Electrical Engineering Technical Journal

Journal homepage*: http://eetj.mtu.edu.iq*

RESEARCH ARTICLE

A Survey on Steganography and Image Encryption Techniques

Noor Dheyaa Majeed [1], Ali J. Al-Askery [1, 2*], Fadhil Sahib Hasan [3] and Samir Abood [4]

[1] Electrical Engineering Technical College, Middle Technical University, Baghdad, Iraq
[2] School of Engineering, Newcastle University, Newcastle, UK
[3] College of Engineering, Mustansiriyah University, Baghdad, Iraq
[4] Electrical and Computer Engineering Department, Prairie View A&M University, Texas, USA

[*] Corresponding Author Email: a.al-askery@newcastle.ac.uk

Article Info.

Article history:

Received
13 September 2024

Accepted
2 November 2024

Published in Journal
31 January 2025

Abstract

Modern internet technologies have led to an increase in the transmission and receiving of information across the network, especially images that may contain confidential information, so it has become necessary to increase protection for these images. The processes of protecting information during the transmission are scientifically divided into encryption and hiding techniques. Encryption techniques change the secret data content to become unclear for professional hackers. On the contrary, steganography saves the same content of secret data but inserts it into the medium cover without clearly showing any change in the medium. These covers, such as text, images, or video, whereas images and video are more efficient than other covers because they have powerful and complex structures to achieve more security. The combination of hybrid encryption and steganography gives more multi-level security protection, which is hardly predictable against intruders. This work analyzes the challenges that researchers may face in this field, in addition to discussing the latest technologies proposed. Besides that, the evaluation parameters of these techniques are summarized.

Publisher: Middle Technical University

Keywords: Security; Encryption image; Steganography; Development and challenges; Evaluation parameters.

1. Introduction

The demand for information security techniques is on the rise because of the increased volume of data communication via the Internet. Steganography techniques can be employed to transmit secret messages with a cover medium; these covers can be text, image, or video, thereby accurately obscuring the communication of the secret message to any unintended party. There are three important parameters to evaluate steganography: capacity, which is the amount of confidential data contained within the medium; and imperceptibility, which means the data is inserted in cover without affecting medium quality. Finally, robustness against hackers [1]. The process of embedding confidential data within the medium is divided into two types. Initially, the spatial domain, which means the embedding operation is directly applied in pixels, where this operation is simple and fast but easily penetrated, such as Least Significant Bits (LSB) and Pixel Value Differencing (PVD). Secondly, frequency domains, which means the embedding operation converts the pixels into frequency domains such as Discrete Wave Transform (DWT) and Discrete Cosine Transform (DCT). On the other hand, the encryption concept means changing the original secret data into incomprehensible data for a third party using a key to achieve a high-security level [2]. There are diverse types of encryption algorithms, such as Advance Encryption Standard (AES) and Data Encryption Standard (DES). However, these algorithms are unsuitable for images because the images have high redundancy and correlation coefficients. So, most image encryption algorithms use chaotic systems. These chaotic generate Pseudo Random Number Generators (PRNG), which are used in image encryption to increase confusion and diffusion operations [3]. Figure 1 shows the classification of secure data.

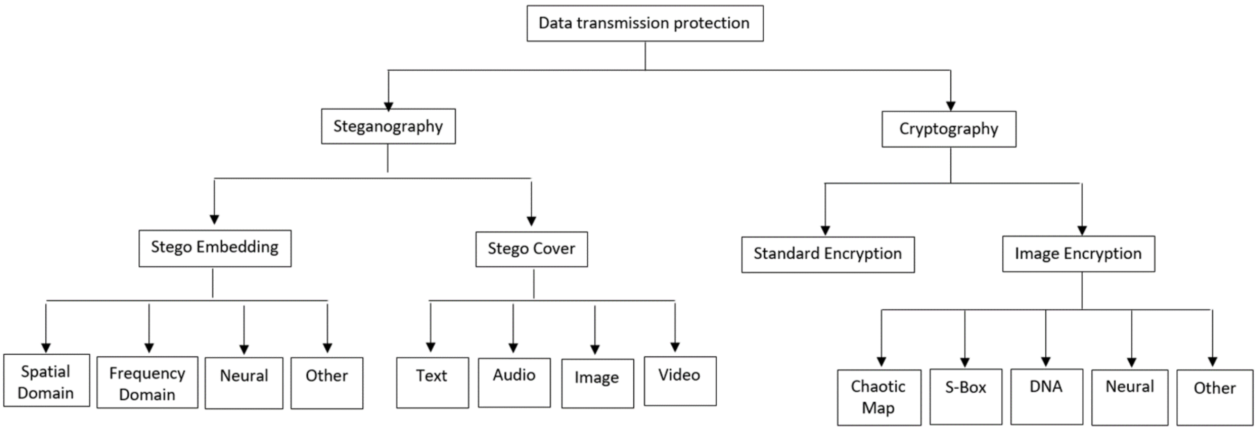


Fig. 1. Classification of transmitted data protection.

The hybrid encryption-steganography design gives a double layer of security. So, this paper presents the techniques connected with this topic, whereas the main contributions in this work are:

- We discuss the strengths and weaknesses of the most recent research in this area.
- We provide a summary of the standards used to evaluate the quality of encryption and concealing techniques.
- Provide recommendations for future solutions to the current problems in this field.

The subsequent sections of the paper are structured in the following manner. Section 2 comprises the literature survey. The evaluation parameters are discussed in Section 3. Section 4 includes the areas for future investigation. The paper's conclusion is presented in Section 5.

2. Literature Survey of Image Encryption

There are a variety of encryption image methods, such as encryption based on chaotic maps, Deoxyribonucleic Acid (DNA), Neural Networks, and the Substitution box. This work discusses the latest previous works for the years (2019-2024) for image encryption.

2.1. Image Encryption Based on Chaotic Maps

Chaotic theory belongs to a nonlinear system since it can be categorized into two essential types: discrete and continuous chaotic [4]. Discrete chaotic systems are dynamical systems with discrete times that are produced by iterative equations. Also, the systems controlled by differential equations are called dynamical systems with continuous time [5]. Discrete chaos is distinguished by its simple structure and easy implementation. However, it is slightly random for security reasons. In contrast, continuous chaos has a more complex structure but is more secure. On the other hand, the chaotic system can be divided into one-dimensional and many-dimensional according to the variables in the chaotic equation. Likewise, the one-dimensional has a narrow range of randomness, but it is fast in implementation. Conversely, more dimensional, which has a wide range of chaos but has more time running [6]. The equations for chaotic maps consist of two essential parameters: the initial condition and the control parameters. The initial seed, which is a secret number known only by the sender and receiver, plays a crucial role in generating a secret key. While the control parameters act as the initial condition to become the system choice and begin the bifurcation round, hence the increase in the bifurcation in chaotic maps increases the key space, so increases the security. Various methods are available for evaluating chaotic work, including randomness tests and Lypanov checks [2]. Figure 2 shows the types of chaos. While traditional encryption is unsuitable for images due to their high redundancy and correlation coefficients, most image encryption research applies chaotic maps. The chaotic maps intensify the process of confusion and diffusion, with the confusion stage frantically searching for bits or pixels to enhance security against hackers. Moreover, the diffusion stage leads to the replacement of bits or pixels in images, disrupting any relationship with the original secure image [3]. In 2019, Wang et al. [7] suggested two rounds of image encryption where the first round is divided by the bits of the image and re-distributed by a random method. In 2019, Khan and Ahmad [8] suggested an image encryption technique with various steps. First partitions the plaintext picture into multiple blocks and subsequently computes the correlation coefficients for each block. The block containing the highest correlation coefficient values is combined with the random numbers generated from a skew tent map using a predetermined threshold value through a pixel-wise XOR operation. Finally, the entire image is rearranged using two random sequences created from the TD-ERCS chaotic map. In 2019, Gan et al. [9] proposed an algorithm that begins by converting the color plain image into 24-bit planes through RGB splitting and bit-plane decomposition. The position sequences for the permutation are derived from the 3D Chen chaotic system, resulting in three confused components. In 2019, Arab et al. [10] introduced an image encryption technique that combines a chaotic sequence with a modified AES algorithm. The encryption key is derived from the Arnold chaos sequence in this approach. Next, the original image is encrypted using the modified AES method, and the chaos system generates the round keys.

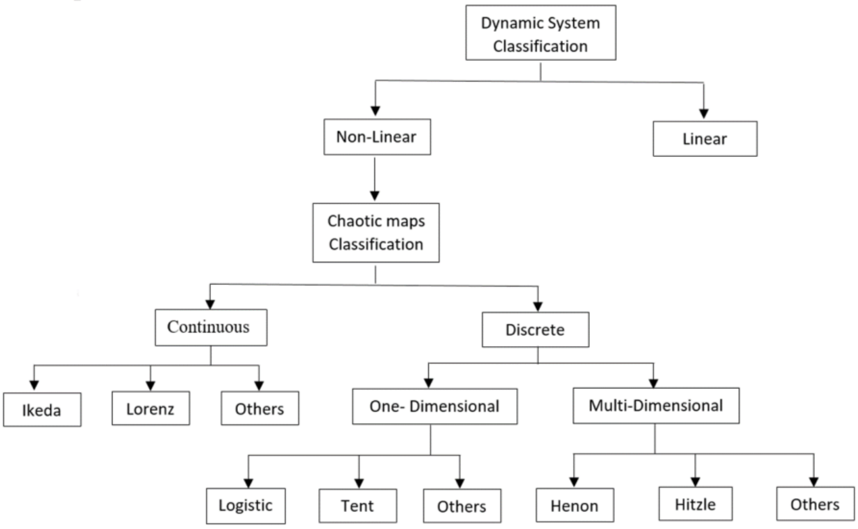


Fig. 2. Classification of chaotic types.

