Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.051826

REVIEW

A Review of Image Steganography Based on Multiple Hashing Algorithm

Abdullah Alenizi[1], Mohammad Sajid Mohammadi[2], Ahmad A. Al-Hajji[2] and Arshiya Sajid Ansari[1,*]

[1]Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al-Majmaah, 11952, Saudi Arabia

[2]Department of Computer Science, College of Engineering and Information Technology, Onaizah Colleges, Qassim, 56312, Saudi Arabia

*Corresponding Author: Arshiya Sajid Ansari. Email: ar.ansari@mu.edu.sa

Received: 16 March 2024 Accepted: 05 June 2024 Published: 15 August 2024

ABSTRACT

Steganography is a technique for hiding secret messages while sending and receiving communications through a cover item. From ancient times to the present, the security of secret or vital information has always been a significant problem. The development of secure communication methods that keep recipient-only data transmissions secret has always been an area of interest. Therefore, several approaches, including steganography, have been developed by researchers over time to enable safe data transit. In this review, we have discussed image steganography based on Discrete Cosine Transform (DCT) algorithm, etc. We have also discussed image steganography based on multiple hashing algorithms like the Rivest–Shamir–Adleman (RSA) method, the Blowfish technique, and the hash-least significant bit (LSB) approach. In this review, a novel method of hiding information in images has been developed with minimal variance in image bits, making our method secure and effective. A cryptography mechanism was also used in this strategy. Before encoding the data and embedding it into a carry image, this review verifies that it has been encrypted. Usually, embedded text in photos conveys crucial signals about the content. This review employs hash table encryption on the message before hiding it within the picture to provide a more secure method of data transport. If the message is ever intercepted by a third party, there are several ways to stop this operation. A second level of security process implementation involves encrypting and decrypting steganography images using different hashing algorithms.

KEYWORDS

Image steganography; multiple hashing algorithms; Hash-LSB approach; RSA algorithm; discrete cosine transform (DCT) algorithm; blowfish algorithm

1 Introduction

1.1 Steganography

Steganography is the method of concealing crucial data inside an innocent-looking file. It is a technique for hiding information that stands out from the norm in confidential or secret files [1]. Steganography in cryptology is often misunderstood because of its association with the storage of secret information. The key distinction is that steganography also requires important details, yet

steganography doesn't seem to conceal anything [2–5]. The name "steganography" is derived from the Greek word "steganos," which means "secret writing." The word "steganos" combines the Greek words for "secret" and "graphic," which means "writing." However, steganography is the practice of concealing information" the form of text or secret messages inside other media resources like images, written text, video, or audio [6]. In common parlance, "steganography" and "cryptography" are often used synonymously. An embedded watermark guarantees the message's authenticity, while cryptography jumbles it and steganography keeps it hidden. To encrypt genuine data successfully, we need to use a steganography approach that can be trusted [7]. Without considering envision characteristics like color, texture, or semantics, adversarial perturbations were applied to the cover images globally. This led to obvious distortions, especially in simple areas [8]. Depending on the kind of carrier, several appropriate steganographic methods are used to establish security, three decades of technological advancements in the field of steganography [9]. A comparison of these tools according to the provided criteria reveals their advantages, disadvantages, practicality, and room for further research. The OpenPuff steganography tool has widespread support in academic and professional communities. This research further analyzes the effectiveness of the OpenPuff tool on a few previously undisclosed criteria to verify and defend its efficacy [10].

The World Wide Web (WWW) has made it possible to send and receive any amount of digital information (movies, music, pictures, documents, and even whole networks) instantly and without effort [11]. Meanwhile, such unrestricted access to a plethora of data has resulted in serious dangers to encrypted and privacy-protected communication via the World Wide Web, making it difficult to protect data sent over an unsecured network. By tampering with the message, attackers or opponents may often compromise the information and cause monetary or moral harm [12]. As a result, several data encryption and concealment methods have been devised to ensure safe transmissions of sensitive data [13,14]. Fig. 1 shows the classification of steganography security systems.

Both steganography and data transmission techniques that could be utilized covertly include encryption. In cryptography, communication is altered in such a manner that only the sender and the intended recipient, who both have access to the encryption key, can read it [15]. However, in steganography, the hidden message is made to hide in a cover picture, making it impossible for an intermediate person to know whether there is a message hidden in the information being shared. This contrasts with cryptography, where it is always clear that the message is in encrypted form. The receiver then receives the cover picture with the concealed message.

1.2 Cryptography

The background of cryptography is extensive and important, spanning from the use of paper and pen through the development of specialized machinery to the use of arithmetic operations. In this study, only a short analysis that is important for transmitting information has been given. Cryptology is the study of how to send and read secret messages using codes (the Greek word for secret or hidden is cryptology). It is typically divided into cryptanalysis and cryptography. Cryptography is the study of designing systems for encoding and decoding messages. It says that the word "cryptography" usually refers to the group of security measures that include:

- Encrypt and decrypt methods.
- Integrity-checking procedures, and
- Digital signature techniques.

Typically, there are four main components to every cryptographic procedure:

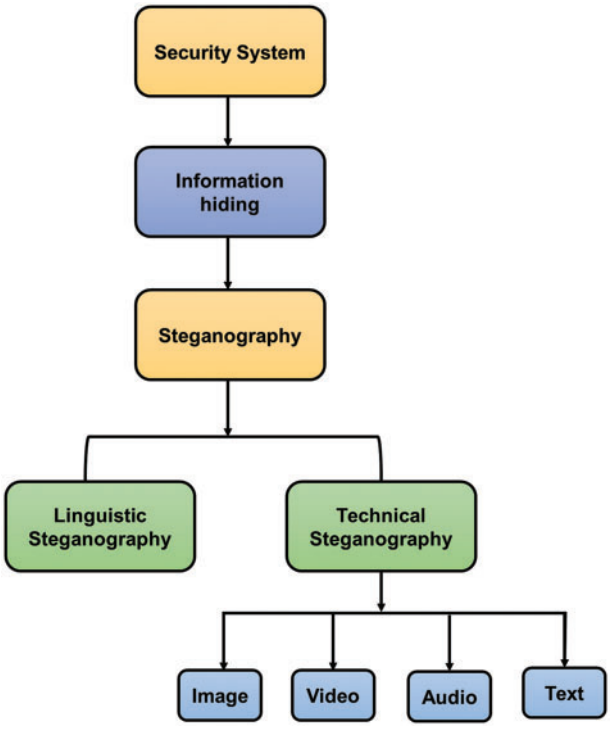

Figure 1: Classification of steganography security systems

1.2.1 Plain Text

A transmission of deciphered data. Anything from a simple text file to a password, credit card number, payroll data, personnel details, or even a top-secret calculation being transmitted between businesses might be included.

1.2.2 Ciphertext

It means simple text that has been made unreadable by a mathematical formula. Ciphertext is an unencrypted message that has been encrypted before transmission.

1.2.3 Key

A numeric or algebraic factor or procedure that controls the encryption or decryption of plaintext communication. You can't read the coded message without the key.

1.2.4 Cryptography Algorithm

A procedure in mathematics that is used to jumble up the original text to get to the cipher. Encryption refers to the process of using encryption techniques to change the plain language into ciphertext, while decryption refers to the process of using the same technique to change ciphertext back into plain text. Cryptography is a method used to protect sensitive information in Fig. 2.

The three kinds of cryptographic algorithms below are widely employed today for data security purposes:

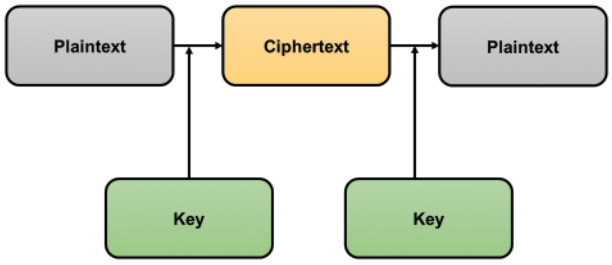

Figure 2: Structure of cryptography

1.2.5 Cryptography with a Secret Key

One key is used to perform both the decrypt and encrypt processes in this technique, which is also known as symmetric-key cryptography. The Data Encryption Standard, which is extensively used by the Federal Government, is the best illustration of this cryptographic algorithm. The stages involved in secret-key cryptography to provide secure communication are shown in Fig. 3.

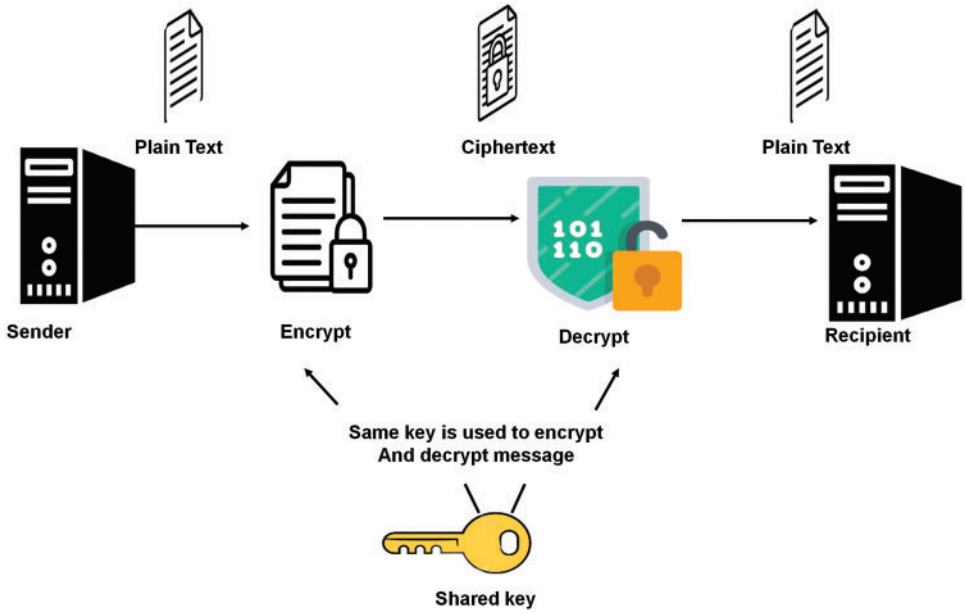

Figure 3: Secret-key cryptography

While this approach increases data protection, it is difficult to distribute the key between sender and recipient since a prohibited person might easily get all of the data if they have the private key. So, using this strategy, key security is a crucial concern for encrypted transmission.

1.2.6 Cryptography Using a Public Key

As an asymmetric method, public key cryptography encrypts sensitive information using a shared "public" key and decrypts it with a shared "private" (or secret) key. With this method, two separate keys are needed to initiate the action. Deducing the secret key from the public key would be computationally impossible. It is possible for anybody with access to a public key to encrypt data, but only the private key owner may read the encrypted file. When data is encrypted, only the owner of the secret key can

read it. Some common asymmetric-key algorithms include RSA, Diffie-Hellman, digital signature algorithms, public key cryptography standards, and key exchange algorithms. The stages that make up this algorithm are shown in Fig. 4.

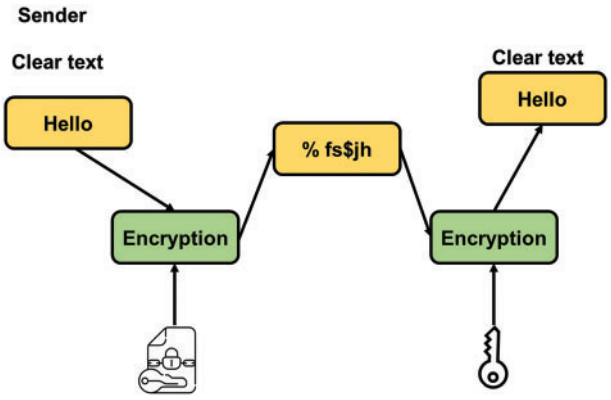

Figure 4: Public key cryptography

1.2.7 Hash Function

Data is irrevocably encrypted using hash functions, which use an algebraic change. Message integrity is the main use of hash functions in cryptography. The hash function gives a communication's payload a digital fingerprint, ensuring that the text has not been tampered with by an outsider, a virus, or any other means. As there is very little chance that two separate plain texts will produce the same hash result, hash algorithms are effective. Hash function structures are shown in Fig. 5.

