

Research Article

Color Image Steganography: From Fundamentals to Advanced Hiding Techniques Based on Least Significant Bit Algorithms

Saeedeh Khajehbydokhti ¹ | Atena Amini ² | Seyed Mohammad Hossein Moatar ^{3*}

¹Department of Computer Engineering,
Mashhad Branch, Islamic Azad
University, Mashhad, Iran,
Khajehbydokhtisaeeedeh@gmail.com

²Department of Computer Engineering,
Mashhad Branch, Islamic Azad
University, Mashhad, Iran,
Aminiatena376@gmail.com

³Department of Computer Engineering,
Mashhad Branch, Islamic Azad
University, Mashhad, Iran,
Mhmoattar@iau.ac.ir

Corresponding Author

*Seyed Mohammad Hossein Moatar,
Associate Professor, Department of
Computer Engineering, Mashhad Branch,
Islamic Azad University, Mashhad, Iran,
Mhmoattar@iau.ac.ir

Main Subjects: Color Image
Steganography

Received: 11 November 2025

Revised: 15 December 2025

Accepted: 19 December 2025

<https://doi.org/10.82195/ntds.2025.1224200>

Abstract

With the widespread growth of internet usage and continuous data exchange, information security has become a critical concern. Steganography is a technique that enables messages to be imperceptibly hidden within digital files, such as images, in a way that conceals their very existence. Among various steganographic methods, the Least Significant Bit (LSB) technique has attracted significant attention due to its simplicity and the high visual quality of the resulting images. The use of color images further enhances data hiding capacity by providing three color channels (RGB), offering more embedding space. This paper presents a comprehensive review of existing research on color image steganography based on LSB techniques. First, fundamental concepts and color models are introduced. Subsequently, various LSB-based methods are reviewed, including classical LSB, adaptive LSB, randomized LSB, multi-bit LSB, and hybrid approaches. Next, common image quality evaluation metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Structural Similarity Index (SSIM) are discussed, followed by an analysis of the advantages and limitations of these methods. In addition,

the most widely used datasets and evaluation criteria for image steganography techniques are examined. Finally, key challenges and future research directions, including the integration of deep learning and hybrid steganographic methods, are highlighted.

Keywords: Steganography, Data Hiding, Least Significant Bit (LSB), Color Images, Quality Evaluation, Information Security

استگانوگرافی تصاویر رنگی: از مبانی تا روش های نوین پنهان سازی با الگوریتم های مبتنی بر بیت کم اهمیت

سعیده خواجه بیدختی¹ | آتنا امینی² | سید محمد حسین معطر³ * 

چکیده:

با گسترش استفاده از اینترنت و تبادل مداوم داده ها، مسئله ی امنیت اطلاعات اهمیت زیادی پیدا کرده است. استگانوگرافی (Steganography) یا پنهان نگاری روشی است که اجازه می دهد پیام ها به شکلی نامحسوس در فایل هایی مثل تصویر مخفی شوند تا هیچ کس متوجه وجود آن ها نشود. در میان روش های مختلف، تکنیک بیت کم اهمیت (Least Significant Bit-LSB) به دلیل سادگی و کیفیت بالای تصاویر خروجی، بیشتر مورد توجه پژوهشگران قرار گرفته است. استفاده از تصاویر رنگی نیز به دلیل داشتن سه کانال رنگی (RGB)، فضای بیشتری برای پنهان سازی فراهم می کند. در این مقاله، یک مرور جامع بر پژوهش های انجام شده در زمینه ی استگانوگرافی تصاویر رنگی با استفاده از روش های LSB ارائه می شود. ابتدا مفاهیم پایه و مدل های رنگ توضیح داده می شوند، سپس روش های مختلف LSB شامل نوع کلاسیک، تطبیقی، تصادفی، چند بیتی و روش های ترکیبی بررسی خواهند شد. بعد از آن معیارهای ارزیابی کیفیت مثل نسبت حداکثر سیگنال به نویز (PSNR)، میانگین مربعات خطا (MSE) و شاخص شباهت ساختاری (SSIM) معرفی می شوند و در ادامه مزایا و محدودیت های این روش ها بیان می گردد. همچنین مهم ترین دادگان ها و معیارهای ارزیابی روش های پنهان نگاری در این مطالعه مورد بررسی قرار گرفته است. در پایان نیز چالش های اصلی و مسیرهای آینده ی تحقیق، مانند استفاده از یادگیری عمیق و روش های ترکیبی، مطرح خواهند شد.

¹ گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی،

مشهد، ایران،

Khajehbeydokhtisaee@iaui.ac.ir

² گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی،

مشهد، ایران،

AminiAtena376@gmail.com

³ گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی،

مشهد، ایران،

Mhmoattar@iaui.ac.ir

*نویسنده مسئول

سید محمد حسین معطر، دانشیار، گروه مهندسی کامپیوتر،

واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

Mhmoattar@iaui.ac.ir

موضوع اصلی: استگانوگرافی تصاویر رنگی

تاریخ دریافت: ۱۴۰۴/۸/۲۰

تاریخ بازنگری: ۱۴۰۴/۹/۲۴

تاریخ پذیرش: ۱۴۰۴/۹/۲۸

<https://doi.org/10.82195/ntds.2025.1224200>

کلیدواژه ها: استگانوگرافی، پنهان نگاری، بیت کم اهمیت، تصاویر رنگی، ارزیابی کیفیت، امنیت اطلاعات.

۱- مقدمه

با رشد سریع اینترنت و استفاده‌ی روزافزون از رسانه‌های دیجیتال، حفاظت از اطلاعات به یک دغدغه‌ی جدی تبدیل شده است. ما هر روز حجم زیادی داده را از طریق شبکه‌های عمومی ردوبدل می‌کنیم و همین موضوع احتمال سوءاستفاده یا حمله به اطلاعات محرمانه را بالا می‌برد. یکی از روش‌های مهم برای مقابله با این مشکل، استگنوگرافی یا همان پنهان‌نگاری است. برخلاف رمزنگاری که فقط داده را به شکلی ناخوانا تبدیل می‌کند، استگنوگرافی پا را فراتر می‌گذارد و کاری می‌کند که اصل وجود اطلاعات هم دیده نشود. در این روش، داده مخفی در یک فایل دیگر مثل تصویر قرار می‌گیرد و هیچ‌کس متوجه حضور آن نمی‌شود. در بین روش‌های مختلف پنهان‌نگاری، روش بیت کم‌اهمیت (LSB) یکی از پرکاربردترین‌هاست، چون ساده است، کیفیت تصویر را به‌خوبی حفظ می‌کند و فضای مناسبی برای مخفی‌سازی فراهم می‌آورد. استفاده از تصاویر رنگی هم جذابیت بیشتری دارد، چون سه کانال رنگی (قرمز، سبز و آبی) دارند و این یعنی ظرفیت بیشتری برای پنهان کردن داده‌ها نسبت به تصاویر سیاه‌وسفید. این مقاله تلاش می‌کند مروری روی پژوهش‌هایی که در این زمینه انجام شده داشته باشد؛ از روش‌های پایه‌ای گرفته تا نسخه‌های بهبودیافته، معیارهای ارزیابی، چالش‌ها و مسیرهای آینده. هدف این است که تصویری کلی و دقیق از وضعیت فعلی و جهت‌گیری آینده‌ی استگنوگرافی مبتنی بر LSB در تصاویر رنگی ارائه شود.

۱-۱- روش‌شناسی گردآوری و انتخاب مقالات

در این پژوهش، برای انجام یک مرور دقیق و هدفمند در زمینه‌ی استگنوگرافی مبتنی بر بیت کم‌اهمیت^۱ (LSB) در تصاویر رنگی، فرایند گردآوری و انتخاب مقالات با دقت طراحی شد تا بتوان تصویری جامع از وضعیت فعلی تحقیقات ارائه داد. هدف از این مرور صرفاً جمع‌آوری مطالعات پیشین نبود، بلکه بررسی روند پیشرفت روش‌های LSB، معیارهای ارزیابی و مسیرهای پژوهشی آینده بود تا نقاط قوت و ضعف کارهای انجام‌شده مشخص شود و زمینه برای تحقیقات بعدی فراهم گردد. برای جمع‌آوری مقالات، جستجو در پایگاه‌های علمی معتبر از جمله IEEE Xplore، ScienceDirect، SpringerLink، Wiley Online Library، ResearchGate و Google Scholar انجام شد. بازه‌ی زمانی بررسی بین ۲۰۰۱ تا ۲۰۲۵ انتخاب گردید تا هم مقالات قدیمی‌تر و هم پژوهش‌های جدیدتر پوشش داده شوند. این روند باعث شد که مجموعه‌ی نهایی مقالات، هم دقیق و مرتبط باشد و هم بررسی آن‌ها ساختارمند و قابل پیگیری شود. بر اساس همین جدول و داده‌های ثبت‌شده در Excel، تحلیل‌ها و مقایسه‌های لازم بین مقالات انجام شد و نتایج استخراج گردید. در مجموع، از ۱۲۳ مقاله اولیه، پس از بررسی عناوین و چکیده‌ها، ۷۸ مقاله انتخاب شد و با مطالعه کامل، ۴۲ مقاله‌ی نهایی برای تحلیل و مرور در نظر گرفته شد. جدول ۱ خلاصه‌ای از فراوانی مقالات بر حسب نوع آنها نشان می‌دهد. این روش باعث شد روند انتخاب و ارزیابی مقالات شفاف، منظم و قابل بازتولید باشد. در نهایت، هدف اصلی از این مرور، دستیابی به درکی دقیق‌تر از وضعیت فعلی پژوهش‌ها در زمینه‌ی استگنوگرافی LSB و شناسایی مسیرهای مؤثر برای تحقیقات آینده بود؛ به‌ویژه در زمینه‌هایی مثل افزایش پایداری، ظرفیت جاسازی و مقاومت در برابر تحلیل‌های استگانوآنالیز.