In 2020, Hasan and Safo [11] presented an image encryption design consisting of two rounds inspired by various forms of chaos. The design was performed using the SP605 XC6SLX45T FPGA device. The primary limitation associated with their work pertains to the sequential processing of images, performed bit by bit in a unidirectional flow arrangement, resulting in a sluggish processing pace. In 2020, Tao Li et al. [12] proposed an image encryption technique that utilizes two-dimensional Lorenz and Logistic Systems principles. The encryption tests conducted on many iconic photos demonstrate that the technique possesses high security and exceptional resilience. In 2020, Kaur et al. [13] suggested image encryption based on employing two PWLCMs to produce numerous transform orders in each dimension. The fractional Fourier transform is computed using the produced multiple-order vectors. In 2021, Gao [14] offered a new 2D hyperchaotic map constructed using two 1D-chaotic maps, a linear function, and a multiplier. The encryption algorithm utilizes a 2D hyperchaotic map to scramble the image using row and column shifts. In 2022, Wen et al. [15] introduced a novel picture encryption algorithm that utilizes the 2D-Logistic-adjusted-Sine map (2D-LASM) and Discrete Wavelet Transform (DWT). Initially, a dynamic key is generated using the Message-Digest (MD5), which correlates with plaintext. Subsequently, 2D-LASM chaos is generated based on this key. In 2023, Lai and Liu [16] proposed image encryption that utilizes a two-dimensional hyperchaotic map (2D-SFHM) developed from the Sine map and mathematical function to achieve high sensitivity in cross-channel color picture encryption. A novel cross-channel color picture encryption algorithm is introduced, which incorporates the peripheral-pixel extension technique. This algorithm utilizes circular-shift permutation and bidirectional-parallel diffusion to achieve robust confusion and diffusion qualities. In 2023, Wen et al. [17] presented a novel color image compression-encryption method that utilizes chaos and block permutation to achieve superior quality. In this approach, the color digital image is initially transformed and sampled in the YCbCr color space. Then, the coefficients in the sub-blocks are extracted for compression coding. This extraction is done after performing an 8×8 post-blocking discrete cosine transformation (DCT) to transfer the image to the frequency domain. In 2023, Shakir et al. [18] presented a technique for electronically encrypting and decrypting images using the Lorenz chaotic system. The algorithm was constructed based on the three equations of the Lorenz system. Before that, the image pixels undergo reversible shifting and rotating operations to enhance the randomness of the encrypted pixels and consequently increase the complexity of deciphering the code. However, the structure of the encryption design is simple. In 2024, Toktas et al. [19] introduced a unique chaotic system for Image Encryption (IME), which relies on the Bessel function and a Bessel map. This system also incorporates a novel Bessel map-based IME technique. The Bessel map possesses three control parameters that contribute to its exceptional ergodicity and diversity. The Bessel map has a higher degree of order than the sine map, which is utilized as a control parameter to enhance security.In 2024, Patel et al. [20] introduced a novel two-dimensional triangle function in combination with a discrete chaotic map (2D-TFCDM). The proposed map, in conjunction with the Secure Hash Algorithm (SHA), is employed in picture cryptography applications. Table 1 is a summary of the previous work.

Table 1. Summary of image encryption based on chaotic.

Authors & Year	Objective	Results	Limitations
Wang et al. 2019 [7]	Increasing security	Entropy=7.9993	Two rounds only, so it is low security.
Khan & Ahmad 2019 [8]	Increasing security	Key Space= 2^{299}	Low Key Space
Gan et al. 2019 [9]	Increasing security	Key Space= 2^{318}	Low Key Space
Arab et al. 2019 [10]	Increasing security	Entropy=7.8693	Only one type of 1D-chaos is used, so it is low-security
Hassan & Saffo 2020 [11]	Increasing security	Entropy=7.9973	Only two rounds Stream of bit-by-bit processing so it is slow in encryption operation
Tao Li et al. 2020 [12]	Increasing security	Entropy=7.9894	Only one operation of permutation

Kaur et al. 2020 [13]	Increasing security	PSNR= 9.0095
		MSE=8168.4
			Two stages of substation and scrambling

Gao 2021 [14]	Increasing security	Entropy=7.9973	Simple design, so it is a low-security

Wen et al. 2022 [15]	Increasing security	Key Space=2^{327}
		PSNR=25.6436
		MSE=177.3049
			Low Key Space

Lai and Liu 2023 [16]	Increasing security	MSE=9784.47
		PSNR=8.22543
			Only two stages

Wen et al. 2023 [17]	Increasing security	Entropy=7.9985
		PSNR=43.7469
		Key Space=2^{234}
			Low Key Space

Shakir et al. 2023 [18]	Increasing security	Entropy=7.9974	Simple design
Toktas et al. 2024 [19]	Increasing security	Entropy=7.9994	Simple structure
Patel et al. 2024 [20]	Increasing security	Entropy=7.9989	Low entropy

2.2. Image Encryption Based on S-box

The S-box is a crucial non-linear component utilized in substitution-permutation stages. The S-box generally transforms a given collection of input bits, x, into a corresponding set of output bits, y, without necessarily preserving the same values as x. The S-box can be implemented as a y-bit lookup table [21]. The S-boxes can be categorized into three distinct groups. First, the straight S-box has identical dimensions for both the input and the output. An example of such an S-box is the widely recognized AES. This arrangement is the most fundamental and standard configuration of an S-box. Second, compressed S-box: This refers to an S-box in which the size of the input is more than the size of the output. The Data Encryption Standard (DES) is a prime illustration of an S-box that operates by accepting a 6-bit input and producing a 4-bit output for each block. Finally, the expanded substitution box: This substitution box accepts a reduced number of input bits and generates a greater number of output bits [22]. Recent research has combined the S-box with chaotic maps to enhance security, using PRNG as the index to distribute bits within the S-box through a sorting process. Figure 3 illustrates the three types of chaotic maps, while Figure 4 delineates the S-box operation.

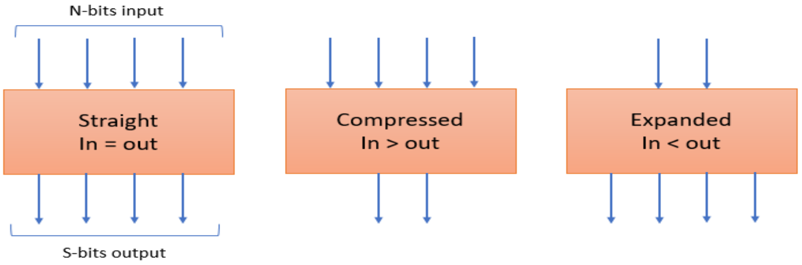
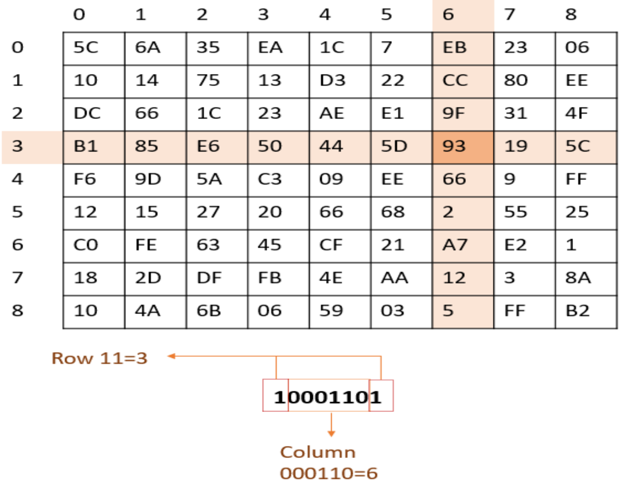


Fig.3. Types of S-box**.**



	0	1	2	3	4	5	6	7	8
0	5C	6A	35	EA	1C	7	EB	23	06
1	10	14	75	13	D3	22	CC	80	EE
2	DC	66	1C	23	AE	E1	9F	31	4F
3	B1	85	E6	50	44	5D	93	19	5C
4	F6	9D	5A	C3	09	EE	66	9	FF
5	12	15	27	20	66	68	2	55	25
6	C0	FE	63	45	CF	21	A7	E2	1
7	18	2D	DF	FB	4E	AA	12	3	8A
8	10	4A	6B	06	59	03	5	FF	B2

Fig. 4. S-box operation.