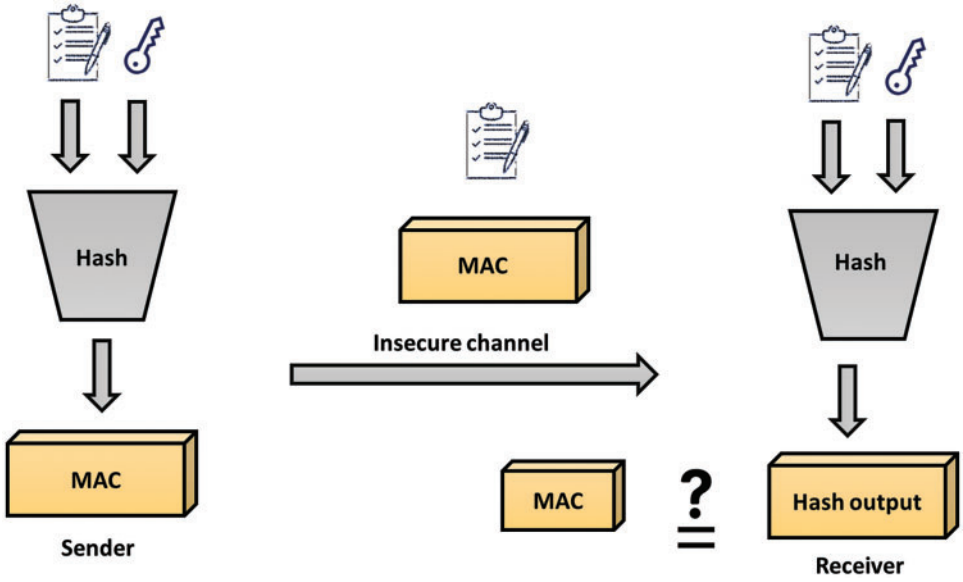

Figure 5: Structure of hash function

There are numerous popular hashing operations in use right now:

1.2.8 Hashed Message Authentication Code: A Message Authentication Method

Identifies users and their devices using a shared secret and then hashes their data for further security.

1.2.9 Message Digest 2 (MD2)

Bit-based generates a 128-bit hash value from a message of any length; optimized for use with smart cards.

1.2.10 MD4

Just like MD2 but optimized for lightning-fast program execution.

1.2.11 MD5

Identical to MD4, but slower due to more data manipulation. Designed as a response to concerns about MD4.

1.2.12 The SHA-2 Safe Hash Algorithm

Creates a 160-bit hash value, and it's modeled around MD4; NIST suggested it for the Secure Hash Standard (SHS).

The communication may be retrieved by the receiver using the retrieval mechanism and secret key supplied by the sender [16]. Fig. 6 depicts a paradigm for steganography using cryptography.

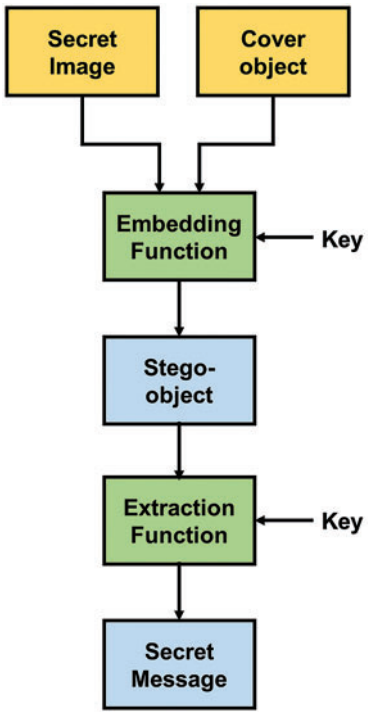

Figure 6: A model of the steganography process with cryptography

The goal of a digital steganography procedure is to covertly bury sensitive data in another medium. Binary bits, text data, and even picture and video files may all fall under the category of "secret data" [17]. All forms of digital content, such as photos, films, and writings, are fair game for the jacket. The term "secret data" is used to describe information that has been effectively concealed inside a cover/host media, whereas the term "stego-media" describes the actual media that has been concealed. It is intended that the stego-media be disseminated over a wide-open or unprotected route of communication [18–21]. Fig. 7 is a block diagrammatic depiction of a typical steganography system.

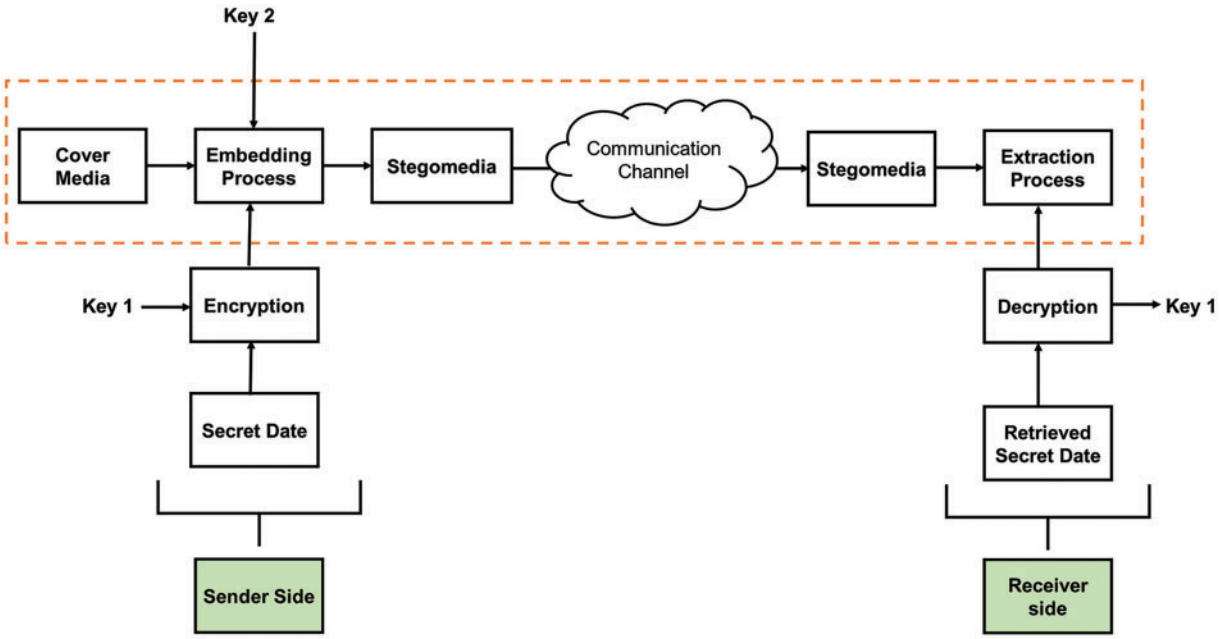

Figure 7: Block diagram of a typical steganography system

Even if the message is picked up, it won't make any sense. When applied to the realm of digital communication, both cryptography and steganography have the same goal: preserving the confidentiality of a message while hiding it from prying eyes [22]. In either combination or alone, these methods are helpful. Combining them also yields outstanding results but should be done in stages for maximum safety. These days, digital steganography may be used to conceal data in a variety of media, including messages, images, Deoxyribonucleic acid (DNA), networks, video, and audio [23]. Considering the breadth of steganography, it is easy to see why current steganography is crucial for security and integrity, particularly in the context of the internet [24]. Secret sharing provides an alternative to traditional methods of exchanging and storing confidential data since it divides the secret into pieces (called shares) that may be stored on different disks and/or sent over other routes. This strategy therefore resolves the single point of failure issue. The dealer, often referred to as the secret holder, splits the secret into n shares in a secret-sharing arrangement. Shares may be awarded to a group of individuals known as shareholders [25].

The internet community's reliance on cryptosystems has diminished because of the restrictions imposed by the government. This is why we rely on steganography, a technique that encodes messages in such a way that they are impossible to decipher without the correct key, even when the host medium is compromised [26]. To the best of our knowledge, picture steganography is still the most popular

medium among the several forms of digital steganography due to its superior capacity to hide hidden data in the cover media with undetectable effects [27,28].

The problem statement involves concealing information by encoding it in the LSB of each Red Green Blue (RGB) pixel value in the cover image. To further protect the confidentiality of the message, the private message must first be transformed to cipher text using the RSA technique before it can be embedded [29,30]. Hash-LSB, a method developed from LSB insertion on pictures, was used in this strategy. To ascertain the optimal locations to insert or hide information, we utilize a hashing algorithm in our Hash-LSB. We possess a challenging task in merging the two systems, one of which is the RSA algorithm originating from cryptography and another is the Hash-LSB method from steganography [31].

This review is important because it addresses the persistent problem of protecting confidential information when communicating. Although several methods, such as steganography, have been developed to enable secure data transfer, there are still gaps in the reviews that have already been published. To be more precise, previous research could have failed to do a sufficient job of examining how different hashing algorithms may be integrated into image steganography or stressing how important it is to have as little volatility in image bits as possible to guarantee security and efficacy. By putting up a fresh approach that solves these drawbacks, this review seeks to close these gaps and progress the field of secure data transfer. Our research has concentrated on uncovering a technique by which sensitive data might be securely sent and distributed. It is normal procedure for all respected enterprises to encode confidential information before transmitting it over the internet to prevent any disclosure of data about the company to adversaries or non-members. Founded the Hash-LSB and RSA algorithms, we formulated a safe steganography approach that is more protected than another alternative presently in utilization for hiding information in transmission. This study aims to investigate the effectiveness of image steganography by utilizing various hashing methods. To supply light on the durability and security of steganography techniques that use diverse hashing algorithms, this research will investigate the degree to which approaches can conceal data from access while safeguarding image integrity and nondisclosure. This article examines and assesses diverse techniques for concealing data within digital images for improved protection.

Motivation of the Study

- Research targets historical to modern data security, prioritizing the protection of sensitive information across eras.
- Researchers pursue covert communication with steganography, highlighting persistent interest in secure encryption methods.
- This review focuses on image steganography employing multiple hashing algorithms such as Hash-LSB, RSA, Blowfish, and DCT.
- A novel method ensuring minimal variance in image bits for heightened security.
- Additionally, encryption mechanisms are integrated, ensuring data confidentiality before embedding it into images.
- Secure data transport using encryption and diverse hashing algorithms prevents interception, bolstering overall security and privacy measures effectively.

Research Gap

- This study addresses the persistent challenge of securely transmitting sensitive information through innovative steganography techniques.

- We explore image steganography employing diverse hashing algorithms such as Hash-LSB, RSA, Blowfish, and DCT.
- The multiple hashing algorithms minimize image bit variance for heightened security and integrate cryptography for further protection.
- Encrypt messages first, use hash table encryption for robust data concealment, safeguarding against interception.
- Additionally, multiple layers of security through varied hashing algorithms enhance protection against unauthorized access.

The following is the remainder of this article: Section 2 provides related material. The method is addressed in Section 3. Section 4 provides main conclusions.

2 Existing Works

The goal of [32] is to provide an image steganography technique that divides the image into parts and hides information for each component. For image segmentation, a variety of clustering techniques can be applied. To keep the data safe, this suggested work [33] combines Hash-LSB steganography, data compression, and RSA cryptography. The RSA encryption technique is used, and the recipient must use their private key to decrypt the message because it was encrypted with a public key. The article [34] presents a combination of three approaches, including a modified version of the RSA cryptographic algorithm, concealed text created with steganography, and the selection of a random pixel from an image, to increase the overall degree of security provided by the system. Steganography and cryptography are two strategies for protecting data from outsiders. Steganography is the artwork and technological know-how of concealing a hid message in a photograph, while cryptography is a manner of converting original text to encrypted text [35]. This article [36] is an exploratory evaluation of the basics of cryptography and steganography methods. Furthermore, the paper offers a brief evaluation of several cryptographic factors which can be widely utilized in the subject of communique safety. Moreover, it consists of numerous mathematical problems and an analysis of safety factors for a number of diverse sorts of offenses. The essential cause of this research [37] is to improve the level of safety supplied by way of cryptography with the aid of utilizing a supplementary approach called steganography. Video images, a sound record, or an image can all consist of hidden facts using steganography methods.

