Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.050834

REVIEW

Randomization Strategies in Image Steganography Techniques: A Review

AFM Zainul Abadin[1,2,*], Rossilawati Sulaiman[1] and Mohammad Kamrul Hasan[1]

[1]Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM) Bangi, Selangor, 43600, Malaysia

[2]Department of Information and Communication Engineering, Pabna University of Science and Technology, Pabna, 6600, Bangladesh

*Corresponding Author: AFM Zainul Abadin. Email: abadin.7@gmail.com

Received: 19 February 2024 Accepted: 18 June 2024 Published: 15 August 2024

ABSTRACT

Image steganography is one of the prominent technologies in data hiding standards. Steganographic system performance mostly depends on the embedding strategy. Its goal is to embed strictly confidential information into images without causing perceptible changes in the original image. The randomization strategies in data embedding techniques may utilize random domains, pixels, or region-of-interest for concealing secrets into a cover image, preventing information from being discovered by an attacker. The implementation of an appropriate embedding technique can achieve a fair balance between embedding capability and stego image imperceptibility, but it is challenging. A systematic approach is used with a standard methodology to carry out this study. This review concentrates on the critical examination of several embedding strategies, incorporating experimental results with state-of-the-art methods emphasizing the robustness, security, payload capacity, and visual quality metrics of the stego images. The fundamental ideas of steganography are presented in this work, along with a unique viewpoint that sets it apart from previous works by highlighting research gaps, important problems, and difficulties. Additionally, it offers a discussion of suggested directions for future study to advance and investigate uncharted territory in image steganography.

KEYWORDS

Information hiding; image steganography; randomized embedding techniques; payload capacity; imperceptibility

1 Introduction

In this modern era, 'information' is the driving force for global development and modern civilization. It plays a vital role in data analysis, knowledge discovering, planning, and decision-making that requires it to be shared with the corresponding parties securely. Information security is preventing unauthorized individuals from vulnerable attacks, accessing, using, disclosing, disrupting, altering, or destroying information and/or information systems to maintain their integrity, confidentiality, and availability [1]. In recent years, the proliferation of digital devices has increased the demand for secure communication and data protection. For secure communication, a number of strategies, including information concealment, watermarking, and cryptography have been developed [2]. Information security can be achieved by implementing cryptographic or data hiding techniques, including either

watermarking or steganography. Fig. 1 represents the taxonomy of different methods of securing information.

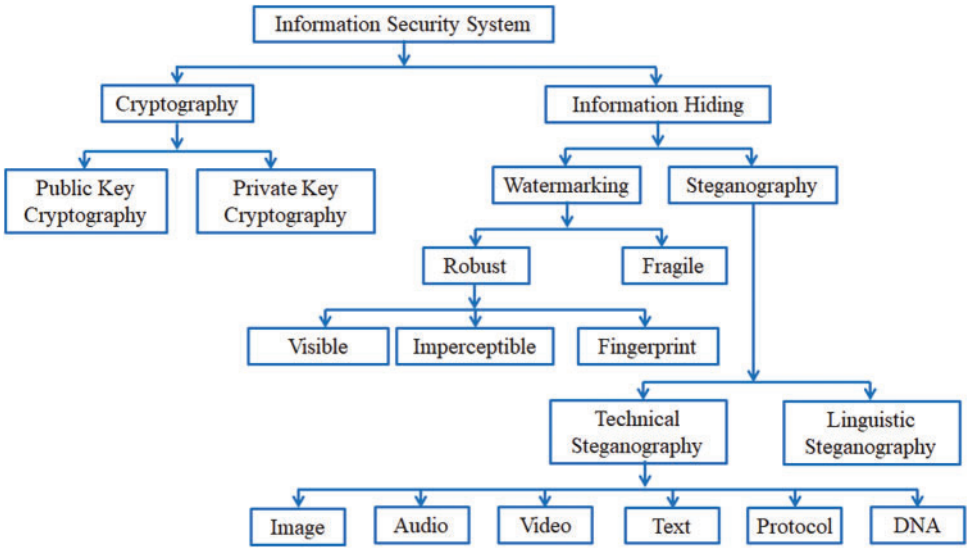

Figure 1: Taxonomy of information security system (Reprinted as reference [3])

To ensure data security, identity, confidentiality, or copyright protection and prevent hackers from detecting and decoding the communications, steganography attempts to encode hidden information into a cover medium [1,2]. Steganography differs significantly from cryptography in that the former works by transforming message data into an unintelligible format that may cause suspicion to intruders. At the same time, the latter prefers to conceal message data within a cover medium, making it challenging for an observer to retrieve it and even hard to identify whether the message is present and its location. Steganography is often used for hiding information within other data, making it undetectable to unauthorized parties [1]. Steganography is useful in situations where secrecy is paramount, and detection must be avoided, such as in intelligence operations or covert communication. Similar keys are typically used in steganography techniques to conceal secret messages and produce stego, or output data. To hide the connection between the two sides, stego should be imperceptible in the cover media. Images, audio, video, text files, protocols, or DNA sequences are examples of digital media assets that are utilized as steganography cover media [3]. Having a lot of redundant space in image files makes it attractive to conceal sensitive information, particularly useful as a cover media. The steganography system deals with images as a hiding media, which is referred to as image steganography. It is the practice of hiding a confidential message inside a cover image without altering its appearance and visual quality [1,2]. Image steganography finds applications in various domains, including covert communication, digital watermarking, and data hiding for security purposes. It ensures safety and privacy by hiding sensitive information such as passwords, login credentials, customer account details, financial data, intellectual property, or any other confidential data within images [2]. It also has applications in copyright protection, forensic investigation, medical images, military communications, and advertising on social media, social engineering, and metadata storage.

An overview of recent studies on different methods and security in image steganography is presented in [4] starting with a summary of the various domain's fundamental knowledge in image

steganography systems. The several types of steganography security techniques such as encryption, randomization, and region-based techniques are then described. Traditional steganographic techniques often employ deterministic algorithms and sequential approaches for embedding confidential data making the system susceptible to attacks and can be detected by steganalysis algorithms. Randomized embedding in image steganography introduces an element of randomness in the data implanting process, making it harder for eavesdroppers and attackers to uncover the concealed message [4]. By incorporating randomness, the image steganographic algorithm can alter the embedding positions or modify the intensity values of pixels in a non-deterministic manner and adds an extra layer of complexity, makes it difficult for attackers to identify the hidden data. The authors in [5] present various techniques of image steganography, including their types, performance criteria, and fundamental ideas. Extensive comparisons are made between the various image steganography techniques to assess the benefits and drawbacks. For a better stego-medium, steganography techniques based on blockchain are studied. Several directions for the future are also indicated. However, data embedding strategies are not grouped under specific methods and discussed.

Authors explore several ways for implementing image steganography, including deep learning, encryption-based, and spatial domain manipulation [6]. This study deals with current advances in image steganography techniques, but traditional image steganography techniques are not elaborately discussed due to the integrated study of large volumes. Additionally, it shows how multiple picture color models interact with image steganography and how different image formats affect different image steganography techniques. Subsequently, steganalysis is clarified and reported. Applying two-layer security, reference [7] reviews recent developments in data security research of steganography incorporation with cryptography techniques. The study outlines the benefits and drawbacks of the current crypto-stego and image steganography approaches and overlooks other approaches.

The key concepts of significant deep learning-based steganography methods are explained in [8]. Three categories for steganography methods: deep learning, hybrid, and traditional, are outlined. Deep learning and hybrid approaches are further broken down into a number of smaller groups. It suggests using standard data sets PASCAL-VOC12, Bossbase, CelebA, ImageNet, USC-SIPI, and CIFAR-100 to assess how well different deep-learning image steganography methods perform. However, the difficulties with the mentioned data sets used in deep learning-based ISS are often overlooked, and other methods are not given enough attention. The technique of information concealment is achieved by coverless steganography, also known as steganography without embedding, which establishes a connection between hidden information and carriers as presented in [9]. The algorithms for coverless video and image steganography are presented in this study and the security of coverless steganography is highlighted.

This study follows a systematic review with the exploration of peer-reviewed journal papers on traditional image steganography methods to summarize the findings in appropriate categories of embedding techniques in association with randomization themes. The purpose of this study was to address the following particular review questions (RQ):

RQ1. Which traditional image steganography methods are used in recent state-of-the-art works?

RQ2. What techniques of randomization are used and how it is involved in association with embedding techniques?

RQ3. What are the performances achieved by different methods in recent works?

Moreover, this study expects to propose different randomization features, research constraints and future recommendations for image steganography research which are consequently presented in

this article. The rest of this article is structured in 5 subsequent sections where Section 2 presents the materials and methods for selecting appropriate research articles to investigate for this study. Review findings are presented in Section 3 highlighting image steganography overview in Section 3.1, system requirements in Section 3.2, traditional image steganography methods in Section 3.3, existing embedding techniques in recent studies in Section 3.4, randomization features in image steganography, and its benefits are presented in Sections 3.5 and 3.6, respectively. Section 4 presents results, discussions, and recommendations. Finally, Section 5 represents the conclusion of this article.

2 Materials and Methods

This study employs a systematic review strategy, which is a formal method for testing and comprehending available research related to a certain research objective and comprises three major phases: review preparation, review leadership, and review reporting [5]. This study was conducted using an appropriate search string to identify relevant articles on existing randomization strategies involved in embedding methods of image steganography, and refining them based on required criteria.

2.1 Review Protocol

The review protocol specifies the methods to be employed in the review. During the planning stage, this study created a review process, and described the context and issues of this study. We only considered all the works published in peer-reviewed journals in English between 2019 and 2023. Only the complete edition of the report in its original format is used. We only used the full edition of the report, where multiple duplicated reports were shown to be accessible in their original formats. The review protocol's main components include data sources, the search process, data selection strategy, and data extraction method. Finally, the findings of this study for critical discussions, and synthesis of the results are presented.

2.2 Data Sources

Relevant research papers were chosen to assist in answering the research questions. Irrelevant research publications that failed to respond to or even support the research topics were excluded. In order to find relevant material, this study used a search method that included selecting appropriate articles from the WoS, Scopus, IEEE Xplore, and ACM digital library online databases. These repositories were selected as they carried significant indexing of multidisciplinary journals, which will limit the exclusion and missing of pertinent publications and include essential research works [5].

2.3 Searching Process

Image steganography was the main field of searching that gives emphasis to the randomization strategies in embedding techniques. Based on a unified query that comprises several keywords, like, "Image steganography", "Data hiding", "Randomized embedding algorithm", "Randomization strategy", "Chaotic function" were syntax for this search execution. Boolean "AND", "OR" operators were utilized to help clarify data based on different keyword patterns for an effective search process. Different search strings generated by symbols and Boolean operators supported by corresponding databases were used to retrieve desired research articles for effective review materials to be investigated. Specific search strings were generated and used for different databases as those databases' have syntax for searching queries are listed below:

WoS shows 27 research articles with the given search string: ALL=((("Image steganography" *OR* "Data hiding") *AND* ("Randomized embedding algorithm" *OR* "Randomization strategy" *OR*

"Chaotic function"))). *Scopus shows 53 research articles with the given search string: TITLE-ABS-KEY ((("Image steganography" OR "Data hiding") AND ("Randomized embedding algorithm" OR "Randomization strategy" OR "Chaotic function"))*. *IEEE Xplore shows 91 research articles with the given search string: ((("Image steganography" OR "Data hiding") AND ("Randomized embedding algorithm" OR "Randomization strategy" OR "Chaotic function"))*. *ACM digital library shows 97 research articles with the given search string: [[All: "image steganography"] OR [All: "data hiding"]] AND [[All: "randomized embedding algorithm"] OR [All: "randomization strategy"] OR [All: "chaotic function"]]*.

