Health and Technology (2022) 12:9–31
https://doi.org/10.1007/s12553-021-00602-1

REVIEW PAPER

Double layer security using crypto-stego techniques: a comprehensive review

Aiman Jan[1] · Shabir A. Parah[1] · Muzamil Hussan[1] · Bilal A. Malik[2]

Received: 3 August 2021 / Accepted: 20 September 2021 / Published online: 13 October 2021

Abstract

Recent advancement in the digital technology and internet has facilitated usage of multimedia objects for data communication. However, interchanging information through the internet raises several security concerns and needs to be addressed. Image steganography has gained huge attention from researchers for data security. Image steganography secures the data by imperceptibly embedding data bits into image pixels with a lesser probability of detection. Additionally, the encryption of data before embedding provides double-layer protection from the potential eavesdropper. Several steganography and cryptographic approaches have been developed so far to ensure data safety during transmission over a network. The purpose of this work is to succinctly review recent progress in the area of information security utilizing combination of cryptography and steganography (crypto-stego) methods for ensuring double layer security for covert communication. The paper highlights the pros and cons of the existing image steganography techniques and crypto-stego methods. Further, a detailed description of commonly using evaluations parameters for both steganography and cryptography, are given in this paper. Overall, this work is an attempt to create a better understanding of image steganography and its coupling with the encryption methods for developing state of art double layer security crypto-stego systems.

Keywords Security · Steganography · Cryptography · Imperceptivity · Attacks

1 Introduction

The increasing bandwidth and data rates of 4G/5G cellular technology and optical fiber communication revolutionized data communication. The exchange of data in form of text, images, audio, and video over the internet has become ubiquitous [1]. The multimedia data is being exchanged by governments, law enforcement agencies, and for telemedicine by the hospitals [2]. During the covid-19 worldwide lockdown traffic of information over the internet saw an upsurge. Although internet usage has various advantages, but security and privacy of data still remain a challenge [3]. Data thefts, modifications, and alterations have become possible due to the availability of various tools in the hands of hackers. Thus, the security of data has become a challenging task of paramount importance for researchers [4]. Various information protecting mechanisms like, cryptography and data hiding methods as shown in Fig. 1, have been put forward to address data security issues [5]. Cryptography scrambles and converts the secret data into an unreadable form for an unauthorized person [6, 7]. Cryptography can be performed either with standard encryption techniques or Chaos based encryption techniques [8]. There are various standard encryption techniques (SET), like Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest Shamir Adleman algorithm (RSA), etc. [9]. In these approaches, the secret key is used to encrypt the important data before embedding [10]. However, the bulk of data with key lengths is the main limitation of the SETs which makes them insecure and less reliable for data encryption [11]. The limitation of SETs has been overcome by the chaos based encryption approaches. Chaos encryption approach uses initial keys for encryption that are sensitive to the changes made [12]. Thus, the chaos-based encryption approaches are more secure cryptographic method to ensure security to the data [13]. Cryptography can provide the considerable

✉ Shabir A. Parah
shabireltr@gmail.com

[1] Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, India

[2] Department of Electronics and Communication Engineering, Institute of Technology, University of Kashmir Zakoora, Srinagar, India