In 2019, Khan et al. [23] presented an image encryption design with a new approach to create a replacement box or Boolean function for block ciphers. This method involves utilizing Gaussian distribution and linear fractional transformation. In 2020, Liu Lidong et al. [24] proposed a novel encryption design that can be categorized into three distinct stages: combining, scrambling, and dissemination. During the combination stage, the image compressing technique is used to compress three plain images. Next, the three compressed images are merged using a stochastic matrix produced by a two-dimensional chaotic system. During the scrambling phase, a new and efficient scrambling method called coded lock scrambling is introduced with the aim of enhancing the speed of processing. In the last phase, the output incorporates a non-linear element known as an S-box, for which we provide the pseudo-code. In 2020, Qing Lu et al. [25] introduced a highly effective and safe image encryption technique that utilizes a chaotic S-Box. The suggested scheme introduces a unique discrete compound chaotic system called the Logistic-Sine system (LSS), which exhibits a broader chaotic range and superior chaotic features. In 2020, Ibrahim and Alharbi [26] presented an efficient algorithm for constructing secure dynamic S-boxes derived from the Henon map. The hash also serves as an image-dependent initialization for the key stream which together with using an image-dependent S-box resists known plaintext attack. In 2021, Talhaoui and Wang [27] suggested an image encryption design based on a new 1D-chaotic by nonlinear iterative function and then used to integrate the substitution and permutation steps to concurrently alter the positions and values of both pixels. In 2022, Tahir and Rashid [28] suggested a method to encrypt the image by utilizing a chaotic system derived from the piecewise linear chaotic map. This chaotic system was used to construct an S-box with a high level of non-linearity. In 2022, Arif et al. [29] proposed an image encryption approach utilizing chaos theory, specifically permutation and substitution techniques, with the inclusion of a single Substitution Box to resolve challenges encountered in current image encryption algorithms. In 2022, Ali et al. [30] suggested a method that involves encrypting images using the Carlisle Adams and Stafford Tavares CAST block cipher algorithm, along with 3D and 2D logistic maps. An incorporated chaotic function enhances the randomness in encrypted data and images, thereby disrupting the sequential relationship throughout the encryption process. In addition, the CAST encryption method was adapted to operate on the private keys and substitution stage. In 2024, Essabry et al. [31] Propose an enhanced method for encrypting 32-bit color images by utilizing the capabilities of four 1D chaotic maps - the Logistic map, Tent map, Chebyshev map, and Sine map. The chaotic maps intricately fill the four matrices in our encryption system, assigning unique integers from 0 to 255. The system suggested 16 x 16 matrices to symbolize the four channels (red, green, blue, and alpha) in a 32-bit color image. In 2024, Ibrahim et al. [32] developed a robust encryption algorithm to enhance the efficiency of encrypting 12-bit medical photos. The core component of the suggested technique is a 12 × 12 S-box that is dependent on the encryption key. This S-box is essential for improving both the security and efficiency of the encryption scheme. In 2024, Ustun et al. [33] presented a new S-Box designed specifically to meet high security requirements. This was accomplished by using real-coded genetic algorithms to iteratively apply crossover and mutation operators, resulting in a strong image encryption method. Table 2 is a summary of the previous work.

Table 2. Summary of image encryption based on S-box.

Authors & Year	Objective	Results	Limitations

Khan et al. 2019 [23]	Increasing security	NPCR= 99.84
		UACI= 33.45
			Single Rounds only, so it is a low security

Lidong et al. 2020 [24]	Increasing security	Key Space= 2^{561}	Exhausting Computation
Lu et al. 2020 [25]	Increasing security	Entropy=7.9971	Simple design, so it is a low security
Ibrahem et al. 2020 [26]	Increasing security	Entropy=7.9994	The authors didn’t mention any details for ECC
Talhaoui and Wang 2021 [27]	Increasing security	Entropy=7.9029	Only one round of permutation and S-box

Tahir and Rashid 2022 [28]	Increasing security	MSE=392.49
		PSNR=22.2370
			Simple design, so it is a low security

Arif et al. 2022 [29]	Increasing security	Entropy=7.9969	Simple design, so it is a low security
Ali et al. 2022 [30]	Increasing security	Entropy=7.991	Simple design, so it is a low security
Es-Sabry et al. 2024 [31]	Increasing security	Entropy=7.9974	Simple design, so it is a low security
Ibrahim et al. 2024 [32]	Increasing security	CC=0.000779 =0.003016 =0.000136	Simple design, so it is a low security
Ustun et al. 2024 [33]	Increasing security	Entropy=7.9994	Simple design, so it is a low security

2.3. Image Encryption Based on DNA

Image encryption can utilize DNA encoding by transforming the binary values of the image's pixels into a DNA sequence. Researchers can utilize DNA coding rules to convert binary information into synthetic DNA sequences. This is possible because the DNA sequence is made up of four nucleotides: adenine (A), guanine (G), cytosine (C), and thymine (T). Specialized laboratory equipment is used to handle DNA synthesis and sequencing [34]. For instance, using Table 3 encoding rules, a pixel with a gray value of 180 in decimal can be represented by the quaternary number "3201" (or a binary sequence "11100001") and encoded to eight different types of DNA sequences: "TGAC", "TCAG", "AGTC," "ACTG", "GTCA", "GACT", "CTGA", and "CAGT".

Table 3. DNA rules.

Binary	1	2	3	4	5	6	7	8
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

In 2020, Zefreh [35] proposed a novel image encryption that integrates hash functions, chaotic systems, and DNA computing. 5D chaos was used in the design. On the other hand, the DNA permutation level is the random reorganization of the components' positions in the DNA image through a mapping effort that relies on the chaotic logistic map. In 2021, Iqbal et al. [36] developed a novel image encryption strategy by combining the chaotic system, DNA computing, and Castle, which is a chess piece. When the original image is provided as an input, its pixels are transferred to the scrambled image at randomly selected pixel locations. The process of scrambling was achieved by utilizing the Image Scrambler using the Castle (ISUC) algorithm. In 2022, Lone et al. [37] proposed a novel approach for encrypting images using DNA and the 3D Arnold chaos system. The method involves generating a key sequence that is altered by DNA rule and XOR operation with a DNA stream to achieve a high level of diffusion. In 2022, Jasra and Moon [38] developed an immune encryption and decryption technique using a DNA algorithm that relies on a hyperchaotic map and elliptic curve cryptography. This design incorporates an authenticated key that is generated and exchanged using a digital signature. In 2022, Alrubaie et al. [39] suggested a picture encryption technique built on a chaotic 2D logistic map with double-dynamic DNA sequence encryption. The three stages of the proposed method are as follows: in the first stage, a position key-based scrambling operation is used to permute the pixel positions. In 2023, Zhao et al. [40] proposed a revolutionary picture encryption technique utilizing a newly developed dynamic system, Zigzag transform, and DNA operation. The plain image is block-scrambled using an enhanced Zigzag transformation technique. The DNA is then encoded using 4D-chaotic sequences that have been processed. In 2024, Zhang et al. [41] proposed a system for encrypting double images that combines DNA, parallel compressed sensing, increased Zigzag confusion, chaotic sparse basis matrix, and chaotic permutation. To begin, employ the logistic map to perturb a Discrete Wavelet Transformation (DWT) matrix in order to acquire a chaotic DWT matrix. Table 4 is a summary of the previous work.

Table 4. Summary of image encryption based on DNA.

Authors & Year	Objective	Results	Limitations
Zefreh 2020 [35]	Increasing security	Entropy=7.9993	Exhausting Computation
Iqbal et al. 2021[36]	Increasing security	Entropy=7.90230	Exhausting Computation
Lone et al. 2022 [37]	Increasing security	Entropy=7.9976	Simple design
Jasra and Moon 2022 [38]	Increasing security	Entropy=7.9924	Simple design

Alrubaie et al. 2023 [39]	Increasing security	Entropy=7.9898
		MSE=3238.1500
		PSNR=13.0618
			Low Entropy

Zhao et al. 2023 [40]	Increasing security	Entropy=7.9916	Low Entropy
Zhang et al. 2024 [41]	Increasing security	PSNR=33.9745 Key Space=2^{279}	Low Key Space

2.4. Image Encryption Based on Neural Networks

Neural networks can be employed in picture encryption techniques to improve the security and effectiveness of the algorithm. Neural networks can rearrange and/or reduce the size of the original images. Moreover, neural networks exhibiting chaotic behaviors can be employed to produce chaotic sequences that serve as keys, input parameters, or to disperse the image. Neural techniques are adapted from the convolutional neural of the human brain by conditional training [42]. The field of image encryption using neural networks has attracted many researchers as the neural network is used to optimally scatter pixels. Various types of neural techniques, such as fuzzy, heuristic, genetic, particle swarm optimization algorithms, and convolutional neural networks, are used with image encryption. In 2021, Man et al. [43] proposed a double image encryption algorithm based on convolutional neural networks (CNN) and dynamic adaptive diffusion. First, a chaotic map is used to control the initial values of the 5D conservative chaotic system to enhance the security of the key. Second, in order to effectively resist known plaintext attacks and chosen-plaintext attacks, the proposal employs a chaotic sequence as the convolution kernel of a convolution neural network to generate a plaintext-related chaotic pointer to control the scrambling operation of two images, a chaotic pointer that is related to the plaintext, which is then used to regulate the scrambling operation of two images. In 2023, Feng et al. [44] described a technique that combines chaotic picture encryption with a convolutional neural network (CNN) to improve both security and performance. The approach utilizes the characteristics of randomness and nonlinear mapping of chaotic sequences, together with the sophisticated feature extraction capabilities of a CNN model, to generate strong picture encryption. Initially, we delineate the core principles of chaotic image encryption and convolutional neural networks. In 2024, Vijayakumar and Ahilan [45] presented a novel encryption technique that utilizes chaotic map Substitution boxes (S-box) and cellular automata (CA). In order to overcome the insufficient randomness generated by the 1D chaotic map, this study introduces a 4D memristive hyper-chaos that exhibits a wider chaotic range, enhanced uncertainty, and ergodicity. This serves as an alternative to the software-based solution, which is susceptible to vulnerabilities and has limited throughput. The proposed encryption method was executed on an Intel Cyclone IV EP4CE115F29C7 FPGA. In 2024, Kocak et al. [46] presented an image encryption system that utilizes key optimization through the Particle Swarm Optimization (PSO) algorithm and a novel modular integrated logistic exponential (MILE) map. The key is optimized for a specific portion of the image to be encrypted rather than the entire image used in previous research. Table 5 is a summary of the previous work.

Table 5. Summary of image encryption based on neural.

Authors & Year	Objective	Results	Limitations

Man et al. 2021 [43]	Increasing security	MSE=6988.5
		PSNR=9.6351
		Entropy=7.9981
			Exhausting Computation

Feng et al. 2023 [44]	Increasing security	PSNR=41.78	Most results didn't measure and the PSNR was high, so the encryption failed.
Vijayakumar & Ahilan 2024 [45]	Increasing security	Entropy=7.984 Key Space=2^{400}	The authors didn't mention any information about the device summary and the Entropy is low.
Kocak et al. 2024 [46]	Increasing security	Entropy=7.9994	Exhausting computation

3. Literature Survey of Steganography

This work discusses steganography techniques in Image and Video covers because these mediums are more efficient and capacity than others. The latest previous works for the years (2019-2024) are discussed for image and video steganography.