2.4 Data Selection

In assessments of previous articles, data selection is important. Based on recognizable and related terms, the study created advanced search strings for four different databases to gather pertinent material that examined related literature and methodologies [4]. Without further refinement, the aforementioned query first generated 268 articles, of which 27 came from the WoS, 55 from Scopus, 91 from IEEE Xplore, and 97 from the ACM digital library. These documents were then gradually narrowed down followed by the methodology.

2.5 Data Extraction

The authors reviewed the preliminary studies to ensure that image steganography was the only field used. All the articles that were found were listed in a spreadsheet along with their titles, descriptions, and supporting information. Based on the set of exclusion and inclusion parameters, the preliminary searched papers were improved to ensure that the review questions and search strategy aligned with the relevant materials. First, the coverage period for the studies to be included was set at 2019–2023. Second, since those topics include more pertinent steganography-related works, only image steganography avoidance of text, audio, video, protocol, or DNA steganography was taken into consideration for inclusion in this study. Thirdly, only published English-language articles apart from books, book chapters, conference proceedings, and review papers were taken into consideration for inclusion in this review. Certain journals are indexed in both because superior quality journals are attributed to two or more databases. It gives rise to the problem of document duplication. After refining 142 conference articles, 39 duplicate records were found and eliminated by a Microsoft Excel spreadsheet merge of the documents taken from four databases. After following the selection and refusal criteria, the pertinent research publications were systematically collected using the search strategy depicted in Fig. 2.

Then, 75 documents are chosen to retrieve from various journals; however 17 of them were unsuccessful. The final step was to manually screen the publications to choose the most related to the RQs. The title, keywords, and abstract of each article were evaluated in order to determine which ones were appropriate for this review and which ones addressed the linkage in embedding techniques linked with randomization procedures. Fourteen documents were eliminated due to their incompatibility with the review questions. The PRISMA process declaration [10] was used throughout the entire process of choosing papers. Consequently, 44 papers were ultimately for review in order to address the study topics.

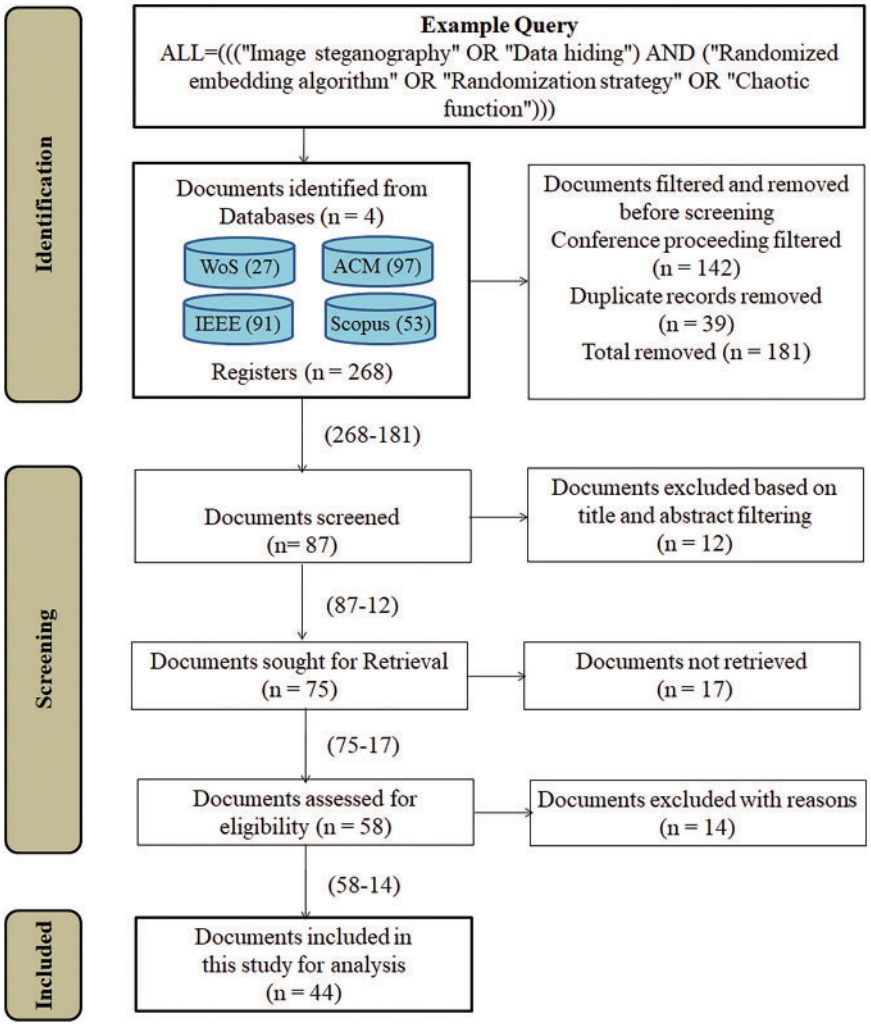

Figure 2: Data collection and extraction process for this study

3 Findings and Interpretations

The data acquired for this review came from the four databases mentioned above. This section offers the descriptive analysis and findings of this study, based on the critical investigation of 44 research articles selected from publications from the last five years. The findings of this study are presented in Sections 3.1 to Section 3.6, while the results, discussions, and future recommendations are reported in the following sections.

3.1 An Overview of Image Steganography

Greeks were renowned for their use of covert communication. The ancient Greek terms "stegano" and "graphy," which both relate to "cover writing," are combined to form the term "steganography." Steganography was first used a hundred years ago. Histiaeus used tattooing as steganography to write secret messages on the skull of his slave, which he then sent out once the slave's hair had grown to cover the tattoo [11]. Demaratus used a waxing coat pad, engraved messages in the tablet, and then waxed the

table. The messages were scratched when scraped off the wax. It must be waxing coated again, making it look like a blank tablet. The messages were transmitted securely, avoiding any suspicion [11,12].

Image steganography (IS) is a technique of hiding or embedding information within an image in such a way that it is difficult to detect or perceive. The primary goal of steganography is to conceal the existence of the embedded data, ensuring that it remains unnoticed by casual observers [13]. Unlike cryptography, which focuses on making data unreadable, steganography focuses on making the presence of the data undetectable. In the context of image steganography, the information such as text, another image, or any data, is integrated into the pixels of the original image. It can be used for secure communication, copyright protection, and digital watermarking, but it can also be employed for malicious purposes, such as hiding malware or unauthorized information transmission. As a result, the detection of steganographic content has become an important area of research in computer forensics and cybersecurity.

The carrier for image steganography is an image that comprises and conceals the hidden information within an image. Fig. 3 illustrates the pictorial presentation of the fundamental image steganography system. "Cover image" is the object used to describe the image that carries the payload, and the term "secret message," contains private information. The "embedding strategy" essentially is the technique or method used to hide the secret message within the cover image, which is also called a "stego-image" and contains an optional "stego-key". This key needs to be communicated between the two parties. This stego-image is the final image output and hides the confidential data. Correspondingly, extraction is the opposite of embedding where "extraction strategy" is the method that recovers the secret message hidden within stego image utilizing the same securely shared stego-key.

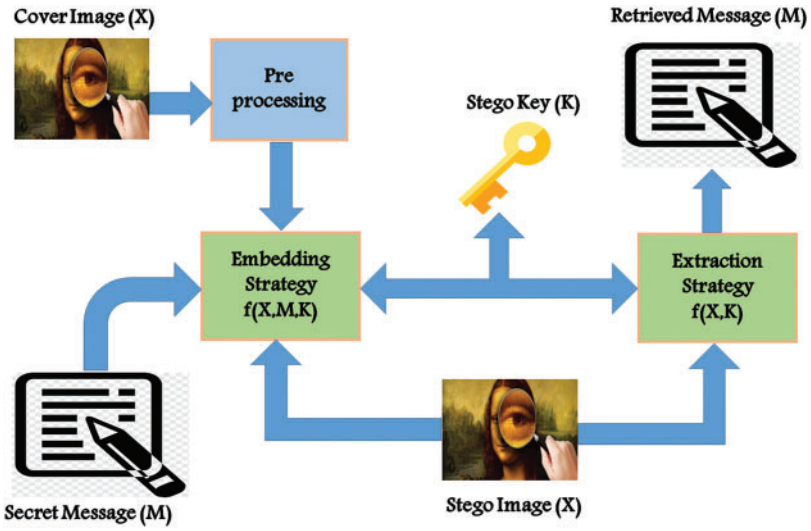

Figure 3: Fundamental technique of image steganography

As seen in Fig. 3, a steganographic encoder uses a steganography scheme for embedding the secret message (M) and additional encryption if needed. The actual file which is referred to as cover media (X) must be concealed. Using least significant bit (LSB) encoding methods, the steganographic encoding function denoted as f(X, M, K) incorporates the hidden secrets within the cover image. The final stego image has no discernible differences from the cover image file. Thus, encoding is finished. A steganographic decoding function denoted as f(X, K) uses an extraction technique to retrieve the original message in such a way that the secret message is recovered after the stego is fed into it.

3.2 Image Steganography System Requirements

Image steganography (IS) has gained significant consideration for its massive applications in areas like covert communication, information security, and digital forensics [14]. The primary challenge of the image steganography technique is to preserve a fair steadiness between stego imperceptibility and more embedding capacity, along with strong security that sets it apart from related systems like watermarking and encryption [15]. The objective of IS is to conceal secret information within an image. The primary task of intruders is to see if anything of value is hidden inside it. They address the possibilities of altering the cover contents in that scenario. Keeping these factors in mind, the effectiveness of steganography is assessed based on its capacity to boost data hiding rates, lower carrier distortion rates, and fend off attacks [15].

Security, payload capacity, and imperceptibility are the three attributes to be considered in image steganography required to conceal secret data [3]. Some of the research mentioned these three properties along with robustness. The requirements ratio for a good system is reflected in Fig. 4, which is mandatory for the fairness of the system. These are the most important variables that affect how well steganography is configured. Nonetheless, the quantity of secret data and the stego image quality are sometimes traded off. Therefore, a good image steganography system should meet the following key requirements (Fig. 4).

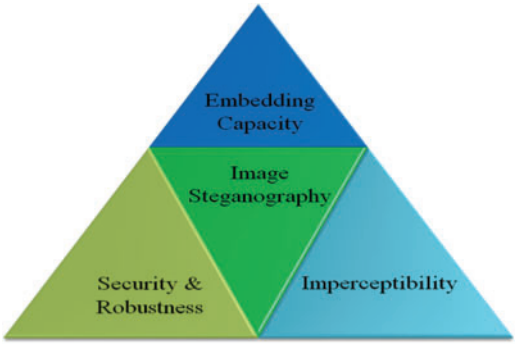

Figure 4: Balancing the requirements of image steganography system (Reprinted as reference [3])

3.2.1 Security

In IS system, "security" refers to "undetectability" and/or "unnoticeability." When the data being hidden by a steganography technique cannot be discovered by a third party, it is considered secure. Mitigating the security requirements would guarantee that the data remains safe by preventing access by unauthorized people or machines when transmitting across insecure channels. Security differs from imperceptibility, where RS analysis, bit error rate (BER), or relative entropy measures the security of hidden data, while imperceptibility measures the index of similarity between stego and cover image. The steganography system must be secure and capable of protecting the hidden message from illegal admittance. In some cases, it should also use strong encryption techniques to prevent data leakage and protect against statistical attacks like chi-square analysis, pixel value differencing-based histogram analysis, etc. [16].