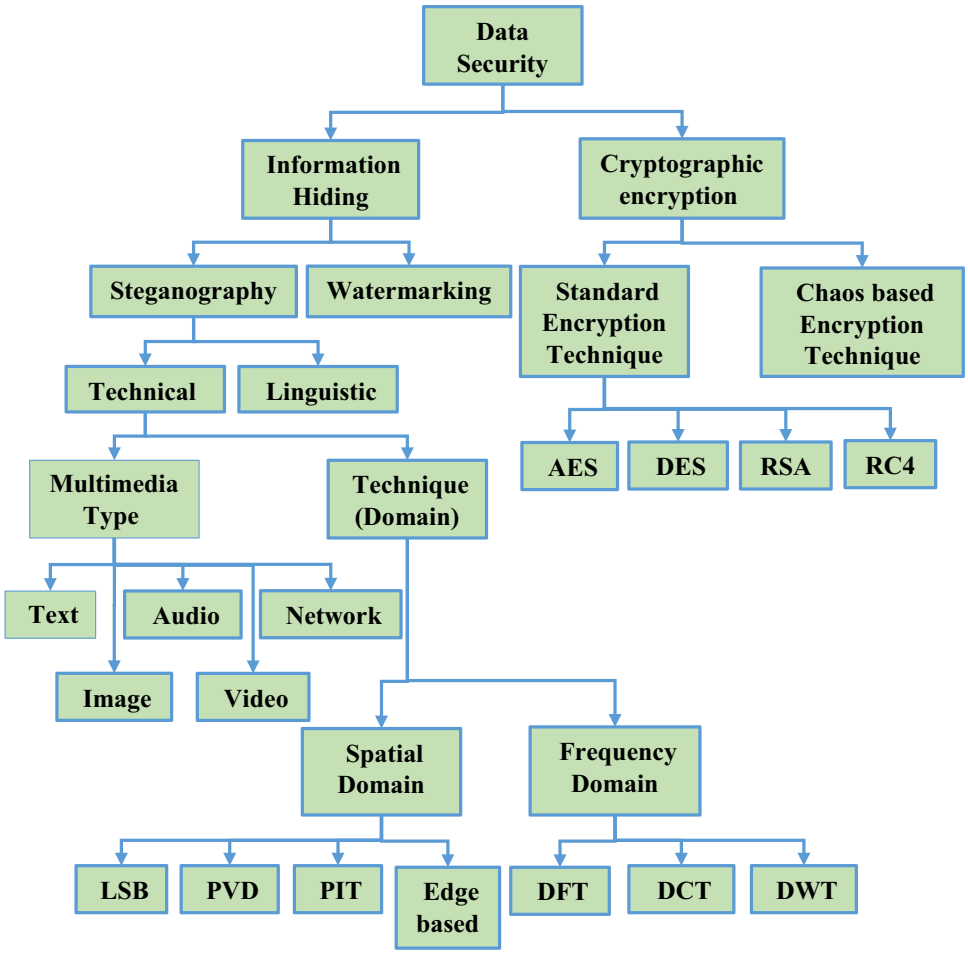


Fig. 1 Different Information Protecting Mechanisms

security to the data by changes the form of the original data through encryption. But, cryptography alone cannot resist security attacks, as its encrypted form attract attacker's attention and hence can be modified or hacked. However, it is an insufficient method to provide data security as its encrypted form may draw the attention of an eavesdropper [14]. Hence, data hiding has been used widely by researchers to hide the existence of important data without being noticed by an intruder [15–17].

Data hiding can be divided into two methods: steganography and watermarking [18]. Watermarking is the method of verifying the authenticity of multimedia (image, video, or audio) for copyright protection [19]. It can be either visible or invisible watermarking to authenticate the ownership. Steganography is the art of hiding important data into any multimedia for secret communication [20]. It is an invisible process in which detection of data is not easy. Steganography can be separated into two categories: Technical and Linguistic steganography approaches [21]. Technical steganography can be further subdivided into two sections based on the multimedia used and the technique applied. Steganography technique has various advantages associated with it, the only difficulty of it is to maintain the image quality with a good amount of payload [22]. Huge secret data size degrades the quality of an image that can suspect the presence of data [23]. And, if the eavesdropper detects the steganographic method, it can easily recover the data. So, with the concealing approach, data should be preprocessed by including some cryptographic approaches [24]. Hence, the present trend is of crypto-stego mechanism in which along with steganography, cryptography method is included to provide double layer security to the data as shown in Fig. 2.

In this paper, the most recent literature in the area of steganography and crypto-stego has been reviewed to facilitate an exhaustive reference for further research in this area. This paper further discusses the various state-of-art techniques, their limitations, and challenges. The analysis parameters have been also discussed. The main contributions of this paper is:

- A comprehensive review of various image crypto-stego methods has been presented.
- Various parameters for evaluation of crypto-stego schemes have been presented.
- A deep insight into double layer schemes and future research directions have been presented.

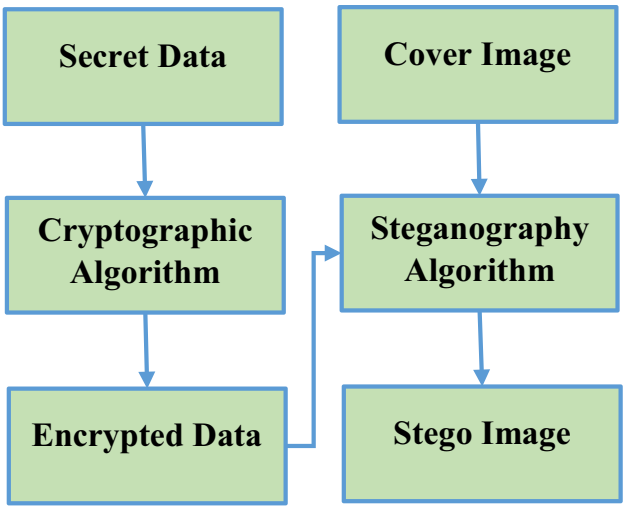


Fig. 2 General Steganography approach together with Cryptography (Crypto-Stego)

The rest of the paper is organized as follows. Section 2 includes the literature survey. Evaluation parameters are discussed in Sect. 3. Section 4 comprises the directions and future research directions. The paper concludes in Sect. 5.

2 Literature survey

Steganography is the art of concealing data into any multimedia for covert communication [25]. Steganography can be divided into many types based on the cover object used to attain security, like text, image, audio, video, and network [26–31]. Further, the steganography can be divided into two domains based on the techniques used to hide data in any multimedia, i.e., spatial domain technique and frequency domain technique [32]. Special domain can be further subdivided into various versions, like least significant bit (LSB), pixel value differencing (PVD), pixel indicator technique (PIT), Edge based technique [33]. Frequency domain can be also subdivided into different types, like discrete fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT) [34]. In this section, the existing literature on different steganographic techniques and crypto-stego has been discussed. The paper focuses on an analysis of publications in reputed journals from 2016–2021 to be taken into consideration for future work. The various steganography data hiding technique and its coupling with cryptographic approaches have been discussed in the subsequent sections. Incorporating cryptography with the steganographic approach provides better security to the data, therefore using the steganography technique alone is 'less secure' compare to the combined approach. As once the steganographic pattern gets revealed to the unintended user, the secret data is prone to hacks and modifications.