3.1. Image Steganography Based on the Spatial Domain

The term "spatial domain" pertains to the manipulation of pixel values or, in simpler terms, dealing directly with the unprocessed data. The spatial domain is defined as the direct manipulation of pixel intensity values within a frame. The most fundamental method for embedding in the spatial domain is the substitution of the least significant bit (LSB). The process of embedding the secret data bit in LSB involves substituting the least significant bits of cover, so numerous researchers have employed the technique of LSB substitution [47]. In 2019, Biswas et al. [48] suggested a method that involves concealing the message within the color image using Multi-bit Least Significant Bit (MLSB) steganography in the spatial domain. The path trace, determined by the eccentricity of pixels, identifies the pixels with the greatest potential for accommodating more hidden information. In 2019, Hameed et al. [49] Presented pixel value differencing (PVD) and least significant bit substitution (LSB) are commonly employed methods in image steganography. Each pixel in most digital photographs contains varying edge directions, and the local shape or appearance of an item is primarily determined by the distribution of its intensity gradients or edge directions. In 2021, AbdelRaouf [50] proposed an innovative technique for concealing data in images using adaptive Least Significant Bits (LSB) based on human visual characteristics. Two distinct approaches are utilized. Firstly, the human eye exhibits varying sensitivity to RGB color channels, allowing for a varied allocation of bits for each color channel. In 2021, Hussain et al. [51] proposed a novel image steganography technique that utilizes the pixel intensity ranges to achieve high embedding rates and ensures the complete recovery of secret data during the extraction phase. The suggested technique partitions the pixels into non-overlapping blocks and calculates the differences between the pixels as well as their corresponding ranges to determine the amount of the secret bits for the adaptive LSB embedding process. In 2023, Jing-yu et al. [52] implemented a unique chaotic system algorithm on the Kintex 7 xc7K3525tfbv676-3 FPGA, which exhibits stable equilibrium points. Chaotic signals produced by chaotic systems are utilized in encryption and steganography to augment security. In addition, the encryption system that employs scrambling-diffusion is integrated with the steganography technique known as least significant bit (LSB)-pixel value differencing (PVD). In 2024, Yanuar et al. [53] revealed a brand-new strategy for image steganography that incorporates Josephus permutation into the LSB 3-3-2 embedding method. This method addresses flaws in simple logistic maps that are vulnerable to steganalysis by increasing the unpredictability of the key stream produced by the chaotic logistic map. In 2024, Ali et al. [54] suggested a method that employs a blend of Most Significant Bit (MSB) matching and Least Significant Bit (LSB) substitution. The algorithm suggested partitioning sensitive information into bit pairs and linking them to the most significant bits (MSBs) of pixels by pair matching. This allows for the storage of six bits within a single pixel by altering a maximum of three bits. In 2024, Al-Rubaie et al. [55] proposed two methods for image steganography: lossless and lossy. Both parties employed encryption and steganography techniques that rely on three distinct chaotic maps in order to guarantee the security of information. Table 6 is a summary of the previous work.

Table 6. Summary of image steganography based on spatial embedding.

Authors & Year	Objective	Results	Limitations

Biswas et al. 2019 [48]	High-quality images and increasing capacity	PSNR=38.20
		Capacity= 2.42 (bpp)
			Low PSNR and the spatial domain are weak

Hameed et al. 2019 [49]	Increase security	PSNR=36.32
		Capacity=100000 bytes
			The spatial domain is weak against hackers

Abedleraouf 2021 [50]	High quality of images	PSNR=84.48	The spatial domain is weak against hackers

Hussain et al. 2021 [51]	Increasing capacity	PSNR=35.47
		Capacity=849188 bits
			The spatial domain is weak against hackers

Jing-Yu et al. 2023 [52]	Increasing security	PSNR=39.7514
		Capacity=528686 bits
			Low PSNR

Yanuar et al. 2024 [53]	Increasing security	PSNR=39.5926
		MSE=7.1493
		Capacity=0.777 KB
			Low PSNR and low capacity

Ali et al. 2024 [54]	Increasing capacity and quality of image	PSNR=36.87
		Capacity=177373 byte
			The spatial domain is weak against hackers and has low PSNR

Al-Rubaie et al. 2024 [55]	Increasing capacity	PSNR=69.964
		Capacity=60.938%
			The spatial domain is weak against hackers

3.2. Image Steganography Based on the Frequency Domain

In contrast to the spatial domain-based approach, which immediately incorporates the secret data into the raw pixel intensities of the cover pixel, the transform domain-based method transfers the blocks of cover frames from the spatial domain to the transform domain. The discrete wavelet transform (DWT) and discrete cosine transform (DCT) are the primary transform functions commonly employed in steganography. The Discrete Wavelet Transform (DWT) breaks down the signal into subsets containing important and unimportant data. The pertinent data pertains to the overall visual characteristics and is referred to as low-frequency discrete wavelet transform (DWT) coefficients [56]. Similarly, the inconsequential data signifies the characteristics of the signals and is referred to as the high-frequency coefficients. A solitary signal is transmitted through a collection of filters and separated into two components - an approximation and details. CT, similar to DWT, is a transform function that partitions the image into spectral sub-bands. The primary distinction between DCT and DWT lies in the fact that the former produces a greater number of frequencies bands and offers superior frequency resolution. However, the discrete wavelet transform (DWT) produces a limited number of frequency bands while maintaining a high level of spatial resolution. A substantial number of studies in the literature have utilized the discrete wavelet transform (DWT) domain to conceal confidential information inside unprocessed films. In contrast to the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) domain is not commonly employed in academic literature for concealing confidential information inside unprocessed films [57]. In 2020, Eysaa et al. [58] introduced a strong color picture steganography method for transmitting images over wireless communication systems. This method aims to conceal three color images under a single-color cover image to enhance the concealing capacity, as many existing steganography methods face limitations in terms of capacity. In 2020, Murugan and Subramaniyam [59] suggested the Discrete Wavelet Transform (DWT) offers several advantages over previous transform algorithms, such as the Discrete Cosine Transform (DCT). The reasons for this are quality scalability, interest in region coding, low bit rate transmission with fast operation, and compatibility with Visual Systems. In 2021, Kaur and Singh [60] presented a new hybrid technique to achieve undetectable and resilient image steganography for secure data communication. The novelty of this work is the precise manipulation of the higher frequency coefficient of the Discrete Cosine Transform (DCT) to preserve the perceptual quality of the image. In 2021, Sharaf et al. [61] proposed the picture steganography technique in the transform domain. To improve the picture transfer, we have implemented a hybrid chaotic map that combines the Sin and Logistic-Tent systems. This method was achieved by using the radical function and several trigonometric functions. In 2023, Rekha et al. [62] suggested utilizing the Elgamal algorithm and the Cohen Daubechies-Feauveau Discrete Wavelet Transform (CDF-DWT) method for data-hiding applications. The Speeded-Up Robust Features (SURF) approach is used to detect and filter the edges of the cover image, which is thought to conceal secret data. Utilizing the Elgamal algorithm, the] input data is encrypted. In 2024, Saeidi et al. [63] proposed a counting-based secret-sharing system that seeks to decrease the computational complexity for longer keys, thereby offering a viable steganographic method for efficient sharing. The system combines counting-based secret sharing with integer wavelet transform (IWT) and steganography. Table 7 is a summary of the previous work.

Table 7. Summary of image steganography based on frequency embedding.

Authors & Year	Objective	Results	Limitations

Eysaa et al. 2020 [58]	Increasing security	PSNR=40.4615
		Capacity=75% of image
			Low PSNR
			The results of capacity is not clear

Munugan & Subramaniyam 2020 [59]	Increasing security	PSNR=54	Low PSNR

Kaur & Singh 2021[60]	Increasing security	PSNR=32.9906
		Capacity=212890 bits
			Low PSNR

Sharafi et al. 2021 [61]	Increasing security	PSNR=54.0027
		Capacity=32768 bits
			Low capacity

Rekha et al 2023 [62]	Increasing security and capacity	PSNR=45.78
		MSE=2.09
		Capacity=80.67%
			Low PSNR

Saeidi et al. 2024 [63]	Reduce the computational complexity	PSNR=80.11	The complexity is high