Steganalysis detection attacks can be of two types: passive and active [7]. These attacks can affect image steganographic systems. Attackers are drawn to the stego-image in an attempt to recover or even identify the presence of hidden data bits. Security is the most important evaluation factor in the steganographic system. Security techniques can be evaluated in terms of how well it withstands

steganalysis attacks. Attackers can use a variety of statistical techniques, such as bit error rate (BER), RS analysis, relative entropy test, and pixel difference histogram (PDH), among others, to ascertain whether confidential information is being exchanged during a conversation between two parties.

3.2.2 Embedding Capacity

A pixel's embedding capacity (EC) is the total number of secret bits it contains [17]. The ability to conceal data is a key component that determines how successful an image steganography technique is. Bit rate, also known as concealing capacity, is the ratio of the size of the hidden data to that of the stego, as demonstrated in [18]. The major goal of IS systems is to enhance steganographic security and capacity while preserving the stego image's perceived transparency. For the system to hold secret data, it must have a large capacity. It should be possible to store a significant quantity of concealed data inside the cover image without sacrificing its quality or making the hidden data noticeable. To keep high payload capacity while preserving security and imperceptibility is a major steganographic difficulty. In image steganography, Average Embedding Capacity (AEC) is evaluated by bits per pixel (bpp) and defined as Eq. (1) or (2) [19]:

$$AEC(bpp) = \frac{Totalembeddedbits}{Totalnumberofpixelsintheimage} \tag{1}$$

It can be written more specifically as

$$AEC(bpp) = \frac{Totalno.ofembeddedbits}{W \times H} \tag{2}$$

In the Eq. (2), W and H stand for the image's width and height.

3.2.3 Imperceptibility

The primary goal of image steganography is imperceptibility, which seeks to conceal secret information behind cover media while maintaining the stego image's nearly identical visual quality [19]. Even when statistical techniques are used, it is not expected that the human eye (HVS) would be capable of understanding it. The stego image must be imperceptible, which means the visual quality of the stego image properties should be almost similar to the cover image. IS system's first concern is imperceptibility, whose goal is to conceal hidden information followed by an algorithm involved in making the stego image undetectable to HVS even when statistical tools are used. A variety visual quality assessing criteria in image steganography have been documented in the literature, including peak signal to noise ratio (PSNR), mean square error (MSE), structural similarity index metric (SSIM),histogram analysis, universal image quality index (UIQI), and normalized cross correlation (NCC), etc. are investigated [19]. The PSNR is one of the important quality evaluating parameters presented in Eq. (3). Researchers must do a visual quality evaluation on the stego image to ensure perfect imperceptibility.

$$PSNR = 10log_{10}\frac{R^2}{MSE} \tag{3}$$

MSE is the mean square error and defined as Eq. (4):

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M \times N} \tag{4}$$

3.2.4 Robustness

Robustness is the capacity to withstand the possibility of altering or erasing sensitive information. Robustness determines the ability of the embedding and extraction process to resist corruption by a third party using any kind of processing [20]. Robustness is often evaluated in the transform domain, although more recently, several spatial domain steganographic techniques have been taken into consideration while developing an algorithm. In reality, robustness is a stego-image's capacity to hold secret data in the face of multiple statistical steganalysis or image processing operations like scaling, sharpening, noise addition, blurring, cropping and rotation, etc. The steganography system should be robust and able to resist various forms of steganalysis and operational attacks like filtering, compression, noise injection, and image modification. The system should also be able to adapt to different types and sizes of images and support a variety of image formats. In addition, the IS system should be efficient and fast, with a low computational overhead [21]. It should be able to work seamlessly across different image formats, devices, and platforms.

3.3 Traditional Image Steganography Methods

Image steganography of the traditional approach involves embedding secret data within specific domains or components of an image. Instead of directly manipulating the pixel values, these techniques exploit the characteristics of different image domains to hide information. In image steganography systems, digital images are used for embedding taking into account any of the image's domains either spatial or temporal or both in adaptive mode [20]. The research articles on image steganography of conventional approaches found in the last decade have shown different steganography methods. Different researchers adopt different methods in spatial domain and temporal/transformation domain, which are reported in the next section based on the taxonomical presentation shown in Fig. 5. Spatial domain IS techniques operate directly with the spatial components of an image.

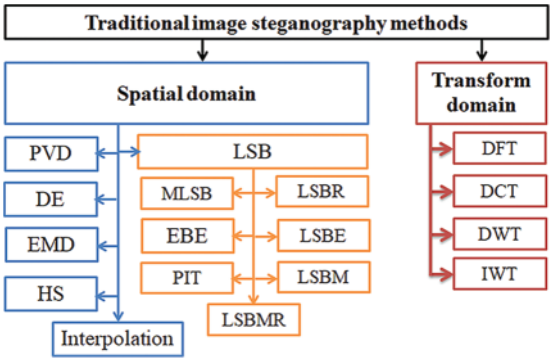

Figure 5: Taxonomy of traditional image steganography methods

Spatial domain image steganography techniques exploit specific image characteristics, such as texture or color variations, to embed secret data. The spatial domain techniques have a better embedding capability with minor image quality deterioration and are based on direct alteration of pixel intensities. There are various conventional methods exist in spatial domain image steganography including Least Significant Bit (LSB) substitution [22,23], LSB exchange [24,25], LSB replacement [24], LSB matching [25], Modified Least Significant Bit (MLSB) [26,27], Pixel Value Differencing (PVD) [28], Difference Expansion (DE) [29], Exploiting Modification Direction (EMD) [30], interpolation based image steganography [31], Histogram Shifting (HS) [32], etc.

LSB the simplified term for least significant bit substitution, replacement, or exchange is an established method of spatial domain image steganography that is frequently used because of its ease of use and high capacity potential. This approach implants the secret bits in the LSBs of selected pixels in the cover image to reduce distortion. Moreover, information may be hidden using more than one LSB of a pixel to boost payload capacity; however, this may reduce the stego image's visual quality [23]. Notably, some enhancements to the original LSB have already been implemented. An improved variant of the LSB approach is called LSB Matching (LSBM) [25]. In an effort to enhance the earlier techniques, [1] presented the LSBMR method which stands for LSB matching revisited. It makes minimal alterations to the carrier image while embedding confidential information within the LSB. Two secret bits are simultaneously embedded into two pixels; the first is implanted directly, and the second is produced based on how those two bits relate to each other. The intention is to make it harder to find the hidden information than it would be with conventional methods [1].

PVD is the concealing technique of binary data in the pixel where the pixels have no overlapping block in the cover image. The number of bits in the payload is determined by calculating and quantizing the difference between the two pixels in several areas [28]. One of the other data-hiding methods is to conceal portions of the edge where the intensity values of the pixels abruptly change. These methods, known as Edges-Based Embedding (EBE) Steganography [23,33] enable the concealment of substantial payloads in those specific edge pixels and, in some cases utilizing both the non-edge and edge pixels. Pixel Indicator Technique (PIT) [34] is an additional LSB technique that improves the resilience and security of traditional systems. This approach utilizes three indicator LSBs from separated RGB channels of the corresponding cover pixel and selects one of the pixel's color channels to serve one as an indicator for two other channels, which are employed in the process of embedding. Another method for improving security is EMD, which divides the cover image into n-pixel segments. These segments correspond to secret digits using the $2n + 1$ arry scheme resulting 1 pixel is changed by ± 1. Since there are 2n possible pixel alterations for a group of n and one scenario where there are no changes, there are $2n+1$ possible digits to be implanted in secret [30]. In the DE-based image steganography, the cover image has been allocated into two pairs of pixel (Px;Py) that are not overlapped [29]. Histogram shifting is used to construct a histogram of the cover image. To allow for message concealing, pixels between the zero and peak places are subsequently moved in the direction of the zero point [32]. A high-resolution image is typically produced from a low-resolution one by image interpolation [31]. This strategy estimates unknown site values using the values at a known location. Neighbor mean interpolation (NMI) is an interpolation method developed by [35] that uses a conventional scaling-up procedure.

Transformation domain or frequency domain image steganography techniques leverage the properties of the frequency components of an image [36]. The techniques involving various transformations like Discrete Cosine Transformation (DCT) [37], Discrete Fourier Transformation (DFT) [38], Discrete Wavelet Transformation (DWT) [39], Integer Wavelet Transform (IWT) [40], etc., are the example of transform domain methods. In transform domain IS, images are converted into frequency domain components and the secrets are implanted by modifying frequency coefficients, such as altering magnitudes or phases [41]. The benefit of frequency or transform domain methods is the potentiality to hide information in perceptually significant areas while minimizing visual artefacts. In the context of capacity and complexity, the lesser payload capacity and greater computational complexity of the transform domain make them slower [42]. When it comes to Reversible Data Hiding (RDH) schemes, the use of transformation domain image steganography more specifically, the complex set of two-dimensional RDH and the transformation of Polar Harmonic Fourier Moments

(PHFMs) provides a robust RDH scheme that improves the system's visual quality and ability to withstand geometric attacks [36].

3.4 Existing Embedding Techniques in Recent Studies

On the basis of this review of the fundamental hidden principles, three groups of currently used image steganographic approaches may be identified: traditional image steganography, coverless image steganography, and deep learning-based image steganography [43]. Spatial domain and transform domain are two categories of traditional image steganography base embedding domains. Coverless image steganography [44] establishes mapping rules between cover image features and secret messages to synthesize the secret data into the image texture through particular algorithms rather than changing the cover image's properties [43] but still suffers with low payload, datasets limitations, and distorted image quality. Deep learning based image steganalysis makes the researcher hungry to develop deep learning image steganography based on Convolutuional Neural Network (CNN) [45], Generative Adversarial Networks (GAN) [46], etc., carring the higher order complexity of training, testing, accuracy, and datasets challenges [43].

According to the review objectives the authors concentrated the traditional image steganography researches and includes Mahdi et al. [47] suggest choosing LSB of cover pixels with random parameters and multi-level encryption for highly secured and improved image steganography. The visual transparency of the stego image is ensured through odd and even pixel categorization. It improves the image's security and PSNR by applying data compression using the Huffman coding technique before implanting the data, which enhances a larger payload capacity. The article by Dash et al. [48] performs Boolean function with a loss-less compression technique has better embedding capacity introducing more space for data embedding. The research by Ahmed et al. [49] uses double XORing with LSB and binary equivalent of secret message, a two-layer security were proposed with the implementation of randomized embedding. First, the message is encrypted using a binary double XOR operation. Then, LSB in the carrier image hides the encrypted data. Well-known assessment metrics, including PSNR, MSE, histogram distribution, and entropy, have been calculated to assess the quality of their suggested system. Bit inversing map (BIM) with the addition of Huffman code to improve the image quality is suggested by [25]. Pradhan et al. have created hybrid image steganography methods [50] that effectively guard against pixel difference histogram (PDH) analysis and RS analysis. These algorithms integrate LSB substitution, EMD, and PVD. They point out that low security and low capacity are the two main obstacles to employing the LSB approach to insert hidden data in image steganography.

The PVD and modified LSB substitution-based IS technique is proposed by taking care of different pixel block scenarios for embedding secret data. This research to increase the hiding capacity improves the quality of the stego while minimizing the complexity of the embedding process in different variations, including pixel difference histogram (PDH), fall of boundary problem (FOBP), and RS analysis [51]. In the current research, randomization is often used with other techniques to increase security. Different modular and chaotic functions with randomization through pseudorandom number generator (PRNG) to select pixels, blocks, patterns, etc. are used during the embedding process. PRNG is also used with the Exclusive OR (XOR) operation to encrypt the secret message before embedding the data into the stego image, which produced high capacity and security [52].