2.1 Spatial domain technique

A detailed description of the spatial domain based image steganography techniques has been presented. Table 1 highlights the pros and cons of the reviewed spatial domain techniques.

In 2021, AbdelRaouf [35] has proposed a novel image steganographic data hiding method. The method has used the adaptive least significant bit (LSB) method for hiding information into every color channel of an image. The method has a huge payload but takes more time for embedding data into an image. Although the technique shows considerable image quality values, however, the proposed method can be improved by introducing an encryption method before embedding to improve security. In 2021, Hussain et al. [36] have put forth an enhanced adaptive data hiding approach in which the least significant bit (LSB) and pixel value differencing (PVD) methods have been used for increasing hiding space. The method has good imperceptibility and embedding capacity. The proposed approach has focused only on payload and imperceptivity. The technique can be improved in the security domain by incorporating an encryption algorithm. In 2020, Sahu and Swain [37] have suggested Dual-layer based reversible image steganography using modified least significant bit (LSB) matching. In this approach double layer embedding has been performed to improve image quality. In the first layer, two bits of the secret data are embedded into each pixel using modified LSB matching to develop intermediate pixel pair (IPP). Whereas, in the second layer, four bits of secret information are embedded using IPP. The technique is good enough to provide a good payload with better image imperceptivity. The proposed approach can be enriched by introducing security algorithms to enhance the security of the data embedded in an image. Also, the proposed method can be extended to color images and can be improved to reduce processing time. In 2017, Hussain et al. [38] have presented a data hiding method to achieve high payload, good visual quality, and maintain security. This method is based on two novel approaches: parity-bit pixel value difference (PBPVT) and improved rightmost digit replacement (iRMDR). In this method, the cover image is separated into two non-overlapping pixel blocks. The embedding algorithm PBPVD (higher level ranges) or iRMDR (lower level ranges) are selected according to the difference value between two pixels in each block. The PBPVD technique increases embedding capacity and iRMDR attains good visual imperceptivity. However, the method can be improved by establishing a security related algorithm to improve the reliability of the method against attacks. Further, the scheme can be extended for color images also.

Table 1 Pros and cons of different special domain based image steganography techniques

Technique	Pros	Cons
AbdelRaouf [35]	• Good image quality • Good embedding capacity	• Less secure
Hussain et al. [36]	• Considerable imperceptivity • Good embedding capacity	• Less secure
Sahu and Swain [37]	• Enough payload • Better image imperceptivity	• Less secure • Analyzed only on grayscale images • Processing time is more
Hussain et al. [38]	• Increases embedding capacity • Attains considerable visual imperceptivity	• Less secure
Malik et al. [39]	• Maintains image quality • Good payload	• Less secure
Kumar et al. [40]	• Considerable payload	• Less secure • Low image quality
Chakraborty and Jalal [41]	• Good payload • Better image quality	• Less embedded data security
Lin et al. [42]	• Considerable image quality	• Less payload • Less secure
Parah et al. [43]	• Considerable image quality • Better payload	• Less secure • Takes more time for the embedding process
Li et al. [44]	• Enhanced payload than compared methods • Good visual image quality	• Tested only on grayscale images • Less secure
Saha et al. [45]	• Increased payload • Reduces image distortion	• Less secure
Shen et al. [46]	• Good embedded efficiency • Considerable image quality	• Less secure • Analyzed only on grayscale images • Computationally inefficient
Bairagi et al. [47]	• Secure than existing steganography approaches	• Less payload
Rim et al. [48]	• Good security • Good imperceptibility	• Capacity is less
Hassan and Gutub [49]	• Huge payload	• Poor image quality • Less secure • Takes more time for embedding the data

In 2018, Malik et al. [39] have come-up with a new data hiding approach using absolute moment block truncation coding (AMBTC) compression. In this method, AMBTC compresses the cover image to embed important data into the compressed pixel values. The method is able to maintain image quality with a good payload. However, security can be improved by incorporating cryptographic approaches. In 2019, Kumar et al. [40] have proposed an enhanced method of data hiding using absolute moment block truncation coding (AMBTC) using pixel value differencing (PVD) and hamming distance. The cover image is compressed with AMBTC and is divided into three sections: smooth, less-complex, and highly-complex blocks. One bit per pixel is embedded into smooth blocks, 8-bits are embedded into a less-complex block using hamming distance calculation, and more data bits are embedded into a highly-complex block using the PVD technique. The method produces a good embedding space. However, can be extended in the security domain to further increase security to the data.

