دوره هجدهم، شماره تابستان ۱۴۰۴

مجله فناوری اطلاعات در طراحی مهندسی

Information Technology in Engineering Design

http://sanad.iau.ir/journal/ited

رمزنگاری تصاویر پزشکی DICOM برای افزایش امنیت و جلوگیری از تغییر و دسترسی غیرمجاز به این تصاویر

محمد سلطانی[۱] حسن شاکری*[۲] محبوبه هوشمند[۳]

(۱) گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

(۲) گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران*

(۳) گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

(تاریخ دریافت: ۱۴۰۴/۰۲/۱۷ تاریخ پذیرش: ۱۴۰۴/۰۴/۱۸)

چکیده

در عصر مدرن، سیستم‌های اطلاعات سلامت و پرونده‌های الکترونیکی سلامت باید به‌عنوان ابزارهایی برای بهبود امنیت مدیریت داده‌های سلامت در برابر حملات سایبری مورد توجه قرار گیرند. اطلاعات پزشکی، از جمله پرونده‌های الکترونیکی سلامت، از طریق شبکه‌ای باز منتقل می‌شوند. یکی از فناوری‌های مورد استفاده برای محافظت از تصاویر پزشکی، رمزنگاری است. در این مقاله، یک الگوریتم رمزنگاری ترکیبی کارآمد برای امنیت تصاویر دیجیتال و ارتباطات پزشکی در حوزه سلامت پیشنهاد شده است. الگوریتم پیشنهادی از یک الگوریتم هوش مصنوعی و الگوریتم رمزنگاری نقشه لجستیک سه‌بعدی استفاده می‌کند. در این الگوریتم، پیش از دریافت تصویر DICOM بیمار، ابتدا اطلاعات بیومتریک بیمار توسط هوش مصنوعی ارزیابی می‌شود و در صورتی که اطلاعات بیومتریک دریافتی صحیح باشد، در مراحل بعدی تصویر DICOM با استفاده از الگوریتم رمزنگاری نقشه لجستیک سه‌بعدی رمزگذاری می‌شود. علاوه بر این، برای افزایش امنیت، در رمزنگاری هر تصویر DICOM، تمامی کلیدهای رمزگذاری و رمزگشایی در تمامی مراحل، به اطلاعات بیومتریک بیمار مانند اثر انگشت یا عنبیه چشم وابسته هستند. براساس نتایج به‌دست‌آمده از الگوریتم پیشنهادی، حداکثر آنتروپی ۷/۹۹۹۸، مقدار NPCR برابر ٪۹۹/۹۹۸، مقدار UACI برابر ٪۳۶/۱۷، فضای کلید بیشتر از $۱۰^{۱۵۰}$ و همبستگی غیر صفر به دست آمده است. همچنین استفاده از اطلاعات بیومتریک بیمار، نشان‌دهنده‌ی مقاومت بالای الگوریتم در برابر حملات جست‌وجوی فراگیر است.

کلمات کلیدی: امنیت، DICOM، رمزنگاری با استفاده از نقشه لجستیک سه بعدی، اطلاعات بیومتریک بیمار، امضای دیجیتال

*عهده‌دار مکاتبات:

حسن شاکری

نشانی: گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

پست الکترونیکی: hassanshakeri@iau.ac.ir

۱- مقدمه

امنیت اطلاعات نقش مهمی در ایمن‌سازی مدیریت داده‌های سلامت ایفا می‌کند [1-3]. سوابق پزشکی مانند تصاویر DICOM[۱] بسیار حساس هستند و از فناوری‌های مختلف تصویربرداری مانند اشعه ایکس معمولی، تصویربرداری فراصوت، توموگرافی کامپیوتری محوری[۲]، ماموگرافی دیجیتال، تصویربرداری با گسیل پوزیترون[۳] و تصویربرداری تشدید مغناطیسی[۴] تولید می‌شوند. برای انجام تشخیص دقیق، لازم است تصاویر DICOM از آسیب‌های بصری و تشخیص‌های نادرست محافظت شوند [5,4]. بر اساس شکل ۱، طرح‌های رمزنگاری نقش کلیدی در ایجاد امنیت برای مدیریت داده‌های مربوط به سلامت[۵] دارند [1-3]. در این مقاله، یک الگوریتم رمزنگاری ترکیبی و مقاوم جدید مبتنی بر کلیدهای متقارن و الگوریتم‌های رمزنگاری برای افزایش امنیت و جلوگیری از دسترسی غیرمجاز به محتوای DICOMهای رمزنگاری‌شده پیشنهاد شده است.

برخی از ویژگی‌های الگوریتم پیشنهادی عبارت‌اند از:

استفاده از هوش مصنوعی[۶] در گام نخست رمزنگاری برای تأیید اعتبار اطلاعات بیومتریک،

در گام بعدی استفاده از الگوریتم رمزنگاری نگاشت لجستیک سه‌بعدی[۷] و بهره‌گیری از اطلاعات بیومتریک بیمار برای ساخت کلید این الگوریتم،

وابستگی تمامی کلیدها به اطلاعات بیومتریک بیمار مانند اثر انگشت یا عنبیه چشم،

استفاده از عملیات XOR برای وابسته‌سازی کلیدها به اطلاعات بیومتریک بیمار و ایجاد کلیدهای منحصر به‌فرد پس از فرایند رمزنگاری، و استفاده از امضای دیجیتال[۸] برای تأیید اصالت DICOMهای رمزگشایی‌شده.

ساختار ادامه مقاله بدین شرح است:

در بخش ۲، پیشینه تحقیق در مورد الگوریتم‌های رمزنگاری تصاویر و در بخش ۳، ادبیات تحقیق مطرح گردیده است. در بخش ۴ الگوریتم پیشنهاد داده شده در این مقاله توضیح داده شده است. در بخش ۵ مهم‌ترین پارامترها در ارزیابی الگوریتم‌های رمزنگاری توضیح داده شده است و در بخش ۶ الگوریتم رمزنگاری پیشنهاد داده شده مورد ارزیابی

---

۱ Digital Imaging and Communications in Medicine (DICOM)

۲ Computed Tomography (CT)

۳ Positron Emission Tomography (PET)

۴ Magnetic Resonance Imaging (MRI)

۵ Healthcare Data Management (HDM)

۶ Artificial Intelligence (AI)

۷ 3D Logistic Map

۸ Digital Signature Algorithm (DSA)

و تحلیل قرار گرفته است و در انتها در بخش نتیجه‌گیری، مهم‌ترین نتایج بدست آمده در این کار تحقیقاتی بیان شده است.

۲- کارهای مرتبط

طبقه‌بندی مقالات مربوط به فناوری‌های امنیتی برای تصاویر پزشکی بر پایه عوامل زیر تعیین می‌شود:

شکل ۱: طبقه‌بندی مقالات مربوط به الگوریتم‌های افزایش امنیت برای تصاویر پزشکی [6]

در ادامه تعدادی از مقالات بر اساس نوع الگوریتم‌های مورد استفاده برای رمزنگاری گروه‌بندی شده‌اند.

- **الگوریتم‌های نگاشت آشوب[۱]**

این مقالات از سیستم‌های آشوبناک برای رمزگذاری تصاویر پزشکی استفاده می‌کنند.

در [7]، با به‌کارگیری نگاشت سه‌بعدی آشوبی Chen، تکنیک جابجایی و پراکندگی پیکسل‌ها را در تصاویر DICOMبه‌کار گرفته‌اند که منجر به افزایش مقاومت در برابر حملات متن آشکار منتخب شده است.

در [8]، یک الگوریتم رمزنگاری برای رمزنگاری تصاویر پزشکی DICOM مطرح شده است. در الگوریتم مطرح شده از ترکیب پیکسل‌ها به شکل بیت به بیت استفاده شده است.

[۱] Chaos-Based Algorithms

همچنین در [5]، الگوریتمی برای رمزنگاری تصاویر پزشکی پیشنهاد داده‌اند که از ترکیب روش مربع لاتین و سیستم آشوبی بهره می‌برد. دو تکنیک اصلی در این پژوهش شامل انتشار تطبیقی دوسویه و جایگشت مبتنی بر مربع‌های لاتین است.

با توجه به اهمییت امنیت داده‌ها در [4]، روشی ترکیبی از نظریه اعداد و نگاشت آشوبی Henon برای رمزنگاری تصاویر DICOM معرفی کرده‌اند. در این طرح، با جابه‌جایی ماتریس‌های کلید و کنترل آشوب توسط نگاشت Henon، امنیت سیستم افزایش یافته است.

در [9]، الگوریتمی برای رمزنگاری تصاویر رنگی ارائه داده‌اند که مبتنی بر نگاشت غیرخطی آشوبی دوبعدی است و ویژگی‌هایی نظیر حساسیت بالا، امنیت زیاد و سرعت مناسب را داراست.

در بسیاری از الگوریتم‌های رمزنگاری تصاویر پزشکی، از نگاشت‌های آشوبی چندبعدی با سه یا چهار متغیر جهت تغییر مقادیر پیکسلی استفاده می‌شود. این تکنیک سطح امنیت را افزایش می‌دهد، اما در مقابل، پیچیدگی الگوریتم و هزینه محاسباتی آن نیز بیشتر می‌شود.

با توجه به اهمییت رمزنگاری در [10]، الگوریتمی ترکیبی از نگاشت لجستیک و Chebyshev برای رمزنگاری تصاویر پزشکی توسعه داده‌اند. در این الگوریتم، ابتدا رمزنگاری اولیه تصویر با استفاده از نگاشت لجستیک و سپس رمزنگاری ثانویه با نگاشت Chebyshev انجام می‌شود. این رویکرد فضای کلید گسترده و امنیت بالایی در فرآیند انتقال اطلاعات فراهم می‌سازد.

در [11]، یک روش رمزنگاری تصویر بر پایه ترکیب سه نگاشت آشوبی یک‌بعدی پیشنهاد شده که نسبت به روش‌های معمول، هم امنیت بیشتری دارد و هم از پیچیدگی محاسباتی کمتری برخوردار است.

در [12]، الگوریتمی رمزنگاری‌شده با استفاده از نگاشت‌های آشوبی شامل لجستیک، چادر و علامت برای افزایش امنیت در کاربردهای تصویربرداری پزشکی بلادرنگ پیشنهاد کرده‌اند. نتایج نشان می‌دهد که این نگاشت‌ها می‌توانند امنیت چنین سامانه‌هایی را به‌طور مؤثری افزایش دهند.

همچنین در [13]، روش رمزنگاری جدیدی برای تصاویر DICOM توسعه داده‌اند که در آن از سیستم آشوبی به همراه کلید مخفی پویا استفاده شده است.

- **الگوریتم (DNA)[1]**

[1] Deoxyribonucleic acid

این روش‌های رمزنگاری از رویکردهای مبتنی بر توالی DNA در ترکیب با تکنیک‌های دیگر مانند سیستم‌های آشوبناک استفاده می‌کنند. در ادامه در مقالات گفته شده از الگوریتم DNA برای رمزنگری تصاویر DICOM استفاده شده است.

در [14]، یک روش رمزنگاری تصویر پزشکی ارائه شده است که بر پایه‌ی ترکیب چند سیستم آشوبی، توابع هش MD5، الگوریتم‌های رمزنگاری DNA و عملیات جبری XOR طراحی شده است. این ترکیب موجب می‌شود که وابستگی تصویر به کلید رمز به‌صورت جزئی افزایش یابد.

در [15]، یک الگوریتم رمزنگاری تصویر پزشکی بر اساس ترکیب نگاشت‌های آشوبی و DNA ارائه کرده‌اند که باعث افزایش مقاومت الگوریتم در برابر تحلیل‌های آماری شده است.

با توجه به مطالعات انجام داده شده در [16]، از روشی مبتنی بر رمزنگاری DNA و نگاشت دوگانه ابرآشوبی برای رمزنگاری تصاویر پزشکی استفاده کرده‌اند. در این روش، فرآیند جایگشت تنها بر تعداد محدودی از پیکسل‌های انتخاب‌شده از تصویر دیجیتال پزشکی اعمال می‌شود.

در [17]، الگوریتمی برای رمزنگاری تصاویر مبتنی بر ضرب ماتریسی و الگوریتم DNA مطرح شده است. این الگوریتم از ساختار ساده‌ای برخوردار بوده و سطح امنیتی بالایی دارد.