In order to increase security and confidentiality, a well-known traditional method was applied [53] to incorporate a fresh take on the circular shape-based encryption of crucial data. The encryption process involves simple calculations for having benefits from the coordinates of the main circle's center. The encrypted data is hidden in the pixels in the circular regions of the cover image [54], employs

the LSBMR technique, which selects a zone on the basis of the absolute differences that exist in two neighbouring pixels. Only sharper edge sections are employed for lower embedding rates, and by modifying a few parameters, more edge pixels can be eventually freed for data concealing at higher embedding rates. Research performed in [55] makes use of mapping secret info into bits of cover pixels. This research introduces multiple-chaotic maps to generate chaotic sequences for tracking shuffled bits' locations, hence improving security performance.

According to Singh et al. [56], it is advised to use a hash-based method with Canny edge detection when putting forth a secure color image steganography. First, different color (RGB) image types are used for cover media; the text is used as secret data. The Canny method is used to detect edges, and a hash function for inserting text data into the cover image is utilized. Various image formats, including jpg, jpeg, bmp, and tiff, are supported by the proposed approach and tested as well. The research proposed by Satar et al. [57] is an approach to combine steganography and cryptography, suggesting two security layers. The RSA and Diffie Hellman algorithms are looked at in the suggested system. Users can embed the secret data in the selected pixel using the Diffie-Hellman method, while RSA handles the encoding and decoding of the secret data. Consequently, the proposed system attains security with higher PSNR and excellent image quality. This model was more complex and showed that hackers cannot obtain confidential data.

A study proposed by [58] suggests using inverted 2-bit LSB and Arnold's Cat Map (ACM) for secure image steganography. An image is encoded using the ACM using the pixels' randomness. The 2-bit LSB is inverted and used to embed the ACM result into a cover. Furthermore, using an inverted 2-bit LSB, two bits in the bit plane of the cover image were changed to secret information bits. This replacement strategy will make attackers hesitant as they attempt to understand the encrypted images. PSNR and entropy were used to assess the experiment's outcomes and compare the quality of the cipher and stego images. The complexity of the embedding technique can be obtained by introducing noise in the temporal domain [59]. Random noise is used against statistical attacks to increase security and capacity, which enhances security by using the night tour algorithm with the Huffman code. With the proposed method, all pixels in the cover image were used. Experimental outcomes exhibit higher PSNR with high embedding capacity. Discrete Wavelet Transform (DWT) [39] in medical images by using de-noising processes while increasing the PSNR and using the LSB substitution method.

Sharma and Srivastava proposed to combine steganography and cryptography [26], which has led to the development of an innovative system. The cover image was subjected to the 2-dimensional haar discrete wavelet transform (2-D HDWT) to extract its coefficient features. Meanwhile, the secret images were subjected to the advanced encryption standard (AES) method to encode them before the concealment within the cover image. The cover image, the secret image, and the stego image were combined using the alpha blending function after the 2-D HIDWT was applied to the alpha blending result. The combined use of steganography and cryptography in the suggested system increased its imperceptibility and dependability [60]. Information in medical images can be concealed without distortion using a hybrid-multi level of image steganography that combines data compression, encryption, and a two-stage high data concealment technique, as presented in [61]. This allows for flexible and secure transfer capabilities. The technique starts with encrypting the secret text using the Triple DES algorithm. The following step is to embed the secret encrypted cipher message into the host image while maintaining the integrity of the image.

3.5 Randomization Features in Stochastic Image Steganography

Stochastic image steganography is a method of hiding information within digital images by using random or pseudo-random processes to determine the embedding locations and patterns [62]. Unlike deterministic approaches, which follow a fixed, predictable pattern, stochastic methods leverage randomness to obscure the presence of hidden data, making it more challenging for unauthorized parties to detect or extract the concealed information. Image steganography techniques based on stochastic computing deals with probabilistic approaches for secret data embedding rather than binary steganography. In the stochastic method, an eight bit pixel may produce 256 (0-255) distinct weighted probability values based on stochastic functions that help increasing the payload capacity than the binary embedding methods [63]. By employing probabilistic models, these techniques can optimize the balance between imperceptibility and payload capacity [62]. Advanced stochastic methods may also adapt to the image content, using more complex algorithms to further disguise the hidden data amidst natural image features. The security of stochastic steganography often relies on the secrecy of the random seed used for data embedding. In contrast to deterministic methods, stochastic approaches make it significantly more challenging for attackers to reverse-engineer the embedding process. Additionally, stochastic methods can incorporate noise-tolerant encoding schemes to ensure that the embedded data remains intact even after image manipulations like compression or scaling [63].

Randomization techniques in nondeterministic or stochastic image steganography methods increase the security and robustness of the hidden data [62,63]. This study discovers a number of randomly selected domains in the data implanting and cover image modification process, making the system challenging for adversaries or steganalysis algorithms to identify the presence of concealed information. The data hiding domains of pixels, blocks, patterns, or bit plane [59] in the cover images may be selected randomly. Operation may be performed by adopting either random permutation, random noise injection, random spread spectrum, or random pixel intensity modification [59], and even multiple features may be applied in the same work to make it more robust. Random permutation involves randomly permuting the order of pixels in an image before embedding data. This strategy generates pixel positions to determine the order in which the secret data will be embedded [64].

The secret message block is mapped to a specific pixel position in the cover image based on the permutation sequence. By rearranging the pixel positions randomly and unpredictably, the random permutation technique provides high security and resistance against steganalysis attacks. Random noise injection comprises adding random noise to an image before embedding data [65]. The noise helps to mask the hidden data, making it more difficult for an attacker to detect. Random spread spectrum involves spreading the hidden data across multiple frequency bands in the image. By doing so, the hidden data becomes more difficult to detect as it is distributed across a wider range of frequencies [66]. Random spread spectrum techniques utilize randomization to embed data using a spread spectrum modulation scheme. Random pixel intensity modification selects pixels randomly in the cover image and modifies their intensity values to encode the hidden data based on the message content. The modifications are designed to be subtle to maintain the image's visual quality [58].

3.5.1 Random Pixel Selection-Based Image Steganography Techniques

This strategy randomly selects pixels within the cover image and replaces them with bits of the hidden data according to the embedding techniques involved. In this method, the embedding algorithm determines the order and number of pixels to modify based on the data to be hidden [59]. Random pixel selection can be achieved by generating random coordinates within the image or using a pseudorandom

sequence generator. By choosing random pixels, the steganography process becomes more secure, as it is more difficult for an attacker to detect the hidden data. The random pixel selection-based image steganography techniques, their strengths, limitations, and performances found in this study are summarized in Table 1.

Table 1: Findings of random pixel selection based image steganography techniques

[Ref.] Method	Method's description, random features, and strengths	Payload PSNR	Limitations
[67] LSBM	Modified LSB matching based reversible data hiding (RHD) method performs two stages of embedding in pixel pairs chosen by random permutation, provides high payload, improves security, and resists pixel difference histogram (PDH) and regular-singular (RS) analysis.	6 bpp 48.14 dB	Time complexity high. Visual quality low.
[68] PVD	Particle swam optimization (PSO) based PVD method selects appropriate pixels by random permutation offers high imperceptibility, and resists RS analysis.	2.14 bpp 42.47 dB	High computational complexity.
[69] DE-EBE	Difference expansion (DE) and edge detection based RDH uses DE areas by random permutation for data embedding. Enhanced DE method of RHD employing edge detection.	1 bpp 30.40 dB	Low PSNR, imperceptibility.
[70] DE	Two-way difference expansion based RDH method calculates 1D array and difference between two adjacent pixels for data embedding by random noise injection. RDH scheme, 2D matrix formatted Stego, low distortion.	0.7 bpp 32.0 dB	Low payload, PSNR near to 30 dB (Threshold).
[53] LSB-ROI	Circle shape region of interest (ROI) based LSB method uses Caesar encryption and random permutation of RGB pixels. Improves visual quality, zero bit error rate (BER), and resists statistical attacks.	1 bpp 71.59 dB	Difficult to identify circle shape pixels. Complexity high.

(Continued)

Table 1 (continued)

[Ref.] Method	Method's description, random features, and strengths	Payload PSNR	Limitations
[71] LSB	Pseudo-random pixel and bit selection-based LSB method uses 3-3-2 bits in RGB for embedding by XOR coding. Two phases PRNG based permutation and spread spectrum embedding achieves high security.	1 bpp 39.27 dB	Low payload. Weak against statistical attacks.
[72] LSB	Skew tent map-based LSB method employs skew tent chaotic map for color channel's pixel selection by pseudo random permutation involving 1st and 4th LSBs embedment. Improves security and imperceptibility.	0.55 bpp 52.62 dB	Low payload. Computational complexity high.
[73] LSB	Enhanced one-dimensional (1D) chaotic map based LSB method involves sine and logistic map for random pixel intensity modification in secure data embedding.	1 bpp 38.02 dB	Weak against histogram analysis.
[74] EMD	Knight tour (KT) algorithm-based EMD method adopts compression, encryption, and random permutation. Improves security, and resist chi square analysis.	1 bpp 52.73 dB	Higher payload causes poor imperceptibility.
[16] HS-LSB	Block-based HS and LSB method measures the pixels based on peak and zero distribution of histograms and uses peak histograms by random pixel intensity modification for secret data embedding. Robust and RDH system offers high security and visual quality.	0.9 bpp 58 dB	Steganalysis tests required. The structure of the cover image is ignored.
[75] MLSB	Modified LSB method employs DES encryption, and XOR operations with compression embeds data by random key sequences picked by random permutation. Secured system, and simple to implement.	- 53.51 dB	No benchmark is compared. Not sufficient tests performed.

(Continued)

Table 1 (continued)

[Ref.] Method	Method's description, random features, and strengths	Payload PSNR	Limitations
[13] LSB	Random color pixel and MLSB method. XOR encrypts secret message and embeds data using random pixel intensity modification employing Duffing and Circle map chaotic functions. Good visual quality and high security.	0.62 bpp 82.73 dB	Low payload. Encryption key needed.

3.5.2 Random Block Selection-Based Image Steganography Techniques

In this approach, instead of individual pixels, blocks or regions of the image are randomly selected for embedding data [58]. The block size can vary, and the embedding algorithm determines the specific blocks to modify based on the embedding strategy. Random block selection can be performed using random block scanning or pseudorandom numbers. The random block selection-based image steganography techniques, their strengths, limitations, and performances in this study are summarized in Table 2.

Table 2: Findings of random block selection based image steganography techniques

[Ref.] Method	Method's description, random features, and strengths	Payload PSNR	Limitations
[76] Interpolation	Interpolation-based LSB method uses interpolation scale hiding space and random spread spectrum for embedding. High payload and security; resists PDH and RS analysis.	3 bpp 37.54 dB	No steganalysis test performed.
[77] DDE-MPVD	Multidirectional pixel value differencing (MPVD) method based on decreased difference expansion (DDE) uses non-overlapping 2×2 blocks of pixels for data embedding with random permutation. High payload, imperceptibility, and resists Benchmark 4.0.	2.88 bpp 38.5 dB	Non-structural attack analysis absent. Irreversible system.