¹ Least Significant Bit

جدول ۱: فراوانی مقالات مرتبط و مورد بررسی از دیدگاه محل انتشار

Table 1: Frequency of related and reviewed articles by publication venue

نوع مقاله	تعداد اولیه مقالات	تعداد پس از غربالگری عنوان و چکیده	تعداد نهایی مقاله در مرور
مقالات مجلات	۹۱	۶۳	۳۵
مقالات کنفرانس	۳۲	۱۵	۷
مجموع	۱۲۳	۷۸	۴۲

۲- پیش زمینه

۲-۱- مقدمه ای بر استگانوگرافی

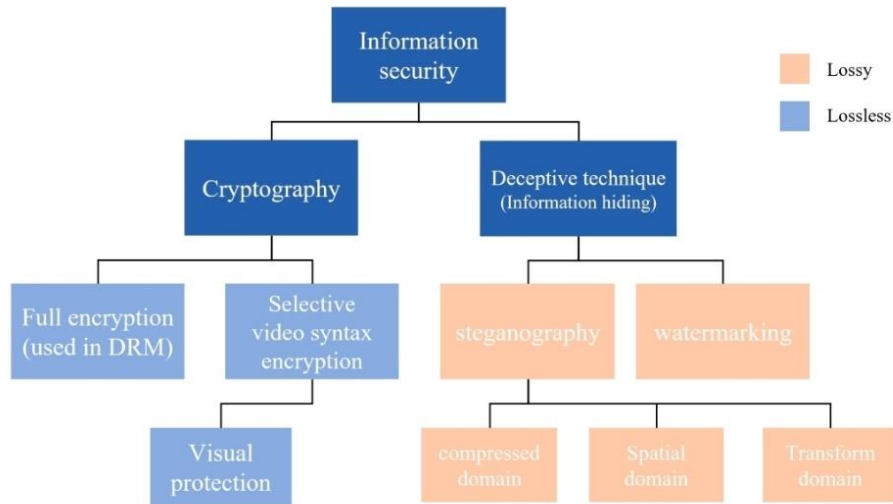
استگانوگرافی^۱ واژه ای است برگرفته از دو واژه ی یونانی steganos به معنای «پوشیده» و graphia به معنای «نوشتن»؛ بنابراین به طور تحت اللفظی «نوشتن پنهان» معنا می دهد. این علم به مطالعه و توسعه ی روش هایی می پردازد که در آن پیام یا داده ای درون رسانه ای دیگر پنهان می شود، به گونه ای که وجود پیام برای ناظران یا مهاجمان غیر قابل تشخیص باشد. با گسترش اینترنت و افزایش حجم تبادل داده های دیجیتال، استگانوگرافی به عنوان یکی از ابزارهای مهم در حوزه ی امنیت اطلاعات، ارتباطات محرمانه و حتی حفاظت از حقوق مالکیت فکری مطرح شده است [1].

۲-۲- تفاوت استگانوگرافی با رمزنگاری و واترمارکینگ

در حالی که رمزنگاری^۲ داده ها را رمزگذاری می کند تا از خوانده شدن آنها توسط اشخاص غیرمجاز جلوگیری شود، استگانوگرافی بر پنهان سازی اصل وجود پیام تمرکز دارد. در رمزنگاری، مهاجم متوجه وجود یک پیام می شود، اما در استگانوگرافی حتی از وجود پیام نیز بی اطلاع است. از سوی دیگر، واترمارکینگ دیجیتال برای اثبات اصالت یا مالکیت داده ها استفاده می شود، نه برای پنهان سازی پیام. تمایز این سه حوزه باعث می شود استگانوگرافی جایگاه ویژه ای در امنیت داده ها داشته باشد [2]. در شکل ۱ و شکل ۲ ساختار کلی امنیت اطلاعات و جایگاه استگانوگرافی نسبت به رمزنگاری و واترمارکینگ نشان داده شده است.

¹ Steganography

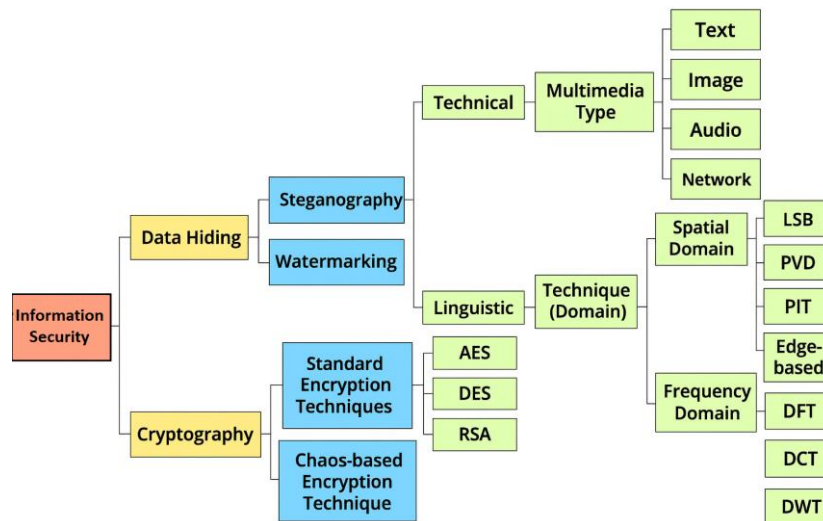
² Cryptography



شکل ۱: ساختار کلی امنیت اطلاعات و جایگاه استگنوگرافی در مقایسه با رمزنگاری و واترمارکینگ [3]

Figure 1: General structure of information security and the position of steganography compared to encryption and watermarking

شکل (۱) به صورت کلی دو شاخه‌ی اصلی امنیت اطلاعات را نمایش می‌دهد: یکی رمزنگاری که مبتنی بر رمزگذاری کامل یا جزئی داده‌هاست، و دیگری تکنیک‌های پنهان‌سازی^۱ که شامل استگنوگرافی و واترمارکینگ می‌شود. در این فلوچارت، مسیر رمزنگاری برای حفاظت مستقیم داده‌ها (مثل DRM یا رمزنگاری انتخابی) استفاده می‌شود، در حالی که استگنوگرافی و واترمارکینگ برای پنهان‌سازی یا تأیید هویت اطلاعات به کار می‌روند. این شکل جایگاه استگنوگرافی را به عنوان بخشی از شاخه‌ی پنهان‌سازی در امنیت اطلاعات مشخص می‌کند.



شکل ۲: نمایش مقایسه‌ای از سه رویکرد اصلی در حفاظت از اطلاعات: رمزنگاری، واترمارکینگ و استگنوگرافی [4]

Figure 2: Comparative representation of the three main approaches in information protection: encryption, watermarking, and steganography

¹ Deceptive Techniques

شکل (۲)، ساختار جامع تری از روش های حفاظت اطلاعات را نشان می دهد و جزئیات بیشتری درباره ی هر حوزه ارائه می کند. در بخش مخفی کردن داده^۱، استگانوگرافی به دو دسته ی فنی^۲ و زبانی^۳ تقسیم شده و در هر کدام از آن ها، حوزه های مکانی^۴ و فرکانسی^۵ مثل DCT، PVD^۶، LSB^۷ و DWT^۸ معرفی شده اند. در کنار آن، شاخه ی رمزنگاری نیز به دو دسته ی رمزنگاری استاندارد (مثل AES^۹، DES^{۱۰}، RSA^{۱۱}) و رمزنگاری مبتنی بر آشوب^{۱۲} تقسیم شده است. این شکل دید عمیق تری از نحوه ی ارتباط میان استگانوگرافی، واترمارکینگ و رمزنگاری در سیستم های امنیت داده ارائه می دهد.

قبل از این مقاله مروری تعداد دیگری از مقالات مروری منحصراً در زمینه نهان نگاری با روش های مبتنی بر LSB ارائه شده اند که از جمله آنها می توان به مقالات [5] و [6] اشاره نمود.