3.3. Image Steganography Based on Neural Networks

The neural network is used in steganography to embed the secret data into the cover by choosing the optimal hidden pixel, for instance, in 2019, Duan et al. [64] presented a novel image steganography system utilizing a U-Net architecture. Initially, the trained deep neural network consists of a hidden network and an extraction network. Subsequently, the sender employs the hiding network to include the secret image in a separate full-size image without making any alterations. In 2020, Li et al. [65] presented an innovative grayscale picture steganography method that may conceal an encrypted secret image under a cover image of identical dimensions. The covert image is encrypted using the chaos encryption technology prior to being concealed. A convolutional neural network (CNN) is used to convert both the encrypted image and the cover image into the stego image. In 2020, Qin et al. [66] suggested a kind of steganography without a cover still faces issues such as limited storage space and subpar quality. To address these issues, employ a Generative Adversarial Network (GAN), which is a powerful deep learning framework, to encode confidential information into the cover image. In 2020, Shang et al. [67] suggested an innovative approach to improve the security of steganography technologies based on deep learning. So, exploit the linear characteristics of a cutting-edge CNN-based steganalysis and employ adversarial example methods to enable stego to evade detection. In 2023, Bahaddad et al. [68] suggested a design for the Bald Eagle Search Optimal Pixel Selection with Chaotic Encryption (BESOPS-CE) image steganography technology. The BESOPS-CE approach successfully conceals the secret image within the encrypted version of the cover image. The BESOPS-CE approach utilizes a BES to carry out an optimal pixel selection (OPS) procedure. In 2024, Huo et al. [69] outlined a Chaotic mapping-enhanced image Steganography network (CHASE) that improves the security of the steganography by reducing the disparity between the container and cover pictures through the image permutation method and pioneering the concealing of color images in grey images. In addition to using Generative Adversarial Networks (GANs) to increase image fidelity in large capacity steganographic scales. In 2024, Cheng et al. [70] introduced a secure image-hiding network (SIHNet) to minimize the unauthorized disclosure of confidential data. The proposed reversible secret image processing (SIP) module utilizes invertible neural networks to effectively hide secret images and minimize the leakage of confidential information in the resulting stego images. In addition, a reversible lost information hiding (LIH) module is employed to conceal the missing information within the cover images. In 2024, Ramandi et al. [71] introduced VidaGAN, a steganography system that employs deep learning algorithms. The suggested network consists of three components: an encoder, a decoder, and a critic. Additionally, it presents a new architectural design and other inventive solutions to tackle the unresolved issues. In 2024, Ali et al. [72] presented a novel steganography system utilizing HMPSO (Hybrid Multi-Objective Particle Swarm Optimization) and DDV (Dynamic Data Verification) was proposed. The acronym HMPSO stands for Henon map and particle swarm optimization, and DDV is an abbreviation for distinction disparity value. The planned scheme comprised four phases, each with distinct contributions. In the initial stage, the secret messages and cover images were subjected to processing. During this stage, the confidential message has been condensed using the Huffman technique. The second phase encompassed the process of embedding. This phase has two distinct contributions: HMPSO and DDV. The HMPSO is responsible for selecting the most optimal pixels. The DDV is accountable for the process of embedding. The third phase entails the utilization of the extraction technique. Table 8 is a summary of the previous work.

Table 8. Summary of image steganography based on neural embedding.

Authors & Year	Objective	Results	Limitations

Duan et al. 2019 [64]	High-quality images and increasing capacity	PSNR=40.4716
		Capacity=524288 bits
			Low PSNR

Li et al. 2020 [65]	Increasing security	PSNR=41.2	Low PSNR

Qin et al. 2020 [66]	Increasing security	PSNR=39.80
		Capacity=2.36 (bpp)
			Low PSNR

Shang et al. 2020 [67]	Increasing security	PSNR=27.9957
		Capacity=0.4 (bpp)
			Low PSNR

Bahaddad et al. 2023 [68]	Increasing impeccability	PSNR=55.3159
		MSE=0.1912
			Low PSNR

Huo et al. 2024 [69]	Increasing security	PSNR=34.41	Low PSNR
Cheng et al. 2024 [70]	Increasing the quality of an image	PSNR=40.06	Low PSNR

Ramandi et al. 2024 [71]	Increasing the quality of an image	PSNR=37.51
		Capacity=3.9 (bpp)
			Low PSNR

Ali et al. 2024 [72]	Increasing security	PSNR=78.09
		MSE=0.1012
		Capacity=16384 byte
			Low capacity

3.4. Video Steganography

Video steganography is a more effective material than a picture, text, or audio cover [73]. The video is composed of a series of frames, each of which depicts an image. A grayscale frame has 8 bits, a color frame has 24, and the single pixel in the cover video has either 8 or 24 bits. There are three RGB channels in the color image, with eight bits per pixel in each channel [74]. Figure 5 shows the essential steps for video steganography.

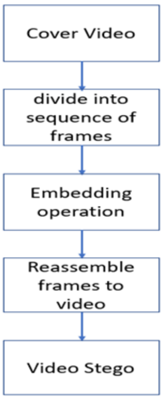


Fig. 5. Basic steps of video steganography.

In 2019, Abed et al. [75] presented an innovative automated approach for attaining dual degrees of security for videos, involving the utilization of encryption and steganography techniques. During the initial stage, confidential information undergoes encryption using the Advanced Encryption Standard (AES) algorithm, resulting in the data becoming unintelligible. The work utilizes the Least Significant Bit (LSB) method as a steganography technique. In 2020, Mstafa et al. [76] presented a novel methodology for video steganography, utilizing the corner point principle and LSB algorithm. The proposed approach initially employs the Shi-Tomasi algorithm to identify areas of corner points in the frames of the cover video. Next, it employs the 4-LSBs algorithm to conceal sensitive information within the designated corner locations. Before the embedding procedure, the proposed method enhances the security level by encrypting confidential data using Arnold's cat map method. In 2021, Shehab et al. [77] introduced a proposal aimed at easily concealing and reconstructing a secret image of significant dimensions by mixing encryption and concealment techniques. This method involves using a movie as a disguise for concealing huge picture blocks within its frames. The selection of frames is determined by 5D hyperchaotic algorithms, which in turn affect the value of each pixel in the original image. In 2022, Dalal and Juneja [78] introduced a novel video steganography method that achieves a consistent balance between resilience and invisibility by employing a 2D-DWT (Discrete Wavelet Transform) approach, which relies on object identification and tracking. The primary contribution of this paper involves the incorporation of confidential information into moving objects by utilizing object recognition on video frames. The secret bits are then embedded in the intermediate frequency sub-bands using 2D-DWT. In 2022, Fan et al. [79] presented a strong video steganography technique that can effectively hide information in videos, even when they are transcoded. The goal is to establish a secure method of secret communication on social media platforms. A novel approach utilizing principal component analysis is presented to identify resilient embedding zones. In addition, further information is provided to assign labels to these chosen regions. In 2022, Hassan and Gutub [80] suggested a novel method for reversible data hiding (RDH) in photos, ensuring accurate image recovery following data extraction. The proposed interpolation-based RDH (IRDH) system enhances both the embedding capacity and security compared to existing state-of-the-art schemes. We conducted a study on enhancing the parabolic interpolation (PI) method for enlarging the original image. Additionally, we developed a novel embedding technique to incorporate secret data into the image. In 2023, Cui et al. [81] suggested a new, effective, and efficient Deeply Recursive Attention Network (DRANet) for video steganography, which models spatiotemporal attention to discover appropriate locations for information hiding. A Non-Local Self-Attention (NLSA) block and a Non-Local Co-Attention (NLCA) block are the two basic components that make up the DRANet. By calculating the correlations between inter- and intra-cover frames, the NLSA block can specifically choose the cover frame areas that are appropriate for concealment. In order to strengthen the model's resilience and lessen the impact of various regions in the hidden video, the NLCA block attempts to efficiently generate improved representations of the secret frames. In 2024, Vergara et al. [82] proposed architecture for video steganography based on the Spatial-Temporal Adaptive Filter Network (STFAN) and the Attention mechanism. This architecture utilizes filters and maps to enhance the efficiency and effectiveness of frame processing. It takes advantage of the redundancy in the temporal dimension of the video, as well as fine details like edges, fast-moving pixels, and the context of secret and cover frames. Additionally, the architecture incorporates the DWT method for feature extraction, which has similar characteristics when applied to an image file. In 2024, Wang [83] described steganography technique specifically involving using thumbnail movies as a means of concealing data, a method that is widely employed on many social media platforms. The inquiry into the technique of concealing confidential information within post-down sampled video results in the suggestion of an adaptable, resistant approach to video steganography that is specifically designed to exploit the distinct features of these commonly employed video formats. In order to make the target frames harder to discover, a pseudorandom number method is used. This algorithm intelligently chooses the target frames by considering a secret key and the specific properties of the movie. Table 9 is a summary of the previous work.

Table 9. Summary of video steganography.

Authors & Year	Objective	Results	Limitations
Abed et al. 2019 [75]	High quality of images	PSNR= 57.1	LSB is weak against hackers

Mstafa et al. 2020[76]	Increasing security	PSNR=60.7
		Capacity=1978044 bits
			The authors didn’t mention any details about choosing the frame in the video

Shehab et al. 2021 [77]	Increasing security	PSNR=61.132
		Capacity=200×200 image size
			The random selection of farms leads to increased distortion

Dalal & Juneja 2022 [78]	Increasing security and high-quality image	PSNR=46.59	Low PSNR
Fan et al. 2022 [79]	Increasing security	PSNR=48	Low PSNR

Hacimurtazaoglu & Tutuncu 2022 [80]	Increasing the quality of the image	PSNR=80.0145
		Capacity=42.8Kb
			Low capacity

Cui et al. 2023 [81]	Increasing the quality of images	PSNR=28.4507	Low PSNR
Vergara et al. 2024 [82]	Increasing security	PSNR=27.0164	Low PSNR
Wang 2024 [83]	Increasing security	PSNR=51.06	The random selection operation causes a low ratio in PSNR

4. Evaluation Parameters

Many criteria measure the quality of performance in the encryption and concealment process. Table 10 summarizes the most important of these criteria.

Table 10. Summary of evaluation parameters.