(Continued)

Table 2 (continued)

[Ref.] Method	Method's description, random features, and strengths	Payload PSNR	Limitations
[78] Interpolation	Scaling of the image performed by inverse interpolation method used and intersectional blocks are solved by inverse interpolation equation. Random permutation and spread spectrum used. RDH scheme; resists RS analysis.	0.5 bpp 58.7 dB	Higher execution time. Low bpp.
[79] Interpolation	2D parabolic interpolation method uses of local diversity and random permutation for data hiding. RHD scheme of high payload capacity.	1.7 bpp 32.74 dB	Low security. Execution time high.
[80] HS	Pixel value grouping based on multilevel histogram modification method uses max and min blocks shifting. Robust and secure system uses random permutation and spread spectrum for data embedding.	0.6 bpp 35 dB	Time complexity high. Low payload capacity.
[81] HS	Histogram shifting based on prediction error (HSPE) uses signed representation to improve visual quality, and security. Random noise injection based data embedding.	0.31 bpp 34.96 dB	Very low payload No steganalysis test observed.
[82] DCT	Block selection-based DCT method utilizes frequency coefficients and random spread spectrum based blocks for data embedding. Reduces stego's distortion, and highly secure system.	- 52 dB	Payload not measured. Steganalysis test absent.
[83] DFT	Computer sensing DFT method uses both the real and imaginary coefficients for customizable payload. Random spread spectrum and pixel intensity used for data embedding; provides high security and payload capacity.	2 bpp 40 dB	High complexity. BER present. Statistical analysis needed.

(Continued)

Table 2 (continued)

[Ref.] Method	Method's description, random features, and strengths	Payload PSNR	Limitations
[84] DWT	DWT method based on HVS and cover model. Random noise injection and spread spectrum used for data hiding. Performs high security, and resists statistical attacks.	1500 bits 70.2 dB	Computational complexity high. More test needed.
[85] IWT	Multilevel integer wavelet transform (IWT) method based on sub-band coefficients and location maps; uses lossless compression and random spread spectrum in embedding. Improved IWT scheme with high security.	0.77 bpp N/A	Steganalysis test required. Imperceptibility not clear.
[86] IWT-MDLE	Integer wavelet transform (IWT) and multidirectional line encoding (MDLE) method uses four sub-bands of three by three non-overlapping blocks of embedding regions. Random spread spectrum and permutation used. Resists image processing, RS and PDH attacks.	1.84 bpp 34 dB	Edge pixels are not enough for high payload. PSNR near 30 dB.
[87] IWT-PSO	Particle swam optimization based IWT method finds suitable hiding matrix of pixel blocks for embedding with random noise injection and spread spectrum. Chi square and RS tests performed successfully.	2.25 bpp 41.45 dB	Time complexity high. Visual quality should improve.
[88] LSB	XOR encoded LSB method groups the block of pixels and random pixel intensity feature based data embedding. The Stego key is shared with the recipient. High security, identical SSIM, resists RS and PDH analysis.	0.25 bpp 51 dB	Low payload for overhead data. Computational complexity high.

(Continued)

Table 2 (continued)

[Ref.] Method	Method's description, random features, and strengths	Payload PSNR	Limitations
[37] DCT	Histogram modification-based DCT method employs double chaotic function based encryption and random spread spectrum increases security and HVS quality.	0.26 bpp 41.7 dB	Extra note affects payload capacity. Avoid attack tests.
[89] DCT	Quantized DCT method shuffles row column and Huffman coding employs random spread spectrum based embedding. Enhances security and capacity of simple DCT method. Security high and defend geometric attacks.	0.25 bpp 53.68 dB	Poor payload. Time complexity high.
[90] LSB-EBE	Block-based edge adaptive LSB method uses texture region, edge and non-edge blocks for embedding chosen by local complexity of standard deviation of blocks. Random permutation and pixel intensity used for embedding. Highly secure and defend statistical attacks.	∼1 bpp 65.78 dB	Complex and inaccurate for big block size. Low payload.
[30] EMD	Compression and encryption-assisted EMD method uses Huffman Coding and Vigenere cipher with Knight tour algorithm. Random block and pixel intensity modification based embedding enhances EMD's performances. High security, visual quality, and resist chi-square attack.	1.6 bpp 55.71 dB	Huffman tree and encryption key reduces payload. Nonstructural test required.

3.5.3 Random Pattern Selection-Based Image Steganography Techniques

This method introduces random patterns or masks for embedding data in the image. The patterns define the positions or regions where the data will be embedded, creating a randomized distribution [91]. The patterns can be dynamically predefined or generated using algorithms based on random numbers or pseudo-random functions like chaotic map, collatz conjecture, nonlinear congruential generator, etc. The embedding algorithm applies the patterns to the cover image, modifying the corresponding pixels or regions based on the hidden data. The random pattern selection-based image

steganography techniques, their strengths, limitations, and performances found in this study are summarized in Table 3.

Table 3: Findings of random pattern selection based image steganography techniques

[Ref.] Method	Method's description, random features, and strengths	Payload PSNR	Limitations
[28] PVD-LSB	PVD and LSB combined method randomly uses 2 × 2 pixel blocks to select pixel patterns and difference table is produced for determining no of bits to be embedded. High security and imperceptibility with good capacity.	3.5 bpp 35.5 dB	High time complexity. Steganalysis test absent.
[92] LSB	LSB method with XNOR and Fibonacci uses Huffman coding and Boolean encryption with random permutation to boost capacity and security. High security, good visual transparency, and more hiding space in RGB image.	0.49 bpp 66.61 dB	Computational complexity high. Low payload.
[93] LSB	Chaotic bit pattern-based LSB method selects bit patterns by XOR generated control bits for grayscale image. Random pixel intensity modification is used for data embedding. High payload, security, and imperceptibility.	2.75 bpp 51.96 dB	Image format restricted. Steganalysis test required.
[94] LSB	Optical character reader based LSB method utilizes character features of Chars74K dataset. Random spread spectrum based hiding offers good HVS and security.	2–3 bpp 43.09–36.44 dB	Complexity high. Steganalysis test absent.
[95] DE	DE method based on image color palette transformation changing feature plane selects pixels for embedding based on random noise injection and spread spectrum.	0.35 bpp 74.58 dB	Low payload Statistical attack test required.
[96] LSB	Hamming code-based LSB method uses canny edge detector and random pixel intensity and spread spectrum for data embedding to edge and non-edge pixels. Enhances visual quality and security.	0.2 bpp 68.43 dB	Poor payload. Hamming code adds extra payload.

(Continued)

Table 3 (continued)

[Ref.] Method	Method's description, random features, and strengths	Payload PSNR	Limitations
[97] LSBMR	Complex block pair and texture complexity-based LSB Matching Revisited method uses high pass filter with 3×3 mask. Multi-bit XOR with random noise injection and permutation used for data embedding. System performs high-quality, security, capacity, and resists steganalysis.	2.09 bpp 44.16 dB	Computational complexity high. More attacks test required.
[98] LSB	Logistic map of OTP-XOR and Huffman coding-based LSB method performs region-adaptive embedding using random noise injection and permutation. High security, good visual quality and statistically robust system.	1 bpp 61.9 dB	Huffman tree overhead exist. Computational complexity high.
[99] EBE-LSB	Edge detection based XOR encoded LSB method uses Canny and Soble edge detectors to find sharp edges and embedding is done by XORing and random permutation. Enhanced payload and PSNR with reduced distortion.	40 Kbits 64.2 dB	Non edge pixels not used.

3.5.4 Random Bit-Plane Selection-Based Image Steganography Techniques

Random bit-plane embedding involves randomly selecting bit-planes within the cover image and replacing them with the bits of the hidden data. Each bit-plane represents a specific bit position in the pixel values. For example, in an 8-bit grayscale image, each pixel has eight-bit planes [59]. The embedding algorithm randomly selects bit-planes and substitutes the maximum allowed bits with the hidden message bits. The random bit-plane selection-based image steganography techniques, their strengths, limitations, and performances found in this study are summarized in Table 4.

Table 4: Findings of random bit-plane selection based image steganography techniques

[Ref.] Method	Method's description, random features, and strengths	Payload PSNR	Limitations
[55] LSB	Multiple chaotic data mapping in LSB method shuffles the bits of the cover pixel and improves the security of the simple LSB. Random spread spectrum and noise injection used for data embedding. Highly secure system, robust against steganalysis attacks and histogram analysis.	1 bpp 73.46 dB	Low payload. Complexity high.
[100] EMD	Exploiting modification direction based hiding method uses 2×4 mask for 256×256 embedding matrix replacement. Random pixel intensity modification is used for embedding. The system is secure and robust against bit-plane attacks.	1 bpp 49 dB	Payload limited. RS analysis required.
[101] EMD	Hashed-Weightage Array-based Extended EMD method prepares an array by PRNG. Variable payload depends on the weighted array and embedding rate is 2KN uses random pixel intensity modification and permutation. Reduced Stego's distortion and resists RS analysis.	4 bpp 35 dB	Low PSNR. Security decreases after 3 bpp.
[102] LSB	Shuffled and flipping channel modified LSB method employs multilayer encryption LSBs of the other two channels hide data by random pixel intensity modification. Performs high security and resist statistical attacks.	0.86 bpp 71.05 dB	Poor payload. Computational complexity high.
[103] LSB	Lucas sequence-based LSB method employs Fibonacci random sequence. R channel of RGB is used as R indicator and random pixel intensity is used for embedding. Low visual distortion, geometrically and statistically robust.	0.8 bpp 57.27 dB	Cover's structure is ignored. Low payload than LSB.

(Continued)

Table 4 (continued)

[Ref.] Method	Method's description, random features, and strengths	Payload PSNR	Limitations
[104] DWT-LSB	Hybrid of DWT and LSB method involves RSA encryption and Huffman coding compression. Random spread spectrum and permutation is used for embedding. Performs high Security, imperceptibility and resist various attacks.	1.32 bpp 40.31 dB	Lower capacity for extra bits of encryption key.

3.6 Benefits of Randomization in Image Steganography

Randomization technique (RT) in image steganography offers a variety of advantages, including the following:

- **Increased security:** The randomization strategy helps enhancing the protection of the steganographic system as the embedding locations become unpredictable and difficult to detect [55].
- **Improved resistance against statistical analysis:** RT distributes the hidden data randomly across the cover image, making it harder for statistical analysis to identify, thus enhancing the resistance against steganalysis attacks [90].
- **Enhanced imperceptibility:** RT often prioritizes maintaining the cover image's visual quality. By distributing hidden data randomly, changes made to the image are spread out, reducing the likelihood of noticeable visual artefacts [105], thus preserving the imperceptibility of the stego image [96].
- **Increased capacity:** RT allows for a higher embedding capacity than deterministic methods. The random selection of embedding locations permits a more flexible allocation of bits, increasing payload capacity [77].
- **Improved robustness against compression:** Random embedding techniques exhibit better resistance to compression operations, such as lossy image compression algorithms maintaining the integrity of the hidden information even after compression [101].
- **Flexibility in embedding algorithms:** RT provides flexibility in choosing the most effective algorithm to mitigate specific requirements, applications or scenarios [98].
- **Efficient embedding and extraction processes:** RT can be designed to have efficient embedding and extraction algorithms, enabling secret messages to be retrieved accurately and efficiently [100].

