلفی همراه است. ارتقای کیفیت داده‌ها، به‌روزرسانی مداوم الگوریتم‌ها و تأمین منابع محاسباتی کافی از جمله الزامات اصلی در این زمینه هستند. با این حال، با رفع این چالش‌ها و ایجاد زیرساخت‌های مناسب، می‌توان به بهره‌برداری مؤثر از این تکنیک‌ها امیدوار بود و گامی مؤثر در جهت

[1] Graphical Processing Units

پیشگیری از پولشویی و تقویت سیاست جنایی در قبال رمزارزها برداشت. پیاده‌سازی الگوریتم‌های یادگیری ماشینی در مبارزه با پولشویی همچنین با مشکلات قانونی و مقرراتی خاصی روبه‌روست:

پیاده‌سازی الگوریتم‌های یادگیری ماشینی در مبارزه با پولشویی در تراکنش‌های رمزارزی، علاوه بر مزایای متعدد، با چالش‌های قانونی و مقرراتی قابل‌توجهی روبه‌رو است. یکی از مهم‌ترین این چالش‌ها، عدم تنظیم‌گری و استانداردسازی مناسب در این زمینه است [۱۹]. لذا چالش‌های قانونی و مقرراتی یکی از مشکلات اصلی در استفاده از یادگیری ماشینی در ایران است. در حال حاضر، قوانین و مقررات خاصی برای نظارت و استفاده از این فناوری در زمینه شناسایی پولشویی در کشور وجود ندارد. نبود استانداردهای مشخص می‌تواند به مشکلاتی در اجرای مدل‌های یادگیری ماشینی منجر شود. برای مثال، حادثه حمله هکری گسترده به صرافی «Bitfinex» در سال ۲۰۱۶ نشان داد که نبود چارچوب‌های قانونی و نظارتی و عدم استانداردها و مقررات کافی می‌تواند به مشکلات جدی در امنیت و کارایی سیستم‌ها منجر شود. هکرها با بهره‌برداری از ضعف‌های امنیتی و نبود استانداردهای مشخص، مقدار زیادی رمزارز را از حساب‌های کاربران سرقت کردند که مشخص می‌تواند باعث آسیب‌پذیری سیستم‌های مالی شود. در ایران، تدوین و اجرای استانداردهای قانونی و نظارتی دقیق برای استفاده از یادگیری ماشینی در شناسایی پولشویی، یک نیاز اساسی است که باید مورد توجه سیاست‌گذاران قرار گیرد. این حادثه نشان‌دهنده ضرورت تدوین چارچوب‌های قانونی و مقرراتی خاص ذیل سیاست جامع هوشمند برای استفاده از یادگیری ماشینی در شناسایی جرم پولشویی در حوزه رمزارزها است. یکی دیگر از چالش‌ها، مسائل حقوقی و اعتبار مدل‌های یادگیری ماشینی در دادگاه‌ها و نزد نهادهای قضایی است. در ایران، نهادهای نظارتی ممکن است با مشکلاتی در پذیرش نتایج حاصل از این مدل‌ها مواجه شوند، به‌ویژه در مواردی که تصمیمات مبتنی بر این مدل‌ها به مسدودسازی حساب‌های کاربران یا اعمال جریمه‌های قانونی منجر می‌شود. برای مثال، در پرونده «Crypto Capital»[1] در سال ۲۰۱۹، استفاده از این الگوریتم‌ها باعث شناسایی نادرست برخی تراکنش‌های مشروع به‌عنوان فعالیت‌های مشکوک شد. این اشتباهات منجر به مسدود شدن حساب‌های کاربران و بروز مشکلات حقوقی قابل توجهی برای شرکت شد. کاربران به دلیل مسدود شدن غیرقانونی حساب‌هایشان دعاوی حقوقی علیه شرکت مطرح کردند که این مسئله منجر به بروز مشکلات حقوقی برای شرکت و کاهش اعتماد عمومی شد [۱۱]. این موضوع نشان می‌دهد که توسعه و استفاده از الگوریتم‌های یادگیری ماشینی باید با دقت، نظارت بسیار بالا همراه با به‌روزرسانی‌های مستمر باشد و در عین حال سازوکارهای جبران خسارت به‌طور جدی مورد توجه قرار گیرد تا حقوق قانونی کاربران رعایت و از مشکلات مشابه جلوگیری گردد. در نهایت، یکی دیگر از چالش‌های مهم، شفافیت و پاسخگویی الگوریتم‌ها است. مدل‌های پیچیده یادگیری ماشینی، مانند شبکه‌های عصبی عمیق، ممکن است به‌سختی قابل تفسیر باشند. به‌عنوان مثال، در پرونده «Bitfinex» در سال ۲۰۱۹، این صرافی به دلیل استفاده از الگوریتم‌های پیچیده برای شناسایی عملیات پولشویی، قادر به ارائه توضیحات واضحی درباره تصمیمات خود نبود که این مسئله منجر به فشار نهادهای نظارتی، مشکلات قانونی و کاهش اعتماد به سیستم‌های تحلیل داده‌های صرافی شد [۱۹]. این امر می‌تواند در ایران، به‌ویژه زمانی که نهادهای نظارتی نیاز به توضیحات شفاف درباره تصمیمات الگوریتمی دارند، مشکل‌ساز شود. برای رفع این چالش، نیاز است که نهادهای نظارتی کشور از تکنیک‌های تفسیرپذیری در مدل‌های خود استفاده کنند تا بتوانند پاسخگوی تصمیمات مبتنی بر یادگیری ماشینی باشند. در مجموع، استفاده از الگوریتم‌های یادگیری ماشینی در شناسایی و پیشگیری از پولشویی در تراکنش‌های رمزارزی نیازمند تنظیم و استانداردسازی دقیق، توجه به مسائل قضایی و حقوقی، و بهبود شفافیت و پاسخگویی الگوریتم‌ها است. تنها با رعایت این موارد می‌توان از کارایی و امنیت این الگوریتم‌ها بهره‌مند شد و از بروز تبعات و مشکلات قانونی جلوگیری کرد.

۸- جایگاه حقوقی یادگیری ماشینی در سیاست جنایی مهار پولشویی با تراکنش‌های رمزارزی

استفاده از یادگیری ماشینی در شناسایی پولشویی در تراکنش‌های رمزارزی موضوعی است که در سطح بین‌المللی و منطقه‌ای توجه بسیاری را به خود جلب کرده است. این فناوری، به‌ویژه در زمینه سیاست‌های جنایی و مسائل حقوقی، نشان‌دهنده نیاز به بررسی و تطبیق قوانین و مقررات موجود با فناوری‌های نوین در این زمینه است. در سطح بین‌المللی، گروه ویژه اقدام مالی (FATF) به‌طور مستقیم به استفاده از یادگیری ماشینی اشاره نکرده است، اما تأکید می‌کند که کشورها باید از فناوری‌های پیشرفته برای ارتقای کارایی سیستم‌های نظارتی خود بهره ببرند. این نهاد به کشورهای عضو توصیه می‌کند که از تکنولوژی‌های نوین برای مقابله با پولشویی و تأمین مالی تروریسم استفاده کنند. در اتحادیه اروپا، «دستورالعمل‌های مبارزه با پولشویی» نیز بر اهمیت استفاده از ابزارهای فناورانه دیجیتال و تحلیل داده‌ها تأکید دارد، هرچند به‌طور خاص به یادگیری ماشینی اشاره نکرده است. در ایالات متحده، قوانین و نهادهای نظارتی مانند «شبکه اجرای جرایم مالی» از استفاده از فناوری‌های نوین برای شناسایی و گزارش تراکنش‌های مشکوک حمایت می‌کنند، هرچند یادگیری ماشینی به‌طور مستقیم در قوانین ذکر نشده است. سازمان‌های بین‌المللی مانند بلنک جهانی و صندوق بین‌المللی پول [2] نیز بر اهمیت این فناوری‌ها

[1] Crypto Capital، در سال ۲۰۱۳ تأسیس شده و به‌عنوان یک شرکت خدمات مالی و پردازش پرداخت‌های رمزارزی فعالیت می‌کرد. این شرکت به‌طور گسترده به صرافی‌های رمزارز و کسب‌وکارهای آنلاین خدمات می‌داد و در سال ۲۰۱۹ به دلیل ارتباط با پولشویی و مشکلات قانونی تحت بررسی شدید قرار گرفت. در پی این مشکلات، شرکت مزبور به دلیل نقض قوانین ضدپولشویی و ارتباط با فعالیت‌های غیرقانونی، تحت فشارهای قانونی و مسدود شدن حساب‌های بانکی قرار گرفت.

[2] International Monetary Fund

تأکید دارند و از کشورهای عضو خواسته‌اند که از یادگیری ماشینی برای بهبود سیستم‌های نظارتی خود استفاده کنند.

در ایران، قانون مبارزه با پولشویی مصوب ۱۳۸۶ و آیین‌نامه اجرایی آن، چارچوب قانونی اصلی برای مقابله با پولشویی را تشکیل می‌دهند. هرچند این قانون بر استفاده از فناوری‌های نوین تأکید کرده است، ولی به‌طور مستقیم به یادگیری ماشینی اشاره نمی‌کند. اصلاحات جدیدی که در سال ۱۳۹۷ در این قانون اعمال شده است، بر اهمیت ارتقای کارایی سیستم‌های نظارتی با استفاده از فناوری‌های پیشرفته تأکید دارند، اما همچنان جای کار دارد تا استفاده خاص از یادگیری ماشینی به‌طور مستقیم در قوانین گنجانده شود. در ایران، چالش‌هایی در زمینه به‌کارگیری یادگیری ماشینی برای مقابله با جرم پولشویی توسط رمزارزها وجود دارد. عدم وجود چارچوب‌های قانونی صریح، نیاز به توسعه زیرساخت‌های فنی و آموزشی، و محدودیت‌های بین‌المللی از جمله مشکلاتی هستند که باید برطرف شوند. برای استفاده مؤثر از یادگیری ماشینی، نهادهای مالی و نظارتی نیاز به تدوین مقررات جدید و به‌روزرسانی قوانین دارند؛ همچنین باید به آموزش‌های لازم برای پرسنل و فراهم کردن زیرساخت‌های فنی مناسب توجه کنند.

پولشویی در تراکنش‌های رمزارزی، به دلیل ویژگی‌هایی مانند ناشناس بودن و جهانی بودن این تراکنش‌ها، یک چالش بزرگ برای نهادهای نظارتی و اجرای قانون است. استفاده از یادگیری ماشینی در شناسایی و پیشگیری از جرائم این حوزه، به‌ویژه پولشویی، به‌عنوان یک ابزار کلیدی و اثرگذار در اجرای سیاست جنایی مقتضی در این حوزه شناخته می‌شود. این فناوری می‌تواند نقش مهمی در ساختار سیاست جنایی پیشگیرانه، فناورانه، اقتصادی، اجرایی و مشارکتی ایفا کند و تولنایی آن در تحلیل داده‌های مالی پیچیده، به نهادهای نظارتی امکان می‌دهد تا با دقت بیشتری به مقابله با پولشویی در فضای رمزارزی بپردازند. «سایت‌های جعلی با استفاده از تبلیغات گسترده در فضای مجازی سعی در کسب اعتماد مردم می‌کنند تا آنها با پرداخت مبالغی، برای آنها حساب کاربری و کیف پول دیجیتالی ایجاد کنند. آگاه‌سازی کاربران از گذر برگزاری کلاس‌های آشنایی با رمزارزها و همچنین فیلترینگ سایت‌های مشکوک به ارتکاب فعل مجرمانه» [۲۰]. در قالب سطوح سیاست جنایی پیشگیرانه وضعی و اجتماعی، تقنینی و قضائی و اجرائی و مشارکتی ضروری است.

سیاست جنایی پیشگیرانه به دنبال ممانعت از وقوع جرم قبل از ارتکاب آن است. این سیاست بر شناسایی و کاهش عوامل و فرصت‌های جرم‌زایی متمرکز است تا به‌طور مؤثری از وقوع جرم جلوگیری کند. در زمینه پولشویی در زمینه رمزارزها، یادگیری ماشینی به‌عنوان یک ابزار پیشگیرانه برجسته عمل می‌کند. با استفاده از الگوریتم‌های یادگیری ماشینی، می‌توان رفتارهای مالی غیرعادی را شناسایی کرده و به‌طور زودهنگام به مقامات مربوطه اطلاع داد تا از پیشرفت فعالیت‌های پولشویی جلوگیری شود. سیاست جنایی فنی و فناورانه بر کاربرد فناوری‌های پیشرفته برای مقابله با جرائم پیچیده و نوظهور تأکید دارد. در مورد پولشویی دیجیتال، یادگیری ماشینی به‌عنوان یک ابزار فنی پیشرفته، نقشی کلیدی ایفا می‌کند. فناوری‌هایی مانند «جنگل‌های تصادفی» و «شبکه‌های عصبی عمیق» به تحلیل دقیق‌تر و شناسایی مؤثرتر تراکنش‌های مشکوک کمک می‌کنند. به‌طور مثال، در ایالات متحده، در سال ۲۰۱۹، شرکت‌های فناوری با استفاده از الگوریتم‌های یادگیری ماشینی موفق به شناسایی یک شبکه پولشویی بین‌المللی شدند که از تراکنش‌های رمزارزی برای پنهان کردن فعالیت‌های غیرقانونی خود استفاده می‌کردند. این نوع فناوری‌های پیشرفته به مقامات و نهادهای مالی این امکان را می‌دهند که با دقت بیشتری به تحلیل داده‌ها بپردازند و فعالیت‌های پولشویی را شناسایی کنند؛ که این امر بهبود قابل توجهی در فرآیندهای نظارتی و اجرائی به همراه دارد [۱۲].

سیاست جنایی اجرائی بر اجرای قوانین و مقررات مربوط به مبارزه با جرائم توسط نهادهای اجرائی مانند پلیس، دادستانی و دستگاه قضائی تمرکز دارد. یادگیری ماشینی می‌تواند کارایی و دقت این نهادها را در شناسایی و مقابله با پولشویی افزایش دهد. این موضوع نشان‌دهنده توانایی یادگیری ماشینی در ارتقاء فرآیندهای اجرائی و قضائی و تقویت اقدامات قانونی در مقابله با جرم پولشویی توسط رمزارزها است. به‌طور مثال، در سال ۲۰۲۱، دادستانی فدرال ایالات متحده از تحلیل‌های مبتنی بر یادگیری ماشینی برای شناسایی و تعقیب یک شبکه گسترده پولشویی که از طریق رمزارزها فعالیت می‌کرد، استفاده کرد. این تحلیل‌ها به‌عنوان شواهد دیجیتال در پرونده‌های قضائی مورد استفاده قرار گرفت و منجر به محکومیت عاملان شد [۲۱]. سیاست جنایی مشارکتی بر همکاری و هماهنگی بین نهادهای دولتی و خصوصی و نهادهای بین‌المللی برای مقابله با جرائم تأکید دارد. استفاده از یادگیری ماشینی در شناسایی پولشویی نیازمند همکاری نزدیک بین این نهادها است. به‌عنوان مثال، گروه FATFبا همکاری بانک‌های بین‌المللی و شرکت‌های فناوری، سیستم یادگیری ماشینی را برای شناسایی تراکنش‌های مشکوک در سطح جهانی توسعه داد. این همکاری منجر به شناسایی و مسدودسازی میلیون‌ها دلار پولشویی از طریق تراکنش‌های رمزارزی شد. این نمونه تأکید می‌کند که سیاست جنایی مشارکتی با استفاده از فناوری‌های نوین و همکاری‌های بین‌المللی می‌تواند به شناسایی و مقابله مؤثرتر با پولشویی کمک کند [۹]. همکاری‌های بین‌المللی و تبادل اطلاعات در این زمینه به بهبود کارایی و دقت الگوریتم‌های یادگیری ماشینی در شناسایی فعالیت‌های غیرقانونی کمک شایانی می‌کند.

۹- نتیجه‌گیری

این پژوهش به بررسی نقش یادگیری ماشینی در شناسایی و پیشگیری از پولشویی در تراکنش‌های رمزارزی پرداخته است. الگوریتم‌های پیشرفته‌ای مانند جنگل تصادفی، XGBoost، شبکه‌های پیچشی گراف و شبکه‌های عصبی عمیق در شناسایی الگوهای مشکوک و پنهان که ممکن است از دید روش‌های نظارتی سنتی پنهان بمانند، بسیار مؤثر عمل می‌کنند. این مدل‌ها با تحلیل داده‌های عظیم و پیچیده، امکان شناسایی دقیق‌تر و سریع‌تر فعالیت‌های پولشویی را فراهم

می‌آورند. همچنین، یادگیری ماشـــینی به‌عنوان بخشـــی از رویکردهای سـیاسـت جنایی پیشـگیرانه در حوزه رمزارزها، نقشـی کلیدی در بهبود کارایی نهادهای نظارتی ایفا می‌کند.

نتایج این تحقیق نشان داد که یادگیری ماشینی می‌تواند به شکل مؤثری به شـناسـایی و پیشـگیری از پولشـویی در تراکنش‌های رمزارزی کمک کند. یافته‌های مقاله نشان می‌دهد که:

- پاســخ بـه پرســش اول: یـادگیری مـاشـــینی می‌توانـد چارچوب‌های نظارتی و حقوقی برای مقابله با پولشـویی را بهبود بخشـد. با بهره‌گیری از این تکنیک‌ها، نهادهای نظارتی قادر خواهند بود تا الگوهای مشکوک در تراکنش‌های رمزارزی را شناسایی کرده و از وقوع جرم‌های مالی جلوگیری کنند.
- پاسخ به پرسش دوم: الگوریتم‌های یادگیری ماشینی مانند شبکه‌های عصبی عمیق و مدل‌های پیچشی گراف می‌توانند به شناسایی الگوهای غیرعادی و پیچیده در تراکنش‌های رمزارزی کمک کنند. این فناوری‌ها امکان تحلیل حجم بالای داده‌ها را فراهم می‌کنند و می‌توانند به‌طور مداوم با داده‌های جدید به‌روزرسـانی شـوند تا در برابر روش‌های جدید پولشویی عملکرد بهتری داشته باشند.
- پاسخ به پرسش سوم: در زمینه تدوین سیاست‌های جنایی هوشـــمندانه، یادگیری ماشـــینی به نهادهای نظارتی کمک می‌کند تا سـیاسـت‌های پیشـگیرانه و مبتنی بر داده‌ها را اتخاذ کنند که به کاهش جرایم مالی نظیر پولشویی کمک می‌کند. همچنین استفاده از یادگیری ماشـــینی نیازمند تقویت همکاری‌های بین‌المللی اســـت تا قوانین و چارچوب‌های نظارتی جهانی بتوانند بهتر با چالش‌های رمزارزی مقابله کنند.

در پایان، با توجه به اهمیت اســـتفاده از یادگیری ماشـــینی در شـناسـایی و پیشـگیری از پولشـویی در ایران، پیشـنهادات کاربردی زیر ارائه می‌شود:

۱- تدوین چارچوب‌های قانونی و مقرراتی: ســـیاســـت‌گذاران ایران باید مقررات و چارچوب‌های قانونی مناسـب برای اسـتفاده از یادگیری ماشینی در شـناسـایی و مبارزه با پولشـویی را تدوین کنند. این مقررات باید جمع‌آوری و پردازش داده‌ها را تسـهیل کرده و در عین حال حریم خصـوصـی کاربران را حفظ کنند. همکاری با نهادهای بین‌المللی برای هماهنگی بیشتر در این زمینه نیز ضروری است.

۲- تقویت زیرساخت‌های نظارتی و آموزشی: نهادهای نظارتی ایران باید در جهت توسـعه زیرسـاخت‌های نظارتی برای به‌کارگیری یادگیری ماشینی در تحلیل تراکنش‌های رمزارزی سرمایه‌گذاری کنند. همچنین، آموزش نیروی انسانی و تقویت مهارت‌های نظارتی برای استفاده مؤثر از این فناوری از اهمیت بالایی برخوردار است.

۳- بهبود کیفیت داده‌ها و توســـعه مدل‌های یادگیری ماشـــینی: داده‌های تراکنش‌های رمزارزی باید به‌طور مستمر به‌روزرسانی و کیفیت داده‌ها بهبود یابد تا مدل‌های یادگیری ماشـــینی با داده‌های دقیق و صـــحیح کار کنند. همچنین، توســـعه و بهینه‌ســـازی مدل‌های موجود به‌منظور تطبیق با تکنیک‌های جدید پولشویی بسیار ضروری است.

۴- حمایت از تحقیقات و توسعه فناوری: حمایت از تحقیقات علمی و توسـعه فناوری در زمینه یادگیری ماشـینی می‌تواند به ارتقای کارایی سیستم‌های نظارتی و پیشگیری از پولشویی کمک کند. سیاست‌گذاران و نهادهای مالی باید به‌طور مداوم از جدیدترین دسـتاوردهای علمی در این حوزه بهره‌برداری کنند.

۵- همکاری‌های بین‌المللی: برای مقابله با پولشویی در تراکنش‌های رمزارزی، همکاری‌های بین‌المللی و تبادل اطلاعات میان نهادهای مالی و نظارتی ایران و دیگر کشـورها ضـروری اسـت. تدوین اسـتانداردهای بین‌المللی برای شناسایی و جلوگیری از جرایم مالی در فضای رمزارزها می‌تواند به کارآمدی این فرآیند کمک کند.

مراجع

[۱] ع. محمودی, ا. احمدی ,و ر. علی پور, "تأثیر قانون مبارزه با پول‌شویی بر کشف جرم منشأ و پیشگیری از فعالیت‌های اقتصادی مجرمانه در ایران "پژوهشنامه حقوق کیفری , no. Online First, Oct. 2023, ۲۰۲۳.۲۵۱۳۳.۲۳۹۶/jol.۱۰.۲۲۱۲۴https://doi.org/

[۲] م. مددی و س. قماشی, "جستاری در پول‌شویی از طریق ارزهای رمزنگاری شده" مطالعات حقوق کیفری و جرم شناسی , vol. 51, no. 2, Feb. 2022, ۲۰۲۳.۲۵۱۳۳.۲۳۹۶/jol.۱۰.۲۲۱۲۴https://doi.org/

[۳] ش. عبدالهی قهفرخی, ب. پاکزاد, ح. عالی پور و م. الهی منش, "پیشگیری از پولشویی الکترونیکی: رویکرد دفاعی و رویکرد هجومی.https://doi.org/10.22034/jclc.2021.290298. 1510," JCLC, vol. 9, no. 18, Jan. 2022

[۴] م. حاجی ده‌آبادی و م. خاقانی‌اصفهانی، "گونه‌شناسی سیاست کیفری فنی در قبال جرم رمزنگاری اطلاعات از منظر آزادی‌گرایی و امنیت‌گرایی،" آموزه‌های حقوق کیفری، vol. 10, no. 5, 1392. https://dorl.net/dor/20.1001.1.22519351.1392.10.5.4.0.

[5] Dreżewski, J. Sepielak, and W. Filipkowski, "The application of social network analysis algorithms in a system supporting money laundering detection," *Information Sciences*, vol. 295, pp. 18–32, Feb. 2015. https://doi.org/10.1016/j.ins.2014.10.015.

[6] Y. Dorogy and V. Kolisnichenko, "Blockchain transaction analysis: A comprehensive review of applications, tasks and methods," *System Research and Information Technologies*, no. 4, pp. 37–53, 2023https://doi.org/10.20535/srit.2308-8893.2023.4.03

[7] Y. Zhang and P. Trubey, "Machine learning and sampling scheme: An empirical study of money laundering detection," *Computational Economics*, vol. 54, no. 3, pp. 1043–1063, 2018 https://doi.org/10.1007/s10614-018-9864-z.

[8] S. R. Sandeep, S. Ahamad, D. Saxena, K. Srivastava, S. Jaiswal, and A. Bora, "To understand the relationship between machine learning and artificial intelligence in large and diversified business organisations," *Materials Today: Proceedings*, vol. 56, pp. 2082–2086, 2022. https://doi.org/10.1016/j.matpr.2021.11.409

[9] J. Lorenz, M. I. Silva, D. Aparício, J. T. Ascensão, and P. Bizarro, "Machine learning methods to detect money

laundering in the bitcoin blockchain in the presence of label scarcity," in *Proceedings of the First ACM International Conference on AI in Finance (ICAIF '20)*, 2020. https://doi.org/10.1145/3383455.3422549

[10] M. Ramalingam, G. C. Selvi, N. Victor, R. Chengoden, S. Bhattacharya, P. K. R. Maddikunta, D. Lee, Md. J. Piran, N. Khare, G. Yenduri, and T. R. Gadekallu, "A comprehensive analysis of blockchain applications for securing computer vision systems," *IEEE Access*, vol. 11, pp. 107309–107330, 2023. https://doi.org/10.1109/access.2023.3319089

[11] O. Japinye, "Integrating machine learning in anti-money laundering through crypto: A comprehensive performance review," European Journal of Accounting, Auditing and Finance Research, vol. 12, no. 4, pp. 54–80, 2024. https://doi.org/10.37745/ejaafr.2013/vol12n45480

[12] E. Petterson Ruiz, J. Angelis, and et al., "Combating money laundering with machine learning – Applicability of supervised-learning algorithms at cryptocurrency exchanges," *Journal of Money Laundering Control*, vol. 25, no. 4, pp. 766–778, 2021. https://doi.org/10.1108/jmlc-09-2021-0106

[13] H. Almeida, P. Pinto, and A. Fernández Vilas, "A review on cryptocurrency transaction methods for money laundering," in *Proceedings of the 5th International Conference on Finance, Economics, Management and IT Business*, 2023. https://doi.org/10.5220/0011993300003494

[14] C. Wronka, "Money laundering through cryptocurrencies - Analysis of the phenomenon and appropriate prevention measures," *Journal of Money Laundering Control*, vol. 25, no. 1, pp. 79–94, 2021. doi: [10.1108/jmlc-02-2021-0017](https://doi.org/10.1108/jmlc-02-2021-0017).

[15] F. M. J. Teichmann and M.-C. Falker, "Money laundering via cryptocurrencies – Potential solutions from Liechtenstein," *Journal of Money Laundering Control*, vol. 24, no. 1, pp. 91–101, 2020. doi: 10.1108/jmlc-04-2020-0041

[16] G. L. Gray, "An exploration of the money laundering associated with the Bitfinex Bitcoin hack," *Journal of Emerging Technologies in Accounting*, vol. 21, no. 1, pp. 43–57, 2024. doi: 10.2308/jeta-2023-017

[17] B. N. Pambudi, I. Hidayah, and S. Fauziati, "Improving money laundering detection using optimized support vector machine," in *2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2019. doi: 10.1109/isriti48646.2019.9034655.

[18] A. Gupta, D. N. Dwivedi, J. Shah, and A. Jain, "Data quality issues leading to sub-optimal machine learning for money laundering models," Journal of Money Laundering Control, vol. 25, no. 3, pp. 551–555, 2021. doi: 10.1108/jmlc-05-2021-0049.

[19] Y. Suga, M. Shimaoka, M. Sato, and H. Nakajima, "Securing cryptocurrency exchange: Building up standard from huge failures," in *Lecture Notes in Computer Science*, pp. 254–270, 2020. doi: 10.1007/978-3-030-54455-3_19.

[۲۰] زهرا ایزدی و نسترن ارزانیان، «پیشگیری از جرایم پولشویی و کلاهبرداری در بستر استفاده از رمزارزهای جهانی»، فصلنامه رهیافت پیشگیری از جرم، دوره ۲، شماره ۱، صفحات ۱-۱۴، ۱۳۹۸.

[21] N. Thoiba Singh, M. Mehra, I. Verma, N. Singh, D. Gandhi, and M. Ahmad Alladin, "Advancing crime analysis and prediction: A comprehensive exploration of machine learning applications in criminal justice," in *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, 2024. doi: 10.1109/idciot59759.2024.10467221

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

A Review of CP-ABE Access Control Schemes In Fog Computing

Mohammad Ali Alizadeh[1], Somayyeh Jafarali Jassbi[2*], Ahmad Khademzadeh[3]
[1]PhD student, Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
mohammadali.alizadeh@srbiau.ac.ir
[2]Assistant Professor, Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
s.jassbi@srbiau.ac.ir
[3]Professor, ICT Research Institute, Tehran, Iran
zadeh@itrc.ac.ir

Abstract: Fog computing with cloud computing is useful for real-time processing in the IoT ecosystem. Fog computing can be used to outsource and lighten the computations of the end nodes because it is closer to the end nodes and has higher processing and communication power. On the other hand, the privacy and security of users of IOT are significant.This can be achieved by attribute encryption fine-grained access control schemes like ciphertext-policy attribute-based encryption (CP-ABE). Along with the improvements of the mentioned schemes, there are challenges such as attribute revocation and user revocation. In this article, we intend to review the new schemes based on CP-ABE, examine their extensive capabilities, and find an approach to the challenges each of them tried to solve. Also, clarify the architectural details of the mentioned designs implemented in the fog computing framework, such as the access policy model, attribute authority model, and underlying operations. Finally, we examine the weak points of the schemes to predict future development trends and present open issues.

Keywords: IoT, Fog computing, Access control, CP-ABE, RNS

JCDSA, Vol. 2, No. 3, Autumn 2024	Online ISSN: 2981-1295	Journal Homepage: https://sanad.iau.ir/en/Journal/jcdsa
Received: 2024-08-12	Accepted: 2024-11-26	Published: 2024-12-20

CITATION

Alizadeh, M.A., et al., " *A review of CP-ABE access control schemes in fog computing",* Journal of Circuits, Data and Systems Analysis (JCDSA), Vol. 2, No. 3, pp. 16-30, 2024.
DOI: 00.00000/0000

* Corresponding author

Extended Abstract

1- Introduction

To maintain the confidentiality and privacy of users in the Internet of Things (IoT) network, it is necessary to benefit from access control schemes. One of the most practical access control schemes in the IoT ecosystem is based on attribute-based encryption (ABE). The most important feature of these designs is granularity and support for one-to-many public key encryption algorithms. These features help secure and efficient authentication and authorization of multiple users with minimal need for key management. Designs based on ABE are divided into two general models: CP-ABE and KP-ABE. In general, the framework of these schemes includes four algorithms: setup, key generation, encryption, and decryption. In the less-used KP-ABE model, each data user must decrypt the ciphertext based on an access structure they define and a secret key provided by the data owner. The access structure and secret key are determined based on the attributes of the data users. This scheme has received less attention due to the inflexibility of the data owner in defining the access policy. However, the CP-ABE design, which is designed in contrast to KP-ABE, has been highly regarded due to its flexible and fine-grained structure. The data owner defines and encrypts the plaintext based on an access structure. If the data user's secret key can satisfy the access structure, it can decrypt the ciphertext. The main drawback of these two models is the underlying operation of bilinear pairing, which has a high computational overhead. Also, the operation of revoking users and their attributes is not agile. For this purpose, in many types of research, the authors outsourced operations with high overhead to the cloud server to lighten the calculations. However, the cloud server is not a suitable option due to its centralized structure and long distance from the end nodes, which often have limited processing resources. Therefore, in relatively recent research, designers took advantage of fog computing architecture with cloud computing. The RNS-ABE model was introduced as a special case in which the ABE access control scheme uses the residue number system (RNS) instead of bilinear pairing.

2- Methodology

This article first introduces basic concepts and definitions in the field of ABE, such as bilinear pairing, basic CP-ABE access control scheme, RNS, RNS-based access structures, access tree and LSSS, IoT for health and transportation, and proxy re-encryption (PRE) are discussed. Then, we reviewed and analyzed the latest articles in the field of ABE that implemented the infrastructure of fog computing and cloud computing in their architecture. In the end, the most relevant and newest articles have all implemented fog calculations from the perspective of the access structure model, attribute authority model, attribute and user revocation capabilities, underlying operations and other plugin capabilities such as hiding the access structure or blockchain implementation has been compared to be a basis for researchers in the field of ABE.

3- Results and discussion

In recent articles, more attention has been paid to the implementation of blockchain and it has been used in entities such as multiple attribute authority and fog computing. In addition, due to the high computational overhead of bilinear pairing, the focus has been on the underlying operations such as RNS, so that the calculations are inherently fast and there is no need to outsource expensive operations to fog calculations. Another shortcoming of CP-ABE schemes is the obviousness of the access structure embedded in the ciphertext, which some researchers have introduced ideas to hide from data users. Another challenge of these plans, which Bettencourt, the creator of the CP-ABE basic plan, also acknowledges, is the revocation of attributes and users, which have not been considered in many plans. In some designs, only one of the two has been given attention. Of course, all these designs have used PRE, which imposes a high computational overhead. In one of the research studies, the concept of user cooperation for decrypting the ciphertext was discussed, which is a practical and interesting idea.

4- Conclusion

ABE schemes are one of the most practical access control schemes that maintain user confidentiality, privacy, and security of devices and sensors in the IoT. The most important and flexible model of these designs is CP-ABE. This model has features such as granularity, the ability to design an access policy by the data owner, and easier management of encryption keys due to their one-to-many nature. But along with its advantages, it also has challenges and drawbacks. Their underlying operations, such as bilinear pairing and powering, have a high computational overhead, and features such as revocation of attributes, revocation of users, key escrow, non-confidentiality of the access policy embedded in the ciphertext, and the use of a single attribute authority, which will reduce its scalability; It has a challenge. Several solutions have been used to solve the above issues, such as fog computing implementation, multiple attribute authorities, blockchain, and using operations such as RNS and XOR instead of bilinear pairing. In the future, we suggest designing revocation algorithms in RNS, combining blockchain and RNS, and creating additional features such as hiding and user cooperation in RNS.

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

مروری بر طرح‌های کنترل دسترسی رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز در محاسبات مه

محمدعلی علی‌زاده[۱]، سمیه جعفرعلی جاسبی*[۲]، احمد خادم‌زاده[۳]

۱- دانشجوی دکتری، گروه مهندسی کامپیوتر، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران (mohammadali.alizadeh@srbiau.ac.ir)

۲- استادیار، گروه مهندسی کامپیوتر، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران (s.jassbi@srbiau.ac.ir)

۳- استاد، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران (zadeh@itrc.ac.ir)

چکیده: محاسبات مه در کنار رایانش ابری توسعه مناسبی را برای پردازش‌های بلادرنگ در اینترنت اشیاء فراهم می‌کند. محاسبات مه به دلیل نزدیکی به گره‌های پایانی و دارابودن قدرت پردازشی و ارتباطی بالاتر، می‌تواند برای برون‌سپاری و سبک‌وزن سازی محاسبات گره‌های پایانی مورد استفاده قرار گیرد. از سوی دیگر حفظ حریم خصوصی و امنیت کاربران در اینترنت اشیاء نیز دارای اهمیت است. این مهم توسط طرح‌های کنترل دسترسی رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز (CP-ABE) به‌صورت ریزدانه و منعطف قابل‌دستیابی است. در کنار محسنات طرح‌های مذکور، چالش‌هایی نیز نظیر ابطال ویژگی و ابطال کاربر وجود دارد. در این مقاله در نظر داریم ضمن مرور طرح‌های نوین مبتنی بر CP-ABE به بررسی قابلیت‌های افزونه آنها نیز بپردازیم و به رهیافتی از چالش‌هایی که هر یک تلاش نمودند تا حل نمایند پی ببریم. همچنین جزئیات معماری هریک از طرح‌های مذکور را که در چارچوب محاسبات مه پیاده‌سازی شده‌اند نظیر مدل خط‌مشی دسترسی، مدل مرجع ویژگی و عملیات زیربنایی روشن نماییم. در پایان به بررسی نقاط ضعف طرح‌ها می‌پردازیم و روندهای توسعه آینده را پیش‌بینی می‌کنیم و مسائل باز را ارائه می‌دهیم.

واژه‌های کلیدی: اینترنت اشیاء، محاسبات مه، کنترل دسترسی، رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز (CP-ABE)، سیستم اعداد مانده‌ای (RNS)

نوع مقاله: مروری

تاریخ ارسال مقاله: ۱۴۰۳/۰۵/۲۲ تاریخ پذیرش مقاله: ۱۴۰۳/۰۹/۰۶ تاریخ چاپ مقاله: ۱۴۰۳/۰۹/۳۰

DOI: 00.00000/0000

۱- مقدمه

با محبوبیت ارتباطات نسل پنجم[۲]، تحقیقات در مورد کاربرد اینترنت اشیاء[۳] به طور فزاینده‌ای افزایش‌یافته است. برنامه‌های کاربردی اینترنت اشیاء بیشتر و بیشتر در زندگی روزمره مردم ظاهر می‌شوند. اینترنت اشیاء به اشیاء فیزیکی، اجازه تولید و تبادل داده می‌دهد، بنابراین خدمات هوشمند مختلفی را به کاربران ارائه می‌دهد. استفاده از اینترنت اشیاء تنها به ارائه خدماتی مانند دفاتر هوشمند، خانه‌های هوشمند و غیره محدود نمی‌شود، بلکه در حوزه صنایع مختلف نیز مانند شبکه‌های انرژی، مراقبت‌های بهداشتی، سیستم‌های حمل‌ونقل نیز گسترش‌یافته است. امروزه، اکثر کسب‌وکارهای جدید به روشی از طریق فناوری اینترنت اشیاء پشتیبانی می‌شوند. مشاهده می‌شود که ساعت دیجیتال به یک ساعت هوشمند، تلفن همراه به یک تلفن هوشمند، و عینک‌آفتابی به یک عینک هوشمند در حال تکامل است. به‌عبارت‌دیگر اینترنت اشیاء مجموعه‌ای از حسگرها، نرم‌افزارها و محرک‌های تعبیه‌شده در دستگاه‌هایی است که از طریق اینترنت برای ایجاد هوش با یکدیگر در ارتباط هستند و از طریق جمع‌آوری، پردازش و مبادله داده‌های تولید شده، خدمات موردنیاز را ارائه می‌دهند [۱].

اگرچه اینترنت اشیاء راحتی را در زندگی ما به ارمغان می‌آورد، اما تجزیه‌وتحلیل، محاسبه و ذخیره حجم عظیم‌داده‌های تولید شده برای دستگاه‌های اینترنت اشیاء چالش‌برانگیز است؛ زیرا چنین دستگاه‌هایی به‌طورکلی منابع محدودی باتوجه‌به توانایی‌های ذخیره‌سازی و پردازش دارند. برای غلبه بر این، رایانش ابری به‌عنوان یک راه‌حل بالقوه ظاهر شده است. رایانش ابری فناوری اطلاعات را متحول کرده است و در آن، نرم‌افزارها و زیرساخت‌های فناوری اطلاعات به‌عنوان یک سرویس در دسترس هستند. هزینه‌های سرمایه‌گذاری اولیه را کاهش می‌دهد، زمان راه‌اندازی زیرساخت را کوتاه می‌کند و خدمات مبتنی بر درخواست را به کاربران نهایی ارائه می‌کند. بااین‌حال، برای برنامه‌های حساس به تأخیر

* نویسنده مسئول

[2] 5G
[3] Internet of Things (IoT)

و موقعیت جغرافیایی مانند ایمنی در برابر آتش، نظارت بر سلامت و خودروهای خودران، نامناسب است. علاوه بر این، حجم داده‌های تولید شده توسط دستگاه‌های اینترنت اشیاء می‌تواند باتوجه‌به نیازهای برنامه، زیاد و مکرر باشد؛ بنابراین، ارسال تمام داده‌ها به ابر برای تجزیه‌وتحلیل، پردازش و ذخیره‌سازی به طور قابل‌توجهی بر پهنای باند شبکه تأثیر نامطلوب می‌گذارد. علاوه بر این، منابع ابری فقط از طریق اینترنت قابل‌دسترسی هستند و وجود یک اتصال پایدار به اینترنت پرسرعت، ممکن است برای دستگاه‌های اینترنت اشیاء امکان‌پذیر نباشد [۲].

برای مقابله با چالش‌های مذکور، الگوی محاسبات مه معرفی گردید. اساساً، محاسبات مه نوعی زیرساخت غیرمتمرکز است که در آن منابع محاسباتی و ذخیره‌سازی در اختیار دستگاه‌های اینترنت اشیاء به‌صورت بلادرنگ قرار گرفته و کمک به پردازش، تجزیه‌وتحلیل، ذخیره‌سازی داده‌ها و تسهیل ارتباط با ابر می‌کند. به‌عبارت‌دیگر، محاسبات مه گسترش رایانش ابری در لبه شبکه است و کمک می‌کند تا دستگاه‌های اینترنت اشیاء به ابر متصل و کیفیت خدمات بهبود بخشیده شود. بااین‌حال، برون‌سپاری داده‌های حساس برای پردازش و ذخیره‌سازی به گره‌های ثالث (ابر و مه) خطر امنیت داده‌ها و نقض حریم خصوصی را افزایش می‌دهد؛ زیرا این گره‌ها ممکن است دسترسی غیرمجاز داشته باشند یا ممکن است داده‌ها را برای منافع مالی به اشتراک بگذارند؛ بنابراین، تأمین امنیت داده‌های برون‌سپاری شده یک جنبه جدایی‌ناپذیر از محاسبات مه و رایانش ابری است. برای تأمین امنیت داده‌های برون‌سپاری شده، رمزگذاری قبل از برون‌سپاری رویکرد مناسبی است. بااین‌حال، سیستم‌های رمزنگاری سنتی مانند رمزنگاری با کلید متقارن یا رمزنگاری با کلید عمومی نمی‌توانند برای چنین اهدافی مورداستفاده قرار گیرند، زیرا نمی‌توانند کنترل دسترسی دقیق و ریزدانه، مدیریت و توزیع کلید کارآمد را فراهم کنند [۲].

در محیط‌های گسترده، به‌ویژه محیط‌های ابری، فناوری‌های رمزگذاری متقارن با کلید یکسان برای رمزگذاری و رمزگشایی از مشکلات توزیع و مدیریت کلید رنج می‌برند. بااین‌حال، روش‌های رمزگذاری نامتقارن مانند زیرساخت کلید عمومی[1] که از کلیدهای عمومی و خصوصی استفاده می‌کنند، فاقد کارایی محاسباتی هستند، زیرا مالکان داده‌ها باید هویت هر گیرنده و کلید عمومی آنها را از قبل مشخص کنند تا الگوریتم رمزگذاری را پیاده‌سازی کنند و متن رمزگذاری شده مختص هر گیرنده را به طور جداگانه ارسال کنند. در واقع زیرساخت کلید عمومی، مجموعه‌ای از ابزارها، رویه‌ها، سیاست‌ها، نرم‌افزارها و سخت‌افزارهایی است که برای ایجاد، مدیریت، توزیع، استفاده، ذخیره‌سازی و ابطال گواهینامه‌های دیجیتالی و کلیدهای عمومی استفاده می‌شود [۳]. هرچند هدف زیرساخت کلید عمومی، آسان‌تر کردن و امن‌تر کردن انتقال اطلاعات از طریق اینترنت است اما فرایند رمزگذاری باتوجه‌به تعداد گیرندگان کلید تکرار می‌شود و منجر به ایجاد سربار محاسباتی و ارتباطی می‌شود. ازآنجایی‌که نمی‌توان از این نوع زیرساخت برای یک‌بار رمزگذاری داده‌ها و ارسال آن به چندین کاربر استفاده کرد، رمزنگاری ویژگی مبنا[2] به‌عنوان راه‌حل مناسبی برای کاهش سربار محاسباتی بالای عملیات رمزگذاری سنتی و حفظ محرمانگی داده‌ها، اشتراک‌گذاری داده‌ها و کنترل دسترسی ریزدانه و منعطف توسط ساهای و واترز[3] ارائه شد [۴].

این یک مکانیسم رمزگذاری است که به کاربران اجازه می‌دهد تا داده‌ها را باتوجه‌به ویژگی‌های خود، مانند سن، جنسیت، تخصص، محل اشتغال، پست سازمانی و غیره، رمزگذاری و رمزگشایی کنند. رمزنگاری ویژگی مبنا، یک تکنیک رمزنگاری نامتقارن برای رمزگذاری یک به چند است که درک سنتی از رمزگذاری کلید عمومی را تغییر داد. در رمزگذاری سنتی با کلید عمومی، پیام برای یک گیرنده خاص با استفاده از کلید عمومی گیرنده رمزگذاری می‌شود. در مقابل، در رمزنگاری ویژگی مبنا، یک کلید عمومی برای کنترل دسترسی به داده‌های رمزگذاری شده، با استفاده از سیاست‌ها و ویژگی‌های دسترسی استفاده می‌شود [۵]. کاربردی‌ترین مدل رمزنگاری ویژگی مبنا، مدل مبتنی بر خط‌مشی متن رمز[4] است که توسط بتنکورت[5] و همکاران [۶] معرفی گردید. عملیات زیربنایی در این طرح، زوج نگار دوخطی[6] است.

۲- مبانی نظری

در ادامه مفاهیم و عملیات پایه‌ای در حوزه CP-ABE بیان می‌شود.

۲-۱- تعاریف

زوج نگار دوخطی:

اگر G_1 و G_T دو گروه چرخه‌ای ضربی از مرتبه اول p[7] باشند و سه شرط زیر صادق باشد، آنگاه $e: G_1 \times G_1 \rightarrow G_T$ یک نقشه زوج نگار دوخطی است [۷].

- دوخطی بودن[8]: برای هر $g_1, g_2 \in G_1$ و $a, b \in Z_p$ داریم:

$$e(g_1^a, g_2^b) = e(g_1^b, g_2^a) = e(g_1, g_2)^{ab} \quad (۱)$$

- عدم انحطاط[9]: برای هر $g_1, g_2 \in G_1$ معادله $e(g_1, g_2) = 1$ وجود ندارد.
- قابلیت محاسبه[10]: برای هر $g_1, g_2 \in G_1$، می‌توانیم $e(g_1, g_2)$ را به طور موثر محاسبه کنیم.