Parameters	Abbreviation	Definition	Equations	Preference in steganography	Preference in encryption
Histogram [84]	H(s)	This method displays the distribution of pixel values.	-------------------------------------	Unequal distribution	equal distribution
Entropy [85]	$E(s)$	It quantifies the level of uncertainty or randomness.	$E(s) = -\sum_{i=1}^{n} p(c_i) log_2 p(c_i)$ (1) Where s is the collection of symbols, p (ci) is the probability, and n represents the number of symbols	must be decreasing than 8 value	must be near 8 value
Correlation Coefficient [86]	CC	evaluating the degree of association between pixels	$r_{xy} = \frac{cov\ (x,y)}{s_x s_y}$ (2) $\text{cov(x,y)}=\frac{1}{N}\sum_{i=1}^{N}\left(x_i\text{-P(x)}\right)\left(y_i\text{-P(y)}\right)$ Type equation here. $s_x = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - P(x))^2}$ (4) $\text{P(x)}=\frac{1}{N}\sum_{i=1}^{N} x_i$ (5) Since P(X) is the predictable value, Sx represents the discrepancy rating. And x and y represent the values of N adjacent pixels	Near to 1	Near to -1
Key Space [87]	-------------	The set of all potential keys that can be utilized to initialize the cryptographic algorithm.	--------------------------------------	-------------	exceed 2100
Number Pixel based on Change Rate [88]	NPCR	used to assess picture encryption algorithms/ciphers' differential attack resistance	$\text{NPCR} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} D(i,j)}{m \times n} \times 100\%$ (6) $D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases}$ (7)	-------------	Acceptable value 99.61%
Unified Average based on Changing Intensity [88]	UACI	The Change Rate measures the differential attack resistance	$\text{UACI} = \frac{1}{m \times n}\left(\sum_{i=1}^{m}\sum_{j=1}^{n}\frac{\lvert C_1(i,j) - C_2(i,j)\rvert}{255}\right) \times 100\%$ (8) C1 is the cipher picture before, and C2 is the cipher picture after the change.	-------------	Acceptable value 33.44%
Mean Square Error [89]	MSE	It measures the error ratio between the original plain image and the steganography or encrypted image.	$\text{MSE} = \frac{1}{w \times h}\sum_{i=1}^{w}\sum_{j=1}^{h}(P(i,j) - C(i,j))^2$ (9) Where p is the initial image before the encrypted operation, and c is the cipher or steganography picture. Variables w and h are the image's width and height	Decreasing (near to zero)	Increasing (near to infinite)
Peak Signal Noise Ratio [90]	PSNR	Serves as a signal match ratio between an encrypted or steganography image and a plain image.	$\text{PSNR} = 10 \times \log_{10}\frac{\text{MAX}^2}{\text{MSE}}$ (10) MAX is the highest pixel rate, representing 255	Increasing (near to infinite)	Decreasing (near to zero)

Figure 6 first compares the entropy values for various image encryption techniques based on chaos, using references [12], [14], [17], [18], and [20], respectively. Secondly, Refs. [25], [27], [29], [30], and [31] compare the entropy when the image undergoes S-box encryption. Thirdly, Refs. [36-40] describe the entropy in the DNA technique. Finally, Refs. [43], [45], and [46] compare the entropy in neural techniques. On the other hand, figure 7 compares steganography techniques, where the capacity increases, leading to decreased vision quality in images. In this work, the capacity was measured by Kilo Byte (KB). The speed of the spatial domain makes it more commonly used than other techniques. However, the use of a sample structure constrains its security. The comparison in this work was applied using Ref. [49], Ref. [52], and Ref. [54] in the spatial domain. Moreover, Refs. [60] and [61] were applied in the frequency domain. Finally, Ref. [64] and Ref. [72] in neural embedding techniques. However, the complexity of the neural operation exceeds that of other methods.

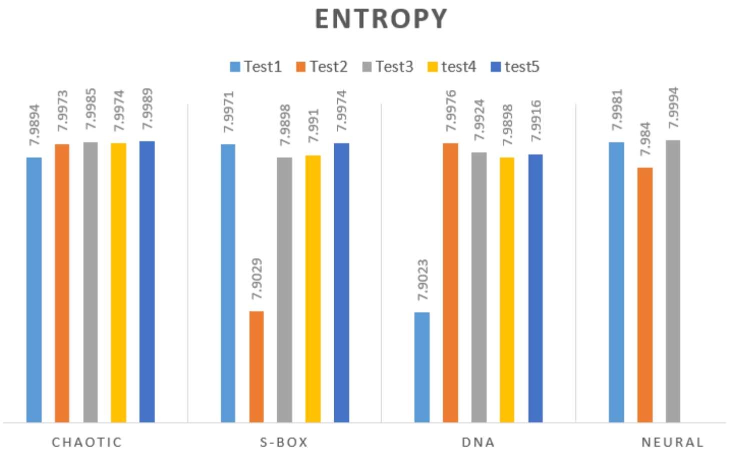


Fig. 6. Comparison among image encryption techniques.

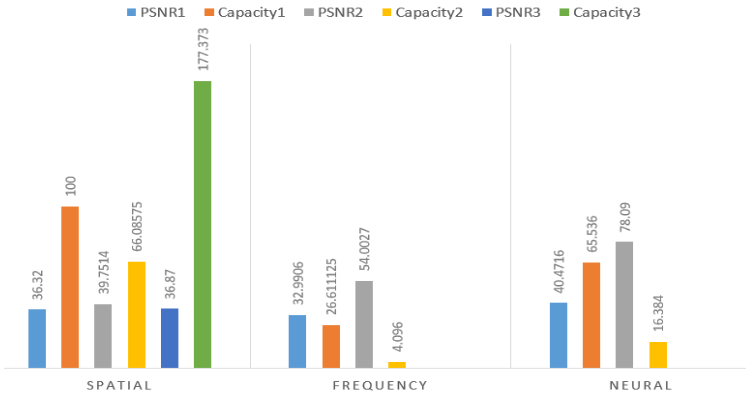


Fig. 7. Comparison among steganography embedding techniques.

5. Conclusion

The techniques of security data are scientifically divided into two essential types: cryptography and steganography. Most encryption techniques are not strong enough to resist hackers and intruders. On the other hand, most steganography techniques don't satisfy the evaluation of the three requirements. Moreover, most algorithms are designed as a single scheme. So, in this work, some recommendations are suggested to fortify these techniques, such as the implementation of a new hybrid design of encryption and steganography to increase unpredictability. The suggested encryption design is based on hyper-chaos with a simple structure and high bifurcation range with different rounds of confusion and diffusion. Besides that, a new steganography algorithm should be suggested that considers the trade-off relation between capacity, imperceptibility, and robustness. This work can suggest the following summary recommended:

- Implementing the hybrid design of encryption and steganography to overcome low security in single-phase.
- The complexity of design has more security. However, this leads to increased time in execution, so in this work, a balanced design is suggested.
- Due to the lack of hardware implementation for most designs, previous work did not meet real-time application requirements.
- Most designs neglected the effect of the channel on the sender and receiver. However, the transmission channel can lose secret information; hence, this work suggests a design that protects sensitive information with efficient channel bandwidth.

References

[1] X. Wang, X. Wang, B. Ma, Q. Li, and Y.-Q. Shi, "High precision error prediction algorithm based on ridge regression predictor for reversible data hiding," *IEEE Signal Process. Lett.*, vol. 28, pp. 1125–1129, 2021. DOI:10.1109/LSP.2021.3080181

[2] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Arch. Comput. Methods Eng.*, vol. 27, no. 1, pp. 15–43, 2020. DOI:10.1007/s11831-018-9298-8

[3] K. C. Jithin and S. Sankar, "Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set," *J. Inf. Secur. Appl.*, vol. 50, no. 102428, p. 102428, 2020. DOI:10.1016/j.jisa.2019.102428

[4] R. B. Naik and U. Singh, "A review on applications of chaotic maps in pseudo-random number generators and encryption," Ann. Data Sci., vol. 11, no. 1, pp. 25–50, 2024. DOI:10.1007/s40745-021-00364-7

[5] J. S. Muthu and P. Murali, "Review of chaos detection techniques performed on chaotic maps and systems in image encryption," SN Comput. Sci., vol. 2, no. 5, 2021. DOI: 10.1007/s42979-021-00778-3

[6] M. Z. Talhaoui, X. Wang, and M. A. Midoun, "A new one-dimensional cosine polynomial chaotic map and its use in image encryption," Vis. Comput., vol. 37, no. 3, pp. 541–551, 2021.DOI: 10.1007/s00371-020-01822-8

[7] X. Wang, S. Gao, L. Yu, Y. Sun, and H. Sun, "Chaotic image encryption algorithm based on bit-combination scrambling in decimal system and dynamic diffusion," IEEE Access, vol. 7, pp. 103662–103677, 2019. DOI: 10.1109/ACCESS.2019.2931052

[8] K. J. Sher and J. Ahmad, "Chaos-based efficient selective image encryption," Multidimensional Systems and Signal Processing, vol. 30, pp. 943–961, 2019. DOI:10.1007/s11045-018-0589-x

[9] Z.-H. Gan, X.-L. Chai, D.-J. Han, and Y.-R. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," Neural Comput. Appl., vol. 31, no. 11, pp. 7111–7130, 2019. DOI:10.1007/s00521-018-3541-y

[10] A. Alireza, M. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," The Journal of Supercomputing, vol. 75, pp. 6663–6682, 2019. DOI: 10.1007/s11227-019-02878-7

[11] F. S. Hasan and M. A. Saffo, "FPGA hardware co-simulation of image encryption using stream cipher based on chaotic maps," Sens. Imaging, vol. 21, no. 1, 2020. DOI:10.1007/s11220-020-00301-7

[12] L. Tao, D. Baoxiang, and X. Liang, "Image encryption algorithm based on logistic and two-dimensional Lorenz," Ieee Access, vol. 8, pp. 13792–13805, 2020. DOI: 10.1109/ACCESS.2020.2966264

[13] G. Kaur, R. Agarwal, and V. Patidar, "Chaos based multiple order optical transform for 2D image encryption," Eng. Sci. Technol. Int. J., vol. 23, no. 5, pp. 998–1014, 2020. DOI: 10.1016/j.jestch.2020.02.007