4 Result, Discussion, and Recommendations

4.1 Observations

A critical scrutiny of the recent works of traditional image steganography techniques discovers some sort of randomization strategies that select cover image domains for secret data hiding and a variety of random operations performed for boosting the security strength of the embedding algorithm. The review results show some articles in this study employ random pixel selection-based image steganography techniques, some utilize random block selection-based image steganography

techniques, some involve random pattern selection-based image steganography techniques, and others use random bit-plane selection-based image steganography techniques in association with different image steganography methods. The secret data implanting domains are randomly chosen by adopting either any one or more randomization operations such as random permutation, random spread spectrum, random noise injection, and random pixel intensity modification. Data embedding algorithms employ a variety of PRNGs including the chaotic function of linear and nonlinear properties, collatz conjecture, linear congruential generator (LCG), nonlinear congruential generator, etc., with their user-defined logic to implant secret data in an efficient random fashion instead of sequential embedding. Researchers assessed their research using meaningful and precise performance criteria. Fig. 6 reflects the different randomization-associated data embedding scenarios in recent image steganography systems. The random sequences, frequently used in image steganography, depend on the "chaos function", a mathematical function that exhibits chaotic behavior characterized by sensitivity to initial conditions and a seemingly random, unpredictable trajectory over time. Chaos functions produce pseudo-random sequences from the complex and unpredictable behavior of the chaotic system that improves the security of the image steganography systems and, unfortunately has low payload capacity, one of the research challenges to be addressed in this field.

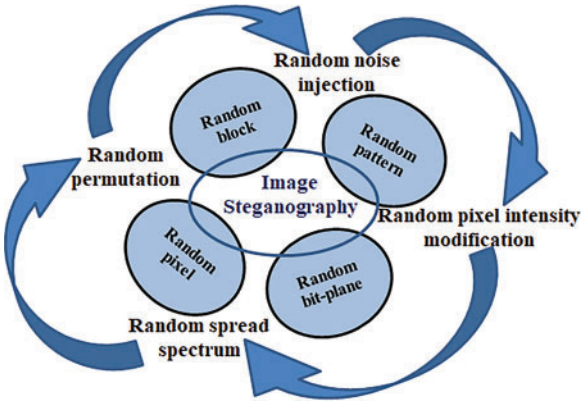

Figure 6: Summary of randomized strategies in image steganography techniques

4.2 Discussions

The principal goal of an image steganography system is to hide sensitive data within a cover image without adding untrustworthy artifacts. In order to attain optimal security, strong imperceptibility, and a high embedding rate, it is imperative to address the primary issues present in the current state of work and strengthen the system. Researchers have improved the performance of steganographic algorithms to achieve large payload capacity, high security, and high imperceptibility. The primary focus is security; the method should conceal from the attacker that embedded data exists within the cover image. Furthermore, even if an attacker finds the original secret message, it should be concealed so well that they cannot decipher its meaning. Recently, several ideas have been applied to image steganography to provide excellent security; some are more secure than others. In most cases, high security has been achieved by implementing random strategies in the embedding phase in addition to an extra layer of cryptographic security employed on the secret message to be hidden. Improved embedding algorithm employing random features along with suitable cover image manipulation found in this study improves stego's visual quality and enhances imperceptibility. As the volume of data is

increased to be hidden, the system needs more hiding capacity for secret data to be implanted. But high bpp causes the stego image distortion and makes it suspicious in HVS.

The state of the works uses a variety of intelligent techniques to find more embedding space by choosing the edge and non-edge pixels, sharp and smooth regions, and randomly embedding into them, which improves the meaningful hiding capacity, keeping visual quality identical. Since an image is made up of smooth and non-smooth or high and low-frequency regions, the visible features of the image are also used to create a security level. Data embedded in a smooth region may become more distorted, compromising the privacy of sensitive information. Another way to conceal the relationship between pixels and secret information without producing obvious distortion is using number systems to generate virtual bit planes. The security constraints of the conventional spatial domain approaches are circumvented by such features. Another method that has been used to ensure steganography security is frequency domain steganography, which involves selecting suitable positions to implant secret data that needs high computational cost but low hiding capacity. Encryption is the most commonly utilized idea, adding extra protection level in steganographic techniques and enhancing security. To improve the system's security, encryption can be achieved using techniques like OTP, RSA, AES, and 3DES, in conjunction with security keys. On the other hand, the ideas of permutation, substitution, XOR, or XNOR operations are also used in user-defined encryption algorithms. By scattering the secret bits around the cover image using random sequences generated by chaos functions, the degree of security can also be greatly increased.

4.3 Recommendations

- The future research recommendations based on this study are as follows:
- Using randomness-based technique in conjunction with edge-based steganography to create higher security methods that withstand statistical steganography;
- Enhancing hiding capacity by using lossless data compression techniques;
- Enhancing security by applying the current encryption techniques;
- Data can be hidden in specific region of interest (ROI) which thwarts statistical attacks by disrupting statistical relationships between neighboring pixels, rather than using the entire image to embed the secret data;
- Paying greater attention to the YCBCR color system visuals, as they have not gotten as much attention as they should in this particular context;
- 3D may be a viable option for embedding hidden data in images;
- Lessening distortion and enhancing security can be achieved by utilizing the adaptiveness idea to combine multiple hiding algorithms based on user-defined criteria or image features. High imperceptibility can also be achieved with specific optimization techniques. By combining the benefits of both the transform and spatial domain techniques, system performance can be improved by using hybrid solutions;
- Developing steganographic methods that dynamically adapt to changes in the environment or to counteract evolving detection techniques. Explore approaches that adjust the hiding strategies based on real-time feedback, ensuring continued effectiveness;
- Developing steganographic techniques that are resistant to adversarial attacks. Explore methods to detect and defend against attacks to reveal or alter the hidden information within images;
- Exploring the integration of deep learning techniques in image steganography for improved capacity, imperceptibility, security and efficiency. Develop neural network architectures that automatically learn and adapt to different image characteristics, leading to more effective hiding and extraction processes.

- Investigating the application of quantum computing principles to image steganography. Explore how quantum cryptography and key distribution can be integrated into steganographic processes to provide enhanced security and resistance against quantum attacks. IS techniques of reversible data hiding (RHD) and non-RHD can be used in quantum steganography, which may be an emerging research field.

5 Conclusions

Image steganography allows for the concealment of confidential data inside a cover image. It is widely used to ensure privacy when transmitting data over untrustworthy networks. An extensive analysis of traditional image steganography approaches was conducted, mostly using WoS, Scopus, IEEE Explore, and ACM research. Due to its efficiency and simplicity, LSB-based steganography and its variations are used in the majority of techniques in traditional IS techniques. PVD, DE, EMD, PIT, ROI, and edge-based embedding, are also employed in various spatial domain IS on the contrary, DCT, DFT, DWT, IWT, etc., are used in transformation based IS systems. This article critically examines randomization strategies used in image steganography techniques. More precisely, the pixels, blocks of pixels, patterns, and bit-plane-based data hiding spaces are randomly chosen for embedding secret data employing random permutation, random noise injection, random spread spectrum, and/or random pixel intensity modification associated with embedding algorithms. A brief discussion of the shortcomings and potential benefits of randomization strategies employed in IS principles is also mentioned in this review. Furthermore, observation-based suggestions and recommendations for future research are given to both seasoned and novice researchers who are interested in this area. In order to increase the system's capacity, imperceptibility, and security, the authors have tried to recommend future research directions for a secure image steganography model combining novel cryptography and steganography algorithms that use advanced randomization and stochastic approaches.

Acknowledgement: The author AFM Zainul Abadin would like to acknowledge Center for Cyber Security, Faculty of Information Science and Technology, UKM for ensuring excellent research environment. He would like to express his gratitude and thanks to all co-authors for their contribution, effort, and guidance. Mr. Abadin acknowledges ICT division, Ministry of Posts Telecommunication and Information Technology, Bangladesh with cordial gratitude as one of the PhD fellow selected by the division.

Funding Statement: This research was funded by the Ministry of Higher Education (MOHE) through Fundamental Research Grant Scheme (FRGS) under the Grand Number FRGS/1/2020/ICT01/UKM/02/4, and University Kebangsaan Malaysia for open access publication.

Author Contributions: The authors confirm contribution to the paper as follows: study conceptualization and design: AFM Zainul Abadin, Rossilawati Sulaiman; data collection: AFM Zainul Abadin; data analysis and interpretation of results: AFM Zainul Abadin, Rossilawati Sulaiman, Mohammad Kamrul Hasan; draft manuscript preparation: AFM Zainul Abadin; manuscript review and literature update: Rossilawati Sulaiman, Mohammad Kamrul Hasan. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Fateh, M. Rezvani, and Y. Irani, "A new method of coding for steganography based on LSB matching revisited," *Secur. Commun. Netw.*, vol. 2021, no. 5, pp. 1–15, 2021. doi: 10.1155/2021/6610678.

[2] N. F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures*. Boston, Dordrecht, London: Kluwer academic publishers; Springer Science & Business Media, 2001, vol. 1.

[3] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A review on text steganography techniques," *Mathematics*, vol. 9, no. 21, pp. 2829, 2021. doi: 10.3390/math9212829.

[4] S. Ghoul, R. Sulaiman, and Z. Shukur, "A review on security techniques in image steganography," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 6, pp. 361–385, 2023. doi: 10.14569/issn.2156-5570.

[5] S. Kaur, S. Singh, M. Kaur, and H. -N. N. Lee, "A systematic review of computational image steganography approaches," *Arch. Comput. Methods Eng.*, vol. 29, no. 7, pp. 4775–4797, 2022. doi: 10.1007/s11831-022-09749-0.

[6] A. Kumar, R. Rani, and S. Singh, "A survey of recent advances in image steganography," *Secur. Priv.*, vol. 6, no. 3, pp. e281, 2023. doi: 10.1002/spy2.281.

[7] A. Jan, S. A. Parah, M. Hussan, and B. A. Malik, "Double layer security using crypto-stego techniques: A comprehensive review," *Health Technol.*, vol. 12, no. 1, pp. 9–31, 2022. doi: 10.1007/s12553-021-00602-1.

[8] M. A. Wani and B. Sultan, "Deep learning based image steganography: A review," *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.*, vol. 13, no. 3, pp. e1481, 2023.

[9] L. Meng, X. Jiang, and T. Sun, "A review of coverless steganography," *Neurocomputing*, vol. 566, pp. 126945, 2023.

[10] M. J. Page *et al.*, "The PRISMA, 2020 statement: An updated guideline for reporting systematic reviews," *Int. J. Surg.*, vol. 88, pp. 105906, 2021. doi: 10.1016/j.ijsu.2021.105906.

[11] D. Kahn, "The history of steganography," in *Information Hiding*, 1996, pp. 1–5.

[12] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, 2010. doi: 10.1016/j.sigpro.2009.08.010.

[13] K. Kordov and S. Zhelezov, "Steganography in color images with random order of pixel selection and encrypted text message embedding," *PeerJ Comput. Sci.*, vol. 7, no. 11, pp. 1–21, 2021. doi: 10.7717/peerj-cs.380.

[14] S. Chutani and A. Goyal, "A review of forensic approaches to digital image Steganalysis," *Multimed. Tools Appl.*, vol. 78, no. 13, pp. 18169–18204, 2019. doi: 10.1007/s11042-019-7217-0.

[15] M. A. Hameed, O. A. Abdel-Aleem, and M. Hassaballah, "A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 5, pp. 4639–4657, 2023. doi: 10.1007/s12652-022-04366-y.

[16] S. Kamil, M. Sahu, K. R. Raghunandan, and A. K. Sahu, "Secure reversible data hiding using block-wise histogram shifting," *Electronics*, vol. 12, no. 5, pp. 1222, 2023. doi: 10.3390/electronics12051222.

[17] F. F. Qian, N. Xu, and W. L. Lyu, "High capacity reversible data hiding scheme based on interpolation and tetris matrix," in *Chinese Control Conf. CCC*, Hefei, China, 2022, vol. 19, pp. 7471–7478. doi: 10.23919/CCC55666.2022.9902681.