با توجه به مطالعات انجام داده شده در [18]، از توالی‌یابی DNA و سیستم آشوبی برای رمزگذاری زیرتصاویر بهره برده‌اند. روش رمزنگاری مبتنی بر آشوب در این پژوهش، گزینه‌ای ایده‌آل برای رمزنگاری تصاویر پزشکی در دستگاه‌های هوشمند به‌حساب می‌آید، چرا که علاوه بر امنیت بالا، از سرعت پردازشی مناسبی نیز برخوردار است.

در نهایت، در [19]، روشی برای رمزنگاری تصاویر دیجیتال پزشکی پیشنهاد کرده‌اند که بر پایه‌ی ترکیب تبدیل موجک عددی، سیستم‌های آشوبی و DNA بنا شده است. این روش سطح بالایی از امنیت را در انتقال تصاویر پزشکی تضمین می‌کند.

- **درهم‌آمیختگی و پراکندگی پیکسل**[1]

در [20]، الگوریتمی برای رمزنگاری تصاویر DICOM ارائه کرده‌اند که با رویکردی نوین، فرآیند رمزنگاری را در سطح صفحات بیتی انجام می‌دهد. در این روش، تعیین تعداد صفحات بیت نه بر اساس پیکسل‌ها، بلکه بر اساس ویژگی‌های ذاتی بیت‌های ذخیره‌شده صورت می‌گیرد که باعث افزایش کارایی سیستم می‌شود.

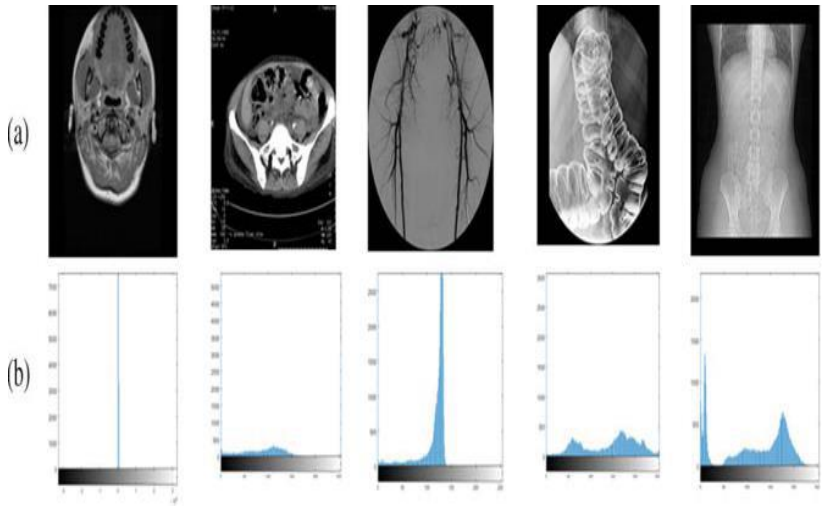
[1] Pixel Scrambling and Diffusion

۳- ادبیات تحقیق

ادبیات تحقیق بر اساس موارد زیر تعریف می‌شود:

DICOM -۱-۳

DICOM استانداردی برای مدیریت و تبادل اطلاعات تصویربرداری پزشکی و داده‌های مرتبط با آن است. این استاندارد بیش‌تر برای ذخیره‌سازی و انتقال تصاویر پزشکی مانند عکس‌های رادیولوژی[۱]، سی‌تی اسکن، سونوگرافی، پرتودرمانی و تصویربرداری تشدید مغناطیسی مورد استفاده قرار می‌گیرد [14,4]. در شکل شماره ۲ چند نمونه از تصاویر پزشکی DICOM و هیستوگرام هر یک از تصاویر نشان داده شده است.



شکل ۲: چند نمونه از تصاویر پزشکی DICOM و هیستوگرام هر یک از تصاویر [6].

۳-۲- اطلاعات بیومتریک

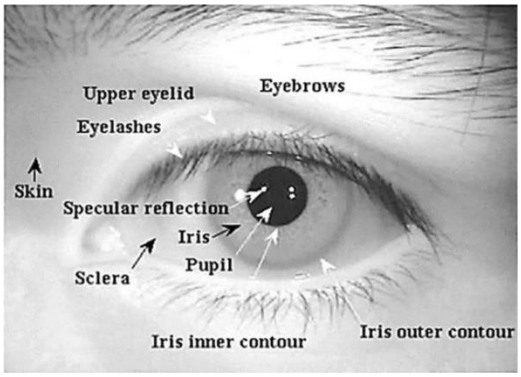
بیومتریک‌ها ویژگی‌های فیزیکی یا رفتاری انسان هستند که می‌توان از آن‌ها برای شناسایی دیجیتالی افراد و اعطای دسترسی به سامانه‌ها، دستگاه‌ها یا داده‌ها استفاده کرد. اطلاعات بیومتریک، مانند اثر انگشت، می‌تواند منحصربه‌فرد برای هر فرد تلقی شود [21-23]. اثر انگشت به‌عنوان یک سامانه‌ی شناسایی بیومتریک موفق شناخته شده و در حوزه‌های متنوعی کاربرد یافته است [23].

[۱] X-ray

عنبیه نیز به‌عنوان یک ویژگی بیومتریک منحصربه‌فرد و قدرتمند در نظر گرفته می‌شود که می‌توان از آن به‌عنوان عاملی برای احراز هویت بهره گرفت. حفاظت از محرمانگی نمونه‌ی عنبیه‌ی هر فرد، یک ضرورت فوری محسوب می‌شود [24].

در شکل شماره ۳ و ۴ نمونه تصاویر اثر انگشت و عنبیه چشم نشان داده شده است.

شکل ۳: نمونه تصویر اثر انگشت [23]



شکل ۴: نمونه تصویر عنبیه چشم [25-26]

۳-۲-۱- مهم‌ترین علت‌های استفاده از اطلاعات بیومتریک بیمار

در ساختار الگوریتم ترکیبی پیشنهاد داده شده، کلیدها به اطلاعات بیومتریک بیمار وابسته می‌شوند. مهمترین ویژگی-ها و علت‌های استفاده شده برای هر یک از اطلاعات بیومتریک اثر انگشت و عنبیه چشم در موارد ذیل تقسیم بندی می‌شوند.

- **مهم‌ترین ویژگی‌های تصویر اثر انگشت در موارد ذیل تقسیم بندی می‌شوند** [32-26,24,23,21]:

۱- منحصربه‌فرد بودن[۱]: هر فرد دارای الگوی اثر انگشت یکتایی است که حتی در دوقلوهای همسان نیز متفاوت است. این ویژگی باعث می‌شود اثر انگشت به‌عنوان یک ابزار مطمئن برای شناسایی فردی مورد استفاده قرار گیرد.

۲- ثبات در طول زمان[۲]: الگوهای اثر انگشت از زمان تولد تا مرگ تغییر نمی‌کنند، مگر در صورت وقوع آسیب‌های شدید فیزیکی. این پایداری، اثر انگشت را برای شناسایی بلندمدت مناسب می‌سازد.

۳- قابلیت جمع‌آوری آسان[۳]: اثر انگشت به‌راحتی و با استفاده از اسکنرهای مخصوص قابل جمع‌آوری است که این امر فرایند احراز هویت را سریع و کارآمد می‌کند.

۴- تراکم خطوط[۴]: تعداد خطوط برجسته در یک ناحیه مشخص از اثر انگشت می‌تواند در شناسایی فرد مؤثر باشد. تراکم خطوط در افراد مختلف متفاوت است و می‌تواند به‌عنوان یک ویژگی تمایزدهنده استفاده شود.

۵- فاصله بین خطوط[۵]: فاصله بین خطوط برجسته اثر انگشت نیز می‌تواند به‌عنوان یک ویژگی فیزیکی مهم در شناسایی فرد به کار رود. این فاصله‌ها در هر فرد منحصربه‌فرد هستند.

۶- نقاط ویژگی[۶]: نقاطی مانند پایان خطوط[۷] و انشعابات[۸] که در اثر انگشت وجود دارند، به‌عنوان نقاط ویژگی شناخته شناخته می‌شوند و در فرایند تطبیق اثر انگشت نقش اساسی دارند.

۷- قابلیت تشخیص زنده‌بودن[۹]: تشخیص زنده‌بودن اثر انگشت برای جلوگیری از حملات جعل اهمیت دارد. روش‌های مبتنی بر یادگیری عمیق برای بهبود دقت در تشخیص زنده‌بودن اثر انگشت توسعه یافته‌اند.

۸- قابلیت استفاده در سطوح مختلف: اثر انگشت می‌تواند بر روی سطوح مختلفی مانند شیشه، فلز و پلاستیک باقی بماند که این ویژگی در تحقیقات جنایی و شناسایی افراد مفید است.

- **مهمترین ویژگی‌های تصویر عنبیه چشم در موارد ذیل تقسیم‌بندی می‌شوند** [35-33,28,26,25]:

[۱] Uniqueness
[۲] Permanence
[۳] Collectability
[۴] Ridge Density
[۵] Ridge Spacing
[۶] Minute Points
[۷] Ridge endings
[۸] Bifurcations
[۹] Liveness detection

۱- منحصربه‌فرد بودن: الگوی عنبیه در هر فرد یکتا است و حتی در دوقلوهای همسان نیز تفاوت دارد. این ویژگی باعث می‌شود عنبیه به‌عنوان یک ابزار مطمئن برای شناسایی فردی مورد استفاده قرار گیرد.

۲- ثبات در طول زمان: الگوهای عنبیه در طول زندگی فرد تغییر نمی‌کنند که این پایداری، عنبیه را برای شناسایی بلندمدت مناسب می‌سازد.

۳- پیچیدگی ساختاری[۱]: ساختار پیچیده و الگوهای فراوان در عنبیه، امکان استخراج ویژگی‌های متنوع و دقیق را فراهم می‌کند که در افزایش دقت سیستم‌های شناسایی مؤثر است.

۴- عدم تأثیرپذیری از عوامل خارجی: عنبیه کمتر تحت‌تأثیر عوامل خارجی مانند سن، بیماری‌ها یا شرایط محیطی قرار می‌گیرد که این امر قابلیت اطمینان آن را افزایش می‌دهد.

۵- قابلیت تشخیص از فاصله دور: با استفاده از دوربین‌های با رزولوشن بالا و تکنیک‌های پردازش تصویر، می‌توان عنبیه را از فاصله دور تشخیص داد که این ویژگی در کاربردهای امنیتی مفید است.

۶- مقاومت در برابر جعل[۲]: به دلیل ساختار پیچیده و الگوهای منحصربه‌فرد، جعل عنبیه دشوار است و سیستم‌های تشخیص عنبیه معمولاً در برابر حملات جعل مقاوم هستند.

۷- قابلیت ترکیب با سایر اطلاعات بیومتریک: عنبیه می‌تواند با سایر ویژگی‌های بیومتریکی مانند چهره یا اثر انگشت ترکیب شود تا سیستم‌های چندوجهی بادقت بالاتر ایجاد شود.

۸- سرعت بالا در تطبیق[۳]: الگوهای عنبیه به‌گونه‌ای طراحی شده‌اند که فرایند تطبیق و شناسایی با سرعت بالا انجام شود که این امر در کاربردهای زمان‌حساس اهمیت دارد.

۹- عدم نیاز به تماس فیزیکی: تشخیص عنبیه به‌صورت غیرتماسی انجام می‌شود که این ویژگی از نظر بهداشتی و راحتی کاربر مزیت محسوب می‌شود.

۱۰- پایداری در برابر تغییرات فیزیولوژیکی[۴]: الگوهای عنبیه به طور شگفت‌انگیزی در برابر تغییرات فیزیولوژیکی بدن مانند فشارخون، بیماری‌ها، خستگی، یا افزایش سن مقاوم باقی می‌مانند. برخلاف چهره یا صدا که تحت‌تأثیر شرایط روانی یا محیطی تغییر می‌کنند، عنبیه تقریباً بدون تغییر باقی می‌ماند. این ویژگی، پایداری بالایی را برای استفاده بلندمدت در سیستم‌های احراز هویت فراهم می‌کند.