[14] X. Gao, "Image encryption algorithm based on 2D hyperchaotic map," Opt. Laser Technol., vol. 142, no. 107252, p. 107252, 2021.DOI: 10.1016/j.optlastec.2021.107252

[15] H. Wen, Z. Chen, J. Zheng,Y. Huang, S. Li, L. Ma, Y. Lin, Z. Liu, R. Li, L. Liu, W. Lin, J. Yang, C. Zhang, H.Yang, "Design and embedded implementation of secure image encryption scheme using DWT and 2D-LASM," Entropy (Basel), vol. 24, no. 10, p. 1332, 2022.DOI: 10.3390/e24101332

[16] Q. Lai and Y. Liu, "A cross-channel color image encryption algorithm using two-dimensional hyperchaotic map," Expert Syst. Appl., vol. 223, no. 119923, p. 119923, 2023.DOI: 10.1016/j.eswa.2023.119923

[17] H. Wen, Y. Huang, and Y. Lin, "High-quality color image compression-encryption using chaos and block permutation," J. King Saud Univ. - Comput. Inf. Sci., vol. 35, no. 8, p. 101660, 2023.DOI: 10.1016/j.jksuci.2023.101660

[18] D. A. Q. Shakir, A. Salim, S. Q. A. Al-Rahman, and A. M. Sagheer, "Image encryption using Lorenz chaotic system," Journal of Techniques, vol. 5, no. 1, pp. 122–128, 2023.DOI: 10.51173/jt.v5i1.840

[19] A. Toktas, "A robust bit-level image encryption based on Bessel map," Applied Mathematics and Computation, vol. 462, 2024.DOI: 10.1016/j.amc.2023.128340

[20] S. Patel, V. Thanikaiselvan, and A. Rearajan, "Secured quantum image communication using new two dimensional chaotic map based encryption methods," Int. J. Theor. Phys., vol. 63, no. 2, 2024.DOI: 10.1007/s10773-024-05548-4

[21] D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," Nonlinear Dyn., vol. 100, no. 1, pp. 699–711, 2020.DOI: 10.1007/s11071-020-05503-y

[22] C. Easttom, "s-box Design," in Modern Cryptography, Cham: Springer International Publishing, 2022, pp. 193–212.DOI:10.1007/978-3-031-12304-7_8

[23] K. M. Fahad, A. Ahmed, and K. Saleem, "A novel cryptographic substitution box design using Gaussian distribution," IEEE Access, vol. 7, pp. 15999–16007, 2019. DOI: 10.1109/ACCESS.2019.2893176

[24] L. Lidong, D. Jiang, X. Wang, L. Zhang, and X. Rong, "A dynamic triple-image encryption scheme based on chaos, S-box and image compressing," IEEE Access, vol. 8, pp. 210382–210399, 2020. DOI: 10.1109/ACCESS.2020.3039891

[25] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," IEEE Access, vol. 8, pp. 25664–25678, 2020. DOI: 10.1109/ACCESS.2020.2970806

[26] S. Ibrahim and A. Alharbi, "Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography," IEEE Access, vol. 8, pp. 194289–194302, 2020.DOI: 10.1109/ACCESS.2020.3032403

[27] M. Z. Talhaoui and X. Wang, "A new fractional one dimensional chaotic map and its application in high-speed image encryption," Inf. Sci. (Ny), vol. 550, pp. 13–26, 2021.DOI: 10.1016/j.ins.2020.10.048

[28] T. Sajjad and R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box," Multimedia Tools and Applications, vol. 81, pp. 20585–20609, 2022.DOI: 10.1007/s11042-022-12268-6

[29] Arif et al., "A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution," IEEE Access, vol. 10, pp. 12966–12982, 2022.DOI: 10.1109/ACCESS.2022.3146792

[30] R. S. Ali and O. Z. Akif, S. A. Jassim, Farhan, A. K. Farhan, E. S. El-Kenawy, A. Ibrahim, M. E. Ghoneim, A. Abdelhamid, "Enhancement of the CAST block algorithm based on novel S-Box for image encryption," Sensors (Basel), vol. 22, no. 21, p. 8527, 2022.DOI: 10.3390/s22218527

[31] E.-S. El Akkad L. Khrissi K. Satori W. El-Shafai T. Altameem R. S. Rathore, "An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers," Egypt. Inform. J., vol. 25, no. 100449, p. 100449, 2024.DOI: 10.1016/j.eij.2024.100449

[32] S. Ibrahim, A. M. Abbas, A. A. Alharbi, and M. A. Albahar, "A new 12-bit chaotic image encryption scheme using a 12 × 12 dynamic S-box," IEEE Access, vol. 12, pp. 37631–37642, 2024. 10.1109/ACCESS.2024.3374218

[33] D. Ustun, S. Sahinkaya, and N. Atli, “Developing a secure image encryption technique using a novel S-box constructed through real-coded genetic algorithms crossover and mutation operators,” Expert Systems with Applications, 2024.DOI 10.1016/j.eswa.2024.124904:

[34] T.-Y. Wu, X. Fan, K.-H. Wang, C.-F. Lai, N. Xiong, and J. M.-T. Wu, “A DNA computation-based image encryption scheme for cloud CCTV systems,” IEEE Access, vol. 7, pp. 181434–181443, 2019. DOI: 10.1109/ACCESS.2019.2946890

[35] E. Z. Zefreh, “An image encryption scheme based on a hybrid model of DNA computing, chaotic systems, and hash functions,” in Multimedia Tools and Applications 79, 2020, pp. 24993–25022.DOI: 10.1007/s11042-020-09111-1

[36] N. Iqbal et al., “On the image encryption algorithm based on the chaotic system, DNA encoding, and castle,” IEEE Access, vol. 9, pp. 118253–118270, 2021. DOI: 10.1109/ACCESS.2021.3106028

[37] P. N. Lone, D. Singh, and U. H. Mir, “Image encryption using DNA coding and three-dimensional chaotic systems,” Multimed. Tools Appl., vol. 81, no. 4, pp. 5669–5693, 2022. DOI:10.1007/s11042-021-11802-2

[38] B. Jasara and A. H. Moon, “Color image encryption and authentication using dynamic DNA encoding and hyperchaotic system,” Expert Systems with Applications, vol. 206, 2022.DOI: 10.1016/j.eswa.2022.117861

[39] A. Alrubaie, a. A. A. Maisa, and A. T. Khodher, “Image encryption based on 2DNA encoding and chaotic 2D logistic map,” Journal of Engineering and Applied Science, vol. 70, 2023. DOI:10.1186/s44147-023-00228-2

[40] Zhao, S. Wang, and L. Zhang, “Block image encryption algorithm based on novel chaos and DNA encoding,” Information, vol. 14, 2023.DOI: 10.3390/info14030150

[41] C. Zhang, S. Zhang, K. Liang, and Z. Chen, “Double image encryption algorithm based on parallel compressed sensing and chaotic system,” IEEE Access, vol. 12, pp. 54745–54757, 2024. DOI: 10.1109/ACCESS.2024.3389975

[42] B. Han, Y. Jia, G. Huang, and L. Cai, “A medical image encryption algorithm based on Hermite chaotic neural network,” in 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2020. DOI: 10.1109/ITNEC48623.2020.9085079

[43] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, “Double image encryption algorithm based on neural network and chaos,” Chaos Solitons Fractals, vol. 152, no. 111318, p. 111318, 2021.DOI: 10.1016/j.chaos.2021.111318

[44] Feng, “Image encryption algorithm combining chaotic image encryption and convolutional neural network,” Electronics, vol. 12, 2023.DOI: 10.3390/electronics12163455

[45] Vijayakumar and A. Ahilan, “An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map,” Ain Shams Eng. J., vol. 15, no. 4, p. 102620, 2024.DOI: 10.1016/j.asej.2023.102620

[46] Kocak, U. Erkan, A. Toktas, and S. Gao, “PSO-based image encryption scheme using modular integrated logistic exponential map,” Expert Syst. Appl., vol. 237, no. 121452, p. 121452, 2024.DOI: 10.1016/j.eswa.2023.121452

[47] M. Dalal and M. Juneja, “A survey on information hiding using video steganography,” Artif. Intell. Rev., vol. 54, no. 8, pp. 5831–5895, 2021.DOI: 10.1007/s10462-021-09968-0

[48] R. Biswas, I. Mukherjee, and S. K. Bandyopadhyay, “Image feature based high capacity steganographic algorithm,” Multimed. Tools Appl., vol. 78, no. 14, pp. 20019–20036, 2019.DOI: 10.1007/s11042-019-7369-y

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

[50] A. AbdelRaouf, “A new data hiding approach for image steganography based on visual color sensitivity,” Multimed. Tools Appl., vol. 80, no. 15, pp. 23393–23417, 2021. DOI:10.1007/s11042-020-10224-w

[51] 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, 2021.DOI: 10.1007/s11042-021-10652-2

[52] Jing-yu, C. Hong, W. Gang, G. Zi-bo, and H. Zhang, “FPGA image encryption-steganography using a novel chaotic system with line equilibria,” Digit. Signal Process, vol. 134, no. 103889, p. 103889, 2023.DOI: 10.1016/j.dsp.2022.103889

[53] M. R. Yanuar, S. Mt, C. Apriono, and M. F. Syawaludin, “Image-to-image steganography with Josephus permutation and least significant bit (LSB) 3-3-2 embedding,” *Appl. Sci. (Basel)*, vol. 14, no. 16, p. 7119, 2024.DOI: 10.3390/app14167119

[54] M. Z. Ali, O. Riaz, H. M. Hasnain, W. Sharif, T. Ali, and G. S. Choi, “Elevating image steganography: A fusion of MSB matching and LSB substitution for enhanced concealment capabilities,” Comput. Mater. Contin., vol. 79, no. 2, pp. 2923–2943, 2024. DOI: 10.32604/cmc.2024.049139