In 2020, Chakraborty and Jalal [41] have put forth a novel image hiding method using local binary pattern (LBP). In this scheme, the cover image is separated into 3×3 non-overlapping blocks. The reference pixel of each block is encoded using LBP. The encoded image is XORed with the secret image. The image has been shuffled further to embed secret image bits in the LSB of the cover image. The method has strong statistical features against attacks. The presented method can be further extended to embed data by applying payload-specific hand-crafted descriptors. In 2020, Lin et al. [42] have proposed a new image hiding method for Dynamic GIF (Graphics Interchange Format) images. The presented scheme is based on the Palette sort. In this method, the cover image is decomposed into frames (static GIF image). A new distortion function is applied to all frames. The data is then embedded into these frames to form the stego frames. In this technique, the data is secured by hiding it into an image but with less payload. In 2018, Parah et al. [43] have presented computationally efficient and reversible data hiding method

for secure electronic health record (EHR) communication. In this method, modular arithmetic has been used for embedding EHR into a medical image. Prior to embedding, the cover medical image is scaled up using the pixel reputation method. The proposed scheme has improved image quality with a better amount of payload but takes a good amount of time for embedding data into an image. The security of the method can be improved by implementing some encryption method. The technique can also be extended to color images to increase EHR embedding capacity.

In 2021, Li et al. [44] have suggested a high capacity image steganography technique. The method has used retracing extended Sudoku (RE-Sudoku) reference matrix for data embedding. The paper has an enhanced payload with good image quality. The method can be improved in security domain to enhance its superiority. Also, the method can be analyzed on color images to show its generality. In 2020, Saha et al. [45] have come up with a new image hiding method using a hashed-weightage Array. The method is based on extended exploiting modification direction (EMD) that creates less distortion in an image. The presented method has improved payload and reduces distortion of an image than the existing method. The security of proposed scheme can be enhanced by encrypting the secret data. In 2018, Shen et al. [46] have proposed a new data hiding method based on improved exploiting modification direction (EMD) and interpolation techniques with consideration of human visual system (HVS). In this scheme, the cover image is separated into various 3×3 non-overlapping blocks. The presented method hides data into each block by calculating the neighbor mean value and the difference value. The discussed method has improved embedding efficiency and quality than the traditional EMD technique. The presented method takes more time for processing the task. The scheme can be enriched by applying stegna-analysis resist method to improve security. Moreover, the technique can be improved by applying it to color images as well.

In 2016, Bairagi et al. [47] have put forth an efficient image steganography method for secure communication in the Internet of Things (IoT) infrastructure. This article has presented three information hiding approaches using RGB image steganography. In this method, data has been embedded in an image using a secret key and carrier information. The technique has improved the security of the data than the traditional steganographic techniques. This work can be enhanced by applying encryption approaches for security improvement. In 2020, Rim et al. [48] have presented a Beta chaotic map based image hiding method. The method used a Beta chaotic map to sort the embedding positions of an image. The simple least significant bit (LSB) technique has been used to embed data into an image. The technique has provided good security to the data than the traditional steganographic approaches. However, the method can be improved to gain more capacity with good image quality. In 2021, Hassan and Gutub [49] have introduced an efficient image reversible data hiding (RDH) approach. In this method, interpolation optimization has been used to scale up the original image before embedding. The advantage of this method is a good image quality with a huge payload. However, the cryptographic technique can be applied to the secret data before embedding to enhance security.

2.2 Edge based technique

This subsection discusses different edge-based image steganography methods. Table 2 highlights the pros and cons of these techniques after analyzing the surveyed papers.

In 2021, Atta and Ghanbari [50] have put forth a new data hiding mechanism based on dual tree complex wavelet transform (DT-CWT). In this method, the cover image has been divided into subbands and neutrosophic edge detector (NSED) has been applied on these subbands to attain edge areas. The secret data is embedded into the detected subband edge regions of an image. The method has been able to get good imperceptivity with a good amount of payload. However, needs to secure data by applying some encryption algorithms. In 2019, Dhargupta et al. [51] have proposed an image steganography approach using Fuzzy edge detection (FED). In this approach, edges of the cover image are detected by FED to embed data into edge areas of an image. Data to be embedded in an edge region depends upon the Euclidean distance and is determined by the Gaussian function. The technique shows good embedding capacity, but with an increase in payload, its quality gets degraded. The method has been applied only on grayscale images. In 2019, Ahmadian and Amirmazlaghani [52] have suggested a secret image sharing steganography scheme. This method is dependent on fully exploiting modification direction (FEMD) and edge detection technique to embed data into the cover image. The method has been able to improve image quality than the existing methods, but, has less embedding space. In 2018, Kich et al. [53] have offered an edge detection method based image steganography method. In this approach, secret information has been dissimulated into edge pixels of an image using modified simple linear iterative clustering (M-SLIC) algorithm. The technique has a good payload, robustness, and imperceptivity. However, the scheme can be also upgraded in the security domain. In 2018, He et al. [54] have suggested a reversible information hiding method using edge information. The method has been proposed for high dynamic range (HDR) color images. The data has been embedded into HDR color images by using edge information. The approach has achieved less visual distortion after embedding secret data into an image. However, the security of the data by preprocessing has not been considered to increase data security. In 2018, Gaurav and Ghanekar [55] have introduced an edge region detection