۲-۳- مدل کلی استگانوگرافی دیجیتال

در یک سیستم استگانوگرافی دیجیتال، چهار جزء اصلی وجود دارد: شیء پوششی^{۱۳}، داده ی محرمانه^{۱۴}، الگوریتم جاسازی^{۱۵} و تصویر نهایی یا تصویر استگو^{۱۶}. در مرحله ی ارسال، داده ی محرمانه درون تصویر پوششی جای گذاری می شود تا تصویری جدید ایجاد شود که از نظر بصری با تصویر اصلی تقریباً یکسان است. در سمت گیرنده نیز با استفاده از الگوریتم استخراج، داده ی پنهان شده بازیابی می شود [7]. شکل (۳) مدل کلی استگانوگرافی دیجیتال را نشان می دهد. در این ساختار، داده ی محرمانه با استفاده از الگوریتم جاسازی در تصویر پوششی ادغام شده و یک تصویر استگو تولید می شود. در سمت گیرنده نیز با استفاده از الگوریتم استخراج، داده ی پنهان شده بازیابی می گردد.

¹ Data Hiding

² Technical

³ Linguistic

⁴ Spatial

⁵ Frequency

⁶ Pixel Value Differencing

⁷ Discrete Cosine Transform

⁸ Discrete Wavelet Transform

⁹ Advanced Encryption Standard

¹⁰ Data Encryption Standard

¹¹ Rivest-Shamir-Adleman

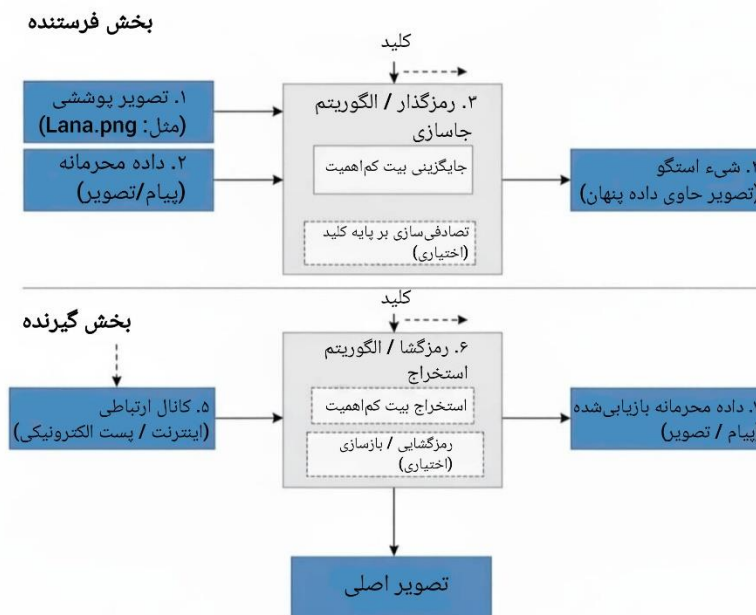
¹² Chaos-based

¹³ Cover Image

¹⁴ Secret Data

¹⁵ Embedding Algorithm

¹⁶ Stego Image



شکل ۳: فلوچارت کلی فرایند استگنوگرافی
Figure 3: Overall flowchart of the steganography process

۲-۴- انواع رسانه‌ها در استگنوگرافی

رسانه‌های مختلفی می‌توانند به‌عنوان بستر پنهان‌سازی داده مورد استفاده قرار گیرند، از جمله متن، صوت، ویدئو و تصویر. در میان این رسانه‌ها، تصویر به دلیل وفور، اندازه‌ی مناسب و تحمل تغییرات جزئی، بیشترین کاربرد را دارد. در این پژوهش، تمرکز بر استگنوگرافی در تصاویر رنگی است، زیرا در مقایسه با تصاویر خاکستری، ظرفیت بالاتری برای جاسازی داده دارند [8].

۲-۵- مبانی پنهان‌نگاری در تصاویر

در استگنوگرافی تصویری، داده‌های محرمانه درون ساختار پیکسلی تصویر دیجیتال جاسازی می‌شوند. هدف این است که داده‌ها به‌گونه‌ای در تصویر پوششی قرار گیرند که برای بیننده یا سیستم‌های پردازشی قابل تشخیص نباشند. برای این کار معمولاً از ویژگی‌هایی مانند شدت رنگ، بافت، یا موقعیت مکانی پیکسل‌ها استفاده می‌شود. در تصاویر رنگی، هر پیکسل از سه مؤلفه‌ی رنگی قرمز (R)، سبز (G) و آبی (B) تشکیل شده است. روش‌های مختلف پنهان‌نگاری تلاش می‌کنند داده را در بخشی از این مؤلفه‌ها قرار دهند که تغییرات آن، کمترین اثر بصری را بر تصویر بگذارد. انتخاب محل مناسب برای جاسازی و طراحی الگوریتمی که بین «ظرفیت»، «کیفیت بصری» و «امنیت» تعادل برقرار کند، از مهم‌ترین چالش‌های این حوزه است [9].

۲-۶- روش بیت کم‌اهمیت (LSB)

روش بیت کم‌اهمیت (LSB) یکی از پایه‌ای‌ترین و پرکاربردترین تکنیک‌های استگنوگرافی تصویری است. ایده‌ی اصلی آن این است که در هر مؤلفه‌ی رنگی (R، G یا B)، بیت آخر یا چند بیت آخر جایگزین بیت‌های داده‌ی محرمانه می‌شوند. از آنجاکه این بیت‌ها کمترین تأثیر را بر مقدار رنگ دارند، تفاوت ایجادشده برای چشم انسان قابل مشاهده نیست. در یک پیکسل ۲۴ بیتی، می‌توان در هر یک از سه کانال رنگی بیت‌هایی را تغییر داد تا داده مخفی شود. برای نمونه، اگر بیت پایانی مقدار رنگ آبی از ۰ به ۱ تغییر

کند، تفاوت عددی در مقدار کلی رنگ بسیار جزئی است، اما همان بیت می تواند بخشی از پیام را در خود نگه دارد. این روش به دلیل سادگی، سرعت بالا و حفظ کیفیت تصویر، به عنوان زیربنای بسیاری از روش های پیشرفته تر مانند LSB تصادفی، تطبیقی یا ترکیبی استفاده می شود [7][10].

۲-۷- مدل های رنگ در استگانوگرافی تصویری

در تصاویر رنگی، مدل رنگی نقش مهمی در کیفیت و کارایی استگانوگرافی دارد. مدل RGB متداول ترین مدل است، اما مدل هایی مانند YCbCr، HSV و CMYK نیز به کار می روند. انتخاب کانال مناسب برای جاسازی داده تأثیر زیادی در کیفیت دارد. برای مثال، [8] از کانال آبی برای جاسازی داده استفاده کرد زیرا چشم انسان نسبت به تغییرات در رنگ آبی حساسیت کمتری دارد، در نتیجه تغییرات بصری کمتری ایجاد می شود. برای بررسی دقیق تر عملکرد مدل های رنگی مختلف در استگانوگرافی، در جدول (۲) مقایسه ای میان چهار مدل متداول ارائه شده است. همان گونه که مشاهده می شود، انتخاب مدل رنگی می تواند تأثیر مستقیمی بر ظرفیت جاسازی و کیفیت بصری تصویر استگو داشته باشد.

جدول ۲: مقایسه مدل های رنگی متداول در استگانوگرافی تصویر
Table 2: Comparison of Common Color Models in Image Steganography

مدل رنگی	اجزای اصلی	حوزه کاربرد در استگانوگرافی	مزایا	معایب
RGB	Red, Green, Blue	پرکاربردترین مدل برای تصاویر دیجیتال رنگی	سادگی، سازگاری بالا با تصاویر خام	حساسیت بصری در کانال های G و R
YCbCr	Luminance (Y) + Chrominance (Cb, Cr)	کاربرد در فشرده سازی (مثل JPEG)	امکان جاسازی در کانال های رنگی بدون افت کیفیت روشنایی	نیاز به تبدیل رنگ
HSV	Hue, Saturation, Value	کاربرد در روش های تطبیقی مبتنی بر ادراک رنگ	مقاومت بالاتر در برابر فشرده سازی	پیچیدگی محاسباتی بالا
CMYK	Cyan, Magenta, Yellow, Black	کاربرد در چاپ دیجیتال و استگانوگرافی صنعتی	تفکیک دقیق رنگ ها	مناسب نبودن برای تصاویر RGB معمولی

۲-۸- معیارهای ارزیابی عملکرد

برای ارزیابی کیفیت تصاویر استگو، معمولاً از سه معیار اصلی PSNR، MSE و SSIM استفاده می شود. این معیارها به صورت عددی نشان می دهند که تصویر استگو تا چه اندازه از نظر کیفیت و ساختار بصری با تصویر اصلی تفاوت دارد.

۱. میانگین مربعات خطا (MSE):

$$MSE = \left(\frac{1}{MN}\right) \sum_{i=1}^M \sum_{j=1}^N [I(i,j) - K(i,j)]^2 \quad (1)$$

در این رابطه، (i,j) : مقدار پیکسل در موقعیت (i,j) از تصویر اصلی

$K(i,j)$: مقدار متناظر در تصویر استگو

M و N : ابعاد تصویر (تعداد پیکسل ها در سطر و ستون)

هر چه مقدار MSE کمتر باشد، تفاوت بین دو تصویر کمتر و کیفیت بالاتر است.