---

[۱] Complexity

[۲] Anti spoofing

[۳] High Matching Speed

[۴] Physiological Robustness

۱۱-قابلیت نرمال‌سازی و مقیاس‌پذیری بالا: الگوهای عنبیه به‌راحتی با استفاده از مدل‌هایی مانند Rubber Sheet Model نرمال‌سازی می‌شوند. این کار باعث افزایش دقت تطبیق و کاهش نرخ خطا در شناسایی می‌شود.

۱۲-مقاومت در برابر نویز محیطی[۱]: عنبیه نسبت به نویزهای محیطی مانند گردوغبار یا نوسانات نور پس‌زمینه حساسیت کمتری دارد. سیستم‌های مدرن با استفاده از فیلترهای چندکاناله یا شبکه‌های عصبی کانولوشنی[۲] این ویژگی را بهبود داده‌اند.

۱۳-وابستگی کم به حالت روانی[۳]: برخلاف چهره یا صدا، الگوی عنبیه تحت‌تأثیر هیجانات روانی، استرس، یا خستگی تغییر نمی‌کند. این ویژگی باعث ثبات بیشتر سیستم‌های بیومتریکی در محیط‌های پر تغییر و بحرانی می‌شود.

۱۴-تنوع بافتی بالا[۴]: عنبیه دارای ساختارهای بسیار متنوعی مانند کریپتاها[۵]، فورک‌ها[۶]، رشته‌ها[۷] و دوایر پیازی‌شکل است. این تنوع بافتی بسیار بالا، باعث افزایش دقت در شناسایی و کاهش نرخ تطابق اشتباه[۸] می‌شود.

۱۵-قابلیت استفاده در شرایط چند طیفی[۹]: برخلاف برخی ویژگی‌های بیومتریک، عنبیه می‌تواند در طیف‌های نوری مختلف (مادون‌قرمز نزدیک، نور مرئی و فرابنفش) تصویربرداری و تحلیل شود. این ویژگی باعث افزایش قابلیت انعطاف و امنیت در کاربردهای حساس مثل امنیت مرزی، تشخیص هویت فرامرزی و دفاعی می‌شود.

۳-۳- استفاده از هوش مصنوعی برای تایید اعتبار اطلاعات بیومتریک

ارزیابی امنیت سایبری و شناسایی جرایم در حوزه‌ی تشخیص اطلاعات بیومتریک با چالش‌های زیادی همراه است. به منظور شناسایی ویژگی‌های منحصربه‌فرد و تمایزدهنده‌ی داده‌های بیومتریک، از روش‌های پیشرفته‌ی هوش مصنوعی مانند SVM[۱۰] و ANFIS[۱۱] استفاده شده است [32]. علاوه بر این الگوریتم‌ها، در [29] نیز الگوریتم‌های دیگری معرفی شده‌اند که با هدف بررسی و تأیید دقت اطلاعات بیومتریک به کار گرفته می‌شوند.

---

۱ Noise Robustness
۲ Convolutional Neural Network
۳ Emotion independence
۴ High Textural Richness
۵ Crypts
۶ Furrows
۷ Striae
۸ False Match Rate
۹ Multispectral Compatibility
۱۰ Support Vector Machine (SVM)
۱۱ Adaptive Neuro-Fuzzy Inference System (ANFIS)

۳-۳-۱- الگوریتم SVM

الگوریتم SVM یک روش قدرتمند برای تأیید هویت از طریق ویژگی‌های بیومتریک مانند اثر انگشت و عنبیه چشم است. این الگوریتم با استفاده از روش‌های پیش‌پردازش تصویر، استخراج ویژگی و یادگیری ماشین می‌تواند افراد را بادقت بالا شناسایی کند. باوجود برخی محدودیت‌ها، در بسیاری از کاربردهای امنیتی و احراز هویت، SVM یکی از انتخاب‌های اصلی محسوب می‌شود [32,29].

۳-۳-۲- الگوریتم ANFIS

الگوریتم ANFIS یک روش قدرتمند و تطبیقی برای تأیید اعتبار اطلاعات بیومتریک است که با ترکیب هوش مصنوعی و منطق فازی، دقت بالایی در شناسایی افراد ارائه می‌دهد. این روش قابلیت یادگیری و بهینه‌سازی خودکار دارد که آن را به گزینه‌ای مناسب برای سیستم‌های امنیتی و احراز هویت تبدیل کرده است [32,29].

۳-۳-۳- مقایسه دقیق الگوریتم‌های تایید اعتبار ANFIS و SVM

در سیستم‌های تأیید اعتبار بیومتریک، انتخاب الگوریتم مناسب تأثیر زیادی بر دقت، سرعت و امنیت دارد. دو الگوریتم پرکاربرد در این حوزه، SVM و ANFIS هستند که هر یک ویژگی‌های خاص خود را دارند. در جدول ۱، مقایسه دقیقی بین این دو الگوریتم ارائه می‌شود.

جدول ۱: مقایسه دقیق الگوریتم‌های تأیید اعتبار ANFIS و SVM [36,32,29]

ویژگی	ANFIS	SVM
نوع الگوریتم	ترکیبی از شبکه عصبی و منطق فازی.	یادگیری ماشین نظارت‌شده.
نحوه عملکرد	استفاده از توابع عضویت فازی و یادگیری تطبیقی.	یافتن ابرصفحه بهینه برای جداسازی کلاس‌ها.
مدل یادگیری	ترکیبی از قوانین فازی و یادگیری عصبی.	مبتنی بر بردارهای پشتیبان و کرنل‌های مختلف.

توانایی پردازش داده‌های غیرخطی	بسیار بالا، به دلیل استفاده از منطق فازی.	بالا، اما وابسته به انتخاب کرنل مناسب.
سرعت پردازش	کندتر، به دلیل نیاز به پردازش چندلایه‌ای و تنظیم قوانین فازی.	سریع‌تر، مخصوصاً در مجموعه‌داده‌های کوچک تا متوسط.
میزان دقت	بسیار بالا، مخصوصاً در داده‌های پیچیده و نویزی.	بالا، مخصوصاً در داده‌های تفکیک‌پذیر.
نیاز به حجم داده	نیاز به داده‌های زیاد برای تنظیم قوانین فازی.	عملکرد خوب با داده‌های کم تا متوسط.
تفسیرپذیری	بالا، به دلیل استفاده از قوانین فازی که قابل‌فهم هستند.	کم، مدل بیشتر بر اساس محاسبات ریاضی است.
مقاومت در برابر نویز	انعطاف‌پذیر، زیرا فازی‌سازی عدم قطعیت داده‌ها را مدیریت می‌کند.	مقاوم، اما بستگی به پارامترهای داده ورودی دارد.
پیچیدگی پیاده‌سازی	پیچیده‌تر، نیاز به تنظیم دقیق توابع عضویت و قوانین فازی.	ساده‌تر، با استفاده از کتابخانه‌های استاندارد مانند scikit-learn.
مقیاس‌پذیری	پردازش سنگین‌تر برای داده‌های حجیم، اما دقیق‌تر در پردازش‌های پیچیده.	مناسب برای داده‌های کوچک تا متوسط، اما در داده‌های حجیم کند می‌شود
نیاز به سخت‌افزار قوی	بیشتر، به دلیل پیچیدگی محاسباتی بالاتر.	کمتر، قابل‌اجرا روی پردازنده‌های معمولی.
بهترین کاربردها	امنیت پیشرفته با سیستم‌های ترکیبی بیومتریک.	احراز هویت سریع.
محدودیت کلیدی	نیاز به حجم داده بالا، سرعت پردازش پایین‌تر ازSVM.	وابستگی به انتخاب کرنل مناسب، کاهش عملکرد در داده‌های بسیار بزرگ.

۳-۳-۴- انتخاب الگوریتم مناسب برای تایید اعتبار اطلاعات بیومتریک (اثر انگشت و عنبیه چشم) با SVM و ANFIS

انتخاب بین SVM و ANFIS برای احراز هویت اثر انگشت و عنبیه چشم‌بستگی به چندین فاکتور بستگی دارد، از جمله دقت، سرعت پردازش، پیچیدگی داده‌ها، و میزان نویز موجود در تصاویر. در ادامه، بررسی می‌کنیم که کدام الگوریتم برای کدام کاربرد بهتر است.

در جدول ۲ ویژگی‌های تایید هویت از طریق اثر انگشت با استفاده از SVM و ANFIS مقایسه شده است.

جدول ۲: مقایسه دقیق الگوریتم‌های تأیید اعتبار اثر انگشت با استفاده از دو الگوریتم ANFIS و SVM [36,32,29].

معیار	ANFIS	SVM
دقت	بسیار بالا، مخصوصاً برای داده‌های پیچیده و غیرخطی	بالا، به‌ویژه در داده‌های تفکیک‌پذیر
سرعت پردازش	کندتر، به دلیل پردازش قوانین فازی	سریع‌تر، مناسب برای سیستم‌های بلادرنگ

مقاومت در برابر نویز	مقاوم‌تر، چون فازی‌سازی به مدیریت داده‌های نامطمئن کمک می‌کند	مقاوم، ولی به داده رودی بستگی دارد
حجم داده	نیاز به داده‌های بزرگ‌تر برای تنظیم قوانین فازی	بهینه برای داده‌های کم تا متوسط
پیچیدگی پردازش	بیشتر، نیازمند تنظیم توابع عضویت فازی	کمتر، پیاده‌سازی ساده‌تر
بهترین کاربرد	سیستم‌های امنیتی پیشرفته با تحلیل دقیق الگوهای اثر انگشت	سیستم‌های حضوروغیاب، گوشی‌های هوشمند، قفل‌های دیجیتال

در جدول ۳ ویژگی‌های تایید هویت از طریق عنبیه چشم با استفاده از SVM و ANFIS مقایسه شده است.

جدول ۳: مقایسه دقیق الگوریتم‌های تأیید اعتبار عنبیه چشم با استفاده از دو الگوریتم ANFIS و SVM [36,32,29].

معیار	ANFIS	SVM
دقت	بسیار بالا، به دلیل تطبیق بهتر با تغییرات نوری و نویز	بالا، اما ممکن است در شرایط نوری نامناسب افت کند
سرعت پردازش	کندتر، اما دقت بالاتر در شرایط مختلف	سریع‌تر، اما در شرایط پیچیده کارایی آن کاهش می‌یابد
مقاومت در برابر تغییرات محیطی	بالا، زیرا قوانین فازی می‌توانند داده‌های نامطمئن را بهتر پردازش کنند	متوسط، نیاز به پیش‌پردازش بیشتر برای بهبود نتایج
توانایی تشخیص الگوهای پیچیده	بسیار قوی، قادر به تحلیل دقیق‌تر جزئیات عنبیه	وابسته به نوع کرنل، ممکن است برای الگوهای پیچیده محدودیت داشته باشد
حجم داده	نیازمند مجموعه‌داده‌های بزرگ‌تر برای تنظیم بهینه	مناسب برای داده‌های کم تا متوسط
بهترین کاربرد	تحلیل‌های دقیق در سیستم‌های نظامی، امنیتی و بانکی	کاربردهای عمومی مانند سیستم‌های کنترل مرزی، ورود به مکان‌های امنیتی

۳-۴- عملکرد الگوریتم در شرایط استفاده از اطلاعات بیومتریک نویزدار یا نامطمئن

در این الگوریتم باید از اطلاعات بیومتریک مطمئن استفاده کرد و در صورت نامطمئن بودن و نویزدار بودن اطلاعات بیومتریک، می‌توان برای اصلاح کردن این اطلاعات از روش‌های ذیل استفاده کرد [37-46].

- **اصلاح اطلاعات بیومتریک اثر انگشت**

برای اصلاح اطلاعات بیومتریک اثر انگشت دو روش پیشنهاد شده است:

روش اول: فیلتر بانک کمانی گابور[۱] + افزایش کنتراست[۲].

روش دوم: فیلتر بیلاترال[۳] + بازسازی با استفاده از شبکه GAN[۴].

- **اصلاح اطلاعات بیومتریک عنبیه چشم**

برای اصلاح اطلاعات بیومتریک عنبیه چشم دو روش پیشنهاد شده است:

روش اول: تشخیص دایره[۵] + نرمال‌سازی قطبی.

روش دوم: درونیابی تطبیقی + افزایش وضوح.