Table 2 Pros and cons of different edge based image steganography techniques

Technique	Pros	Cons
Atta and Ghanbari [50]	• Good imperceptivity • Good amount of payload	• Less secure
Dhargupta et al. [51]	• Good embedding capacity	• More distorted image • Less secure
Ahmadian and Amirmazlaghani [52]	• Improved image quality	• Less embedding space
Kich et al. [53]	• Robust • Imperceptible	• Less secure • Low payload
He et al. [54]	• Good payload with considerable visual image quality	• Less secure
Gaurav and Ghanekar [55]	• Good image quality • Better payload	• Less secure
Prasad and Pal [56]	• Good payload • Considerable image quality	• Tested only on grayscale images • Less secure
Mukherjee and Sanyal [57]	• Good image quality • Good hidden data capacity	• Less secure
Kadhim et al. [58]	• Good embedding capacity • Good image quality	• Less secure
Ghosal et al. [59]	• Increased payload • Increased image quality	• Less secure
Ghosal et al. [60]	• Improved payload • Less image distortion	• Less secure
Banik et al. [61]	• Good image quality • Good payload	• Less secure • Implemented only on grayscale images
Wang et al. [62]	• Good payload • Better image quality	• Less secure
Tripathy and Srivastava [63]	• Can hide the vast amount of data into an image • Good visual image quality	• Less secure
Tuncer and Sonmez [64]	• Good capacity • Good visual quality	• Less secure

based image steganography technique. The secret data has been embedded into the least significant bit (LSB) bits of edge pixels. The approach has good image quality with a better payload. However, can be improved to insert a cryptographic approach along with a steganographic method to ensure better security to the data. In 2020, Prasad and Pal [56] have introduced a new image steganography algorithm, using edge detector and modulus function. For embedding, the modulus function has been used, whereas, edge detector has been used to find edge locations to embed data into edge areas. The method has been tested only on greyscale images. Further, the technique can be improved by introducing an encryption algorithm to increase security.

In 2019, Mukherjee and Sanyal [57] have presented an edge based image steganography method with a variable threshold. The edges of an image have been detected by the Sobel edge detector with respect to the threshold key. These detected regions are used to hide secret information. The scheme has gained good image quality with considerable hidden data capacity. The suggested method can be further improved by incorporating encryption schemes to the embedding data before hiding. In 2018, Kadhim et al. [58] have put forth an adaptive image steganography technique. The technique is based on edge detection over dual-tree complex wavelet transform (DT-CWT). Edge regions of an image have been detected using the canny edge detection method. Even though the method has good embedding capacity and image quality, however, can be extended in the security domain to increase data security against attacks. In 2018, Ghosal et al. [59] have put forth an image steganography technique based on the Laplacian of Gaussian (LoG) edge detector. In this approach, the data has been embedded into all non-edge pair, edge pair and mixed pair of an image. By this technique, the burden of payload into the traditional method of embedding all data into edge areas only has been reduced. The method no doubt has increased payload and image quality. However, the technique can be further enhanced in the security domain. In 2021, Ghosal et al. [60] have suggested an image hiding approach based on the Kirsch edge detector. In this method, the data has been embedded into both edge and non-edge regions of an image in such a way that image distortion is minimized. The

method has improved payload with less image distortion. The proposed method can be improved by applying a cryptographic method to enhance security. In 2019, Banik et al. [61] have discussed an image steganography method for embedding capacity improvement. The technique has used Kirsch detector to find the edge regions of an image for data hiding. The threshold value has been used as a key to embed data into edge areas of an image. The technique has good image quality with a good payload. The algorithm has been implemented only on greyscale images. Thus, the method can be extended to color images as well. In 2020, Wang et al. [62] have presented a high capacity hybrid steganography method based on the least significant bit (LSB) and hamming code (HLAH). In this technique, the color cover image is separated into 9×9 blocks and the red (R) plane is extracted. The LSB of the R plane is set to '0' and then the canny edge detection technique is used to find the edges of a plane. The method has used the canny edge detection technique to find edges. The data is embedded into the non-edge and edge regions using LSB and (3,1) hamming code. The method has been able to provide a good payload with better image quality than the existing methods. However, the security of the algorithm can be improved by encrypting the secret data prior to embedding.

In 2020. Tripathy and Srivastava [63] have proposed an edge based data hiding technique using Modulus-3 strategy and comparative analysis. In this method, the data has been changed into ternary data and has been embedded into edge areas of an image using the Modulus-3 strategy. The edge regions have been detected with Sobel, Prewitt, Canny, and Laplacian edge detectors. The method has been able to hide a vast amount of data into an image with good visual image quality. However, the security of the secret data can be further improved by introducing an encryption method along with the proposed algorithm. In 2019, Tuncer and Sonmez [64] have introduced the image steganography algorithms based on edge detectors and a 2^k correction scheme. The method has used Sobel, Canny, Laplacian of Gaussian (LoG), block based edge detection (BED), and hybrid edge detectors (HED) to find edge pixels of an image. These detected regions have been used to embed data into it using the least significant method (LSB) and 2^k correction method. The technique has the good capacity with good visual quality, but, has not improved much upon security parameter.