درخت دسترسی:

فرض می‌شود درخت دسترسی T باریشه r، یک ساختار (خط‌مشی) دسترسی را نشان می‌دهد [۶]. هر گره غیر برگ درخت نشان‌دهنده یک دروازه آستانه است که توسط فرزندان آن و یک مقدار آستانه توصیف

[1] Public Key Infrastructure (PKI)
[2] Attribute-based encryption (ABE)
[3] Sahai و Waters
[4] Ciphertext policy attribute-based encryption (CP-ABE)
[5] Bethencourt
[6] Bilinear pairing
[7] Multiplicative cyclic group of prime order p
[8] Bilinearity
[9] Non degeneracy
[10] Computability

شده است. اگر num_x تعداد فرزندان یک گره x و k_x مقدار آستانه آن باشد، $0<k_x\leq num_x$ است. (یعنی اگر هر k_x یا تعداد بیشتری از فرزندان گره x راضی باشند، گره x راضی است.) وقتی $k_x=1$ باشد، دروازه آستانه یک گیت OR و وقتی $k_x=num_x$ باشد، یک گیت AND است. هر گره برگ x با یک ویژگی و یک مقدار آستانه $k_x=1$ توصیف می‌شود. برای تسهیل کار با درخت‌های دسترسی، چند تابع تعریف می‌شود. والد گره x در درخت را با $parent(x)$ نشان می‌دهیم. تابع $att(x)$ تنها در صورتی تعریف می‌شود که x یک گره برگ باشد و نشان‌دهنده ویژگی مرتبط با گره برگ x در درخت باشد. درخت دسترسی T نیز ترتیبی را بین فرزندان هر گره تعریف می‌کند، یعنی فرزندان یک گره از ۱ تا num شماره‌گذاری می‌شوند. تابع $index(x)$ چنین عددی را مرتبط با گره x برمی‌گرداند. زیر درخت T که ریشه آن گره x است با T_x نشان داده می‌شود. اگر مجموعه‌ای از ویژگی‌ها که γ نامیده می‌شود، درخت دسترسی T_x را راضی کند، آن را به‌صورت $T_x(\gamma)=1$ نشان می‌دهیم. $T_x(\gamma)$ را به‌صورت بازگشتی بدین صورت محاسبه می‌کنیم که اگر x یک گره غیر برگ باشد، $T_{x'}(\gamma)$ را برای همه فرزندان x' از گره x محاسبه می‌کنیم. $T_x(\gamma)$ مقدار ۱ را برمی‌گرداند اگر و فقط اگر حداقل k_x فرزندان، ۱ را برگردانند. اگر x یک گره برگ باشد، آنگاه $T_x(\gamma)$ مقدار ۱ را برمی‌گرداند اگر و فقط اگر $att(x)\in\gamma$.

طرح به‌اشتراک‌گذاری راز خطی[1]:

این طرح [۷] اغلب برای تعریف خط‌مشی دسترسی در طرح‌های مبتنی بر خط‌مشی متن رمز استفاده می‌شود. با اعمال طرح اشتراک‌گذاری راز خطی، انتظار داریم فقط مجموعه‌های ویژگی مجاز که خط‌مشی دسترسی را برآورده می‌کنند، بتوانند به عدد مخفی $s\in Z_p$ دسترسی داشته باشند. خط‌مشی دسترسی مبتنی بر اشتراک‌گذاری راز خطی دارای دو جزء است: ماتریس تولید سهم[2] و تابع نگاشت $\rho()$ از دو الگوریتم تشکیل شده است: $share(s,(A_{l\times n},\rho()))$ و $reconstruction(S,\{\lambda_x\}_{x\,\epsilon\,l},\ (A_{l\times n},\rho()))$. ابتدا، مالک داده که مسئول تعریف خط‌مشی دسترسی است $A_{l\times n}$ را تشکیل می‌دهد. ماتریس تولید سهم دارای l ردیف و n ستون است. همه عناصر $A_{l\times n}$ باید در محدوده Z_p باشند. l همچنین برابر است با تعداد کل ویژگی‌های مورد استفاده در خط‌مشی دسترسی. n برابر است با پیچیدگی الگوریتم‌های $share()$ و $reconstruction()$. سپس تابع $\rho()$ را تشکیل می‌دهد. این تابع هر ردیف از $A_{l\times n}$ را دریافت می‌کند، به عنوان مثال، ردیف x یا A_x، در ورودی، و یک ویژگی متناظر $attr_x$ در خط‌مشی دسترسی در خروجی تولید می‌کند.

- $share\left(s,(A_{l\times n},\rho(x))\right)$:

ابتدا، مالک داده یک ماتریس عمودی $\vec{v}=(s,v_2,v_3,\cdots,v_n)^T$ را تشکیل می‌دهد. اولین عضو آن s است. $n\text{-}1$ عضو دیگر از اعداد تصادفی در محدوده Z_p تشکیل شده‌اند. سپس، سهام $\{\lambda_x=A_x\times\vec{v}\}_{x\,\epsilon\,l}$ را محاسبه می‌کند. به عبارت دیگر، $\vec{\lambda}=(\lambda_1,\lambda_2,\lambda_3,\cdots,\lambda_l)$ یک ماتریس ردیفی است که اعضای آن در محدوده Z_p قرار دارد و برای هر ویژگی در خط مشی دسترسی یک عضو وجود دارد.

- $reconstruction(S,\{\lambda_x\}_{x\,\epsilon\,l},\ (A_{l\times n},\rho()))$

مجموعه ویژگی‌های کاربر S (حرف بزرگ) را که در کلید محرمانه خود تعبیه شده است به‌عنوان ورودی دریافت می‌کند. اگر مجموعه مجاز باشد، مجموعه ثابت‌ها $\{w_x\in Z_p\}_{x\,\epsilon\,I}$ برای $I=\{x:\rho(x)\in S\}\subseteq\{1,2,\cdots,l\}$ از طریق معادله $\sum_{x\,\epsilon\,I}w_x\times A_x=(1,0,0,\cdots,0)$ با پیچیدگی زمانی چندجمله‌ای محاسبه می‌شود. سپس از طریق معادله $\sum_{x\,\epsilon\,I}w_x\times\lambda_x$، s محاسبه شده و در خروجی قرار می‌گیرد.

۲-۲- رمزگذاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز

بتنکورت [۶] برای اولین‌بار طرح CP-ABE عملیاتی را مبتنی بر زوج نگار دوخطی و خط‌مشی درخت دسترسی معرفی نمود. در این طرح، ویژگی‌ها با کلید محرمانه کاربر مرتبط می‌شوند و متن رمزگذاری شده با خط‌مشی دسترسی مرتبط است؛ بنابراین، افراد مجاز، تنها در صورتی می‌توانند پیام را رمزگشایی کنند که کلیدهای مخفی آنها با ویژگی‌های مرتبط با خط‌مشی دسترسی متن رمز مطابقت داشته باشد. این اجازه می‌دهد تا داده‌های محرمانه رمزگذاری شده با استفاده از CP-ABE در سرورهای غیرقابل‌اعتماد مانند ابر، بدون اجرای کنترل‌های احراز هویت برای دسترسی به داده‌ها، ذخیره شود. باتوجه‌به ادبیات موجود، CP-ABE در مقایسه با تکنیک‌های رمزنگاری سنتی، مزایای بیشتری دارد. این مزایا به شرح زیر است [۵]:

- سطح بالایی از محرمانگی داده‌ها را فراهم می‌کند.
- مکانیزم کنترل دسترسی رمزگذاری شده را برای برنامه‌های کاربردی فراهم می‌کند.
- سربار ارتباطی را کاهش می‌دهد، زیرا تولید کلید محرمانه کاربر فقط یک‌بار اتفاق می‌افتد.
- در برابر تبانی مقاوم می‌شود، زیرا هر ویژگی با یک چندجمله‌ای یا یک عدد تصادفی مرتبط است که از تبانی کاربران قانونی با یکدیگر جلوگیری می‌کند.
- از مقیاس‌پذیری کاربران پشتیبانی می‌کند. با افزایش تعداد کاربران مجاز، سیستم می‌تواند به طور مؤثر کار کند.

این طرح از چهار الگوریتم پایه «راه‌اندازی، تولید کلید، رمزگذاری و رمزگشایی» به شرح زیر تشکیل شده است که در مقالات جدید مانند [۲،۹،۱۶] دچار تغییراتی گردید و قابلیت‌هایی نظیر ابطال و صحت‌سنجی عملیات برون‌سپاری شده به آن اضافه شد. هر کاربر داده دارای یک کلید محرمانه است که بر اساس ویژگی‌های متعلق به او ساخته می‌شود. هر مالک داده یک خط‌مشی (سیاست) دسترسی تعریف می‌کند تا تنها کاربران داده مجاز بتوانند آن را راضی نمایند و متعاقباً

[1] Linear Secret Sharing Scheme (LSSS)

[2] Share-generating matrix $A_{l\times n}$

بتوانند متن رمز را رمزگشایی کنند. خط‌مشی دسترسی در متن رمز جاسازی شده است و ساختارهای متنوعی دارند؛ مانند درخت دسترسی، اشتراک‌گذاری راز خطی و گیت‌های *AND* و *OR*.

۱. $Setup(1^k) \rightarrow PK, MK$: پارامتر امنیتی 1^k را به‌عنوان ورودی می‌گیرد و کلید عمومی PK و کلید مخفی اصلی MK را خارج می‌کند. g مولد گروه G_1 است.

$$PK = \left(G_1; g; h = g^{\beta}; f = g^{1/\beta}; e(g, g)^{\alpha}\right) \quad (۲)$$
$$MK = (\beta; g^{\alpha})$$

۲. $Keygen(PK, MK, S) \rightarrow SK$: مجموعه ویژگی‌های کاربر S، PK و MK را به‌عنوان ورودی می‌گیرد و کلید محرمانه SK کاربر را خارج می‌کند. $j \epsilon S$ و $r \epsilon Z_p$ و $r_j \epsilon Z_p$ است و همگی تصادفی هستند.

$$SK = \left(g^{(\alpha+r)/\beta}; \forall j \epsilon S : D_j = g^{r}.H(j)^{rj}; D'_j = g^{rj}\right) \quad (۳)$$

۳. $Enc(PK, PT, T) \rightarrow CT$: متن ساده PT، خط‌مشی دسترسی T و PK را به‌عنوان ورودی می‌گیرد و متن رمز CT را خارج می‌کند.

$H : \{0, 1\}^* \rightarrow G_1$ ،$q_r(0) = s$ و $q_{x(0)} = q_{parent(x)}(index(x))$ است. تابع H هر رشته دلخواه از ۰ و ۱ را به یک عضو یکتا گروه G_1 نگاشت می‌کند. Y مجموعه برگ‌های درخت دسترسی است. در طرح بتنکورت [۵]، خط‌مشی دسترسی از مدل درخت دسترسی است.

$$CT = \left(T; C' = PT.e(g; g)^{\alpha s}; C = h^{s}; \forall y \epsilon Y : C_y = g^{q_y(0)}.H(j)^{rj}; C'_y = g^{rj} = H(att(y))^{q_y(0)}\right) \quad (۴)$$

۴. $Dec(PK, SK, CT) \rightarrow PT$: SK و CT را به‌عنوان ورودی می‌گیرد. اگر S، T را برآورده کند، PT را خارج می‌کند. اگر گره x یک گره برگ باشد و $i = att(x)$، می‌بایست به‌صورت بازگشتی و به کمک تابع زیر عمل نمود تا پس از راضی شدن درخت دسترسی امکان رمزگشایی توسط کاربر داده مجاز فراهم شود. درصورتی‌که $i \neq att(x)$ باشد $DecryptNode(CT, SK, x) = \perp$ و عملیات ناتمام باقی می‌ماند. جزئیات بیشتر را می‌توانید در [۶] ملاحظه بفرمائید.

$$DecryptNode(CT, SK, x) = \frac{e(D_i, C_x)}{e(D_i, C_x)} = e(g, g)^{rq_x(0)} \quad (۵)$$

۲-۳- سیستم اعداد مانده‌ای

سیستم اعداد مانده‌ای[1] در [۸] به تفضیل این سیستم عددی نامتعارف معرفی شده است. در RNS ابتدا یک عدد صحیح بزرگ بر اساس تبدیل به جلو[2] به مجموعه‌ای از باقیمانده‌ها که اعداد صحیح کوچک هستند تبدیل می‌شود. سپس محاسباتی مانند جمع، تفریق و ضرب بر روی آنها انجام می‌شود. در پایان به کمک تبدیل معکوس[3] مجدداً مجموعه مانده‌ها به یک عدد صحیح بزرگ تبدیل می‌شود. در واقع حسن این سیستم، کمک به انجام محاسبات با سربار کمتر و به شکل موازی است. در تبدیل به جلو به ترتیب مراحل زیر را انجام می‌دهیم:

۱- مجموعه‌ای از اعداد صحیح نسبتاً کوچک را انتخاب می‌کنیم که نسبت به یکدیگر اول هستند و به آن مجموعه پیمانه $\{m_1, m_2, \cdots, m_n\}$ می‌گوییم.

۲- باقیمانده یک عدد صحیح دلخواه بزرگ X را نسبت به پیمانه‌های متعلق به مجموعه پیمانه با طول n را محاسبه می‌کنیم.

$$\{x_i \mid x_i = X \bmod m_i \ \ for\ 1 \leq i \leq n\} \quad (۶)$$

قضیه باقیمانده چینی[4] (CRT) و تبدیل ریشه مختلط[5] (MRC) دو تکنیک اصلی برای تبدیل معکوس هستند. اخیراً تکنیک‌های جدید مبتنی بر این دو روش مانند New CRT-I، New CRT-II و Mixed-Radix CRT نیز ارائه شده است [۸]. MRC ساختار سریال دارد و CRT ساختار موازی دارد. باتوجه‌به قابلیت‌های CRT، معمولاً از این روش استفاده می‌شود. جایی که $M_i = M/m_i$ برای $i = 1, 2, \ldots, n$ و $M = \prod_{i=1}^{n} M_i$ به عنوان محدوده دینامیکی شناخته می‌شود. هر عدد صحیح بزرگ تنها زمانی نمایش منحصر بفرد RNS دارد که مقدارش بین ۰ و محدوده دایناميکی باشد. $\left(\frac{1}{M_i}\right)_{m_i}$ به‌عنوان معکوس ضربی نسبت به پیمانه M_i شناخته می‌شود.

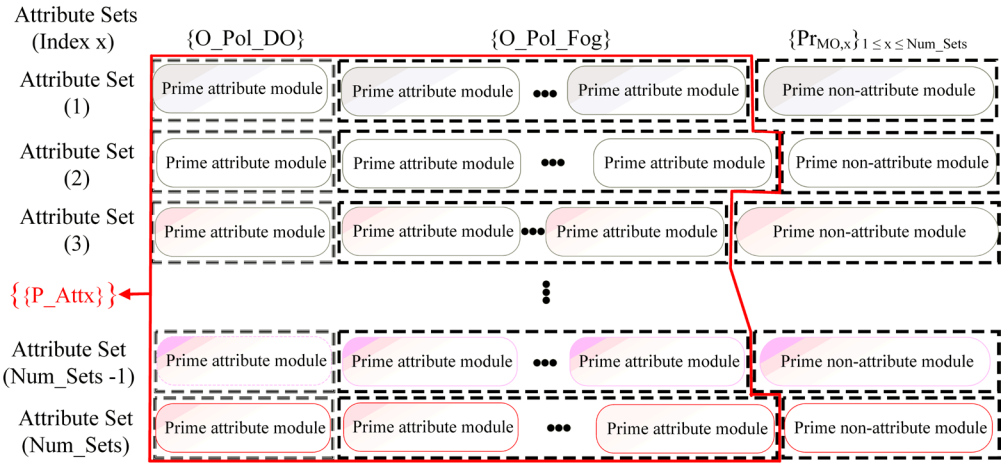
$$X = \sum_{i=1}^{n} x_i M_i \left(\frac{1}{M_i}\right)_{m_i} \bmod M \quad (۷)$$

$$\left(M_i \left(\frac{1}{M_i}\right)\right)_{m_i} = 1 \quad (۸)$$

۲-۴- خط‌مشی دسترسی سیستم اعداد مانده‌ای

مطابق با شکل (۱) هر ویژگی استفاده شده در این ساختار [۹] که دارای طول متغیر است، باید از طریق تابع هش SHA ۳-۵۱۲[6] به یک‌رشته عددی ۵۱۲ بیتی تبدیل شود. آن را ماژول ویژگی[7] نام‌گذاری می‌کنیم. در طول رمزگذاری، باقیمانده‌های یک عدد صحیح بزرگ را نسبت به ماژول‌های ویژگی محاسبه می‌کنیم. در واقع عدد صحیح بزرگ، متن ساده است و مجموعه باقیمانده‌ها نسبت به ماژول‌های ویژگی، متن رمز است. ازآنجاکه لازم است ماژول‌ها در سیستم اعداد مانده‌ای عدد اول[8] باشند، همه ماژول‌های ویژگی باید به یک عدد اول معادل تبدیل شوند؛ بنابراین، کوچک‌ترین عدد اول بزرگ‌تر از مقدار هر ماژول ویژگی را انتخاب می‌کنیم و آن را ماژول ویژگی اول[9] می‌نامیم.

[1] Residue number system (RNS)
[2] Forward conversion
[3] Reverse conversion
[4] Chinese Remainder Theorem
[5] Mixed Radix Conversion
[6] SHA3-512 hash function
[7] Attribute module
[8] Prime
[9] Prime attribute module



شکل (۱): خط‌مشی دسترسی سیستم اعداد مانده‌ای [۹]

در این طرح که هدف آن اجرای کنترل دسترسی ریزدانه با استفاده از رمزنگاری ویژگی مبنا است، ویژگی، ماژول ویژگی و ماژول ویژگی اول را برای سادگی معادل یکدیگر در نظر می‌گیریم. این ساختار یک آرایه دوبعدی است که در آن مجموعه معتبری از ماژول‌های ویژگی اول در هر سطر به جز آخرین ستون بارگذاری می‌شود. در هر ستون، یک ماژول ویژگی اول که عضوی از آن مجموعه است قابل‌بارگذاری است. تعداد سطرها برابر با Num_sets است و تعداد ستون‌های هر سطر می‌تواند متفاوت باشد. اگر ویژگی‌های متعلق به یک کاربر داده دقیقاً با ماژول‌های ویژگی اول هر خط از خط‌مشی دسترسی سیستم اعداد مانده‌ای مطابقت داشته باشد، می‌تواند آن را راضی نماید. هر خط از خط‌مشی دسترسی، یا به‌عبارت‌دیگر، هر مجموعه ویژگی که خط‌مشی دسترسی را تشکیل می‌دهد، از سه مدل ماژول به شرح زیر تشکیل شده است:

۱- مدل اول دارای طول ثابت ۵۱۲ بیت است و توسط مالک داده به ماژول‌های ویژگی اول تبدیل می‌شود. این ماژول‌ها همه، اعضای مجموعه $\{O\_Pol\_DO\}$ هستند. این مجموعه باید نزد مالک داده محرمانه بماند و به کاربر داده، مه و سرورهای ابری ارسال نخواهد شد. این امر امنیت را بهبود می‌بخشد و اگر دشمن به آنها نفوذ کند، از دسترسی به کل خط‌مشی دسترسی محروم می‌شود.

۲- مدل دوم دارای طول ثابت ۵۱۲ بیت است و توسط مالک داده تعریف شده است. بااین‌حال، برای تولید ماژول‌های ویژگی اول معادل، آنها به گره مه برون‌سپاری می‌شوند تا سربار محاسباتی را کاهش دهند. همه این ماژول‌ها اعضای مجموعه $\{O\_Pol\_Fog\}$ هستند. پس از تکمیل هر دو مجموعه $\{O\_Pol\_DO\}$ و $\{O\_Pol\_Fog\}$، مالک داده بخشی از خط‌مشی دسترسی را طراحی کرده و آنها را در ردیف‌های مرتبط قرار می‌دهد. ما آن را خط‌مشی دسترسی جزئی $\{\{P\_Attx\}\}$ می‌نامیم. سپس $\{\{P\_Attx\}\}$ را به مرجع ویژگی[1] ارسال می‌کند تا مدل سوم ماژول‌های موردنیاز را دریافت کند.

۳- مدل سوم نه یک ماژول ویژگی است و نه طول ثابت ۵۱۲ بیت دارد. طول این ماژول‌ها باید متناسب با طول متن ساده و طول هر ردیف از $\{\{P\_Attx\}\}$ باشد؛ بنابراین اعداد تصادفی با طول موردنظر تولید می‌شوند و متعاقباً مرجع ویژگی کوچک‌ترین عدد اول بزرگ‌تر از آنها را محاسبه می‌کند. ما آنها را ماژول‌های بدون ویژگی اول $\{Pr_{MO,x}\}$ می‌نامیم، جایی که MO کلید عمومی مالک داده است. برای مطالعه جزئیات بیشتر به مقاله [۹] مراجعه بفرمایید.

۲-۵- طرح‌های کنترل دسترسی مبتنی بر زنجیره قالب[2]

زنجیره قالب، یک دفترکل[3] غیرقابل‌تغییر است که شامل مجموعه‌ای از بلوک‌های مرتبط است که توسط استخراج‌کنندگان در یک شبکه همتا به همتا[4] تأیید شده‌اند [۱۰]. ویژگی‌های اصلی زنجیره قالب را می‌توان به‌صورت زیر خلاصه کرد:

- تمرکززدایی: جنبه غیرمتمرکز زنجیره قالب می‌تواند هر نقطه از شکست را از بین ببرد و در نتیجه تحمل خطا را بهبود بخشد. دستگاه‌های اینترنت اشیاء می‌توانند بدون دخالت هیچ واسطه‌ای با استفاده از زنجیره قالب با یکدیگر تعامل داشته باشند.
- توزیع: زنجیره قالب به‌عنوان یک دفترکل توزیع شده، توانایی ذخیره و توزیع داده‌ها را دارد. سیستم اعتبارسنجی بر روی گره‌های مختلف تضمین می‌شود.
- تغییرناپذیری: داده‌های موجود در زنجیره قالب را نمی‌توان تغییر داد. در واقع، زنجیره قالب دنباله‌ای از بلوک‌ها است که فهرست کاملی از تراکنش‌ها را در خود جای‌داده است. هر بلوک از طریق یک مرجع به بلوک قبلی اشاره می‌کند که اساساً یک مقدار هش بلوک قبلی است. هر گونه تغییر در یک بلوک منجر به قطع ارتباط بین بلوک‌ها می‌شود که تغییرناپذیری را تضمین می‌کند.

[1] Attribute Authority (AA)
[2] Block chain
[3] Ledger
[4] Peer-to-peer (P2P)

• مقیاس‌پذیری: فناوری زنجیره قالب می‌تواند جمع‌آوری و پردازش داده‌های صادر شده از تعداد زیادی از دستگاه‌های اینترنت اشیاء را کنترل کند.
• ناشناس بودن: امکان تعامل با یک آدرس کلی وجود دارد. اطلاعات شخصی برای افزودن تراکنش، ضروری نیست.

انواع زنجیره قالب را می‌توان به سه دسته زیر طبقه‌بندی کرد:

• عمومی: همه می‌توانند به شبکه بپیوندند و می‌توانند در فرایند اعتبارسنجی تراکنش‌ها (ماینینگ) شرکت کنند.
• خصوصی: برعکس زنجیره قالب عمومی است، زیرا یک شبکه محدود است که هر عضوی که می‌خواهد به شبکه بپیوندد باید توسط یک سازمان مجاز شناخته شود.
• مرکب: ترکیبی از زنجیره قالب خصوصی و عمومی است. فرایند اعتبارسنجی توسط شرکت‌کنندگان منتخب انجام می‌شود.

راه‌حل‌های کنترل دسترسی مبتنی بر زنجیره قالب را می‌توان به دو زیر طبقه تقسیم کرد: راه‌حل‌های ایستا که در آنها خط‌مشی کنترل دسترسی در ابتدا مشخص می‌شود و راه‌حل‌های پویا که در آنها خط‌مشی به دلیل شرایط مختلف می‌تواند به‌صورت پویا تغییر کند.

۲-۶- رمزگذاری مجدد پراکسی

رمزگذاری مجدد پراکسی[1] یک پروتکل رمزگذاری سراسری است که مقیاس‌پذیرتر و انعطاف‌پذیرتر از رمزگذاری کلید عمومی است و گروهی از موجودیت‌های پراکسی مانند رایانش ابری را قادر می‌سازد تا داده‌های رمزگذاری شده را از یک کلید عمومی به کلید عمومی دیگر تبدیل کنند، بدون اینکه قدرت رمزگشایی داده‌ها را یا دسترسی به هر کلید محرمانه را پیدا کنند [۱۱]. برای درک بهتر این پروتکل اجازه دهید با مثالی آن را توضیح دهیم. فرض کنید یک مالک داده بنام محمد و دو کاربر داده به نام علی و مجید در نظر گرفته‌ایم. یک گره میانی ابری نیز جهت اشتراک‌گذاری داده بین این سه شخص مستقر شده است. محمد در ابتدا می‌خواهد متن رمزی را با استفاده از رمزگذاری کلید عمومی تولید نماید، به شکلی که فقط علی بتواند رمزگشایی کند و برای گره ابر و مجید ناممکن باشد؛ بنابراین با کلید عمومی علی، متن رمز را تولید می‌کند و آن را در اختیار ابر قرار می‌دهد تا علی بتواند به آن دسترسی بیاید. پس از مدتی، نظرش عوض می‌شود و تصمیم می‌گیرد تا بجای علی، مجید بتواند متن رمز به اشتراک گذاشته شده در گره ابری را رمزگشایی کند. روش غیر امن و با سربار محاسباتی بالاتر، آن است که کلید محرمانه محمد برای گره ابری افشا شود تا متعاقباً پس از رمزگشایی آن توسط ابر و تولید متن ساده، با استفاده از کلید عمومی مجید مجدداً رمزگذاری شود. اما در روش رمزگذاری مجدد پراکسی، یک کلید محرمانه در اختیار پراکسی قرار داده می‌شود تا بدون افشا کلید محرمانه محمد و متن ساده، متن رمز را به شکلی تغییر یابد که دیگر تنها مجید آن را بتواند رمزگشایی نماید و امکان رمزگشایی توسط علی میسر نباشد. این روش در طرح‌های کنترل دسترسی مبتنی بر خط‌مشی متن رمز برای ابطال کاربر[2] یا ابطال ویژگی[3] کاربردی است. برای شناخت بهتر طرح‌هایی که از پروتکل رمزگذاری مجدد پراکسی استفاده نمودند، مطالعه [۱۱] پیشنهاد می‌شود.

۲-۷- اینترنت وسایل نقلیه مبتنی بر معماری محاسبات مه

اینترنت وسایل نقلیه[4] با توسعه اینترنت وسایل نقلیه [۱۲]، انواع برنامه‌های کاربردی وسایل نقلیه متنوع‌تر شده‌اند و در نتیجه، درخواست‌های خدمات ایجاد شده افزایش یافته‌اند. باتوجه‌به محدودیت قدرت محاسباتی و ذخیره‌سازی وسایل نقلیه، درخواست منابع برای بسیاری از وظایف محاسباتی دشوار است. علاوه بر این، مدل‌های خدمات محاسبات ابری سنتی از تراکم شبکه، تأخیر شبکه بالا و هزینه‌های عملیاتی بالا رنج می‌برند. برای این منظور، محاسبات مه خودرو[5] در حال ظهور است. در محاسبات مه خودرو، وسایل نقلیه با چندین حسگر نصب شده برای جمع‌آوری اطلاعات ترافیک عمل می‌کنند. از طریق فناوری ارتباطات بی‌سیم، وسایل نقلیه می‌توانند ارتباطات همه‌جانبه شبکه مانند خودرو به زیرساخت[6]، وسیله نقلیه به‌وسیله نقلیه[7] و غیره را تحقق بخشند. واحدهای کنار جاده[8] مستقر در جاده‌ها به‌عنوان گره‌های مه برای پاسخگویی به درخواست‌های خودرو در زمان واقعی عمل می‌کنند و خدمات متنوعی را برای وسایل نقلیه مانند جمع‌آوری داده‌ها، ناوبری و انتقال داده ارائه می‌دهند. به‌این‌ترتیب، محاسبات مه خودرو می‌تواند به طور قابل‌توجهی تأخیر شبکه را کاهش دهد و درعین‌حال به کاربران خدمات و تجارب رانندگی ایمن، آسان، هوشمند، و کارآمد ارائه دهد.

علی‌رغم مزایای بزرگی که محاسبات مه خودرو برای ما به ارمغان می‌آورد، دستیابی به‌اشتراک‌گذاری امن و مطمئن داده در آن یک چالش بزرگ است. داده‌های مبادله شده بین وسایل نقلیه، حاوی مقادیر زیادی اطلاعات خصوصی مانند مسیرهای رانندگی و هویت کاربران است. در این سیستم پیچیده، حریم خصوصی کاربر به‌راحتی می‌تواند به خطر بیفتد. علاوه بر این، کنترل دسترسی منعطف و ریزدانه در به‌اشتراک‌گذاری داده‌ها برای جلوگیری از دسترسی غیرمجاز بسیار مطلوب است. رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز یک رویکرد برجسته برای دستیابی به کنترل دسترسی دقیق و یک به چند است. مالکان داده‌ها[9]، مجاز به تدوین خط‌مشی‌های دسترسی هستند که با فراخوانی الگوریتم رمزگذاری در متن‌های رمز جاسازی می‌شوند. کلیدهای خصوصی توزیع‌شده کاربران داده[10] به ویژگی‌هایی که دارند مربوط می‌شود. کاربران داده، تنها در صورتی می‌توانند متن‌های رمزی

[1] Proxy re-encryption (PRE)
[2] User revocation
[3] Attribute revocation
[4] Internet of Vehicles
[5] Vehicular fog computing (VFC)
[6] Vehicle-to-infrastructure (V2I)
[7] Vehicle-to-vehicle (V2V)
[8] Road side units (RSU)
[9] Data Owner (DO)
[10] Data user (DU)

را رمزگشایی کنند و متن اصلی را کشف نمایند که ویژگی‌های آنها با خط‌مشی‌های دسترسی مطابقت داشته باشد.

بااین‌وجود، قبل از به‌کارگیری طرح کنترل دسترسی مبتنی بر خط‌مشی متن رمز در محاسبات مه خودرو، موارد عملی زیر باید در نظر گرفته شود [۱۲]:

۱. ابطال ویژگی ناکارآمد: در محاسبات مه خودرو، ویژگی‌های وسیله نقلیه ممکن است به طور مکرر برای الزامات برنامه‌های مختلف تغییر کند. هنگامی که کاربر، یک ویژگی را ابطال می‌کند، حق دسترسی مربوطه باید به‌سرعت ابطال شود. بااین‌حال، این موضوع پیچیده است. ازآنجایی‌که ویژگی‌های کاربر در سیستم معمولاً توسط همه کاربران استفاده می‌شود، هر ابطال ویژگی بر سایر کاربران ابطال نشده که آن ویژگی را نیز دارند، تأثیر می‌گذارد. یکی از راه‌های رایج برای مقابله با این مسئله، رمزگذاری مجدد متن رمزی مربوط به ویژگی ابطال‌شده برای کاربرانی است که ابطال نشده‌اند، اما همچنین باید اطمینان حاصل کنیم که این متون رمزگذاری شده مجدداً می‌توانند به طور معمول توسط کاربران موجود که در ابتدا دارای امتیاز دسترسی بودند، دسترسی داشته باشند. برای این منظور، طرح‌های موجود نیز از این کاربران می‌خواهند که کلیدهای رمزگشایی مربوطه خود را به‌روزرسانی کنند. عملیات پیچیده فوق هزینه‌های محاسباتی و ارتباطی زیادی را به همراه دارد. برای خودروهایی که به تأخیر کم و کارایی بالا نیاز دارند، انجام چنین عملیات پیچیده‌ای هر بار که یک ویژگی باطل می‌شود، به طور قابل‌توجهی غیرعملی است.

۲. ذخیره‌سازی متمرکز داده: طرح‌های اشتراک داده معمولاً داده‌های کاربر را در سرورهای ابری ذخیره می‌کنند. بااین‌حال، ازآنجایی‌که ابر یک شخص ثالث نیمه قابل‌اعتماد است، یک نقطه شکست وجود دارد. هنگامی که ابر توسط یک دشمن مورد حمله قرار می‌گیرد، ممکن است تمام داده‌های کاربر را فاش کند. به‌عنوان‌مثال، در سال ۲۰۱۷، مرکز امنیتی کرامتچ[1] دریافت که یک سرور متمرکز بیش از ۵۰۰۰۰۰ سوابق خودرو، از جمله وضعیت تجهیزات خودرو، مسیرهای رانندگی و غیره را به بیرون درز داده است و حریم خصوصی صدها هزار کاربر را به خطر انداخته است. خوشبختانه، ظهور فناوری زنجیره قالب ، اجرای ذخیره‌سازی داده‌های توزیع‌شده را امکان‌پذیر کرده است. بااین‌حال، زنجیره قالب نیاز به همگام‌سازی تمام داده‌ها از زمان تشکیل بلوک پیدایش[2] (بلوک پیدایش، اولین بلوکی است که ساخته می‌شود) دارد که منجر به کمبود جدی فضای ذخیره‌سازی در زنجیره قالب می‌شود.

۲-۸- اینترنت پزشکی اشیاء

اینترنت پزشکی اشیاء[3] با ظهور دستگاه‌های پزشکی قابل پوشیدن و کاشتنی و سایر فناوری‌هایی که امکان جمع‌آوری داده‌های پزشکی را فراهم می‌کند، اینترنت پزشکی اشیاء منجر به پیشرفت‌های فناوری در مراقبت‌های بهداشتی می‌شود [۵]. بااین‌حال این پیشرفت‌ها، چالش‌های زیادی را به‌ویژه برای امنیت و حریم خصوصی اطلاعات پزشکی ایجاد می‌کنند؛ بنابراین، حفظ محرمانگی و امن نمودن اطلاعات جمع‌آوری‌شده توسط دستگاه‌های اینترنت پزشکی اشیاء همچنان موضوع اصلی تحقیقاتی است. اگرچه ظهور محاسبات مه مشکلات متعددی را که در معماری‌های مبتنی بر رایانش ابر سنتی آشکار بود حل می‌کند، اما امنیت داده‌های پزشکی همچنان یک نگرانی است. معماری‌های فعلی که برای محافظت از داده‌ها توسعه یافته‌اند، توانایی‌های محدود دستگاه‌ها را در نظر نمی‌گیرند، مانند ظرفیت ذخیره‌سازی و انرژی که بر طول عمر دستگاه‌ها و اثربخشی آنها در گرفتن و ارسال سیگنال‌ها تأثیر می‌گذارد؛ بنابراین، به‌منظور اطمینان از حفاظت کافی از اطلاعات پزشکی، یک معماری امن مبتنی بر رایانش ابری و محاسبات مه موردنیاز است.

۳- مروری بر طرح‌های پیشین

بتنکورت و همکاران برای اولین‌بار یک مدل عملیاتی مبتنی بر خط‌مشی متن رمز بر اساس رمزنگاری مبتنی بر زوج نگار دوخطی ارائه نمود. مهم‌ترین مزیت این طرح رمزگذاری یک به چند است که به زیرساخت محاسبات ابری کاملاً مطمئن نیاز ندارد. بااین‌حال، مشکل اصلی این طراحی، عدم سادگی محاسبات ابطال کاربر و ابطال ویژگی است. همچنین، این طرح مستعد حملات تبانی است [۶]. در [۱۳]، یک طرح کنترل دسترسی کارآمد باقابلیت برون‌سپاری و به‌روزرسانی ویژگی با استفاده از محاسبات مه پیشنهاد شده است. در [۱۴] که اساس [۱۵] است، نویسندگان یک معماری چندلایه برای مرجع ویژگی بر اساس رمزنگاری ویژگی مبنا سلسله‌مراتبی[4] پیشنهاد کرده‌اند. علاوه بر این، با استفاده از امضای مبتنی بر ویژگی، تغییر مجاز داده‌ها تضمین می‌شود. بااین‌حال، محاسبات مه در این مقاله استفاده نشده است. سپس، نویسندگان در [۱۵] یک طرح برون‌سپاری داده امن و سبک‌وزن ارائه می‌کنند و بیشتر عملیات پرهزینه را از دستگاه‌های اینترنت اشیاء به گره‌های مه منتقل می‌کنند. همچنین امکان به‌روزرسانی متن رمز در زیرساخت ابری را با استفاده از امضای مبتنی بر ویژگی فراهم می‌کند. در [۱۶]، یک طرح یادگیری الکترونیکی امن و کارآمد مبتنی بر مه معرفی شده است و متعاقباً محاسبات مه را در سیستم آموزش الکترونیکی ادغام می‌کند تا تأخیر خدمات آموزش الکترونیکی ارائه شده را کاهش دهد. براین‌اساس، نویسندگان، یک طرح کم هزینه ترکیبی با کمک رمزنگاری ویژگی مبنا و رمزنگاری پخش مبتنی بر هویت[5] طراحی

[1] Kromtech
[2] Genesis Block
[3] Medical Internet of Things (MIoT)
[4] Hierarchical attribute-based encryption (HABE)
[5] Identity-Based Broadcast Encryption (IBBE)

می‌کنند. رمزنگاری پخش مبتنی بر هویت، یک روش کارآمد برای پخش یک پیام به چندین هویت پیشنهاد می‌دهد. در این روش متن رمز با یک لیست پخش هویت، رمزگذاری می‌شود به طوری که تنها کاربرانی که هویتشان به لیست تعلق دارد می‌توانند متن رمز را رمزگشایی کنند. برخلاف روش رمزنگاری پخش مبتنی بر هویت، رمزنگاری مبتنی بر هویت[1] سنتی باید پیام را به چندین گیرنده یک به یک و به ترتیب و نه همزمان ارسال کند. این قابلیت، بکارگیری روش رمزنگاری پخش مبتنی بر هویت را در بسیاری از برنامه های کاربردی مانند سیستم‌های ایمیل کارا می‌کند. با این حال، مشکل سپردن (ذخیره‌سازی) کلید[2]، یک چالش جدی است [۱۷].

نویسندگان [۱۸] ابتدا یک مدل رمزنگاری ویژگی مبنا به نام MABE[3] را با یک تابع هش مقاوم در برابر برخورد معرفی می‌کند. سپس از آن برای ایجاد یک سیستم کنترل دسترسی اشتراک‌گذاری داده در رایانش ابری استفاده می‌کند. طرح‌های مبتنی بر خط‌مشی متن رمز به‌ندرت بر ابطال کاربر و ابطال ویژگی در محاسبات مه تمرکز می‌کند و همچنان سربار محاسباتی و ذخیره‌سازی بالایی را بر روی دستگاه‌های اینترنت اشیاء با منابع محدود تحمیل می‌کند؛ بنابراین، [۱۹] یک طرح برون‌سپاری رمزگذاری کارآمد مبتنی بر ابطال کاربر و ابطال ویژگی برای اینترنت اشیاء با استفاده از محاسبات مه ارائه می‌دهد. در [۲۰]، نویسندگان طرح‌های رمزگذاری مبتنی بر هویت فازی[4] اصلاح‌شده را پیشنهاد می‌دهند که از عملیات زوج‌نگار کمتری در مقایسه با طرح رمزگذاری مبتنی بر هویت فازی اصلی استفاده می‌کنند. طرح رمزگذاری مبتنی بر هویت فازی یک مورد خاص از رمزنگاری ویژگی مبنا است که خط‌مشی دسترسی به جای درخت دسترسی از یک دروازه آستانه ساده استفاده می‌نماید. در این طرح، یک مفهوم امنیتی جدید به نام امنیت انتخابی مشروط ۲[5] معرفی می‌شود که از مفهوم امنیتی انتخابی قوی تر است. همچنین در [۲۰] دو طرح رمزگذاری ویژگی مبنا مبتنی بر خط‌مشی کلید[6] پیشنهاد شده است که از عملیات زوج نگار کمتری در مقایسه با طرح‌های مشابه قبلی استفاده می‌کنند. در این طرح، عملیات سنگین مانند ضرب اسکالر در یک نقطه منحنی، توان و زوج نگار برون‌سپاری می‌شوند تا دستگاه‌های اینترنت اشیا بتوانند با پیچیدگی‌ها کنار بیایند.

در [۲۱]، میائو و همکاران. یک سیستم جستجوی متن رمزی ریزدانه سبک‌وزن[7] با معماری محاسبات مه مبتنی بر خط‌مشی متن رمز و رمزگذاری قابل‌جستجو[8] ارائه کرد. با انتقال محاسبات با سربار زیاد به گره مه، این طرح می‌تواند دسترسی به متن رمز را با کمک کلمات کلیدی با کارایی مناسب جستجو و کنترل کند. ژانگ و همکاران [۲۲] طرحی را با ساختار دسترسی پنهان در محاسبات ابری ارائه می‌دهد که می‌تواند حریم خصوصی کاربران را حفظ نماید و قابلیت‌های برون‌سپاری صحت‌سنجی شده و کنترل دسترسی ریزدانه را ارائه دهد. اینترنت وسایل نقلیه دارای رانندگی خودکار و ارتباطات نسل پنجم است که توجه بی‌سابقه‌ای را در دانشگاه و صنعت به خود جلب کرده است. رمزگشایی برون‌سپاری شده به مه در این طرح‌ها همچنان از محاسبات سریالی با سرعت پایین استفاده می‌کند و تجربه کاربری ضعیفی را ایجاد می‌کند؛ بنابراین، فنگ و همکاران [۲۳] یک مدل رمزگشایی برون‌سپاری شده موازی هوشمند لبه[9] برای اینترنت وسایل نقلیه پیشنهاد کردند. نویسندگان [۱۱] ترکیبی از الگوریتم‌های رمزگذاری متقارن و نامتقارن سبک‌وزن را بر اساس رمزگذاری مجدد پراکسی برای افزایش امنیت داده‌ها با کمک محاسبات مه در اکوسیستم اینترنت اشیاء پیشنهاد کرد. سیستم‌های پرونده پزشکی الکترونیکی[10]، کارایی خدمات پزشکی را افزایش می‌دهد، عملکرد منابع انسانی را بهبود می‌بخشد و تجویز دارو را دقیق‌تر می‌کند. باتوجه‌به حساسیت سوابق پزشکی، مسائل امنیتی در سیستم‌های اشتراک از اهمیت بالایی برخوردار است. طرح [۲۴] یک کنترل دسترسی سبک‌وزن برای به‌اشتراک‌گذاری سیستم‌های پرونده الکترونیک پزشکی در رایانش ابری با همکاری محاسبات مه پیشنهاد کرد. در [۲۵]، مدل استاندارد برای خط‌مشی دسترسی بر اساس مدل اشتراک‌گذاری راز خطی تعریف شد. این مدل نسبت به خط‌مشی دسترسی مبتنی بر درخت، عمومی‌تر است و عملکرد مطلوبی دارد. این ساختار مبتنی بر ماتریس تولید سهم است.

لی و همکاران [۱۹] طرحی را ارائه کردند که ابطال ویژگی و ابطال کاربر هم‌زمان را با استفاده از درخت باینری کِک[11] و محاسبات مه اجرا می‌کرد. همچنین سربار به‌روزرسانی متن رمز با جداسازی اطلاعات سرصفحه[12] از آن کاهش می‌یابد. سارما و همکاران [۲۶] طرحی به نام پک‌فیت[13] را با کمک محاسبات مه معرفی کردند که در برابر سپردن کلید مقاوم است. به‌عبارت‌دیگر، هیچ مرجعی به‌تنهایی نمی‌تواند متن رمز را رمزگشایی کند. آنها از مکانیزم ابطال ویژگی استفاده می‌کنند که فقط عناصر ابطال شده را بروز می‌کند، نه همه اجزای متن رمز را. سارما و همکاران در [۲]، طرحی به نام آرم‌فیت[14] ارائه کردند که از محاسبات مه استفاده می‌کرد. هدف آن ابطال ویژگی‌ها، ادغام[15] دو یا چند ویژگی، برون‌سپاری محاسبات سربار سنگین و اعطای دسترسی ویژه به کاربران خاص به طور کارآمد و هم‌زمان بود. مقاله [۲۷] یک طرح اشتراک داده شبکه هوشمند[16] مبتنی بر کنترل دسترسی ویژگی را بر اساس معماری محاسبات مه پیشنهاد می‌کند که دارای ابطال اختیارات امنیتی برای برآورده‌کردن الزامات امنیتی شبکه هوشمند است. در این طرح پارامترهای نسخه به بخشی از متن رمز و کلید محرمانه اضافه می‌شود و

[1] Identity-based encryption (IBE)
[3] Key escrow
[3] Matchmaking attribute-based encryption
[4] Fuzzy identity-based encryption (FIBE)
[5] Conditional Chosen Ciphertext Attack-2 (Conditional CCA-2)
[6] Key Policy-Attribute Based Encryption (KP-ABE)
[7] Lightweight Fine-Grained ciphertexts Search (LFGS)
[8] Searchable encryption (SE)
[9] ABEM-POD
[10] Electronic medical record (EMR)
[11] KEK tree
[12] Header
[13] PAC-FIT
[14] ARM-FIT
[15] Merging
[16] Smart Grid

امنیت را بهبود می‌بخشد. قابلیت‌های دیگر آن، رمزگشایی برون‌سپاری شده قابل‌تأیید، مراجع ویژگی چندگانه و ابطال کاربران است. مهم‌ترین اشکال طرح، هزینه زیاد به‌روزرسانی کلید در صورت ابطال مجوز است. برخلاف [۲۷]، در [۲۸] محاسبات سنگین در هر دو مرحله رمزگذاری و رمزگشایی به محاسبات مه و رایانش ابری برون‌سپاری شده است و نتایج پس از بازگرداندن به کاربران مورد بررسی و آزمون قرار می‌گیرند. در واقع، هرگاه دستگاه‌ها در اینترنت اشیاء دارای محدودیت منابع پردازشی باشند، بخشی از عملیات رمزگذاری یا رمزگشایی به سرورهای ابری یا محاسبات مه برون‌سپاری می‌شود. ممکن است محاسبات مه و رایانش ابری از الگوریتم‌های تعریف شده پیروی نکنند، فقط بخشی از محاسبات را اجرا کنند یا عمداً نتایج نادرستی را برگردانند. اگر این اتفاق بیفتد، مالک داده یا کاربر داده نمی‌تواند متوجه خطا شود و بخش بزرگی از محاسبات تحت تأثیر قرار می گیرد. بنابراین، لازم است نتایج رمزگذاری و رمزگشایی برون‌سپاری شده توسط کاربران صحت‌سنجی و تأیید گردند.