۳-۵- امضای دیجیتال

الگوریتم DSA نوعی رمزنگاری مبتنی بر کلید نامتقارن است که به‌منظور ایجاد امضای دیجیتال به کار می‌رود [47]. امضای دیجیتال مستقیماً بر متن ساده تأثیری ندارد، بلکه یک روش ریاضی برای تأیید صحت و اصالت پیام‌هایی نظیر متن ساده ایمن یا فایل‌های DICOM محسوب می‌شود. این نوع امضا، سطح بالاتری از امنیت داده را برای فایل‌های DICOM و سایر گزارش‌های پزشکی فراهم می‌سازد. همچنین می‌توان از آن برای احراز هویت فرستنده و گیرنده استفاده نمود.

در فرآیند DSA، به‌کارگیری یک الگوریتم هش نظیر MD5 (الگوریتم خلاصه‌سازی پیام) یا SHA-256 (الگوریتم هش ایمن ۲۵۶ بیتی) ضروری است. فرستنده با استفاده از یک تابع هش، خلاصه‌ای از پیام تولید کرده و آن را با بهره‌گیری از کلیدهای خصوصی و عمومی رمزنگاری کرده، به‌صورت دیجیتال امضا نموده و برای گیرنده ارسال می‌نماید. گیرنده نیز برای اعتبارسنجی امضا، از کلید عمومی فرستنده جهت رمزگشایی استفاده کرده و امضا زمانی معتبر تلقی می‌گردد که مقادیر هش ساخته شده در هر دو سوی ارتباط برابر باشند [48].

---

۱ Gabor filters

۲ Contrast

۳ Bilateral

۴ Generative Adversarial Network

۵ Hough transform

۳-۶- رمزنگاری با استفاده از تابع آشوب لجستیک سه‌بعدی

در تابع لجستیک سه‌بعدی با اعمال شرایط اولیه و پارامترهای مربوط سه دنباله با اعداد تصادفی بین صفر و یک ساخته می‌شود که با بهره‌گیری از آن‌ها رمزنگاری تصویر انجام می‌شود. فضای کلید در بهترین حالت باید از $۱۰^{۳۰}$ بیشتر باشد تا از حملات جستجوی فراگیر جلوگیری کند [50,49]. باید توجه داشت در این الگوریتم پارامترهای x1,y1,z1,alfa,beta,gama به عنوان کلید در نظر گرفته میشوند.

توجه: تابع لجستیک سه‌بعدی به‌صورت زیر تعریف می‌شود و به‌ازای پارامترهای مشخص شده دنباله آشوبی تولید می‌کند [50-52]:

$$\begin{cases} x_{i+1} = \lambda x_i(1-x_i) + \beta {y_i}^2 x_i + \alpha {z_i}^3 & 3.53 < \lambda < 3.81 \\ y_{i+1} = \lambda y_i(1-y_i) + \beta {z_i}^2 y_i + \alpha {x_i}^3 & 0 < \beta < 0.022 \\ z_{i+1} = \lambda z_i(1-z_i) + \beta {x_i}^2 z_i + \alpha {y_i}^2 & 0 < \alpha < 0.015 \end{cases} \quad (1)$$

هرکدام از این کلیدها الگوریتم رمزنگاری لجستیک سه‌بعدی، دارای دقت $۱۰^{۱۴}$ میباشند همچنین پارامتر n که در بخش اول رمزنگاری این الگوریتم استفاده می‌شود دقت $۱۰^{۵}$ دارد در نتیجه فضای کلید به شکل تقریبی در این الگوریتم $۱۰^{۱۵۰}$ خواهد بود [54,53].

۴- الگوریتم پیشنهادی

الگوریتم پیشنهادی بر اساس موارد زیر تعریف می‌شود:

۴-۱- الگوریتم رمزنگاری

طرح رمزنگاری پیشنهادی با هدف تضمین انتقال و ذخیره‌سازی ایمن تصاویر پزشکی، به‌ویژه فایل‌های DICOM، ارائه شده است. این روش با ترکیب اطلاعات بیومتریک خاص هر بیمار و الگوریتم رمزنگاری مبتنی بر نگاشت لجستیک سه‌بعدی، امنیت داده‌ها را افزایش می‌دهد. وجه تمایز این روش در بهره‌گیری از داده‌های بیومتریک نه تنها برای احراز هویت، بلکه برای ساخت کلیدهای رمزنگاری منحصربه‌فرد و ایجاد امضای دیجیتال است. نمودار بلوکی سطح بالا در شکل ۵ ارائه شده‌اند.

این روش شامل مراحل زیر است:

۴-۱-۱- دریافت و اعتبارسنجی اطلاعات بیومتریک

در گام نخست، داده‌های بیومتریک بیمار (مانند اثر انگشت، اسکن عنبیه یا ویژگی‌های چهره) دریافت می‌شود. برای اطمینان از صحت و اعتبار داده‌های دریافتی، از الگوریتم‌های هوش مصنوعی نظیر SVM استفاده می‌شود. این الگوریتم‌ها با شناسایی داده‌های نادرست یا دستکاری‌شده، تنها الگوهای معتبر بیومتریک را وارد فرایند رمزنگاری می‌کنند.

۴-۱-۲- ایجاد امضای دیجیتال

پس از اعتبارسنجی داده‌های بیومتریک، یک تابع هش مانند SHA-256 برای تولید خلاصه‌ای از داده‌ها به کار می‌رود. سپس این مقدار هش با استفاده از کلید خصوصی بیمار رمزنگاری شده و امضای دیجیتال ایجاد می‌شود. امضای دیجیتال به‌عنوان مدرک رمزنگاری‌شده‌ای از صحت و اصالت پیام عمل کرده و امکان تأیید عدم تغییر داده در طول انتقال را برای گیرنده فراهم می‌سازد. جزئیات بیشتر در ادامه توضیح داده شده است.

روش هش کردن داده‌های بیومتریک بیمار و ساخت امضای دیجیتال بدین صورت است [55]:

۱- دریافت اطلاعات معتبر بیومتریک بیمار در قالب تصویر.

۲- تغییر سایز استاندارد اطلاعات بیومتریک بیمار در سایزهای ۳۲*۳۲ پیکسل یا ۶۴*۶۴ پیکسل.

۳- حذف پیکسل‌های رنگی از تصویر بیومتریک و ایجاد قالب Grayscale از تصویر بیومتریک.

۴- نرمال سازی قالب Grayscale برای کاهش تاثیر تغیرات روشنایی تصویر.

۵- تبدیل قالب Grayscale مرحله چهار، به یک آرایه از بایت.

۶- خروجی مرحله پنج یا توالی باینری، با استفاده از یکی از الگوریتم‌های هش به یک نمایش عددی Hexadecimal یا سایر خروجی‌های الگوریتم‌های هش تبدیل می‌شود.

۷- رمزنگاری خروجی مرحله ششم، با استفاده از کلید خصوصی موجب ساخت امضای دیجیتال می‌شود.

۴-۱-۳- ایجاد کلید با استفاده از نگاشت لجستیک سه‌بعدی

برای ساخت کلیدهای رمزنگاری، از نگاشت لجستیک سه‌بعدی که نوعی نگاشت آشوبی است، استفاده می‌شود. این سیستم به‌دلیل حساسیت بالا نسبت به شرایط اولیه و رفتار غیرخطی، خروجی‌های شبه‌تصادفی قدرتمندی تولید می‌کند.

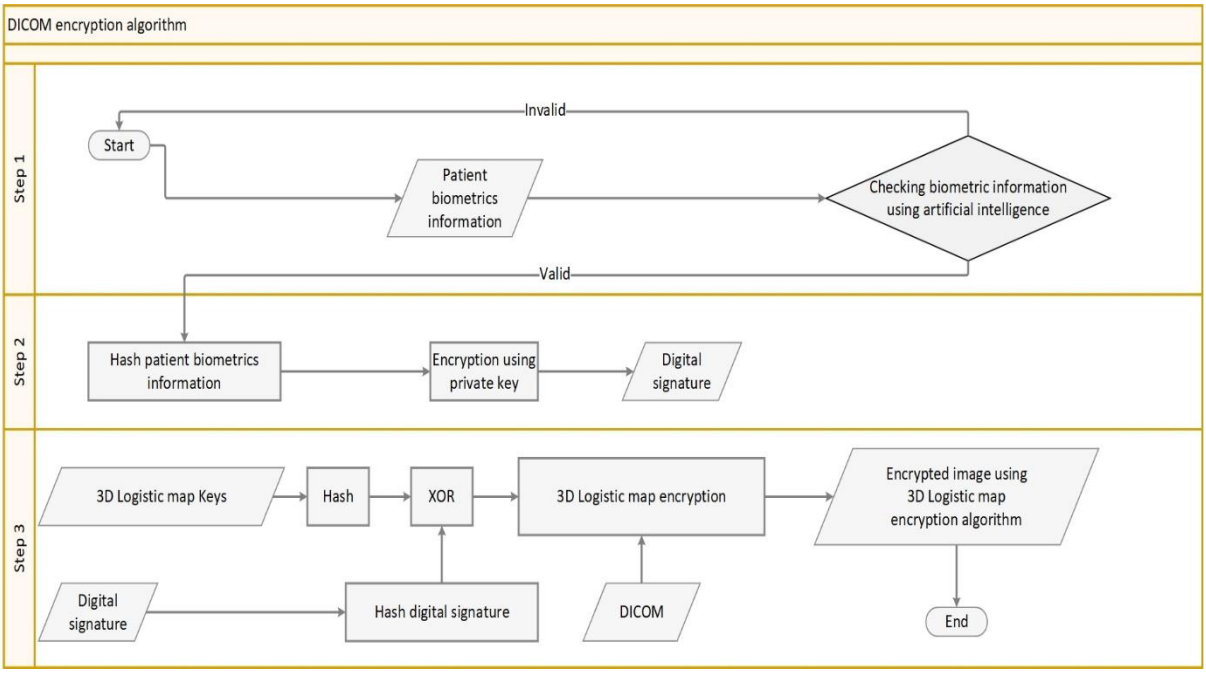
- ابتدا خروجی حاصل از نگاشت لجستیک سه‌بعدی با استفاده از همان الگوریتم هش مرحله قبل، هش می‌شود.
- امضای دیجیتال تولیدشده در مرحله دوم نیز جداگانه هش می‌گردد.
- دو مقدار هش حاصل، از طریق عملیات XOR با یکدیگر ترکیب شده و کلید نهایی رمزنگاری ایجاد می‌گردد؛ کلیدی که برای هر بیمار و هر جلسه رمزنگاری، منحصربه‌فرد خواهد بود.

۴-۱-۴- رمزنگاری فایل DICOM

با استفاده از کلید نهایی به‌دست‌آمده، فایل DICOM با بهره‌گیری از الگوریتم رمزنگاری مبتنی بر نگاشت لجستیک سه‌بعدی رمزنگاری می‌شود. ویژگی آشوبی این الگوریتم موجب گسترش و ابهام گسترده داده‌ها شده و امنیت آن را در برابر حملات آماری و حملات جست‌وجوی فراگیر[۱] به‌طور چشم‌گیری افزایش می‌دهد.

در شکل شماره ۵ ساختار الگوریتم رمزنگاری نشان داده شده است.

[۱] Brute force



شکل ۵: ساختار الگوریتم رمزنگاری پیشنهاد داده شده در این مقاله

در ادامه شبه کد الگوریتم مورد نظر نوشته شده است:

1. START
2. PROGRAM DICOM_Encryption
3. READ INPUT into patient_biometric_information
4. Checking patient_biometric_information using artificial intelligence, If the biometric information is valid, go to the next step.
5. patient_biometric_information
6. FUNCTION Patient_Biometric_Information_Hash
7. Pass IN: patient_biometric_information
8. Pass Out: Hash_result_of_the_Patient_Biometric_Information
9. END FUNCTION
10. CALL: Patient_Biometric_Information_Hash
11. READ INPUT into Private_Key
29. Call: DigitalSignature_Hash
30. FUNCTION XOR
31. Pass IN: Hash_result_of_the_3D_LOGISTIC_MAP_Key
32. Pass IN: Hash_result_of_the_Digital_Signature
33. Pass Out: XOR_Result1
34. END FUNCTION
35. Call: XOR
36. FUNCTION 3D_LOGISTIC_MAP_Encryption
37. Pass IN: XOR_Result1
38. Pass IN: DICOM

12. FUNCTION Digital Signature
13. Pass IN: Private Key
14. Pass IN: Hash_result_of_the_Patient_Biometric_Information
15. Pass Out: Digital_Signature
16. END FUNCTION
17. CALL: Digital Signature
18. READ INPUT into Digital_Signature
19. FUNCTION DigitalSignature_Hash
20. Pass IN: Digital_Signature
21. Pass Out: Hash_result_of_the_Digital_Signature
22. END FUNCTION

23. READ INPUT into 3D_LOGISTIC_MAP_Key
24. FUNCTION 3D_LOGISTIC_MAP_Key_Hash
25. Pass IN: 3D_LOGISTIC_MAP_Key
26. Pass Out: Hash_result_of_the_3D_LOGISTIC_MAP_Key
27. END FUNCTION
28. Call: 3D_LOGISTIC_MAP_Key_Hash

39. Pass Out: Encrypted_Image_Using_3D_LOGISTIC_MAP
40. END FUNCTION

۴-۲- الگوریتم رمزگشایی

۴-۲-۱- دریافت فایل DICOM رمزنگاری‌شده و امضای دیجیتال

در این مرحله، گیرنده ابتدا فایل DICOM رمزنگاری‌شده را همراه با امضای دیجیتال دریافت می‌کند. این فایل توسط فرستنده با استفاده از روش الگوریتم‌های رمزنگاری و امضای دیجیتال ایجاد شده است. امضای دیجیتال در واقع ثابت می‌کند که فایل توسط فرستنده اصلی ارسال شده است و در طول انتقال تغییر نکرده است.