The act of concealing a file, message, picture, or video within another file, message, image, or video is referred to as steganography [38]. Picture steganography is presented in this study [39], along with assessment criteria that consider a variety of characteristics related to the ability to hide data and increase security. The results of the testing show that the proposed approach may successfully disguise data while also providing a very high degree of security. The purpose of that research [40] is to provide a high-level overview of steganography in cloud technology and to assess different studies based on their technique choices, carrier kinds, payload capacities, and embedded methods to prepare the way for new and exciting research. This study will also evaluate and contrast these investigations to open crucial research avenues.

The major objective of this study [41] is to investigate the many ways in which steganography and cryptographic procedures might be combined to produce a hybrid security solution. Additionally, several contrasts between cryptographic approaches and steganography were discussed and given. Table 1 compares the previous studies.

Table 1: Literature survey

Reference	Methods	Finding	Advantages	Disadvantages	Limitation
[31]	The cover image is into super pixels and uses Modified Simple Linear Iterative Clustering (M-SLIC) for over-segmentation to conceal secret data inside grayscale image edge regions.	The proposed steganography method using M-SLIC for edge-based concealment achieves enhanced capacity, security, and imperceptibility compared to recent methods.	The approach leverages human visual system characteristics, enhancing imperceptibility. It offers good capacity and security compared to recent techniques.	Complexity in determining the optimal parameter K for M-SLIC can pose challenges. Additionally, the method cannot be suitable for all types of images or scenarios.	Requires careful parameter tuning for optimal performance and cannot evade sophisticated detection methods.
[32]	Utilizing RSA cryptography, data compression via Huffman coding, and Discrete Wavelet Transform (DWT) for image compression, the approach embeds encrypted data into cover images using Hash-LSB steganography.	The method ensures secure, efficient data transmission. Evaluated metrics Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Compression ratio, and Mean Squared Error (MSE) showcase integrity preservation and minimal overhead.	Enhanced security via encryption, compression, and steganography. Efficient internet data transmission with RSA cryptography, and Hash-LSB steganography for covert embedding.	Complexity impedes upkeep. Susceptible to RSA flaws, steganography detection. Lossy compression can degrade images. Demands precise parameter tuning for efficiency and safety.	Dependent on computational resources, vulnerable to advanced decryption techniques, potential for data loss.

(Continued)

Table 1 (continued)

Reference	Methods	Finding	Advantages	Disadvantages	Limitation
[33]	The modified RSA cryptography, steganography with LSB technique, and random pixel selection from fluid motion images for enhanced security.	Using these methods, the system achieves high security, demonstrated through PSNR, MSE, SSIM, and histogram comparisons between original and stego-images.	Enhanced security due to the combination of techniques, preventing detection and sharing of information by intruders.	Potential complexity in implementation and computational overhead due to the combination of multiple techniques.	Increased computational complexity and potential reduction in image quality due to multiple techniques.
[34]	The research explores substitution techniques in image steganography, emphasizing techniques for the least and most important bits.	It reveals the efficacy of hiding information within image files while maintaining secrecy, suitable for secure communication.	Provides an extra layer of security, applicable for secret service agencies and common individuals.	Requires decoding to access hidden information, potential for detection with advanced analysis.	Steganography conceals information but can be vulnerable if detection techniques improve over time.
[35]	Empirical study on medical imaging devices, including threat modeling, attack technique proposal, protection mechanism design, and effectiveness evaluation.	Identified security vulnerabilities in medical imaging devices, proposed attack techniques and evaluated protection mechanisms' effectiveness.	Enhances understanding of cybersecurity issues in medical cyber-physical systems, and provides actionable suggestions for device manufacturers.	With the limited scope of devices and manufacturers investigated the potential for evolving threats is not fully addressed.	Limited empirical scope, narrow device selection, and potentially overlooked security aspects pose study limitations.

(Continued)

Table 1 (continued)

Reference	Methods	Finding	Advantages	Disadvantages	Limitation
[36]	A new approach embeds hidden messages in images using steganography, cryptography, and chaotic pseudo-random generators to determine pixel placement and order.	Evaluation employs tests, key space, visuals, etc. Results confirm the stegoalgorithm's efficacy in covertly embedding messages in images, preserving visual integrity.	Strong security is achieved by combining cryptography with steganography. Complexity is increased by chaotic pseudo-random creation. Thorough assessment ensures dependability and successfully blocks attackers.	Complex implementation can demand ample computational power. Balancing security and visual quality poses challenges; advanced adversaries can require continual adjustments.	Vulnerable to advance, potentially compromising secrecy, and susceptible to visual distortion.
[37]	Steganography conceals data within other data, typically images, videos, or audio files.	Steganography, complementing cryptography, conceals messages, bolstering security. Originating in 1499 with Trithemius, predating contemporary encryption methods.	Enhances security by embedding messages in harmless data, minimizing detection risk, and suitable for discreet transmission of encrypted information.	Extra resources are needed for coding/decoding. Evolving detection poses a secrecy challenge. Misuse can entail legal consequences in encryption-restricted jurisdictions.	Susceptible to detection if the steganography method or key is discovered or compromised.

(Continued)

Table 1 (continued)

Reference	Methods	Finding	Advantages	Disadvantages	Limitation
[38]	The image steganography involves de-colorization and colorization processes.	The method embeds secret information during color translation, countering embedding influence through de-colorization networks.	A robust embedding algorithm considers color translation as an attack, enhancing security.	Increased complexity due to additional processes.	Embedding operation distorts cover image distribution, posing security risks despite sophisticated distortion functions.
[39]	A concealed attack using generative adversarial networks (GANs) and perceptual losses for robust watermarking.	The proposed method improves imperceptibility and attack ability compared to existing watermarking attack methods.	Utilizes GANs and perceptual losses to generate watermarked images with better visual quality and robustness against extraction.	Requires computational resources and can still affect visual quality to some extent.	The concealed attack method can still reduce the visual quality of watermarked images despite improvements.
[40]	Examines merging steganography, and cryptography for stronger communication, assessing techniques for their integration into hybrid systems.	Steganography hides, and cryptography secures, forming strong defenses against breaches and unauthorized access.	Enhanced security, confidentiality, and resilience against attacks. Allows for secure communication over unsecured networks.	Complexity in implementation and potential performance overhead. Requires careful integration and management of both techniques.	Limitations include potential attacks, network changes, and difficulty establishing secure communication over unsecured networks.

3 Analysis of Hashing Algorithms Used for Image Steganography and Cryptography

Hashing methods provide unique hash values for images, which helps to ensure data authenticity and reliability in image steganography. The image can have these hash values stored in it or utilized to check the integrity of the file as it is being sent. Hashing techniques result in fixed-length hash values that uniquely reflect input data, offering a dependable method for data protection and verification. Though hashing improves the security of cryptography and image steganography, it's vital to be aware of its drawbacks, including its susceptibility to colliding threats and the requirement for additional encryption techniques for complete data protection.

3.1 Techniques for Enhancing Steganography in the Spatial Domain

The most popular steganography techniques in the spatial realm work to alter the embedding and noise of the image's LSB layer. The LSB technique is a simple presentation method that works for both visual and auditory content. In the context of images, LSB approaches are cognizant of the need to communicate securely by exchanging just the least prominent advantage of pixel values. For illustration, the value of grayscale can vary from 0 to 255, denoted by 8 bits (shown in Fig. 8). To embed additional data into the cover object, the lowest N bits are swapped or replaced. When applied to a picture, approaches that use the least significant bits reveal no change. Multiple photographs of the same-looking subject have been corroborated by eyewitnesses, proving this to be the case.

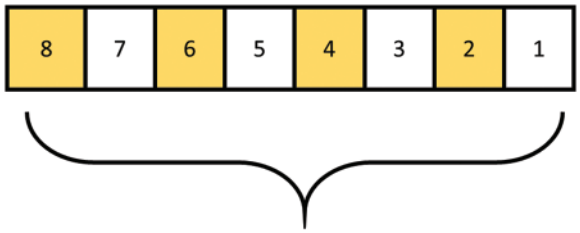

Figure 8: LSB replacement

The LSB method involves exchanging pixels for a hidden message. Fig. 9 shows because the concealed message's components are scattered carelessly. This method is often used to redistribute the bits; as a result, the LSBs will be altered in half of the instances. For ways to hide information. The LSB method is used to modify pixels randomly, while other algorithms are used to change pixels in certain parts of an image. There's another way to hide the hidden message improvements to steganography techniques for the spatial domain are used to randomly add noise to pixels in a way that statistically looks like a common way that images get distorted, such as with scanner noise or standard digital noise. When a shared key is used with a pseudo-random noise generator, it creates distortion. These methods of embedding and extracting are used to find a place and make a list of places that point to parts object.

The procedures of the embed algorithm are used to alter the elements, like pixels in a picture, to conceal the message, while the procedures of the extraction algorithm are used to retrieve the message by examining the same sequence of places. In the LSB-improved methods, an embedding and extraction algorithm is used. The LSB procedure, which swaps the LSB of the messages, is at the heart of the LSB improvement methods used in the embedding process. If two message bits were to be stored in the two LSBs of a single cover element, it would be an example of an LSB operation that modifies more than one bit of the cover. The stego-object is chosen, extracted, and aligned using LSB enhancement methods to retrieve the hidden message.

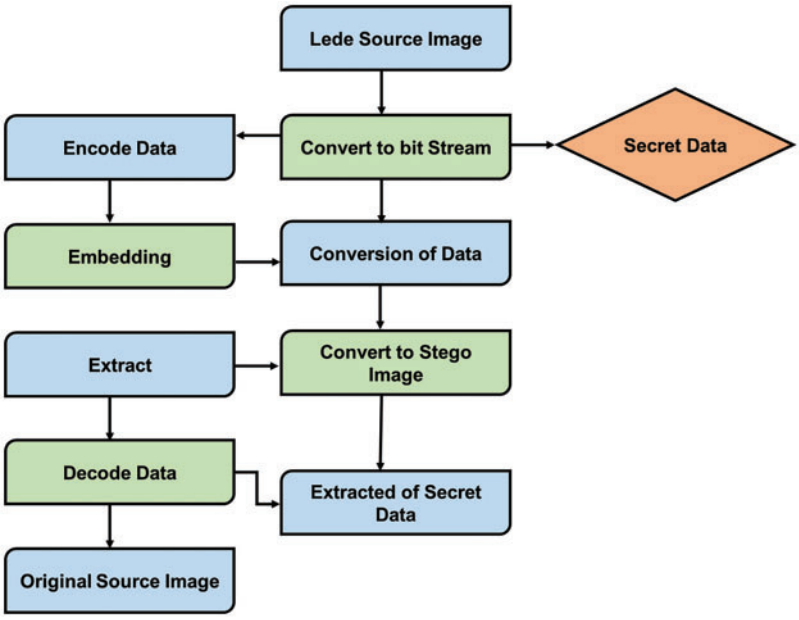

Figure 9: Block diagram for the LSB method

3.2 H-LSB-Based Method

The Hash-based Least Significant Bit Technique, for example, steganography is the practice of concealing information or messages inside images [42–46]. Steganography is nothing more than covered writing; it uses a mechanism to hide secret messages as well as information that is hidden inside other data. The art of covert communication or the science of undetectable communication is steganography. The fundamental objective of the hash-based least significant bit approach for picture steganography, which has been presented, is to embed a secret file or piece of information in a specific image file, which can subsequently be extracted using a stego key or password. To embed data in the cover picture with a change in the lower bit, in this cryptography, the Least Significant Bits inserting technique is used. There is no indication of this LSB insertion [47–51]. It has been suggested to use an image steganography technique that performs encoding and decoding for hiding and extracting messages, respectively. First, a message file will be steganographically hidden inside a cover image file using LSB techniques. The Hash-LSB algorithm is a common technique in steganography, the art of hiding information within digital media. In this method, secret data is embedded into the least significant bit of pixel values in an image or audio file. Because the LSBs have the least impact on the overall appearance, alterations are often imperceptible to the human eye or ear. Hash functions are utilized to ensure the integrity of the embedded data, generating a unique fingerprint for verification. By employing Hash-LSB, steganographers can conceal information securely while minimizing detectable alterations to the carrier medium. To extract embedded data, this steganography program is once again used with this file [52–56]. The hidden data is placed as a payload in the frames that make up the cover picture, which is composed of several pixels. Following are explanations of data encoding, data decoding, and data concealment in images [57–61].