۲. نسبت اوج سیگنال به نویز (PSNR):

$$PSNR = 10 \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \quad (2)$$

که در آن MAX_I بیشترین مقدار ممکن برای یک پیکسل است (برای تصاویر ۸ بیتی، $MAX_I = 255$). مقدار بالاتر PSNR (مثلاً بیشتر از ۴۰ دسی‌بل) نشان‌دهنده‌ی کیفیت بصری بسیار خوب است و معمولاً تغییرات ایجادشده برای چشم انسان غیرقابل تشخیص هستند.

۳. شاخص شباهت ساختاری (SSIM):

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (3)$$

که در آن، μ_x و μ_y : میانگین شدت روشنایی در تصاویر x و y

σ_x^2 و σ_y^2 : واریانس تصاویر

σ_{xy} : کوواریانس بین دو تصویر

C_1 و C_2 : ضرایب ثابت برای جلوگیری از ناپایداری در صورت کوچک بودن مقادیر مخرج

مقدار SSIM بین ۰ تا ۱ است؛ هرچه به ۱ نزدیک‌تر باشد، شباهت ساختاری بین تصویر اصلی و استگو بیشتر است. نویسندگان [22] در پژوهش خود نشان دادند که ترکیب روش‌های هیبریدی منجر به افزایش مقادیر PSNR (تا حدود ۵۲ dB) و SSIM (تا ۰.۹۹) در مقایسه با روش‌های سنتی LSB می‌شود که نشان‌دهنده‌ی بهبود کیفیت و پایداری بالاتر است.

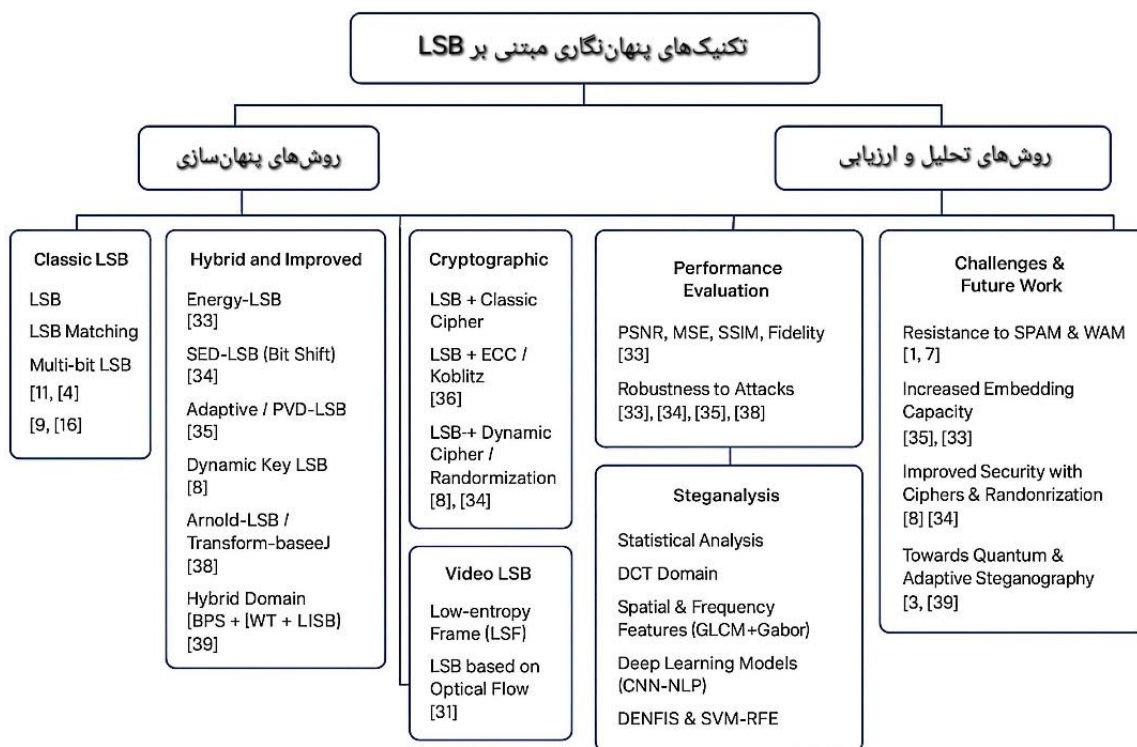
۲-۹- چالش‌های موجود در روش‌های مبتنی بر LSB

باوجود سادگی و کارایی بالا، روش‌های مبتنی بر LSB با چالش‌هایی همراه هستند. از جمله این چالش‌ها می‌توان به حساسیت نسبت به نویز، فشردگی و پردازش مجدد تصویر اشاره کرد. علاوه بر این، روش‌های تحلیل استگانوگرافی^۱ مانند SPAM می‌توانند وجود داده‌های مخفی را شناسایی کنند [10]. نویسندگان [11] تأکید کردند که افزایش ظرفیت جاسازی در عین حفظ غیرقابل تشخیص بودن همچنان یکی از چالش‌های اصلی این حوزه است. همچنین مقاله [12] در مطالعات تحلیل نهان نگاری LSB در تصاویر خاکستری نشان دادند که شناسایی این نوع استگانوگرافی حتی با ابزارهای پیشرفته‌ی یادگیری ماشین دشوار است. در مجموع، روش‌های مبتنی بر LSB به دلیل سادگی، سرعت و کیفیت مطلوب خروجی، از پرکاربردترین روش‌ها در استگانوگرافی تصاویر رنگی محسوب می‌شوند. با این حال، برای دستیابی به امنیت و پایداری بیشتر، تحقیقات جدید به سمت روش‌های ترکیبی حرکت کرده‌اند [9][13]. بنابراین، در بخش بعدی به بررسی دقیق‌تر این رویکردها و بهبودهای مبتنی بر LSB پرداخته می‌شود.

¹ Steganalysis

۳- روش های مبتنی بر LSB

پنهان نگاری مبتنی بر بیت کم اهمیت (LSB) یکی از پرکاربردترین و ساده ترین تکنیک ها در نهان نگاری دیجیتال است که با جایگزینی بیت های کم اهمیت پیکسل ها در تصویر پوشش با بیت های پیام محرمانه، داده را درون رسانه جاسازی می کند [14]. مزیت اصلی این روش سادگی پیاده سازی، ظرفیت نسبتاً بالا و حداقل تغییر در ویژگی های بصری تصویر است. با این حال، آسیب پذیری در برابر تحلیل های آماری و حملات فشرده سازی باعث شده پژوهش های بسیاری در جهت بهبود امنیت، کیفیت و پایداری آن انجام شوند [1, 11, 15, 16, 17]. در شکل (۴)، دسته بندی کلی روش های نهان نگاری مبتنی بر LSB نشان داده شده است.



شکل ۴: تکنیک های نهان نگاری مبتنی بر LSB

Figure 4: LSB-based steganography techniques

۳-۱- روش‌های LSB کلاسیک و اصلاح‌شده

در رویکردهای اولیه، بیت کم‌اهمیت هر پیکسل مستقیماً با بیت پیام جایگزین می‌شد. این روش اگرچه ساده است، اما در برابر حملات آماری و فشرده‌سازی مقاوم نیست [18]. به منظور رفع این محدودیت، پژوهشگران روش‌های اصلاح‌شده‌ای پیشنهاد کرده‌اند که شامل انتخاب تصادفی پیکسل‌ها، تنظیم تطبیقی موقعیت جاسازی و به‌کارگیری فیلترهای مکانی است. برای دسته بندی و مقایسه رویکردهای اصلاح شده LSB، جدول (۳) انواع روش‌های بهبود این تکنیک را نشان می‌دهد.

جدول ۳: خلاصه‌ای از روش‌های اصلاح شده LSB

Table 3: A summary of modified LSB methods

نوع روش اصلاح شده	توضیح مختصر	مزیت اصلی
انتخاب تصادفی پیکسل‌ها (Random Pixel Selection)	در این روش، پیکسل‌های تصویر برای جاسازی داده‌ها به‌صورت تصادفی انتخاب می‌شوند تا الگوی پنهان‌سازی قابل تشخیص نباشد	افزایش امنیت در برابر تحلیل آماری و جلوگیری از الگوهای تکراری
تطبیق موقعیت جاسازی (Adaptive Embedding Position)	موقعیت جاسازی بر اساس ویژگی‌های محلی تصویر (مثل لبه‌ها و بافت‌ها) انتخاب می‌شود تا تغییرات کمتر قابل‌رؤیت باشند	بهبود کیفیت بصری و افزایش PSNR
استفاده از فیلترهای مکانی (Spatial Filtering)	فیلترهای مکانی قبل از جاسازی برای هموارسازی یا افزایش جزئیات تصویر استفاده می‌شود	کاهش نویز و بهبود نسبت سیگنال به نویز
رمزنگاری کلید پویا (Dynamic Key Encryption)	پیش از جاسازی، داده‌ها با کلید پویا رمز می‌شوند تا در برابر حملات مقاوم باشند	افزایش امنیت دولایه (رمزنگاری + پنهان‌سازی)
ترکیب با تبدیل‌های حوزه فرکانس (Hybrid with Transform Domain)	ترکیب LSB با تبدیل‌های DWT یا DCT برای بهبود مقاومت در برابر فشرده‌سازی	افزایش پایداری و کارایی در فشرده‌سازی یا انتقال