نویسندگان [۲۹] طرحی با نام RLT-CPABE را معرفی می‌کنند که امنیت داده‌ها را با ادغام مکان و زمان در فرایند رمزگذاری و رمزگشایی بهبود می‌بخشد. طرح از یک تابع اشتقاق محدوده واحد[1] برای پیاده‌سازی مقایسه محدوده زمانی و تکنیک رمزگذاری مجدد برای جاسازی زمان جاری در متن رمز استفاده می‌کند. از دیگر قابلیت‌های آن می‌توان به پشتیبانی مؤثر از ویژگی‌های متنی ثابت (ویژگی‌های عادی) و پویا (زمان و مکان)، ابطال کاربر و برون‌سپاری رمزگشایی به سرورهای مه اشاره نمود. نویسندگان در مقاله [۳۰]، یک طرح اشتراک‌گذاری سبک‌وزن و کارآمد برای حفظ حریم خصوصی پرونده‌های پزشکی الکترونیکی، بر اساس فناوری‌های اینترنت اشیاء، محاسبات مه و زنجیره قالب پیشنهاد کردند. علاوه بر این، قراردادهای هوشمندی[2] را برای پشتیبانی از پرس‌وجوهای متن رمز از طریق فهرست ذخیره‌شده، احراز هویت کاربر و قابلیت ممیزی[3] توسعه دادند. در مقاله [۳۱]، نویسندگان یک تکنیک به‌اشتراک‌گذاری داده چند مرجع امن و ترکیبی را برای یک سیستم مدیریت هوشمند بیمارستان[4] با رمزنگاری ویژگی مبنا، رمزگذاری بلو فیش[5] و امضای دیجیتال BLS[6] پیشنهاد شده است. در این طرح، داده‌های پزشکی در سرورهای مه و سرورهای ابری ذخیره و از احراز هویت چندگانه برای جلوگیری از فریب استفاده می‌شود. در مقاله [۳۲]، طرح SHARE-ABE پیشنهاد می‌شود که دارای قابلیت‌های همکاری[7] بین کاربران یک گروه و بهره‌گیری از خط‌مشی دسترسی پنهان[8] با معرفی ویژگی‌های نادرست[9]است. به‌عبارت‌دیگر، یک ویژگی همکاری تعریف می‌شود تا به کاربران درون یک گروه اجازه داده شود تا ویژگی‌های خود را درحالی‌که خط‌مشی دسترسی را برآورده می‌کنند ترکیب نمایند. علاوه بر این، از یک پروکسی برای افزودن ویژگی‌های نادرست به خط‌مشی دسترسی استفاده می‌شود تا کاربران مخرب نتوانند ویژگی‌های واقعی را حدس بزنند. همچنین فرایند رمزگشایی به سرورهای مه برون‌سپاری می‌شود.

در [۳۳] یک طرح رمزگذاری پخش ویژگی مبنا چند مرجع[10] پیشنهاد می‌شود که با تنظیم چند مرجع، مشکل سپردن کلید را حل می‌کند و از محدودیت‌های پهنای باند جلوگیری می‌نماید؛ بنابراین، چندین مقام به طور مشترک توزیع ویژگی‌ها را در طول فرایند تولید کلید مدیریت می‌کنند. به‌علاوه فرایند رمزگشایی به گره مه برون‌سپاری می‌شود. در [۳۴] طرح SPMAC معرفی شده است که معماری آن همانند طرح قبلی، مبتنی بر مراجع چندگانه است. این طرح از ابطال کاربر و ویژگی پشتیبانی می‌کند و با مخفی‌سازی کامل خط‌مشی دسترسی، از حریم خصوصی کاربران حمایت می‌کند. یانگ و همکاران [۳۵] یک طرح غیرمتمرکز ارائه کردند. آنها از دو روش ابطال ویژگی دوره‌ای و ابطال ویژگی فوری به طور هم‌زمان استفاده کردند. آنها همچنین از روش برون‌سپاری اختیاری برای رمزگشایی استفاده کردند. علی‌زاده و همکاران در [۹] یک طرح کنترل دسترسی رمزنگاری ویژگی مبنا ارائه کردند که می‌تواند در سیستم اعداد مانده‌ای پیاده‌سازی شود و از محاسبات با سربار ناچیز به‌جای عملیات نمایی و زوج نگار دوخطی استفاده می‌کند. آنها همچنین یک ساختار دسترسی مبتنی بر سیستم اعداد مانده‌ای ارائه کرده‌اند که دارای قابلیت موازی‌سازی است و از توابع بازگشتی استفاده نمی‌کند. در [۳۶]، لو و همکاران طرحی را بر اساس فناوری زنجیره قالب و رمزگذاری مجدد پراکسی ارائه کردند که دارای ویژگی‌های ابطال ویژگی، جستجوی کلمه کلیدی و ردیابی ویژگی در کلید محرمانه است. بااین‌حال، دارای نقاط ضعفی مانند نشت اطلاعات محرمانه، راندمان اجماع کم و به‌روزرسانی پیچیده مجوز برای حفظ داده‌ها در پلتفرم‌های ابری است. رمزگذاری ویژگی مبنا مقاوم در برابر نشت[11]، یکی از روش‌های کارآمد برای مقابله با حملات کانال جانبی[12] است. از طریق حمله کانال جانبی، کاربران مخربی که از ماهیت فیزیکی عملیات رمزنگاری مانند زمان‌بندی، توان مصرفی و تشعشعات، استفاده مجدد از کلید محرمانه یا تصادفی بودن برخی از برنامه‌ها سوءاستفاده می‌کنند، می‌توانند برخی از اطلاعات مخفی را دریافت کنند [۳۷]. در [۳۸]، طرح کنترل دسترسی PRE-CPABE برای حل مشکلات زنجیره قالب ، به‌روزرسانی متن رمزنگاری شده و رمزگذاری متقارن انجام شده است. در [۳۹]، تلاشی برای مقابله با حملات ایداس[13]و ابطال کاربران مخرب با کمک زنجیره قالب، به‌روزرسانی متن رمز و رمزگذاری متقارن انجام شده است. هیچ یک از طرح‌های [۳۶-۳۹] از محاسبات مه

[1] Single range derivation function
[2] Smart contracts
[3] Auditability
[4] Smart hospital management systems (SHMS)
[5] Blowfish
[6] Boneh-Lynn-Sacham
[7] Collaboration
[8] Hidden access policy
[9] False attribute
[10] Multi-authority attribute-based broadcast encryption (MA-ABBE)
[11] Leakage-resilient
[12] Side-channel attack
[13] EDoS

استفاده نکرده‌اند. فوگکیا[1] و همکاران [۴۰] یک طرح کنترل دسترسی برای حفاظت از پرونده‌های الکترونیک سلامت[2] بر اساس فناوری زنجیره قالب و محاسبات مه پیشنهاد کردند. این طرح دارای قابلیت ابطال کاربر بر اساس مدل‌سازی مبتنی بر نمودار است. با درنظرگرفتن حفاظت از حریم خصوصی و انتقال امن داده‌های مشترک در شبکه‌های اجتماعی خودرویی[3]، رِن و همکاران [۴۱]، طرح کنترل دسترسی BFDAC مبتنی بر زنجیره قالب و محاسبات مه را پیشنهاد کردند. شبکه‌های اجتماعی خودرویی، خدمات متعددی مانند رانندگی ایمن، به‌اشتراک‌گذاری داده‌ها و مدیریت ترافیک را در اختیار مسافران، رانندگان و وسایل نقلیه قرار می‌دهند. طرح BFDAC از ردیابی و ابطال کاربر پشتیبانی می‌کند و کاربران می‌توانند داده‌های اشتراک‌گذاری شده ذخیره شده در ابر را نیز باطل کنند.

۴- ارزیابی قابلیت‌های طرح‌ها

طرح‌هایی که از معماری محاسبات مه بهره بردند و در بخش قبلی مورد بررسی قرار گرفتند را طبق جدول (۱) و جدول (۲) مقایسه می‌کنیم و از منظر قابلیت‌ها و ویژگی‌های طرح‌های کنترل دسترسی مبتنی بر CP-ABE نظیر ابطال ویژگی و ابطال کاربر، پنهان‌سازی خط‌مشی، مدل خط‌مشی دسترسی، عملیات زیربنایی، کاربرد طرح و سایر قابلیت‌های افزونه، آنها را مورد آنالیز قرار می‌دهیم. همان‌گونه که ملاحظه می‌شود قابلیت ابطال ویژگی و کاربر دارای اهمیت است و بسیاری از مقالات مانند [۲،۱۹،۲۶،۲۷،۲۹،۳۴،۴۰،۴۱،۴۲] هردو یا یکی از آنها را پیاده‌سازی نموده‌اند. متأسفانه سربار محاسباتی عملیات ابطال زیاد است. به طور کلی در ابطال ویژگی دو عمل انجام می‌شود. ۱- بروزرسانی کلید محرمانه کاربرانی که ویژگی‌های مشابه آنها ابطال نشده است و ۲- بروزرسانی متن رمز برای کاربرانی که ویژگی‌های مشابه آنها ابطال نشده است. در معماری مبتنی بر محاسبات مه و رایانش ابری، وظیفه بروزرسانی متن رمز بر عهده سروهای ابری است و به چند مدل انجام می‌شود. در مدل اول [۴۲] که دارای بیشترین سربار است کلیه پارامترهای متن رمز شامل پارامترهای وابسته به ویژگی‌ها و پارامترهای غیر وابسته به ویژگی‌ها بروزرسانی می‌شود. در این مدل ویژگی‌هایی که ابطال نیز نشده‌اند تغییر می‌کنند. علاوه بر این به دلیل تغییر اجزای محرمانه متن رمز توسط سرور ابری، امنیت ابطال طرح کاهش می‌یابد. در مدل دوم [۲،۲۶] تنها ویژگی‌هایی که برای برخی کاربران ابطال شده است بروزرسانی می‌شود و در نتیجه سربار عملیات ابطال ویژگی کاهش می‌یابد. در مدل سوم [۷،۱۹] از روش رمزگذاری مجدد پراکسی برای بروز رسانی پارامترهای ویژگی‌های غیر ابطال شده متن رمز استفاده می‌شود و دارای امنیت مناسبی است. امکان دسترسی سرور ابری به پارامترهای محرمانه متن رمز وجود نخواهد داشت. مقالات [۱۹،۲۷،۲۹،۳۴] دارای قابلیت ابطال کاربر هستند. در این مقالات به هر کاربر علاوه بر ویژگی‌ها، هویت یا شناسه‌ای منحصر بفرد نیز اعطا می‌شود

جدول (۱): مقایسه قابلیت‌های طرح‌های مبتنی بر محاسبات مه

مقاله	نام طرح	کاربرد خاص	سایر قابلیت‌ها
[۱]	-	VFC	پنهان‌سازی
[۲]	ARM-FIT	ندارد	ادغام ویژگی
[۹]	RNS-ABE	ندارد	ندارد
[۱۶]	IBBE-ABE	E-learning	IBBE
[۱۸]	MABE	ندارد	Matchmaking
[۱۹]	-	ندارد	ندارد
[۲۱]	LFGS	ندارد	- رمزگذاری قابل‌جستجو - به‌روزرسانی ویژگی
[۲۲]	-	ندارد	- صحت‌سنجی عملیاتِ برون‌سپاری شده - پنهان‌سازی
[۲۳]	ABEM-POD	IoV	محاسبات موازی
[۲۴]	-	EMR	KP-ABKS[4]
[۲۶]	PAC-FIT	ندارد	مقاوم با سپردن کلید
[۲۷]	-	Smart Grid	صحت‌سنجی عملیاتِ برون‌سپاری شده
[۲۹]	RLT-CPABE	ندارد	ویژگی‌های پویا مبتنی بر زمان و مکان
[۳۰]	-	EMR	- زنجیره قالب - توسعه قراردادهای هوشمند - ممیزی
[۳۱]	-	SHMS	امضای BLS
[۳۲]	SHARE-ABE	ندارد	- همکاری کاربران - پنهان‌سازی
[۲۹]	MA-ABBE	ندارد	رمزگذاری پخش
[۳۴]	SPMAC	ندارد	تکنیک توکن‌های وب JSON[5] - پنهان‌سازی
[۴۰]	-	EHR	- زنجیره قالب -رمزگذاری متقارن
[۴۱]	BFDAC	VSN	- زنجیره قالب - ردیابی کاربران

تا بتوان بر اساس آن دسترسی یک کاربر ابطال شود. چالش جدی آن است که بتوان طرحی با قابلیت ابطال ویژگی و کاربر ارائه نمود که تنها کاربران یا ویژگی‌های ابطال شده بروزرسانی گردند تا سربار محاسباتی کاهش یابد و وابستگی به تمامی کاربران نداشته باشد.

قابلیت دیگر، پنهان‌سازی خط‌مشی دسترسی در متن رمز است تا بتوان حریم خصوصی را برای کاربران داده حفظ نمود. در مقالات [۲۲،۳۲،۳۴] به این مهم توجه شده است. با توجه به آنکه خط‌مشی دسترسی در متن رمز جایگذاری می‌شود، لازم است تمهیدی اندیشه شود تا بدون تحمیل سربار محاسباتی زیاد آنرا رمزگذاری کرد و تنها کاربران مجاز امکان دسترسی به آنرا به صورت محدود و بدون افشای ویژگی‌هایی که دارا نمی‌باشند، داشته باشند.

[1] Fugkeaw
[2] Electronic Health Record (EHR)
[3] Vehicular social networks (VSN)

[2] Key-policy attribute-based keyword search encryption
[3] JavaScript Object Notation (JSON) web tokens technique

جدول (۲): مقایسه ویژگی‌های طرح‌های مبتنی بر محاسبات مه

مقاله	نام طرح	قابلیت ابطال	عملیات زیر بنایی	مرجع ویژگی	مدل خط‌مشی
[۱]	-	خیر	زوج نگار	یگانه	LSSS
[۲]	ARM-FIT	ویژگی	زوج نگار	یگانه	درخت
[۹]	RNS-ABE	خیر	RNS	یگانه	RNS
[۱۶]	IBBE-ABE	خیر	زوج نگار	یگانه	درخت
[۱۸]	MABE	خیر	زوج نگار	یگانه	LSSS
[۱۹]	-	ویژگی کاربر	زوج نگار	چندگانه	درخت
[۲۱]	LFGS	خیر	زوج نگار	یگانه	درخت
[۲۲]	-	خیر	زوج نگار	یگانه	LSSS
[۲۳]	ABEM-POD	خیر	زوج نگار	یگانه	درخت یا Lsss
[۲۴]	-	خیر	زوج نگار	یگانه	درخت
[۲۶]	PAC-FIT	ویژگی	زوج نگار	چندگانه	درخت
[۲۷]	-	ویژگی کاربر	زوج نگار	چندگانه	درخت
[۲۹]	RLT-CPABE	کاربر	زوج نگار	یگانه	درخت
[۳۰]	-	خیر	XOR	یگانه	-
[۳۱]	-	خیر	زوج نگار	چندگانه	AND-OR
[۳۲]	SHARE-ABE	خیر	زوج نگار	یگانه	درخت
[۲۹]	MA-ABBE	خیر	زوج نگار	چندگانه	درخت
[۳۴]	SPMAC	ویژگی کاربر	زوج نگار	چندگانه	LSSS
[۴۰]	-	کاربر	زوج نگار	یگانه	درخت
[۴۱]	BFDAC	کاربر	زوج نگار	چندگانه	LSSS

اکثریت قاطع طرح‌های CP-ABE از عملیات زیربنایی زوج نگار دوخطی استفاده می‌کنند. در این طرح‌ها باهدف کاهش سربار محاسباتی دستگاه‌های با منابع محدود پردازشی، بخشی از عملیات زوج نگار دوخطی به سرورهای مه یا سرورهای ابری برون‌سپاری می‌شود. برون‌سپاری محاسبات چالش‌های امنیتی و حفظ حریم خصوصی ایجاد می‌کند؛ بنابراین چالش مهمی که هنوز باقی‌مانده است، آن است که آیا می‌توان از عملیات زیربنایی ذاتاً سبک‌وزن بهره برد طوریکه نیاز به برون‌سپاری محاسبات به طور کامل مرتفع گردد. نویسندگان در [۸] تلاش نمودند این چالش را برطرف کنند. اما تنها توانستند مرحله رمزگشایی را ذاتاً سبک‌وزن سازند. در این طرح آنها از سیستم اعداد مانده‌ای بهره گرفتند و خط‌مشی دسترسی مختص به آنرا طراحی نمودند. یکی دیگر از قابلیت‌های ضروری صحت‌سنجی کلیه عملیات برون‌سپاری شده است که در [۲۲،۲۷] به آن توجه شده است. متأسفانه سربار محاسباتی به کاربران تحمیل می‌شود و لازم است در جهت کاهش آن در آینده تلاش نمود.

براین‌اساس، پیشنهاد می‌شود در آینده، محققین گرامی در حوزه بهبود قابلیت‌ها، کارایی و امنیت طرح‌های CP-ABE مبتنی بر معماری محاسبات مه پژوهش‌های جامع‌تری انجام داده و تلاش نمایند تا به کمک فناوری‌هایی نظیر زنجیره قالب و RNS، کارایی آنها را به طور ذاتی بهبود دهند.

۵- نتیجه

یکی از کاربردی‌ترین مدل‌های کنترل دسترسی که کمک به حفظ محرمانگی و حریم خصوصی کاربران و همچنین امنیت دستگاه‌ها و سنسورها در اینترنت اشیاء می‌کند، طرح‌های کنترل دسترسی رمزنگاری ویژگی مبنا است. مهم‌ترین و منعطف‌ترین مدل آن، طرح‌های رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز است. در این تحقیق به بررسی ویژگی‌ها و جزئیات معماری انواع طرح‌های پیشنهاد شده مبتنی بر خط‌مشی متن رمز مانند ریزدانه بودن، ساختار خط‌مشی دسترسی، ساختار مراجع ویژگی و عملیات زیربنایی آن پرداخته‌ایم. اخیراً به دلیل ماهیت عملیات زوج نگار دوخطی و محدودیت پردازشی و ذخیره‌سازی داده در بسیاری از دستگاه‌های متصل به اینترنت اشیاء، از محاسبات مه در طرح‌های مختلف بهره‌گیری شده است. باتوجه‌به اهمیت محاسبات مه در کاربردهای بلادرنگ و وابسته به مکان، به نظر می‌رسد طرح‌های مختلف مبتنی بر خط‌مشی متن رمز که از محاسبات مه بهره برده‌اند کاربردی‌تر هستند.

براین‌اساس در این تحقیق علاوه بر موارد فوق به بررسی قابلیت‌های کاربردی طرح‌های رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز نظیر ابطال ویژگی‌ها، ابطال کاربران، سپردن کلید، مخفی‌سازی خط‌مشی دسترسی تعبیه‌شده در متن رمز پرداخته‌ایم. به نظر می‌رسد تمامی طرح‌های مرور شده در کنار محسناتی که دارند، چالش‌ها و ایراداتی نیز دارند. عملیات زیربنایی آنها نظیر زوج نگار دوخطی و توان رسانی، دارای سربار بالای محاسباتی است و قابلیت‌هایی نظیر ابطال ویژگی‌ها، ابطال کاربران، سپردن کلید، عدم محرمانگی خط‌مشی دسترسی تعبیه‌شده در متن رمز و به‌کارگیری مرجع ویژگی یگانه که سبب کاهش مقیاس‌پذیری آن خواهد شد؛ دارای چالش است. باهدف رفع چالش‌های فوق، چندین راهکار توسط مقالات مختلف نظیر برون‌سپاری محاسبات زوج نگار دوخطی به محاسبات مه، استقرار مراجع ویژگیِ توزیع‌یافته و به‌کارگیری عملیاتی نظیر RNS و XOR بجای زوج نگار دوخطی موردتوجه قرار گرفته است.

مراجع

[1] T. Gan, Y. Liao, Y. Liang, Z. Zhou, and G. Zhang, "Partial policy hiding attribute-based encryption in vehicular fog computing," *Soft Computing,* vol. 25, pp. 10543-10559, 2021, doi: 10.1007/s00500-021-05996-8.

[2] R. Sarma and F. A. Barbhuiya, "A secure and efficient access control scheme with attribute revocation and merging capabilities for fog-enabled IoT," *Computers and Electrical Engineering,* vol. 104, p. 108449, 2022, doi: 10.1016/j.compeleceng.2022.108449.

[3] M. El-Hajj and P. Beune, "Lightweight public key infrastructure for the Internet of Things: A systematic literature review," Journal of Industrial Information Integration, p. 100670, 2024, doi: 10.1016/j.jii.2024.100670.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24*, 2005: Springer, pp. 457-473., doi: 10.1007/11426639_27.

[5] S. Alshehri and T. Almehmadi, "A secure fog-cloud architecture using attribute-based encryption for the medical internet of things (MIoT)," *International Journal of Advanced Computer Science and Applications,* vol. 12, no. 12, 2021, doi: 10.14569/IJACSA.2021.01212112.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*, 2007: IEEE, pp. 321-334., doi: 10.1109/SP.2007.11.

[7] J. Zhao, P. Zeng, and K.-K. R. Choo, "An efficient access control scheme with outsourcing and attribute revocation for fog-enabled E-health," *IEEE Access*, vol. 9, pp. 13789-13799 ,2021, doi: 10.1109/ACCESS.2021.3052247.

[8] P. Ananda Mohan, "Residue number systems: Theory and applications," *Basel: Birghauser, Mathematics*, 2016, doi: 10.1007/978-3-319-41385-3.

[9] M. A. Alizadeh, S. Jafarali Jassbi, A. Khademzadeh, and M. Haghparast, "Novel lightweight and fine-grained fast access control using RNS properties in fog computing," *Cluster Computing,* vol. 27, no. 3, pp. 3799-3817, 2024, doi: 10.1007/s10586-023-04169-6.

[10] R. Trabelsi, G. Fersi, and M. Jmaiel, "Access control in Internet of Things: A survey," *Computers & Security,* p. 103472, 2023, doi: 10.1016/j.cose.2023.103472.

[11] O. A. Khashan, "Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment," *IEEE Access,* vol. 8, pp. 66878-66887, 2020, doi: 10.1109/ACCESS.2020.2984317.

[12] Z. Guo, G. Wang, G. Zhang, Y. Li, and J. Ni, "A multifactor combined data sharing scheme for vehicular fog computing using blockchain," *IEEE Internet of Things Journal,* vol. 10, no. 22, pp. 20049-20064, 2023, doi: 10.1109/JIOT.2023.3282672.

[13] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," *Future Generation Computer Systems,* vol. 78, pp. 753-762, 2018, doi: 10.1016/j.future.2016.12.015.

[14] Q. Huang, Y. Yang, and M. Shen, "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing," *Future Generation Computer Systems,* vol. 72, pp. 239-249, 2017, doi: 10.1016/j.future.2016.09.021.

[15] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things," *IEEE Access,* vol. 5, pp. 12941-12950, 2017, doi: 10.1109/ACCESS.2017.2727054.

[16] A. B. Amor, M. Abid, and A. Meddeb, "Secure fog-based e-learning scheme," *IEEE Access,* vol. 8, pp. 31920-31933, 2020, doi: 10.1109/ACCESS.2020.2973325.

[17] Y. Mahi Gayathri and K. Rekha, "Comparative analysis of identity-based-broadcast encryption with attribute-based encryption for reduced storage cost of multi users in a public cloud," in AIP Conference Proceedings, 2024, vol. 2729, no. 1: AIP Publishing, doi: 10.1063/5.0168813.

[18] S. Xu *et al.*, "Match in my way: Fine-grained bilateral access control for secure cloud-fog computing," *IEEE Transactions on Dependable and Secure Computing,* vol. 19, no. 2, pp. 1064-1077, 2020, doi: 10.1109/TDSC.2020.3001557.

[19] L. Li, Z. Wang, and N. Li, "Efficient attribute-based encryption outsourcing scheme with user and attribute revocation for fog-enabled IoT," *IEEE Access,* vol. 8, pp. 176738-176749, 2020, doi: 10.1109/ACCESS.2020.3025140.

[20] M. Mahdavi, M. H. Tadayon, M. S. Haghighi, and Z. Ahmadian, "IoT-friendly, pre-computed and outsourced attribute based encryption," Future Generation Computer Systems, vol. 150, pp. 115-126, 2024, doi: 10.1016/j.future.2023.08.015.

[21] Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, "Lightweight fine-grained search over encrypted data in fog computing," *IEEE Transactions on Services Computing,* vol. 12, no. 5, pp. 772-785, 2018, doi: 10.1109/TSC.2018.2823309.

[22] J. Zhang, Z. Cheng, X. Cheng, and B. Chen, "OAC-HAS: outsourced access control with hidden access structures in fog-enhanced IoT systems," *Connection Science,* vol. 33, no. 4, pp. 1060-1076, 2021, doi:10.1080/09540091.2020.1841096.

[23] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv, and S. Mumtaz, "Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV," *IEEE Transactions on Vehicular Technology,* vol. 69, no. 11, pp. 13784-13795, 2020, doi: 10.1109/TVT.2020.3027568.

[24] A. Zhang, X. Wang, X. Ye, and X. Xie, "Lightweight and fine-grained access control for cloud–fog-based electronic medical record sharing systems," *International Journal of Communication Systems,* vol. 34, no. 13, p. e4909, 2021, doi: 10.1002/dac.4909.

[25] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *International workshop on public key cryptography*, 2011: Springer, pp. 53-70., doi: 10.1007/978-3-642-19379-8_4.

[26] R. Sarma, C. Kumar, and F. A. Barbhuiya, "PAC-FIT: An efficient privacy preserving access control scheme for fog-enabled IoT," *Sustainable Computing: Informatics and Systems,* vol. 30, p. 100527, 2021, doi: 10.1016/j.suscom.2021.100527.

[27] Z. Wu, R.-h. Shi, K. Li, and Y. Yang, "Attribute-based data access control scheme with secure revocation in fog computing for smart grid," Cluster Computing, vol. 25, no. 6, pp. 3899-3913, 2022, doi: 10.1007/s10586-022-03616-0.

[28] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "A secure and verifiable outsourced access control scheme in fog-cloud computing," Sensors, vol. 17, no. 7, p. 1695, 2017, doi: 10.3390/s17071695.

[29] K. Routray and P. Bera, "RLT-CPABE: Revocable Location and Time Aware Ciphertext Policy Attribute-Based Encryption," in *2022 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2022: IEEE, pp. 409-414, doi: 10.1109/ANTS56424.2022.10227786.

[30] S. Fugkeaw, L. Wirz, and L. Hak, "An efficient medical records access control with auditable outsourced encryption and decryption," in *2023 15th International Conference on Knowledge and Smart Technology (KST)*, 2023: IEEE, pp. 1-6, doi: 10.1109/KST57286.2023.10086904.

[31] G. Thushara and S. M. S. Bhanu, "A new hybrid encryption in fog–cloud environment for secure medical data-sharing," *Iran Journal of Computer Science,* vol. 6, no. 2, pp. 169-183, 2023, doi: 10.1007/s42044-022-00129-2.

[32] A. Saidi, O. Nouali, and A. Amira, "SHARE-ABE: an efficient and secure data sharing framework based on ciphertext-policy attribute-based encryption and Fog computing," *Cluster Computing,* vol. 25, no. 1, pp. 167-185, 2022, doi: 10.1007/s10586-021-03382-5.

[33] J. Chen, J. Niu, H. Lei, L. Lin, and Y. Ling, "Adaptively secure multi-authority attribute-based broadcast encryption

in fog computing," *Computer Networks,* vol. 232, p. 109844, 2023, doi: 10.1016/j.comnet.2023.109844.
[34] R. Ma and L. Zhang, "SPMAC: Secure and privacy-preserving multi-authority access control for fog-enabled IoT cloud storage," *Journal of Systems Architecture,* vol. 142, p. 102951, 2023, doi: 10.1016/j.sysarc.2023.102951.
[35] F. Yang, H. Cui, and J. Jing, "Decentralized Attribute-Based Access Control with Attribute Revocation and Outsourced Decryption," in *2023 15th International Conference on Computer Research and Development (ICCRD)*, 2023: IEEE, pp. 246-257, doi: 10.1109/ICCRD56364.2023.10080306.
[36] Y. Lu, T. Feng, C. Liu, and W. Zhang, "A Blockchain and CP-ABE Based Access Control Scheme with Fine-Grained Revocation of Attributes in Cloud Health," *CMC-COMPUTERS MATERIALS & CONTINUA,* vol. 78, no. 2, pp. 2787-2811, 2024, doi: 10.32604/cmc.2023.046106.
[37] L. Zhang and Y. Shang, "Leakage-resilient Attribute-based Encryption with CCA2 Security," Int. J. Netw. Secur., vol. 21, no. 5, pp. 819-827, 2019, doi: 10.6633/IJNS.201909 21(5).14.
[38] C. Ruan, C. Hu, X. Li, S. Deng, Z. Liu, and J. Yu, "A Revocable and Fair Outsourcing Attribute-Based Access Control Scheme in Metaverse," *IEEE Transactions on Consumer Electronics,* 2024, doi: 10.1109/TCE.2024.3377107.
[39] Q. Zhang, C. Xu, H. Zhong, C. Gu, and J. Cui, "Revocable and Efficient Blockchain-based Fine-grained Access Control against EDoS Attacks in Cloud Storage," *IEEE Transactions on Computers,* 2024, doi: 10.1109/TC.2024.3398502.
[40] S. Fugkeaw, R. P. Gupta, and K. Worapaluk, "Secure and Fine-grained Access Control with Optimized Revocation for Outsourced IoT EHRs With Adaptive Load-Sharing in Fog-Assisted Cloud Environment," *IEEE Access,* 2024, doi: 10.1109/ACCESS.2024.3412754.
[41] Y. Ren, C. Chen, M. Hu, G. Feng, and X. Zhang, "Bfdac: A blockchain-based and fog computing-assisted data access control scheme in vehicular social networks," *IEEE Internet of Things Journal,* 2023, doi: 10.1109/JIOT.2023.3296906.
[42] S. Tu, M. Waqas, F. Huang, G. Abbas, and Z. H. Abbas, "A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing," *Computer Networks,* vol. 195, p. 108196, 2021, doi: 10.1016/j.comnet.2021.108196.

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

A New Approach of MRI and CT-Scan Images Fusion using Texture Segmentation and Fuzzy Weighting in Wavelet Transfer

Khalil Mowlani[1], Mehdi Jafari Shahbazzadeh[2*], Maliheh Hashemipour[3]

[1] Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran
Kh.mowlani@gmail.com
[2] Department of Electrical Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran
mjafari@iauk.ac.ir
[3] Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran
m.hashemi@iauk.ac.ir

Abstract: CT images provide information about bony structures but cannot support tissue information, whereas MRI images show details about soft tissues. Obtaining the maximum information and key features from the source images, increasing the visual quality and contrast of the fused image, and reducing the computational tasks remain a major challenge for many medical image fusion algorithms. In this article, the integration of medical images is based on two-dimensional discrete wavelet transform (DWT). First, the original images are decomposed by the Db2 discrete wavelet package into two sets of approximate coefficients and partial coefficients. For the matrix of approximate coefficients, the fuzzy weighting technique of the matrix of approximate coefficients of the input images is used, and for partial coefficients, the average method of the matrix of detail coefficients is used. Weighting uses the mask technique obtained by segmenting the texture of the images. This research has been extended to the composition of color medical images, which effectively prevents color distortion and enhances visual quality. The obtained results show that the proposed algorithm not only performs better in edge and contour detection and visual features, but also has improvements in in quantitative parameter values compared to other researches.

Keywords: Images Fusion, Medical Image Processing, Discrete Wavelet Transform, Texture Segmentation, Fuzzy Weighting.

JCDSA, Vol. 2, No. 3, Autumn 2024	Online ISSN: 2981-1295	Journal Homepage: https://sanad.iau.ir/en/Journal/jcdsa
Received: 2023-12-11	Accepted: 2024-11-19	Published: 2024-12-20

CITATION

Mowlani. Kh, et. al., *"A New Approach of MRI and CT-Scan Images Fusion using Texture Segmentation and Fuzzy Weighting in Wavelet Transfer"*, Journal of Circuits, Data and Systems Analysis (JCDSA), Vol. 2, No. 3, pp. 31-42, 2024.
DOI: 00.00000/0000

* Corresponding author

Extended Abstract

1- Introduction

Recently, there has been an upsurge of attention towards the use of multiple sensors to increase the ability of machines and intelligent systems. Pictures are considered as true descriptions of things. When pictures are taken with a camera, there are limitations of the camera. One of these restrictions is the focal distance, in which case only the objects that are in the focal distance of the camera are seen correctly and the rest of the images are blurred. Image fusion is the process of gathering information from multiple images into one fused image in order to provide more interpretation capabilities. Image fusion has several merits due to widespread applications in medical image processing, military field, remote sensing.

2- Methodology

In view of this and as a longstanding interest, in the current study, an optimal method in the fusion of different CT and MRI medical images is presented with the help of image texture transformation with fuzzy weighting in the wavelet domain, which suggests single-level decomposition in the spatial domain. The final images are presented based on a new optimization approach of medical images fusion under wavelet transform with fuzzy weighting for segmented tissue images of each image pair.

The main achievements of the paper are given below:

- A new method for integrating medical images is proposed.
- A new method based on new fuzzy weighting has been introduced.
- A texture transformation is used to optimize the wavelet coefficients in different parts of the fusion image. This transform improves the fuzzy weighting rate for the wavelet transform coefficients. The texture transform function is capable of computing SVD, Eigen, QR or LU texture transforms. The transformation result highlights the texture areas; it can be used for image segmentation.
- Method of using three different indicators to analyze its efficiency.
- Comparing the efficiency of the proposed method with some other advanced methods.

2-1- Fuzzy Logic Technique

The term fuzzy image processing refers to the entire collection of methods that comprehend, represent, and process images, their segments, and features as fuzzy sets. In fact, the two most important steps in fuzzy image processing representation and processing depend on the fuzzy procedure that is selected as well as the issue that has to be resolved. The first stage in using fuzzy logic to govern an image is to transform it into a grayscale image. Then, during the fuzzyification process, the image is transformed into a membership function, allowing fuzzy logic to easily alter its value.

2-2- Discrete Two-Dimensional Wavelet Transform

The signal is broken down into its frequency components using the wavelet transform. Instead of two-dimensional wavelet, first, two high-pass and low-pass filters are applied on the lines and the sampling rate is reduced. Two signals with high and low frequencies are created and the high-pass and low-pass filters are applied on the columns and the sampling rate is reduced.

2-3- Texture Conversion

Importantly, up to date a great number of researches on texture approaches have been well documented. . Consider a w × w square neighborhood of one pixel in a picture, and let the gray values of that region define the W matrix. It can be made into a diagonal or triangular matrix by multiplying before and after the appropriate matrix, just like any other square matrix.

3- Results and discussion

The wavelet analysis technique of images has been established and developed using the averaging of high frequency partial coefficients, discrete wavelet transforms and fuzzy weighting based on texture transformation in a simple pixel-by-pixel manner. The result of fusion based on wavelet transform and fuzzy selection and averaging rules. The wavelet used here is the Db2 wavelet and each of the MRI and CT images are converted into eight frequency bands after two stages of analysis.

As can be seen, the fusion of images using the mentioned method in comparison with another method has achieved a better and more acceptable result. Four standard evaluation metrics are utilized in this article. They are as follows; Standard deviation, Peak Signal to Noise Ratio and Structural similarity index measurement. According to results the suggested technique produces a fused image with more usable information and a higher degree of similarity to the source image compared to other fused methods. This indicates that the proposed method excels in terms of visual effects.

4- Conclusion

In this article, pixel order fusion algorithm based on wavelet transform with fuzzy weighting and texture transformation is presented, which uses fuzzy integration rules to fuse images obtained from different imaging systems. Proposed technique has been able to achieve a significant improvement in increasing the quality of the merged images. Also, due to the simplicity of the proposed technique, it has achieved good results for improving the speed of fusion and making images resistant to noise and roughness of images.

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

رویکردی جدید از ادغام تصاویر MRI و CT-Scan با استفاده از تقسیم‌بندی بافت و وزن‌دهی فازی برپایه‌ی تبدیل موجک

خلیل مولانی[۱] ، مهدی جعفری شهباز زاده*[۲]، ملیحه هاشمی پور[۳]

۱- گروه مهندسی کامپیوتر، واحد کرمان، دانشگاه آزاد اسلامی، کرمان، ایران (kh.mowlani@gmail.com)

۲- گروه مهندسی برق، واحد کرمان، دانشگاه آزاد اسلامی، کرمان، ایران (mjafari@iauk.ac.ir)

۳- گروه مهندسی کامپیوتر، واحد کرمان، دانشگاه آزاد اسلامی، کرمان، ایران (m.hashemi@iauk.ac.ir)

چکیده: تصاویر CT اطلاعاتی در مورد ساختارهای استخوانی ارائه می‌دهند، اما نمی‌توانند اطلاعات بافتی را پشتیبانی کنند؛ در مقابل، تصاویر MRI جزئیاتی را در مورد بافت‌های نرم نشان می‌دهند. به دست آوردن حداکثر اطلاعات و ویژگی‌های کلیدی از تصاویر منبع، افزایش کیفیت بصری و کنتراست تصویر ترکیب شده همچنین کاهش وظایف محاسباتی برای بسیاری از الگوریتم‌های هم‌جوشی تصاویر پزشکی، به صورت یک چالش بزرگ باقی مانده است. در این مقاله، ادغام تصاویر پزشکی بر اساس تبدیل موجک گسسته دو بعدی صورت گرفته است. ابتدا تصاویر اصلی توسط بسته موجک گسسته‌ی Db2 به دو مجموعه ضرایب تقریبی و ضرایب جزئی تجزیه می‌شوند. برای ماتریس ضرایب تقریبی تکنیک وزن‌دهی‌فازی، ماتریس ضرایب تقریبی تصاویر ورودی و برای ضرایب جزئی، از روش میانگین ماتریس ضرایب جزئیات استفاده می‌شود. وزن‌دهی از تکنیک ماسک حاصل از بخش‌بندی بافت تصاویر استفاده می‌کند. این تحقیق، به ترکیب تصاویر پزشکی رنگی گسترش یافته است که به طور موثری از اعوجاج رنگ جلوگیری می‌کند و کیفیت بصری را افزایش می‌دهد. نتایج به‌دست آمده نشان می‌دهد که الگوریتم پیشنهادی نه تنها در تشخیص لبه و کانتور و ویژگی‌های بصری برتر عمل می‌کند، بلکه در مقایسه با دیگر پژوهش‌ها، در مقادیر پارامترهای کمی نیز دارای بهبود است.

واژه های کلیدی: هم‌جوشی تصاویر، پردازش تصاویر پزشکی، تبدیل موجک گسسته، تقسیم‌بندی بافت، وزن‌دهی فازی

نوع مقاله: پژوهشی

DOI: 00.00000/0000

تاریخ ارسال مقاله: ۱۴۰۲/۰۹/۲۰ تاریخ پذیرش مقاله: ۱۴۰۳/۰۸/۲۹ تاریخ چاپ مقاله: ۱۴۰۳/۰۹/۳۰

۱- مقدمه

استفاده از حسگرهای چندگانه برای افزایش توانایی ماشین‌ها و سیستم‌های هوشمند در سال‌های اخیر رشد قابل توجهی داشته است. تصاویر، توصیف حقیقی از اشیا هستند. وقتی که تصویر با دوربین گرفته می‌شود، محدودیت‌هایی از دوربین در آن‌ها دیده می‌شود. یکی از این محدودیت‌ها فاصله‌ی کانونی است؛ به این صورت که تنها اشیایی که در فاصله‌ی کانونی دوربین می‌باشند به درستی دیده می‌شوند و مابقی تصاویر به صورت مات دیده به نظر می‌آیند. ادغام تصاویر، فرآیند جمع‌آوری اطلاعات از چندین تصویر به یک تصویر جهت فراهم آوردن توانایی های تفسیر بیشتر است. ادغام تصویر به طور وسیعی در پردازش تصاویر پزشکی، حوزه نظامی و سنجش از راه دور کاربرد دارد [۱-۲]. ادغام تصاویر حاصل از چند سیستم تصویربرداری مخصوصاً در حوزه‌ی پزشکی از موضوعات اصلی محققان شده است [۳-۴]. اطلاعاتی که تحت فرآیند ادغام قرار می‌گیرند، ممکن است حاصل سیستم‌های تصویربرداری چندگانه در یک زمان و یا اطلاعات یک سیستم در یک تناوب زمانی باشند. بنابراین منظور از واژه‌ی "ادغام تصویر" فرآیندی است که تصویر واحدی ایجاد می‌کند؛ به طوری‌که حاوی توصیفات بیشتری از یک سوژه نسبت به تک تک هر کدام از منابع باشد. این تصویر ادغام شده برای ادراک چشم انسان و ماشین مفید واقع می‌شود. این نوع ادغام تصویر را ادغام چند سیستمی مرتبه‌ی پیکسل نیز می‌نامند. نکته‌ی حائز اهمیتی که در اینجا وجود دارد این است که سیستم‌های تصویربرداری که در ادغام مورد استفاده قرار می‌گیرند، بایستی انطباق مکانی دقیقی داشته باشند.

یکی از ساده‌ترین روش‌های ادغام تصویر متوسط‌گیری پیکسل به پیکسل در تصویر است. علیرغم سادگی، استفاده از این روش باعث پدیدار شدن اثرات جانبی متعددی در تصویر می‌گردد که کنتراست را کاهش می‌دهد. مطالعه‌ی مقالات و پژوهش‌های سال‌های اخیر نشان می‌دهد که بسیاری از محققان استفاده از تبدیل‌های چندمقیاسی برای تجزیه و تحلیل محتوای اطلاعات تصویر به منظور ادغام را بسیار مفید

می‌دانند. اطلاعات چندمقیاسی می‌توانند برای تعدادی از کاربردهای پردازش تصویر مفید واقع شوند [۵]. با معرفی تبدیل هرم در سال ۱۹۷۵ روشهای پیشرفته‌تری پدیدار شدند. مشخص شد که اگر ادغام در حوزه تبدیل انجام شود، نتایج بهتری به‌دست می‌آید. با پیشرفت تئوری موجک، تجزیه‌ی موجک جای تجزیه هرمی را برای ادغام تصاویر گرفت [۶]. روش‌های مختلف و متنوعی در ادغام تصاویر استفاده می‌شوند؛ از جمله روش منطق فازی [۷]، و روش LTM [۸] که از یک مدل جریان با رویکرد چشمک‌زن روی دامنه شرلت (انسداد برشی)، است. همچنین روش NSST که بر مبنای تبدیل شرلت و پالس شبکه‌ی عصبی پیشنهاد شده است نیز در مطالعات متعددی استفاده شده است [۹].

در این مطالعه، روشی بهینه در هم‌جوشی تصاویر مختلف پزشکی CT و MRI به کمک تبدیل بافت تصاویر با وزن‌دهی فازی در حوزه موجک که تجزیه تک سطحی در حوزه مکان را پیشنهاد می‌دهد، ارائه شده است. دستاوردهای اصلی مقاله در زیر آورده شده است:

- روش جدیدی برای ادغام تصاویر پزشکی پیشنهاد شده است.
- روش جدیدی مبتنی بر وزن‌دهی فازی معرفی شده است.
- از تکنیک تبدیل بافت برای بهینه‌سازی ضرایب موجک در بخش‌های مختلف تصویر هم‌جوشی بهره گرفته شده است. این تبدیل نرخ وزن‌دهی فازی برای ضرایب تبدیل موجک را بهبود می‌بخشد. تابع TextureTransform قادر به محاسبه تبدیل بافت SVD، Eigen، QR یا LU است که در [۱۰]. توضیح داده شده است. در نتیجه تبدیل، مناطق بافت برجسته می‌گردند که می‌توان از آن‌ها برای تقسیم‌بندی تصویر استفاده می‌گردد.
- از چهار شاخص مختلف برای تحلیل کارایی روش پیشنهادی استفاده شده است.
- مقایسه‌ی کارآیی روش پیشنهادی با چند روش پیشرفته‌ی دیگر انجام شده است.

در ادامه، در بخش دوم، به کارهای انجام شده در زمینه‌ی هم‌جوشی تصاویر پزشکی پرداخته می‌شود. در بخش سه مفاهیم اولیه‌ی این کار تشریح می‌شود. ساختار روش ارائه شده به همراه DWT بهینه شده با وزن‌دهی فازی از روی داده‌های تبدیل بافت در بخش چهارم تجزیه و تحلیل می گردند. در بخش پنجم عملکرد سیستم ارزیابی شده و مقایسه‌ها انجام می‌گیرند. نتیجه‌گیری مقاله در بخش ششم ارائه شده است.