۴-۲-۲- دریافت و تأیید اطلاعات بیومتریک بیمار

در این مرحله، گیرنده نیاز دارد تا اطلاعات بیومتریک معتبر از همان بیمار دریافت کند. این داده‌های بیومتریک (مانند اثر انگشت، اسکن عنبیه یا ویژگی‌های صورت) از بیمار گرفته می‌شود. برای اطمینان از صحت و معتبر بودن این

اطلاعات، از الگوریتم‌های هوش مصنوعی مانند الگوریتم ANFIS، SVM یا سایر تکنیک‌های شبیه‌سازی استفاده می‌شود تا داده‌ها به درستی پردازش و تأیید شوند.

۴-۲-۳- ایجاد هش از داده‌های بیومتریک

در این مرحله، پس از دریافت و تأیید داده‌های بیومتریک، یک تابع هش مانند (SHA-256) به این داده‌ها اعمال می‌شود. این تابع هش باعث می‌شود که داده‌های بیومتریک به یک مقدار ثابت با اندازه مشخص تبدیل شوند که به‌عنوان نماینده داده‌های اصلی عمل می‌کند. این هش در واقع به‌عنوان "اثر انگشت دیجیتال" اطلاعات بیومتریک عمل می‌کند.

۴-۲-۴- اعتبارسنجی امضای دیجیتال با استفاده از کلید عمومی

پس از ایجاد هش از داده‌های بیومتریک، در این مرحله گیرنده امضای دیجیتال فرستنده را با استفاده از کلید عمومی فرستنده رمزگشایی می‌کند. برای این منظور:

- گیرنده کلید عمومی فرستنده را دریافت کرده و با آن امضای دیجیتال را رمزگشایی می‌کند.
- سپس هش حاصل از امضای دیجیتال که به همراه فایل DICOM ارسال شده است را با هش داده‌های بیومتریک که در مرحله ۳ تولید شده است، مقایسه می‌کند.
- اگر این دو هش برابر باشند، صحت داده‌های دریافت‌شده و اصالت فرستنده تأیید می‌شود. در غیر این صورت، فایل به‌طور احتمالی دستکاری شده یا از فرستنده اصلی ارسال نشده است.

۴-۲-۵- ایجاد مجدد کلید رمزگشایی

در این مرحله، کلید رمزگشایی باید با کلید استفاده‌شده در مرحله رمزنگاری مطابقت داشته باشد. برای تولید کلید رمزگشایی:

- هش داده‌های بیومتریک که در مرحله ۳ تولید شده است.

- هش حاصل از خروجی نگاشت لجستیک سه‌بعدی که در مرحله رمزنگاری تولید شده بود .با هم ترکیب می‌شوند. ترکیب این دو هش با استفاده از عملیات XOR (عملیات «یا» به‌صورت بیت به بیت) انجام می‌شود. این عمل باعث تولید کلید نهایی رمزگشایی می‌شود.

۴-۲-۶- رمزگشایی فایل DICOM

در این مرحله، کلید نهایی رمزگشایی که در مرحله قبل تولید شده، برای رمزگشایی فایل DICOM استفاده می‌شود. برای این کار:

- فایل DICOM رمزنگاری‌شده با استفاده از الگوریتم نگاشت لجستیک سه‌بعدی معکوس رمزگشایی می‌شود.
- الگوریتم نگاشت لجستیک سه‌بعدی به‌طور طبیعی یک سیستم آشوبی است و هر تغییر در شرایط اولیه منجر به تولید داده‌های کاملاً متفاوتی می‌شود. با این حال، چون کلید رمزگشایی دقیقاً برابر با کلید استفاده‌شده در مرحله رمزنگاری است، فایل DICOM به‌طور صحیح و بدون خطا رمزگشایی می‌شود.
- در نهایت، فایل DICOM اصلی و تصاویر پزشکی آن بازیابی می‌شوند.

۵- پارامترهای مورد نیاز در تحلیل عملکرد الگوریتم

پارامترهای مورد نظر بر اساس موارد زیر تعریف شده‌اند:

۵-۱- پارامتر MSE[۱]

خطای میانگین مربع یا MSE مشخص‌کننده میزان تفاوت تصویر رمزنگاری شده با تصویر اصلی است. هرچه مقدار MSE بیشتر باشد عملکرد الگوریتم رمزنگاری بهتر بوده است [58-56,53,51]. MSE یک تصویر از رابطه ۲ محاسبه می‌شود.

$$\text{MSE}=\sum_{i=0}^{m-1}\sum_{i=0}^{n-1}\ (f(i,j)-g(i,j))^2/\ m\times n \qquad (2)$$

۵-۲- پارامتر PSNR[۲]

[۱] Mean square error

[۲] Peak signal to noise ratio

PSNR پارامتری است که برای اندازه‌گیری کیفیت کمی تصویر دیجیتال استفاده می‌شود. هر چه مقدار PSNR کمتر باشد عملکرد الگوریتم رمزنگاری بهتر بوده است [58-56,53,51]. این معیار امنیتی میزان اختلاف بین کیفیت تصویر اصلی f(x,y) و تصویر رمزگشایی شده‌ی g(x,y) را نشان می‌دهد و با رابطه‌ی ۳ تعریف می‌شود.

$$PSNR=10\ \log_{10}\frac{255^2}{MSE} \quad (3)$$

تمایز تصویر اصلی و تصویر رمز شده: یک الگوریتم رمزنگاری امن باید حساسیت شدید نسبت به تغییرات جزئی در تصویر اصلی داشته باشد. در حملات تفاضلی، فرد مهاجم تلاش می‌کند با ایجاد یک تغییر بسیار کوچک در تصویر اصلی و مشاهده تغییرات حاصل در تصویر رمز شده، ارتباط معناداری بین تصویر رمز و تصویر اصلی پیدا نماید. اگر یک تغییر بسیار کوچک در تصویر اصلی موجب تغییرات چشمگیری در تصویر رمز شده گردد، آنگاه الگوریتم در مقابل حملات تفاضلی مقاوم خواهد بود. دو معیار مهم در تحلیل حملات تفاضلی NPCR[۱] (نرخ پیکسل‌های تغییریافته در تصویر رمز شده به‌ازای یک بیت تغییر در تصویر اصلی) و UACI[۲] (متوسط اختلاف شدت سطح روشنایی دو تصویر رمز شده) می‌باشند [58-56,53,51].

۵-۳- پارامتر NPCR

این معیار امنیتی نرخ تعداد پیکسل‌های تغییریافته تصویر رمز را در حالتی محاسبه می‌کند که تصاویر اصلی آن‌ها در یک پیکسل با هم تفاوت دارند. (هر چه مقداد NPCR بیشتر باشد، الگوریتم رمزنگاری عملکرد بهتری دارد). این پارامتر از رابطه ۴ محاسبه می‌شود [58-56,53,51].

$$NPCR=\frac{\sum_{i,j} D(i,j)}{W\times H}\times 100\% \quad (4)$$

۵-۴- پارامتر UACI

[۱] Number of pixel change rate

[۲] Unified average changing intensity

این معیار امنیتی بیانگر میانگین یکنواخت تغییر شدت است (هر چه مقداد UACI بیشتر باشد، الگوریتم رمزنگاری عملکرد بهتری دارد). UACI یک تصویر از رابطه ۵ محاسبه می‌شود [58-56,53,51].

$$\mathrm{UACI} = \frac{1}{W \times H}\left[\sum_{i,j}\frac{|c_1(i,j) - c_2(i,j)|}{255}\right] \times 100\% \quad (5)$$

در پارامترهای گفته شده H و W طول و عرض تصاویر و C_1 و C_2 دو تصویر رمزنگاری شده هستند که از دو تصویر با یک پیکسل اختلاف گرفته شده‌اند و D به‌صورت زیر تعریف می‌شود:

$$\mathrm{D(i,j)} = \begin{cases} 0 & if \quad c_1(i,j) = c_2(i,j) \\ 1 & if \quad c_1(i,j) \neq c_2(i,j) \end{cases} \quad (6)$$

۵-۵- آنتروپی[۱] تصویر رمزنگاری شده

این معیار امنیتی یکی از خصوصیت‌های برجسته برای تصادفی بودن است. آنتروپی اطلاعات یک تئوری ریاضی برای ارتباط داده و ذخیره‌سازی است که در سال ۱۹۴۹ توسط Claude E Shannon معرفی‌شده است.

آنتروپی اطلاعات می‌تواند به‌عنوان معیاری برای به‌دست‌آوردن میزان آشفتگی سطوح خاکستری پیکسل‌ها استفاده شود. آنتروپی یک تصویر از رابطه ۷ محاسبه می‌شود.

$$\mathrm{H(m)}=\sum_{i=0}^{2^N-1} \mathrm{P(m_i)}\log_2 \frac{1}{\mathrm{P(m_i)}} \quad (7)$$

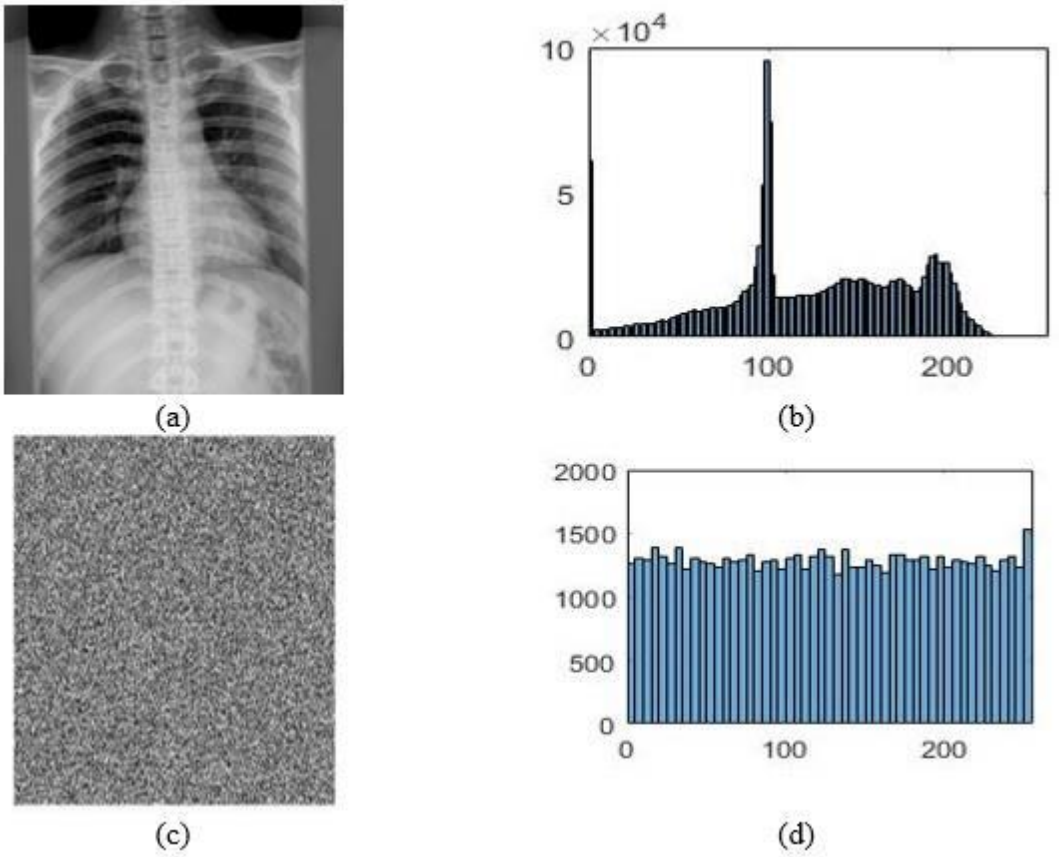
دراین‌رابطه $p(m_i)$ احتمال وقوع سطح خاکستری m_i و ۲^N تعداد سطوح خاکستری ممکن است. در یک تصویر غیریکنواخت که احتمال وقوع تمام پیکسل‌ها یکسان است مقدار آنتروپی بیشترین مقدار خود یعنی ۸ خواهد بود که این به معنی وجود بیشترین بی‌نظمی در میان پیکسل‌های تصویر است. نزدیک بودن مقدار آنتروپی تصویر رمز شده به ۸ به منزله کارایی روش ارائه‌شده در رمزنگاری است [58-56,53,51,25].