همان‌طور که در جدول مشاهده می‌شود، روش‌های اصلاح شده عمدتاً بر افزایش امنیت، کیفیت بصری و پایداری در برابر تحلیل‌های استگانوآنالیز تمرکز دارند. برای مثال، [19] با ترکیب تابع انرژی و LSB روشی ارائه داد که در آن بخش‌های پرانرژی تصویر برای جاسازی انتخاب می‌شوند، و بدین ترتیب اعوجاج تصویر استگو کاهش‌یافته و معیارهای PSNR و MSE بهبود یافتند. همچنین نویسندگان [20] با معرفی روش SED-LSB از عملیات bit-shifting روی داده‌های رمزگذاری شده پیش از تعبیه در LSB استفاده کردند که موجب افزایش امنیت و کیفیت تصویر (PSNR تقریباً برابر ۵۱.۶ و SSIM تقریباً برابر ۰.۹۹۹) شد. از سوی دیگر، برخی روش‌ها با بهره‌گیری از تحلیل لبه یا انتخاب کانال‌های خاص رنگی، به دنبال بهبود کیفیت بصری بوده‌اند.

۳-۲- روش‌های ترکیبی مبتنی بر LSB

برای غلبه بر محدودیت‌های امنیتی LSB ساده، پژوهشگران به ترکیب آن با رمزنگاری یا تبدیل‌های ریاضی روی آورده‌اند. در این گروه، LSB به‌عنوان بخش جاسازی داده باقی می‌ماند، اما پیش‌پردازش رمزنگاری یا درهم‌ریزی^۱ بر داده یا تصویر پوشش اعمال

¹ scrambling

می شود تا امنیت افزایش یابد. به عنوان نمونه، [21] با ترکیب LSB و دو روش رمزنگاری کلاسیک (جایگزینی و جابه جایی) توانستند پیام های متنی را با امنیت بالاتر در تصاویر پنهان کنند و بازیابی بدون از دست رفتن داده را تضمین کنند. در پژوهش [12]، از تبدیل آرنولد برای درهم ریزی تصویر محرمانه قبل از جاسازی در LSB استفاده شد؛ این ترکیب، علاوه بر افزایش امنیت، اعوجاج کمی در تصویر استگو ایجاد کرد و معیارهای PSNR و MSE مقادیر مطلوبی را نشان دادند. روش های مبتنی بر ترکیب حوزه ها نیز از جمله تلاش های مهم برای بهبود کیفیت و پایداری هستند. در این راستا، [22] با ترکیب LSB ، BPS و IWT الگوریتمی چند مرحله ای معرفی کردند که منجر به افزایش PSNR نسبت به روش های کلاسیک شد. این الگوریتم با تقسیم پیام به دو بخش و استفاده از روش های متفاوت برای هر بخش، میان ظرفیت و کیفیت تعادل ایجاد کرد. در ادامه، برخی پژوهش ها از رمزنگاری مدرن نیز در کنار LSB بهره گرفتند؛ مانند [23] که از روش Koblitz در رمزنگاری منحنی بیضوی (ECC) برای رمزگذاری پیام پیش از جاسازی در فریم های ویدئو استفاده کردند. این روش امنیت را به طور چشمگیری افزایش داد، هر چند جزئیات کمی از ارزیابی عددی ارائه شد.

۳-۳- روش های مبتنی بر LSB در تصاویر رنگی

در بسیاری از مطالعات جدید، تصاویر رنگی به دلیل ظرفیت بالاتر و تنوع کانال های رنگ (B, G, R) به عنوان رسانه پوششی انتخاب شده اند. از آنجاکه سیستم بینایی انسان نسبت به تغییرات در کانال آبی حساسیت کمتری دارد، اکثر روش ها داده را در این کانال جاسازی می کنند [19, 24]. به عنوان مثال، نویسندگان [25] با ترکیب تکنیک PVD و LSB ، الگوریتمی تطبیقی برای تصاویر رنگی پیشنهاد کردند که با استفاده از اختلاف پیکسل های مجاور و رمزگذاری XOR، هم ظرفیت جاسازی را افزایش داد و هم مقاومت در برابر تحلیل های RS و هیستوگرام را بهبود بخشید. در مطالعه ای دیگر، نویسندگان [26] از نگاشت X-Box برای توزیع بیت های مخفی در کانال های RGB استفاده کردند؛ این رویکرد باعث افزایش امنیت در برابر نفوذگران و حفظ PSNR بالا شد. همچنین پژوهش [27] با تکیه بر انتخاب تصادفی موقعیت ها در کانال آبی، نشان داد که کیفیت بصری تصویر استگو در حد تصویر اصلی باقی می ماند. این دسته از روش ها با بهره گیری از ویژگی های ادراکی رنگ، بین امنیت و نامحسوس بودن تعادل برقرار کرده اند.

۳-۴- روش های مبتنی بر LSB در نهان نگاری ویدئویی

در حوزه ویدئو، روش های LSB معمولاً فریم به فریم اعمال می شوند و به دلیل حجم زیاد داده ها ظرفیت جاسازی بالایی دارند. با این حال، پایداری و کیفیت در برابر فشرده سازی و تغییرات حرکتی چالش برانگیز است. در این راستا، نویسندگان [28] با استفاده از تبدیل موجک گسسته (DWT) در ویدئوی پوششی، باندهای کم اهمیت را برای جاسازی فریم های ویدئوی محرمانه انتخاب کردند. این روش امکان بازیابی دقیق ویدئوی پنهان را با حفظ کیفیت پوشش فراهم کرد. همچنین نویسندگان [29] با معرفی مفهوم «فریم کم اهمیت» (LSF) و ترکیب آن با LSB توانستند کیفیت ویدئوی استگو را با افزایش PSNR از ۳۹.۵ به ۴۴.۴ دسی بل بهبود دهند. پژوهش های جدیدتر نیز از رویکردهای رمزنگاری برای تقویت امنیت در سطح فریم استفاده کرده اند، مانند [23] که روش ECC- LSB را برای پنهان سازی داده در ویدئو معرفی کرد. روش های مبتنی بر LSB همچنان ستون فقرات بسیاری از الگوریتم های

¹ Bit Plane Slicing

² Integer Wavelet Transform

³ Pixel Value Differencing

پنهان‌نگاری دیجیتال محسوب می‌شوند. سادگی، کارایی، و ظرفیت بالای جاسازی باعث شده این روش، حتی در ترکیب با الگوریتم‌های پیچیده‌تر مانند DWT، IWT یا ECC، نقش محوری داشته باشد.

۴- چالش‌ها، معیارهای ارزیابی و کاربردهای روش‌های مبتنی بر LSB

استگنوگرافی مبتنی بر بیت کم‌اهمیت (LSB) از پرکاربردترین و درعین‌حال آسیب‌پذیرترین روش‌های پنهان‌نگاری در حوزه‌ی تصویر محسوب می‌شود. باوجود سادگی، ظرفیت بالا و کیفیت بصری مطلوب، این روش در برابر انواع تحلیل‌ها و حملات استگانوآنالیز همواره مورد چالش بوده است. مرور مطالعات انجام‌شده در دو دهه‌ی اخیر نشان می‌دهد که پژوهشگران در مسیر بهبود امنیت، ارزیابی کیفی و کاربردپذیری LSB مسیر طولانی و پرفراز و نشیبی را پیموده‌اند.