۲- کارهای مروری

هدف از ادغام تصاویر پزشکی چندوجهی استخراج اطلاعات از تصاویر مختلف به یک تصویر واحد است به‌طوری‌که تصویر تلفیقی منفرد دارای ویژگی‌های برجسته‌ی تصاویر منبع با حداکثر میزان باشد. در مقاله‌ی [۱۱] ترکیب و ادغام تصاویر چندوجهی در یک تصویر واحد برای به دست آوردن اطلاعات برتر و کیفیت بصری عالی بدون هیچ گونه ابهامی انجام شده است. ابتدا، تصاویر منبع با استفاده از فیلتر گاوسی به لایه‌های پایه و جزئی تجزیه می‌شوند. لایه‌های جزئیات با استفاده از فرکانس فضایی ادغام می‌شوند تا جزئیات لبه و وضوح تصویر حفظ شود. به دلیل این‌که لایه‌ی پایه حاوی اطلاعات تقریبی تصویر منبع با کنتراست کم است، به تصویر فازی شهودی تبدیل می‌شود سپس اطلاعات بافت برای ترکیب لایه‌های پایه از آن، استخراج می‌گردد. در نهایت، تصویر خروجی ادغام شده با کنتراست بهبود یافته و جلوه‌های بصری بهتر بازسازی می‌شود. اما با توجه به عملکرد خوب این تکنیک متاسفانه از سرعت عمل بالایی برخوردار نیست. روش‌های مختلف تصویربرداری پزشکی مانند CT و MRI به عنوان مورفولوژی بصری متفاوت ارائه می‌شوند که اغلب ویژگی‌های برجسته مکمل متفاوتی را در تشخیص بالینی نشان می‌دهند. در [۱۲] برجستگی بصری دو تصویر منبع ثبت شده توسط الگوریتم GBVS محاسبه می‌شود و باندهای فرکانس پایین و فرکانس بالا با تجزیه تصاویر منبع در دامنه NSST به دست می‌آیند. برای زیر باندهای فرکانس پایین، سیستم منطق فازی برای به دست آوردن وزن‌های مربوطه، از نمودار GBVS به عنوان ورودی استفاده می‌کند. برای زیر باندهای فرکانس بالا، مقادیر NSML هر زیرباند، محاسبه می‌شود. تصویر ادغام شده نهایی با تبدیل معکوس NSST به دست می‌آید. علاوه بر این، از الگوریتم PSO برای بهینه‌سازی تابع عضویت سیستم منطق فازی برای تطبیق بهتر با تصاویر پزشکی و استخراج ویژگی‌ها استفاده می‌شود. با استفاده از این روش، کیفیت بصری تصویر نهایی به طور موثری بهبود می‌یابد و ویژگی‌های برجسته‌ی بافت‌ها به خوبی حفظ می‌شود. اما با توجه به ارجحیت فازی در تصاویر ادغام شده یک برهم‌نهی اطلاعاتی در تصاویر اتفاق افتاده است که در نهایت تغییر ناهمگن در تصاویر نهایی حاصل شده است.

مقاله [۱۳] یک رویکرد ترکیبی تصویر پزشکی را بر اساس فیلتر نمودار قطعه (SGF) و نمایش پراکنده (SR) پیشنهاد می‌کند. با استفاده ازSGF، تصاویر منبع به تصاویر پایه و جزئیات تجزیه می‌شوند که بر اساس آن، اطلاعات لبه تا حد امکان در تصویر ترکیب شده یکپارچه می‌شود. سپس تصاویر پایه با اعمال یک قاعده‌ی ادغام بر اساس آنتروپی شانون نرمال شده ترکیب می‌شوند، در حالی که تصاویر جزئیات با استفاده از روش هم‌جوشی مبتنی بر SR ترکیب می‌گردند. در[۱۴]، یک طرح تجزیه‌ی دو لایه توسط فیلتر دوطرفه‌ی مشترک شامل، لایه‌ی انرژی حاوی اطلاعات شدت، و لایه‌ی ساختار، شامل جزئیات تصاویر است، پیشنهاد شده است. سپس یک عملگر مبتنی بر انرژی گرادیان محلی بر اساس بردار ساختار و انرژی همسایه برای ترکیب لایه ساختار و قانون l1-max، برای ادغام لایه انرژی معرفی می‌شود. در مجموع ۱۱۸ جفت تصویر پزشکی ثبت شده‌ی مشترک که پنج دسته‌ی مختلف از چالش‌های همجوشی تصویر پزشکی را پوشش می‌دهند، در تصاویر آزمایش می‌شوند. یک الگوریتم بهبود یافته بر اساس مجموعه‌های فازی با ویژگی‌های محلی و NSML در دامنه NSST در [۱۵] ارائه شده است. ابتدا، با بهره‌گیری کامل از NSST، دو تصویر ثبت شده از یک صحنه به یک زیر باند فرکانس پایین (LFS) و چندین زیر باند فرکانس بالا (HFS) تجزیه می‌شوند. سپس، قوانین هم‌جوشی مبتنی بر پیکسل فازی بر روی LFS برای محاسبه‌ی وزن هر پیکسل در ضریب هم‌جوشی مورد نیاز اعمال می‌شوند. وزن‌ها کاملاً بر اساس انرژی‌های محلی و آنتروپی های LFS هستند. ضرایب HFS ادغام شده با محاسبه و مقایسه NSML هر HFS انتخاب می‌شوند تا اطلاعات حداکثر و مفیدتری استخراج شود. در نهایت، NSST معکوس برای به‌دست آوردن تصویر هم‌جوشی مورد نیاز اعمال می‌شود. مساله‌ای که در این تحقیق مورد

بررسی قرار نگرفته است، عدم بررسی مقاومت طرح پیشنهادی در برابر نویز است. در [۱۶]، یک الگوریتم ترکیبی تصویر پزشکی چندوجهی بهبود یافته بر اساس تبدیل فازی (FTR) پیشنهاد شده است. ایده‌ی اصلی پشت الگوریتم پیشنهادی، بهبود عملکرد الگوریتم ترکیبی تصویر پزشکی چندوجهی با در نظر گرفتن تصاویر خطای به‌دست‌آمده با استفاده از کوپل FTR است.

مقاله‌ی [۱۷] یک روش ارزیابی کیفیت ادراکی برای ترکیب تصویر پزشکی چندوجهی (MMIF) ارائه می‌کند. در این رویش یک رویکرد بدون مرجع برای ارزیابی کیفیت ادراکی تصاویر MMIF پیشنهاد می‌شود که از شبکه عصبی همراه پالس (PCNN) در تبدیل Contourlet غیرنمونه‌برداری شده (NSCT) استفاده می‌کند. تصاویر توسط NSCT به زیر باند فرکانس پایین (LFS) و زیر باند فرکانس بالا (HFS) تجزیه می‌شوند. روش ارائه‌شده از معیارهای ارزیابی کیفیت ترکیب تصویر خوبی برخوردار است، اما دارای پیچیدگی محاسباتی بالایی می‌باشد. در [۱۸]، یک الگوریتم ترکیبی تصویر پزشکی چندوجهی برای طیف وسیعی از مسائل تشخیصی پزشکی پیشنهاد شده است. روش پیشنهادی، مبتنی بر کاربرد یک استراتژی هم‌جوشی شبکه عصبی با پالس جفت شده مرزی و استراتژی همجوشی ویژگی انرژی در یک حوزه تبدیل شرلت غیر نمونه‌برداری شده است. الگوریتم مورد نظر در مجموعه داده‌هایی با چندین بیماری مختلف که شامل بیش از ۱۰۰ جفت تصویر است، اعتبارسنجی می‌گردد. در [۱۹]، یک تکنیک بهینه‌سازی ترکیبی برای توسعه‌ی یک روش با کارآیی بالا برای ادغام تصاویر پزشکی ارائه شده است. روش ارائه شده از هر دو مزیت تبدیل موجک و فیلتر هوموروفیک برای بهبود کارایی سیستم استفاده می‌کند. برای دستیابی به مقادیر بهینه‌ی سیستم، یک الگوریتم بهینه‌سازی جدید بر اساس دو روش جدید معرفی می‌گردد. الگوریتم بهینه سازی بوی کوسه و الگوریتم بهینه سازی جام جهانی. در روش مورد نظر با توجه به استفاده از الگوریتم‌های مختلف دارای سرعت هم‌جوشی پایین برای تصاویر مختلف است.

در [۲۰]، تصاویر چندوجهی برای تشخیص تومور GBM با استفاده از روش همجوشی تصویر بر اساس تبدیل موجک گسسته (DWT)، ترکیب شده‌اند به نحوی که زیر باندهای فرکانس پایین از طریق روش میانگین وزنی و زیر باندهای فرکانس بالا، از روش انتخاب حداکثر، ادغام می‌شوند. در [۲۱]، یک الگوریتم هم‌جوشی میانگین وزنی جدید برای ترکیب تصاویر MRI و CT از مغز براساس فیلتر تصویر هدایت‌شده و آمار تصویر ارائه می‌کند. الگوریتم پیشنهادی به شرح زیر است: لایه‌های جزئیات از هر تصویر منبع با استفاده از فیلتر تصویر هدایت شونده استخراج می‌شوند. وزن‌های مربوط به هر تصویر منبع از لایه‌های جزئیات با کمک آمار تصویر محاسبه می‌شوند. سپس یک استراتژی ترکیبی میانگین وزنی برای ادغام اطلاعات تصویر منبع در یک تصویر واحد اجرا می‌شود. مسئله‌ی قابل توجه در این روش، وجود پیچیدگی محاسباتی آماری این روش می‌باشد که برای برخی از تصاویر خطای آماری را نشان می‌دهد. مقاله [۲۲] اندازه گیری‌های آماری ادغام تصویر پزشکی MRI-PET چند وجهی را با استفاده از تبدیل ۲ بعدی هارتلی (HT) در فضای رنگی HSV پیشنهاد می‌کند. این روش پیشنهادی با دو نوع مختلف از تصاویر پزشکی مانند MRI و PET (توموگرافی گسیل پوزیترون) مورد بحث قرار می‌گیرد. این روش شامل ۵ مرحله است: در ابتدا تصویر رنگی PET به کانال‌های HSV تبدیل می‌شود. در مرحله‌ی دوم تصویر MRI و مولفه‌ی V تصویر PET به بلوک های ۸×۸ تقسیم می‌شوند و سپس تبدیل هارتلی ۲بعدی را روی هر بلوک از دو تصویر ورودی اعمال می‌شود. مرحله‌ی سوم، محاسبه واریانس هر بلوک از دو تصویر انجام شده و سپس بهترین بلوک‌ها انتخاب می‌گردند. مرحله‌ی چهارم، اعمال HT دوبعدی معکوس است و همه بلوک‌ها در یک تصویر واحد یعنی جزء V جدید مرتب می‌شوند. در نهایت تطبیق مولفه New V، H، S برای دریافت تصویر HSV و سپس تبدیل HSV به RGB برای به‌دست آوردن تصویر ادغام شده نهایی با دقت بیشتر، انجام می‌شود.

در [۲۳] روشی با عنوان PhotoHelper جهت افزایش کیفیت تصاویر ارائه شده است. این روش کیفیت تصاویر را با استفاده از بازیابی و ادغام ویژگی های عمیق انجام می‌دهد. در این مدل، قوانین زیبایی‌شناسی تجربی، الگوریتم‌های سنتی یادگیری ماشین و شبکه‌های عصبی عمیق برای استخراج انواع مختلف ویژگی‌ها در هر دو جنبه رنگی و فضایی، به‌طور جامع یکپارچه شده است. این ویژگی‌ها برای یک جنگل تصادفی اصلاح‌شده با مجموعه عکس ساختار یافته برای شناسایی انواع عکس‌ها استفاده می‌شوند. همچنین امتیاز تطبیق ترکیب را برای اندازه گیری شباهت بین عکس داده شده و عکس مرجع تعریف می‌کند. آزمایش‌ها و ارزیابی‌ها نشان می‌دهند که کیفیت تصاویر خروجی با استفاده از این رویکرد، به طور قابل‌توجهی افزایش می‌یابند. در [۲۴] یک روش جدید ادغام تصویر پزشکی عمیق مبتنی بر یک شبکه عصبی کانولوشن عمیق (DCNN) برای یادگیری مستقیم ویژگی‌های تصویر از تصاویر اصلی ارائه شده است. این روش از نظر شاخص‌های عینی و کیفیت بصری با چندین رویکرد ترکیبی تصویر پزشکی مقایسه شده است. به طور خاص، تصاویر منبع ابتدا با نمایش رتبه پایین تجزیه می شوند تا به ترتیب اجزای اصلی و برجسته را به‌دست آورند. پس از آن، ویژگی های عمیق از اجزای اصلی تجزیه شده از طریق DCNN استخراج شده و توسط یک قانون میانگین وزنی ترکیب می‌شوند. سپس، با در نظر گرفتن مکمل بین مولفه‌های برجسته‌ی به دست آمده توسط نمایش رتبه‌ی پایین، یک قانون جمع ساده اما موثر برای ترکیب اجزای برجسته طراحی شده است. در نهایت، نتیجه ادغام شده با بازسازی اجزای اصلی و برجسته به‌دست می‌آید.

در این مقاله رویکرد جدیدی در زمینه هم‌جوشی تصاویر پزشکی جهت افزایش کیفیت تصاویر پزشکی ارائه می‌شود. در مطالعات مختلف تلاش هایی برای هم‌جوشی بهینه انجام شده است اما سه چالش مصرف زمانی، پیچیدگی عملکرد ادغام و همچنین مقاوم بودن روش‌های موجود در برابر نویز، هنوز جای بحث و کار را دارند. در این مطالعه، با ارائه‌ی یک تکنیک ساده در تبدیل موجک برای ادغام تصاویر، در عین سادگی کار، به یک هم‌جوشی با کیفیت خوب با سرعت پردازش بالا برای تصاویر مختلف رنگی و خاکستری در زمینه ادغام تصاویر پزشکی، دست یافته‌ایم.

۳- مفاهیم پایه‌ای

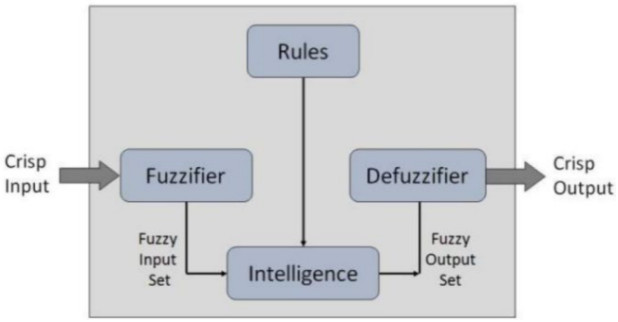
در این قسمت ما به معرفی مباحث پایه‌ای مورد استفاده در این مقاله خواهیم پرداخت. مفاهیم مورد مطالعه شامل مجموعه‌های فازی، تبدیل موجک دو بعدی گسسته و تبدیل بافت تصاویر برای بخش بندی‌های مختلف تصاویر جهت وزن دهی پیکسل‌های مختلف تصاویر هم‌جوشی می‌باشد که در ادامه به تشریح مقدماتی آن‌ها خواهیم پرداخت.

۳-۱- منطق فازی

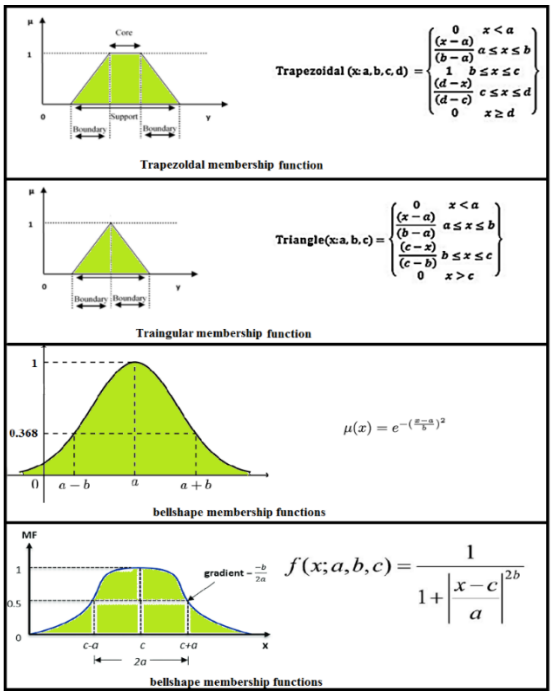
اصطلاح «پردازش تصویر فازی» می‌تواند برای توصیف مجموعه‌ای از روش‌هایی استفاده شود که تصاویر، بخش‌های تصویر و ویژگی‌های تصویر را به‌عنوان مجموعه‌های فازی تشخیص، نمایش، و مدیریت می‌کنند. سه مرحله‌ی کلیدی را می‌توان برای پردازش تصویر فازی در نظر گرفت: فازی سازی تصویر، اصلاح مقادیر عضویت، و در صورت نیاز و فازی زدایی سازی تصویر (شکل (۱)). مراحل فازی سازی کدگذاری داده‌های تصویر و رمزگشایی نتایج (فازی زدایی) است. این مراحل فرصتی را برای پردازش تصاویر با مهارت‌های فازی ارائه می‌دهد [۲۵]. مؤثرترین بخش پردازش تصویر در مرحله‌ی میانی قابل مشاهده است. در این مرحله اصلاح مقادیر عضویت انجام می‌گیرد که آن را مرحله‌ی هوشمندی می‌نامیم. زیرا این مرحله تفاوت بین رویکرد و مرحله‌ی دیگر را ایجاد می‌کند. در منطق فازی انواع مختلفی از تابع عضویت همان‌طور که در شکل (۲) نشان داده شده است، وجود دارند. هر یک از این توابع، اثر متمایز خود را دارند. استفاده از تابع عضویت مناسب توسط استنتاج سیستم فازی، کارآیی روش را افزایش می‌دهد. این روش نقاط مجاور پیکسل ها را فرض کرده و سپس با استفاده از تابع عضویت [۲۶] آن‌ها را به کلاس‌ها تقسیم می‌کند. دلیل برتری منطق فازی بر سایر روش‌های دیگر این است که همه چیز از عدم دقت رنج می‌برد در حالی‌که منطق فازی درک خود را با در نظر گرفتن ساختار می‌سازد. در بسیاری از روش‌های پردازش تصویر، برای حل مسائل پیچیده مانند تشخیص اشیا و تجزیه و تحلیل صحنه، استفاده از منطق انسانی بر اساس قوانین if-then که می‌تواند توسط منطق فازی ارائه شود، پیشنهاد می‌شود. از سوی دیگر دلایل بسیاری مانند تصادفی بودن و مبهم بودن منجر به عدم قطعیت در نتیجه پردازش تصویر و داده ها می‌شود. این عدم قطعیت ها تأثیر منفی بر روش‌های پردازش تصویر دارند که منجر به مشکلات زیادی می‌شود [۲۷].

۳-۲- تبدیل موجک گسسته‌ی دو بعدی

تبدیل موجک برای تجزیه سیگنال به مولفه‌های فرکانسی به کار می‌رود. درتبدیل موجک دوبعدی ابتدا دو فیلتر بالاگذر و پایین گذر بر روی سطرها اعمال می گردد و کاهش نرخ نمونه برداری انجام می‌شود. دو سیگنال با فرکانس‌های بالا و پایین ایجاد می شود و دوباره فیلتر بالاگذر و پایین گذر بر روی ستون‌ها اعمال می‌گردد و مجددا کاهش نرخ نمونه برداری انجام می‌شود.

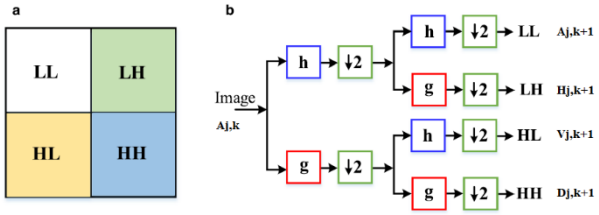


شکل (۱): مراحل مربوط به پردازش فازی تصاویر [۲۵][۲۹]

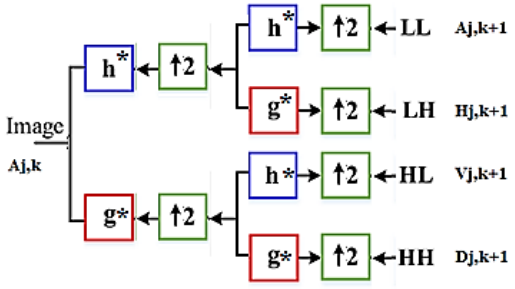


شکل (۲): انواع توابع عضویت فازی [۲۶، ۳۰]

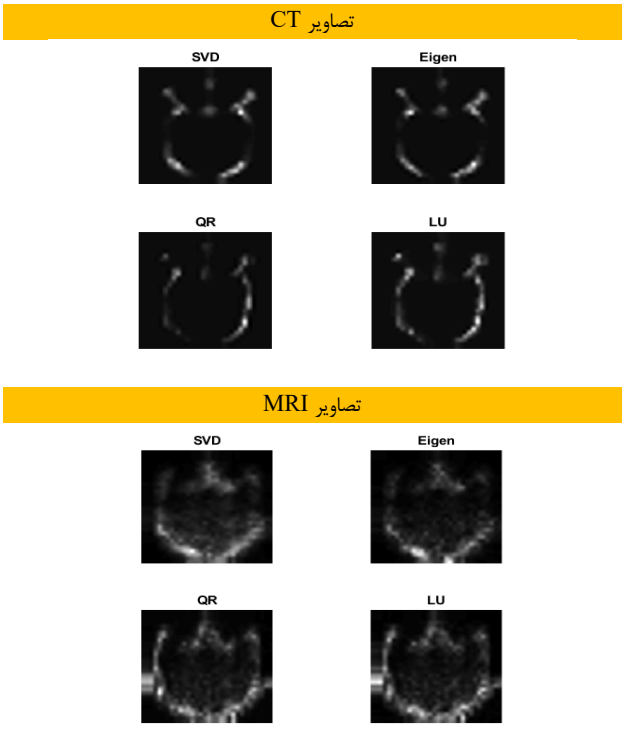
تجزیه‌ی موجک تصویر شامل عملیات فیلترینگ دو جهته و زیرنمونه برداری با مضربی از دو می‌باشد. از آنجا که مقیاس و تابع موجک جداپذیر هستند، تجزیه تصویر را می‌توان با استفاده از بسط جداپذیر تجزیه‌ی تک بعدی روی ردیف‌ها و ستون‌ها به‌دست آورد. در هر مرحله تبدیل، تصویر به چهار زیر تصویر تجزیه می شود. به‌عنوان نمونه Aj,k را تصویر اصلی در نظر بگیرید. طبق شکل (۳)، در هر مرحله تبدیل موجک به چهار زیر تصویر Aj,k+1 و Hj,k+1 و Vj,k+1 و Dj,k+1، تجزیه می‌گردد. اولین جزء که بعد از دو باز عبور از فیلتر پایین گذر به‌دست می‌آید، جزء فرکانس پایین نامیده می‌شود. (به این جز تقریب Aj,k نیز گفته می‌شود). این جزء برای مراحل بعدی تبدیل موجک به عنوان تصویر اولیه و ورودی به کار می‌رود و Hj,k+1 و Vj,k+1 و Dj,k+1 حاوی اطلاعات فرکانس بالای افقی، عمودی و مورب و به عنوان ضرایب جزئی می‌باشند. در شکل (۳)، G یک فیلتر پایین گذر و H یک فیلتر بالاگذر است. بعد از تجزیه، ضرایب جزئی و تقریبی Aj,k و Hj,k و Vj,k و Dj,k هر تصویر به ترتیب با cAj,k و cHj,k و cVj,k و cDj,k نمایش داده می‌شوند، که c معرف تصویر مورد نظر است [۲۶]. فرایند بازسازی موجک تصویر نیز در شکل (۴) نشان داده شده است.



شکل (۳): تجزیه موجک. الف) تبدیل موجک گسسته یک سطحی. ب) بانک فیلترها برای تجزیه یک سطحی [۲۶].



شکل (۴): بازسازی موجک تصویر [۲۸]



شکل (۵): نمونه هایی از تشخیص بافت با عملگر تبدیل بافت تصاویر و MRI , CT نتیجه تبدیل بافت با مقادیر ویژه، تبدیل بافت با قسمت بالایی پایینی، تبدیل بافت با QR و تبدیل بافت با تجزیه مقدار منفرد.

۳-۳- تبدیل بافت

استفاده از رویکردهای مختلف تبدیل بافت، در هنگام پردازش تصاویر، امکان پذیر است. تا به امروز، تحقیقات متعددی در مورد رویکردهای بافت انجام شده است [۲۹، ۳۰]. شکل (۵) چهار نتیجه را با عملگرهای تبدیل بافت با استفاده از یک پنجره مربعی با اندازه ۳۲ پیکسل، نشان می‌دهد [۱۰، ۳۱]. با داشتن یک تصویر، مقادیر خاکستری آن را ماتریس مربعی W، در نظر بگیرید. مانند هر ماتریس مربعی، می‌توان آن را با ضرب در ماتریس‌های مناسب به یک ماتریس مورب یا مثلثی تبدیل کرد. اعداد $\alpha = (\alpha 1; \ldots ; \alpha w)$ در قطر ماتریس به ترتیب قدر نزولی شماره‌گذاری می‌شوند. برای مثال، این اعداد را می‌توان با تجزیه‌های مختلف W محاسبه کرد: تجزیه‌ی مقدار منفرد، تجزیه‌ی مقادیر ویژه، تجزیه به حاصلضرب یک ماتریس متعامد و مثلث بالایی (تجزیه QR)، یا تجزیه‌ی بالا پایین. تبدیل بافت طبق (۱) تعریف می‌شود.

$$\emptyset(l,w) = \sum_{k=l}^{w} \| \alpha_k \|^{\gamma} \qquad 1 \le l \le w \qquad (۱)$$

هر پیکسل با یک عدد نمایش داده می شود که به سه پارامتر بستگی دارد. عدد w به وضوح با مقیاس مطابقت دارد. دو پارامتر دوم l و γ بصورت تجربی انتخاب شده‌اند، $l = [w/2]$ و $\gamma = 2$، همان مقادیری که در [۳۱] بیان شده است. از آن‌جایی‌که بافت یک ویژگی محلی است نه یک ویژگی نقطه‌ای، لازم نیست توصیف‌گر در آن محاسبه شود. بر اساس تصاویر استخراج شده بافت از تصاویر MRI و CT، روش LU توانسته است کامل‌ترین ساختار را برای تبدیل بافت ایجاد کند.

۴- روش پیشنهادی

- **مرحله‌ی اول**: تصاویر لایه جزئیات با کمک روش بافت به‌عنوان ماسک برای آشکارسازی نواحی تار از بخش واضح به‌دست می‌آید.
- **مرحله دوم**: تصاویر جزئیات با استفاده از یک قاعده‌ی هم‌جوشی فازی برای مولفه اصلی تبدیل موجک، ترکیب می‌شوند.

روش پیشنهادی به شرح زیر توضیح داده شده است.

تصاویر MRI بافتهای نرم بدن و تصاویر CT بافت‌های سخت را شناسایی و تصویربرداری می‌کنند. در این کار از یک تکنیک بخش‌بندی مبتنی بر بافت استفاده می‌شود. در روش پیشنهادی، بر اساس یک حق انتخاب برای پیکسل‌های با وضوح بالاتر با روش منطق فازی یک وزن دهی قابل قبول به سیستم داده می‌شود. برای پیکسل‌هایی که در تصاویر CT دارای وضوح است، بیشترین وزن‌دهی به تصاویر CT داده می‌شود و بر عکس برای پیکسل‌هایی که در تصاویر MRI دارای وضوح است مقدار وزن‌دهی بیشتر به سمت تصاویر MRI معطوف می‌شود. به همین دلیل در این مقاله از یک تکنیک تفاضل تبدیل بافت تصاویر MRI و CT (رابطه‌ی (۲)) ارائه شده است. در نتیجه یک مرزبندی تصاویر با وضوح بیشتر برای پیکسل‌های با مقدار مثبت و منفی حاصل می‌شود که بعد از نرمال‌سازی در محدوده‌ی (۱- و ۱+) برای وزن‌دهی توسط روش فازی پیشنهادی بارگذاری می‌گردد. بر اساس رابطه‌ی ۲، هر چه وضوح و کیفیت بافت تصویر MRI بیشتر باشد مقدار $D_{tx\text{-}t}$ به مقدار ۱+ نزدیکتر می‌شود و برعکس برای بخش‌های بافت با کیفیت بیشتر برای تصویر CT ، مقدار $D_{tx\text{-}t}$ به مقدار ۱- نزدیک‌تر خواهد بود.

$$D_{tx-t} = TX_{t(MRI)} - TX\_t(CT) \qquad (۲)$$

حال با توجه به مقادیر $D_{tx\text{-}t}$ به‌دست آمده از در هر پیکسل از تصویر تبدیل بافت به یک ماتریس با ابعاد مشابه ابعاد ماتریس تصاویر دست خواهیم یافت. بعد از گرفتن تبدیل موجک از تصاویر MRI و CT و با استفاده از ضرایب موجود در ماتریس وزن‌دهی، ادغام تصاویر

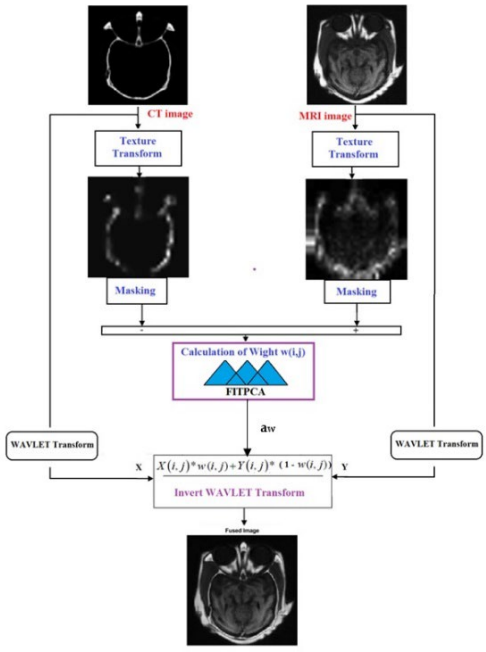
انجام می‌شود. برای ادغام تصاویر از دو تصویر B و A استفاده شده است. مراحل ادغام تصاویر به شرح ذیل می‌باشد:

گام اول: محاسبه تبدیل موجک تصاویر ورودی: ضرایب موجک تصویر اول را با [A1,B1,C1,D1] و تصویر دوم را با[A2 ,B2 ,C2 ,D2] نمایش می‌دهیم.

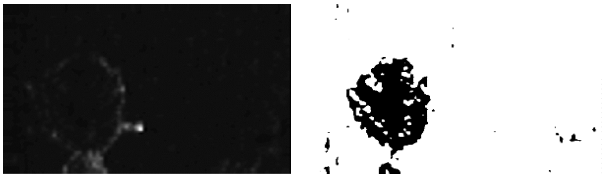
گام دوم: ضرایب فرکانس بالای تصاویر ورودی را (شامل ضرایب جزئی) میانگین‌گیری کرده و مقدار حاصله در تصویر خروجی قرار می‌گیرد. برای ضرایب فرکانس پایین (ضرایب تقریبی)، مقدار ضریب تصاویر ورودی از (۳) گرفته می‌شود و در تصویر خروجی نمایش داده می‌شود. در نهایت مقدار وزنی در (۳)، معرف مولفه اصلی تبدیل موجک گسسته در تصویر ادغام شده خواهد بود. مقدار aw در واقع ضریب تقریبی و فرکانس پایین حاصل از ماتریس وزندهی فازی می‌باشد.

$$a_3 = a_1 \times (1 - aw) + a_2 \times (aw) \qquad (۳)$$

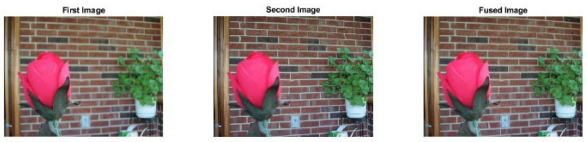
گام سوم: در نهایت برای مشخص شدن تصویر ادغام شده عکس تبدیل موجک گرفته می‌شود. برای درک بهتر این موضوع ما از تصاویر غیر پزشکی برای تفهیم طرح پیشنهادی استفاده کرده‌ایم. شکل (۶) مراحل کار را بیان می‌کند. در شکل (۷)، یک نمونه از ادغام تصاویر غیر پزشکی به کمک تکنیک پیشنهادی نشان داده شده است. شکل (۸)، ساختار و قوانین ادغام تصاویر بر مبنای منطق فازی را نمایش می دهد. بر اساس قوانین تشریح شده بخش‌های با وضوح بهتر در اولویت ادغام برای تصویر نهایی قرار گرفته‌اند. جدول (۱)، به معرفی این قوانین فازی پیشنهادی پرداخته است. بر مبنای تعریف انجام شده برای سیستم منطق فازی پیشنهادی در این تحقیق، برای پیکسل‌های با وضوح بالاتر در تصاویر CT یا MRI، مقدار وزن‌دهی بالاتر برای آن‌ها انتخاب می‌شود و برای مورد با وضوح کمتر در ساختار تصویر ادغام شده، حذف می‌گردد. برای تصاویر با وضوح و کیفیت مشابه از هر دو تصویر، برای مولفه های فرکانس پایین تبدیل موجک میانگین وزنی را انتخاب شد.



شکل (۶): تکنیک پیشنهادی ادغام تصاویر



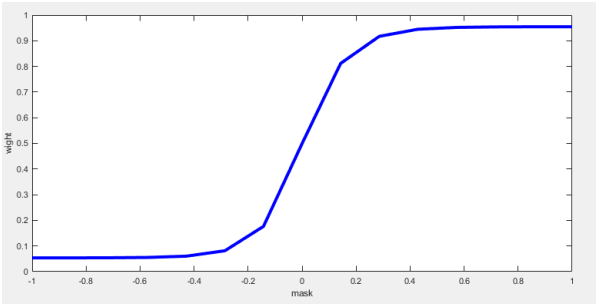
الف- تصویر ماسک گذاری شده بخش واضح از تار به کمک فیلتر انتقال بخش بندی بافت.



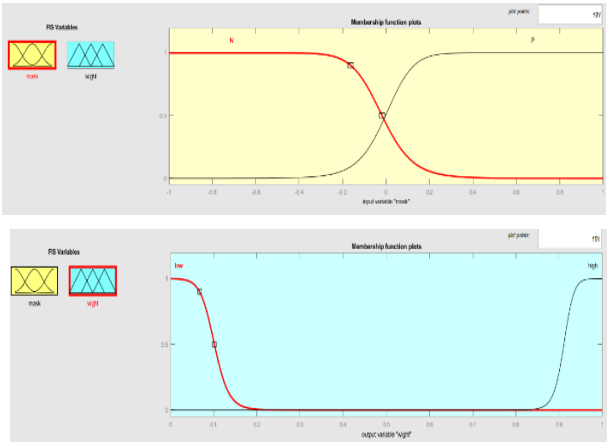
ب- مقایسه تصاویر ادغام شده اول و دوم.

شکل (۷): نمایش ادغام تصویر غیر پزشکی به کمک تکنیک پیشنهادی.

الف- نمای سیستم فازی ممدانی



ب- مشخصه ورودی خروجی سیستم فازی پیشنهادی



ج- نمایش توابع عضویت ورودی و خروجی

شکل(۸): نمایش مدل ادغام فازی

جدول (۱): قوانین ادغام فازی

Normalized D_{tx-t}	Weight
Low	Low
High	High

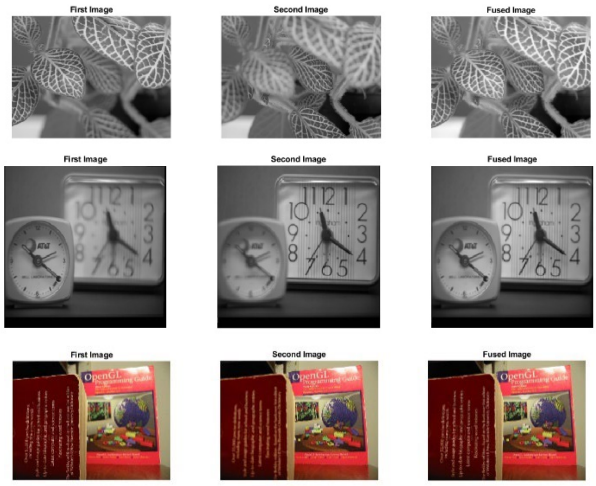
۵- نتایج روش پیشنهادی و ارزیابی عملکرد

در این بخش ابتدا روش پیشنهادی ارزیابی شده و سپس با روش های موجود در حوزه‌ی هم‌جوشی تصاویر، مقایسه می‌گردد. تصاویر مورد استفاده در این پژوهش، تصاویر MRI و CT سر و جمجمه هستند . این تصاویر از یک فرد خاص و در یک روز اخذ شده‌اند. سیستم تصویر برداری CT مدل Emotion متعلق به شرکت زیمنس و سیستم MRI نیز مدل Intera و ساخت فیلیپس است. همه‌ی تصاویر با ابعاد یکسان ۴۲۶ در ۴۲۶ پیکسل هستند. به منظور اطمینان از یکسان بودن مقاطع تصویر برداری شده، از نشان‌گرهای ویژه‌ای استفاده شده است.

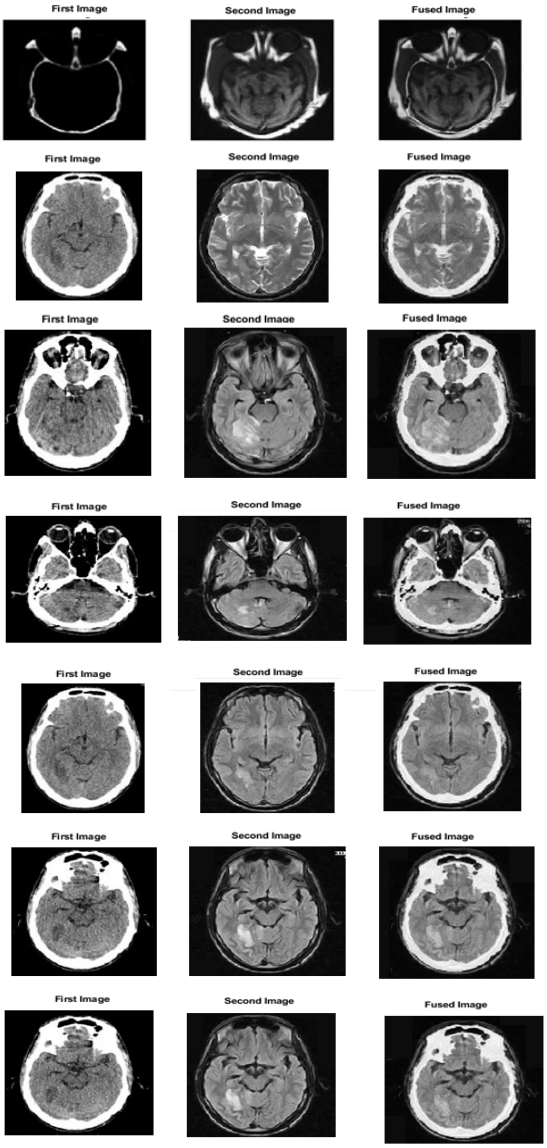
۵-۱- نتایج تکنیک همجوشی تصاویر

بخش قابل توجهی از کاربردهای بالینی با تلفیق تصاویر پزشکی چند حالته انجام می‌شود. تشخیص ناهنجاری در ساختارهای بافت نرم بدن را می‌توان به روشنی در تصاویر MRI و تصاویر بسیار واضح از ساختار استخوان را از طریق تصاویر CT مشاهده کرد. در تحقیق پیشنهادی، دو تصویر CT و MRI از یک بیمار با هم ادغام می‌شوند که این کار باعث گسترش دامنه اطلاعات می‌گردد. تصویر ادغام شده در تشخیص تومور و بیماری های دیگر می تولند مورد استفاده قرار گیرد. در این کار، برای دستیابی به هم‌جوشی بهتر تصویر، پیشنهاد شده است که تجزیه‌ی تصویر با استفاده از تبدیل موجک گسسته انجام گردد.

به جای در نظر گرفتن هر مجموعه‌ی ممکن از موقعیت و مقیاس، DWT فقط بر موقعیت‌ها و مقیاس‌های توان دو تمرکز می‌کند. تصاویر ورودی به زیر باندهای فرکانس پایین و بالا تقسیم می‌شوند که از چهار زیر باند LL، LH، HL و HH تشکیل شده است. با استفاده از قوانین هم‌جوشی اولین زیر باند فرکانس ورودی با زیر باند فرکانس مربوطه از تصویر ورودی دیگر ادغام می‌شوند. از دو قانون هم‌جوشی یعنی حداکثر قانون میانگین معمولی و قانون میانگین وزنی استفاده می شود. با قانون میانگین وزنی، زیر باندهای فرکانس پایین و با استفاده از قانون میانگین معمولی، بلندهای فرعی بالا با هم ترکیب می‌شوند. در قانون میانگین وزنی، با در نظرگرفتن شدت متوسط وزنی پیکسل‌های مربوطه در زیر باند فرکانس پایین، تصاویر ورودی CT و MRI بررسی می‌شوند. سرانجام، از اجزای زیر باند فرکانس ادغام شده برای بازسازی تصویر خروجی هم‌جوشی نهایی استفاده می‌شود. بازسازی تصویر با استفاده از تغییر شکل موجک گسسته معکوس در مجموعه زیر باندهای فرکانس حاصل از هم‌جوشی زیر باند فرکانس هر تصویر انجام می‌شود. در این تحقیق برای بهبود مدل ادغام تصاویر MRI , CT از تبدیل بافت برای تعیین مدل‌های خروجی، بهره گرفته‌ایم. این کار پیچیدگی تکنیک را کاهش می‌دهد و باعث می‌شود سرعت هم‌جوشی بالا برود. همچنین باعث افزایش جزئیات اطلاعات تصویر نهایی می‌گردد. شکل (۹) نمایش خروجی ادغام تصاویر مختلف غیر پزشکی و شکل (۱۰)، ادغام چند نمونه از تصاویر پزشکی (MRI و CT-Scan) را با استفاده از روش پیشنهادی، نمایش می‌دهد.



شکل (۹): ادغام چند نمونه از تصاویر غیر پزشکی با استفاده از روش پیشنهادی



شکل (۱۰): ادغام چند نمونه از تصاویر پزشکی (MRI و CT-Scan) با استفاده از روش پیشنهادی

۵-۲- ارزیابی عملکرد روش پیشنهادی

کیفیت هم‌جوشی تصویر باید با یک استاندارد پذیرفته شده اندازه‌گیری شود. این شاخص‌های ارزیابی عینی عبارتند از EN (آنتروپی)، MI (اطلاعات متقابل)، انحراف استاندارد (SD)، نسبت سیگنال به نویز پیک (PSNR)، اندازه‌گیری شاخص تشابه ساختاری (SSIM)، گرادیان متوسط (AG)، ریشه‌ی میانگین مربعات خطا (RMSE)، شدت لبه (ES)، وفاداری اطلاعات بصری (VIF)، بسامد فضایی (SF) و غیره. در این مقاله چهار شاخص رایج ارزیابی به شرح زیر استفاده شده است.

- انحراف استاندارد (STD): انحراف استاندارد برای اندازه‌گیری کنتراست کلی تصویر ادغام شده استفاده می‌شود و برای تعیین تفاوت بین داده‌ها و میانگین استفاده می‌گردد. اگر مقدار STD بزرگتر باشد، عملکرد همجوشی بهتر بوده و تصویر واضح‌تر می‌شود. فرمول محاسبه STD ، طبق رابطه ی ۴ خواهد بود.

$$std = \sqrt{\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(f(i,j)-\mu)^2}{MN}} \quad (۴)$$

که در آن M و N نشان دهنده‌ی طول و عرض تصویر f خواهند هستند. μ برابر با میانگین مقادیر تصویر است.

- نسبت پیک سیگنال به نویز (PSNR): این شاخص یک روش اندازه‌گیری کمی بر اساس میانگین مربعات خطا است. در تصویر تلفیقی، هر چه PSNR بالاتر باشد، تصویر خروجی به به تصاویر منبع نزدیک‌تر خواهد بود. رابطه‌ی ۵، این معیار را توصیف می‌کند.

$$PSNR = 10 * log_{10}(\frac{L^2}{RSME^2}) \quad (۵)$$

RMSE میانگین مربعات خطا است و محاسبه آن طبق (۶)، است.

$$RSME = \sqrt{\frac{\sum_{m=1}^{M}\sum_{n=1}^{N}(ground(m,n)-fused(m,n)^2}{M\times N}} \quad (۶)$$

خطای میانگین مربع یک روش اندازه‌گیری کیفیت تصویر است. ارزش RMSE با کیفیت نسبت معکوس دارد. هرچه مقدار RMSE کمتر باشد، کیفیت تصویر ترکیب شده بهتر است. ground و fused، به ترتیب مقادیر شدت پیکسل ها در تصاویر منبع و مقصد (حاصل هم‌جوشی) را نشان می‌دهند .طول و عرض تصویر به ترتیب M و N هستند.