۵-۶- هیستوگرام[۲]

هیستوگرام نیز یکی دیگر از معیارهای امنیتی است. این معیار یک نمودار ساده است که نشان می‌دهد سطوح مختلف روشنایی موجود در صحنه، از تاریک‌ترین تا روشن‌ترین سطح در چه محدوده‌ای واقع‌شده‌اند. هر نوار به طور معمول

[۱] Entropy
[۲] Histogram

دامنه‌ای از مقادیر عددی را بنام bin یا class پوشش می‌دهد. هر چه هیستوگرام یک تصویر رمزنگاری شده بیشتر مسطح باشد نشان‌دهنده عملکرد بهتر الگوریتم رمزنگاری است [59-63].



شکل ۶: هیستوگرام تصویر DICOM قبل و بعد از رمزنگاری

۵-۷- ضریب همبستگی

فاکتور ضریب همبستگی متقابل درواقع همبستگی متقابل بین داده‌های رمز نشده و رمز شده است. هر چه این مقدار به یک نزدیک‌تر باشد همبستگی سیگنال‌ها بیشتر خواهد بود و هر چه به صفر نزدیک‌تر باشد داده‌ها همبستگی کمتری دارند. همبستگی کمتر نشان‌دهنده بالاتر بودن کیفیت رمزنگاری است. ضریب همبستگی در سه حالت عمودی[۱]، افقی[۲] و قطری[۳] تقسیم می‌شود [60-63].

[۱] Vertical
[۲] Horizontal
[۳] Diagonal

۵-۸- فضای کلید

فضای کلید تعداد کل کلیدهای مختلفی است که می‌تواند در رمزنگاری مورد استفاده قرار گیرد. هر چه فضای کلید الگوریتم رمزنگاری بزرگ‌تر باشد نشان‌دهنده کارایی بهتر آن و مقاومت مؤثرتر آن در برابر حملات رمزنگاری است.

۶- نتایج اجرای الگوریتم پیشنهاد داده شده و تحلیل امنیت آن

طبق طرح پیشنهادی در بخش ۴، برای شبیه‌سازی‌های اجرای الگوریتم در این بخش، تصاویر DICOM به‌صورت تصادفی برای آزمایش‌ها انتخاب شده‌اند. برخی تحلیل‌های امنیتی رایج مانند هیستوگرام، آنتروپی، NPCR، UACI، MSEو PSNR نیز برای ارزیابی امنیت الگوریتم پیشنهادی مورد استفاده قرار گرفته‌اند.

نتایج آزمایش‌ها بر اساس موارد زیر تعریف شده‌اند:

۶-۱- مشخصات سیستم استفاده شده برای ارزیابی

CPU : Intel Core i۷ , ۲٫۱۰ GHz
RAM : ۸ GB
Operator system : Microsoft Windows ۱۰
System type : ۶۴ bit
Simulation software and programming language :
MATLAB (R۲۰۱۶b), Python

۶-۲- منابع داده

برای تصاویر DICOM از منابع [65,64] استفاده شده است و داده‌های بیومتریک که از یافته‌های این مطالعه پشتیبانی می‌کنند، در منابع [67,66] در دسترس هستند. تحلیل‌های تفاضلی و آماری الگوریتم پیشنهادی نیز در داخل این مطالعه ارائه شده‌اند. تعداد دقیق تصاویر DICOM بررسی شده در این مقاله برابر با ۱۳ عدد تصویر DICOM است.

۶-۳- بررسی پارامترهای Entropy, NPCR, UACI, MSE, PSNR بعد از اجرای الگوریتم

با توجه به شکل شماره ۷ و ۸ ، در جدول ۴ نتایج خروجی الگوریتم نشان داده شده است.

شکل ۷: نمونه تصاویر DICOM قبل از رمزنگاری

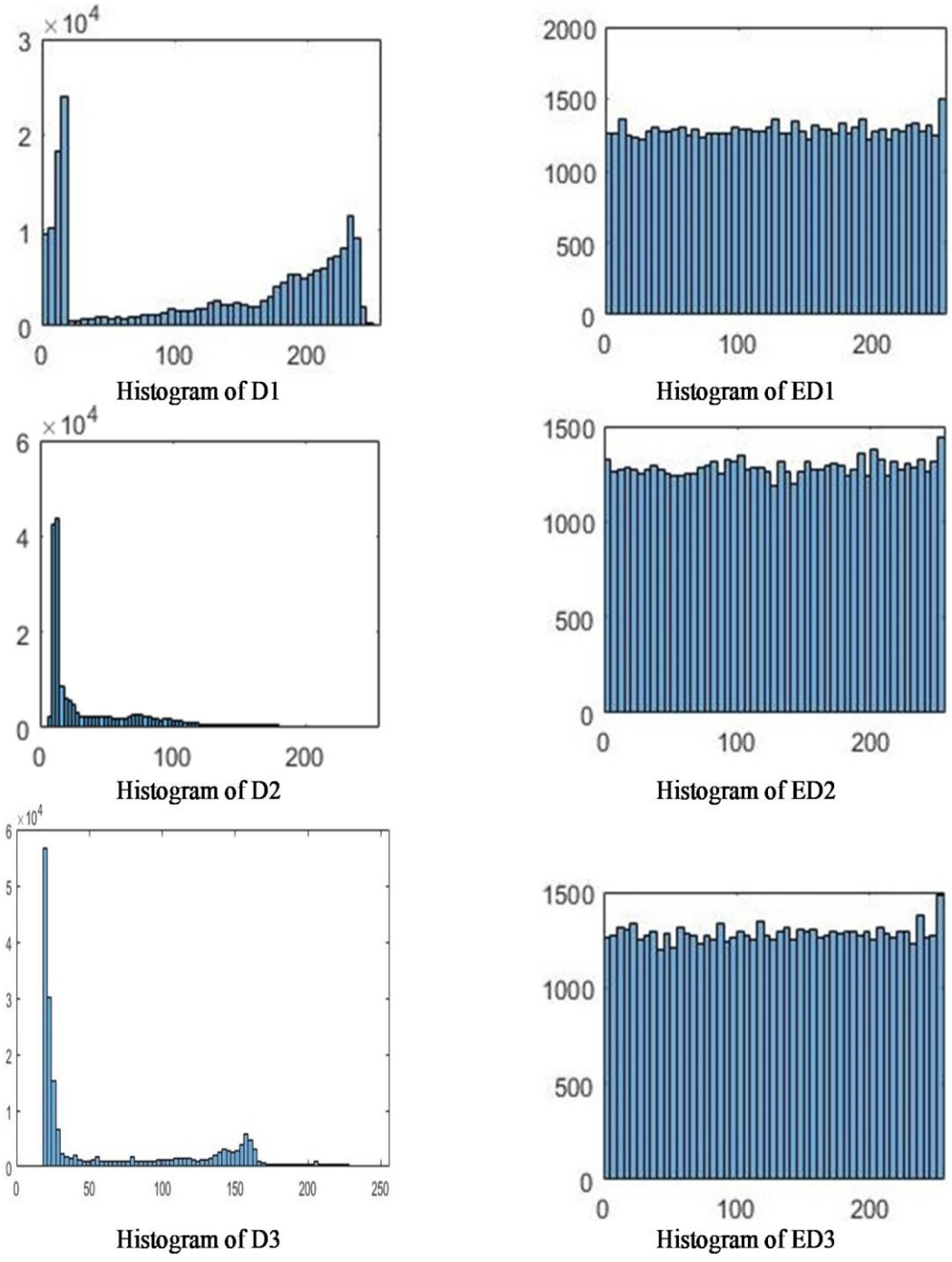
شکل ۸: نمونه تصاویر DICOM بعد از رمزنگاری

جدول ۴: پارامترهای تصاویر رمزنگاری شده

تصویر	تصویر رمزنگاری	آنتروپی (bit/pixel)	MSE (%)	PSNR (%)	UACI (%)	NPCR (%)
D1	۱ED	7.997926374	116.41	27.5050786	0.33	0.995412
D2	۲ED	7.997775945	57	30.6058256	0.329236	0.993411
D3	۳ED	7.998042883	112.49	27.6537821	0.36174	0.998169

۶-۴- بررسی هیستوگرام

تصویر رمزنگاری‌شده ایده‌آل باید دارای هیستوگرام یکنواخت باشد [41]. بر این اساس، این بخش به تحلیل کمی انحراف موجود در هیستوگرام میان تصویر ساده و تصویر رمزنگاری‌شده می‌پردازد، تا میزان اثربخشی الگوریتم رمزنگاری پیشنهادی از منظر توزیع آماری پیکسل‌ها مورد ارزیابی قرار گیرد. بررسی هیستوگرام در شکل شماره ۹ نشان داده شده است.



شکل ۹: هیستوگرام D1، هیستوگرام D2، هیستوگرام D3، هیستوگرام ED1، هیستوگرام ED2، هیستوگرام ED3