۴-۱- چالش‌ها در استگانوگرافی LSB

یکی از اساسی‌ترین چالش‌ها در روش‌های مبتنی بر LSB، تشخیص‌پذیری^۱ است. نویسندگان [16] در یکی از نخستین مطالعات کلاسیک نشان دادند که تغییرات ناشی از جاسازی LSB حتی در سطح ۰.۰۰۵ بیت بر پیکسل نیز می‌تواند از طریق تحلیل ظرفیت قابل‌شناسایی باشد. این یافته آغازگر شاخه‌ای از پژوهش‌ها شد که به بررسی مرزهای جاسازی امن^۲ پرداختند. در ادامه، پژوهش‌های بعدی مانند [30] و [31] نیز نشان دادند که تطابق LSB که در آن مقدار بیت تغییر می‌کند تا تفاوت محسوس کاهش یابد، همچنان در برابر تحلیل‌های آماری و ویژگی محور آسیب‌پذیر است. برای مثال، Liu و همکاران با ترکیب انتخاب ویژگی مبتنی بر SVM-RFE و سیستم عصبی - فازی DENFIS توانستند دقت بالاتری در شناسایی تصاویر پنهان‌نگاری شده به دست آورند، و این موضوع خود بیانگر ضعف ذاتی LSB در برابر مدل‌های یادگیری ماشین است. نویسندگان [32] نیز با استفاده از ویژگی‌های مکانی و فرکانسی (مانند فیلتر گابور) نشان دادند که الگوهای بافت و بسامد تصویر می‌توانند نشانه‌هایی از وجود پیام پنهان در LSB را آشکار کنند؛ بنابراین، حتی در صورتی که تغییرات پیکسلی از نظر بصری نامحسوس باشد، تحلیل‌های آماری و فرکانسی قادرند اثرات جاسازی را تشخیص دهند. افزون بر آسیب‌پذیری، ظرفیت محدود جاسازی نیز یکی دیگر از چالش‌های کلیدی است. چنان‌که نویسندگان [9] اشاره کرده‌اند، افزایش ظرفیت بدون افت کیفیت یا افزایش خطر تشخیص یکی از دشوارترین تعادل‌ها در طراحی سیستم‌های LSB است. در این زمینه، مطالعاتی مانند [33] تلاش کرده است با به‌کارگیری نقشه‌های آشوبی^۳ به‌جای مولدهای شبه‌تصادفی سنتی، الگوهای جاسازی را غیرقابل‌پیش‌بینی‌تر و در نتیجه مقاوم‌تر کند. از سوی دیگر، [34] از منظر تئوری اطلاعات استدلال کرد که امنیت LSB تنها در ایجاد عدم قطعیت در فرایند جاسازی نهفته است. این مقاله با بررسی سناریوهای حمله‌ی Known-Cover و Known-Message نشان داد که اگر الگوریتم‌های جاسازی از الگوی ثابت پیروی کنند، کشف آن توسط تحلیل‌گر محتمل است. در کنار جنبه‌های فنی، یکی دیگر از چالش‌های اساسی، وابستگی روش‌ها به ساختار رسانه و الگوریتم فشرده‌سازی است. نویسندگان [30] نشان دادند که آشکارسازهای طراحی‌شده برای تصاویر بازفشرده‌شده تنها در صورتی کارآمدند که الگوریتم JPEG مورد استفاده شناخته شده باشد. این وابستگی، چالش‌های جدی در کاربرد عملی روش‌های LSB در محیط‌های ناهمگن ایجاد می‌کند.

۴-۲- معیارهای ارزیابی کیفیت و کارایی

¹ Detectability

² Safe Embedding Limit

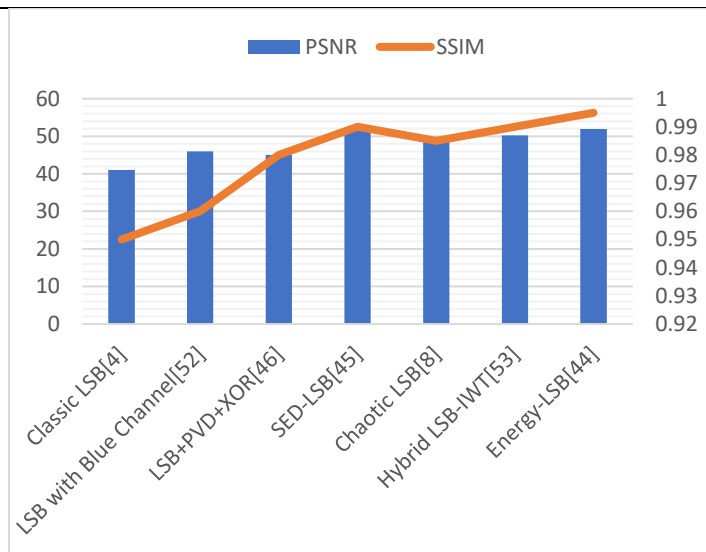
³ Chaotic Maps

در اغلب پژوهش های اخیر، ارزیابی عملکرد روش های مبتنی بر LSB بر پایه ی معیارهای کیفیت بصری و آماری صورت گرفته است. شاخص PSNR به عنوان متداول ترین معیار برای سنجش کیفیت تصویری مطرح است و هر چه مقدار آن بیشتر باشد، اعوجاج تصویر کمتر است. مطالعاتی مانند [26] و [7] نشان دادند که روش های LSB اصلاح شده می توانند مقادیر PSNR بالاتر از 40dB را حفظ کنند، که نشان دهنده ی حفظ کیفیت بصری بالاست. در کنار PSNR، معیارهایی مانند MSE^1 ، $SSIM^2$ و ظرفیت نیز برای ارزیابی دقت بازسازی، شباهت ساختاری و ظرفیت جاسازی داده به کار می روند. مهم ترین این معیارها در جدول (۴) خلاصه شده اند.

جدول ۴: معیارهای ارزیابی

Table 4: Evaluation Criteria

معیار	هدف ارزیابی	بازه مطلوب	تفسیر
PSNR	کیفیت تصویر پس از جاسازی	بالاتر از 40dB	کیفیت عالی
SSIM	شباهت ساختاری تصویر	نزدیک به ۱	حفظ جزئیات
MSE	میزان خطا بین تصویر اصلی و استگو	نزدیک به صفر	تغییرات کم
ظرفیت	میزان داده قابل جاسازی	بسته به روش	هرچه بیشتر بهتر
نرخ خطای بیت	دقت بازایی داده	نزدیک به صفر	بازایی دقیق



شکل ۵: مقایسه مقادیر تقریبی PSNR و SSIM برای چند روش برتر مبتنی بر LSB

Figure 5: Comparison of approximate PSNR and SSIM values for several top LSB-based methods

شکل ۵، مقایسه ای از مقادیر تقریبی PSNR و SSIM برای چند روش برتر مبتنی بر LSB را نشان می دهد. همانطور که مشاهده می شود، روش های ترکیبی مانند LSB آشوبی و SED-LSB در مقایسه با روش های کلاسیک مقادیر بالاتری از PSNR و SSIM ارائه داده اند. این موضوع بیانگر حفظ بهتر کیفیت بصری و شباهت ساختاری در تصاویر استگو نسبت به

¹ Mean Squared Error² Structural Similarity Index

روش‌های پایه است. علاوه بر این، در پژوهش‌های مرتبط با شناسایی و تشخیص، معیارهای دقت^۱، صحت^۲ و نرخ خطای مثبت کاذب^۳ برای ارزیابی مدل‌های یادگیری ماشین به کار گرفته شده‌اند. این معیارها کمک می‌کنند تا علاوه بر جنبه‌ی بصری، امنیت آماری و مقاومت در برابر تشخیص نیز به صورت عددی سنجیده شود. برای مثال، روش‌های مبتنی بر کلید پویا [35] و روش‌های ترکیبی رمزنگاری-LSB اغلب توانسته‌اند بدون کاهش محسوس PSNR، مقاومت بیشتری در برابر تحلیل‌های استگانوآنالیز ایجاد کنند.

۴-۳- کاربردها و حوزه‌های عملی

روش‌های مبتنی بر LSB به دلیل سادگی، سرعت بالا و تطبیق‌پذیری گسترده، در حوزه‌های متعددی مورد استفاده قرار گرفته‌اند. این کاربردها از ارتباطات امن در شبکه‌ها و پیام‌رسان‌ها [18] تا ذخیره‌سازی محرمانه در سامانه‌های چندرسانه‌ای و نظارتی [29] را دربر می‌گیرند. در صنایع نظامی، پزشکی و تجاری نیز از LSB برای پنهان‌سازی داده‌های حساس در تصاویر، ویدیوها و حتی سیگنال‌های صوتی استفاده می‌شود. با این حال، همان‌طور که [16] و [9] اشاره کرده‌اند، گسترش روش‌های استگانوآنالیز باعث شده است که این کاربردها به شدت نیازمند روش‌های LSB تقویت‌شده، تصادفی‌شده و رمزنگاری‌شده باشند. از سوی دیگر، پژوهش‌های نوین مانند [36] که از ترکیب یادگیری عمیق و تحلیل معنایی (CNN-NLP)^۴ بهره برده‌اند، کاربردهای جدیدی را در حوزه‌های قضایی و کشف جرم‌های سایبری گشوده‌اند، جایی که شناسایی پنهان‌نگاری دیجیتال می‌تواند به عنوان مدرک قانونی مورد استفاده قرار گیرد. برآیند مرور گسترده‌ی پژوهش‌ها نشان می‌دهد که استگانوگرافی مبتنی بر LSB، با وجود مزایای متعدد، در برابر تهدیدات تحلیل آماری و یادگیری ماشین همچنان آسیب‌پذیر است. ضعف‌های ذاتی این روش در نواحی زیر متمرکز می‌شود:

- تشخیص‌پذیری در سطوح پایین جاسازی [14], [37], [38]
- وابستگی به نوع تصویر و الگوریتم فشرده‌سازی [16]
- ظرفیت محدود جاسازی در مقابل حفظ کیفیت بصری [39]
- پیش‌بینی‌پذیری مولدهای تصادفی سنتی [15]
- نبود معیارهای ارزیابی امنیتی استاندارد در مقیاس بزرگ [18]

۴-۴- مجموعه داده‌ها و ارزیابی عملکرد

در ارزیابی روش‌های مبتنی بر LSB، از مجموعه داده‌های مختلفی برای سنجش کیفیت و مقاومت الگوریتم‌ها استفاده شده است. در بیشتر پژوهش‌های کلاسیک از دیتاست‌هایی مانند USC-SIPI Image، BOSSBase و BOWS-2 بهره گرفته شده است، درحالی‌که مطالعات جدید تر برای افزایش تنوع داده و ارزیابی در شرایط مختلف، از دیتاست‌های بزرگ‌تری مانند COCO و ImageNet نیز استفاده کرده‌اند. مقایسه مهم‌ترین این دیتاست‌ها در جدول (۵) خلاصه شده‌اند.