- شاخص تشابه ساختاری SSIM: این شاخص برای اندازه‌گیری شباهت ساختاری بین یک تصویر ترکیب شده و یک تصویر منبع استفاده می‌شود. مقدار آن بین ۰ و ۱ است که ۰ نشان دهنده همبستگی صفر با تصویر اصلی و ۱ نشان دهنده دقیقا همان تصویر است. هر چه مقدار SSIM بزرگ‌تر باشد، تصویر ادغامی بیشتر شبیه تصویر منبع است. یعنی اثر هم‌جوشی، بهتر است. از (۷)، به‌دست می‌آید.

$$SSIM_{(A,B,F)} = 0.5 \times (SSIM_{(A,F)} + SSIM_{(B,F)})$$
$$SSIM_{(A,F)} = \frac{(2\mu_A\mu_F + C_1)(2\sigma_{AF} + C_2)}{(\mu_A^2 + \mu_F^2 + C_1)(\sigma_A^2 + \sigma_F^2 + C_2)}$$
$$SSIM_{(B,F)} = \frac{(2\mu_B\mu_F + C_1)(2\sigma_{BF} + C_2)}{(\mu_B^2 + \mu_F^2 + C_1)(\sigma_B^2 + \sigma_F^2 + C_2)} \quad (۷)$$

μ_A، μ_B و μ_F به ترتیب مقادیر متوسط تصویر منبع و تصویر ادغام شده هستند. σ^2_A، σ^2_B و σ^2_F، به ترتیب واریانس های تصویر منبع و تصویر ادغام شده می‌باشند. σ_{AF} و σ_{BF} ، به ترتیب واریانس مشترک دو تصویر منبع و تصویر ادغام شده را نشان می دهند.

- فرکانس فضایی (SF): فرکانس فضایی وضوح تصویر حاصل از هم‌جوشی را منعکس می‌کند، یعنی میزان تغییر خاکستری تصویر. هرچه SF بزرگتر باشد، وضوح تصویر بالاتر است. از رابطه‌ی ۸، محاسبه می گردد.

$$Sf = \sqrt{Rf^2 + CF^2}$$
$$RF = \sqrt{\frac{1}{M(N-1)}\sum_{i=1}^{M}\sum_{j=2}^{N}(X(i,j-1)-X(i,j))^2}$$
$$CF = \sqrt{\frac{1}{M(N-1)}\sum_{i=2}^{M}\sum_{j=1}^{N}(X(i,j)-X(i-1,j))^2} \quad (۸)$$

در ادامه، روش پیشنهادی با تعدادی از تحقیقات انجام شده درحوزه‌ی ادغام تصاویر MRI-CT، مقایسه می‌شود. به منظور ارزیابی عملکرد روش‌های ادغام تصویر پزشکی چندوجهی فوق، ۴ معیار برای ارزیابی‌های کیفیت عینی مانند STD، PSNK، SSIM و SF اعمال می‌شود [۳۲]. پس از آن، عملکرد عینی آن روش‌ها در جدول (۲) نشان داده شده است. از این جدول، قابل تشخیص است که تصویر تلفیقی روش پیشنهادی از نظر جلوه‌های بصری نیز نسبت به سایر روش‌های تلفیقی برتری دارد و این نشان می‌دهد که تصویر تلفیقی شامل اطلاعات مفیدتری بوده و مشابه تصویر منبع است. وضوح روش پیشنهادی بهتر از روش‌های دیگر است، بنابراین الگوریتم DWT +fuzzy+ TXT، بالاترین مقدار را در SF دارد و در شاخص‌های ارزیابی SSIM و STD بهترین عملکرد را در بین روش‌های بررسی شده، داشته است.

جدول (۲): نتایج مقایسه‌ی روش پیشنهادی با سایر روش‌ها

	Fusion methods	*STD*	*PSNR*	*SSIM*	*SF*
Spatial domain	GFF[38]	53.726	31.159	0.486	16.003
	MSA[39]	43.522	35.071	0.483	10.822
Transform domain	NSCT+SR[40]	60.777	29.560	0.482	17.638
	NSCT+PCNN[41]	58.813	31.234	0.504	17.026
	NSCT+LE[42]	57.344	31.610	0.486	16.926
	NSCT+RPCNN[43]	57.972	31.684	0.500	17.253
	NSCT+PAPCNN[46]	57.262	32.919	0.491	15.855
	DWT[44]	41.986	31.972	0.429	13.389
	DWT+WA[45]	55.405	30.981	0.487	18.106
DL	CNN [47]	42.882	26.419	0.322	17.759
	CNN [48]	60.038	28.964	0.475	17.621
	CNN-GFEUs [49]	--	16.984	0.7281	--
	ILWT + DCT [50]	57.63	--	0.777	--
proposed	**DWT+Fuzzy+TXT**	**61.434**	**32.434**	**0.8114**	**18.325**

۶- نتیجه

تصاویر حاصل از سیستم‌های تصویر برداری پزشکی مختلف به تنهایی قادر به بیان خصوصیات کامل ساختاری و کارکردی بافت نیستند. ادغام تصاویر یکی از روش‌های مهم در بهبود تفسیر تصاویر یک صحنه حاصل از سیستم‌های تصویربرداری مختلف است. در این مقاله الگوریتم ادغام مرتبه پیکسل مبتنی بر تبدیل موجک با وزن‌دهی فازی و تبدیل بافت ارائه شده است که از قوانین ادغام فازی برای ترکیب تصاویر حاصل از سیستم‌های تصویر برداری مختلف استفاده می‌کند. با توجه به اینکه در مساله هم‌جوشی تصاویر MRI و CT با دو بافت تصویر نرم و سخت به ترتیب روبرو هستیم، در این تحقیق از یک رویکرد بهینه برای بخش بندی بافت تصاویر جهت هم‌جوشی استفاده شده است که توانسته به نتایج خوبی برای تفکیک کردن بخش‌های مختلف زوج تصاویر ادغامی، دست یابد. این کار در مقایسه با روش‌های هم‌جوشی تصاویر پزشکی دیگر توانسته است بهبود قابل توجهی در افزایش کیفیت تصاویر ادغام شده حاصل کند. همچنین با توجه به سادگی تکنیک پیشنهادی این مقاله نتایج خوبی را برای بهبود سرعت هم‌جوشی و مقاوم‌سازی تصاویر در برابر نویز و ناهمواری‌های تصاویر، حاصل کرده است.

مراجع

[1] Aghamaleki, J.A., Ghorbani, A.: Image fusion using dual tree discrete wavelet transform and weights optimization. Visual Comput. 39(3), 1181-1191 (2023), https://doi.org/10.1007/s00371-021-02396-9.

[2] Jiang, H. et al.: Casting defect region segmentation method based on dual-channel encoding–fusion decoding network. Expert Syst Appl., 123254 (2024), https://doi.org/10.1016/j.eswa.2024.123254

[3] Bayoudh, K., Knani, R., Hamdaoui, F. Mtibaa, A.: A survey on deep multimodal learning for computer vision: advances, trends, applications, and datasets. Visual Comput. 38(8), 2939-2970 (2022), https://doi.org/10.1007/s00371-021-02166-7

[4] Dinh, P.: Medical image fusion based on enhanced three-layer image decomposition and Chameleon swarm algorithm, Biomedical Signal Processing and Control,

[5] Volume 84, 2023,104740,ISSN 1746 8094, https://doi.org/10.1016/j.bspc.2023.104740

[6] Shang, X. et al.: Holistic Dynamic Frequency Transformer for image fusion and exposure correction. Inf. Fusion 102, 102073 (2024), https://doi.org/10.1016/j.inffus.2023.102073

[7] Sun, T. et al.: Artificial Intelligence Meets Flexible Sensors: Emerging Smart Flexible Sensing Systems Driven by Machine Learning and Artificial Synapses. Nano-Micro Lett. 16, 14 (2024), https://doi.org/10.1007/s40820-023-01235-x

[8] Kittusamy, K. , Kumar, L. S. V. S.: Non-Sub-Sampled Contourlet with Joint Sparse Representation Based Medical Image Fusion. Comput. Syst. Sci. Eng. 44, 1989-2005 (2023), https://doi.org/10.32604/csse.2023.026501

[9] Pan, Y., Lan, T., Xu, C., Zhang, C. ,Feng, Z.: Recent advances via convolutional sparse representation model for pixel-level image fusion. Multimed. Tools Appl., 1-32 (2023), https://doi.org/10.1007/s11042-023-17584-z

[10] Avcı, D., Sert, E., Özyurt, F. ,Avcı, E.: MFIF-DWT-CNN: Multi-focus ımage fusion based on discrete wavelet transform with deep convolutional neural network. Multimed. Tools Appl. 83, 10951-10968 (2024), https://doi.org/10.1007/s11042-023-16074-6

[11] Luo, Y. et al.: Texture classification combining improved local binary pattern and threshold segmentation. Multimed. Tools Appl., 1-18 (2023), https://doi.org/10.1007/s11042-023-14749-8

[12] Palanisami, D., Mohan, N. ,Ganeshkumar, L.: A new approach of multi-modal medical image fusion using intuitionistic fuzzy set. Biomed. Signal Process. Control. 77, 103762 (2022), https://doi.org/10.1016/j.bspc.2022.103762

[13] Li, Q., Wang, W., Chen, G. ,Zhao, D.: Medical image fusion using segment graph filter and sparse representation. Comput. Biol. Med. 131, 104239 (2021), https://doi.org/10.1016/j.compbiomed.2021.104239

[14] Li, X., Zhou, F., Tan, H., Zhang, W. ,Zhao, C.: Multimodal medical image fusion based on joint bilateral filter and local gradient energy. Inf. Sci. 569, 302-325 (2021), https://doi.org/10.1016/j.ins.2021.04.052

[15] Hermessi, H., Mourali, O. ,Zagrouba, E.: Multimodal medical image fusion review: Theoretical background and recent advances. Signal Process. 183, 108036 (2021), https://doi.org/10.1016/j.sigpro.2021.108036

[16] ULLAH, Hikmat, et al. Multimodality medical images fusion based on local-features fuzzy sets and novel sum-modified-Laplacian in non-subsampled shearlet transform domain. Biomedical Signal Processing and Control, 2020, 57. Jg., S. 101724, https://doi.org/10.1016/j.bspc.2019.101724

[17] Manchanda, M. , Sharma, R.: An improved multimodal medical image fusion algorithm based on fuzzy transform. J. Vis. Commun. Image Represent. 51, 76-94 (2018), https://doi.org/10.1016/j.jvcir.2017.12.011

[18] TANG, Lu, et al. Perceptual quality assessment for multimodal medical image fusion. Signal Processing: Image Communication, 2020, 85. Jg., S. 115852, https://doi.org/10.1016/j.image.2020.115852

[19] TAN, Wei, et al. Multimodal medical image fusion algorithm in the era of big data. Neural Computing and Applications, 2020, S. 1-21, https://doi.org/10.1007/s00521-020-05173-2

[20] XU, Lina, et al. medical image fusion using a modified shark smell optimization algorithm and hybrid wavelet-homomorphic filter. Biomedical Signal Processing and Control, 2020, 59. Jg., S. 101885, https://doi.org/10.1016/j.bspc.2020.101885

[21] Brindha, V., Jayashree, P.: Fusion of radiological images of Glioblastoma Multiforme using weighted average and maximum selection method in 11th International Conference on Advanced Computing (ICoAC), 328-332 (IEEE), https://doi.org/10.1109/ICoAC48765.2019.246861

[22] Bavirisetti, D. P., Kollu, V., Gang, X. ,Dhuli, R.: Fusion of MRI and CT images using guided image filter and image statistics. Int. J. Imaging Syst. Technol. 27, 227-237 (2017), https://doi.org/10.1002/ima.22228

[23] Haribabu, M. , Guruvaiah, V.: Statistical measurements of multi modal MRI–PET medical image fusion using 2D–HT in HSV color space. Procedia Comput. Sci. 165, 209-215 (2019), https://doi.org/10.1016/j.procs.2020.01.090

[24] Nan Jiang, Bin Sheng; Ping Li; Tong-Yee Lee, "PhotoHelper: Portrait Photographing Guidance Via Deep Feature Retrieval and Fusion", IEEE Trans. Multim. 25, 2226-2238 (2023), https://doi.org/10.1109/TMM.2022.3144890

[25] Liang, N., Medical image fusion with deep neural networks. Scientific Reports, 2024. 14(1): p. 7972, https://doi.org/10.1038/s41598-024-58665-9
[26] Arora, S. , Kaur, A.: Modified edge detection technique using fuzzy inference system. Int. J. Comput. Appl. 44, 9-1 (2012), https://doi.org/10.5120/6409-8757
[27] Anindyaguna, K., Basjaruddin, N. C. ,Saefudin, D.: Overtaking assistant system (OAS) with fuzzy logic method using camera sensorin 2016 2nd International Conference of Industrial, Mechanical, Electrical, and Chemical Engineering (ICIMECE). 89-94 (IEEE), https://doi.org/10.1109/ICIMECE.2016.7910420
[28] Zhang, Z. , Blum, R. S.: A categorization of multiscale-decomposition-based image fusion schemes with a performance study for a digital camera application. Proceedings of the IEEE 87, 1315-1326 (1999), http://doi.org/10.1109/5.775414
[29] Ming, L. , Shunjun, W.: A novel hybrid image fusion method based on integer lifting wavelet and discrete cosine transformer for visual sensor networks in Proceedings Fifth International Conference on Computational Intelligence and Multimedia Applications. ICCIMA 2003. 154-159 (IEEE), https://doi.org/10.1007/s11042-018-6676-z
[30] Laws, K. I. in Image processing for missile guidance. 376-381 (SPIE), https://doi.org/10.1080/713820676
[31] Kassner A, Thornhill RE. Texture analysis: a review of neurologic MR imaging applications. AJNR Am J Neuroradiol. 2010 May;31(5):809-16, https://doi.org/10.3174/ajnr.A2061
[32] Targhi, A. T., Hayman, E., Eklundh, J.-O. ,Shahshahani, M. in Asian Conference on Computer Vision. 70-79 (Springer).

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

Modeling the speech recognition system using the deep learning technique of spiking neural networks

Melika Hamian*[1], Karim Faez[2], Sohila Nazari[3], Maliheh Sabeti[4]

[1] Department of Engineering, Payame Noor University (PNU), Hamedan, Iran.
hamian.melika@gmail.com
[2] Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran.
karim.faez@gmail.com
[3] Department of Electrical Engineering, Shahid Beheshti University, Tehran, Iran.
msoheilanazari21@yahoo.com
[4] Department of Computer Engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran.
malihe.sabeti@gmail.com

Abstract: The architecture of spiking neural network (SNN) is introduced inspired by dynamic spiking neurons. SNNs have great potential to understand time-dependent entanglement pattern by dynamic spiking neurons and can process coded data according to time event. However, training deep SNNs is not straightforward. In this paper, we propose a new layered SNN learning framework for fast and efficient pattern recognition, which uses optimization algorithms to learn deep SNNs. In the mentioned method in the deep learning problem of our deep SNN layers, with the help of different algorithms of gradient-based optimization (GBO) and wild horse optimization (WHO), the two main parameters of spike neurons are searched and calculated for different layers. We use SNN to model the digital speech recognition system and compare and evaluate their performance in different scenarios with other deep learning methods. The results of SNN training for data extracted from different datasets show an increase in identification and estimation accuracy compared to the performed tasks. Comparing the results, the proposed SNN-WHO method was able to achieve accuracies of 95.47% and 92.3% among its counterparts, and they show an increase in the accuracy of identification and estimation compared to the performed works.

Keywords: spiking Neural Networks (SNN); Gradient Based Optimization (GBO) ; Wild Horse Optimization (HWO).

JCDSA, Vol. 2, No. 3, Autumn 2024	Online ISSN: 2981-1295	Journal Homepage: https://sanad.iau.ir/en/Journal/jcdsa
Received: 2023-12-06	Accepted: 2024-09-23	Published: 2024-12-20

CITATION

Hamian, M., et. al., " *Modeling the speech recognition system using the deep learning technique of spiking neural networks*", Journal of Circuits, Data and Systems Analysis (JCDSA), Vol. 2, No. 3, pp. 43-52, 2024.
DOI: 00.00000/0000

* Corresponding author

Extended Abstract

1- Introduction

The architecture of spiking neural network is introduced inspired by dynamic spiking neurons. SNNs have great potential to understand time-dependent entanglement pattern by dynamic spiking neurons and can process coded data according to time event. However, training deep SNNs is not straightforward. In this paper, we propose a new layered SNN learning framework for fast and efficient pattern recognition, which uses optimization algorithms to learn deep SNNs. In the mentioned method in the deep learning problem of our deep SNN layers, with the help of different algorithms of gradient based optimization (GBO) and wild horse optimization (WHO), two main parameters of spike neurons are searched and calculated for different layers. We use SNN to model the digital speech recognition system and compare and evaluate their performance in different scenarios with other deep learning methods. Comparing the results, the proposed SNN-WHO method was able to achieve accuracies of 95.47 and 92.3 among its counterparts, and they show an increase in the accuracy of identification and estimation compared to the performed works.

2- Methodology

Considering the problem of SNN training according to systematic data, providing an optimization approach with the help of optimization algorithms is the main solution to adapt the trained systems to the expected values. Therefore, in this article, an effective error measure is used to calculate the objective function. First, we prepare the training data for the desired system. In this step, with the help of a genetic algorithm, the data sets or features that have the closest match with the system outputs are normalized to train the SNN network in the interval [0,1]. Other input features are removed from the training set. After preparing the training data for the SNN network and defining the network structure for the number of layers and neurons in each layer, we determine the learning parameters of the DSNN deep spiking neural network by algorithms.

In this method, by determining the number of layers of the deep SNN network and the number of neurons in each layer, a general definition of the network is obtained, which is used to match the results of the desired system to estimate the output of the network. The system will use the optimization algorithms proposed in this article (GBO and WHO).

To match the simulation results, we need to calculate the generated network for each test data and calculate the effective error or deviation for their equivalent outputs. In the next step, the objective function of aggregating all errors is determined based on the following relationship. The important point for calculating and valuing the output of the network in this work is to calculate the RMS value of the turn spike in the output of the output neuron, which is calculated for the interval 0 to 0.21.

$$F(x) = (\exp(\mu * \sum error(i)^2) - 1) \quad \text{for} \quad i = 1, \ldots, \text{number of training set}$$

3- Results and discussion

In this article, we have used two data sets to analyze the performance of our proposed design for different samples. Three machine learning methods have been applied, which include feedforward ANN and ANFIS, adaptive neural network, and the proposed SNN method with two GBO and WHO algorithm approaches. For this case study, the defined network of a three-layer network with the number of neurons [5 3 1] has been used for all machine learning networks. Comparing the results, the proposed SNN-WHO method was able to achieve accuracies of 95.47 and 92.3 among its counterparts, and they show an increase in the accuracy of identification and estimation compared to the performed works.

4- Conclusion

Preliminary results have shown that the detection performance of SNNs is either comparable or slightly worse than that of ANNs with the same network architecture. A possible reason for this performance reduction is the reduced representation power of the discrete neural representation (i.e. spike count) compared to the continuous floating point representation of artificial neural networks. In addition, the identification performance of ANFIS and ANN and SNN models in a scenario with few resources is also investigated. In this scenario, SNN noise models outperform conventional artificial neural networks, which can be attributed to the noisy training of the burst learning framework. The neural encoding scheme adopted in this work allows the input features to be encoded in a short encoding time window for fast processing by SNNs. Recurrent neural networks by exploring the long temporal context information in the input signals have excellent modeling capability for the signals. They have shown once. As future work, we will investigate recurrent networks of spiking neurons for speech recognition applications for digit classification to improve recognition performance.

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

مدل‌سازی سیستم تشخیص گفتار با استفاده از تکنیک یادگیری عمیق شبکه‌های عصبی اسپایکینگ

ملیکا حامیان*[1] ، کریم فایز[2]، سهیلا نظری[3]، ملیحه ثابتی[4]

۱- عضو هیات علمی دانشگاه پیام نور همدان، ایران(hamian.melika@ pnuhp.ac.ir)
۲- گروه مهندسی برق، دانشگاه صنعتی امیرکبیر، تهران، ایران(karim.faeez@gmail.com)
۳- دانشکده مهندسی برق، دانشگاه شهید بهشتی، تهران، ایران(msoheilanazari21@yahoo.com)
۴- مهندسی کامپیوتر، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران(malihe.sabeti@gmail.com)

چکیده: ساختار شبکه عصبی اسپایکینگ با الهام از نورون‌های اسپایکینگ پویا معرفی شده است. شبکه‌های عصبی اسپایکینگ پتانسیل فوق‌العاده‌ای برای درک الگوی درهم وابسته به زمان توسط نورون‌های اسپایکینگ پویا دارند و می‌توانند داده‌های رمزگذاری شده را مطابق با رویداد زمان پردازش کنند. با این حال، آموزش شبکه‌های عصبی اسپایکینگ عمیق ساده نیست. در این مقاله، یک چارچوب جدید یادگیری لایه‌ای شبکه عصبی اسپایکینگ برای تشخیص الگوی سریع و کارآمد پیشنهاد می‌شود که از الگوریتم‌های بهینه‌سازی برای یادگیری شبکه‌های عصبی اسپایکینگ عمیق استفاده می‌کند. در روش اشاره شده در مساله یادگیری عمیق، به کمک الگوریتم‌های مختلف بهینه‌سازی مبتنی بر گرادیان و بهینه‌سازی اسب وحشی، دو پارامتر اصلی نرون‌های اسپایک برای لایه‌های مختلف جستجو و محاسبه می‌شود. در این مقاله، از شبکه عصبی اسپایکینگ برای مدل‌سازی سیستم تشخیص گفتار رقمی استفاده و عملکرد آن‌ها در سناریوهای مختلف با سایر روش‌های یادگیری عمیق مقایسه و ارزیابی می‌شود. در مقایسه نتایج، روش پیشنهادی شبکه‌های عصبی اسپایکینگ با بهینه‌سازی اسب وحشی توانسته به دقت‌های ۹۵.۴۷٪ و ۹۲.۳٪ در بین همتایان خود دست پیدا کند؛ که افزایش دقت شناسایی و تخمین را نسبت به کارهای انجام شده نشان می‌دهند.

واژه های کلیدی: شبکه‌های عصبی اسپایکینگ، بهینه‌سازی مبتنی بر گرادیان، بهینه‌سازی اسب وحشی.

نوع مقاله: پژوهشی
DOI: 00.00000/0000
تاریخ ارسال مقاله: ۱۴۰۲/۰۹/۱۵ تاریخ پذیرش مقاله: ۱۴۰۳/۰۷/۰۲ تاریخ چاپ مقاله: ۱۴۰۳/۰۹/۳۰

۱- مقدمه

در سالهای اخیر، شبکه‌های عصبی اسپایکینگ[2] به عنوان نسل جدیدی از شبکه‌های عصبی عمیق کم مصرف به دلیل پردازش پراکنده، ناهمزمان و رویداد محور باینری و قابل اجرا در سخت افزار ظهور کرده‌اند [۱]. شبکه عصبی مصنوعی عمیق به صورت کنترل‌شده از طریق انتشار برگشتی آموزش داده می‌شود [۲] و به‌طور گسترده‌ای به عنوان ابزار محاسباتی برای حل مشکل طبقه‌بندی، رگرسیون، تشخیص الگو و مسئله تخمین تابع و همچنین مسئله بهینه‌سازی پیچیده با ساختار بسیار غیر خطی و ناپیوسته مورد استفاده است. برخی از اشکالات شبکه‌های عصبی مصنوعی به عنوان مجموع چالش‌ها و محدودیت‌های قابل توجه شناخته می‌شوند.

- چند بعدی بودن داده‌ها از جمله محدودیت‌های قابل توجه در یادگیری تحت نظارت است که زمانی اتفاق می‌افتد که میزان ویژگی‌ها و امتیازات آموزشی به طرز وحشتناکی زیاد شود.
- با توجه به حافظه حاصله و نیازهای محاسباتی و حجم غیرقابل مقاومت داده برای آموزش در بعد سخت‌افزاری، یادگیری شبکه‌های عصبی را چالش برانگیزتر می‌کند.
- چالش اضافی در طبقه‌بندی، همپوشانی ویژگی مشخصه بین کلاس‌های مختلف است، زیرا داده‌ها غیرخطی هستند، کار تقسیم کلاس‌ها را چالش‌برانگیز کرده است.
- مدل‌های یادگیری عمیق معمولاً در بسیاری از انواع داده‌ها عملکرد خوبی دارند، اما همواره یک مجموعه داده بزرگ برای آموزش آنها برای تولید نتایج معنی‌دار ضروری است.

* نویسنده مسئول

[2] spiking neural networks (SNN)

با تمرکز بر بهبود این اشکالات با استفاده از روش اکتشافی، مدل‌های شبکه عصبی اسپایکی خوشه‌بندی داده‌ها در این کار بررسی می‌شود. اگرچه شبکه عصبی اسپایکینگ دارای مزایای شباهت مغزی قوی و مصرف کم انرژی به دلیل استفاده از اسپایک‌های گسسته برای نمایش و انتقال اطلاعات است، عملکرد آن هنوز نیاز به بهبود دارد و آموزش مستقیم شبکه عصبی اسپایکینگ چالش‌برانگیز است و در مقایسه با شبکه‌های عصبی از دقت بالایی برخوردار نیست.

- شبکه‌های عصبی اسپایکینگ قابلیت‌هایی را برای پردازش اطلاعات داده‌های منابع مختلف با تعریف این وزن‌ها، نشان داده‌اند.
- علاوه بر این، مدل‌های مبتنی بر شبکه‌های عصبی اسپایکینگ توانایی شبیه‌سازی موفقیت‌آمیز دینامیک عصبی زیربنایی برای کاربردهای تشخیص را نشان داده‌اند.
- با توجه به تعاریف انجام شده برای شبکه عصبی اسپایکینگ و قابلیت اجرای سخت‌افزاری ساده این سیستم در پردازنده‌های کم مصرف، به کاربردهای مهم در این شبکه‌ها برای طبقه‌بندی و پردازش‌های هوش مصنوعی دست یافته‌ایم.

بنابراین تلاش شده است تا مسائل مختلف با کمک شبکه‌های عصبی اسپایکینگ پردازش و حل گردد. اما برای این مدل از هوش مصنوعی با چالش‌هایی برای آموزش و بهینه‌سازی روبرو هستیم. از مهمترین چالش‌ها، برخورد با نحوه آموزش شبکه برای داده‌های مختلف کلاسه‌بندی طبق تعریف وزن‌های مختلف برای نرون‌های لایه‌های مختلف در شبکه عصبی اسپایکینگ عمیق است. ارائه یک مدل آموزش برای شبکه‌های عصبی اسپایکینگ عمیق برای افزایش دقت طبقه‌بندی، از چالش‌های مهم تحقیقاتی اخیر برای کاربردهای کلاسه‌بندی و هوش مصنوعی است. در رویکردهای ارائه شده در مساله آموزش، برای افزایش دقت شبکه نیازمند افزایش نرون‌ها و تعداد لایه‌های شبکه‌های عصبی اسپایکینگ هستیم که این با مشکل پیچیدگی محاسباتی برای آموزش روبرو می‌شود. این مساله ما را بر این داشت تا به دنبال یک روش جدید برای پشتیبانی از شبکه‌های عصبی اسپایکینگ عمیق و پیچیده به منظور افزایش دقت آموزش طبقه‌بندی باشیم.

در [۴]، یک چارچوب جدید تبدیل شبکه‌های عصبی به شبکه‌های عصبی اسپایکینگ و چارچوب یادگیری لایه‌ای را برای تشخیص الگوی سریع و کارآمد پیشنهاد شده است که به عنوان یادگیری پشت سر هم پیشرونده شبکه‌های عصبی اسپایکینگ عمیق شناخته می‌شود. با انگیزه بهره‌وری انرژی بی‌سابقه و قابلیت پردازش سریع اطلاعات، استفاده از شبکه‌های عصبی اسپایکینگ را برای تشخیص گفتار در [۵] بررسی شده است. در این کار، از شبکه‌های عصبی اسپایکینگ برای مدل‌سازی صوتی استفاده شده است و عملکرد آن‌ها را در چندین سناریو تشخیص واژگان بزرگ ارزیابی می‌گردد. نتایج تجربی دقت تشخیص خودکار گفتار واژگان بزرگ رقابتی را به همتایان شبکه‌های عصبی خود نشان می‌دهند.

ازدحام بیش از حد طیف و انسداد شبکه مخابرات بیسیم که باعث قطع تماس می‌شود از نگرانی‌های مهم این شبکه‌ها است. برای مقابله با این مسائل به طور همزمان یک شبکه رله مبتنی بر فناوری رادیویی شناختی در [۶] پیشنهاد شده است. ابتدا یک تکنیک حسگر طیفی مبتنی بر شبکه عصبی اسپایکینگ آموزش دیده با الگوریتم بهینه‌سازی نهنگ اصلاح‌شده جهش یافته برای تشخیص کارآمد حفره‌های طیف پیشنهاد شده است. در اینجا، وزن‌های شبکه‌های عصبی اسپایکینگ با استفاده از این الگوریتم برای پیش‌بینی مؤثر حفره‌های طیف آموزش داده می‌شوند. در[۷]با استفاده از بهینه‌سازی الگوریتم ژنتیک مرتب‌سازی غیرمسلط روی یک مدل شبکه‌های عصبی اسپایکینگ کارآمد خاص، با استفاده از مدل عصبی ایژیکویچ، برای انجام بهینه‌سازی چند هدفه در شبکه‌های عصبی اسپایکینگ، با تمرکز بر جستجوی پارامترهای اتصال شبکه برای دستیابی به نرخ شلیک هدف انواع عصبی تحریک‌کننده و مهارکننده، به کار رفته است. در [۸]، یک معماری عصبی رویداد محور مدولار آموزش‌پذیر انتها به انتها ارائه می‌شود که از قوانین انطباق سیناپسی و آستانه‌ای محلی برای انجام دگرگونی‌های بین الگوهای سنبله مکانی-زمانی دلخواه استفاده می‌کند. این معماری یک مدل بسیار انتزاعی از معماری‌های شبکه عصبی اسپایکی موجود را نشان می‌دهد. معماری شبکه عصبی اسپایکی مبتنی بر رویداد عمیق پیشنهادی (ODESA) می‌تواند به طور همزمان ویژگی‌های مکانی-زمانی سلسله مراتبی را در مقیاس‌های زمانی دلخواه متعدد بیاموزد. این مدل یادگیری آنلاین را بدون استفاده از پس انتشار خطا یا محاسبه گرادیان انجام می دهد. در [۹]، چارچوبی مبتنی بر بهینه‌سازی انرژی آزاد تکراری با شبکه‌های عصبی اسپایکینگ برای مدل‌سازی سیستم فرونتو – مخطط (PFC-BG) برای تولید و یادآوری توالی‌های حافظه صوتی ارائه می‌کند. در راستای مطالعات تصویربرداری عصبی انجام شده در PFC، یک استراتژی کدگذاری واقعی با استفاده از مکانیسم افزایش مدولاسیون پیشنهاد می‌شود تا توالی‌های انتزاعی را تنها بر اساس رتبه و مکان آیتم‌ها در آن‌ها نشان داد. بر اساس این مکانیسم، می‌توان مجموعه‌ای از نورون‌های حساس به ساختار زمانی را در توالی‌هایی ساخت که از آن‌ها بتوان هر دنباله جدیدی را نشان داد. شبکه‌های عصبی اسپایکینگ های پیشرفته برای دستیابی به دقت بالا به حافظه زیادی نیاز دارند، در نتیجه استقرار آنها در سیستم‌های تعبیه شده، به عنوان مثال، در دستگاه‌های تلفن همراه با باتری و گره‌های لبه اینترنت اشیا دشوار می‌شود. در این راستا، مقاله [۱۰]، FSpiNN را پیشنهاد می‌کند، یک چارچوب بهینه‌سازی برای به دست آوردن شبکه‌های عصبی اسپایکینگ‌های کارآمد با حافظه و انرژی کارآمد برای آموزش و پردازش استنتاج، با قابلیت یادگیری بدون نظارت و در عین حال حفظ دقت ارائه شده است.

اکثر تکنیک‌های قبلی شبکه‌های عصبی اسپایکینگ که داده‌ها را مدیریت می‌کنند به شبکه‌های کم عمق محدود می‌شوند و بنابراین، عملکرد پایینی را نشان می‌دهند. به طور کلی، رفتار ادغام و آتش‌سوزی نورون‌های اسپایک، فعالیت اسپایک را در لایه‌های عمیق‌تر کاهش می‌دهد. فعالیت پراکنده اسپایک منجر به یک راه حل بهینه جهانی (به

عنوان مثال، کاهش تابع هدف) در طول آموزش می‌شود. برای پرداختن به این محدودیت، مقاله [۱۱] پیشـــرفت‌های الگوریتمی و معماری جدیدی را برای تسریع آموزش شبکه‌های عصبی اسپایکینگهای بسیار عمیق بر روی داده‌های DVS[1] پیشـــنهاد می‌کند. به طور خاص، با آموزش بالابر فعال‌سازی اسپایک (SALT) که با بهینه‌سازی وزن‌ها و آستانه‌ها در لایه‌های کانولوشن، فعالیت سنبله را در تمام لایه‌ها افزایش می‌دهد. پس از اعمال SALT، وزنه ها را بر اساس افت آنتروپی متقاطع آموزش می یابد.

تاکنون مشخص نیست که این فرآیند خودبهینه‌سازی تا چه حد در مغزهای واقعی نیز مؤثر اســت. در [۱۲] اجرای یک مدل شـــبکه عصـــبی اســـپایکینگ خودبهینه‌ســاز عملی شـــده اســت. در این کار، با استفاده از این شبکه عصبی اسپایک برای شبیه‌سازی شبکه هاپفیلد با یادگیری هبی، سعی می‌شود بین سیستم‌های عصبی مبتنی بر نرخ و مبتنی بر کدگذاری زمانی ارتباط برقرار گردد. اگرچه کارایی فرآیند خودبهینه‌سازی مستقل از فرضیات ساده‌سازی یک شبکه هاپفیلد معمولی است اما، برای واقعی‌تر کردن این مدل در حوزه سخت افزار به کار بیشتری نیاز است.

نوآوری ما در این مقاله اســتفاده از یک چارچوب جدید ســیســتم یادگیری ماشین مبتنی بر شبکه‌های عصبی اسپایکینگ با الگوریتم‌های بهینه‌سازی می‌باشد. در این راستا برای آموزش از یک سیستم تطبیق نتایج طبقه‌بندی با کمک دو الگوریتم بهینه ســازی مبتنی بر گرادیان[2] و بهینه‌ســازی اســب وحشــی[3] برای تعیین پارامترهای شـبکه نرون‌های اســپایکینگ بهره برده اســت. در حقیقت در این تحقیق برای توســعه آموزش‌های نرون‌های اســـپایکینگ از الگوریتم‌های بهینه‌ســـازی بهره برده‌ایم تا برای اطلاعات مختلف پارامترهای شـــبکه‌های عصـــبی اســپایکینگ شــامل وزن و مقدار آســتانه هر نرون محاســبه شــود و با مقدارهای نمونه داده‌های آموزش تطبیق یابد.

۲- مفاهیم اولیه

در این بخش به مفاهیم اولیه مورد اســـتفاده در این مقاله خواهیم پرداخت. در ابتدا شبکه عصبی اسپایکینگ معرفی و مدلسازی می‌شود. ســپس الگوریتم‌های بهینه‌ســازی مورد اســتفاده در این مقاله معرفی می‌شـــود. در آخر، مزایا و محدودیت‌های این شـــبکه‌های عصـــبی اسپایکینگ ها تشریح می‌شود و نیاز به یک تکنیک آموزش جدید برای شبکه‌های عصبی اسپایکینگ بیان می‌شود.

۲-۱- مفهوم عصب‌های مصنوعی

ساده‌ترین مدل نورون که معمولاً برای کاربرد عملی مورد بررسی قرار گرفته می‌شود، مدل مک‌کالوخ-پیتس است که در سال ۱۹۴۳ توصیف شد [۱۳] و توسط روزنبلت در سال ۱۹۵۸ [۱۴] پیاده‌سازی شد. در این مدل، یک نورون به عنوان یک ماژول جمع وزنی معرفی می‌شود که تمام مقادیر ورودی را جمع می‌کند و آن را در مقداری به نام وزن ضرب می‌کند. سپس این مقدار از یک تابع انتقال عبور می‌کند و به عنوان یک خروجی محاسبه می‌شود. مدل را می‌توان به صورت (۱) نشان داد [۱۵]:

$$y = f(u), \mathrm{u} = \sum_{k=0}^{n} wixi + w0x0 \qquad (۱)$$

در (۱)، xi نشان‌دهنده سیگنال‌های ورودی، wi نشان‌دهنده وزن‌های ورودی و $\mathrm{f(u)}$ یک تابع انتقال است. پارامترهای $x0$ و $w0$ مقدار اولیه یک نورون را معرفی می‌کنند. تابع انتقال تعیین می‌کند که سیگنال خروجی چگونه به مجموع وزنی سیگنال‌های ورودی وابسته باشد. معمولاً نیاز به ارضای چند شرط مانند محدود بودن ارزش، افزایش یکنواختی، تعیین بر روی همه آرگومان‌های واقعی و قابل تمایز بودن برای تسهیل الگوریتم های یادگیری تعریف می‌شود.

۲-۲- مدل نورون های اسپایکینگ

شبکه‌های عصبی اسپایکینگ، شبکه های عصبی مصنوعی هستند که از نزدیک، شـبکه‌های عصـبی طبیعی را تقلید می‌کنند. علاوه بر حالت عصبی و سیناپسی، شبکه‌های عصبی اسپایکینگ مفهوم زمان را در مدل عملیاتی خود قرار می‌دهند. ایده این اســت که نورون‌ها در شـبکه‌های عصـبی اسـپایکینگ اطلاعات را در هر چرخه انتشـار منتقل نمی‌کنند، بلکه اطلاعات را فقط هنگامی انتقال می‌دهند که پتانســیل غشای - کیفیت ذاتی نورون مربوط به بار الکتریکی غشای آن - به یک مقدار خاص می‌رسد که آستانه نامیده می‌شود. وقتی پتانسیل غشا به آســتانه می‌رســد، نورون آتش می‌کند و ســیگنالی تولید می‌کند که به نورون های دیگر می‌رود که به نوبه خود، در پاســخ به این ســیگنال، پتانسیل‌های خود را افزایش یا کاهش می‌دهند. به یک مدل نورونی که در لحظه عبور از آســتانه آتش‌ســوزی می‌کند، مدل نورون ســنبله گفته می‌شـود. برجسته‌ترین مدل نورون سـنبله‌ای، مدل ادغام و آتش است. در مدل ادغام و آتش، ســطح فعال‌ســازی لحظه‌ای (به عنوان معادله دیفرانسیل مدل‌سازی شده) به طور معمول حالت نورون در نظر گرفته می‌شـود. با افزایش ســنســورهای ورودی، این مقدار را بالاتر یا پایین می‌کند تا اینکه در نهایت حالت پوســیدگی یا در صــورت رســیدن به آستانه شلیک - نورون شلیک می‌کند. پس از شلیک ، متغیر حالت به مقدار کمتری تنظیم می‌شود.

روش‌های مختلف رمزگشـایی برای تفسـیر سـنبله یا اسـپایک به عنوان یک عدد با ارزش واقعی وجود دارد، با تکیه بر فرکانس سـنبله‌ها (کد نرخ)، زمان ســنبله برای اولین بار پس از تحریک، یا فاصــله بین خوشـــه در این مقاله برای بخش مقداردهی نهایی نرون آخر از مفهوم میانگین پالس‌های نرون خروجی برای ارزش‌گذاری سیستم شبکه‌های عصـبی اسـپایکینگ پیشـنهاد و اسـتفاده شـده اسـت. برای درک نحوه عملکرد مغز، باید مطالعات تجربی سیستم عصبی حیوان و انسان را با شـــبیه‌ســـازی عددی مدل‌های مغز در مقیاس بزرگ ترکیب کنیم.

[1] Dynamic Vision Sensor
[2] Gradient Based Optimization (GBO)
[3] Wild Horse Optimization (HWO)

همانطور که ما چنین مدل‌های مغزی در مقیاس بزرگی متشـــکل از نورون‌های پراکنده را توسـعه می‌دهیم، باید مصـالحه‌ای بین دو الزام به ظاهر منحصـر به فرد پیدا کنیم: مدل یک نورون منفرد باید: ۱) از نظر محاسـباتی سـاده، در عین حال ۲) قادر به تولید الگوهای شـلیک غنی باشد. نورون‌های بیولوژیکی واقعی استفاده از مدل‌های دقیق بیوفیزیکی نوع هوچکین-هاکسـلی از نظر محاسـباتی بسـیار منع اسـت، زیرا ما می‌توانیم تنها تعداد انگشـــت شـــماری از نورون‌ها را در زمان واقعی شـبیه‌سـازی کنیم. در مقابل، اسـتفاده از یک مدل ادغام و آتش از نظر محاسباتی مؤثر است، اما این مدل به‌طور غیرواقعی ساده است و قادر به تولید پویایی‌های پرشتاب و انفجاری است که توسط نورون‌های قشر مغز به نمایش گذاشته می‌شود.

در این مقاله، یک مدل اسپایکی ساده استفاده شده است که از نظر بیولوژیکی به اندازه مدل هوچکین-هاکسلی قابل قبول است، اما از نظر محاســباتی به اندازه مدل ادغام و آتش کارآمد اســت. بســته به چهار پارامتر، این مدل رفتار جهش و انفجار انواع شـــناخته شـــده نورون‌های قشر مغز را بازتولید می کند. تجزیه و تحلیل ریاضی مدل در مونوگراف ایژیکویچ [۱۶] منتشر شده است.

۲-۳- نورون‌های ادغام و آتش

این مدل، پرکاربردترین مدل است که عموماً به عنوان شبکه عصبی اسپایکینگ استفاده می‌شود. این مدل بر اصول الکترونیک تکیه داشت. یک اسپایک از آکسون پایین می‌رود و توسط یک کانال پایین گذر تغییر می‌کند، که در طول پالس کوتاه به یک پالس جریان $I(t-t_j(f))$ تبدیل می‌شود که مدار مختصات و آتش را شارژ می‌کند. یک پتانسیل پس سیناپسی $\varepsilon(t-t_i{}^f)$ را می‌توان با افزایش ولتاژ حاصل افزایش داد. با این حال، نورون یک پالس ارسال می‌کند که ولتاژ از مقدار آستانه بیشتر شود [۱۸، ۱۹].

$$\tau_m \frac{\partial u}{\partial m} = -u(t) + RI(t) \qquad (۲)$$

برای به تصویر کشیدن پیامدهای یک پتانسیل غشایی u بعد از مدتی، با τ_m زمان لایه‌ای است که در آن ولتاژ "نشت" می‌کند. به طور مشابه با مدل واکنش اسپایک، هنگامی که u از حد عبور کرد و یک پالس کوتاه σ تحریک شد، نورون شلیک می‌شود.

$$I_i(t) = \sum_{j\in\Gamma_i} c_{ij} \sum_{t_j} \delta(t - t_j^{(0)}) \qquad (۳)$$

جریان ورودی I برای نورون I به طور منظم صفر خواهد بود، زیرا پالس‌های نزدیک به طول کوتاه محدودی دارند. هنگامی که یک اسپایک ظاهر می شود، توسط عامل زنده ماندن سیناپسی c_{ij} افزایش می‌یابد که پتانسیل پس سیناپسی را که خازن را شارژ می‌کند، شکل می‌دهد. این مدل از نظر محاسباتی ساده است و بدون شک می‌توان آن را برای سخت افزارهای چندبعدی اعمال کرد [۱۸].

۲-۴- الگوریتم بهینه‌ساز اسب وحشی

الگوریتم‌های بهینـه‌ســـازی معمولاً از رفتار طبیعی یک عامل الهام می‌گیرند که می‌تواند انســـان، حیوان، گیاه یا یک عامل فیزیکی یا شـیمیایی باشـد. بسـیاری از الگوریتم‌های ارائه شـده در دهه گذشـته از رفتار حیوانات الهام گرفته شـده‌اند. در این مقاله از یک الگوریتم جدید به نام بهینه‌سـاز اسـب وحشـی اسـتفاده می‌کنیم که از رفتار اجتماعی اسب‌های وحشی الهام گرفته شده است. اسب‌ها معمولاً در گروه‌هایی متشـکل از یک اسـب نر و چند مادیان و کره اسـب زندگی می‌کنند. اســـب‌ها رفتارهای زیادی از خود نشـــان می‌دهند، مانند چرا، تعقیب، تســـلط، رهبری و جفت گیری. رفتار جذابی که اســـب‌ها را از ســـایر حیوانات متمایز می‌کند، ادب آنهاسـت. رفتار پرورش اسـب به گونه‌ای است که کره اسب‌ها قبل از رسیدن به سن بلوغ گروه را ترک کرده و به گروه‌های دیگر می‌پیوندند. این خروج برای جلوگیری از جفت شـــدن پدر با دختر یا خواهر و برادر است. الهام‌بخش اصلی الگوریتم پیشنهادی رفتار مؤدبانه اسب است[۲۰].

۲-۵- الگوریتم مبتنی بر گرادیان

در الگوریتم مبتنی بر گرادیان پیشـــنهادی کـه ترکیبی از روش‌های گرادیان و جمعیت است، جهت جستجو با روش نیوتن مشخص می‌شود تا دامنه جســـتجو را با اســـتفاده از مجموعه ای از بردارها و دو عملگر اصلی (یعنی قانون جستجوی گرادیان و عملگرهای محلی فرار) جستجو کند. به حداقل رساندن تابع هدف در مسائل بهینه‌سازی در نظر گرفته می‌شود. [۲۱].