2.3 Frequency domain technique

A thorough summary of the techniques reviewed under the frequency domain is given as follows and their pros and cons are pointed out in Table 3.

In 2021, Abdel-Aziz et al. [65] have offered an improved data hiding method for securing color images. In this work, the authors have used a hyper chaotic map and left-most significant bit (LMSB) embedding method to embed data into an image. In this approach, the cover image has been first encrypted using a hyper chaotic map to form the encrypted image and is then converted into the YCbCr channels. Of them, the first channel (Y) has been divided into non-overlapping blocks using the DCT technique. The resulted blocks are quantized and secret data has been embedded into frequency coefficients of these quantized discrete cosine transform (DCT) blocks using Huffman coding. The output stego image is further XORed with the remaining two channels (CbCr) to form the encrypted stego image. The scheme has good security and image quality. However, an encrypted form of stego image can suspect the presence of data. Also, the technique can be extended for embedding any type of data into color images. In 2021, Yao et al. [66] have presented a reversible data hiding (RDH) approach for dual JPEG images. In this method, the cover image is preprocessed to attain DCT coefficients and to ascribe embedding space. Then, secret data has been embedded into obtained frequency coefficients of image pixels using the dual-JPEG RDH scheme. The technique has gained a considerable embedding space with good visual image quality. However, the secret data to be embedded has not been preprocessed to improve data security. In 2018, Liu and Chang [67] have suggested a reversible data hiding (RDH) technique for JPEG images for hiding a great amount of data. In this approach, the discrete cosine transform (DCT) technique has been used to gain the coefficient values for non-overlapping 8×8 blocks. The quantization method has been applied to each block of an image to attain JPEG quantized block. Then, the AC coefficients are scanned in a zigzag direction to embed secret data into non-zero elements. The proposed method has been able to gain good image quality with considerable payload, but, the enhancement of security to the data with preprocessing has not been taken into consideration. In 2018, Attaby et al. [68] have put forth a novel data hiding approach using discrete cosine transform (DCT) to embed data into JPEG images. The difference value of two DCT coefficients using modulus 3 has been applied to insert two secret data bits into the values of the coefficients of an image. This significantly reduces the image distortion with improvement in image embedding space. However, the data security of the scheme can be improved by applying a cryptography approach to secret information before embedding. In 2016, El-Rahman [69] has given a new steganographic tool to hide data into the frequency domain of an image using the discrete cosine transform (DCT) method. The technique has hidden the important information about nuclear reactor in the middle frequency. The scheme is able to protect image quality with a high considerable amount of embedding capacity. However, the confidential information of the nuclear reactor needs to be more secure from

Table 3 Pros and cons of different frequency domain based image steganography techniques

Technique	Pros	Cons
Abdel-Aziz et al. [65]	• Good embedding space • Good security • Better image quality	• Complex • Tested only on grayscale images
Yao et al. [66]	• Considerable embedding capacity • Good visual image quality	• Less secure • Complex
Liu and Chang [67]	• Good image quality • Considerable payload	• Less secure • Complex
Attaby et al. [68]	• Reduces image distortion • Improves image embedding space	• Less secure • Complex
Mohamed et al. [70]	• High embedding capacity • Considerable image quality • Secure	• Complex
Rabie et al. [71]	• Better payload	• Poor image visual quality • Complex • Less secure for embedded data
Saidi et al. [72]	• Good payload • Secure	• Less imperceptibility • Complex
Nipanikar et al. [73]	• Good image imperceptivity • Good payload	• Less secure • Complex
Nevriyanto et al. [74]	• Good image quality	• Less payload • Complex • Less secure
Miri and Faez [75]	• Good image quality • Considerable embedding space	• Less secure • Complex
Kalita et al. [76]	• Good visual quality of an image • Considerable embedding capacity	• Less secure • Complex
Ghosal et al. [77]	• Good payload • Good image quality	• Less secure • Complex • Takes good time for completing embedding and extraction process
Ma et al. [78]	• Large data hiding capacity • Good image imperceptivity	• Less secure • Complex
Murugan and Subramaniyam [79]	• Provides good payload while preserving image quality • Secure than the existing techniques	• Complex