¹ Accuracy

² Precision

³ False Positive Rate

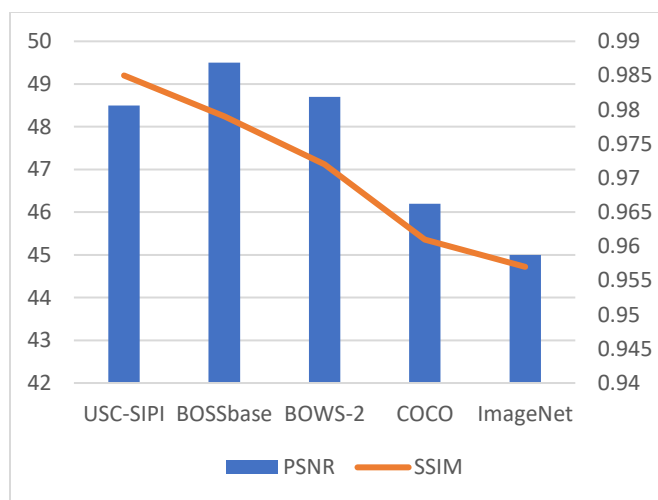
⁴ Convolutional Neural Networks- Natural Language Processing

جدول ۵: مجموعه داده های متداول در ارزیابی روش های مبتنی بر LSB

Table 5: Common datasets used in evaluating LSB-based methods

دیتاست	توضیحات	فرمت و اندازه تصویر	کاربرد	مراجع
USC-SIPI	مجموعه ای از تصاویر عمومی شامل مناظر، چهره و اشیا	۵۱۲*۵۱۲ (BMP, TIFF)	آزمون روش های کلاسیک و تطبیقی LSB	[39],[36],[34],[19]
BOSSbase	مجموعه ای از ۱۰۰۰۰ تصویر خاکستری طبیعی	512*512 (PGM)	ارزیابی روش های هیبریدی LSB	[30],[9],[31],[40]
BOWs-2	مجموعه ای از ۱۰۰۰۰ تصویر طبیعی برای آزمون مقاومت در برابر تشخیص	512*512 (PNG)	مقایسه امنیت و مقاومت روش ها	[16],[28],[25]

برای مقایسه عملکرد روش های مبتنی بر LSB بر اساس معیارهای PSNR و SSIM، شکل (۶) نمودار میانگین این مقادیر را برای چند روش برتر نشان می دهد.



شکل ۶: مقایسه تقریبی مقادیر PSNR و SSIM برای دیتاست های متداول استگنوگرافی تصویری

Figure 6: Approximate comparison of PSNR and SSIM values for common image steganography datasets

بنابراین، مسیر آینده ی تحقیقات در این حوزه به سمت طراحی الگوریتم های هوشمند ترکیبی^۱، استفاده از رمزنگاری پویا و تصادفی سازی آشوبی، و همچنین به کارگیری یادگیری عمیق برای مقاوم سازی جاسازی ها سوق پیدا کرده است. این جهت گیری می تواند به خلق نسل جدیدی از سیستم های پنهان نگاری منجر شود که هم از نظر بصری نامحسوس اند و هم در برابر استگانوآنالیز مقاوم هستند.

¹ Hybrid Intelligent Algorithms

۵- کارهای آینده

باتوجه به مرور انجام‌شده بر پژوهش‌های مختلف در زمینه پنهان‌نگاری مبتنی بر LSB، می‌توان گفت که این حوزه هنوز ظرفیت زیادی برای پیشرفت و نوآوری دارد. بیشتر مطالعات روی بهبود ظرفیت جاسازی، کیفیت تصویر و امنیت متمرکز بوده‌اند، اما همچنان چالش‌هایی وجود دارد که باید در تحقیقات آینده به آن‌ها توجه شود. یکی از مسیرهای مهم آینده، افزایش مقاومت روش‌های LSB در برابر ابزارهای تشخیص مدرن است. همان‌طور که نویسندگان [9] اشاره کرده‌اند، بسیاری از الگوریتم‌های فعلی در مقابل آشکارسازهای پیشرفته هنوز آسیب‌پذیر هستند. بنابراین، طراحی روش‌هایی که بتوانند با تحلیل محتوای تصویر و به‌صورت هوشمند محل جاسازی را انتخاب کنند، می‌تواند باعث افزایش پایداری و امنیت شود. استفاده از مدل‌های تطبیقی مبتنی بر یادگیری ماشین یا شبکه‌های عصبی می‌تواند در این زمینه مؤثر باشد. از سوی دیگر، ورود پنهان‌نگاری به دنیای پردازش کوانتومی فرصت تازه‌ای برای تحقیقات آینده ایجاد کرده است. نویسندگان [17] نشان دادند که می‌توان با استفاده از کد گری بازتابی در تصاویر کوانتومی رنگی، ظرفیت جاسازی را تا ۴ بیت در هر پیکسل افزایش داد. ادامه‌ی این مسیر می‌تواند شامل طراحی الگوریتم‌هایی باشد که در محیط‌های کوانتومی واقعی قابل پیاده‌سازی باشند و امنیت داده‌ها را در سطحی بسیار بالاتر تضمین کنند. همچنین، ترکیب روش‌های LSB با تکنیک‌های رمزنگاری و الگوریتم‌های هوشمند می‌تواند به افزایش امنیت ارتباطات کمک کند. نویسندگان [41] بر اهمیت بهبود امنیت در ارتباطات دیجیتال تأکید کرده‌اند و پیشنهاد داده‌اند که روش‌های LSB باید با رمزنگاری پویا و تولید کلید تصادفی ترکیب شوند. این ایده‌ها می‌توانند در آینده منجر به طراحی سیستم‌های پنهان‌نگاری هوشمندی شوند که به‌صورت خودکار محل و شیوه جاسازی را بر اساس ویژگی‌های تصویر و نوع داده تعیین می‌کنند. در مجموع، مسیرهای آینده‌ی پژوهش در زمینه استگنوگرافی مبتنی بر LSB باید به سمت استفاده از الگوریتم‌های ترکیبی، یادگیری عمیق، و حتی محاسبات کوانتومی حرکت کند تا بتوان به سطحی از امنیت و کیفیت دست‌یافت که پاسخ‌گوی نیازهای ارتباطی و امنیتی دنیای دیجیتال آینده باشد.

۶- نتیجه‌گیری

پنهان‌نگاری مبتنی بر بیت کم‌اهمیت (LSB) همچنان یکی از بنیادی‌ترین و پرکاربردترین روش‌ها در حوزه امنیت داده و ارتباطات محرمانه است. مرور پژوهش‌های انجام‌شده در این زمینه نشان می‌دهد که این روش به دلیل سادگی، کارایی و قابلیت پیاده‌سازی بالا، در کاربردهای متنوعی از جمله تصاویر رنگی، ویدئو، و حتی محیط‌های کوانتومی مورد استفاده قرار گرفته است. با این حال، چالش‌های متعددی همچون آسیب‌پذیری در برابر تحلیل‌های آماری، محدودیت ظرفیت جاسازی، و افت کیفیت بصری همچنان پابرجا هستند.

پژوهش‌های اخیر تلاش کرده‌اند تا این محدودیت‌ها را از طریق بهبود روش‌های جاسازی و ترکیب LSB با تکنیک‌های مکمل برطرف کنند. روش‌هایی مانند Energy-LSB، SED-LSB، یا ترکیب LSB با رمزنگاری‌های پویا و کلیدهای تصادفی، موجب افزایش امنیت و پایداری در برابر استگانوآنالیز شده‌اند. در همین راستا، استفاده از الگوریتم‌های هوشمند مانند شبکه‌های عصبی کانولوشنی (CNN) نیز نقش چشمگیری در شناسایی الگوهای نهان و ارزیابی کیفیت تصاویر داشته است. از سوی دیگر، بخش قابل توجهی از پژوهش‌ها به بهبود معیارهای ارزیابی از جمله PSNR، MSE، SSIM و شاخص‌های مقاومتی پرداخته‌اند. این معیارها نه تنها برای سنجش کیفیت تصویر استگو به کار می‌روند، بلکه در تحلیل عملکرد الگوریتم‌ها در برابر حملات تشخیصی نیز نقش دارند. همچنین، برخی تحقیقات روی افزایش ظرفیت جاسازی از طریق تحلیل ویژگی‌های مکانی و رنگی تصویر یا استفاده از حوزه‌های ترکیبی مانند IWT و BPS تمرکز داشته‌اند که منجر به حفظ کیفیت بصری در کنار افزایش حجم داده‌ی مخفی‌شده شده است. در کنار پیشرفت‌ها، چالش‌های امنیتی و فنی همچنان مهم‌ترین دغدغه‌ی این حوزه باقی مانده‌اند. نتایج پژوهش‌هایی مانند Fridrich و

Zhang نشان می‌دهد که روش‌های LSB در برابر تحلیل‌های آماری یا آشکارسازهای پیشرفته همچنان آسیب‌پذیر هستند. از این رو، جهت‌گیری بسیاری از مطالعات جدید به سمت طراحی سیستم‌های هوشمند مقاوم در برابر تشخیص و استفاده از رمزنگاری‌های چندلایه معطوف شده است.