3.2.1 Encoding Technique

The process of encoding begins with the selection of an image file, followed by the collection of data concerning the cover-free pixel LSB [62,63]. These picture pixels are isolated from one another, and then inside this image, a secret message is concealed by utilizing a technique that is based on the hash of the least significant bit [64–68]. After the hash code has been created, it is helpful to embed the data within the frame. Then, it will find the four LSBs of the pixels in which the secret message is stored [69–71]. When extra pixels are added to the mix of Stego pixels, a picture known as Stegno is produced. This Stegno picture will be sent to the specified recipient after it has finished transmitting. This encoding method was formerly employed to conceal data [72–74].

3.2.2 Decoding Technique

To decode the message, a Stegno picture must first be captured, and then, to derive the confidential data or information from the image, information regarding the image must be gathered. To decode the data, this pixel from the Stego picture will be sent into the de-steganography program [75,76]. It is possible to extract secret information from this pixel. Decoding the data so that it may be read by the intended recipient will require the use of a password. This password is sometimes referred to as the Stego key [77]. Fig. 10 represents the encoding and decoding techniques.

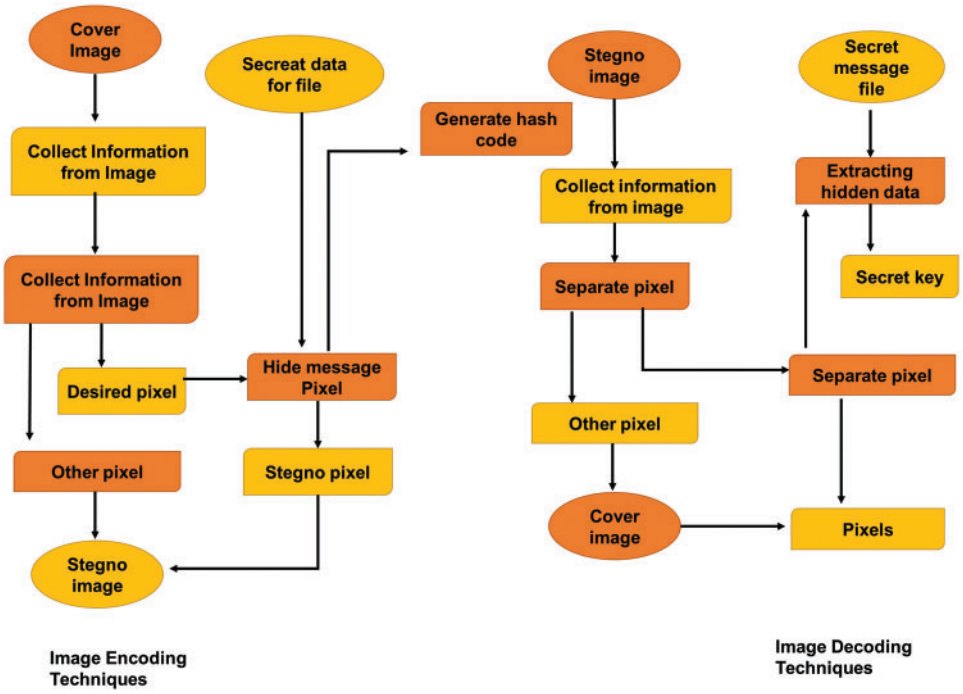

Figure 10: Encoding and decoding techniques

3.2.3 Hash-LSB Decoding

In the decoding procedure, we employed the hash function once again to determine the locations of the LSBs where the embedded data bits were located. After specifying the location of the bits, the segments are recovered from their location in the similar sequence in which they existed as encased. After this procedure, we will receive the information in dual form, which is then transformed into

denary form, and the encrypted instant text will be obtained using the same procedure. After obtaining the locations of LSBs containing secret information, the receiver will use the RSA technique to decode the secret data. Fig. 11 depicts the decryption flow. To use the RSA algorithm, the recipient will utilize his/her private key, since the public key of the receiver has already encrypted the secret data. With the private key of the receiver, the encrypted text will be transformed into the original, readable message.

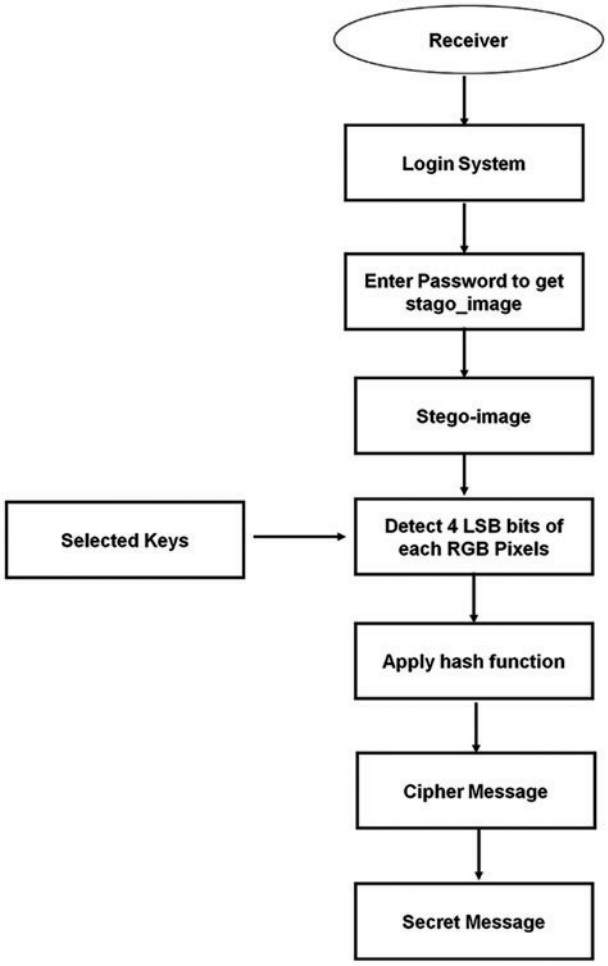

Figure 11: Decryption flowchart

A Method for Data Recovery:

Step 1: Get a steganographic picture.

Step 2: Determine the four LSBs of each RGB pixel in the steganographic picture.

Step 3: Use the hash function to find the location of LSBs containing concealed data.

Step 4: Obtain the bits using places 3, 3, and 2 in that sequence.

Step 5: Decrypt the recovered data using the RSA technique.

Step 6: Ultimately, the hidden message was revealed.

3.2.4 Algorithm Hash Flow

The process that creates the hash function is known as the least significant bit of hashing. This hash function not only counts the number of LSB bits in the picture but also considers the location of each hidden pixel and where it is inside the pixel [78–81]. A digital string of a predetermined length is generated in response to a hash value that accepts input of a variable length. In huge files, the hash function is also utilized for identifying instances of duplicate records [82–86].

The hash function is often provided as shown in Eq. (1).

$$x = y\,\%\,z \tag{1}$$

where x, y, and z represent the coordinates of the LSB inside the pixel, (x, y, z) represent the coordinates of each pixel in the concealed picture, and z represents the total number of [87–89]. Fig. 12 indicates the bits of the private message that are distributed.

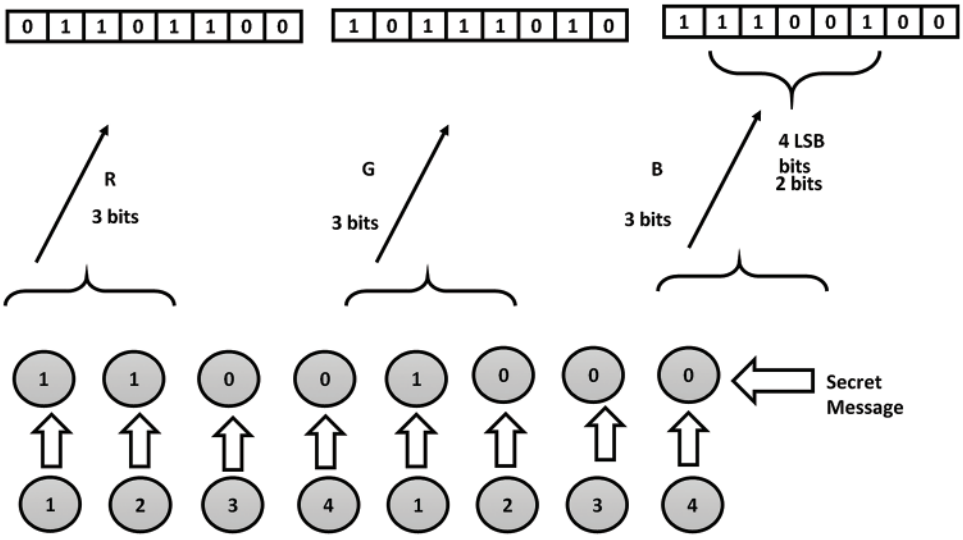

Figure 12: Bits of the secret message is distributed

3.3 Analysis of the RSA Algorithm

The RSA algorithm is a message-encrypting cryptosystem that uses the product of two prime integers to create a pair of keys, which are then used to encrypt and decode messages. The original content might be placed in the cover picture as encrypted text using the RSA method in conjunction with Hash-LSB. We are raising the degree of security by employing the RSA. In the instance of steganalysis, only cipher text that is encrypted and unreadable may be recovered, making it secure. The RSA algorithm, a cornerstone of modern encryption, contributes significantly to steganography the concealing of messages within other media. In steganography, RSA aids by encrypting the secret message before embedding it within an innocuous carrier file, such as an image or audio clip. RSA's strength lies in its use of public and private keys: the sender uses the recipient's public key to encrypt the message, which only the recipient can decrypt using their private key. This ensures the secrecy of the embedded message, enhancing the security of steganography techniques, and safeguarding against unauthorized access and detection.

The RSA algorithm:

(i) Choose two very huge, powerful prime numbers, k and l. Let $m = kl$.

(ii) Calculate the totient value of Euler for m: $g(m) = (k-1)(l-1)$.

(iii) Find a randomly generated e that is satisfactory $1 < e < g(m)$ and relatively prime to $g(m)$, i.e., $abc(d, g(m)) = 1$.

(iv) Determine a value for e such that $e = d - 1\, modg(m)$.

(v) Encryption: Given an unencrypted text m, $o < m$, then the ciphertext $c = nd\, mod\, m$.

(vi) Decryption: The process of decrypting the ciphertext $n = be\, mod\, m$.

This approach relies on the following mathematical concepts, all of which should be familiar to the user (It must seek out the final one, the Euler totient function since they are unfamiliar to each other):

- Exponentials
- Prime numbers
- Modular arithmetic
- Prime factorization
- Euler totient function
- Greatest Common Denominator (GCD)

Since this is being planned with development in mind, we should probably be familiar with binary, char, bits, ASCII, and UTF-8 [90,91].

When it uses algorithms with single-character parameters [92] as examples. This may be the theoretically right way to do it, but we find that we prefer the developer-style approach, where each variable has a meaningful name. We decided to put pen to paper and make sure we fully grasped how RSA operates. We observe how developers effectively employ a solitary symbol in this case.

For both decryption and encryption, the RSA method makes use of a pair of keys, d, and e. The transformation from a plaintext message P to cipher text C is accomplished by

$$X = O^{w} mod\ b \tag{2}$$

The original text may be retrieved using Eq. (3).

$$B = X^{s} mod\ b \tag{3}$$

Because modular arithmetic is symmetric, decryption and encryption are reversed operations that can be performed against one another. This allows these two processes to be interchanged. Therefore,

$$O = X^{s} mod\ b = (O^{w})^{s}\ mod\ b = (O^{s})^{w}\ mod\ b \tag{4}$$

As a result of this connection, either the encryption or decryption transformation might be applied first [93].

One will never write code in this manner, and upon first glance, a non-expert would question what the variables, X, s, w, and n stand for. Is it necessary to use uppercase O and X when using lowercase letters for s and w? Let's rebuild these with classy developer variable names that reflect what they are in actuality. The definitions of each variable in the paragraph that was cited above are apparent, but read further to find out what "mod n" means. The source of the values for each variable is also not specified.

Upon further reading, this resulted in the addition of more equations to the list. In the alphabetical procedure, these are the equations [94,95].

3.4 Encryption Phase

A username and password are required for the initial stage of accessing the model to hide the data. After successfully logging into the system, the client may compose a text to encrypt the information using the private keys before embedding the data into a picture, as shown in Fig. 13. The proposed method in our system uses the affine algorithm to encrypt private data. The affine cipher is one method for information encryption.