any thefts. Therefore, encryption of important information before embedding could be more effective for data security. In 2020, Mohamed et al. [70] have presented an L*a*b* (luminance channel 'L*' and chrominance channels 'a*and b*') color space image steganography technique using quad-trees. The method has applied the quad-tree of the gray-scaled cover to the RGB of the cover image. The resultant blocks of the quad-tree are transformed to L*a*b* color space using 2dimentional-discrete cosine transform (2D-DCT) to embed data into the largest zero areas of DCT. The method has considerable embedding capacity, good image quality, and secure than the existing spatial and frequency domain steganography methods. However, the technique is complex. In 2018, Rabie et al. [71] have suggested increased embedding space and image quality data hiding scheme based on transform domain mechanism. The presented scheme uses the quad tree segmentation method to divide the blocks of the cover image. In each block, quantization step and piecewise linear curve fitting are used to hide secret data in the least significant areas of discrete cosine transform (DCT) coefficient areas. The method has tried to gain a better image payload. However, the data is embedded directly without pre-processing that may lead to security issues. In 2017, Saidi et al. [72] have put forth a new steganographic approach Based on discrete cosine transform (DCT) and chaotic map. The presented approach is used to find coefficients of the cover image. Piecewise linear chaotic map (PWLCM) has been used to scramble embedding positions to improve security to the embedding data. The algorithm has a good payload, however, the technique has poor image imperceptivity. Also, the technique can be improved further to resist any statistical attacks.

In 2018, Nipanikar et al. [73] have discussed a sparse representation based image steganography technique using particle swarm optimization (PSO) and discrete wavelet transform (DWT) approaches. These approaches have been used to locate the appropriate pixels for embedding speech signal in the cover image. The method is able to achieve good image imperceptibility and payload. However, the algorithm can be extended in the security domain to enhance data security. In 2018, Nevriyanto et al. [74] have presented an image steganography method using discrete wavelet transform (DWT) and singular value decomposition (SVD) techniques. In this scheme, a text file has been converted into an image to form a watermark for embedding it into an image. The secret watermark has been embedded into the frequency coefficients of an image using the SVD method. The method can be further made secure enough against attacks by incorporating encryption methods on the data and can be also extended to color images. In 2018, Miri and Faez [75] have introduced an image steganography technique for hiding important data into frequency coefficients of an image. This method has used the integer wavelet transform (IWT) method to obtain the frequency coefficients of an image. The method has been analyzed on greyscale images that can be extended to color images. The security of the data can be further improved by introducing encryption methods to the secret data before embedding. In 2019, Kalita et al. [76] have proposed a new steganography method using integer wavelet transform (IWT) and the least significant bit (LSB) substitution method. To estimate the embedding capacity, the coefficient value differencing method has been applied. The scheme has good visual quality of an image and considerable embedding capacity. However, the data can be secured from statistical attacks by introducing encryption algorithms. In 2021, Ghosal et al. [77] have presented exploiting Laguerre transform (LT) based image hiding method. In this scheme, the cover is separated into m-pixel non-overlapping groups. Each pixel of these groups is then transformed into its equivalent coefficients using LT. The secret data is embedded into these coefficients. The resulted pixels are adjected to minimize distortion and have been recomputed by applying inverse LT (ILT). The presented scheme has been able to increase payload with good image quality but takes more time for completing the process. However, the method can be secured by encrypting the data. In 2019, Ma et al. [78] have come up with a new reversible data hiding (RDH) approach for medical images. The method is based on block classification and code division multiplexing (CDM). In this scheme, the non-overlapping blocks of the medical image are categorized into smooth and texture groups by calculating mean square error (MSE). The secret information has been embedded into transformed frequency coefficients using the integer-to-integer discrete wavelet transform (IDWT) technique of the texture block. The method has large data hiding capacity with good image imperceptibly. Security to the secret data can be further improved by applying cryptography approaches to the secret data prior to embedding. In 2020, Murugan and Subramaniyam [79] have proposed an image steganography technique to ensure the data security transaction over an insecure network. The data has been embedded into coefficient values of an image using the alpha factor. The image pixels have been transformed with the 2dimentional-Haar discrete wavelet transform (2D-Haar DWT) to gain four sub-bands. The method has good embedding space while preserving image quality than the existing schemes. Also, the proposed method is secure than already existing frequency domain techniques. However, the proposed method is complex.

2.4 Joint Crypto-stego schemes

This subsection includes the reviewed papers of different dual security image steganography techniques. These techniques have encrypted the secret data/ secret image with either standard encryption method or chaotic method before embedding to provide double layer security to the secret data. The pros and cons of different dual security image steganography methods are shown in Table 4. The following subsections discuss the different combined image steganography and encryption techniques.

a) **Simple domain crypto-stego schemes**

The review of different special domain based image steganography and encryption methods are explained below:

In 2021, Maji et al. [80] have presented a spatial domain based image steganography method in which higher order pixel bits have been used to embed data. To encrypt data, XOR operation has been used to enhance security. Since the method has been implemented on the greyscale image. Thus, the presented approach can be extended to color images to prove its generality. In 2017, Sharif et al. [81] have presented an image steganography technique based on a 3-dimensional chaotic map. In this method, the pixel position for embedding changes with the change in the cover image. Thus, makes the system secure against any statistical attacks. However, the method can be improved in terms of complexity. In 2020, Gambhir and Mandal [82] have proposed chaos based least significant bit (CLSB) steganography method. The technique has used logistic map chaotic function to develop random numbers. The scheme shows good security and image quality results. However, can be improved further to increase embedding space to hide huge data into an image. In 2019, Prasad and Pal [83] have proposed logistic map based image steganography.