۲-۶- مزایا و محدودیت‌های شبکه‌های عصبی اسپایکینگ‌های عمیق

یک انگیزه برای مطالعه شـبکه‌های عصـبی اسـپایکینگ‌ها این اسـت که مغزهای طبیعی عملکرد خوبی را برای شناخت در کارهای دنیای واقعی از خود نشـــان می‌دهنـد. با تلاش‌های مـداوم برای بهبود درک مـا از محاسبات مغزی، انتظارات وجود دارد که مدل‌هایی که به زیست‌شناسی نزدیک‌تر هســـتند، نســـبت به مدل‌های انتزاعی‌تر به هوش طبیعی نزدیک‌تر می‌شـــوند و توانایی بیشـــتری برای پیشـــبینی و مدلســـازی سیسـتم‌ها و داده های مختلف را دارند. شـبکه‌های عصـبی اسـپایکینگ برای پردازش اطلاعات مبتنی بر رویداد مکانی-زمانی از حســـگرهای نورومورفیک، که خود کارآمد هســـتند، مناســـب هســـتند. حســـگرها اطلاعات دقیق زمانی را از محیط ضـبط می‌کنند و شـبکه‌های عصـبی اســـپایکینگ می‌توانند از کدهای زمانی کارآمد در محاســـبات خود نیز اســـتفاده کننـد و پردازش اطلاعات را انجام دهنـد [۲۲]. این پردازش اطلاعات نیز رویداد محور اســـت به این معنی که هر زمان که اطلاعات کمی ثبت شـــود یا هیچ اطلاعاتی ثبت نشـــده باشـــد، محاســـبات در شبکه‌های عصبی اسپایکینگ به مقدار زیادی کاهش می‌یابد، اما زمانی که رویدادها یا اسـپایک‌های ناگهانی فعالیت ثبت می‌شـود، شـبکه‌های عصبی اسپایکینگ اسپایک های بیشتری ایجاد می‌کند. با این فرض که

معمولاً اطلاعات از دنیای خارج شامل رویدادهای پراکنده است، این منجر به یک ایجاد روش محاسباتی بسیار کارآمد می‌شود. علاوه بر این، استفاده از ورودی حوزه زمان در مقایسه با رویکردهای فریم محور، که در آن یک مرحله زمانی مصنوعی تحمیل شده توسط سنسور معرفی می‌شود، اطلاعات ارزشمند بیشتری است.

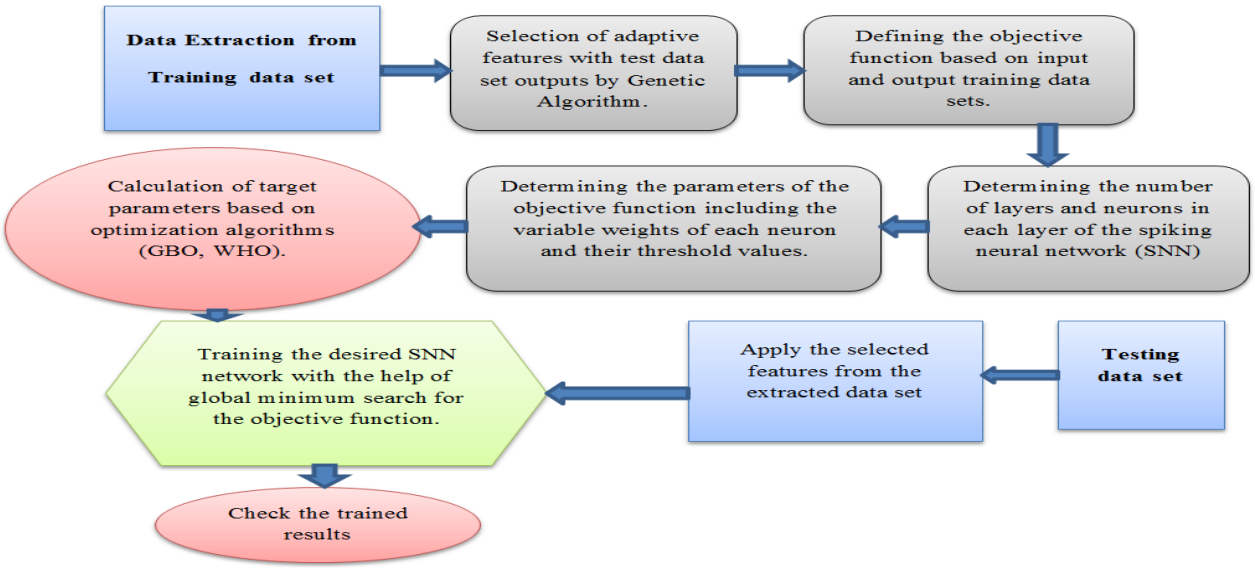
یکی از بزرگترین اشکالات شبکه‌های عصبی اسپایکینگ عمیق این است که علیرغم پیشرفت اخیر [۲۳، ۲۴] دقت آنها در معیارهای معمولی مانند MNIST [۲۵]، CIFAR [۲۶] یا ImageNet [۲۷] به سطوح مشابهی با همتایان یادگیری ماشین خود نمی‌رسند. تا حدودی می‌توان این را به ماهیت این بنچمارک‌ها نسبت داد که بر روی داده‌های ورودی معمولی اعمال می‌شوند. بنابراین، نوعی تبدیل از سیگنال‌های اطلاعاتی به قطارهای سنبله مورد نیاز است که معمولاً دارای تلفات و ناکارآمدی است. عامل محدودکننده دیگر فقدان الگوریتم‌های آموزشی است که از قابلیت‌های نورون‌های اسپایکی، به عنوان مثال، کدهای زمانی کارآمد استفاده می‌کنند. در بحث آموزش شبکه‌های عصبی اسپایکینگ، بیشتر رویکردها از تقریب‌های مبتنی بر نرخ شبکه عصبی عمیق معمولی استفاده می‌کنند، که به این معنی است که هیچ افزایش دقتی در این روش‌های آموزش نسبت به شبکه عصبی عمیق، قابل انتظار نیست. شبکه‌های عصبی اسپایکینگ عمیق ممکن است در چنین سناریوهایی مفید باشند، زیرا نتایج تقریبی ممکن است سریعتر و کارآمدتر از سیستم های معمولی به دست آید، به خصوص اگر شبکه‌های عصبی اسپایکینگ بر روی سخت افزار نورومورفیک اجرا شود. اما به‌عنوان یک روش آموزش مستقل و مجزا قابل تعمیم نمی‌باشد. از سوی دیگر، طراحی و تجزیه و تحلیل الگوریتم‌های آموزشی برای شبکه‌های عصبی اسپایکینگ نیز دشوارتر است، زیرا روش محاسباتی ناهمزمان و ناپیوسته است، که استفاده مستقیم از تکنیک‌های پس‌انتشار موفقیت‌آمیز را که برای شبکه عصبی عمیق استفاده می‌شود، دشوار می‌کند.

۳- روش پیشنهادی

با توجه به مساله آموزش شبکه‌های عصبی اسپایکینگ منطبق با داده‌های سیستماتیک ارائه یک رویکرد بهینه‌سازی با کمک الگوریتم‌های بهینه‌سازی راهکار اصلی برای تطبیق سیستم‌های آموزش یافته با مقادیر مورد پیش بینی می‌باشد. بنابراین در این مقاله از یک معیار خطای موثر برای محاسبه تابع هدف استفاده شده است. در شکل (۱) نمای کلی طرح پیشنهادی معرفی شده است. هدف این بخش ارائه یک رویکرد آموزشی برای شبکه‌های عصبی اسپایکینگ عمیق می‌باشد. بنابراین ابتدا داده‌های آموزش برای سیستم مورد نظر را آماده‌سازی می‌کنیم. در این مرحله با کمک یک الگوریتم ژنتیک مجموعه داده‌ها یا ویژگی‌هایی که نزدیکترین انطباق با خروجی‌های سیستم را دارند برای آموزش شبکه شبکه‌های عصبی اسپایکینگ در بازه [0,1] انتخاب و نرمالسازی می‌شوند. سایر ویژگی‌های ورودی هم از مجموعه آموزش حذف می‌شوند. بعد از آماده‌سازی داده‌های آموزش برای شبکه‌های عصبی اسپایکینگ و تعریف ساختار شبکه برای تعداد لایه‌ها و نرون‌های هر لایه به تعیین پارامترهای یادگیری شبکه عصبی اسپایکینگ عمیق توسط الگوریتم‌ها می‌رسیم که در ادامه اشاره می‌شود.

۳-۱- مدل یادگیری پیشنهادی

در این روش با تعیین تعداد لایه‌های شبکه‌های عصبی اسپایکینگ عمیق و تعداد نرون‌های هر لایه به یک تعریف کلی از شبکه دست می‌یابیم که برای انطباق نتایج سیستم مورد نظر جهت تخمین خروجی سیستم از الگوریتم‌های بهینه‌سازی پیشنهاد شده در این مقاله (الگوریتم بهینه‌ساز اسب وحشی و الگوریتم مبتنی بر گرادیان) بهره خواهیم برد.



شکل (۱): نمای کلی روش پیشنهادی برای آموزش شبکه‌های عصبی اسپایکینگ.

برای انطباق نتایج شبیه‌سازی می‌بایست شبکه ایجاد شده را برای تک تک داده‌های تست محاسبه کرده و برای خروجی‌های معادل انها خطا یا انحراف موثر را محاسبه کنیم. در مرحله بعد تابع هدف از تجمیع تمام خطاها بر اساس رابطه زیر تعیین می‌شود. نکته مهم برای محاسبه و ارزش‌گذاری خروجی شبکه در این کار محاسبه مقدار جذر میانگین مربعات قطار اسپایک در خروجی نرون خروجی می‌باشد که برای محدوده ۰ تا ۰/۲۱ محاسبه می‌شود. برای تغییر محدوده عملیاتی شبکه‌های عصبی اسپایکینگ از تغییر محدوده زمانی محاسباتی یا فرکانس عملیاتی اسپایک های ورودی می‌توان بهره برد. در این کار ما فرکانس عملیاتی برای تعریف اسپایک‌های ورودی برابر ۱۰ کیلوهرتز در نظر گرفته‌ایم. این فرکانس انتخابی برای سخت‌افزارهای مختلف با توجه تکنولوژی مورد استفاده قابل تغییر است. محدوده زمانی محاسبه برای انجام عملیات پاسخ‌دهی شبکه برابر ۰/۵ ثانیه محاسبه شده است.

۳-۲- استخراج خروجی داده‌های آزمایشی از شبکه عصبی اسپایکینگ آموزش دیده

در این بخش بعد از آموزش شبکه با تکنیک پیشنهادی نوبت به بررسی نتایج عملکرد سیستم برای داده‌های آزمایشی می‌شودکه به اثبات نتایج برای تکنیک پیشنهادی می‌پردازد. در بحث یادگیری عمیق داده‌های ورودی و خروجی به دو گروه داده‌های اموزشی و داده‌های آزمایشی تقسیم می‌شوند. در این بخش تابع هدف با توجه به پاسخ‌های سیستم اسپایکینگ به ازای تک‌تک داده‌های آموزش بررسی و خروجی آنها با مقدار واقعی مقایسه می‌شود. خروجی تابع هدف با مقدار مجموع انحراف پاسخ‌های داده‌های آموزش به توان دوم و طبق رابطه تابع نمایی زیر تعریف می‌شوند. این مقادیر برای مجموعه داده‌های آموزش محاسبه و پارامترهای هدف به عنوان پاسخ‌های بهینه نهایی الگوریتم‌های بهینه‌سازی محاسبه میشود.

$$F(x) = (\exp(\mu * \sum error(i)2) - 1)$$
$$for \;\; i = 1, \ldots\ldots, number\ of\ training\ set$$

که برای سیستم‌های مختلف مقدار μ متغیر و مثبت است.

۴- نتایج و بحث

در این مقاله دو مساله یادگیری ماشین شامل مجموعه داده‌های IRIS در کتابخانه نرم افزار متلب و همچنین پردازش سیگنال صوتی برای تشخیص ارقام ۰-۹ از مجموعه داده های ۲۰۰ نمونه صوت از افراد مختلف TIDIGITS برای [۳۰] ارائه شده است. نمونه‌ها از مجموعه‌های مختلف زن و مرد استفاده شده است. هدف از این کار، یافتن نقطه شروع و پایان هر رقم گفتاری در ضبط رشته‌های رقم‌های ۰ تا ۹ و ساختن سیستمی برای تشخیص این رقم‌های گفتاری است. بر اساس شناخت این سخنان گفتار، می‌توان کاربرد تلفن صوتی را پیاده‌سازی نمود. همچنین از روش‌های پردازش سیگنال دیجیتال برای استخراج ویژگی‌های سیگنال و ایجاد یک سیستم تشخیص وابسته به بلندگو استفاده می‌گردد.

۴-۱- استخراج ویژگی‌ها

در کارهای مختلف [۵و۹] عمدتاً از ضرایب کپسترال فرکانسی مل [1] برای تمایز ارقام مختلف گفتاری استفاده شده است. کپسترال فرکانسی مل طیف قدرت کوتاه مدت یک گفتار است که بر اساس تبدیل کنوانسیون خطی از یک طیف قدرت ورود به سیستم در مقیاس مل غیرخطی از فرکانس است. ضرایب کپسترال فرکانسی مل ضرایبی هستند که کپسترال فرکانسی مل را تشکیل می دهند [۳۱]. برای ضرایب محاسبه شده از پنجره سیگنال صوت در این کار از یک مدل ویژگی های آماری استفاده شده است که در کنار ویژگی های مختلف ZCR [2] و توان سیگنال‌های صوتی جمعاً ۷۷ ویژگی برای هر سیگنال استخراج می‌شود. به دلیل بالا بودن حجم پردازش محاسباتی در این مطالعه موردی به کمک الگوریتم ژنتیک تنها ۷ ویژگی اصلی شناخته و انتخاب می‌شود. معیار انتخاب ویژگی‌ها هم بر اساس بالاترین تطبیق نتایج برای بسط تیلور چندجمله‌ای مرتبه ۵ برای تک تک ویژگی‌ها می‌باشد. بنابراین هر ویژگی‌ای که کمترین انحراف از مقدار خروجی داده‌های تست داشتند، به‌عنوان ویژگی برتر انتخاب می‌گردد.

برای سیستم دیتابیس IRIS برای آموزش از کل مجموعه ورودی‌های که شامل ۴ ویژگی است استفاده شده است. در این مقاله از دو مجموعه داده استفاده کرده‌ایم تا عملکرد طرح پیشنهادی خود را برای نمونه‌های مختلف بررسی و تحلیل گردد. در زمینه داده های IRIS که از دیتابیس کتابخانه متلب استفاده شده است، سه روش یادگیری ماشین اعمال شده که شامل روش شبکه‌های عصبی پیشخور و شبکه فازی عصبی تطبیقی [3] و روش پیشنهادی شبکه‌های عصبی اسپایکینگ با دو رویکرد الگوریتم بهینه‌ساز اسب وحشی و الگوریتم مبتنی بر گرادیان آورده شده است. برای این مطالعه موردی شبکه تعریف شده یک شبکه سه لایه با تعداد نرون‌های [5 3 1] برای تمام شبکه‌های یادگیری ماشین استفاده شده است. جدول (۱) نتایج مقایسه را برای دو مطالعه مورد نظر نشان می‌دهد. همانطور که نشان داده شده است شبکه عصبی اسپایکینگ با الگوریتم مبتنی بر گرادیان [4] توانسته بالاترین دقت را در مقایسه سایر روش‌های یادگیری ماشین ایجاد کند.

در این میان روش شبکه عصبی اسپایکینگ با الگوریتم بهینه‌ساز اسب وحشی [5] توانسته است بالاترین دقت را ایجاد کند. در نتایج محدوده برچسب گذاری برای شبکه شبکه‌های عصبی اسپایکینگ مطابق با محدوده ۱ تا ۱۱ برای مشخصه اعداد به ترتیب۱ تا ۹ و O و صفر برچسب گذاری شده است که به محدوده عملیاتی شبکه در بازه [0 0.2] نرمالسازی شده است.

[1] Mel-frequency cepstral coefficients (MFCC)
[2] zero-crossing rate (ZCR)
[3] adaptive network-based fuzzy inference system (ANFIS)
[4] SNN-GBO
[5] SNN-WHO

جدول ۱- مقایسه نتایج دقت روش‌های مختلف یادگیری ماشین.

ML methods (%)	ANFIS	ANN	SNN-GBO	SNN-WHO
Digit recognize	81.2	84.38	88.3	**92.3**
IRIS	95.85	96.27	97.13	**95.47**

۵- نتیجه‌گیری

تقاضاهای رو به رشد سریع خدمات تشخیص گفتار نگرانی‌هایی را در مورد کارایی محاسباتی، عملکرد بلادرنگ، و امنیت داده‌ها و غیره ایجاد کرده است. همانطور که از محاسبات مبتنی بر رویداد که در سیستم‌های عصبی بیولوژیکی مشاهده می‌شود، این مقاله با استفاده از شبکه‌های عصبی اسپایکی الهام‌گرفته از مغز و الگوریتم‌ها بهنیه‌سازی الهام گرفته از طبیعت برای وظایف مختلف در حوزه شناسایی ارقام از سیگنال‌های صوتی و سایر موارد بررسی کرده است. برای این منظور، ما یک چارچوب جدید سیستم یادگیری ماشین مبتنی بر شبکه‌های عصبی اسپایکینگ با الگوریتم بهینه‌ساز اسب وحشی و الگوریتم مبتنی بر گرادیان را پیشنهاد کردیم، که در آن شبکه‌های عصبی اسپایکینگ برای طبقه بندی سیگنال‌های صوتی و دیتابیس ISIR استفاده می‌شود و ویژگی‌های مختلف را در مجموعه‌ای از واحدهای صوتی استخراج می‌کند. این خروجی‌ها از استخراج ویژگی‌های مختلف، اطلاعات سطح رقم برچسب گذاری شده را از مدل زبان مربوطه با الگوریتم ژنتیک انتخاب می‌کنند تا نزدیکترین ویژگی‌های مربوط به سیگنال گفتار ورودی را پیدا کنند. در مجموعه دیگر که از دیتابیس ISIR کتابخانه متلب استفاده شده است، سیستم یادگیری ماشین پیشنهادی را مدل کرده و برای اعتبارسنجی طرح پیشنهادی در کنار سایر روشهای یادگیری ماشین استفاده می شود.

نتایج اولیه نشان داده است که عملکرد تشخیص شبکه‌های عصبی اسپایکینگ یا قابل مقایسه یا کمی بدتر از شبکه‌های عصبی با همان معماری شبکه است. یک دلیل احتمالی برای این کاهش عملکرد، کاهش قدرت نمایش بازنمایی عصبی گسسته (یعنی تعداد سنبله) در مقایسه با نمایش ممیز شناور پیوسته شبکه‌های عصبی مصنوعی [۳۲] است. این شکاف عملکرد به طور بالقوه می‌تواند با گسترش پنجره کدگذاری شبکه‌های عصبی اسپایکینگ بستگی داشته باشد. علاوه بر این، عملکرد شناسایی مدل‌های شبکه فازی عصبی تطبیقی و شبکه‌های عصبی و شبکه‌های عصبی اسپایکینگ در سناریویی با منابع کم نیز بررسی می‌شود. در این سناریو، مدل‌های صوتی شبکه‌های عصبی اسپایکینگ از شبکه‌های عصبی مصنوعی معمولی که می‌تواند به آموزش پر نویز چارچوب یادگیری پشت سر هم نسبت داده شود، بهتر عمل کند. طرح رمزگذاری عصبی اتخاذ شده در این کار به ویژگی‌های ورودی اجازه می‌دهد تا در یک پنجره زمانی رمزگذاری کوتاه برای پردازش سریع توسط شبکه‌های عصبی اسپایکینگ ها کدگذاری شوند. برای کارهای کلاسه‌بندی سیگنال گفتار، همگام زمانی که نیاز به عملکرد زمان واقعی دارند جذاب است. شبکه‌های عصبی مکرر با کاوش اطلاعات بافت زمانی طولانی در سیگنال‌های ورودی، قابلیت مدل‌سازی بسیار خوبی برای سیگنال‌های زمانی نشان داده‌اند [۳۳]. به عنوان کار آینده، ما شبکه‌های مکرر نورون‌های اسپایکینگ را برای کاربرد تشخیص گفتار برای کلاسه‌بندی ارقام را بررسی خواهیم کرد تا عملکرد تشخیص را بهبود ببخشیم.

مراجع

[1] J. L. Lobo, J. Del Ser, A. Bifet, and N. Kasabov, "Spiking Neural Networks and online learning: An overview and perspectives," *Neural Networks*, vol. 121, pp. 88–100, Jan. 2020, doi: https://doi.org/10.1016/j.neunet.2019.09.004.

[2] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," *Nature*, vol. 323, no. 6088, pp. 533–536, Oct. 1986, doi: https://doi.org/10.1038/323533a0.

[3]Stork, "Is backpropagation biologically plausible?," *International Joint Conference on Neural Networks*, 1989, doi: https://doi.org/10.1109/ijcnn.1989.118705.

[4] J. Wu, C. Xu, D. Zhou, H. Li, and K. C. Tan, "Progressive Tandem Learning for Pattern Recognition with Deep Spiking Neural Networks," *arXiv.org*, 2020. https://arxiv.org/abs/2007.01204

[5]J. Wu, E. Yilmaz, M. Zhang, H. Li, and K. C. Tan, "Deep Spiking Neural Networks for Large Vocabulary Automatic Speech Recognition," *arXiv.org*, 2019. https://arxiv.org/abs/1911.08373

[6] G. Eappen, S. T, and R. Nilavalan, "Cooperative relay spectrum sensing for cognitive radio network: Mutated MWOA-SNN approach," *Applied Soft Computing*, vol. 114, p. 108072, Jan. 2022, doi: https://doi.org/10.1016/j.asoc.2021.108072.

[7] J. Fitzgerald and KongFatt Wong-Lin, "Multi-Objective Optimisation of Cortical Spiking Neural Networks With Genetic Algorithms," *Ulster University Research Portal (Ulster University)*, vol. 71, pp. 1–6, Jun. 2021, doi: https://doi.org/10.1109/issc52156.2021.9467860.

[8] Yeshwanth Bethi, Y. Xu, G. Cohen, A. V. Schaik, and S. Afshar, "An Optimized Deep Spiking Neural Network Architecture Without Gradients," *IEEE Access*, vol. 10, pp. 97912–97929, Jan. 2022, doi: https://doi.org/10.1109/access.2022.3200699.

[10]A. Pitti, Mathias Quoy, C. Lavandier, and Sofiane Boucenna, "Gated spiking neural network using Iterative Free-Energy Optimization and rank-order coding for structure learning in memory sequences (INFERNO GATE)," *Neural Networks*, vol. 121, pp. 242–258, Jan. 2020, doi: https://doi.org/10.1016/j.neunet.2019.09.023.

[11]Y. Kim and P. Panda, "Optimizing Deeper Spiking Neural Networks for Dynamic Vision Sensing," *Neural Networks*, vol. 144, pp. 686–698, Dec. 2021, doi: https://doi.org/10.1016/j.neunet.2021.09.022.

[12]A. Woodward, T. Froese, and T. Ikegami, "Neural coordination can be enhanced by occasional interruption of normal firing patterns: A self-optimizing spiking neural network model," *Neural Networks*, vol. 62, pp. 39–46, Feb. 2015, doi: https://doi.org/10.1016/j.neunet.2014.08.011.

[13]W. S. McCulloch and W. Pitts, "A logical calculus of the ideas immanent in nervous activity," *The Bulletin of Mathematical Biophysics*, vol. 5, no. 4, pp. 115–133, Dec. 1943, doi: https://doi.org/10.1007/bf02478259.

[14]"APA PsycNet," *psycnet.apa.org*. https://psycnet.apa.org/record/1959-09865-001

[15]K. S. Sayarkin, A. V. Popov, and A. A. Zhilenkov, "Spiking neural network model MATLAB implementation based on

Izhikevich mathematical model for control systems," vol. 8, pp. 979–982, Jan. 2018, doi: https://doi.org/10.1109/eiconrus.2018.8317253.
[16]"Dynamical Systems in Neuroscience: The Geometry of Excitability and Bursting (Computational Neuroscience) by Izhikevich, Eugene M. (2010) Paperback (Computational Neuroscience Series): Izhikevich, Eugene M. M: 9780262514200: Amazon.com: Books," *Amazon.com*, 2024. https://www.amazon.com/Dynamical-Systems-Neuroscience-Excitability-Computational/dp/0262514206 (accessed Nov. 08, 2024).
[17] www.izhikevich.com.
[18] J. Vreeken, "Spiking neural networks, an introduction." Accessed: Nov. 08, 2024. [Online]. Available: https://webdoc.sub.gwdg.de/ebook/serien/ah/UU-CS/2003-008.pdf
[19] H. Paugam-Moisy and S. Bohte, "Computing with Spiking Neuron Networks," *Handbook of Natural Computing*, pp. 335–376, 2012, doi: https://doi.org/10.1007/978-3-540-92910-9_10.
[20] I. Naruei and F. Keynia, "Wild horse optimizer: a new meta-heuristic algorithm for solving engineering optimization problems," *Engineering with Computers*, Jun. 2021, doi: https://doi.org/10.1007/s00366-021-01438-z.
[21]I. Ahmadianfar, O. Bozorg-Haddad, and X. Chu, "Gradient-based optimizer: A new metaheuristic optimization algorithm," *Information Sciences*, vol. 540, pp. 131–159, Nov. 2020, doi: https://doi.org/10.1016/j.ins.2020.06.037.
[22] H. Mostafa, "Supervised learning based on temporal coding in spiking neural networks," *arXiv.org*, 2016. https://arxiv.org/abs/1606.08165 (accessed Nov. 08, 2024).
[23] B. Rueckauer, I.-A. Lungu, Y. Hu, M. Pfeiffer, and S.-C. Liu, "Conversion of Continuous-Valued Deep Networks to Efficient Event-Driven Networks for Image Classification," *Frontiers in Neuroscience*, vol. 11, Dec. 2017, doi: https://doi.org/10.3389/fnins.2017.00682.
[24] A. Sengupta, Y. Ye, R. Wang, C. Liu, and K. Roy, "Going Deeper in Spiking Neural Networks: VGG and Residual Architectures," *arXiv.org*, 2018. https://arxiv.org/abs/1802.02627 (accessed Nov. 08, 2024).
[25]"Gradient-based learning applied to document recognition - IEEE Journals & Magazine," *Ieee.org*, 2019. https://ieeexplore.ieee.org/document/726791
[26] A. Krizhevsky, "Learning Multiple Layers of Features from Tiny Images," Apr. 2009. Available: https://www.cs.toronto.edu/~kriz/learning-features-2009-TR.pdf
[27] O. Russakovsky *et al.*, "ImageNet Large Scale Visual Recognition Challenge," *arXiv.org*, 2014. https://arxiv.org/abs/1409.0575
[28] A. Tavanaei, M. Ghodrati, S. R. Kheradpisheh, T. Masquelier, and A. Maida, "Deep learning in spiking neural networks," *Neural Networks*, vol. 111, pp. 47–63, Mar. 2019, doi: https://doi.org/10.1016/j.neunet.2018.12.002.
[29] "Spiking Neural Networks: Learning, Applications, and Analysis: 9783845405155: Computer Science Books @ Amazon.com," *Amazon.com*, 2024. https://www.amazon.com/Spiking-Neural-Networks-Learning-Applications/dp/3845405155 (accessed Nov. 08, 2024).
[30] D. Ellis. Clean Digits and Digit Strings (Sound Examples), http://www.ee.columbia.edu/~dpwe/sounds/tidigits/
[31] M. Xu, L.-Y. Duan, J. Cai, L.-T. Chia, C. Xu, and Q. Tian, "HMM-Based Audio Keyword Generation," *Advances in Multimedia Information Processing - PCM 2004*, pp. 566–574, 2004, doi: https://doi.org/10.1007/978-3-540-30543-9_71.
[32] M. Xu, L.-Y. Duan, J. Cai, L.-T. Chia, C. Xu, and Q. Tian, "HMM-Based Audio Keyword Generation," *Advances in Multimedia Information Processing - PCM 2004*, pp. 566–574, 2004, doi: https://doi.org/10.1007/978-3-540-30543-9_71.
[33] A. Graves and N. Jaitly, "Towards End-To-End Speech Recognition with Recurrent Neural Networks," *proceedings.mlr.press*, Jun. 18, 2014. https://proceedings.mlr.press/v32/graves14.html

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

Temperature Modulation of a Tin Oxide-Based Gas Sensor for Detecting Vinegar Purity using the K-Nearest Neighbors Algorithm

Ali Fatehifar[1], Fatemeh Safari[2], Vahid Khorramshahi[*3]

[1]Materials and Energy Research Center, Dezful Branch, Islamic Azad University, Dezful, Iran
ali.fatehifar@gmail.com
[2]Materials and Energy Research Center, Dezful Branch, Islamic Azad University, Dezful, Iran
Fatemeh.Safari@iau.ac.ir
[3]Materials and Energy Research Center, Dezful Branch, Islamic Azad University, Dezful, Iran
va.khoramshahi@iau.ac.ir

Abstract: Temperature modulation in gas sensors based on metal oxides, such as SnO_2, alters the operating temperature of the sensor. These changes enhance the sensor's sensitivity and selectivity in detecting acetic acid in vinegar, enabling the determination of vinegar purity. In temperature modulation for gas sensors, temperature cycles are employed to record the sensor's response to different compounds. These responses are then processed as classification features to differentiate and identify various compounds. In this study, the nearest neighbor (k-NN) algorithm was used to classify vinegar samples and assess their purity based on these features. A square voltage waveform was applied to the microheater of the MQ2 gas sensor, inducing temperature variations that generated distinct patterns in the sensor's response. The sensor's voltage response to vinegar vapors with varying purities was recorded in three stages. From each pattern, seven unique features were extracted to serve as inputs for the classification algorithm. The proposed algorithm demonstrated an accuracy of 86% in determining vinegar purity, making it suitable for use in automated detection systems.

Keyword: Tin oxide, temperature modulation, electronic nose, gas sensor, classification.

JCDSA, Vol. 2, No. 3, Autumn 2024	Online ISSN: 2981-1295	Journal Homepage: https://sanad.iau.ir/en/Journal/jcdsa
Received: 2024-08-03	Accepted: 2024-10-30	Published: 2024-12-20

CITATION

Fatehifar, A., et. al.," *Temperature modulation of a tin oxide-based gas sensor for detecting vinegar purity using the k-Nearest Neighbors algorithm*", Journal of Circuits, Data and Systems Analysis (JCDSA), Vol. 2, No. 3, pp. 53-62, 2024.
DOI: 00.00000/0000

* Corresponding author

Extended Abstract

1- Introduction

An alternative to traditional chemical analysis for quality control of vinegar and its component analysis is the use of electronic noses. Electronic noses typically employ an array of multiple sensors coupled with machine learning algorithms to classify various gases. Machine learning classification algorithms can be broadly categorized into linear and nonlinear methods. Prominent linear algorithms include Principal Component Analysis (PCA) classifiers and k-Nearest Neighbors (k-NN).

Various sensor types are employed in electronic noses, including metal oxide, polymer, and micro-electrochemical sensors. Among these, metal oxide semiconductor sensors are particularly favored due to their high sensitivity to organic vapors, stable drift behavior, long operational lifespan, and cost-effectiveness. Tin oxide (SnO_2), in particular, is one of the most widely used metal oxide sensors for detecting diverse gases, including those relevant to electronic nose applications.

Metal oxide gas sensors operate based on resistive changes induced upon exposure to a gas, resulting in corresponding voltage variations, which are regarded as the sensor's response to the target gas. Furthermore, applying variable temperatures to the sensor generates distinctive response patterns, rich in information about the target gas. By extracting features from these patterns, it becomes possible to detect and classify gases more effectively, thereby enhancing the selectivity of temperature-modulated sensors.

The unique properties of metal oxide sensors, combined with advanced data analysis techniques, position them as suitable candidates for robust and efficient electronic nose systems, particularly for applications such as vinegar quality analysis.

2- Methodology

In this study, a square wave with an 8-volt amplitude and a frequency of 100 mHz was applied to control the heating of an MQ2 gas sensor, which operates based on the semiconductor metal oxide SnO_2. This temperature modulation allowed the sensor's operating temperature to oscillate between 200°C and 320°C, producing distinct response patterns under varying thermal conditions. When exposed to vinegar vapors with varying purity levels (20%, 40%, 60%, 80%, and 100%), these temperature-induced response patterns were reflected as unique voltage variations across the sensor.

To extract meaningful information from these patterns, seven distinct features were derived from each of the three response phases—rise, steady, and fall—observed during the sensor's interaction with vinegar vapors. These features were subsequently analyzed using the k-Nearest Neighbors (k-NN) algorithm for classification. To ensure a robust evaluation of the classifier's performance, k-fold cross-validation was employed, providing a reliable framework for assessing the model's accuracy.

3- Results and discussion

Controlled temperature variations enhance the sensor's sensitivity and selectivity, enabling precise detection of different purity levels in vinegar samples. These temperature-induced responses yield distinct and reliable signal profiles for various impurities. The proposed algorithm, with an accuracy of 86% in identifying vinegar purity, demonstrates strong potential for integration into automated detection systems. This approach offers a cost-effective and efficient solution for quality control in the food and beverage industry.

4- Conclusion

In this study, a vinegar purity detection system was developed using the cost-effective and readily available MQ2 sensor, which employs tin oxide (SnO_2) for gas detection. Although traditionally used for detecting flammable gases, the MQ2 sensor was repurposed in this research to assess vinegar purity levels. By applying the k-nearest neighbors (k-NN) algorithm, the system achieved a satisfactory classification accuracy, effectively distinguishing between various purity levels based on the sensor's response. The integration of the MQ2 sensor with the k-NN algorithm offers a practical, low-cost solution for real-time quality assessment, making it particularly suitable for resource-limited settings and small-scale quality control applications.

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

مدولاسیون دمایی حسگر گاز مبتنی بر اکسید قلع جهت تشخیص خلوص سرکه با استفاده از الگوریتم k نزدیکترین همسایگی

علی فاتحی فر[۱]، فاطمه صفری[۲]، وحید خرمشاهی[*۳]

۱- مرکز تحقیقات مواد و انرژی، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران (ali.fatehifar@gmail.com)
۲- مرکز تحقیقات مواد و انرژی، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران (Fatemeh.Safari@iau.ac.ir)
۳- مرکز تحقیقات مواد و انرژی، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران (va.khoramshahi@iau.ac.ir)

چکیده: مدولاسیون دما در حسگرهای گاز مبتنی بر اکسیدهای فلزی، از جمله SnO_2، موجب تغییر دمای عملیاتی حسگر می‌شود. این تغییرات، حساسیت و گزینش‌پذیری حسگر را در تشخیص اسید استیک موجود در سرکه افزایش داده و امکان تعیین خلوص سرکه را فراهم می‌کنند. در مدولاسیون دمایی حسگرهای گاز، از چرخه‌های دمایی برای ثبت پاسخ حسگر به ترکیبات مختلف استفاده می‌شود. این پاسخ‌ها به‌عنوان ویژگی‌های طبقه‌بندی استخراج شده و امکان تمایز و شناسایی ترکیبات را فراهم می‌کنند. در این پژوهش، با استفاده از الگوریتم نزدیک‌ترین همسایه، ویژگی‌های استخراج‌شده به‌طور مؤثری برای طبقه‌بندی نمونه‌های سرکه و تعیین خلوص آن‌ها به کار گرفته شد. به ریزگرمکن حسگر گاز MQ2 یک ولتاژ مربعی اعمال شد که موجب تغییر دمای حسگر و ایجاد الگوهای متمایز در پاسخ آن گردید. پاسخ ولتاژ حسگر به بخارات سرکه با خلوص‌های مختلف در سه مرحله ثبت شد. از هر الگوی ایجادشده در پاسخ حسگر، هفت ویژگی متمایز انتخاب شد که به‌عنوان ورودی‌های الگوریتم طبقه‌بندی مورد استفاده قرار گرفتند. دقت الگوریتم پیشنهادی در تشخیص خلوص سرکه برابر با ۸۶ درصد بوده و این روش قابلیت استفاده در سیستم‌های تشخیص خودکار را دارد.

واژه های کلیدی: اکسید قلع، مدولاسیون دما، بینی الکترونیکی، حسگر گاز، طبقه بندی.

نوع مقاله: پژوهشی
تاریخ ارسال مقاله: ۱۴۰۳/۰۵/۱۳ تاریخ پذیرش مقاله: ۱۴۰۳/۰۸/۰۹ تاریخ چاپ مقاله: ۱۴۰۳/۰۹/۳۰
DOI: 00.00000/0000

۱- مقدمه

سرکه، که اغلب به عنوان یک چاشنی و نگهدارنده استفاده می‌شود، معمولاً طی یک فرآیند دو مرحله‌ای از مواد حاوی قند مانند سیب، انگور، جو، برنج و خرما تولید می‌شود. در ایران، سرکه قرمز و سرکه سفید انگور از پرمصرف‌ترین انواع سرکه محسوب می‌شوند. متأسفانه، برخی سودجویان با به خطر انداختن سلامت مردم، محصولات تقلبی تولید کرده و وارد بازار می‌کنند. به همین دلیل، از گذشته تاکنون روش‌های متعدد تحلیل شیمیایی برای کنترل کیفیت سرکه و بررسی ترکیبات آن توسعه داده شده‌اند، از جمله الکترودهای انتخاب‌گر یونی [۱]، طیف‌سنجی جذب اتمی [۲]، کروماتوگرافی گازی [۳] و طیف‌سنجی جرمی پیرولیز [۴]. با این حال، از آنجا که سرکه بیش از ۱۰۰ ترکیب مختلف دارد، استفاده از این روش‌های تحلیل شیمیایی برای بررسی کیفیت آن، فرآیندی پیچیده و پرهزینه است و برای کاربردهای زمان-حقیقی نیز مناسب نیستند. بنابراین توسعه روش‌های جایگزین که بتوانند با دقت بالا کیفیت سرکه را مشخص کرد اهمیت بسزایی دارد.

یکی از روش‌های جایگزین روش‌های تحلیلی شیمیایی، استفاده از بینی الکترونیکی است. تاکنون بینی‌های الکترونیکی برای ارزیابی کیفیت بسیاری از مواد خوراکی، از جمله قهوه، شیر، روغن و سرکه، مورد استفاده قرار گرفته‌اند [۵-۱۰]. معمولاً بینی‌های الکترونیکی از آرایه‌ای متشکل از چندین حسگر استفاده می‌کنند که با کمک الگوریتم‌های یادگیری ماشین قادر به طبقه‌بندی گازهای مختلف هستند. الگوریتم‌های دسته‌بندی یادگیری ماشین به دو دسته خطی و غیرخطی تقسیم می‌شوند. از میان الگوریتم‌های خطی می‌توان به مدل‌های طبقه‌بندی‌کننده بیزی، تحلیل موئلفه‌های اصلی[۲] و الگوریتم نزدیک‌ترین همسایه[۳] اشاره کرد. در مقابل، الگوریتم‌های غیرخطی شامل ماشین

[*] نویسنده مسئول

[2] Principal component analysis (PCA)
[3] k-nearest neighbors algorithm (k-NN)

بردار پشتیبان[1]، جنگل تصادفی[2] و شبکه‌های عمیق هستند [۱۱]. در این مقاله، به دلیل پایداری بالا، پیاده‌سازی آسان، و دقت مناسب، از الگوریتم نزدیک‌ترین همسایه برای دسته‌بندی داده‌ها استفاده شده است.

در بینی‌های الکترونیکی از حسگرهای متنوعی بهره گرفته می‌شود که شامل حسگرهای اکسیدهای فلزی، پلیمری، میکروالکتروشیمیایی، و کوارتز است [۱۲، ۱۵]. در میان این حسگرها، حسگرهای نیمه‌هادی مبتنی بر اکسیدهای فلزی به دلیل حساسیت بالا به بخارات آلی، تعادل مناسب میان رانش، عمر طولانی، و قیمت اقتصادی، بیشترین کاربرد را در بینی‌های الکترونیکی دارند[۶، ۲۱]. از میان اکسیدهای فلزی، اکسید قلع (SnO_2) یکی از پرکاربردترین مواد برای تشخیص انواع گازها محسوب می‌شود و در بینی‌های الکترونیکی نیز به‌کار گرفته شده است [۲۲، ۲۴]. این ماده نیمه‌هادی نوع n با شکاف نواری عریض ۳.۶ الکترون‌ولت، علاوه بر کاربرد در حسگرهای گاز، در تجهیزات الکترونیکی دیگری نظیر حسگرهای زیستی، سلول‌های خورشیدی، و ابزارهای الکترونیک نوری نیز استفاده می‌شود [۲۵، ۲۷]. حسگرهای گاز مبتنی بر اکسیدهای فلزی، زمانی که در معرض گاز قرار می‌گیرند، دچار تغییرات مقاومتی می‌شوند. این تغییرات که معادل تغییرات ولتاژ حسگر است، به عنوان پاسخ حسگر به گاز هدف در نظر گرفته می‌شود. این حسگرها معمولاً دارای یک ریزگرمکن حرارتی هستند که دمای کافی برای فعال‌سازی آن‌ها را فراهم می‌آورد. سطح پاسخ و حساسیت این حسگرها به شدت به دما وابسته است، به‌گونه‌ای که تغییرات جزئی در دمای کاری می‌تواند منجر به نوسانات قابل توجهی در پاسخ آن‌ها شود. وابستگی پاسخ به دما، به واکنش‌های شیمیایی و الکترونیکی اجتناب‌ناپذیری که در سطح مؤثر حسگر رخ می‌دهد، مرتبط است. شدت این واکنش‌ها بسته به نوع گاز متفاوت بوده و هر حسگر به یک یا چند نوع گاز حساسیت بیشتری نسبت به دیگر گازها دارد [۲۸].

اعمال دمای متغیر به حسگر باعث ایجاد الگوهایی در پاسخ آن می‌شود که اطلاعاتی در خصوص گاز هدف دربردارند [۲۹، ۳۱]. از این اطلاعات می‌توان برای تشخیص و دسته‌بندی گازهای مختلف استفاده کرد [۳۲]. تغییر ولتاژ اعمالی به ریزگرمکن حسگر باعث مدوله شدن دمای کاری آن می‌شود. به عبارت دیگر، هر تغییر در سطح ولتاژ اعمالی به ریزگرمکن باعث تغییر دمای حسگر و در نتیجه تغییر در شکل الگوی پاسخ آن می‌شود. روش معمول کار حسگرهای گاز به این صورت است که حسگر در یک دمای ثابت عمل می‌کند و در صورت مواجهه با گاز، پس از گذشت زمان مشخص، پاسخ ماندگاری ناشی از تغییرات مقاومتی متناسب با غلظت گاز اعمالی ایجاد می‌شود. اما در مدولاسیون دما، زمان فرآیند تشخیص گاز در هر دما محدود است که این امر موجب نوسانات پاسخ زمانی می‌شود. این نوسانات حاوی اطلاعاتی هستند که در حالت دمای ثابت وجود ندارند. در واقع، افزودن ویژگی‌های پاسخ مرتبط با تغییرات دما به همراه اطلاعات پاسخ ماندگار، گزینش‌پذیری حسگر مدوله‌شده با دما را افزایش می‌دهد [۳۲].

برای مدولاسیون دمای حسگر گاز بسته به کاربرد، از اشکال مختلف موج ولتاژی استفاده می‌شود [۳۳-۳۵] که بر اساس آن‌ها می‌توان روش‌های مدولاسیون دمایی را به دو دسته کلی گذار دمایی و روش دوره‌های دمایی تقسیم‌بندی کرد. همچنین، روش‌های ترکیبی نیز وجود دارند که از خواص هر دو روش بهره می‌برند [۳۶]. در روش گذار دمایی، تغییرات ولتاژ اعمالی به ریزگرمکن به صورت پله‌ای یا چند سطحی است که می‌تواند با توابع شیب یا نمایی ترکیب شود. یکی از ساده‌ترین و سریع‌ترین روش‌ها برای مشاهده پاسخ دمایی و وابستگی دمایی حسگرهای اکسید فلزی، استفاده از کلید در منبع تغذیه ریزگرمکن حسگر است که می‌تواند به صورت قطع و وصل عمل کند [۳۷]. میبائو و همکارانش با استفاده از نانوساختارهای SnO_2، توانسته‌اند به کمک مدولاسیون دمایی، ترکیبات آلی فرار مانند الکل‌ها، آلدئیدها، کتون‌ها، آمین‌ها و ترکیبات معطر را شناسایی کنند. آن‌ها با اعمال ولتاژ گرمایش موج مربعی، رفتارهای پاسخ دینامیکی گاز نسبت به ترکیبات آلی فرار را به طور سیستماتیک بررسی کرده‌اند. در این تحقیق، برای تفکیک گازها از الگوریتم تحلیل مولفه‌های اصلی استفاده شده است [۳۳]. در روش مدولاسیون دوره‌های دمایی، ریزگرمکن حسگر به‌صورت متناوب تحت تأثیر مجموعه‌ای از تک‌فرکانس‌های سینوسی قرار می‌گیرد. مقدار این فرکانس‌های موج سینوسی اعمال‌شده براساس مشخصات ابتدایی حسگر و ویژگی‌ها و رفتار گاز هدف تعیین می‌شود. لازم به ذکر است که در این روش، علاوه بر شکل موج سینوسی، از شکل موج‌های دیگری مانند مربعی و پلکانی نیز به‌عنوان ولتاژ اعمالی به ریزگرمکن حسگر استفاده شده است [۳۸-۳۹]. البته باید به این نکته نیز اشاره کرد که شکل موج بهینه برای ریزگرمکن حسگر، بسته به نوع گاز هدف و ویژگی‌های حسگر، منحصر به فرد نیست و ممکن است در هر کاربرد متفاوت باشد [۲۹].