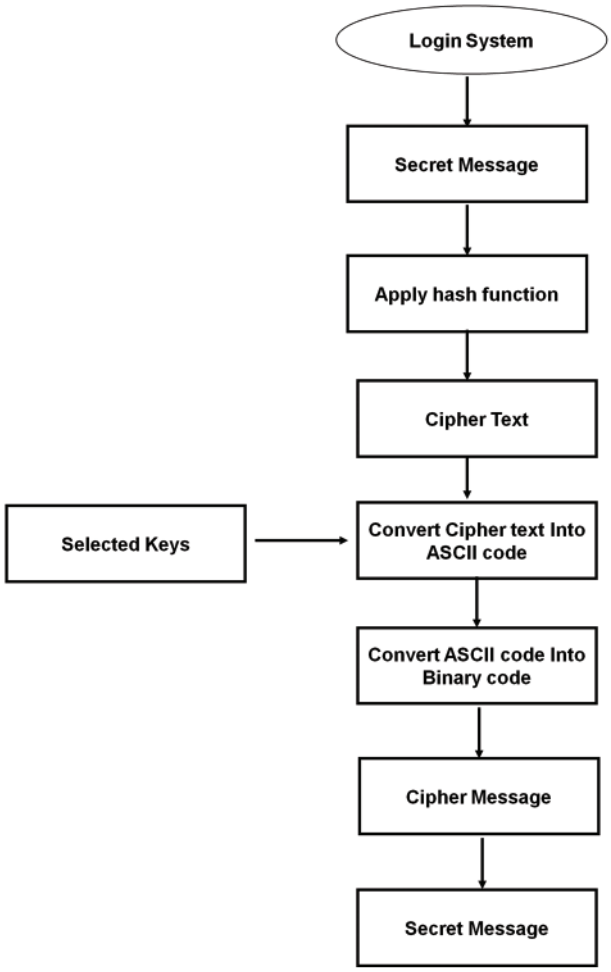

Figure 13: Encryption phase flowchart

In this procedure, mapping each letter of the alphabet to its corresponding number is encoded using an algebraic function, before changing once more into a letter. Each letter encrypts to every other letter and back again due to the equation used, suggesting that the cipher is really just a standard substitution algorithm with a rule dictating which character is sent to another. This technology offers superior privacy to secure the data user from illegal network access, making it difficult to retrieve the information without the receiver key. After turning plain text into cipher text using the affine method,

we took the cipher text and transformed each letter into ASCII codes, which were then translated into a sequence of binary digits to give further security. This suggested approach is used to prevent attackers from obtaining the true data while attempting to acquire it. This encrypted data will be integrated into the picture with little modification to the actual picture.

Process of encryption

Step 1: Choose the hidden message.

Step 2: Text encryption using the Affine Cipher method.

Step 3: Transform the encrypted message into ASCII code.

Step 4: Convert text from ASCII to binary.

Tables 2 and 3 display the detected value and the encrypted value using cryptography techniques.

Table 2: Determining the Y value

Plaintext	S	I	D	R	U	K
Y	18	8	3	17	20	10

Table 3: Change unencrypted text into encrypted

Plaintext	S	I	D	R	U	K
Y	18	8	3	17	20	10
(3y + 6)	60	30	12	57	66	36
(3y + 6) 26	8	4	12	5	14	10
Cipher text	I	E	M	F	O	K

Solve the initial portion of the equation (3y + 6), for each possible value of y. After getting the value of (3y + 6) for each character, divide that number by 26 and save the leftover. The first four stages of encryption are laid out in Table 3.

To decipher encrypted text to normal ASCII: 105 101 109 119 111 75 converting from the ASCII code to binary: 01101001 01100101 01101101 0111011101101111 01001011.

3.5 Embedding Phase

When the secret message has been encrypted, we have offered a method for embedding it into an image. The least significant bit is swapped out for a hash value utilizing a hash-based LSB. One of the most popular uses of steganography is to encrypt data contained in image files. and LSB is the technique of choice for doing so. This approach has been successfully used to encrypt a message, embed it in a picture, and then deliver the image to its intended recipient.

A simple LSB matching method that uses a *random* ± 1 modification process to conceal one-bit regarding data in each pixel. Here, in contrast to LSB replacement techniques, LSB matching might effectively fend off the RS attack because of the unpredictability in raising or lowering the original pixel following the concealment of the secret bits. Below is a presentation of the embedding and extraction process with concrete instance. The embedding equation and the function $E(.)$ are provided in Eqs. (5)

and (6), respectively, may be used to generate the stego-pixels (p_1^*, p_2^*) for the original pixels (p_1, p_2) during embedding, where a_1, and a_2 indicate the two bits of the confidential data.

$$\left(p_1^*,\ p_2^*\right) = \left\{ \begin{array}{l} \left(p_1,\ p_2\right), if\ \left(LSB\left(p_1\right) = a_1\right) and\ \left(LSB\left(p_1,\ p_2\right) = a_2\right) \\ \left(p_1,\ p_2 + 1\right), if\ \left(LSB\left(p_1\right) = a_1\right) and\ \left(LSBE\left(p_1,\ p_2\right) \neq a_2\right) \\ \left(p_1 - 1,\ p_2\right), if\ \left(LSB\left(p_1\right) \neq a_1\right) and\ \left(LSB\left(p_1 - 1, p_2\right)\ = a_2\right) \\ \left(p_1 + 1,\ p_2\right), if\ \left(LSB\left(p_1\right) \neq a_1\right) and\ \left(LSB\left(p_1 - 1, p_2\right)\ \neq a_2\right) \end{array} \right\} \tag{5}$$

$$E((p_1,\ p_2) = LSB\left(\lfloor p_1/2 \rfloor + p_2\right) \tag{6}$$

$$p_2 = LSB\left(\left\lfloor p_1^*/2 \right\rfloor + p_2^*\right) \tag{7}$$

In this study, we propose a multi-layered security system that combines cryptography and steganography to make our data more impenetrable to outsiders. To protect sensitive information during data transfer via an unsecured connection, users may wish to use both of these techniques. To begin, we encrypt the text that will eventually be hidden in the cover photo, making it nearly impossible for anyone but the intended recipient to read without access to their private key. Next, we use a hash function to figure out where the message should go, and finally, we use a technique that embeds eight bits of secret data into the LSB of each pixel's value in the color channels of RGB. The hash function of LSB for RGB is shown in Fig. 14. Our methods for concealing information inside a picture include embedding three bits into the LSB of each red pixel, three bits into the LSB of each *G* pixel, and two bits into the LSB of each blue pixel. Blue has a greater prismatic impact on the human eye than *R* or *G*, thus these eight bits are placed in that sequence.

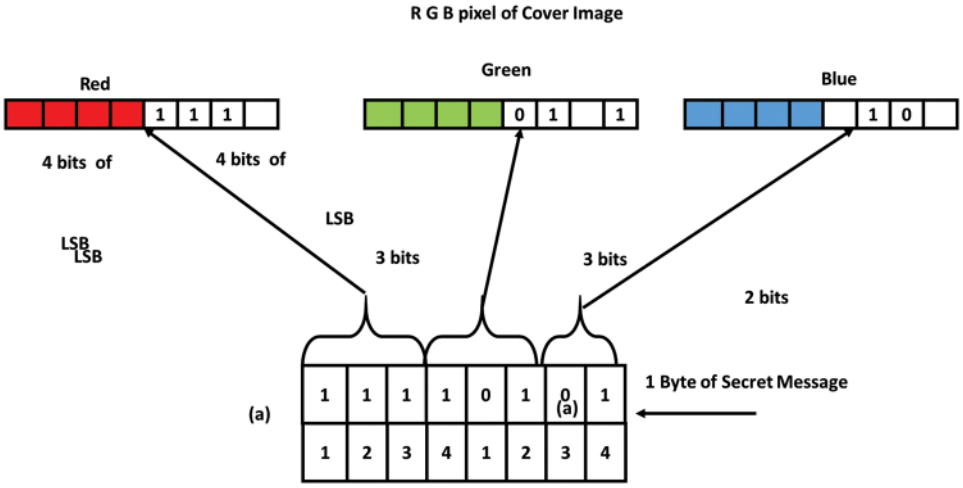

Figure 14: Hash process to determine the LSB of RGB

This procedure is repeated until the full-bit message has been included in the cover art. Using this method, we can determine where in the cover image's RGB color space each pixel may be utilized to conceal information.

$$P = r\%m \tag{8}$$

where P is the location of the LSB bit inside the pixel, r is the positioning of each concealed picture pixel, and M is the number of LSB bits.

Embedding proposed algorithm:

Step 1: Take the message and code it.

Step 2: Pick the picture on the cover.

Step 3: Extract four LSB bits from each RGB pixel of the cover image.

Step 4: In the sequence of 3, 3, and 2, respectively, encrypt eight bits of the ciphered information into four bits of the LSB of the RGB colors that make up the cover image using the coordinates indicated by the hashing algorithm in Eq. (5).

3.6 Blowfish Algorithm

When ciphering statistics, the Blowfish technique applies a Feistel machine, this is repeated 16 times.

Every repetition contains a rearrangement of the key and a substitute of the facts. Blowfish, a symmetric-key block cipher, performs a critical element in steganography by way of presenting a secure manner to different records. In steganography, Blowfish secures the information to be hid, creating a coded message. This encrypted text is subsequently inserted into a host medium, such as an image or sound file. Blowfish's durability lies in its key-reliant S-boxes and complicated key schedule, making it resistant to exhaustive attacks.

Thus, Blowfish improves methods of steganography by offering a robust security layer, protecting the secrecy of concealed data.

The following are the stages of the data encryption process:

1. Using a divider, separate the 64-bit block into two 32-bit halves. The result of applying the XOR operator to the first element of the P-block with the left-hand block XL is then sent to the F function block as shown in Fig. 15.
2. The input of 32 bits is substituted by another output of the same size in the F function block.
3. After each cycle is completed successfully, the right half becomes the new left half or vice versa by XORing the output from the F function block with the right half's XR, as shown in Fig. 15.
4. The above procedure is repeated for a maximum of 16 iterations.
5. The final two halves, instead of being swapped, are XORed with the seventeenth and eighteenth parts of the P box. The resulting encrypted text is unintelligible to potential adversaries [96,97].

3.7 DCT

DCT is like an encoder and decoder. DCT is the initial stage of image compression. The entropy encoder, quantizer, and FDCT make up this system [98]. DCT decoding is the second stage. Entropy decoder, dehumanizer, and inverse mapped make up this system [99–101]. The DCT algorithm is pivotal in steganography due to its ability to efficiently transform spatial information into frequency domain representation. In steganography, it conceals secret data within cover media such as images or audio. By applying DCT, the original signal is decomposed into frequency components, facilitating the embedding of hidden information in less perceptible frequency coefficients. Altering these coefficients slightly maintains the cover media's graphical or aural qualities while including the hidden message. Upon retrieval, the DCT algorithm is reversed to recover the hidden data. Its effectiveness lies in

balancing data concealment with maintaining cover media fidelity. Fig. 16 represents the compressed and decompressed steps.