[18] M. Fan, S. Zhong, and X. Xiong, "Reversible data hiding method for interpolated images based on modulo operation and prediction-error expansion," *IEEE Access*, vol. 11, no. 1, pp. 27290–27302, 2023. doi: 10.1109/ACCESS.2023.3258461.

[19] A. H. M. Kamal and M. M. Islam, "Uses of local binary pattern codes for enriching the embedding performance," in *2022 IEEE Delhi Sect. Conf. (DELCON)*, 2022. doi: 10.1109/DELCON54057.2022.9753033.

[20] P. Milosav, M. Milosavljević, and Z. Banjac, "Steganographic method in selected areas of the stego-carrier in the spatial domain," *Symmetry*, vol. 15, no. 5, pp. 1015, 2023. doi: 10.3390/sym15051015.

[21] W. Li, S. Wu, B. Li, W. Tang, and X. Zhang, "Payload-independent direct cost learning for image steganography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 34, no. 3, pp. 1970–1975, 2023. doi: 10.1109/TCSVT.2023.3294291.

[22] S. Rahman *et al.*, "A Huffman code LSB based image steganography technique using multi-level encryption and achromatic component of an image," *Sci. Rep.*, vol. 13, no. 1, pp. 1–20, 2023. doi: 10.1038/s41598-023-41303-1.

[23] H. Sultana, A. H. M. Kamal, G. Hossain, and M. A. Kabir, "A novel hybrid edge detection and LBP code-based robust image steganography method," *Futur. Internet*, vol. 15, no. 3, pp. 1–23, 2023. doi: 10.3390/fi15030108.

[24] R. S. Hameed, S. S. Mokri, M. S. Taha, and M. M. Taher, "High capacity image steganography system based on multi-layer security and LSB exchanging method," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 8, pp. 108–115, 2022. doi: 10.14569/issn.2156-5570.

[25] A. D. Molato, F. B. Calanda, A. M. Sison, and R. P. Medina, "LSB-based random embedding image steganography technique using modified Collatz conjecture," in *2022 7th Int. Conf. Signal Image Process. (ICSIP)*, 2022, pp. 367–371. doi: 10.1109/ICSIP55141.2022.9886754.

[26] F. B. Calanda, A. M. Sison, M. R. D. Molato, and R. P. Medina, "A modified least significant bit randomized embedding method based on image partitioning and columnar transposition with encryption," in *Proc. 2nd Int. Conf. Comput. Big Data*, 2019, pp. 68–72. doi: 10.1145/3366650.

[27] A. Tasheva, Z. Tasheva, and P. Nakov, "Image based steganography using modified LSB insertion method with contrast stretching," in *Proc. 18th Int. Conf. Comput. Syst. Technol., in CompSysTech'17*, New York, NY, USA: Association for Computing Machinery, 2017, pp. 233–240. doi: 10.1145/3134302.3134325.

[28] W. Wu and H. Li, "A novel scheme for random sequential high-capacity data hiding based on PVD and LSB," *Signal Image Video Process.*, vol. 18, no. 3, pp. 2277–2287, pp. 1–11, 2023.

[29] Y. Hu, H. K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," *IEEE Trans. Multimed.*, vol. 10, no. 8, pp. 1500–1512, 2008. doi: 10.1109/TMM.2008.2007341.

[30] Z. S. Younus and M. K. Hussain, "Image steganography using exploiting modification direction for compressed encrypted data," *J. King Saud Univ.–Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2951–2963, 2022. doi: 10.1016/j.jksuci.2019.04.008.

[31] C. F. Lee and Y. L. Huang, "An efficient image interpolation increasing payload in reversible data hiding," *Expert Syst. Appl.*, vol. 39, no. 8, pp. 6712–6719, 2012. doi: 10.1016/j.eswa.2011.12.019.

[32] M. Li and Y. Li, "Histogram shifting in encrypted images with public key cryptosystem for reversible data hiding," *Signal Process.*, vol. 130, no. 8, pp. 190–196, 2017. doi: 10.1016/j.sigpro.2016.07.002.

[33] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on lsb matching revisited," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 2, pp. 201–214, 2010. doi: 10.1109/TIFS.2010.2041812.

[34] S. Ghoul and R. Sulaiman, "Imperceptible image steganography technique using a novel PIT-based technique," in *Int. Conf. Cyber Resilience, ICCR 2022*, 2022. doi: 10.1109/ICCR56254.2022.9995838.

[35] K. H. Jung and K. Y. Yoo, "Data hiding method using image interpolation," *Comput. Stand. Interfaces*, vol. 31, no. 2, pp. 465–470, 2009. doi: 10.1016/j.csi.2008.06.001.

[36] B. Ma *et al.*, "A high-performance robust reversible data hiding algorithm based on polar harmonic Fourier moments," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 34, no. 4, pp. 2763–2774, Apr. 2024. doi: 10.1109/TCSVT.2023.3311483.

[37] R. Kaur and B. Singh, "A robust and imperceptible n-Ary based image steganography in DCT domain for secure communication," *Multimed. Tools Appl.*, vol. 83, no. 1, pp. 1–30, 2023. doi: 10.1007/s11042-023-16330-9.

[38] A. Melman and O. Evsutin, "On the efficiency of metaheuristic optimization for adaptive image steganography in the DFT domain," in *2021 17th Int. Symp. Probl. Redundancy Inf. Control Syst. (REDUNDANCY)*, 2021, pp. 49–54. doi: 10.1109/REDUNDANCY52534.2021.9606459.

[39] V. Sabeti and M. Amerehei, "Secure and imperceptible image steganography in discrete wavelet transform using the XOR logical function and genetic algorithm," *ISeCure*, vol. 14, no. 2, pp. 167–179, 2022. doi: 10.22042/isecure.2022.274305.641.

[40] Z. Saeidi, A. Yazdi, S. Mashhadi, M. Hadian, and A. Gutub, "High performance image steganography integrating IWT and Hamming code within secret sharing," *IET Image Process*, vol. 18, no. 1, pp. 129–139, 2023. doi: 10.1049/ipr2.12938.

[41] U. Zia *et al.*, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Int. J. Inf. Secur.*, vol. 21, no. 4, pp. 917–935, 2022. doi: 10.1007/s10207-022-00588-5.

[42] M. A. Idakwo, M. B. Muazu, E. A. Adedokun, and B. O. Sadiq, "An extensive survey of digital image steganography: State of the art," *ATBU J. Sci. Technol. Educ.*, vol. 8, no. 2, pp. 40–54, 2020.

[43] B. Ma, K. Li, J. Xu, C. Wang, J. Li and L. Zhang, "Enhancing the security of image steganography via multiple adversarial networks and channel attention modules," *Digit. Signal Process.*, vol. 141, no. 7, pp. 104121, 2023. doi: 10.1016/j.dsp.2023.104121.

[44] A. H. S. Saad, M. S. Mohamed, and E. H. Hafez, "Coverless image steganography based on jigsaw puzzle image generation," *Comput. Mater. Contin.*, vol. 67, no. 2, pp. 2077–2091, 2021. doi: 10.32604/cmc.2021.015329.

[45] G. Xie, J. Ren, S. Marshall, H. Zhao, and R. Li, "A novel gradient-guided post-processing method for adaptive image steganography," *Signal Process.*, vol. 203, no. 1, pp. 108813, 2023. doi: 10.1016/j.sigpro.2022.108813.

[46] Y. Sun, J. Liu, and R. Zhang, "Generative image steganography based on guidance feature distribution," *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 19, pp. 123, Sep. 2023. doi: 10.1145/3625297.

[47] M. H. Mahdi, A. A. Abdulrazzaq, M. S. Mohd Rahim, M. S. Taha, H. N. Khalid and S. A. Lafta, "Improvement of image steganography scheme based on LSB value with two control random parameters and multi-level encryption," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 518, no. 5, pp. 052002, 2019. doi: 10.1088/1757-899X/518/5/052002.

[48] S. R. Dash, A. Sen, S. Sarif Hassan, R. Roy, C. Misra and K. N. Singh, "Steganography technique to prevent data loss by using Boolean functions," in *Artif. Intell. Evol. Comput. Eng. Syst.*, 2018, pp. 263–270.

[49] A. Ahmed and A. Ahmed, "A secure image steganography using LSB and double XOR operations," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 20, no. 5, pp. 139, 2020.

[50] A. Pradhan, K. R. Sekhar, and G. Swain, "Digital image steganography using LSB substitution, PVD, and EMD," *Math. Probl. Eng.*, vol. 2018, no. 2, pp. 1–11, 2018. doi: 10.1155/2018/1804953.

[51] G. Swain, "High capacity image steganography using modified LSB substitution and PVD against pixel difference histogram analysis," *Secur. Commun. Netw.*, vol. 2018, no. 5, pp. 1–14, 2018. doi: 10.1155/2018/1505896.

[52] R. D. Rashid and T. F. Majeed, "Edge based image steganography: Problems and solution," in *2019 3rd Int. Conf. Commun. Signal Process. Their Appl. (ICCSPA)*, Sharjah, United Arab Emirates, 2019. doi: 10.1109/ICCSPA.2019.8713712.

[53] Z. N. Al-Kateeb, M. J. Al-Shamdeen, and F. S. Al-Mukhtar, "Encryption and steganography a secret data using circle shapes in colored images," *J. Phys. Conf. Ser.*, vol. 1591, no. 1, pp. 012019, 2020. doi: 10.1088/1742-6596/1591/1/012019.

[54] J. Vellingiri, K. Saravanan, and R. Asokan, "Data hiding in images by edge adaptive steganography," *Int. J. Appl. Eng. Res.*, vol. 9, no. 23, pp. 22097–22105, 2014.

[55] H. H. Alwan and Z. M. Hussain, "A multiple-chaotic approach for steganography," *J. Comput. Sci.*, vol. 15, no. 10, pp. 1461–1489, 2019. doi: 10.3844/jcssp.2019.1461.1489.

[56] S. Singh and A. Datar, "Improved hash based approach for secure color image steganography using canny edge detection method," *Int. J. Comput. Sci. Netw. Secur.*, vol. 15, no. 7, pp. 92, 2015.

[57] S. D. M. Satar, N. A. Hamid, F. Ghazali, R. Muda, M. Mamat and P. K. An, "Secure image steganography using encryption algorithm," in *Annu. Int. Conf. Intell. Comput., Comput. Sci. Inf. Syst. (ICCSIS-16)*, 2016.

[58] E. J. Kusuma, C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "A combination of inverted LSB, RSA, and Arnold transformation to get secure and imperceptible image steganography," *J. ICT Res. Appl.*, vol. 12, no. 2, pp. 103–122, 2018. doi: 10.5614/itbj.ict.res.appl.2018.12.2.1.

[59] A. H. Ali, L. E. George, A. A. Zaidan, and M. R. Mokhtar, "High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain," *Multimed. Tools Appl.*, vol. 77, no. 23, pp. 31487–31516, 2018. doi: 10.1007/s11042-018-6213-0.

[60] M. Ragab, S. Alshehri, H. A. Alhadrami, F. Kateb, E. B. Ashary and S. Abdel-Khalek, "Encryption with Image steganography based data hiding technique in IIoT environment," *Comput. Mater. Contin.*, vol. 72, no. 1, pp. 1223–1338, 2022. doi: 10.32604/cmc.2022.024775.

[61] A. Munshi, "Randomly-based stepwise multi-level distributed medical image steganography," *Eng Technol. Appl. Sci. Res.*, vol. 13, no. 3, pp. 10922–10930, 2023. doi: 10.48084/etasr.5935.

[62] J. Blackledge and A. Al-Rawi, "Steganography using stochastic diffusion for the covert communication of digital images," *Int. J. Appl. Math.*, vol. 41, no. 4, pp. 270–298, 2011. doi: 10.21427/D7KG8B.