لیدینگر و همکارانش با استفاده از روش مدولاسیون دوره‌های دمایی و تحلیل پاسخ‌های به‌دست‌آمده به‌وسیله الگوریتم تحلیل تشخیص خطی، به شناسایی ترکیبات آلی خطرناکی مانند فرمالدئید و نفتالین پرداخته‌اند. با استفاده از این روش، تیم تحقیقاتی موفق به شناسایی و تفکیک گازهای سمی تا غلظت‌های بسیار پایین در محدوده ppb و کمتر از ppb شده‌اند [۴۰]. به‌طور کلی، قابلیت‌های منحصربه‌فرد حسگری اکسیدهای فلزی، همراه با تکنیک‌های پیشرفته تجزیه و تحلیل داده‌ها، این حسگرها را به گزینه‌های مناسبی برای توسعه سیستم‌های مبتنی بر بینی الکترونیکی قوی و کارآمد برای تحلیل سرکه تبدیل کرده است. در این مقاله نیز با استفاده از یک حسگر مبتنی بر اکسید قلع (SnO_2) و بکارگیری روش مدولاسیون دما و الگوریتم k نزدیک‌ترین همسایگی، کیفیت سرکه تجاری تولیدی یکی از شرکت‌های معتبر داخلی مورد تحلیل قرار گرفته است که دقت تشخیص روش پیشنهادی ۸۶ درصد به‌دست آمده است.

[1] Support vector machines (SVM)

[2] Random Forest

۲- مواد و روش‌ها

۲-۱- مواد

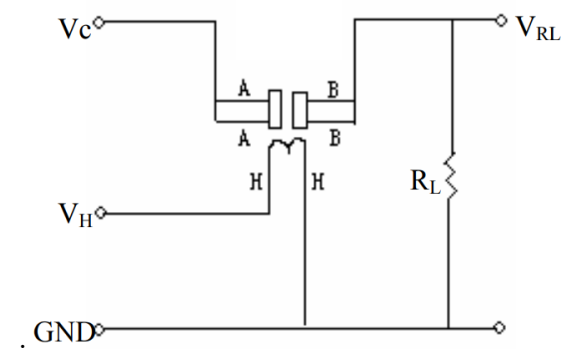
در این تحقیق، محصول سرکه یک شرکت تجاری داخلی معتبر به‌عنوان نمونه خالص فرض می‌شود که از این پس آن را "نمونه ۱۰۰ درصد خالص" نام‌گذاری می‌کنیم. با ترکیب آب با نمونه ۱۰۰ درصد خالص، نمونه‌هایی با خلوص ۲۰، ۴۰، ۶۰ و ۸۰ درصد به‌دست آمد. شایان ذکر است که سرکه خوراکی به‌طور معمول دارای ۵ درصد اسید استیک است و مابقی آن را آب تشکیل می‌دهد. هدف این تحقیق، ارائه روشی کم‌هزینه جهت شناسایی محصولاتی است که کیفیت و خلوص آن‌ها به‌دلیل افزودن بیش از حد آب کاهش یافته است. حسگری که در این مطالعه استفاده شده است از نوع MQ2 می‌باشد. این حسگر یک حسگر گاز همه‌کاره است که قادر به تشخیص طیف وسیعی از گازها از جمله الکل، مونوکسید کربن، هیدروژن، ایزوبوتن، گاز مایع، متان، پروپان و حتی دود است. به‌دلیل هزینه کم، حساسیت بالا و زمان پاسخ سریع، حسگر MQ2 در کاربردهای تشخیص گاز به‌طور گسترده‌ای استفاده می‌شود. این حسگر گاز با ۵ ولت جریان مستقیم کار می‌کند و به‌طور میانگین تقریباً ۸۰۰ میلی‌وات مصرف دارد. ماده حساس این حسگر اکسید قلع است که دارای طول عمر بالا بوده و با یک مدار ساده قابل راه‌اندازی است. از آنجا که حسگر MQ2 یک حسگر فعال شونده با دما است، اگر برای مدت طولانی در انبار بماند، کالیبراسیون آن ممکن است تغییر کند. در صورتی که پس از یک دوره طولانی (یک ماه یا بیشتر) برای اولین بار مورد استفاده قرار گیرد، حسگر باید به‌طور کامل برای مدت ۲۴ تا ۴۸ ساعت گرم شود تا حداکثر دقت حاصل شود. البته اگر حسگر اخیراً استفاده شده باشد، تنها ۵ تا ۱۰ دقیقه زمان لازم است تا به‌طور کامل گرم شود.

۲-۲- سیستم آزمایش حسگر گاز

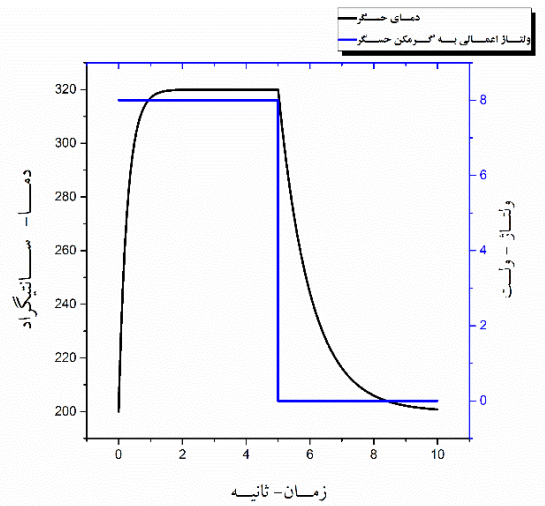
شکل (۱) طرحواره داخلی و مدار راه‌انداز حسگر گاز استفاده‌شده را نشان می‌دهد. دو ولتاژ Vc و VH به‌ترتیب ولتاژ تغذیه و ولتاژ ریزگرمکن حسگر هستند. جهت انجام مدولاسیون دما، VH به یک موج مربعی با فرکانس ۱۰۰ میلی‌هرتز و دامنه ۸ ولت وصل می‌شود. تقسیم ولتاژ نیز از طریق یک مقاومت ۱۰ کیلو اهمی انجام می‌شود. همان‌طور که در شکل (۲) مشخص است، ولتاژ اعمالی به ریزگرمکن باعث می‌شود تا دمای حسگر بین ۲۰۰ تا ۳۲۰ درجه سانتی‌گراد تغییر کند. محفظه آزمایش حسگر گاز استفاده‌شده در این تحقیق، یک ظرف شیشه‌ای ۸/۵ لیتری است که تصویر آن در شکل (۳) نمایش داده شده است. این محفظه شامل ریزگرمکن تبخیر سرکه، دمنده، دریچه خروج گاز، رطوبت‌سنج، دماسنج و نگهدارنده حسگر گاز MQ2 است.

فرآیند کلی آزمایش حسگر گاز به این صورت است که ریزگرمکن حسگر به یک موج مربعی متصل می‌شود تا دمای فعال‌سازی آن فراهم آید. از آنجا که این موج با فرکانس مشخصی در حال نوسان است، باعث می‌شود دمای حسگر در بازه مشخصی نوسان داشته باشد. جهت ثبت ولتاژ از یک مولتی‌متر دیجیتال با قابلیت اتصال به کامپیوتر استفاده شده است که نرخ نمونه‌برداری آن ۵ نمونه در ثانیه است. حسگر با یک مقاومت سری می‌شود که با ثبت مقدار ولتاژ این مقاومت می‌توان ولتاژ حسگر را نیز به‌دست آورد.

در محفظه، یک ریزگرمکن مخصوص بخار کردن نمونه‌های مایع وجود دارد که برای هر آزمایش مقدار ثابتی از هر نمونه روی آن ریخته می‌شود تا تبدیل به بخار شود. بخار ایجاد شده توسط یک دمنده به‌طور یکنواخت در محفظه پخش می‌شود. بعد از اینکه حسگر در معرض بخار سرکه قرار گرفت، به مرور زمان مقاومت آن کاهش پیدا می‌کند تا به مقدار ماندگار خود برسد. به این مرحله، مرحله پاسخ‌دهی می‌گویند. پس از اتمام آزمایش، با باز کردن مسیر خروجی گاز، بخار از محفظه خارج می‌شود. در این مرحله بازیابی حسگر اتفاق می‌افتد، که به این مفهوم است که بعد از گذشت چند دقیقه مقدار مقاومت حسگر افزایش می‌یابد و تقریباً به مقدار قبل از در معرض قرار گرفتن با بخار سرکه برمی‌گردد. در طول انجام کلیه آزمایش‌ها، دمای محیط ۲۰ درجه سانتی‌گراد و رطوبت نسبی هوا ۳۰ درصد بوده است. ولتاژ کاری حسگر و ولتاژ مورد نیاز ریزگرمکن بخارکننده سرکه توسط یک منبع متغیر جریان مستقیم تأمین می‌شود و ولتاژ ریزگرمکن حسگر نیز از طریق یک دستگاه فانکشن ژنراتور تأمین گردیده است.



شکل (۱): طرحواره داخلی و مدار راه انداز حسگر گاز MQ2

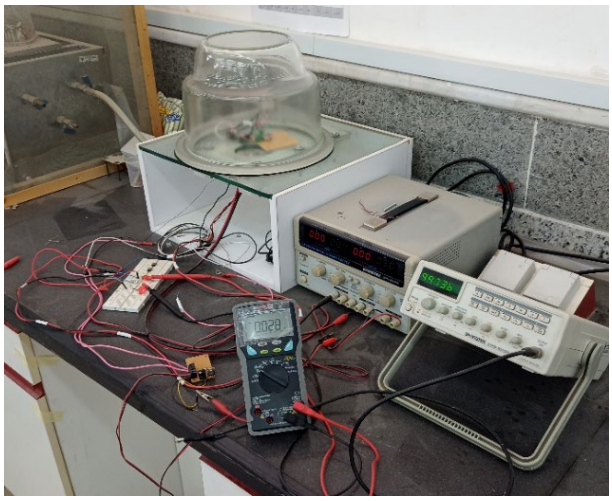


شکل (۲): یک دوره تناوب شکل موج اعمالی به ریزگرمکن حسگر و پروفایل حرارتی ایجاد شده روی سطح حسگر

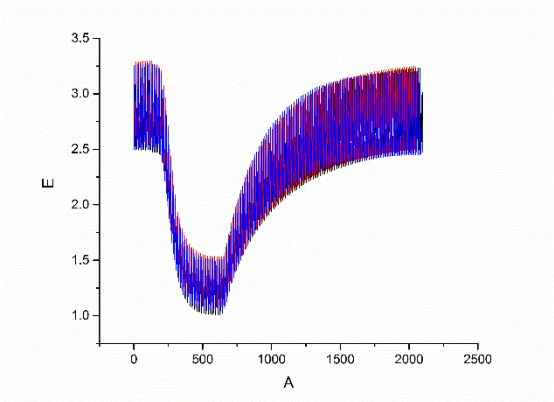
جهت ایجاد تعداد ویژگی کافی برای انجام مرحله دسته‌بندی، فرایند آزمایش تشخیص گاز برای هر غلظت سرکه سه بار تکرار شد. با توجه به اینکه پنج غلظت مختلف سرکه در این تحقیق مورد بررسی قرار گرفته است، در مجموع ۱۵ مرتبه آزمایش تشخیص گاز انجام شده است. شکل‌های (۴-۸) پاسخ ولتاژی حسگر MQ2 استفاده شده به خلوص‌های ۲۰، ۴۰، ۶۰، ۸۰ و ۱۰۰ درصد سرکه را نشان می‌دهند. در هر شکل، پاسخ هر سه بار تکرار آزمایش تشخیص گاز رسم شده‌اند. لازم به ذکر است که این پاسخ‌ها جهت استفاده در الگوریتم دسته‌بندی به صورت نرمال درآمده‌اند.

۲-۳- مکانیزم جذب گاز حسگر مبتنی بر SnO2

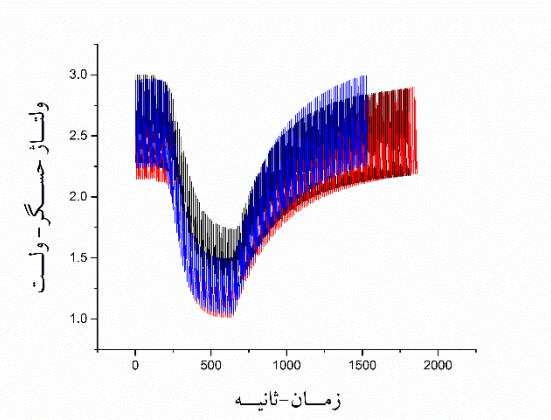
زمانی که حسگر در معرض هوا قرار می‌گیرد، مولکول‌های اکسیژن (O_2) بر روی سطح حسگر اکسید فلزی جذب می‌شوند و گونه‌هایی از اکسیژن جذب شده شیمیایی تشکیل می‌شوند [۴۱]. ایجاد این گونه‌ها به این معنی است که مولکول‌های اکسیژن با سطح حسگر واکنش می‌دهند و الکترون‌ها را از لایه هدایت اکسید قلع به دام می‌اندازند و همانطور که در شکل (۹) نشان داده شده است، باعث ایجاد یک ناحیه تخلیه پیرامون ذرات اکسید فلزی می‌گردند. در این حالت، چگالی الکترون‌ها در سطح کاهش یافته و به تبع آن، مقاومت الکتریکی حسگر افزایش می‌یابد.



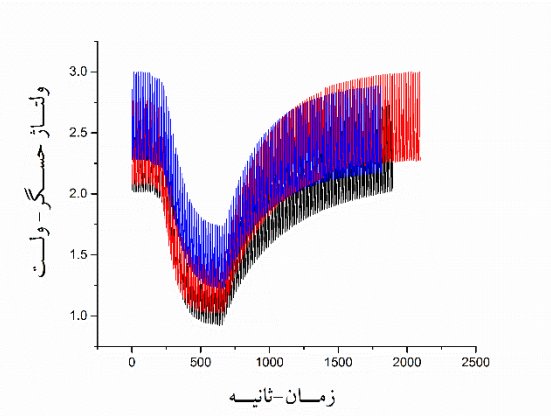
شکل (۳): سیستم آزمایش حسگر گاز



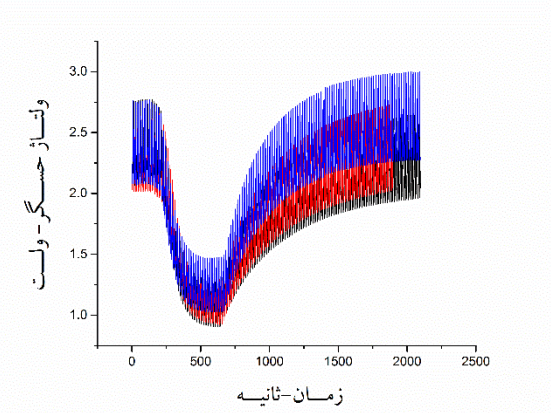
شکل (۴): پاسخ حسگر MQ2 به سرکه با خلوص ۲۰ درصد



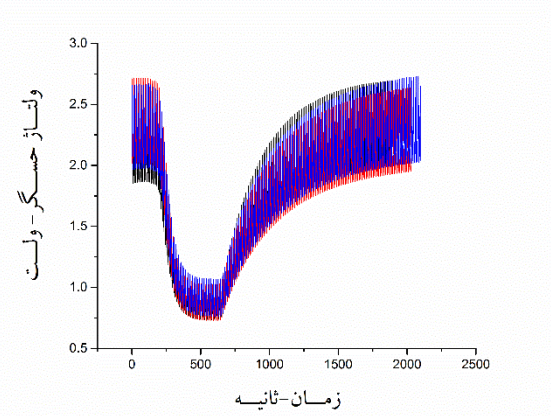
شکل (۵): پاسخ حسگر MQ2 به سرکه با خلوص ۴۰ درصد



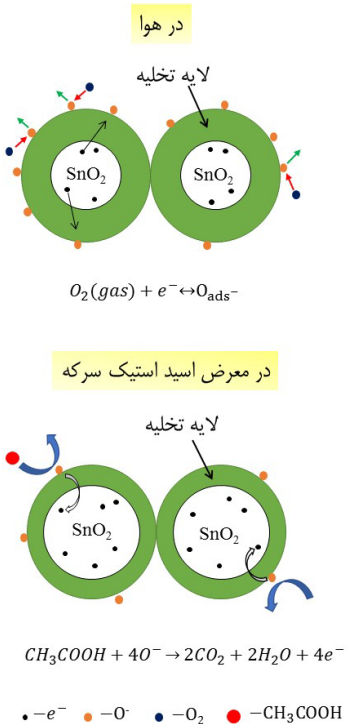
شکل (۶): پاسخ حسگر MQ2 به سرکه با خلوص ۶۰ درصد



شکل (۷): پاسخ حسگر MQ2 به سرکه با خلوص ۸۰ درصد



شکل (۸): پاسخ حسگر MQ2 به سرکه با خلوص ۱۰۰ درصد



شکل (۹): سازوکار جذب حسگر مبتنی بر اکسید قلع

زمانی که حسگر در معرض بخار سرکه قرار می‌گیرد، مولکول‌های اسید استیک با یون‌های اکسیژن جذب شده روی سطح حسگر واکنش می‌دهند و الکترون‌هایی که در دام اکسیژن‌ها افتاده‌اند را رها کرده و به ماده حسگر باز می‌گردانند. این واکنش باعث کاهش عرض ناحیه تخلیه می‌شود. کاهش عرض ناحیه تخلیه پیرامون ذرات سطحی، به معنای افزایش جریان کلی حسگر و کاهش مقاومت الکتریکی آن است.

معادله جذب مولکول‌های اکسیژن (O_2) روی سطح حسگر به صورت زیر است:

$$O_2(gas) + e^- \leftrightarrow O^-(ads) \quad (۱)$$

$$+4O^- \rightarrow 2CO_2 + 2H_2O + 4e^- \; CH_3COOH \quad (۲)$$

در این تحقیق با توجه به اینکه دمای کاری حسگر بین ۲۰۰ °C تا ۳۲۰ °C متغیر است ، بیشترین گونه غالب موجود بر روی سطح حسگر از نوع O^- است [۴۲].

۲-۴- الگوریتم دسته‌بندی

الگوریتم نزدیک‌ترین همسایگی یکی از الگوریتم‌های یادگیری ماشین تحت نظارت و بدون پارامتر است که به دلیل سادگی، پایداری، آسانی پیاده‌سازی و دقت بسیار بالا، محبوبیت زیادی در مسائل دسته‌بندی پیدا کرده است [۴۳][۴۶]. این الگوریتم بر اساس نزدیک‌ترین فاصله عمل می‌کند و با توجه به یک نقطه داده جدید، k نزدیک‌ترین همسایه از مجموعه داده‌های آموزش را شناسایی کرده و برچسب کلاس اکثریت در میان این همسایه‌ها را به نقطه جدید اختصاص می‌دهد. انتخاب مقدار k (تعداد همسایه‌ها) تأثیر قابل توجهی بر عملکرد این الگوریتم دارد. انتخاب مقادیر کوچک‌تر برای k باعث انعطاف‌پذیری بیشتر مرزهای تصمیم‌گیری می‌شود، در حالی که مقادیر بزرگ‌تر k باعث هموارتر شدن مرز مناطق تصمیم‌گیری می‌شوند. این الگوریتم به ویژه زمانی که با داده‌های نویزی روبه‌رو هستیم یا توزیع داده‌ها ناشناخته است، عملکرد خوبی دارد. فرآیند الگوریتم نزدیک‌ترین همسایگی به شرح زیر است:

۱. بارگذاری داده‌ها :ابتدا داده‌ها بارگذاری می‌شوند و معمولاً ۷۰ درصد داده‌ها برای آموزش و ۳۰ درصد برای آزمون اختصاص می‌یابد.
۲. تنظیم مقدار :k مقدار k تعیین می‌شود، که تعداد همسایه‌هایی است که برای پیش‌بینی برچسب کلاس استفاده می‌شود.
۳. محاسبه فاصله :فاصله بین داده‌های آزمون و هر ردیف از داده‌های آموزشی محاسبه می‌شود. معمولاً از فاصله اقلیدسی به عنوان فاصله سنجش استفاده می‌شود که یکی از متداول‌ترین روش‌ها است.
۴. مرتب‌سازی فاصله‌ها :فاصله‌های محاسبه شده به صورت صعودی مرتب می‌شوند.
۵. انتخاب k همسایه نزدیک‌تر :پس از مرتب‌سازی، k طر بالای آرایه فاصله انتخاب می‌شود.
۶. دریافت کلاس‌های اکثریت :کلاس‌های موجود در این k همسایه بررسی می‌شود و کلاس با بیشترین تکرار به داده آزمون اختصاص می‌یابد.
۷. بازگشت کلاس پیش‌بینی‌شده :در نهایت، کلاس پیش‌بینی‌شده برای داده آزمون بازگشت داده می‌شود.

برای اطمینان از قدرت الگوریتم و ارزیابی عملکرد آن، معمولاً از اعتبارسنجی k-fold استفاده می‌شود. در این روش، داده‌ها به صورت تصادفی به k بخش یکسان تقسیم می‌شوند. سپس مدل k بار آموزش می‌بیند و در هر بار از k-1 بخش برای آموزش و یک بخش باقی‌مانده برای اعتبارسنجی استفاده می‌شود. عملکرد مدل در تمام k بخش‌ها میانگین‌گیری شده و تخمینی از عملکرد مدل بر روی داده‌های ناشناخته ارائه می‌دهد. این الگوریتم با استفاده از نزدیکی نقاط داده در فضای ویژگی‌ها، پیش‌بینی دقیقی از برچسب کلاس داده‌ها به عمل می‌آورد و برای مسائل مختلف دسته‌بندی مانند شناسایی و تفکیک کیفیت سرکه به‌کار می‌رود.

۲-۵- استخراج ویژگی

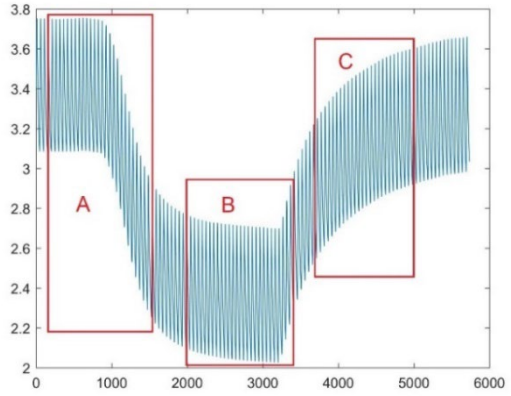
در این مقاله، برای استخراج ویژگی از نمودار ولتاژ پاسخ حسگر به گاز هدف، نمودار پاسخ به سه ناحیه مختلف تقسیم شده است که هر ناحیه اطلاعات خاصی را در مورد رفتار حسگر در مراحل مختلف آزمایش نشان می‌دهد. این نواحی به شرح زیر تعریف شده‌اند:

۱. ناحیه (A : ورود گاز هدف): این ناحیه مربوط به زمانی است که گاز هدف وارد محفظه تست حسگر می‌شود. در این مرحله، تغییرات اولیه ولتاژ و مقاومت حسگر رخ می‌دهد که نشان‌دهنده واکنش ابتدایی حسگر به گاز است.
۲. ناحیه (B : حالت ماندگار حسگر): در این ناحیه، حسگر به وضعیت پایداری رسیده و واکنش‌های آن به گاز هدف به حالت

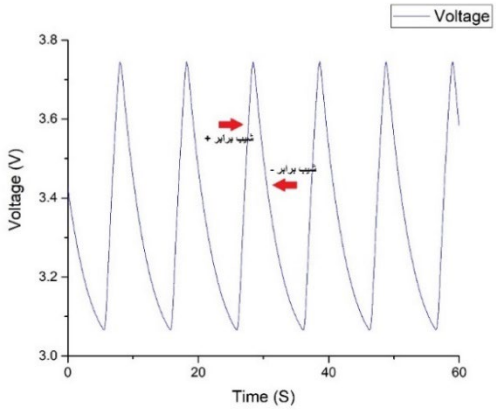
ثابت درآمده‌اند. در این بخش، ویژگی‌هایی مانند مقاومت ماندگار حسگر که به غلظت گاز بستگی دارد، استخراج می‌شود.

۳. ناحیه (C : خروج گاز هدف): پس از خروج گاز از محفظه، تغییرات ولتاژ به حالت بازگشتی یا بازیابی می‌روند. این ناحیه نمایانگر فرآیند بازیابی حسگر پس از تماس با گاز است و شامل ویژگی‌هایی است که به نحوه بازگشت حسگر به وضعیت اولیه مرتبط هستند.

ویژگی‌ها از هر سه بخش این نمودار استخراج می‌شوند و برای انجام تحلیل‌های بیشتر یا استفاده در الگوریتم‌های دسته‌بندی و شناسایی گاز هدف استفاده می‌شوند. این ویژگی‌ها می‌توانند شامل زمان رسیدن به حالت ماندگار، میزان تغییرات ولتاژ در هر ناحیه، و سرعت بازیابی حسگر باشند که به شناسایی دقیق‌تر و تحلیل رفتار حسگر کمک می‌کنند. با توجه به استفاده از مدولاسیون دما در این مقاله، در هر بخش از نمودار پاسخ حسگر، خط‌هایی با شیب مثبت و شیب منفی وجود دارد که توسط نرم‌افزار پیاده‌سازی شده تمامی این شیب‌ها در سه ناحیه A، B، C بعنوان ویژگی استخراج شده‌اند. نظر به اینکه شیب های مثبت و منفی در هر ناحیه مشخص شده در شکل (۱۰) تقریبا برابر هستند از هر ناحیه دو شیب (مثبت و منفی) انتخاب می‌شود (شکل ۱۱). بنابراین از هر بخشِ نمودار پاسخ حسگر، شش ویژگی معادل شش شیب استخراج می‌شود. علاوه بر مقادیر شیب‌ها، مقدار سیگنال پاسخ محاسبه شده نیز به عنوان ویژگی هفتم در نظر گرفته شده است.



شکل (۱۰): نمودار ولتاژ پاسخ حسگر به گاز هدف



شکل (۱۱): بزرگ‌نمایی نمودار پاسخ حسگر در ناحیه A

۳- نتایج

هدف این تحقیق ارائه یک سیستم دسته‌بندی‌کننده برای شناسایی غلظت‌های مختلف بخار سرکه و تشخیص خلوص آن است. برای این منظور، ویژگی‌های استخراج‌شده از نمودارهای ولتاژ پاسخ حسگر به گاز هدف برای سرکه با خلوص‌های مختلف (۲۰، ۴۰، ۶۰، ۸۰ و ۱۰۰ درصد) به عنوان ورودی به الگوریتم دسته‌بندی نزدیک‌ترین همسایگی اعمال شده است. به هر یک از این خلوص‌ها یک کلاس مجزا اختصاص داده شده است و ویژگی‌هایی که برای هر خلوص استخراج شده‌اند، در قالب یک بردار ورودی به دسته‌بندی‌کننده اعمال شده‌اند. در این تحقیق، تعداد همسایه‌های k در الگوریتم نزدیک‌ترین همسایگی برابر با ۳ انتخاب شده است. همچنین برای ارزیابی عملکرد این الگوریتم از روش اعتبارسنجی k-fold استفاده شده است که دقت مدل را بر اساس تقسیم تصادفی داده‌ها به k بخش و انجام آزمایشات مختلف ارزیابی می‌کند. نتایج این تحقیق نشان داده است که دقت تشخیص خلوص سرکه با استفاده از این سیستم، ۸۶ درصد بوده است که این مقدار دقت قابل قبول برای یک سیستم تشخیص خلوص سرکه محسوب می‌شود. این دقت بالای مدل نزدیک‌ترین همسایگی نشان می‌دهد که با استفاده از ویژگی‌های استخراج‌شده از ولتاژ پاسخ حسگر و الگوریتم‌های یادگیری ماشین، می‌توان به‌طور مؤثر و دقیق خلوص سرکه را شناسایی کرد.

۴- نتیجه‌گیری

در این تحقیق، یک سیستم تشخیص خلوص سرکه با استفاده از حسگر ارزان‌قیمت و در دسترس MQ2 مبتنی بر اکسید قلع توسعه داده شده است. این سیستم با استفاده از الگوریتم k-NN قادر به تشخیص خلوص سرکه با دقت قابل قبول ۸۶ درصد می‌باشد.

ملاحظات اخلاقی پیروی از اصول اخلاق پژوهش

همکاری مشارکت‌کنندگان در تحقیق حاضر به صورت داوطلبانه و با رضایت آنان بوده است.

حامی مالی

هزینه تحقیق حاضر توسط نویسندگان مقاله تامین شده است.

تعارض منافع

بنابر اظهار نویسندگان، مقاله حاضر فاقد هرگونه تعارض منافع بوده است. کنند تمام موارد ذکر شـــده را دقیقاً رعایت کنند، و از همین ســـند به‌عنوان الگوی نگارش مقاله خود استفاده کنند.

مرجع

[1] R. A. S. Lapa, J. F. C. Lima, R. Pérez-Olmos, and M. P. Ruiz, “Simultaneous automatic potentiometric determination of acidity, chloride and fluoride in vinegar,” Food Control, vol. 6, no. 3, pp. 155–159, 1995.

[2] M. Guerrero, “Multivariate characterization of wine vinegars from the south of Spain according to their metallic content,” Talanta, vol. 45, no. 2, pp. 379–386, Dec. 1997, doi: 10.1016/S0039-9140(97)00139-2.

[3] R. Castro Mejías, R. Natera Marín, M. De Valme García Moreno, and C. García Barroso, “Optimisation of

nanohybrids as chemiresistive E-nose for H2, H2S and NO2 detection," *Mater. Sci. Semicond. Process.*, vol. 147, p. 106706, 2022.

[19] Z. Khatoon, H. Fouad, O. Y. Alothman, M. Hashem, Z. A. Ansari, and S. A. Ansari, "Doped SnO2 nanomaterials for e-nose based electrochemical sensing of biomarkers of lung cancer," *ACS omega*, vol. 5, no. 42, pp. 27645–27654, 2020.

[20] Z. Li *et al.*, "E-nose based on a high-integrated and low-power metal oxide gas sensor array," *Sensors Actuators B Chem.*, vol. 380, p. 133289, 2023.

[21] B. Mahata, S. Acharyya, P. Banerji, and P. K. Guha, "Assessment of fish adulteration using SnO2 nanopetal-based gas sensor and machine learning," *Food Chem.*, vol. 438, p. 138039, 2024.

[22] A. Taurino, S. Capone, C. Distante, M. Epifani, R. Rella, and P. Siciliano, "Recognition of olive oils by means of an integrated sol–gel SnO2 Electronic Nose," *Thin Solid Films*, vol. 418, no. 1, pp. 59–65, 2002, doi: https://doi.org/10.1016/S0040-6090(02)00596-5.

[23] Z. Hu, X. Li, H. Wang, C. Niu, Y. Yuan, and T. Yue, "A novel method to quantify the activity of alcohol acetyltransferase Using a SnO2-based sensor of electronic nose," *Food Chem.*, vol. 203, pp. 498–504, 2016, doi: https://doi.org/10.1016/j.foodchem.2016.02.087.

[24] F. Bravo-Hualpa *et al.*, "SnO2-TiO2 and SnO2-MoO3 Based Composite Gas Sensors to Develop an E-nose for Peruvian Pisco Varieties Differentiation," *J. Electrochem. Soc.*, vol. 169, no. 1, p. 17511, 2022.

[25] H. Yu, X. Tan, S. Sun, L. Zhang, C. Gao, and S. Ge, "Engineering paper-based visible light-responsive Sn-self doped domed SnO2 nanotubes for ultrasensitive photoelectrochemical sensor," *Biosens. Bioelectron.*, vol. 185, p. 113250, 2021, doi: https://doi.org/10.1016/j.bios.2021.113250.

[26]Z. Huang *et al.*, "Tin Oxide (SnO2) Nanoparticles: Facile Fabrication, Characterization, and Application in UV Photodetectors," *Nanomaterials*, vol. 12, no. 4, 2022, doi: 10.3390/nano12040632.

[27] C. Wang *et al.*, "High-effective SnO2-based perovskite solar cells by multifunctional molecular additive engineering," *J. Alloys Compd.*, vol. 886, p. 161352, 2021, doi: https://doi.org/10.1016/j.jallcom.2021.161352.

[28] S. R. Morrison, "Mechanism of semiconductor gas sensor operation," *Sensors and Actuators*, vol. 11, no. 3, pp. 283–287, Apr. 1987, doi: 10.1016/0250-6874(87)80007-0.

[29] S. M. Hosseini-Golgoo and F. Hossein-Babaei, "Assessing the diagnostic information in the response patterns of a temperature-modulated tin oxide gas sensor," *Meas. Sci. Technol.*, vol. 22, no. 3, p. 35201, 2011.

[30] S. M. Hosseini-Golgoo, F. Salimi, A. Saberkari, and S. Rahbarpour, "Comparison of information content of temporal response of chemoresistive gas sensor under three different temperature modulation regimes for gas detection of different feature reduction methods," in *Journal of Physics: Conference Series*, 2017, vol. 939, no. 1, p. 12005.

[31] C. Krutzler, A. Unger, H. Marhold, T. Fricke, T. Conrad, and A. Schütze, "Influence of MOS gas-sensor production tolerances on pattern recognition techniques in electronic noses," *IEEE Trans. Instrum. Meas.*, vol. 61, no. 1, pp. 276–283, 2011.

[32] K. Yan and D. Zhang, "Improving the transfer ability of prediction models for electronic noses," *Sensors Actuators B Chem.*, vol. 220, pp. 115–124, 2015, doi: https://doi.org/10.1016/j.snb.2015.05.060.

headspace solid-phase microextraction for analysis of aromatic compounds in vinegar," J. Chromatogr. A, vol. 953, no. 1–2, pp. 7–15, Apr. 2002, doi: 10.1016/S0021-9673(02)00122-X.

[4] E. Anklam, M. Lipp, B. Radovic, E. Chiavaro, and G. Palla, "Characterisation of Italian vinegar by pyrolysis–mass spectrometry and a sensor device ('electronic nose')," *Food chemistry*, vol. 61, no. 1–2, pp. 243–8, Jan. 1998.

[5] J. Tan and J. Xu, "Applications of electronic nose (e-nose) and electronic tongue (e-tongue) in food quality-related properties determination: A review," *Artif. Intell. Agric.*, vol. 4, pp. 104–115, Jan. 2020, doi: 10.1016/j.aiia.2020.06.003.

[6] M. Wang and Y. Chen, "Electronic nose and its application in the food industry: a review," *Eur. Food Res. Technol.*, vol. 250, no. 1, pp. 21–67, Jan. 2024, doi: 10.1007/s00217-023-04381-z.

[7] R.-C. Liu, R. Li, Y. Wang, and Z.-T. Jiang, "Analysis of volatile odor compounds and aroma properties of European vinegar by the ultra-fast gas chromatographic electronic nose," *J. Food Compos. Anal.*, vol. 112, p. 104673, Sep. 2022, doi: 10.1016/j.jfca.2022.104673.

[8] E. Martín-Tornero, J. D. Barea-Ramos, J. Lozano, I. Durán-Merás, and D. Martín-Vertedor, "E-Nose Quality Evaluation of Extra Virgin Olive Oil Stored in Different Containers," *Chemosensors*, vol. 11, no. 2, 2023, doi: 10.3390/chemosensors11020085.

[9] E. Zhang *et al.*, "Application of an electronic nose for the diagnosis of ketosis in dairy cows," *Food Biosci.*, vol. 60, p. 104355, Aug. 2024, doi: 10.1016/j.fbio.2024.104355.

10] E. Aghdamifar, V. R. Sharabiani, E. Taghinezhad, M. Szymanek, and A. Dziwulska-Hunek, "E-nose as a non-destructive and fast method for identification and classification of coffee beans based on soft computing models," *Sensors Actuators B Chem.*, vol. 393, p. 134229, 2023, doi: https://doi.org/10.1016/j.snb.2023.134229.

[11] P. Jia, X. Li, M. Xu, and L. Zhang, "Classification techniques of electronic nose: a review," *Int. J. Bio-Inspired Comput.*, vol. 23, no. 1, pp. 16–27, 2024.

[12] A. T. John, K. Murugappan, D. R. Nisbet, and A. Tricoli, "An Outlook of Recent Advances in Chemiresistive Sensor-Based Electronic Nose Systems for Food Quality and Environmental Monitoring," *Sensors*, vol. 21, no. 7, 2021, doi: 10.3390/s21072271.

[13] A. Sierra-Padilla, J. J. García-Guzmán, D. López-Iglesias, J. M. Palacios-Santander, and L. Cubillana-Aguilera, "E-Tongues/Noses Based on Conducting Polymers and Composite Materials: Expanding the Possibilities in Complex Analytical Sensing," *Sensors*, vol. 21, no. 15, 2021, doi: 10.3390/s21154976.

[14] H. L. Gan, Y. B. C. Man, C. P. Tan, I. NorAini, and S. A. H. Nazimah, "Characterisation of vegetable oils by surface acoustic wave sensing electronic nose," *Food Chem.*, vol. 89, no. 4, pp. 507–518, 2005, doi: https://doi.org/10.1016/j.foodchem.2004.03.005.

[15] S. Ampuero and J. O. Bosset, "The electronic nose applied to dairy products: a review," *Sensors Actuators B Chem.*, vol. 94, no. 1, pp. 1–12, 2003, doi: https://doi.org/10.1016/S0925-4005(03)00321-6.

[16] M. Tonezzer *et al.*, "Electronic noses based on metal oxide nanowires: A review," *Nanotechnol. Rev.*, vol. 11, no. 1, pp. 897–925, 2022.

[17] W. S. Al-Dayyeni *et al.*, "A review on electronic nose: coherent taxonomy, classification, motivations, challenges, recommendations and datasets," *IEEE Access*, vol. 9, pp. 88535–88551, 2021.

[18] B. Bhangare, K. R. Sinju, N. S. Ramgir, S. Gosavi, and A. K. Debnath, "Noble metal sensitized SnO2/RGO

[33] G.-Y. Miao, S.-S. Chen, Y.-J. Wang, Z. Guo, and X.-J. Huang, “SnO2 Nanostructures Exposed with Various Crystal Facets for Temperature-Modulated Sensing of Volatile Organic Compounds,” *ACS Appl. Nano Mater.*, vol. 5, no. 8, pp. 10636–10644, 2022.
[34] A. Schütze and T. Sauerwald, “Dynamic operation of semiconductor sensors,” in *Semiconductor Gas Sensors*, Elsevier, 2020, pp. 385–412. doi: 10.1016/B978-0-08-102559-8.00012-4.
[35] T. Iwata, M. Saeki, Y. Okura, and T. Yoshikawa, “Gas discrimination based on enhanced gas-species related information obtained by a single gas sensor with novel temperature modulation,” *Sensors Actuators B Chem.*, vol. 354, p. 131225, Mar. 2022, doi: 10.1016/j.snb.2021.131225.
[36] W. An and C. Y. Yang, “Review on Temperature Modulation Technology of Gas Sensors,” in *Electrical Information and Mechatronics and Applications*, 2012, vol. 143, pp. 567–571. doi: 10.4028/www.scientific.net/AMM.143-144.567.
[37] F. Rastrello, P. Placidi, and A. Scorzoni, “A System for the Dynamic Control and Thermal Characterization of Ultra Low Power Gas Sensors,” *IEEE Trans. Instrum. Meas.*, vol. 60, no. 5, pp. 1876–1883, 2011, doi: 10.1109/TIM.2010.2089130.
[38] E. Brauns, E. Morsbach, S. Kunz, M. Baeumer, and W. Lang, “Temperature modulation of a catalytic gas sensor,” *Sensors*, vol. 14, no. 11, pp. 20372–20381, 2014.
[39] A. Far, B. Guo, F. Flitti, and A. Bermak, “Temperature modulation for tin-oxide gas sensors,” in *4th IEEE International Symposium on Electronic Design, Test and Applications (delta 2008)*, 2008, pp. 378–381.
[40] M. Leidinger, T. Sauerwald, T. Conrad, W. Reimringer, G. Ventura, and A. Schütze, “Selective detection of hazardous indoor VOCs using metal oxide gas sensors,” *Procedia Eng.*, vol. 87, pp. 1449–1452, 2014.
[41] V. Khorramshahi, J. Karamdel, and R. Yousefi, “Acetic acid sensing of Mg-doped ZnO thin films fabricated by the sol–gel method,” *J. Mater. Sci. Mater. Electron.*, vol. 29, no. 17, pp. 14679–14688, 2018, doi: 10.1007/s10854-018-9604-0.
[42] V. Khorramshahi, J. Karamdel, and R. Yousefi, “High acetic acid sensing performance of Mg-doped ZnO/rGO nanocomposites,” *Ceram. Int.*, vol. 45, no. 6, pp. 7034–7043, Apr. 2019, doi: 10.1016/j.ceramint.2018.12.205.
[43] A. Boujnah, A. Boubaker, S. Pecqueur, K. Lmimouni, and A. Kalboussi, “An electronic nose using conductometric gas sensors based on P3HT doped with triflates for gas detection using computational techniques (PCA, LDA, and kNN),” *J. Mater. Sci. Mater. Electron.*, vol. 33, no. 36, pp. 27132–27146, 2022.
[44] M. Abbatangelo, E. Núñez-Carmona, V. Sberveglieri, E. Comini, and G. Sberveglieri, “k-NN and k-NN-ANN combined classifier to assess mox gas sensors performances affected by drift caused by early life aging,” *Chemosensors*, vol. 8, no. 1, p. 6, 2020.
[45] M. Ismail and S. A. D. Prasetyowati, “Classification Of Alcohol Type Using Gas Sensor And K-Nearest Neighbor,” *J. Nas. Tek. Elektro*, pp. 59–64, 2022.
[46] W. Xia, T. Song, Z. Yan, K. Song, D. Chen, and Y. Chen, “A Method for Recognition of Mixed Gas Composition Based on PCA and KNN,” in *2021 19th International Conference on Optical Communications and Networks (ICOCN)*, 2021, pp. 1–3.

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

OFDM Radar for Detecting a Rayleigh Fluctuating Target in Gaussian Noise

Mahboobeh Eghtesad*

Department of Electrical Engineering, Shiraz branch, Islamic Azad University, Shiraz, Iran
mah_ehgtesadi@yahoo.com

Abstract: we develop methods for detecting a target for continuous wave orthogonal frequency division multiplexing (OFDM) based radars. As a preliminary step we introduce the target and Gaussian noise models in discrete time form. Then resorting to match filter (MF) we derive a detector for two different scenarios (a non- fluctuating target and a Rayleigh fluctuating target). It will be shown that a MF is not suitable for Rayleigh fluctuating targets. In this paper we propose a reduced complexity method based on fast Fourier transform (FFT) for such a situation. The proposed method has better detection performance. The effectiveness of the proposed approach is demonstrated both by providing theoretical performance prediction expressions and by using simulated analyses.

Keywords: Constant false alarm rate (CFAR), match filter (MF), fast Fourier transform (FFT), OFDM radars, Rayleigh fluctuating target.

JCDSA, Vol. 2, No. 3, Autumn 2024	Online ISSN: 2981-1295	Journal Homepage: https://sanad.iau.ir/en/Journal/jcdsa
Received: 2024-08-06	Accepted: 2024-11-26	Published: 2024-12-20

CITATION

Eghtesad, M., "*OFDM Radar for Detecting a Rayleigh Fluctuating Target in Gaussian Noise*", Journal of Circuits, Data and Systems Analysis (JCDSA), Vol. 2, No. 3, pp. 63-71, 2024.
DOI: 00.00000/0000

* Corresponding author

Extended Abstract

1- Introduction

In this corresponding, we consider a multi frequency radar that employs an orthogonal frequency division multiplexing (OFDM) signal. The advantage of OFDM radar signaling has been well established in various algorithms, such as improved wideband ambiguity function.

2-Methodology

We consider on OFDM signaling system.

$$x(t) = \sum_{m=1}^{M}\left[\sum_{p=0}^{P-1} a_{p,m}\exp\left(j2\pi f_p t\right)\right] s(t-(m-1)t_c) \quad (1)$$

Where

$$S(t) = \begin{cases} 1, 0 \le t < tc \\ 0, otherwise \end{cases} \quad (2)$$

and $f_p = \frac{p}{t_c}$, p=0,1,…,P-1 denotes the subcarrier frequency. The subcarrier distance is equal to the inverse of the chip duration, forming OFDM. In this paper 5 carriers are used (P=5), and the consecutive ordered cyclic shift of a p4 code with length 5 has been used to modulate these five carriers. The phase vector of p4 code that is used is given by:

$$a = [0^\circ - 144^\circ - 216^\circ - 216^\circ - 144^\circ] \quad (3)$$

Detection of a target in an echo-location system is often accomplished through the use of a matched filter receiver. after sampling the received signal, it is correlated with a template. The match filter is the optimal linear filter for maximizing the signal to noise ratio (SNR) in the presence of additive Gaussian noise. To study the performance of matched filter, we separately considered two different scenarios: In the first scenario there is a constant target cross section. In the second one we account for variations in the target cross section (a Rayleigh fluctuating target). Swerling classified the temporal autocorrelation of a fluctuating target in the terms of its decorrelation time relative to the pulse repetition interval and scan interval of the subject radar. The complex envelope of the received signal is given by:

$$y[n] = \sum_{p=0}^{p-1}\sum_{m=1}^{M} x_p[n]a_{p,m}\, exp\left(j2\pi\frac{np}{NP}\right) s\left(\frac{nt_c}{NP} - (m-1)t_c\right) + e[n] \quad (4)$$

Where $x_p[n]$ is a complex Gaussian random variable whose envelope has a Rayleigh distribution representing a Rayleigh fluctuating target. $x_p[n]$ is assumed uncorrelated from pulse to pulse, that stands for Swerling II target return. e[n] is the additive white Gaussian noise. The performance of the matched filter will be evaluated by simulation mainly focusing on a Rayleigh fluctuating target. Target fluctuation lowers the probability of detection for matched filter algorithm. another method for the realization of the matched filter is presented to compress the OFDM signal. To calculate the matched filter output in each sample time, first the last received NPM samples are divided into M segments each containing NP samples.

$$[x[n-NPM+1]x[n-NPM+2]\ldots x[n]] = [x_1 x_2 \ldots x_M] \quad (5)$$

where

$$X_i = [x[n-(M-i+1)NP+1] \; x[n-(M-i+1)NP+2] \; \ldots x[n-(M-i+1)NP+NP]] \quad (6)$$

Then the FFT of length NP is computed for each segment.

$$F_{X_I} = FFT(X_i) \quad (7)$$

The first P samples of each FFT are demultiplexed and the resulting P sequences are filtered by P different conventional single carrier pulse compression filters that are matched to the codes modulated on each sub carrier respectively.

$$S_P = \sum_{i=1}^{M} Fx_i(P)a_{p,i}^* \quad (8)$$

At the end, different channels data are added in order to compute the final output for the given sample time.

$$y[n] = \sum_{p=1}^{p} S_p \quad (9)$$

This operation is performed sequentially by sliding on all of the sample times.