- The image input measures B by N.
- Image intensity at the intersection of rows u and columns h is denoted by $D\ (u,\ h)$.
- Row j_1 and columns j_2 of the DCT matrix include the coefficient D for the discrete cosine transform $(t,\ z)$.
- Low frequencies, which may be seen in the DCT's top left corner, contain most of the signal energy for the majority of images.
- Since the lower right numbers frequently indicate higher frequencies and are modest enough to be ignored with little to no obvious distortion, compression is made possible.
- An array of integers measuring 8 by 8 is the DCT input. The grayscale value of each pixel is contained in this array.
- Levels in 8-bit pixels range from 0 to 255.

$$X\ (y,\ c) = \frac{\alpha(c)}{2}, \frac{\alpha(y)}{2} \sum_{t=0}^{7} \sum_{z=0}^{7} d\ (t, z)\ .Cos\left[\frac{\prod (2z+1)\, y}{16}\right].Cos\left[\frac{\prod (2t+1)\, c}{16}\right] \tag{9}$$

$For\ y,\ c\ =\ 0,\ 1,\ 2, \ldots, 7$

$$d\ (t,\ z) = \sum_{t=0}^{7} \frac{\alpha(c)}{2} \sum_{z=0}^{7} \frac{\alpha(y)}{2} X\ (y,\ c)\ .Cos\left[\frac{\prod (2z+1)\, y}{16}\right].Cos\left[\frac{\prod (2t+1)\, c}{16}\right] \tag{10}$$

$Forz,\ x\ =\ 0,\ 1,\ 2, \ldots, 7$

$$\alpha = \begin{bmatrix} \frac{1}{\sqrt{2} if} y = 0 \\ 1\ if\ y\ \Theta\ 0 \end{bmatrix} \tag{11}$$

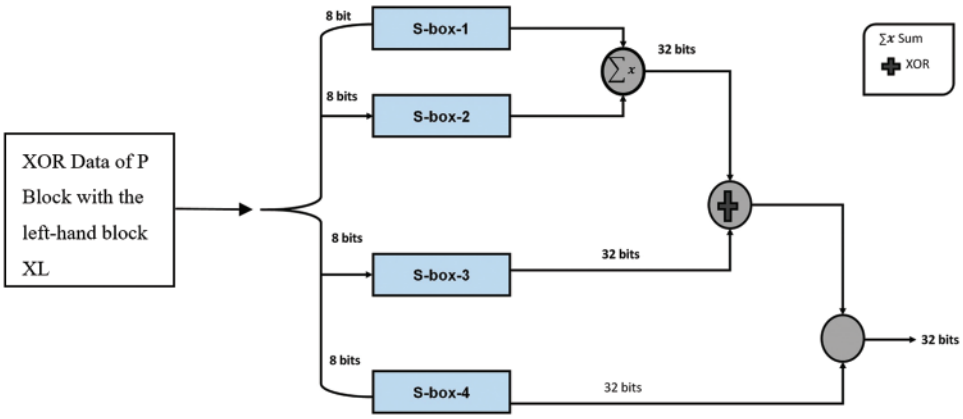

Figure 15: Blowfish algorithm flow (F function block)

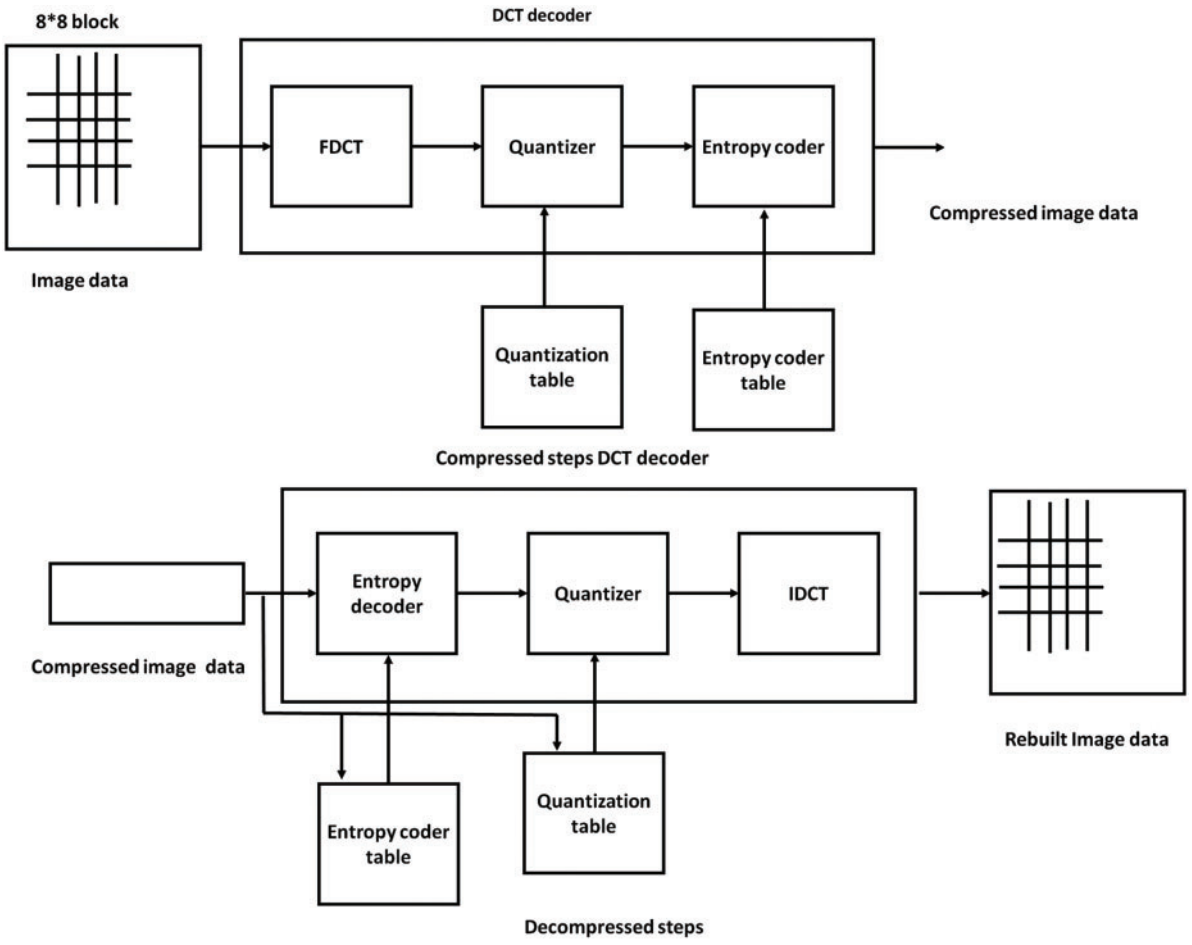

Figure 16: Compressed and decompressed steps

3.8 Discussion

These methods are highly relevant across diverse fields, including secure messaging, cyber forensics, copyright safeguarding, and hidden data transfer. In safe communication, they facilitate the transfer of confidential data while preserving privacy. Computerized forensics takes advantages from their capability to hide and remove concealed data for research-oriented reasons. In copyright safeguarding, those methods help in embedding possession data inside digital media to discourage unlawful use. Additionally, they promote hidden statistics transfer, allowing for a diffused switch of facts in private circumstances. Their realistic implications encompass strengthening information and techniques, enhancing confidentiality, and progressing the vicinity of statistics protection through presenting efficient equipment for safeguarding digital assets and private correspondences. Applying numerous hashing techniques for enciphering and interpreting boosts the electricity of the steganography technique opposing multiple threats. Forceful breaches, that attempt to thoroughly look for the cipher key, are decreased by using the problem added through several hashing strategies. Furthermore, the exam of attacks in diverse hashing strategies yields several allocations of ciphered facts, making it tough for attackers to discover patterns or reap vast information. This approach assures enhanced protection by means of boosting the computational intricacy needed for decoding and lowering the

probability of effective attacks, therefore protective the privateness of hidden transmissions. The realistic execution of the numerous hashing techniques for involves evaluations of computational complexity, abilities needs, and actual-global implementations.

4 Conclusion

Image steganography is a Hash-LSB method dependent on the RSA method utilized. Using Discrete Cosine Transform (DCT) and the Hash-LSB method, the confidential data file is enciphered using the efficient Ciphering method RSA then affecting the ability to view the image. After utilizing the blowfish cipher and encrypted key value to secure the covered image, the aim is to provide user verification. In this work, a novel method of concealing information in an image with minimal variance in image bits has been developed, making our method more effective and safer. This method also uses the RSA algorithm to safeguard the secret message, making it difficult to decrypt the data without the proper key. The RSA algorithm is very secure in and of itself, therefore we employed this method to enhance the protection of confidential information. The H-LSB approach has been used on images having .tiff extension, but it may also be used in any other format with only small procedural changes, such as compressed images. A very good MSE and PSNR value for the stego pictures were obtained by comparing the created technique's performance analysis with that of the straightforward LSB technique. Limitations in this study the lack of comparative analysis among different hashing algorithms, limited scope in exploring newer, emerging hashing techniques, and potential bias towards existing methods. Future work investigates the effectiveness of hybrid hashing schemes, the exploration of robustness against advanced steganalysis techniques, and the examination of real-world application scenarios for diverse hashing algorithms.

Acknowledgement: Arshiya S. Ansari would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project No. R-2024-1170.

Funding Statement: This study did not receive any funds from anywhere.

Author Contributions: Data collection: Abdullah Alenizi, Mohammad Sajid Mohammadi; Analysis and interpretation of results: Ahmad A. Al-Hajji, Arshiya Sajid Ansari; Draft manuscript preparation: Mohammad Sajid Mohammadi, Abdullah Alenzi. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable. All references are from Google Scholar.

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

References

[1] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "A comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019. doi: 10.1016/j.neucom.2018.06.075.

[2] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image steganography: A review of the recent advances," *IEEE Access*, vol. 9, pp. 23409–23423, Jan. 2021. doi: 10.1109/ACCESS.2021.3053998.

[3] K. S. Hsieh and C. M. Wang, "Constructive image steganography using example-based weighted color transfer," *J. Inf. Secur. Appl.*, vol. 65, pp. 103126, Mar. 2022. doi: 10.1016/j.jisa.2022.103126.

[4] S. Hossain, S. Mukhopadhyay, B. Ray, S. K. Ghosal, and R. Sarkar, "A secured image steganography method based on ballot transform and genetic algorithm," *Multimed. Tools Appl.*, vol. 81, pp. 1–30, Nov. 2022. doi: 10.1007/s11042-022-13158-7.

[5] G. Swain and A. Pradhan, "Image steganography using remainder replacement, adaptive QVD, and QVC," *Wirel. Pers. Commun.*, vol. 123, no. 1, pp. 273–293, Mar. 2022. doi: 10.1007/s11277-021-09131-6.

[6] P. C. Mandal, I. Mukherjee, G. Paul, and B. N. Chatterji, "Digital image steganography: A literature survey," *Inform. Sci.*, vol. 609, pp. 1451–1488, Sep. 2022. doi: 10.1016/j.ins.2022.07.120.

[7] X. Liao, J. Yin, M. Chen, and Z. Qin, "Adaptive payload distribution in multiple images steganography based on image texture features," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 2, pp. 897–911, Jun. 2020. doi: 10.1109/TDSC.2020.3004708.

[8] V. Sharma, R. N. Mir, and R. K. Rout, "Towards secured image steganography based on content-adaptive adversarial perturbation," *Comput. Electric. Eng.*, vol. 105, pp. 108484, Jan. 2023. doi: 10.1016/j.compeleceng.2022.108484.

[9] X. Liao, Y. Yu, B. Li, Z. Li, and Z. Qin, "A new payload partition strategy in color image steganography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 3, pp. 685–696, Jan. 2019. doi: 10.1109/TCSVT.2019.2896270.

[10] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless image steganography: A survey," *IEEE Access*, vol. 7, pp. 171372–171394, Nov. 2019. doi: 10.1109/ACCESS.2019.2955452.

[11] D. R. I. M. Setiadi, "PSNR vs SSIM: Imperceptibility quality assessment for image steganography," *Multimed. Tools Appl.*, vol. 80, no. 6, pp. 8423–8444, Mar. 2021. doi: 10.1007/s11042-020-10035-z.

[12] K. A. Zhang, A. Cuesta-Infante, L. Xu, and K. Veeramachaneni, "SteganoGAN: High-capacity image steganography with GANs," arXiv preprint arXiv:1901.03892. Jan. 2019. doi: 10.48550/arXiv.1901.03892.

[13] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics Laser Technol.*, vol. 116, pp. 92–102, Aug. 2019. doi: 10.1016/j.optlastec.2019.03.005.

[14] D. M. Abdullah *et al.*, "Secure data transfer over the Internet using image steganography," *Asian J. Res. Comput. Sci.*, vol. 10, pp. 33–52, Jul. 2021. doi: 10.9734/AJRCOS/2021/v10i330243.

[15] W. Tang, B. Li, M. Barni, J. Li, and J. Huang, "An automatic cost learning framework for image steganography using deep reinforcement learning," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 952–967, Sep. 2020. doi: 10.1109/TIFS.2020.3025438.

[16] W. You, H. Zhang, and X. Zhao, "A Siamese CNN for image steganalysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 291–306, Jul. 2020. doi: 10.1109/TIFS.2020.3013204.