[63] M. EL-Hady, M. H. Abbas, F. A. Khanday, L. A. Said, and A. G. Radwan, "DISH: Digital image steganography using stochastic-computing with high-capacity," *Multimed. Tools Appl.*, 2024. doi: 10.1007/s11042-023-17998-9.

[64] M. Jana, B. Jana, and S. Jana, "A secured reversible data hiding technique for multiple secrets using image interpolation with bit reversal permutation," 2022. doi: 10.21203/rs.3.rs-2018874/v1.

[65] S. Ganguly and I. Mukherjee, "Image sterilization through adaptive noise blending in integer wavelet transformation," in *INDICON 2022—2022 IEEE 19th India Counc. Int. Conf.*, 2022, pp. 1–6. doi: 10.1109/INDICON56171.2022.10039861.

[66] E. H. Rachmawanto, D. R. I. M. Setiadi, C. A. Sari, P. N. Andono, O. Farooq and N. Pradita, "Spread embedding technique in LSB image steganography based on Chaos theory," *Int. Proc.*, vol. 17, pp. 39–44, 2019. doi: 10.1109/ISEMANTIC.2019.8884266.

[67] A. K. Sahu and G. Swain, "Reversible image steganography using dual-layer LSB matching," *Sens. Imaging*, vol. 21, no. 1, pp. 3210, 2020. doi: 10.1007/s11220-019-0262-y.

[68] R. Roselinkiruba and T. S. Sharmila, "Performance evaluation of encryption algorithm using fruit fly optimization improved hybridized seeker and PVD algorithm," *Int. J. Inf. Technol.*, vol. 13, no. 5, pp. 1797–1803, 2021. doi: 10.1007/s41870-021-00774-z.

[69] S. Gujjunoori and M. Oruganti, "Difference expansion based reversible data embedding and edge detection," *Multimed. Tools Appl.*, vol. 78, no. 18, pp. 25889–25917, 2019. doi: 10.1007/s11042-019-07767-y.

[70] W. Wang, "A reversible data hiding algorithm based on bidirectional difference expansion," *Multimed. Tools Appl.*, vol. 79, no. 9–10, pp. 5965–5988, 2020. doi: 10.1007/s11042-019-08255-z.

[71] U. A. M. Ehsan Ali, E. Ali, M. Sohrawordi, and M. N. Sultan, "A LSB based image steganography using random pixel and bit selection for high payload," *Int. J. Math. Sci. Comput.*, vol. 7, no. 3, pp. 24–31, 2021. doi: 10.5815/ijmsc.2021.03.03.

[72] J. L. Pichardo-Méndez, L. Palacios-Luengas, R. F. Martínez-González, O. Jiménez-Ramírez, and R. Vázquez-Medina, "LSB pseudorandom algorithm for image steganography using skew tent map," *Arab J. Sci. Eng.*, vol. 45, no. 4, pp. 3055–3074, 2020. doi: 10.1007/s13369-019-04272-0.

[73] C. Pak, J. Kim, K. An, C. Kim, K. Kim and C. Pak, "A novel color image LSB steganography using improved 1D chaotic map," *Multimed. Tools Appl.*, vol. 79, no. 1–2, pp. 1409–1425, 2020. doi: 10.1007/s11042-019-08103-0.

[74] S. A. Nie, G. Sulong, R. Ali, and A. Abel, "The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 6, pp. 5218–5226, 2019. doi: 10.11591/ijece.v9i6.pp5218-5226.

[75] H. R. Kareem, H. H. Madhi, and K. A. -A. Mutlaq, "Hiding encrypted text in image steganography," *Period Eng. Nat. Sci.*, vol. 8, no. 2, pp. 703–707, 2020.

[76] T. N. Vo, T. C. Lu, S. Agrawal, and B. Jana, "Interpolation based reversible hiding scheme by using center folding strategy and adjusting hiding operator," in *2021 Int. Conf. Technol. Appl. Artif. Intell. (TAAI)*, 2021, pp. 90–95. doi: 10.1109/TAAI54685.2021.00025.

[77] P. C. Mandal and I. Mukherjee, "High capacity data hiding based on multi-directional pixel value differencing and decreased difference expansion," *Multimed. Tools Appl.*, vol. 81, no. 4, pp. 5325–5347, 2022. doi: 10.1007/s11042-021-11605-5.

[78] L. Zhu, X. Luo, Y. Zhang, C. Yang, and F. Liu, "Inverse interpolation and its application in robust image steganography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 6, pp. 4052–4064, 2022. doi: 10.1109/TCSVT.2021.3107342.

[79] A. Shaik and V. T., "High capacity reversible data hiding using 2D parabolic interpolation," *Multimed. Tools Appl.*, vol. 78, no. 8, pp. 9717–9735, 2019. doi: 10.1007/s11042-018-6544-x.

[80] H. Ye, K. Su, X. Cheng, and S. Huang, "Research on reversible image steganography of encrypted image based on image interpolation and difference histogram shift," *IET Image Process.*, vol. 16, no. 7, pp. 1959–1972, 2022. doi: 10.1049/ipr2.12461.

[81] X. -Z. Xie, C. -C. Chang, and Y. -C. Hu, "An adaptive reversible data hiding scheme based on prediction error histogram shifting by exploiting signed-digit representation," *Multimed. Tools Appl.*, vol. 79, pp. 24329–24346, 2020. doi: 10.1007/s11042-019-08402-6.

[82] M. A. Hussein and S. Al-Mome, "Linear feedback shift registers-based randomization for image steganography," *Iraqi J. Sci.*, vol. 64, no. 8, pp. 4131–4146, 2023. doi: 10.24996/ijs.2023.64.8.34.

[83] P. B. Jelušić, A. Poljičak, D. Donevski, and T. Cigula, "Low-frequency data embedding for DFT-based image steganography," *Int. J. Softw. Sci. Comput. Intell.*, vol. 14, no. 1, pp. 1–11, 2022. doi: 10.4018/IJSSCI.

[84] M. Fakhredanesh, M. Rahmati, and R. Safabakhsh, "Steganography in discrete wavelet transform based on human visual system and cover model," *Multimed. Tools Appl.*, vol. 78, no. 13, pp. 18475–18502, 2019. doi: 10.1007/s11042-019-7238-8.

[85] G. Ma and J. Wang, "Efficient reversible data hiding in encrypted images based on multi-stage integer wavelet transform," *Signal Process. Image Commun.*, vol. 75, pp. 55–63, 2019.

[86] H. Zhang and L. Hu, "A data hiding scheme based on multidirectional line encoding and integer wavelet transform," *Signal Process. Image Commun.*, vol. 78, pp. 331–344, 2019.

[87] P. K. Muhuri, Z. Ashraf, and S. Goel, "A novel image steganographic method based on integer wavelet transformation and particle swarm optimization," *Appl. Soft Comput.*, vol. 92, no. s2, pp. 106257, 2020. doi: 10.1016/j.asoc.2020.106257.

[88] G. Maji, S. Mandal, and S. Sen, "Cover independent image steganography in spatial domain using higher order pixel bits," *Multimed. Tools Appl.*, vol. 80, no. 10, pp. 15977–16006, Apr. 2021. doi: 10.1007/s11042-020-10298-6.

[89] M. M. Abdel-Aziz, K. M. Hosny, and N. A. Lashin, "Improved data hiding method for securing color images," *Multimed. Tools Appl.*, vol. 80, no. 8, pp. 12641–12670, 2021. doi: 10.1007/s11042-020-10217-9.

[90] D. Laishram and T. Tuithung, "A novel minimal distortion-based edge adaptive image steganography scheme using local complexity: (BEASS)," *Multimed. Tools Appl.*, vol. 80, no. 1, pp. 831–854, 2021. doi: 10.1007/s11042-020-09519-9.

[91] G. Maji, S. Mandal, N. C. Debnath, and S. Sen, "Pixel value difference based image steganography with one time pad encryption," *IEEE Int. Conf. Ind. Inf.*, vol. 2019, pp. 1358–1363, 2019. doi: 10.1109/INDIN41052.2019.

[92] A. A. Almayyahi, R. Sulaiman, F. Qamar, and A. E. Hamzah, "High-security image steganography technique using XNOR operation and Fibonacci algorithm," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 10, pp. 511–522, 2020. doi: 10.14569/issn.2156-5570.

[93] H. Ogras, "An efficient steganography technique for images using chaotic bitstream," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 2, pp. 21–27, 2019. doi: 10.5815/ijcnis.2019.02.03.

[94] A. Chatterjee, S. K. Ghosal, and R. Sarkar, "LSB based steganography with OCR: An intelligent amalgamation," *Multimed. Tools Appl.*, vol. 79, no. 17–18, pp. 11747–11765, 2020. doi: 10.1007/s11042-019-08472-6.

[95] E. Margalikas and S. Ramanauskaitė, "Image steganography based on color palette transformation in color space," *EURASIP J. Image Video Process.*, vol. 2019, no. 1, pp. 1–13, 2019. doi: 10.1186/s13640-019-0484-x.

[96] Y. Wang, M. Tang, and Z. Wang, "High-capacity adaptive steganography based on LSB and hamming code," *Optik*, vol. 213, no. 1, pp. 164685, 2020. doi: 10.1016/j.ijleo.2020.164685.

[97] A. Saeed *et al.*, "An accurate texture complexity estimation for quality-enhanced and secure image steganography," *IEEE Access*, vol. 8, pp. 21613–21630, 2020. doi: 10.1109/ACCESS.2020.2968217.

[98] M. C. Kasapbasi, "A new chaotic image steganography technique based on Huffman compression of Turkish texts and fractal encryption with post-quantum security," *IEEE Access*, vol. 7, pp. 148495–148510, 2019. doi: 10.1109/ACCESS.2019.2946807.

[99] H. Al-Dmour, "Securing digital data: A new edge detection and XOR coding approach for imperceptible image steganography," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 11, pp. 1214–1220, Nov. 2023.

[100] A. A. Mohammad, "An efficient EMD-based reversible data hiding technique using dual stego images," *Comput. Mater. Contin.*, vol. 75, no. 1, pp. 1139–1156, 2023. doi: 10.32604/cmc.2023.035964.

[101] S. Saha, A. Chakraborty, A. Chatterjee, S. Dhargupta, S. K. Ghosal and R. Sarkar, "Extended exploiting modification direction based steganography using hashed-weightage array," *Multimed. Tools Appl.*, vol. 79, pp. 20973–20993, 2020. doi: 10.1007/s11042-020-08951-1.

[102] S. Rahman *et al.*, "A novel approach of image steganography for secure communication based on LSB substitution technique," *Comput. Mater. Contin.*, vol. 64, no. 1, pp. 31–61, 2020. doi: 10.32604/cmc.2020.09186.

[103] B. Datta, K. Dutta, and S. Roy, "Data hiding in virtual bit-plane using efficient Lucas number sequences," *Multimed. Tools Appl.*, vol. 79, no. 31–32, pp. 22673–22703, 2020. doi: 10.1007/s11042-020-08979-3.

[104] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," *IEEE Access*, vol. 9, pp. 31805–31815, 2021. doi: 10.1109/ACCESS.2021.3060317.

[105] A. Sajjad, H. Ashraf, N. Z. Jhanjhi, M. Humayun, M. Masud and M. A. AlZain, "Improved video steganography with dual cover medium, DNA and complex frames," *Comput. Mater. Contin.*, vol. 74, no. 2, pp. 3881–3898, 2023. doi: 10.32604/cmc.2023.030197.