[55] A. Rubaie, S. Fadhel, and K. M. Maher, “High capacity double precision image steganography based on chaotic maps,” Bulletin of Electrical Engineering and Informatics, vol. 13, pp. 320–331, 2024. DOI:10.11591/eei.v13i1.6055

[56] 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, 2021. DOI: 10.1109/ACCESS.2021.3053998

[57] J. Kunhoth, N. Subramanian, S. Al-Maadeed, and A. Bouridane, “Video steganography: recent advances and challenges,” Multimed. Tools Appl., vol. 82, no. 27, pp. 41943–41985, 2023.DOI: 10.1007/s11042-023-14844-w

[58] A. Eyssa, F. E. Abdelsamie, and A. E. Abdelnaiem, “An efficient image steganography approach over wireless communication system,” Wirel. Pers. Commun., 2020. DOI:10.1007/s11277-019-06730-2

[59] G. V. K. Murugan and R. Uthandipalayam Subramaniyam, “Performance analysis of image steganography using wavelet transform for safe and secured transaction,” Multimed. Tools Appl., vol. 79, no. 13–14, pp. 9101–9115, 2020.DOI: 10.1007/s11042-019-7507-6

[60] Kaur and B. Singh, “A hybrid algorithm for robust image steganography,” Multidimens. Syst. Signal Process., vol. 32, no. 1, pp. 1–23, 2021. DOI https://doi.org/10.1007/s11045-020-00725-0

[61] J. Sharafi, Y. Khedmati, and M. M. Shabani, “Image steganography based on a new hybrid chaos map and discrete transforms,” Optik (Stuttg.), vol. 226, no. 165492, p. 165492, 2021.DOI: https://doi.org/10.1016/j.ijleo.2020.165492

[62] K. Sashi Rekha, M. Joe Amali, M. Swathy, M. Raghini, and B. Priya Darshini, “A steganography embedding method based on CDF-DWT technique for data hiding application using Elgamal algorithm,” Biomed. Signal Process. Control, vol. 80, no. 104212, p. 104212, 2023.DOI: https://doi.org/10.1016/j.bspc.2022.104212

[63] 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, 2024.DOI: https://doi.org/10.1049/ipr2.12938

[64] 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. 1–1, 2019. DOI: 10.1109/ACCESS.2019.2891247

[65] Q. Li, X. Wang, X. Wang,B.Ma, C. Wang, Y. Xian, Y.Shi, "A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks," IEEE Access, vol. 8, pp. 168166–168176, 2020. DOI: 10.1109/ACCESS.2020.3021103

[66] J. Qin, J. Wang, Y. Tan, H. Huang, X. Xiang, and Z. He, "Coverless image steganography based on generative adversarial network," Mathematics, vol. 8, no. 9, p. 1394, 2020.DOI: https://doi.org/10.3390/math8091394

[67] Y. Shang, S. Jiang, D. Ye, and J. Huang, "Enhancing the security of deep learning steganography via adversarial examples," Mathematics, vol. 8, no. 9, p. 1446, 2020.DOI: https://doi.org/10.3390/math8091446

[68] A. Bahaddad, K. Ali Almarhabi, and S. Abdel-Khalek, "Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption," Alex. Eng. J., vol. 75, pp. 41–54, 2023. DOI:https://doi.org/10.1016/j.aej.2023.05.051

[69] L. Huo, R. Chen, J. Wei, and L. Huang, "A high-capacity and high-security image steganography network based on chaotic mapping and Generative Adversarial Networks," Appl. Sci. (Basel), vol. 14, no. 3, p. 1225, 2024.DOI: https://doi.org/10.3390/app14031225

[70] Z. Cheng, X. Jin, Q. Jiang, L. Wu, Y. Dong, and W. Zhou, "SIHNet: A safe image hiding method with less information leaking," IET Image Process., vol. 18, no. 10, pp. 2800–2815, 2024.DOI: https://doi.org/10.1049/ipr2.13138

[71] Y. Ramandi, M. Fateh, and M. Rezvani, "VidaGAN: Adaptive GAN for image steganography," IET Image Process., 2024.DOI: https://doi.org/10.1049/ipr2.13177

[72] A. S. Ali, S. Alsamaraee, and A. A. Hussein, "Optimize image steganography based on distinction disparity value and HMPSO to ensure confidentiality and integrity," J. Comput. Netw. Commun., vol. 2024, no. 1, 2024.DOI: https://doi.org/10.1155/2024/2516567

[73] P. Rachna, K. Lad, and M. Patel, "Study and investigation of video steganography over uncompressed and compressed domain: a comprehensive review," Multimedia Systems, vol. 27, pp. 985–1024, 2021.DOI: 10.1007/s00530-021-00763-z

[74] P. Rachna, L. Kalpesh, P. Mukesh, and D. Madhavi, "A hybrid DST-SBPNRM approach for compressed video steganography," Multimedia Systems, vol. 27, pp. 417–428, 2021.DOI: https://doi.org/10.1007/s00530-020-00735-9

[75] S. Abed, M. Al-Mutairi, A. Al-Watyan, O. Al-Mutairi, W. AlEnizy, and A. Al-Noori, "An automated security approach of video steganography–based LSB using FPGA implementation," J. Circuits Syst. Comput., vol. 28, no. 05, p. 1950083, 2019.DOI: https://doi.org/10.1142/S021812661950083X

[76] J. Mstafa, Y. M. Younis, H. I. Hussein, and M. Atto, "A new video steganography scheme based on Shi-Tomasi corner detector," IEEE Access, vol. 8, pp. 161825–161837, 2020. DOI: 10.1109/ACCESS.2020.3021356

[77] J. N. Shehab, H. A. Abdulkadhim, and T. F. H. Al-Tameemi, "Robust large image steganography using LSB algorithm and 5D hyper-chaotic system," Bull. Electr. Eng. Inform., vol. 10, no. 2, pp. 689–698, 2021. DOI: https://doi.org/10.11591/eei.v10i2.2747

[78] D. Mukesh and M. Juneja, "A secure video steganography scheme using DWT based on object tracking," Information Security Journal: A Global Perspective, vol. 31, pp. 196–213, 2022.DOI: https://doi.org/10.1080/19393555.2021.1896055

[79] F. Pingan, H. Zhang, and X. Zhao, "Robust video steganography for social media sharing based on principal component analysis," EURASIP Journal on Information Security, vol. 2022, 2022. DOI https://doi.org/10.1186/s13635-022-00130-z

[80] F. S. Hassan and A. Gutub, "Novel embedding secrecy within images utilizing an improved interpolation-based reversible data hiding scheme," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 5, pp. 2017–2030, 2022.DOI: https://doi.org/10.1016/j.jksuci.2020.07.008

[81] J. Cui, "Deeply-Recursive Attention Network for video steganography," CAAI Transactions on Intelligence Technology, vol. 8, pp. 1507–1523, 2023.DOI: https://doi.org/10.1049/cit2.12191

[82] G. F. Vergara, P. Giacomelli, A. L. Serrano, F. L. L. Mendonça, G. A. P. Rodrigues, G. D. Bispo, V. P. Gonçalves, R. C. Albuquerque, R. T. S. Júnior, "Stego-STFAN: A novel neural network for video steganography," Computers, vol. 13, no. 7, p. 180, 2024.DOI: https://doi.org/10.3390/computers13070180

[83] Y. Wang, "Hiding Data within Thumbnail Videos: An Adaptive Downsampling-Resilient Video Steganography Method," IEEE Access, 2024. DOI: 10.1109/ACCESS.2024.3386798

[84] A. Benlashram, M. Al-Ghamdi, R. AlTalhi, and P. Kaouther Laabidi, "A novel approach of image encryption using pixel shuffling and 3D chaotic map," J. Phys. Conf. Ser., vol. 1447, no. 1, p. 012009, 2020. DOI 10.1088/1742-6596/1447/1/012009

[85] K. J. Sher and J. Ahmad, "Chaos-based efficient selective image encryption," Multidimensional Systems and Signal Processing, vol. 30, pp. 943–961, 2019. DOI https://doi.org/10.1007/s11045-018-0589-x

[86] M. Yildirim, "A color image encryption scheme reducing the correlations between R, G, B components," Optik (Stuttg.), vol. 237, no. 166728, p. 166728, 2021. DOI:https://doi.org/10.1016/j.ijleo.2021.166728

[87] Sneha, S. Sankar, and A. S. Kumar, "A chaotic color image encryption scheme combining Walsh-Hadamard transform and Arnold-Tent maps," Journal of Ambient Intelligence and Humanized Computing, vol. 11, pp. 1289–1308, 2020.DOI: https://doi.org/10.1007/s12652-019-01385-0

[88] R. Saidi, N. Cherrid, T. Bentahar, H. Mayache, and A. Bentahar, "Number of Pixel Change Rate and Unified Average Changing Intensity for sensitivity analysis of encrypted inSAR interferogram," Ing. Syst. D Inf., vol. 25, no. 5, pp. 601–607, 2020. DOI: https://doi.org/10.18280/isi.250507

[89] A. Sukumar, V. Subramaniyaswamy, V. Vijayakumar, and L. Ravi, "A secure multimedia steganography scheme using hybrid transform and support vector machine for cloud-based storage," Multimed. Tools Appl., vol. 79, no. 15–16, pp. 10825–10849, 2020.DOI: https://doi.org/10.1007/s11042-019-08476-2

[90] Singh, P. Agarwal, and M. Chand, "Image Encryption and Analysis using Dynamic AES," in 2019 5th International Conference on Optimization and Applications (ICOA), 2019. DOI: 10.1109/ICOA.2019.8727711