[17] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang and C. Qin, "Reversible image steganography scheme based on a U-Net structure," *IEEE Access*, vol. 7, pp. 9314–9323, 2019. doi: 10.1109/ACCESS.2019.2891247.

[18] S. Rustad, A. Syukur, and P. N. Andono, "Inverted LSB image steganography using an adaptive pattern to improve imperceptibility," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 6, pp. 3559–3568, Jun. 2022. doi: 10.1016/j.jksuci.2020.12.017.

[19] C. Yuan, H. Wang, P. He, J. Luo, and B. Li, "GAN-based image steganography for enhancing security via adversarial attack and pixel-wise deep fusion," *Multimed. Tools Appl.*, vol. 81, no. 5, pp. 6681–6701, Feb. 2022. doi: 10.1007/s11042-021-11778-z.

[20] T. Muralidharan, A. Cohen, A. Cohen, and N. Nissim, "The infinite race between steganography and steganalysis in images," *Signal Process.*, vol. 201, pp. 108711, Dec. 2022. doi: 10.1016/j.sigpro.2022.108711.

[21] J. Luo *et al.*, "Improving security for image steganography using content-adaptive adversarial perturbations," *Appl. Intell.*, vol. 53, pp. 16059–16076, 2023. doi: 10.1007/s10489-022-04321-6.

[22] J. Liu *et al.*, "Recent advances of image steganography with generative adversarial networks," *IEEE Access*, vol. 8, pp. 60575–60597, Mar. 2020. doi: 10.1109/ACCESS.2020.2983175.

[23] X. Duan, D. Guo, N. Liu, B. Li, M. Gou and C. Qin, "A new high-capacity image steganography method combined with image elliptic curve cryptography and deep neural network," *IEEE Access*, vol. 8, pp. 25777–25788, Feb. 2020. doi: 10.1109/ACCESS.2020.2971528.

[24] A. Gutub and M. Al-Ghamdi, "Hiding shares by multimedia image steganography for optimized counting-based secret sharing," *Multimed. Tools Appl.*, vol. 79, no. 11, pp. 7951–7985, Mar. 2020. doi: 10.1007/s11042-019-08427-x.

[25] A. Nag, J. P. Singh, and A. K. Singh, "An efficient Boolean-based multi-secret image-sharing scheme," *Multimed. Tools Appl.*, vol. 79, no. 23, pp. 16219–16243, Jun. 2020. doi: 10.1007/s11042-019-07807-7.

[26] M. Sharifzadeh, M. Aloraini, and D. Schonfeld, "Adaptive batch size image merging steganography and quantized Gaussian image steganography," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 867–879, 2020. doi: 10.1109/TIFS.2019.2929441.

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

[28] A. Alarood, N. Ababneh, M. Al-Khasawneh, M. Rawashdeh, and M. Al-Omari, "IoTSteg: Ensuring privacy and authenticity in the internet of things networks using weighted pixels classification-based image steganography," *Cluster Comput.*, vol. 25, no. 3, pp. 1607–1618, Jun. 2022. doi: 10.1007/s10586-021-03383-4.

[29] Y. Luo, J. Qin, X. Xiang, and Y. Tan, "Coverless image steganography based on multi-object recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 7, pp. 2779–2791, Oct. 2020. doi: 10.1109/TCSVT.2020.3033945.

[30] J. Jia, M. Luo, S. Ma, L. Wang, and Y. Liu, "Consensus-clustering-based automatic distribution matching for cross-domain image steganalysis," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 6, pp. 5665–5679, Mar. 2022. doi: 10.1109/TKDE.2022.3155924.

[31] M. Hassaballah, M. A. Hameed, A. I. Awad, and K. Muhammad, "A novel image steganography method for industrial internet of things security," *IEEE Trans. Ind. Inform.*, vol. 17, no. 11, pp. 7743–7751, Jan. 2021. doi: 10.1109/TII.2021.3053595.

[32] I. Kich, B. Ameur, and Y. Taouil, "Image steganography by modified simple linear iterative clustering," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 4, pp. 1640–1647, Feb. 2020. doi: 10.35940/ijitee.C8903.029420.

[33] A. Bose, A. Kumar, M. K. Hota, and S. Sherki, "Steganography method using effective combination of RSA cryptography and data compression," presented at the 2022 First Int. Conf. Electric., Electron., Inform. Commun. Technol. (ICEEICT), Trichy, India, Feb. 2022, pp. 1–5.

[34] H. N. Mohaisen and A. K. Hammoud, "Application of modified RSA cryptography and random LSB steganography on color images of fluid flow in a channel," *Int. J. Nonlinear Anal. Appl.*, vol. 12, no. 2, pp. 1725–1734, Nov. 2021. doi: 10.22075/ijnaa.2021.5312.

[35] L. K. Gupta, A. Singh, A. Kushwaha, and A. Vishwakarma, "Analysis of image steganography techniques for different image formats," presented at the Int. Conf. Adv. Electric., Comput., Commun. Sustain. Technol., Bhilai, Feb. 2021, pp. 1–6.

[36] Z. Wang, P. Ma, X. Zou, J. Zhang, and T. Yang, "Security of medical cyber-physical systems: An empirical study on imaging devices," *IEEE INFOCOM 2020-IEEE Conf. Comput. Commun. Workshops*, Oronto, ON, Canada, Jul. 2020, pp. 997–1002.

[37] 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, pp. 380, Jan. 2021. doi: 10.7717/peerj-cs.380.

[38] P. S. Dutta and S. Chakraborty, "Image-based steganography in cryptography implementing different encryption-decryption algorithm," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 6, no. 3, pp. 246–251, Jun. 2020. doi: 10.32628/IJSRCSEIT.

[39] Q. Li, B. Ma, X. Wang, C. Wang, and S. Gao, "Image steganography in color conversion," *IEEE Trans. Circ. Syst. II: Express Briefs*, vol. 71, no. 1, pp. 106–110, Aug. 2023. doi: 10.1109/TCSII.2023.3300330.

[40] Q. Li *et al.*, "Concealed attack for robust watermarking based on generative model and perceptual loss," *IEEE Trans. Circ. Syst. Video Technol.*, vol. 32, no. 8, pp. 5695–5706, Dec. 2021. doi: 10.1109/TCSVT.2021.3138795.

[41] A. Suresh and R. Balasubramanian, "A systematic review on spatial domain steganography & cryptography techniques," *Turk. Online J. Qual. Inq.*, vol. 12, no. 6, pp. 5108–5123, Jul. 2021.
[42] S. Singh, "Adaptive PVD and LSB-based high-capacity data hiding scheme," *Multimed. Tools Appl.*, vol. 79, no. 25, pp. 18815–18837, Jul. 2020.
[43] M. Y. Nejad, M. Mosleh, and S. R. Heikalabad, "An LSB-based quantum audio watermarking using MSB as arbiter," *Int. J. Theor. Phys.*, vol. 58, no. 11, pp. 3828–3851, Nov. 2019. doi: 10.1007/s10773-019-04251-z.
[44] E. Z. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and M. K. Sarker, "LSB-based bit flipping methods for color image steganography," *J. Phys.: Conf. Series, Yogyakarta*, Indonesia, vol. 1501, no. 1, pp. 12019, Mar. 2020. doi: 10.1088/1742-6596/1501/1/012019.
[45] A. Chatterjee, S. K. Ghosal, and R. Sarkar, "LSB-based steganography with OCR: An intelligent amalgamation," *Multimed. Tools Appl.*, vol. 79, no. 17, pp. 11747–11765, May 2020. doi: 10.1007/s11042-019-08472-6.
[46] F. A. Rafrastara, R. Prahasiwi, E. H. Rachmawanto, and C. A. Sari, "Image steganography using inverted LSB based on 2nd, 3rd, and 4th LSB patterns," presented at the 2019 Int. Conf. Inform. Commun. Technol., Yogyakarta, Indonesia, Jul. 2019, pp. 179–184.
[47] V. Moorthy and R. Venkataraman, "Generative adversarial analysis using U-LSB-based audio steganography," presented at the 2021 IEEE 18th India Council Int. Conf., Guwahati, India, Dec. 2021, pp. 1–6. doi: 10.1109/INDICON52576.2021.9691515.
[48] A. Kumar, "A review of the implementation of digital image watermarking techniques using LSB and DWT," *Inform. Commun. Technol. Sustain. Dev.*, vol. 933, pp. 595–602, Jun. 2020. doi: 10.1007/978-981-13-7166-0_59.
[49] M. Y. Nejad, M. Mosleh, and S. R. Heikalabad, "An enhanced LSB-based quantum audio watermarking scheme for nano communication networks," *Multimed. Tools Appl.*, vol. 79, no. 35, pp. 26489–26515, Sep. 2020. doi: 10.1007/s11042-020-09326-2.
[50] P. Ganwani, L. Gupta, C. Jain, R. Kulkarni, and S. Chaudhari, "LSB-based audio steganography using RSA and ChaCha20 encryption," presented at the 2021 12th Int. Conf. Comput. Commun. Netw. Technol., Kharagpur, India, Jul. 2021, pp. 1–6. doi: 10.1109/ICCCNT51525.2021.9580177.
[51] O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," presented at the 2020 IEEE Int. Conf. Inform., IoT, Enabling Technol., Doha, Qatar, Feb. 2020, pp. 131–135. doi: 10.1109/ICIoT48696.2020.9089566.
[52] P. Kanojia and V. Choudhary, "LSB-based image steganography with the aid of a secret key enhances its capacity by reducing bit string length," presented at the 2019 3rd Int. Conf. Electron., Commun. Aerospace Technol., Coimbatore, India, Jun. 2019, pp. 257–262. doi: 10.1109/ICECA.2019.8821917.
[53] M. S. H. Talukder, M. N. Hasan, R. I. Sultan, M. Rahman, A. K. Sarkar and S. Akter, "An enhanced method for encrypting image and text data simultaneously using AES algorithm and LSB-based steganography," presented at the 2022 Int. Conf. Adv. Electric. Electron. Eng., Gazipur, Bangladesh, Feb. 2022, pp. 1–5. doi: 10.1109/ICAEEE54957.2022.9836589.
[54] H. A. Mohammed and N. F. H. Al Saffar, "LSB-based image steganography using McEliece cryptosystem," *Mat. Today: Proc.*, Jul. 2021. doi: 10.1016/j.matpr.2021.07.182.
[55] F. Huma, M. Jahan, I. B. Rashid, and M. A. Yousuf, "Wavelet and LSB-based encrypted watermarking approach to hiding patient information in medical images," presented at the Proc. Int. Joint Conf. Adv. Comput. Intell., Singapore, Springer, May 2021, pp. 89–104. doi: 10.1007/978-981-16-0586-4_8.
[56] P. V. H. Prasad and K. G. Rao, "A new secure LSB-based image steganographical approach for secure data in cloud environment," *Int. J. Mod. Trends Sci. Technolo.*, vol. 8, no. 4, pp. 458–465, 2022. doi: 10.46501/IJMTST0804077.
[57] O. C. Abikoye, R. Oluwaseun Ogundokun, S. Misra, and A. Agrawal, "Analytical study on LSB-based image steganography approach," presented at the Comput. Intell. Mach. Learn., Singapore, Springer, Mar. 2022, pp. 451–457. doi: 10.1007/978-981-16-8484-5_43.

[58] A. D. Molato, F. B. Calanda, A. M. Sison, and R. P. Medina, "LSB-based random embedding image steganography technique using modified collatz conjecture," presented at the 2022 7th Int. Conf. Signal Image Process., Suzhou, China, Jul. 2022, pp. 367–371. doi: 10.1109/ICSIP55141.2022.9886754.

[59] M. A. Hameed, M. Hassaballah, S. Aly, and A. I. Awad, "An adaptive image steganography method based on the histogram of oriented gradient and PVD-LSB techniques," *IEEE Access*, vol. 7, pp. 185189–185204, Dec. 2019. doi: 10.1109/ACCESS.2019.2960254.

[60] L. Wang *et al.*, "Research on LSB-based digital image information camouflage algorithm," presented at the 2020 IEEE Int. Conf. Adv. Electric. Eng. Comput. Appl., Dalian, China, Aug. 2020, pp. 933–938. doi: 10.1109/AEECA49918.2020.9213706.