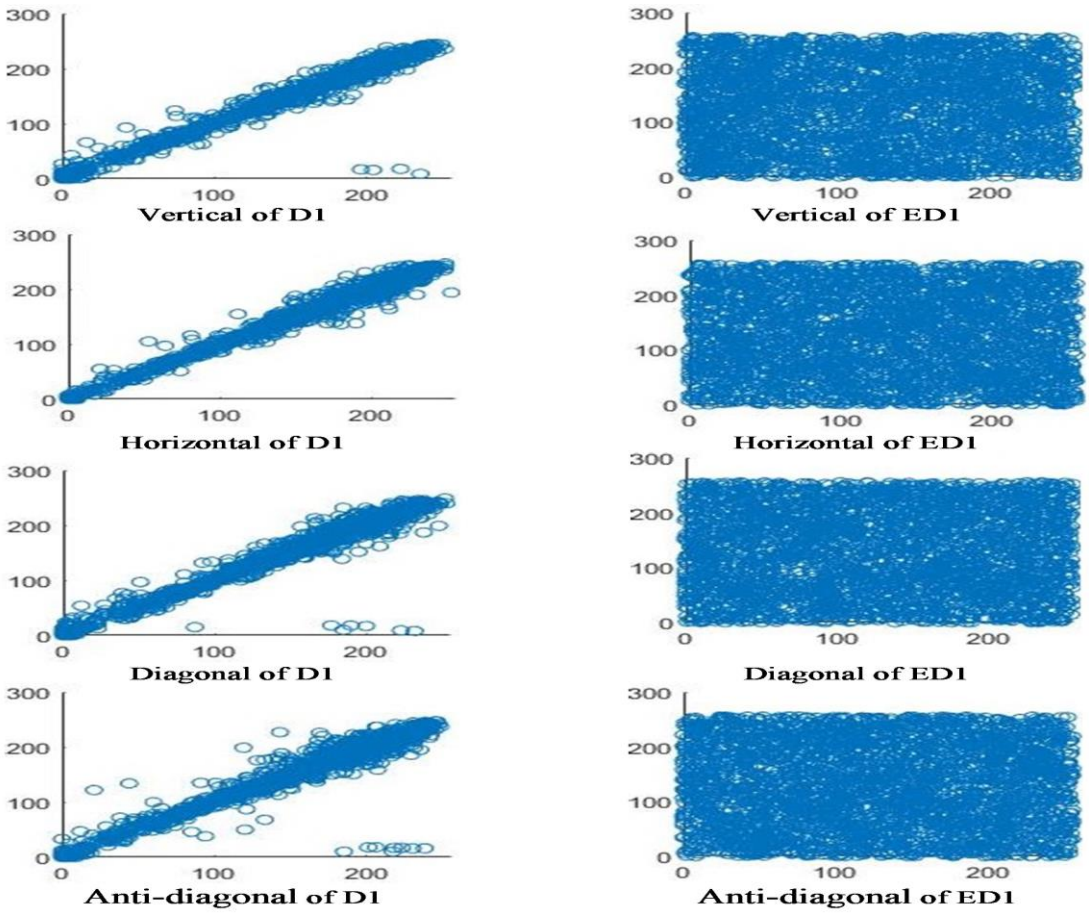
۶-۵- فضای کلید

در الگوریتم لجستیک سه‌بعدی با اعمال شرایط اولیه و پارامترهای مربوط سه دنباله با اعداد تصادفی بین صفر و یک تولید می‌شود که با بهره‌گیری از آن‌ها رمزنگاری تصویر انجام می‌شود. فضای کلید در بهترین حالت باید از $۱۰^{۳۰}$ بیشتر باشد تا از حملات جستجوی فراگیر جلوگیری کند [50,49]. کلیدهای استفاده شده در الگوریتم رمزنگاری لجستیک سه‌بعدی موجب می‌شود فضای کلید این الگوریتم لجستیک سه بعدی به شکل تقریبی $۱۰^{۸۹}$ باشد [54,53]. برای جلوگیری از حملات جستجوی فراگیر علاوه بر بالابودن فضای کلید الگوریتم لجستیک سه‌بعدی ، قسمت‌های دیگر الگوریتم پیشنهاد داده شده مانند استفاده از الگوریتم RSA برای ساخت امضای دیجیتال، اطلاعات بیومتریک بیمار، عملگر XOR و هش‌شدن تعدادی از کلیدها برای استفاده، در جلوگیری از حملات جستجوی فراگیر بسیار مؤثر خواهند بود.

۶-۶- تحلیل همبستگی

در یک تصویر ساده، معمولاً همبستگی بالایی میان بیشتر جفت‌های پیکسل‌های مجاور به‌دلیل پیوستگی پیکسل‌ها وجود دارد. یک الگوریتم رمزنگاری قوی باعث کاهش ضرایب همبستگی می‌شود [68-73]. این بخش به تحلیل کمی همبستگی میان تصویر ساده و تصویر رمزنگاری‌شده اختصاص دارد.

برای نمونه در شکل ۱۰ همبستگی‌های عمودی، افقی، قطری و ضد قطری تصویر D1 و ED1 نشان داده شده است.



شکل ۱۰: ضرایب همبستگی افقی، عمودی و قطری تصویر D1

۶-۷- مقایسه و تحلیل الگوریتم پیشنهادی

در جدول ۵ الگوریتم پیشنهادی با تعدادی از مقالات مقایسه شده است.

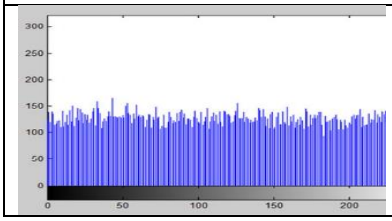
جدول ۵: مقایسه الگوریتم پیشنهادی با سایر الگوریتم‌ها

الگوریتم / مرجع	Dual hyperchaos map	PWLCM[1]	نگاشت آشوب یک‌بعدی	نگاشت آشوب دوبعدی	نگاشت آشوب سه‌بعدی	Latin square	Hash function	RSA	Digital signature	Biometric information	RNA	AI
[74]			✓			✓	✓					
[70]		✓	✓								✓	
[75]				✓			✓				✓	
[16]	✓										✓	
الگوریتم پیشنهادی					✓		✓	✓	✓	✓		✓

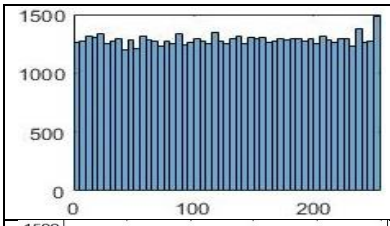
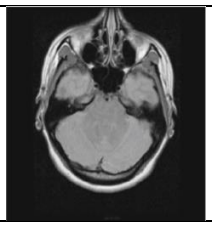
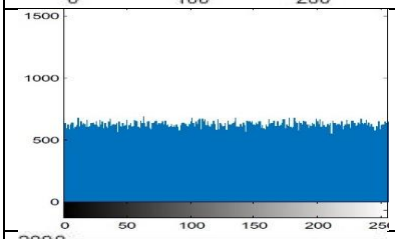
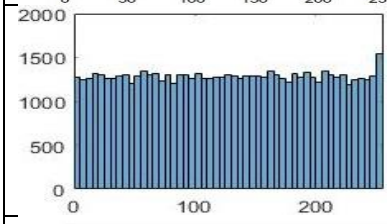
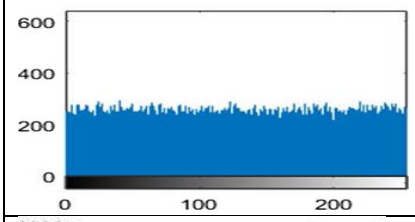
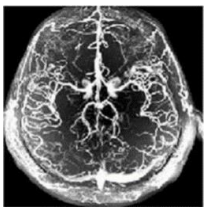
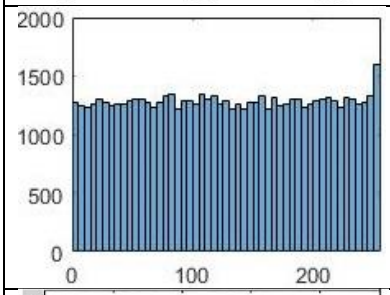
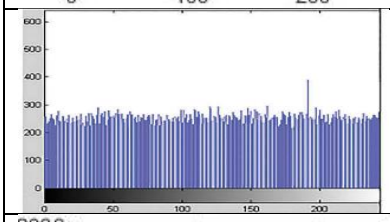
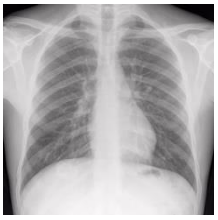
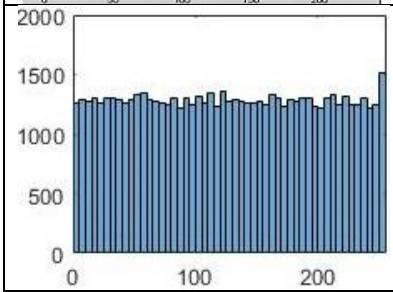
۶-۸- تحلیل عملکرد الگوریتم پیشنهادی

بر اساس برخی از پارامترها مانند آنتروپی، NPCR، UACI و هیستوگرام، تحلیل و عملکرد الگوریتم پیشنهادی در جدول‌های ۴ و ۶ نشان داده شده است.

جدول ۶: مقایسه پارامترهای آنتروپی، NPCR، UACI و هیستوگرام

Histogram	NPCR (%)	UACI (%)	Entropy (bit/pixel)	Plain image [64, 65]	Reference
	99.80	33.49	7.9953		[70]

[1] Piecewise linear chaotic map

	99.81	36.17	7.9979		Proposed algorithm
	99.61	33.41	7.9971		[74]
	99.63	35.14	7.9982		Proposed algorithm
	99.60	33.69	7.9969		[14]
	99.63	35.49	7.9978		Proposed algorithm
	99.8	33.29	7.89		[16]
	99.9	33.41	7.9971		Proposed algorithm

۷- نتیجه‌گیری

سامانه‌های اطلاعات سلامت باید با درنظر گرفتن ملاحظات کلیدیِ حریم خصوصی و امنیت طراحی و پیاده‌سازی شوند [78-76,1]. در این مقاله، ما یک الگوریتم نوین رمزنگاری تصاویر پزشکی بر پایه‌ی یک مدل ترکیبی از رمزنگاری با نگاشت لوجستیک سه‌بُعدی، هوش مصنوعی و امضای دیجیتال پیشنهاد داده‌ایم. در الگوریتم پیشنهادی، از امضای دیجیتال و اطلاعات بیومتریک بیماران برای افزایش امنیت در برابر حملات سایبری و تأیید هویت استفاده شده است. بر اساس این الگوریتم، کلیدهای رمزنگاری به یکدیگر و به اطلاعات بیومتریک بیمار وابسته هستند. الگوریتم رمزنگاری DICOM پیشنهادی، نسبت به تغییرات تصویر اصلی حساسیت بالایی دارد. نتایج شبیه‌سازی و تحلیل‌های کارایی نشان می‌دهند که الگوریتم رمزنگاری پیشنهادی از سطح امنیتی و مقاومت بالایی برخوردار است و در برابر حملات جست‌وجوی فراگیر مقاوم می‌باشد.

منابع

[1] K. S. Mann and A. Bansal, "HIS integration systems using modality worklist and DICOM," *Procedia Computer Science*, vol. 37, pp. 16-23, 2014.

[2] M. Puppala, T. He, X. Yu, S. Chen, R. Ogunti, and S. T. Wong, "Data security and privacy management in healthcare applications and clinical data warehouse environment," in *2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*, 2016: IEEE, pp. 5-8 .

[3] P. Shojaei, E. Vlahu-Gjorgievska, and Y.-W. Chow, "Security and privacy of technologies in health information systems: A systematic literature review," Computers, vol. 13, no. 2, p. 41, 2024.

[4] J. Chandrasekaran and S. J. Thiruvengadam, "A hybrid chaotic and number theoretic approach for securing DICOM images," Security and Communication Networks, vol. 2017, 2017.

[5] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," Optics and Lasers in engineering, vol. 88, pp. 197-213, 2017.

[6] B. Zhang, B. Rahmatullah, S. L. Wang, A. Zaidan, B. Zaidan, and P. Liu, "A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations," Multimedia Tools and Applications, pp. 1-40, 2023.

[7] C. Fu, G.-y. Zhang, O. Bian, W.-m. Lei, and H.-f. Ma, "A novel medical image protection scheme using a 3-dimensional chaotic system," PloS one, vol. 9, no. 12, p. e115773, 2014.

[8] M. N. E. Farandi, A. Marjuni, N. Rijati, and D. R. I. M. Setiadi, "Enhancing image encryption security through integration multi-chaotic systems and mixed pixel-bit level," The Imaging Science Journal, pp. 1-18, 2024.

[9] S. M. Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," Signal processing, vol. 92, no. 5, pp. 1202-1215, 2012.

[10] Y. Dai and X. Wang, "Medical image encryption based on a composition of logistic maps and chebyshev maps," in 2012 IEEE international conference on information and automation, 2012: IEEE, pp. 210-214.

[11] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," Signal processing, vol. 97, pp. 172-182, 2014.

[12] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," Computers in biology and medicine, vol. 72, pp. 170-184, 2016.

[13] S. Mortajez, M. Tahmasbi, J. Zarei, and A. Jamshidnezhad, "A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images," Informatics in Medicine Unlocked, vol. 20, p. 100396, 2020.

[14] J. C. Dagadu, J.-P. Li, and E. O. Aboagye, "Medical image encryption based on hybrid chaotic DNA diffusion," Wireless Personal Communications, vol. 108, pp. 591-612, 2019.

[15] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Medical data sheet in safe havens–A tri-layer cryptic solution," Computers in biology and medicine, vol. 62, pp. 264-276, 2015.

[16] P. T. Akkasaligar and S. Biradar, "Selective medical image encryption using DNA cryptography," Information Security Journal: A Global Perspective, vol. 29, no. 2, pp. 91-101, 2020.

[17] M. Boussif, N. Aloui, and A. Cherif, "Smartphone application for medical images secured exchange based on encryption using the matrix product and the exclusive addition," IET Image Processing, vol. 11, no. 11, pp. 1020-1026, 2017.

[18] W. Wen, K. Wei, Y. Zhang, Y. Fang, and M. Li, "Colour light field image encryption based on DNA sequences and chaotic systems," Nonlinear Dynamics, vol. 99, no. 2, pp. 1587-1600, 2020.