به طور کلی، مرور انجام‌شده نشان می‌دهد که آینده‌ی استگنوگرافی مبتنی بر LSB در گرو حرکت از روش‌های کلاسیک به سمت الگوریتم‌های تطبیقی، یادگیری عمیق و حتی محاسبات کوانتومی است. تلفیق LSB با مدل‌های مبتنی بر داده، رمزنگاری‌های پویا و روش‌های فشرده‌سازی هوشمند، می‌تواند مسیر رسیدن به نسل جدیدی از تکنیک‌های پنهان‌نگاری امن، مقاوم و باکیفیت را هموار سازد.

مراجع

- [1] Mishra, A. K., & Mishra, P. P. (2012). Suitability of LSB substitution based steganography for digital images: A study. *International Journal of Scientific Research*.
- [2] Patel, N., & Meena, S. (2016). LSB based image steganography using dynamic key cryptography. In *Proceedings of the 2016 International Conference on Emerging Trends in Communication Technologies (ETCT)* (pp. 18–19). IEEE.
- [3] Heo, J., & Jeong, J. (2021). Deceptive techniques to hide a compressed video stream for information security. *Sensors*, 21(21), 7200.
- [4] Hussain, A. Z., & Khodher, M. A. A. (2024). Securing medical images using chaotic map encryption and LSB steganography. *Revue d'Intelligence Artificielle*, 38(1), 313–321.
- [5] Kaur, J. (2014). Steganography using Interpolation and LSB with Cryptography on Video Images - A Review. *International Journal of Computer Applications Technology and Research*, 3(9), 589–591.
- [6] Hashem, S. H., & Zgair, E. T. (2017). Review study among traditional LSB, proposed modified LSB and DWT steganography algorithm. *Al-Mansour Journal*, 27, 37-56.
- [7] Sreedhar, G. (2023). Embedding and extracting hidden messages in images using LSB-based steganography. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*.
- [8] Wang, M.-X., Yang, H.-M., Jiang, D.-H., Yan, B., Pan, J.-S., & Liu, T. (2022). A novel quantum color image steganography algorithm based on turtle shell and LSB. *Quantum Information Processing*, 21, 148.
- [9] Chaturvedi, A. K., Sharma, A., & Sharma, K. (2018). Analysis on LSB based detection methods and hiding strategies with color images. *International Journal of Computer Sciences and Engineering*, 6(7), 687–692.
- [10] Astuti, E. Z., Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A., & Sarker, M. K. (2020). LSB-based bit flipping methods for color image steganography. *Journal of Physics: Conference Series*, 1501(1), 012019.

- [11] Viji, G., & Balamurugan, J. (2011). LSB steganography in color and grayscale images without using the transformation. *Bonfring International Journal of Advances in Image Processing*.
- [12] AlKhuwaytiri, R. M. M., & Olaymi, S. E. Z. (2021). LSB based digital image steganography system. *International Journal of Computer Applications*, 174(17), 1–6.
- [13] Yahia, F., & Abushaala, A. (2024). Cryptography and steganography based on hybrid edge detection and LSB comparing with traditional LSB. *The International Journal of Engineering & Information Technology (IJEIT)*, 12(1).
- [14] Rajput, G. G., & Chavan, R. (2017). A novel approach for image steganography based on random LSB insertion in color images. In *Proceedings of the International Conference on Intelligent Computing Systems (ICICS)* (pp. 1–9). Sona College of Technology, Salem, Tamilnadu, India.
- [15] Juneja, M., & Sandhu, P. S. (2013). An improved LSB based steganography technique for RGB color images. *International Journal of Computer and Communication Engineering*, 2(4), 513–517.
- [16] Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color and grayscale images. *IEEE MultiMedia*, 8(4), 22–28.
- [17] Li, P., & Lu, A. (2018). LSB-based steganography using reflected Gray code for color quantum images. *International Journal of Theoretical Physics*, 57, 1516–1548.
- [18] Somwanshi, D. R., & Humbe, V. T. (2021). A secure and verifiable color visual cryptography scheme with LSB based image steganography. *International Journal of Advanced Trends in Computer Science and Engineering*, 10(4).
- [19] Hussain, Z. M. (2015). Steganography using energy-LSB embedded method. *Al-Mansour Journal*, 23, 87–100.
- [20] Solak, S., & Altınışık, U. (2019). A new approach for steganography: Bit shifting operation of encrypted data in LSB (SED-LSB). *Bilişim Teknolojileri Dergisi (Journal of Information Technologies)*, 12(1), 75–81.
- [21] Shukla, I., Joshi, A., & Girme, S. (2023). LSB steganography mechanism to hide texts within images backed with layers of encryption. In *Proceedings of the 16th International Conference on Security of Information and Networks (SIN)* (pp. 1–6).
- [22] Manjunatha Reddy, H. S., & Raja, K. B. (2012). Hybrid domain based steganography using BPS, LSB and IWT. *International Journal of Computer Applications*, 54(3).
- [23] Pehlivanoglu, M. K., Savaş, B. K., & Duru, N. (2015). LSB based steganography over video files using Koblitz's method. In *Proceedings of the 23rd Signal Processing and Communications Applications Conference (SIU)*. IEEE.
- [24] Naveen, P., & Jayaraghavi, R. (2024). Image steganography method for securing multiple images using LSB–GA. *Wireless Personal Communications*, 135, 1–19.

- [25] Kalita, M., Tuithung, T., & Majumder, S. (2019). An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique. *Cryptologia*, 43(6), 414–437.
- [26] Dagar, E., & Dagar, S. (2014). LSB based image steganography using X-Box mapping. In *Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 24–27). IEEE.
- [27] Almazaydeh, L. (2020). Secure RGB image steganography based on modified LSB substitution. *International Journal of Embedded Systems (IJES)*, 12(4).
- [28] Kolakalur, A., Kagalidis, I., & Vuksanovic, B. (2016). Wavelet based color video steganography. *International Journal of Engineering and Technology*, 8(3), 165–169.
- [29] Solichin, A., & Painem. (2016). Motion-based less significant frame for improving LSB-based video steganography. In *Proceedings of the 2016 International Seminar on Application for Technology of Information and Communication (ISemantic)* (pp. 225–229).
- [30] Zhang, J., & Zhang, D. (2010). Detection of LSB matching steganography in decompressed images. *IEEE Signal Processing Letters*, 17(2), 175–178.
- [31] Liu, Q., Sung, A. H., Chen, Z., & Xu, J. (2008). Feature mining and pattern classification for steganalysis of LSB matching steganography in grayscale images. *Pattern Recognition*, 41(1), 56–66.
- [32] Sahil, & Sinwar, D. (2018). A steganography technique based on chaos for pseudo-random LSB images. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*.
- [33] Muhammad, K., Ahmad, J., Ur Rehman, N., Jan, Z., & Sajjad, M. (2016). CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method. *Multimedia Tools and Applications*, 76, 8597–8626.
- [34] Rafat, K. F. (2020). Prudently secure information theoretic LSB steganography for digital grayscale images. *International Journal of Advanced Computer Science and Applications*, 11(8).
- [35] Alizadeharasi, A., & Safaei Rizi, M. (2015). An improvement on the security of odd-even-LSB based steganography by adding encryption. *International Journal of Science and Research (IJSR)*.
- [36] Angulo, K., Gil, D., Yáñez, A., & Espitia, H. (2025). Hybrid CNN-NLP model for detecting LSB steganography in digital images. *Applied System Innovation*, 8(4), 107.
- [37] Manjula, Y., & Shivakumar, K. B. (2020). Secured image transmission using color transformation fragmented mosaic, chaos-based encryption and LSB mapping steganography technique. *Bioscience Biotechnology Research Communications*, 13(13), 58–66.

- [38] Hassan, Y. A., & Rahma, A. M. S. (2025). Enhanced medical image steganography using improved LSB with conditional MSB based on color vector variety. *Iraqi Journal of Science*, 66(2), 830–843.
- [39] Umbarkar, A. J., Kamble, P. R., & Thakre, A. V. (2016). Comparative study of edge based LSB matching steganography for color images. *ICTACT Journal on Image and Video Processing*, 6(3), 1185–1191.
- [40] Malekmohamadi, H., & Ghaemmaghami, S. (2009). Steganalysis of LSB based image steganography using spatial and frequency domain features. In *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME)*. IEEE.
- [41] Kaushal, S., & Kakkar, A. (2018). LSB based steganography techniques for secured communication. *International Journal of Computer Applications*, 181(10), 1–4.