For Rayleigh Fluctuation targets, instead of using just FFT, if we use an absolute, we will have an improvement in the detection of the target.

3-Results and discussion

For Rayleigh Fluctuation targets, instead of using equation (9), if we sum the absolute of S_p we will have an improvement in the detection of the target. More precisely

$$y[n] = \sum_{P=1}^{P} |S_P| \quad (10)$$

We propose a reduced complexity detection algorithm of OFDM signals. We will show that this new algorithm has better performance compared to matched filter. For a constant False alarm probability if we compute Detection probability as a function of signal to noise ratio (SNR), the better performance of the proposed algorithm is determined. The other advantage of our method is the reduction of computational complexity in comparison with matched filter.

4- Conclusion

It is shown that a match filter (MF) is not suitable for a Rayleigh fluctuating target, then for such targets a new approach was presented, that operates on the sub carriers instead on the hole OFDM signal. This sub carrier based processing offers a considerable improvement of OFDM radar performance and has lower computational complexity compared to the MF. Future research will explore alternative fluctuating targets in OFDM radars.

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

رادار OFDM برای آشکار کردن اهداف با اعوجاج رایلی در نویز گوسی

محبوبه اقتصاد*

گروه مهندسی برق، واحد شیراز، دانشگاه آزاد اسلامی، شیراز، ایران (mah_ehgtesadi@yahoo.com)

چکیده: این مقاله به بررسی روش‌هایی برای آشکارسازی اهداف در رادار مدولاسیون تقسیم فرکانس عمودبرهم می‌پردازد. در ابتدا مدل هدف و نویز گسسته گوسی معرفی می‌شوند. سپس برای آشکارسازی هدف از فیلتر منطبق استفاده می‌شود و نشان داده می‌شود که فیلتر منطبق برای اهداف ساده خوب عمل می‌کند؛ اما در مورد اهدافی که اعوجاج رایلی دارند عملکرد فیلتر منطبق به شدت افت می‌کند. در این مقاله چکیده روشی جدید بر اساس تبدیل فوریه سریع برای چنین اهدافی ارائه می‌شود. این روش که بار محاسباتی کمتری نسبت به فیلتر منطبق دارد، دارای عملکرد بهتری در آشکار کردن هدف می‌باشد. اثربخشی رویکرد پیشنهادی هم به صورت تئوری و هم با استفاده از تحلیل‌های شبیه‌سازی، نشان داده شده است.

واژه های کلیدی: نرخ هشدار کاذب ثابت، فیلتر منطبق، تبدیل فوریه سریع، رادار مدولاسیون تقسیم فرکانس عمودبرهم (OFDM)، هدف با اعوجاج رایلی.

نوع مقاله: پژوهشی
تاریخ ارسال مقاله: ۱۴۰۳/۰۵/۱۶ تاریخ پذیرش مقاله: ۱۴۰۳/۰۹/۰۶ تاریخ چاپ مقاله: ۱۴۰۳/۰۹/۳۰
DOI: 00.00000/0000

۱- مقدمه

حد تفکیک بالا در رادار، از جمله ویژگی‌های رادارهای مدرن امروزی به شمار می‌آید. در واقع رادارهای مرسوم که دارای حد تفکیک کمی می‌باشند فقط قادر به کشف هدف و اندازه‌گیری موقعیت آن با دقت نسبتا کمی بوده و نمی‌توانند تصویری را از هدف ایجاد نموده و هدف را تشخیص دهند. بنابراین همیشه دستیابی به قدرت تفکیک بالا چه در فاصله و چه در فرکانس داپلر در کاربردهای راداری مورد بحث و توجه بوده و گام‌های زیادی نیز برای نیل به این هدف برداشته شده است. افزایش حد تفکیک رادار در برد از طریق افزایش پهنای بلند سیگنال ارسالی آن میسر می‌شود. با استفاده از پالس‌های بسیار باریک قدرت تفکیک مطلوب در فاصله برآورده می‌شود، اما مشکل اساسی در این روش این است که با باریکتر شدن عرض پالس، از یک طرف انرژی ارسالی کم شده که نیازمند توان قله ارسالی بالا می‌باشد و از سوی دیگر قدرت تفکیک در فرکانس داپلر به همان نسبت کمتر خواهد شد. از جمله تکنیک‌هایی که می‌توان برای این منظور استفاده کرد روش‌های مرسوم مدولاسیون فاز و یا فرکانس در پالس ارسالی می‌باشد. اما افزایش پهنای باند در سیگنال مدوله شده فاز[2] معادل با کاهش عرض چیپ[3] بوده که کاهش بیش از حد عرض چیپ با محدودیت‌های تکنولوژیک مواجه می‌شود. راهکاری که برای غلبه بر این مشکل ارائه می‌شود استفاده از سیگنال‌های چند حاملی است.

در این راستا مدولاسیون تقسیم فرکانس عمودبرهم (OFDM[4]) به عنوان یکی از روش‌های کارامد جهت افزایش حد تفکیک رادار معرفی شده است. تاکنون تحقیقات زیادی در خصوص رادارهای OFDM صورت گرفته که عمدتا شامل مباحث طراحی سیگنال، الگوریتم های پردازش و کاربردهای این رادار می‌باشد. از محورهای تحقیقاتی در خصوص پردازش سیگنال در رادارهای OFDM، بحث آشکارسازی اهداف در این رادارها است [۱]. در سیگنال چند حاملی OFDM می‌توان به نحو بهتری از پهنای باند در دسترس استفاده کرد و همچنین با انتخاب کدهای مناسب گلبرگ‌های فرعی تابع ابهام سیگنال تا حد مطلوبی کاهش پیدا می‌کند. ضمناً با پردازش ساده‌تری می‌توان اقدام به فشرده‌سازی آن نمود که این مسأله پایه بحث این مقاله می‌باشد. در این مقاله راداری با سیگنال ارسالی OFDM در نظر گرفته شده است [۲]. بسیاری ازکارهایی که تاکنون در این زمینه انجام شده محدود به آشکارسازی اهداف با ضرایب بازگشتی ثابت در حضور تداخلات گوسی است که تا حدود زیادی با واقعیت فاصله دارد. در این

* نویسنده مسئول

[2] phase code modulation (PCM)
[3] Chip width
[4] Orthogonal Frequency Division Multiplexing

مقاله هدف هرچه واقعی‌تر کردن پارامترهای موجود در مساله آشکارسازی اهداف در رادارهای OFDM می‌باشد. بنابراین مساله تموج هدف یا تغییر انعکاسات هدف در نظر گرفته شده است.

در سال‌های اخیر بر روی رادارهای OFDM تحقیقات وسیعی صورت گرفته است. به عنوان نمونه می‌توان به چند مورد زیر اشاره کرد. نشان داده می‌شود که در رادار OFDM می‌توان نرخ نمونه‌برداری سیگنال دریافتی را به نسبت تعداد زیر حامل‌ها کم کرد بدون اینکه بیشترین برد بدون ابهام برای تخمین موقعیت هدف کم شود [۳]. با استفاده از به‌کارگیری سیگنال OFDM در [۴] برای جلوگیری از کاهش نسبت سیگنال به نویز هدف‌های دور در رادارهای موج پیوسته تحقیقاتی انجام شده است. اگر بخواهیم تفکیک برد بالایی داشته باشیم, شکل موج‌های رادار مبتنی برسیگنال OFDM معمولاً به نرخ‌های نمونه‌برداری بالایی نیاز دارند. در مقابل، مقاله [۵] طرحی را پیشنهاد می‌کند که نرخ‌های نمونه‌برداری لازم را در فرستنده و گیرنده ثابت نگه می‌دارد و همزمان پهنای بلند لحظه‌ای سیگنال را در کانال رادار افزایش می‌دهد. مسأله دقت برد بالا و سرعت بدون ابهام بالا نیز در این مقاله مطرح شده است. نویسندگان در این مقاله روشی بر اساس افزایش همزمان پهنای باند لحظه ای سیگنال ارائه داده اند که نیاز به افزایش نرخ نمونه برداری سیگنال را از بین می‌برد. سیگنال‌های OFDM به بایاس فرکانس داپلر و اثرات چند مسیری حساس هستند، که به طور سنتی با پیش کدهای چرخه‌ای که قبل از هر نماد OFDM درج می‌شوند، جبران می‌شوند. این پیش کدهای چرخه ای متاسفانه باعث بالا رفتن تلفات انرژی در سیستم های ارتباطی می‌شوند و نیز پس از پردازش سیگنال رادار، اهداف کاذب را نیز تشکیل می‌دهند. برای رسیدگی به کاستی‌های OFDM معمولی، در [۶] یک سیستم ارتباطی مشترک راداری OFDM بدون پیش کدهای چرخه ای پیشنهاد می‌شود. این سیستم سیگنال پالس OFDM را به اهداف خاص ویا سیستم های ارتباطی ارسال می‌کند و پژواک ها را در بازه تکرار پالس دریافت می‌کند. با حذف پیش کدها، سیستم رادار می تواند پژواک ها را بدون اهداف شبح فشرده کند. از طریق نمونه‌برداری معقول که باید به طور قابل توجهی طراحی شود، سیستم‌های ارتباطی پالس OFDM را برای استخراج اطلاعات بدون تداخل بین نمادی در کلنال‌های چندمسیری تغییر می‌دهند. علاوه بر این، محدودیت‌های زمان، فرکانس و نمونه‌برداری روی سیستم تحلیل شده است.

قدرت آشکارسازی بالا از جمله ویژگی‌های رادارهای مدرن امروزی به شمار می‌آید. بنابراین همیشه بالا بردن احتمال آشکارسازی هدف در کاربردهای راداری مورد توجه بوده و همچنان هم در کانون توجه و بحث می‌باشد و گام‌های زیادی نیز برای نیل به این هدف برداشته شده است. بحث آشکارسازی هدف با استفاده از فیلتر منطبق روشی بسیار کارآمد است که در مقالات روز دنیا مشاهده می‌شود [۷]. در سال‌های اخیر تحقیقات زیادی بر روی رادار پسیو OFDM انجام شده است.در [۸] رادار آرایه متنوع فرکانس یک آفست فرکانس کوچک را در سراسر عناصر آرایه فرستنده مجاور خود اعمال می‌کند تا یک الگوی پرتو وابسته به زاویه و برد ایجاد کند. افزایش درجه آزادی در حوزه برد می‌تواند به بهبود عملکرد رادار در تشخیص هدف، محلی سازی و حذف کلاتر کمک کند. رادار پسیو از سیگنال خارجی غیرقابل کنترل به عنوان روشنگر استفاده می‌کند، که استفاده از روش فرآیند متنوع فرکانس سنتی را دشوار می‌کند. با این حال، روشن‌کننده‌های شخص ثالث سیگنال OFDM تشعشع می‌کنند که معمولاً از چندین حامل مدوله‌شده با فاصله نزدیک تشکیل شده‌اند و در سال‌های اخیر به‌طور گسترده به عنوان روشن‌کننده برای رادار غیرفعال انتخاب شده‌اند. با در نظر گرفتن متعامد بودن بین زیرحامل‌های حتی جدا شده، یک روش فرآیند متنوع فرکانس جدیدی را با استخراج و پردازش هر زیرحامل داده‌های دریافتی به طور مستقل پیشنهاد می‌شود و تلاش می‌شود یک الگوی پرتو وابسته به زاویه برد برای رادار غیرفعال OFDM ارائه شود.

در این مقاله در بخش ۲ سیگنال OFDM معرفی می‌شود. در بخش ۳ یک فیلتر منطبق گسسته برای آشکار کردن هدف به کار می‌رود. دو نوع هدف، یکی هدف ساده و دیگری هدف با تموج رایلی در این قسمت مورد بررسی قرار می‌گیرند. فرض می‌شود که برای هدف متموج ضرایب انعکاس از یک حامل به حامل دیگر مستقل است و نیز در قطاری از پالس‌ها از یک پالس تا پالس دیگر مستقل می‌ملند در حین اینکه خیلی سریع با تابع چگالی احتمال رایلی تغییر می‌کنند (مدل سوئر لینگ[1] نوع ۲). در بخش ۴ روش جدیدی برای فشرده‌سازی معرفی می‌شود و عملکرد آن با روش‌های معمول مقایسه می‌گردد. بخش ۵ به نتیجه‌گیری مقاله می‌پردازد.

۲- سیگنال OFDM

سیگنال معادل باند پایه که بر پایه مدولاسیون OFDM در مخابرات معرفی می‌شود، شامل چند سیگنال حامل متعامد می‌باشد که به صورت همزمان ارسال شده و هر حامل با یک دنباله M بیتی مجزا مدوله فاز می‌گردد، بطوریکه فاصله فرکانسی سیگنال‌های حامل برابر عکس عرض بیت می‌باشد. در این مقاله یک سیگنال OFDM با P زیر حامل در نظر گرفته می‌شود که هر زیر حامل M چیپ دارد. $a_{p,m}$ معرف ضریب مختلط سیگنال ارسالی برای زیر حامل pام و چیپ mام است. ضرایب $\{a_{p,m}\}$ برای m های مختلف از ۱ تا M برابر با رشته کدها به ازای حامل pام می‌باشند. پوش مختلط سیگنال ارسالی را می‌توان به‌صورت زیر نشان داد:

$$x(t) = \sum_{m=1}^{M}\left[\sum_{p=0}^{P-1} a_{p,m}\exp\left(j2\pi f_p t\right)\right] s(t-(m-1)t_c) \quad (۱)$$

که در آن

$$S(t) = \begin{cases} 1, 0 \le t < tc \\ 0, otherwise \end{cases} \quad (۲)$$

t_c معرف عرض چیپ است و $f_p = \frac{p}{t_c}$ برای p=0,1,…,P-1 معرف فرکانس زیر حامل‌ها است. فاصله فرکانسی زیر حامل‌های مختلف برابر با عکس عرض چیپ است که باعث عمود بودن زیرحامل‌ها بر هم

[1] Swerling case II

می‌شود. در این مقاله P=5 است یعنی پنج زیر حامل وجود دارند. از یک کد P_4 با شیفت چرخشی به طول پنج برای مدوله کردن این پنج زیر حامل استفاده شده است. بردار فاز P_4 به‌صورت زیر می‌باشد:

$$a = [0° - 144° - 216° - 216° - 144°] \quad (۳)$$

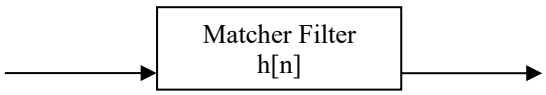
ایده اصلی در رادار OFDM ارسال داده‌ها به صورت موازی بر روی چند حامل متعامد با پهنای باند کم به جای ارسال داده‌ها به‌صورت سری بر روی یک حامل پهن باند می‌باشد.

۳- فیلتر منطبق برای آشکار کردن هدف

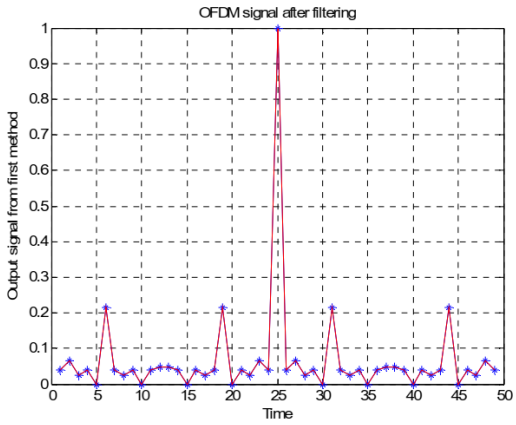
فیلتر منطبق، اغلب در آشکارسازی سیگنال به‌کار می‌رود. برای نمونه، اگر هدف یافتن فاصله یک جسم از راه بازتاب سیگنال از آن باشد؛ یک پالس سینوسی خالص یک هرتزی به‌سوی جسم گسیل می‌کنند. فرض می‌شود که سیگنال بازتابیده از جسم، نسخه‌ای ضعیف‌شده و تغییرفازیافته از سیگنال گسیل‌شده در کنار نویز جمع‌شونده باشد. برای یافتن فاصله جسم، پالس دریافت‌شده را با پاسخ ضربه یک فیلتر منطبق، هم‌بسته[1] می‌کنند، که آن هم در حضور نویز سفید ناهم‌بسته، سینوسی خالص یک هرتزی است. وقتی خروجی فیلتر از آستانه‌ای معین فراتر رود، با احتمال زیاد نتیجه گرفته می‌شود که سیگنال دریافت‌شده، از جسم بازتابیده است. با در نظر گرفتن سرعت انتشار موج و اختلاف زمان میان لحظه گسیل شدن سیگنال و لحظه آشکار شدن سیگنال در خروجی فیلتر، فاصله جسم تخمین زده می‌شود. اگر شکل پالس به روشی خاص تغییر داده شود، نسبت سیگنال به نویز و دقت تخمین فاصله پس‌از فیلتر کردن را می‌توان بهبود بخشید؛ این روشی است که فشرده‌سازی پالس نام دارد.

معمولاً آشکار کردن یک هدف در سیستمی که بر اساس انعکاس موج از هدف باشد با فیلتر منطبق یا محاسبه مستقیم تابع همبستگی انجام می‌شود. همانطور که در شکل (۱) نشان داده شده است، بعد از نمونه‌برداری از سیگنال دریافتی، هم‌بستگی سیگنال حاصل و نمونه‌های سیگنال مرجع محاسبه می‌شود. فیلتر منطبق بهترین فیلتر خطی برای داشتن بیشترین توان سیگنال به نویز[2] در حضور نویز گوسی جمع شونده می‌باشد. فیلتر منطبق در رادار بسیار استفاده می‌شود، که در آن، سیگنال مشخصی گسیل می‌شود و سیگنال منعکس‌شده (دریافت‌شده) برای یافتن ویژگی‌های مشترک با سیگنال گسیل‌شده بررسی می‌شود. فشرده‌سازی پالس نمونه‌ای از کاربرد فیلتر منطبق در رادار است. در واقع پاسخ ضربه فیلتر گیرنده و سیگنال پالسی گسیل‌شده، برهم منطبق هستند. اگر از این سیگنال نمونه‌برداری شود، پاسخ ضربه فیلتر منطبق گسسته به‌دست می‌آید. در نتیجه خروجی فیلتر منطبق به‌صورت زیر می‌باشد که علامت * به معنی کانولوشن خطی است:

$$y[n] = x[n] * h[n] = \sum_{K=-\infty}^{+\infty} x[k]\, h[x-k] \quad (۴)$$



شکل (۱): شمای گیرنده با فیلتر منطبق



شکل (۲): خروجی فیلتر منطبق برای سیگنال OFDM متشکل از پنج حامل و تاخیری برابرپنج سلول فاصل

برای مثال اگر در سیگنال OFDM از پنج حامل استفاده شده و شیفت یافته‌های چرخشی کد مطابق (۳) با طول ۵ روی این ۵ حامل مدوله گردیده باشد، خروجی فیلتر منطبق برای هدفی ساکن به صورت شکل (۲) خواهد بود.

برای مطالعه عملکرد فیلتر منطبق دو سناریوی مختلف بررسی شده است: در سناریوی نخست یک رادار OFDM با پنج زیر حامل یعنی P=5 فاصله فرکانسی $1/t_c = 1Hz$ و پنج چیپ در هر پالس M=5. ضریب انعکاس هدف ثابت است. پوش مختلط سیگنال دریافتی در یک سلول فاصله حاوی هدف پس از نمونه‌برداری بصورت زیر است:

$$y[n] = \sum_{p=0}^{p-1} \sum_{m=1}^{M} x\, a_{p,m} \exp\left(j2\pi \frac{np}{NP}\right) s\left(\frac{nt_c}{NP} - (m-1)t_c\right) + e[n] \quad (۵)$$

که در آن x به منزله ضریب انعکاس هدف می‌باشد. $e[n]$ هم نویز سفید گوسی جمع شونده است. در سناریوی قبل، هدفی ساده بدون اعوجاج در نظر گرفته شد. در اینجا هدفی با ضریب انعکاس متغییر شبیه‌سازی می‌شود. در عمل اکوی بازگشتی از اهداف یا در واقع RCS[3] هدف وابسته به فرکانس و زمان بوده که تغییرات ناشی از آنها تحت عنوان تموج هدف شناخته شده‌اند.

در رادارهای OFDM به‌دلیل اینکه توان بر روی چندین پالس در چند فرکانس ارسال می‌شود، تموج می‌تواند پالس به پالس یا فرکانس به فرکانس رخ دهد. به‌دلیل چند نقطه‌ای بودن اهداف، اکوی بازگشتی از آنها با اختلاف فازها و دامنه‌های مختلفی جمع می‌شوند که این اختلاف فازها به فرکانس و فاصله آنها از رادار وابسته است. این اختلاف فازها به طور مداوم عوض شده و مدل‌های آماری مختلفی را به صورت تصادفی ایجاد می‌کنند. اما در حالت کلی مقدار RCS بازگشتی از هدف دارای تابع چگالی احتمال Chi-square خواهد بود. سوئرلینگ

[1] correlate
[2] Signal-to-Noise Ratio (SNR)
[3] Radar Cross Section

همبستگی زمانی اهداف دارای اعوجاج را با توجه به زمان ناهمبستگی نسبت به PRI[1] و زمان اسکن شی توسط رادار دسته‌بندی کرد [۱۲].

سوئرلینگ نوع اول مدلی است که در آن RCS هدف مطابق با تابع چگالی احتمال کای اسکوئر[2] با دو درجه آزادی تغییر می‌کند در حالی که مقدار RCS آن در طول یک اسکن همواره ثابت می‌ماند. دراین حالت مقدار تابع چگالی احتمال آن به صورت رابطه زیر می‌شود.

$$p(\sigma) = \frac{1}{\sigma_{av}} e^{\frac{-\sigma}{\sigma_{av}}} \quad (۶)$$

که در آن σ مقدار RCS و σ_{av} مقدار میانگین RCSهدف را مشخص می‌کند. که این معادل است با توزیع رایلی برای دامنه سیگنال:

$$p(s,\sigma) = \frac{s}{\sigma^2} e^{\frac{-s^2}{2\sigma^2}} \quad (۷)$$

مدل سوئرلینگ نوع اول معرف یک متغیر تصادفی همبسته است که با تابع طیف توان مدل خواهد شد که پهنای بلند آن از ۳ تا ۳۰ هرتز بسته به اهداف مختلف متغیر خواهد بود. مدل سوئرلینگ نوع دوم از نظر توزیع آماری RCS هدف، شبیه مدل سوئرلینگ نوع اول است و تنها تفاوت آن در این است که مقدار RCS بازگشتی از پالسی به پالسی دیگر مستقل است. یک سناریو که سبب استقلال RCS نقاط منعکس کننده هدف می‌شود، تنوع فرکانسی است. بنابراین مدل سوئرلینگ نوع دوم برای رادارهایی با تغییر فرکانسی مانند رادارهای پالسی با یک فرکانس متفاوت بر روی پالس های مختلف و همچنین رادارهای OFDM با چندین فرکانس بر روی یک پالس، مناسب است. در رادارهای OFDM وقتی فاصله فرکانسی حامل ها زیاد می‌شود، RCS از فرکانسی به فرکانس دیگر مستقل خواهد شد.

در این قسمت عملکرد فیلتر منطبق برای یک هدف دارای اعوجاج رایلی با شبیه‌سازی بررسی می‌شود. پوش مختلط سیگنال دریافتی بصورت زیر می‌باشد:

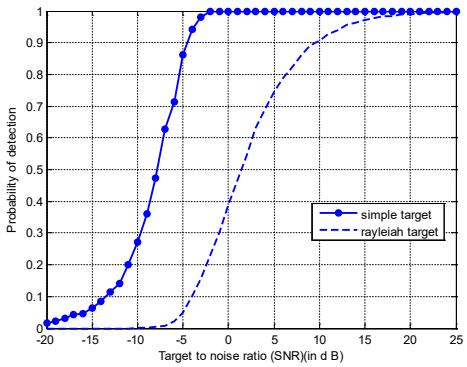
$$y[n] = \sum_{p=0}^{p-1} \sum_{m=1}^{M} x_p[n] a_{p,m} \exp\left(j2\pi \frac{np}{NP}\right) s\left(\frac{nt_c}{NP} - (m-1)t_c\right) + e[n] \quad (۸)$$

که در آن $xp[n]$ یک متغیر تصادفی مختلط گوسی است و اندازه‌ی آن توزیع رایلی دارد و معرف هدفی رایلی است. $xp[n]$ از یک پالس تا پالس دیگر ناهمبسته است و مدل سوئرلینگ نوع ۲ را دارد. $e[n]$ نویز سفید گوسی جمع شونده است.

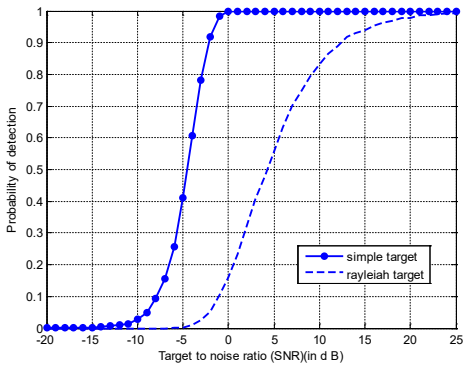
نمونه‌های نویز توزیع مختلط گوسی دارند و در ضریبی ضرب می‌شوند تا SNR دلخواه به‌وجود اید؛ که SNR به‌صورت زیر تعریف می‌شود:

$$SNR = \frac{1}{N} \sum_{n=0}^{NPM-1} (r^2 |x[n]|^2) \quad (۹)$$

r ضریب مورد نظر می‌باشد که باعث می‌شود SNR مطلوب به‌دست آید. شکل‌های (۳-۴) عملکرد فیلتر منطبق را در دو سناریوی هدف ساده و هدف دارای اعوجاج نشان می‌دهند و برای احتمال هشدار کاذب‌های متفاوت کشیده شده‌اند. در رسم این منحنی‌ها ابتدا به روش مونت‌کارلو حد آستانه برای مقایسه خروجی پردازشگر مشخص می‌شود.



شکل (۳): احتمال آشکارسازی برای $p_{fa} = 10^{-2}$



شکل (۴): احتمال آشکارسازی برای $p_{fa} = 10^{-4}$

برای این منظور ابتدا یک احتمال هشدار کاذب در نظر گرفته می‌شود. در حالت هشدار کاذب در سیگنال دریافتی رادار هدفی وجود ندارد و فقط نویز دریافت می‌شود. سپس عدد صد بر احتمال هشدار کاذب تقسیم می‌شود و به این تعداد الگوریتم اجرا می‌شود. فرض می‌شود که در صد مرتبه احتمال هشدار کاذب رخ دهد؛ پس خروجی‌های الگوریتم از کوچک به بزرگ مرتب می‌شوند و از روی داده صدم در یک احتمال هشدار کاذب حد آستانه برای مقایسه خروجی فیلتر منطبق مشخص می‌شود. برای محاسبه احتمال آشکارسازی از این حد آستانه استفاده می‌شود. در این دو شکل احتمال آشکارسازی برای هدف ساده و هدف دارای اعوجاج رایلی کشیده شده است. اعوجاج هدف باعث می‌شود که احتمال آشکارسازی در فیلتر منطبق به شدت افت کند.

۴-روش پیشنهادی برای آشکار کردن هدف دارای اعوجاج

تبدیل فوریه سریع (FFT[3]) یکی از مهم‌ترین الگوریتم‌های مورد استفاده در پردازش سیگنال و تحلیل داده است. در واقع FFT یک الگوریتم است که برای محاسبه تبدیل فوریه گسسته و نیز معکوس آن مورد استفاده قرار می‌گیرد. در این بخش الگوریتمی برای آشکارسازی اهداف متموج پیشنهاد می‌شود که برای سیگنال‌های OFDM پیاده‌سازی می‌شود. بار محاسباتی کمتری نسبت به فیلتر منطبق و

[1] Pulse Repetition Interval
[2] Chi-square
[3] Fast Fourier Transform

عملکرد بسیار بهتری دارد. تحلیل فوریه می‌تواند یک سیگنال از حوزه اصلی، که معمولا زمان یا فضا است را به نمایشی در حوزه فرکانس و نیز بلعکس تبدیل کند. تبدیل فوریه گسسته از طریق تجزیه دنباله مقادیر، به عناصر با فرکانس‌های متفاوت محاسبه می‌شود. این تبدیل در بسیاری از رشته‌ها مفید است، اما مشکلی که وجود دارد این است که محاسبه مستقیم این تبدیل با استفاده از تعریف آن بسیار کند است و در عمل کاربردی ندارد. تبدیل فوریه سریع یا FFT روشی است که به وسیله آن می‌توان تبدیل فوریه گسسته را به سرعت محاسبه کرد.

در [۱۲] روشی برای پیاده‌سازی فیلتر منطبق طبق (۴) ارائه شده است و این روش برای سیگنال OFDM به کار برده می شود. این روش که در شکل (۵) به خوبی نشان داده شده است عملکردی کاملا مشابه با فیلتر منطبق دارد. بر اساس [۱۲]، برای محاسبه خروجی فیلتر منطبق در هر زمان نمونه‌برداری، بر روی NPM نمونه آخر پردازشی انجام می‌شود؛ که در آن N یک عدد طبیعی است. بدین ترتیب که NPM نمونه آخر به M قسمت که هر کدام دارای NP نمونه هستند تقسیم می‌شوند.

$$[x[n-NPM+1]x[n-NPM+2]\dots x[n]] = [x_1 x_2 \dots x_M] \quad (۱۰)$$

که در آن

$$X_i = [x[n-(M-i+1)NP+1] \; x[n-(M-i+1)NP+2] \; \dots x[n-(M-i+1)NP+NP] \quad (۱۱)$$

سپس بر روی هر کدام از نمونه‌ها به طول NP مطابق شکل (۵) یک FFT با طول NP گرفته می‌شود.

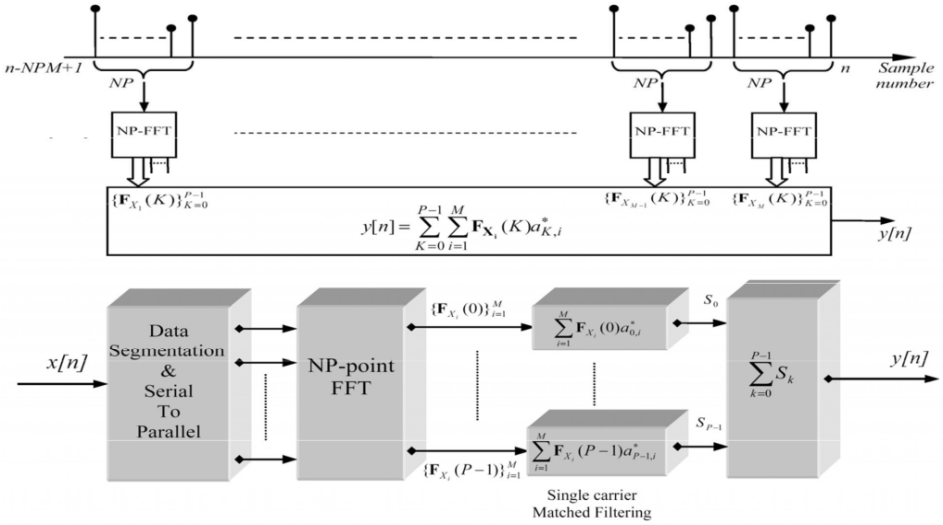
$$F_{X_I} = FFT(X_i) \quad (۱۲)$$

P خروجی اول FFTها بیانگر اطلاعات مدوله شده روی هر یک از حامل‌ها (در صورت صحیح بودن عدد N) می‌باشد. سپس اطلاعات دمدوله شده از هر حامل به فیلتر منطبقی که مبتنی بر کد مدوله شده روی هر حامل می‌باشد عبور داده می‌شود یا به عبارتی عملیات فشرده‌سازی روی هر کانال فرکانسی به صورت مجزا انجام می‌پذیرد.

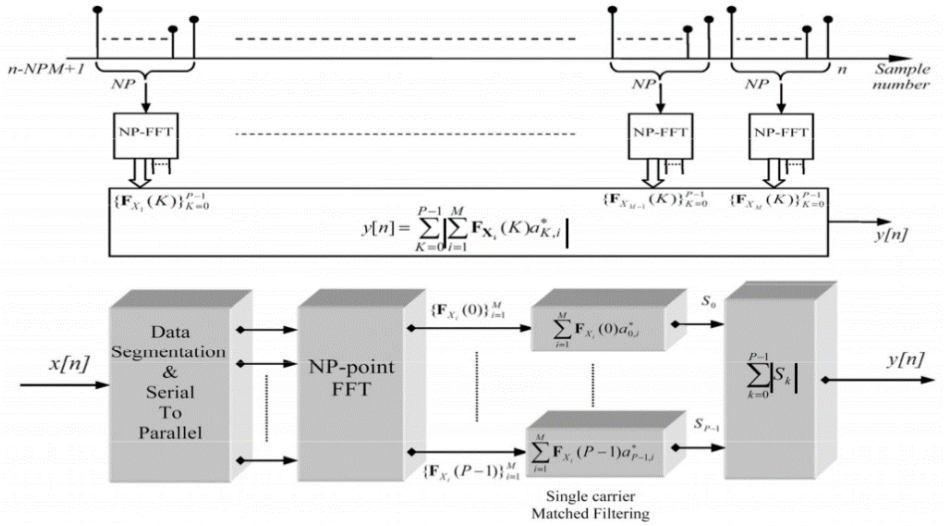
$$S_P = \sum_{i=1}^{M} Fx_i(P) a_{p,i}^* \quad (۱۳)$$

در نهایت اطلاعات کانال‌های مختلف با هم‌دیگر جمع می‌شوند تا خروجی نهایی در لحظه nام حاصل گردد.

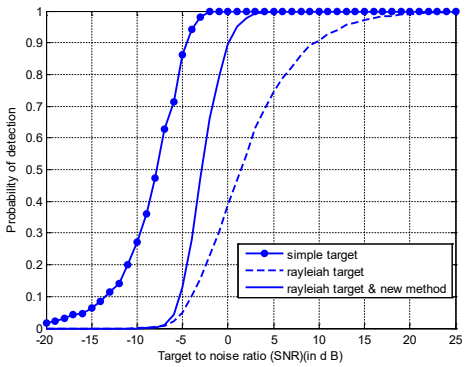
$$y[n] = \sum_{p=1}^{p} S_p \quad (۱۴)$$



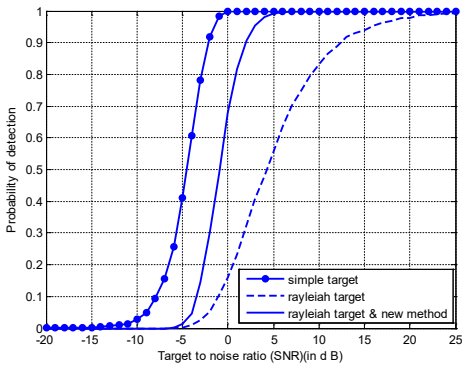
شکل (۵): شمای فیلتر منطبق برای فشرده کردن سیگنال OFDM



شکل (۶): شمای الگوریتم پیشنهادی برای فشرده کردن سیگنال OFDM



شکل (۷): افزایش احتمال آشکارسازی برای $p_{fa} = 10^{-2}$



شکل (۸): افزایش احتمال آشکارسازی برای $p_{fa} = 10^{-4}$

جدول (۱): بهبود در SNR برای الگوریتم پیشنهادی در مقایسه با فیلتر منطبق برای $p_{fa} = 10^{-2}$

احتمال آشکار سازی هدف	SNR(dB)	
	فیلتر منطبق	الگوریتم ارائه شده
۰.۹	۹	۰
۰.۸	۷	-۱
۰.۷	۴	-۲
۰.۵	۲	-۳
۰.۳	-۱	-۴

جدول (۲): بهبود در SNR برای الگوریتم پیشنهادی در مقایسه با فیلتر منطبق برای $p_{fa} = 10^{-4}$

احتمال آشکار سازی هدف	SNR(dB)	
	فیلتر منطبق	الگوریتم ارائه شده
۰.۹	۱۲.۵	۲
۰.۸	۹	۱
۰.۷	۷	۰
۰.۵	۴	-۱
۰.۳	۲	-۲

این عمل به صورت لغزنده و پی‌درپی برای سایر لحظات زمانی (n) هم انجام می‌شود. اگر الگوریتم فوق را برای یک سیگنال OFDM به کار ببریم، نتیجه عیناً با فیلتر منطبق یکسان خواهد بود. برای اهدافی که اعوجاج رایلی دارند اگر به جای جمع SPها در (۱۴) مطابق شکل (۶) قدر مطلق آن‌ها با هم جمع شوند، نتیجه بهتری بدست می‌آید.

$$y[n] = \sum_{P=1}^{P} |S_P| \qquad (۱۵)$$

شکل‌های (۷-۸) احتمال آشکار کردن هدف را به عنوان تابعی از SNR نشان می‌دهند. همانطور که دیده می‌شود روش پیشنهادی این مقاله عملکردی به مراتب بهتر نسبت به فیلتر منطبق دارد. ویژگی مهم روش پیشنهادی جهت آشکارسازی اهداف رایلی این است که اولاً عملکرد بسیار بهتری نسبت به فیلتر منطبق دارد و ثانیاً بار محاسباتی آن کمتر از روش فیلتر منطبق است. همانطور که گفته شد در این روش امکان تخمین کانال و استفاده از آن جهت مدیریت جدول توان در شرایط وجود تموج وابسته به فرکانس اهداف ایجاد می‌شود. جداول (۲-۱) نشان می‌دهند که برای داشتن احتمال آشکارسازی یکسان برای هدف متوج، فیلتر منطبق به چه اندازه به SNR بیشتری نسبت به روش ارائه شده در این مقاله نیاز دارد.

۵-نتیجه گیری

در این مقاله پس از معرفی سیگنال‌های OFDM جهت استفاده در رادار و بیان روش مرسوم فیلتر منطبق در آشکارسازی اهداف برای این رادار، نشان داده شد که فیلتر منطبق برای اهداف با تموج رایلی عملکرد بسیار پایینی دارد؛ سپس برای چنین اهدافی روشی جدید معرفی شد. این روش به جای کل سیگنال OFDM بر روی حامل‌های سیگنال OFDM پردازش انجام می‌دهد. پیاده‌سازی الگوریتم ارائه شده مبتنی بر FFT و جداسازی سیگنال کانال‌های فرکانسی مختلف می‌باشد و نسبت به فیلتر منطبق منجر به بهبود چشم‌گیر عملکرد رادار در آشکارسازی اهداف می‌شود. همچنین بار محاسباتی روش جدید از فیلتر منطبق کمتر است. در راستای زمینه‌های کاری در آینده می‌توان تاثیر تنوع فرکانسی و یا اثر افزایش تعداد پالس‌ها یا زمان مشاهده هدف را بر روی عملکرد آشکارسازی بررسی کرد. آشکارسازی در رادارهای OFDM زمینهٔ نو بنیادی می‌باشد و فضای مناسبی برای انجام کارهای تحقیقی و نوآوری را در اختیار پژوهشگر قرار می‌دهد. طراحی انواع آشکارسازها در حضور کلاترها با توزیع های مختلف می‌تواند زمینه خوبی برای کارهای تحقیقاتی باشد. به خصوص با ارائه مدل‌های سیگنالینگ جدید برای سیگنال OFDM می‌توانند جایگاه خود را خیلی سریع در بین محققین این زمینه پیدا کنند. همانطور که می‌دانیم یک محیط چندمسیری، به عنوان مثال یک محیط شهری تنها بازتاب‌های چند مسیری خاصی را شامل نمی‌شود بلکه انکسارها و میرایی هایی وابسته به لبه‌های تیز و گوشه‌های ساختمان و یا پشت بام‌ها نیز به‌وجود خواهد آمد. بنابراین وارد کردن این رفتارهای فیزیکی اساسی در مدل سیگنال به عنوان یک پدیده حقیقی امکان‌پذیر بسیار مهم خواهد بود. بنابراین در آینده برای حقیقی‌تر کردن پدیده‌های فیزیکی موجود در محیط، می‌توان مدل ارایه شده در این مقاله را گسترش داد و ساختار آشکارساز معادل با این مدل را بیان کرد. برای طراحی سیگنال‌های حقیقی‌تری که در کاربردهای راداری مناسب هستند، می‌توان محدودیت‌هایی در مساله بهینه‌سازی شکل موج اعمال کرد از جمله طراحی شکل موج وفقی و استفاده همزمان آن در آشکارسازی اهداف. تحت هر کدام از این شرایط، در صورت وجود

می‌توان ساختار آشکارساز معادل سیگنال طراحی شده را به‌دست آورد و عملکرد آن را تحت هر کدام از سناریوهای مذکور بیان کرد.

مراجع

[1] M. Mirabella, P.D. Viesti, A. DavolGiorgio, M. Vitetta" Deterministic Signal Processing Techniques for OFDM-Based Radar Sensing: An Overview", IEEE Access , Vol. 11, pp. 68872 – 68889, July.2023. doi: 10.1109/ACCESS.2023.3292937

[2] Li, Hao. Principle of OFDM and multi-carrier modulations. In *Encyclopedia of Wireless Networks*, pp. 1093-1097. Cham: Springer International Publishing, 2020. doi: https://doi.org/10.1007/978-3-319-78262-1_164

[3] Kawon Han, Seonghyeon Kang, Songcheol Hong, "Sub-Nyquist Sampling OFDM Radar", *IEEE Transactions on Radar Systems*, vol. 1, pp. 669-680, Nov. 2023. doi: 10.1109/TRS.2023.3333430

[4] J. T. Rodriguez, F. Colone, and P. Lombardo," Supervised Reciprocal Filter for OFDM radar signal processing," IEEE Transactions on Aerospace and Electronic Systems, vol. 59, no. 4, August 2023.doi: 10.1109/TAES.2023.3235317

[5] B. Nuss, J. Mayer, S. Marahrens, T. Zwick "Frequency comb OFDM radar system with high range resolution and low sampling rate" IEEE Transactions on Microwave Theory and Techniques, Vol.68, Issue: 9, pp. 3861 - 3871 Sep. 2020. doi: 10.1109/TMTT.2020.2988254

[6] G. Liu, Y. Wang, W. Yang "Radar Sensor and Data Communication System Based on OFDM Without Cyclic Prefix" IEEE Sensors Journal, Vol. 23, Issue: 7, pp. 7578-7590 April 2023. doi: 10.1109/JSEN.2022.3229034

[7] A. Coluccia, A. Fascista, G. Ricci" Robust CFAR Radar Detection Using a K-nearest Neighbors Rule" IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2020. doi: 10.1109/ICASSP40776.2020.9054283

[8] Y. RAO, H. HE, X. WAN, J. YI" Range-Angle Dependent Beampattern Synthesis Method for OFDM-Based Passive Radar" Wuhan Univ. J. Nat. Sci.Volume 27, Number 3, 2022. doi: https://doi.org/10.1051/wujns/2022273255

[9] S. Sen and A. Nehorai," Sparsity-based multi-target tracking using OFDM radar," IEEE Trans. Signal Process., vol. 59, no. 4, pp.1902-1906, Apr. 2011. doi: 10.1109/TSP.2010.2103064

[10] A. F. Molisch, *Wideband Wireless Digital Communications*. Upper Saddle River, NJ: Prentice-Hall PTR, 2001.

[11] Peng Yuan, Zulin Wang, Qin Huang, Yuanhan Ni, "Integrated Sensing and Communications System With Multiple Cyclic Prefixes", *IEEE Communications Letters*, vol.27, no.8, pp.2043-2047, 2023. doi: 10.1109/LCOMM.2023.3286985

[12] G. Morris, and L. Harkness, Airborne Pulse Doppler Radar, 2nd ed. Artech House,1996.

Journal of Circuits, Data and Systems Analysis (JCDSA)

Volume 2, Issue 3, Autumn 2024

Papers List

Journal of Circuits, Data and Systems Analysis (JCDSA)

Editorial Board

Islamic Azad University , Shiraz Branch
Journal of Circuits, Data and Systems Analysis

نشریه تحلیل مدارها، داده ها و سامانه ها

Journal of Circuits, Data & Systems Analysis