[19] D. Ravichandran, A. Banu S, B. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain," Medical & biological engineering & computing, vol. 59, pp. 589-605, 2021.

[20] J. S. Muthu and P. Murali, "A novel DICOM image encryption with JSMP map," Optik, vol. 251, p. 168416, 2022.

[21] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," Symmetry, vol. 11, no. 2, p. 141, 2019.

[22] A. Banu S and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," Medical & biological engineering & computing, vol. 58, pp. 1445-1458, 2020.

[23] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "Non-invertible cancellable fingerprint template for fingerprint biometric," Computers & Security, vol. 90, p. 101690, 2020.

[24] W. U. Wickramaarachchi, D. Zhao, J. Zhou, and J. Xiang, "An effective iris biometric privacy protection scheme with renewability," Journal of Information Security and Applications, vol. 80, p. 103684, 2024.

[25] P. P. Polash and M. M. Monwar, "Human iris recognition for biometric identification," in 2007 10th international conference on computer and information technology, 2007: IEEE, pp. 1-5.

[26] F. Jan, S. Alrashed, and N. Min-Allah, "Iris segmentation for non-ideal Iris biometric systems," Multimedia Tools and Applications, vol. 83, no. 5, pp. 15223-15251, 2024.

[27] M. Soltani, H. Shakeri, and M. Houshmand, "A robust hybrid algorithm for medical image cryptography using patient biometrics based on DNA and RNA computing," 2023.

[28] P. Rai and P. Kanungo, "Advancements in Iris Recognition: A Comprehensive Review for Biometric Systems," in International Conference on Information Technology, 2024: Springer, pp. 131-137.

[29] A. P. Iyer, J. Karthikeyan, R. Khan, and P. Binu, "An analysis of artificial intelligence in biometrics-the next level of security," J Crit Rev, vol. 7, no. 1, pp. 571-576, 2020.

[30] A. Galli, M. Gravina, S. Marrone, D. Mattiello, and C. Sansone, "Adversarial liveness detector: Leveraging adversarial perturbations in fingerprint liveness detection," IET Biometrics, vol. 12, no. 2, pp. 102-111, 2023.

[31] Z. H. Choudhury, "Biometric passport security based on face recognition and biometric encryption using secure force algorithm into the HCC2D code," Information Security Journal: A Global Perspective, vol. 33, no. 5, pp. 455-472, 2024.

[32] S. B. Abdullahi et al., "Biometric information recognition using artificial intelligence algorithms: A performance comparison," IEEE Access, vol. 10, pp. 49167-49183, 2022.

[33] J. R. Matey, J. R. Matey, G. W. Quinn, and P. Grother, Forensic Iris: A Review, 2022. US Department of Commerce, National Institute of Standards and Technology, 2022.

[34] J. R. Malgheet, N. B. Manshor, and L. S. Affendey, "Iris recognition development techniques: a comprehensive review," Complexity, vol. 2021, no. 1, p. 6641247, 2021.

[35] G. Babu and A. K. Pinjari, "A new design of iris recognition using hough transform with K-means clustering and enhanced faster R-CNN," Cybernetics and Systems, vol. 55, no. 2, pp. 551-584, 2024.

[36] G. P. Babu, U. S. Aswal, M. Sindhu, V. J. Upadhye, and H. Patil, "Enhancing security with machine learning-based finger-vein biometric authentication system," in 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), 2024: IEEE, pp. 797-802.

[37] N. N. B. Karo, A. Y. Sari, N. Aziza, and H. K. Putra, "The enhancement of fingerprint images using gabor filter," in Journal of Physics: Conference Series, 2019, vol. 1196, no. 1: IOP Publishing, p. 012045.

[38] M. Ahsan, M. Based, J. Haider, and M. Kowalski, "An intelligent system for automatic fingerprint identification using feature fusion by Gabor filter and deep learning," Computers and Electrical Engineering, vol. 95, p. 107387, 2021.

[39] S. S. Omar, W. S. Ahmed, M. N. Ismail, and O. Sieliukov, "In-Depth Examination of a Fingerprint Recognition System Using the Gabor Filter," in 2024 35th Conference of Open Innovations Association (FRUCT), 2024: IEEE, pp. 532-543.

[40] N. Pradeep and J. Ravi, "An revolutionary fingerprint authentication approach using Gabor filters for feature extraction and deep learning classification using convolutional neural networks," in Innovations in Electronics and Communication Engineering: Proceedings of the 9th ICIECE 2021: Springer, 2022, pp. 349-360.

[41] A. Sherine and G. Peter, "A novel biometric recognition system for fingerprint using polar harmonic transform," International Journal of Pharmaceutical Research, vol. 13, no. 01, 2021.

[42] H. Shams, T. Jan, A. A. Khalil, N. Ahmad, A. Munir, and R. A. Khalil, "Fingerprint image enhancement using multiple filters," PeerJ Computer Science, vol. 9, p. e1183, 2023.

[43] S. Shreya and K. Chatterjee, "Gan-enable latent fingerprint enhancement model for human identification system," Multimedia Tools and Applications, vol. 83, no. 9, pp. 27565-27588, 2024.

[44] P. G. Jayadev and S. Bellary, "IrisSeg-drunk: enhanced iris segmentation and classification of drunk individuals using Modified Circle Hough Transform," Iran Journal of Computer Science, vol. 7, no. 1, pp. 41-54, 2024.

[45] R. Bharathi and M. Anandaraju, "Iris Recognition System Using Circular Hough Transform and HOG," in 2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET), 2024: IEEE, pp. 1-4.

[46] A. Soni, T. Patidar, R. Kumar, K. Bharath, S. Balaji, and R. Rajendran, "Iris recognition using Hough transform and neural architecture search network," 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), pp. 1-5, 2021.

[47] H. Khanzadi, M. Eshghi, and S. E. Borujeni, "Image encryption using random bit sequence based on chaotic maps," Arabian Journal for Science and engineering, vol. 39, no. 2, pp. 1039-1047, 2014.

[48] R. Karim, L. S. Rumi, M. Ashiqul Islam, A. A. Kobita, T. Tabassum, and M. Sagar Hossen, "Digital signature authentication for a bank using asymmetric key cryptography

algorithm and token based encryption," in Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020, 2021: Springer, pp. 853-859.

[49] N. Kumar, S. Saini, and D. Garg, "Color Image Encryption Model Based on 3-D Chaotic Logistic Map and JAYA Algorithm," IETE Journal of Research, vol. 70, no. 12, pp. 8414-8424, 2024.

[50] Y. Huang, L. Wang, Z. Li, and Q. Zhang, "A new 3D robust chaotic mapping and its application to speech encryption," Chaos, Solitons & Fractals, vol. 184, p. 115038, 2024.

[51] D. Zhang, L. Chen, and T. Li, "Hyper-chaotic color image encryption based on 3D orthogonal Latin cubes and RNA diffusion," Multimedia Tools and Applications, vol. 83, no. 2, pp. 3473-3496, 2024.

[52] M. Kumari and S. Gupta, "A novel image encryption scheme based on intertwining chaotic maps and RC4 stream cipher. 3D Res 9 (1): 10," ed, 2018.

[53] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "Secure image encryption scheme based on a new robust chaotic map and strong S-box," Mathematics and Computers in Simulation, vol. 207, pp. 322-346, 2023.

[54] C. G. L. Li, and Chunbao Li, "An Image Encryption Scheme Based on The Three dimensional Chaotic Logistic Map," IJ Network Security and Communication Networks, vol. 21, no. 1, pp. 22-29, 2019.

[55] E. Z. Zefreh, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions," Multimedia Tools and Applications, vol. 79, no. 33, pp. 24993-25022, 2020.

[56] Z. Zhuang, Z. Zhuang, and T. Wang, "Medical image encryption algorithm based on a new five-dimensional multi-band multi-wing chaotic system and QR decomposition," Scientific Reports, vol. 14, no. 1, p. 402, 2024.

[57] C. Xu, Y. Shang, Y. Yang, and C. Zou, "An encryption algorithm for multiple medical images based on a novel chaotic system and an odd-even separation strategy," Scientific Reports, vol. 15, no. 1, p. 2863, 2025.

[58] H. Wen et al., "Exploiting high-quality reconstruction image encryption strategy by optimized orthogonal compressive sensing," Scientific Reports, vol. 14, no. 1, p. 8805, 2024.

[59] M. Kumari and S. Gupta, "A novel image encryption scheme based on intertwining chaotic maps and RC4 stream cipher," 3D Research, vol. 9, pp. 1-20, 2018.

[60] M. Kumar, A. S. Chivukula, and G. Barua, "Deep learning-based encryption scheme for medical images using DCGAN and virtual planet domain," Scientific Reports, vol. 15, no. 1, p. 1211, 2025.

[61] H. Kolivand, S. F. Hamood, S. Asadianfam, and M. S. Rahim, "Image encryption techniques: A comprehensive review," Multimedia Tools and Applications, 2024.

[62] S. S. Jamal, M. M. Hazzazi, M. F. Khan, Z. Bassfar, A. Aljaedi, and Z. ul Islam, "Region of interest-based medical image encryption technique based on chaotic S-boxes," Expert Systems with Applications, vol. 238, p. 122030, 2024.

[63] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, "Medical image encryption: a comprehensive review," Computers, vol. 12, no. 8, p. 160, 2023.

[64] Rosset. "The world famous medical imaging viewer." https://www.osirixviewer.com/,2022,5 (accessed.

[65] NCI. "Cancer imaging archive." https://www.cancerimagingarchive.net/,2022 (accessed.

[66] W. Newhauser et al., "Anonymization of DICOM electronic medical records for radiation therapy," Computers in biology and medicine, vol. 53, pp. 134-140, 2014.

[67] R. Gauriau et al., "Using DICOM metadata for radiological image series categorization: a feasibility study on large clinical brain MRI datasets," Journal of digital imaging, vol. 33, pp. 747-762, 2020.

[68] W. Hou, S. Li, J. He, and Y. Ma, "A novel image-encryption scheme based on a non-linear cross-coupled hyperchaotic system with the dynamic correlation of plaintext pixels," Entropy, vol. 22, no. 7, p. 779, 2020.

[69] A. G. Radwan, S. K. Abd-El-Hafiz, and S. H. AbdElHaleem, "Image encryption in the fractional-order domain," in 2012 International Conference on Engineering and Technology (ICET), 2012: IEEE, pp. 1-6.

[70] P. Praveenkumar et al., "Transreceiving of encrypted medical image–a cognitive approach," Multimedia Tools and Applications, vol. 77, pp. 8393-8418, 2018.

[71] M. Soltani, H. Shakeri, and M. Houshmand, "Maintaining Confidentiality and Integrity of Data and Preventing Unauthorized Access to DICOM Medical Images," Iranian Journal of Electrical and computer Engineering, 2023.

[72] M. Soltani and A. K. Bardsiri, "Designing A Novel Hybrid Algorithm for QR-Code Images Encryption and Steganography," J. Comput., vol. 13, no. 9, pp. 1075-1088, 2018.

[73] M. Soltani, "A New Secure Image Encryption Algorithm using Logical and Visual Cryptography Algorithms and based on Symmetric Key Encryption," Journal of Basic and Applied Scientific Research, vol. 3, no. 6, pp. 1193-1201, 2013.

[74] X. Chai, J. Zhang, Z. Gan, and Y. Zhang, "Medical image encryption algorithm based on Latin square and memristive chaotic system," Multimedia Tools and Applications, vol. 78, pp. 35419-35453, 2019.

[75] J. C. Dagadu, J.-P. Li, and E. O. Aboagye, "Medical image encryption based on hybrid chaotic DNA diffusion," Wireless Personal Communications, vol. 108, no. 1, pp. 591-612, 2019.

[76] J. Tully, J. Selzer, J. P. Phillips, P. O'Connor, and C. Dameff, "Healthcare challenges in the era of cybersecurity," Health security, vol. 18, no. 3, pp. 228-231, 2020.

[77] R. Tertulino, N. Antunes, and H. Morais, "Privacy in electronic health records: a systematic mapping study," Journal of Public Health, vol. 32, no. 3, pp. 435-454, 2024.

[78] Priyanka and A. K. Singh, "A survey of image encryption for healthcare applications," Evolutionary Intelligence, vol. 16, no. 3, pp. 801-818, 2023.