[61] S. T. Alam, N. Jahan, and M. M. Hassan, "A new 8-directional pixel selection technique of LSB based image steganography," presented at the Cyber Secur. Comput. Sci.: Second EAI Int. Conf., ICONCS 2020, Dhaka, Bangladesh, Feb. 15–16, 2020. doi: 10.1007/978-3-030-52856-0_8.

[62] D. R. Somwanshi and V. T. Humbe, "A secure and verifiable color visual cryptography scheme with LSB-based image steganography," *Int. J.*, vol. 10, no. 4, pp. 2669–2677, Aug. 2021. doi: 10.30534/ijatcse/2021/031042021.

[63] S. Zheng, X. Liu, R. Chen, S. M. Yuan, and C. C. Lin, "LSB-based visual image encryption scheme in a cloud environment," presented at the 2019 IEEE Intl Conf. Parallel & Distrib. Process. with Appl., Big Data & Cloud Comput., Sustain. Comput. & Commun., Soc. Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom), Xiamen, China, Dec. 2019, pp. 891–896. doi: 10.1109/ISPA-BDCloud-SustainCom–SocialCom48970.2019.00161.

[64] M. Fateh, M. Rezvani, and Y. Irani, "A new method of coding for steganography based on LSB matching was revisited," *Secur. Commun. Netw.*, vol. 2021, pp. 1–15, Feb. 2021. doi: 10.1155/2021/6610678.

[65] A. Gutub and F. Al-Shaarani, "Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons," *Arab. J. Sci. Eng.*, vol. 45, no. 4, pp. 2631–2644, Apr. 2020. doi: 10.1007/s13369-020-04413-w.

[66] M. A. Aslam *et al.*, "Image steganography using Least Significant Bit (LSB)—A systematic literature review," presented at the 2022 2nd Int. Conf. Comput. Inform. Technol., Tabuk, Saudi Arabia, Jan. 2022, pp. 32–38. doi: 10.1109/ICCIT52419.2022.9711628.

[67] K. Patani and D. Rathod, "Advanced 3-Bit LSB based on data hiding using steganography," *Data Sci. Intell. Appl.*, vol. 52, pp. 383–390, Jun. 2020. doi: 10.1007/978-981-15-4474-3_42.

[68] R. Dumre and A. Dave, "Exploring LSB steganography possibilities in RGB images," presented at the 2021 12th Int. Conf. Comput. Commun. Netw. Technol., Kharagpur, India, Jul. 2021, pp. 1–7. doi: 10.1109/ICCCNT51525.2021.9579588.

[69] A. Gupta, A. Ali, A. K. Pandey, A. K. Gupta, and A. Tripathi, "Metamorphic cryptography using AES and LSB method," presented at the 2022 Int. Conf. Adv. Comput., Commun. Mat., Dehradun, India, Nov. 2022, pp. 1–8. doi: 10.1109/ICACCM56405.2022.10009381.

[70] D. Kaur, H. K. Verma, and R. K. Singh, "Image steganography: Hiding secrets in random LSB pixels," presented at the Soft Comput.: Theories Appl., Singapore, Springer, Feb. 2020, pp. 331–341. doi: 10.1007/978-981-15-0751-9_31.

[71] K. Tiwari and S. J. Gangurde, "LSB steganography using pixel locator sequence with AES," presented at the 2021 2nd Int. Conf. Secur. Cyber Comput. Commun., Jalandhar, India, May 2021, pp. 302–307. doi: 10.1109/ICSCCC51823.2021.9478162.

[72] M. Hussain, Q. Riaz, S. Saleem, A. Ghafoor, and K. H. Jung, "Enhanced adaptive data hiding method using LSB and pixel value differencing," *Multimed. Tools Appl.*, vol. 80, no. 13, pp. 20381–20401, May 2021. doi: 10.1007/s11042-021-10652-2.

[73] O. Rachael, S. Misra, R. Ahuja, A. Adewumi, F. Ayeni and R. Mmaskeliunas, "Image steganography and steganalysis based on Least Significant Bit (LSB)," in *Proc. ICETIT 2019*, Sep. 2020, pp. 1100–1111. doi: 10.1007/978-3-030-30577-2_97.

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

[75] G. Luo, R. G. Zhou, J. Luo, W. Hu, Y. Zhou and H. Ian, "Adaptive LSB quantum watermarking method using tri-way pixel value differencing," *Quantum Inform. Process.*, vol. 18, no. 2, pp. 1–20, Feb. 2019. doi: 10.1007/s11128-018-2165-6.

[76] R. Shanthakumari, E. R. Devi, R. Rajadevi, and B. Bharaneeshwar, "Information hiding in audio steganography using LSB matching revisited," presented at the J. Phys.: Conf. Series, Chennai, India, May 2021, vol. 1911, pp. 12027. 10.1088/1742-6596/1911/1/012027.

[77] A. Nolkha, S. Kumar, and V. S. Dhaka, "Image steganography using LSB substitution: A comparative analysis on different color models," *Smart Innov. Syst. Technol.*, vol. 141, pp. 711–718, Oct. 2019. doi: 10.1007/978-981-13-8406-6_67.

[78] Y. Wang, M. Tang, and Z. Wang, "High-capacity adaptive steganography based on LSB and Hamming code," *Optik*, vol. 213, pp. 164685, Jul. 2020. doi: 10.1016/j.ijleo.2020.164685.

[79] D. N. Tran, H. J. Zepernick, and T. M. C. Chu, "On LSB data hiding in high-definition images using morphological operations," presented at the 2019 19th Int. Symp. Commun. Inform. Technol., Ho Chi Minh City, Vietnam, Sep. 2019, pp. 386–391. doi: 10.1109/ISCIT.2019.8905158.

[80] S. E. Ghrare, A. A. M. Alamari, and H. A. Emhemed, "Digital image watermarking method based on LSB and DWT hybrid technique," presented at the 2022 IEEE 2nd Int. Maghreb Meeting Conf. Sci. Tech. Automatic Control Comput. Eng., Sabratha, Libya, May 2022, pp. 465–470. doi: 10.1109/MI-STA54861.2022.9837586.

[81] P. R. Budumuru, G. P. Kumar, and B. E. Raju, "Hiding an image in an audio file using LSB audio technique," presented at the 2021 Int. Conf. Comput. Commun. Inform., Sabratha, Libya, Jan. 2021, pp. 1–4. doi: 10.1109/MI-STA54861.2022.9837586.

[82] A. Sondas and H. Kurnaz, "H NMH: A new hybrid approach based on near maximum histogram and LSB technique for image steganography," *Wirel. Pers. Commun.*, vol. 126, no. 3, pp. 2579–2595, Oct. 2022. doi: 10.1007/s11277-022-09830-8.

[83] A. G. Chefranov and G. Öz, "Adaptive to pixel value and pixel value difference irreversible spatial data hiding method using modified LSB for grayscale images," *J. Inform. Secur. Appl.*, vol. 70, pp. 103314, Nov. 2022. doi: 10.1016/j.jisa.2022.103314.

[84] K. Praghash, C. Vidyadhari, G. NirmalaPriya, and R. Cristin, "Secure information hiding using LSB features in an image," *Materials Today: Proc.*, vol. 335, pp. 299, Jan. 2021. doi: 10.1016/j.matpr.2020.11.362.

[85] D. Laishram, T. Tuithung, and T. Jeneetaa, "Fuzzy edge image steganography using hybrid LSB method," presented at the Internet of Things Connected Technol.: Conf. Proc. 5th Int. Conf. Internet of Things Connected Technol., Cham, Springer, May 2021, pp. 249–258. doi: 10.1007/978-3-030-76736-5_23.

[86] T. Ejidokun, O. O. Omitola, I. Nnamah, and K. Adeniji, "Implementation and comparative analysis of variants of LSB steganographic method," presented at the 2022 30th Southern Afr. Univ. Power Eng. Conf., Durban, South Africa, Jan. 2022, pp. 1–4. doi: 10.1109/SAUPEC55179.2022.9730643.

[87] Z. Phyo and E. C. Htoon, "Text-based shuffling algorithm in digital watermarking," presented at the 2019 Int. Conf. Adv. Inform. Technol., Yangon, Myanmar, Nov. 2019, pp. 183–187. doi: 10.1109/AITC.2019.8921222.

[88] P. C. Mandal, I. Mukherjee, and B. N. Chatterji, "High capacity steganography based on IWT using eight-way CVD and n-LSB ensuring secure communication," *Optik*, vol. 247, pp. 167804, Dec. 2021. doi: 10.1016/j.ijleo.2021.167804.

[89] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," *Optics Lasers Eng.*, vol. 121, pp. 169–180, Oct. 2019. doi: 10.1016/j.optlaseng.2019.03.006.

[90] G. K. Soni, H. Arora, and B. Jain, "A novel image encryption technique using Arnold transform and asymmetric RSA algorithm," presented at the Int. Conf. Artif. Intell.: Adv. Appl. 2019, Singapore, Springer, 2020, pp. 83–90. doi: 10.1007/978-981-15-1059-5_10.

[91] K. Jiao, G. Ye, Y. Dong, X. Huang, and J. He, "Image encryption scheme based on a generalized Arnold map and RSA algorithm," *Secur. Commun. Netw.*, vol. 2020, pp. 1–14, Jun. 2020. doi: 10.1155/2020/9721675.

[92] B. B. Sundaram, N. K. Raja, N. Sreenivas, M. K. Mishra, B. Pattanaik and P. Karthika, "RSA algorithm using performance analysis of steganography techniques in network security," presented at the Int. Conf. Commun., Comput. Electron. Syst., Singapore, Springer, Mar. 2021, pp. 713–719. doi: 10.1007/978-981-33-4909-4_56.

[93] Y. Xu, S. Wu, M. Wang, and Y. Zou, "Design and implementation of distributed RSA algorithm based on Hadoop," *J. Ambient Intell. Hum. Comput.*, vol. 11, no. 3, pp. 1047–1053, Mar. 2020. doi: 10.1007/s12652-018-1021-y.

[94] R. Lin and S. Li, "An image encryption scheme based on Lorenz Hyperchaotic system and RSA algorithm," *Secur. Commun. Netw.*, vol. 2021, pp. 1–18, Jan. 2021. doi: 10.1155/2021/5586959.

[95] Q. Xu, K. Sun, and C. Zhu, "A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map," *Phys. Scr.*, vol. 95, no. 3, pp. 35223, Feb. 2020. doi: 10.1088/1402-4896/ab52bc.

[96] S. K. Salim, M. M. Msallam, and H. I. Olewi, "Hide text in an image using the Blowfish algorithm and development of the least significant bit technique," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 29, no. 1, pp. 339–347, Jan. 2023. doi: 10.11591/ijeecs.v29.i1.pp339-347.

[97] S. Ilasariya, P. Patel, V. Patel, and S. Gharat, "Image steganography using blowfish algorithm and transmission via Apache Kafka," presented at the 2022 4th Int. Conf. Smart Syst. Inventive Technol., Tirunelveli, India, Jan. 2022, pp. 1320–1325. doi: 10.1109/ICSSIT53264.2022.9716292.

[98] N. K. Murthy, S. Sharma, M. J. P. Priyadarsini, R. Ranjan, S. Sarkar and N. S. Basha, "Image steganography using discrete cosine transform algorithm for medical images," in *Advances in Automation, Signal Processing, Instrumentation, and Control*, Singapore: Springer, Mar. 2021, pp. 2349–2358. 10.1007/978-981-15-8221-9_219.

[99] A. Lius, I. A. Pardosi, and H. Gohzali, "Implementation of discrete cosine transform and permutation-substitution scheme based on Henon Chaotic map for images," presented at the 2022 Seventh Int. Conf. Inform. Comput., Denpasar, Bali, Indonesia, Dec. 2022, pp. 1–5. doi: 10.1109/ICIC56845.2022.10007027.

[100] Z. Shao, X. Wang, Y. Tang, and Y. Shang, "Trinion discrete cosine transforms with application to color image encryption," *Multimed. Tools Appl.*, vol. 82, no. 10, pp. 1–27, Apr. 2022. doi: 10.1007/s11042-022-13898-6.

[101] J. B. de Medina Arribas, "Decisive image characteristics to perform image steganography in DCT," Bachelor's thesis, Univ. of Twente, Netherlands, 2022.