Table 4 Pros and cons of different dual security image steganography techniques

Technique	Pros	Cons
Maji et al. [80]	• Good embedding space • Good image quality • Secure	• Tested only on grayscale images
Sharif et al. [81]	• Secure against statistical attacks • Better payload • Considerable image quality	• Complex
Gambhir and Mandal [82]	• Secure • Better image quality	• Less embedding capacity
Prasad and Pal [83]	• Secure • Considerable image quality	• Analyzed on grayscale images only
Mohammad et al. [84]	• Secure for visual content authenticity in social networks	• Complex • Less payload
Alotaibi et al. [85]	• Considerable amount of payload	• Low visual quality of an image
Mathivanan and Balaji [86]	• Secure	• Less embedding space
Abdelwahab et al. [87]	• Good payload • Considerable image quality	• Complex
Parah et al. [88]	• Secure • Authentic • Good image quality • Less processing time	• Analyzed only on greyscale images thus has limited capacity
Parah et al. [89]	• Good capacity • Good image quality • Secure • Low embedding time	• Complex • More extraction processing time
Delmi et al. [90]	• Secure • Good image imperceptivity	• Low payload
Sharma et al. [91]	• Better image quality • Considerable payload	• Complex
Kaushik and Sheokand [92]	• Secure • Better image quality	• Less embedding capacity
Panday [93]	• Secure • Good image quality	• Complex • Low embedding space
Elhoseny et al. [94]	• Good image quality • Secure	• Low payload • Complex
Duan et al. [95]	• Analyzed on both grayscale and color images • Secure • Better capacity • Considerable image quality	• Complex
Subhedar and Mankar [96]	• Secure • Good image quality	• Low payload • Implemented only on grayscale images • Complex
Eyssa et al. [97]	• Secure • Considerable payload and image quality	• Complex
Kaur and Singh [98]	• Good payload • Secure	• Applied only on grayscale images • Complex • Poor image quality
Hureib and Gutub [99]	• Good embedding space • Better image quality	• Not tested for statistical attacks to claim better security
Hureib and Gutub [100]	• Secure • Better visual quality of an image	• Low payload
Samkari and Gutub [101]	• Good image quality • Secure	• Complex
Denis and Madhubala [102]	• Good image quality • Secure	• Low embedding space • Complex
Manikandan et al. [103]	• Considerable image quality	• Low hiding capacity

Table 4 (continued)

Technique	Pros	Cons
Ogundokum et al. [104]	• Good visual quality of an image • Secure	• Low payload
Prasanalakshmi et al. [105]	• Considerable payload • Good image quality	• Complex

This method has used the least significant bit (LSB) and pixel value differencing (PVD) techniques to embed data into the cover image. The embedding data is encrypted using a logistic map to improve security to the data. The proposed algorithm has attained better security. The technique can be modified in a different way to achieve better visual image quality and can be extended to color images also. In 2017, Mohammad et al. [84] have offered image steganography for visual contents authenticity. The method uses color model transformation, three-level encryption algorithm (TLEA), Morton scanning (MS). The data has been embedded with the direct least significant bit (LSB) substitution method using MS. TLEA has been used to encrypt data. The scheme provides the best algorithm for visual content authenticity in social networks. While the technique is complex and has less payload. In 2019, Alotaibi et al. [85] have proposed a secure framework for safe data transmission in mobile devices using hash, cryptography, and steganography. The proposed method has used a hash function for storing the secret password, cryptography with AES method for encrypting password, and LSB method for hiding encrypted password into an image. The method is able to provide a considerable amount of payload but has low visual quality of an image. In 2021, Mathivanan and Balaji [86] have suggested a QR code based color image stego-crypto technique. The method uses dynamic bit replacement and logistic map for embedding and encryption respectively. In this approach, the secret data is converted into 2D binary using base64 encoding method and QR code generator and is then embedded into an image using dynamic bit replacement technique. The image is then scrambled using a logistic map. The method is secure against differential attacks but is able to hide a low amount of secret data. In 2021, Abdelwahab et al. [87] have put forth an efficient image steganography technique to hide data for safe data transmission. In this scheme, plain text is encrypted using the RSA method and is embedded into the YCbCr components of an image using the LSB approach. The resulted stego image is then compressed using Huffman coding, Run Length coding (RLC), or DWT to form compressed stego image. The method has good amount of payload with considerable image quality. However, the scheme is complex.

b) **Edge based crypto-stego techniques**

Few edge detections based image steganography techniques along with data encrypting approaches are discussed as under:

In 2021, Parah et al. [88] have presented efficient security, high payload, and reversible electronic health record (EHR) data hiding approach. In this method, the cover image is scaled up with the pixel reputation method (PRM) and then the boundary conditions are applied to the image. The resulted image is divided into 2×2 blocks to embed data first into counter diagonal pixels and then to the main diagonal pixel after checksum computation. The EHR is secured by adding a watermark and applying the RC4 encryption method. The encrypted data is divided into 3-bit chunks and has been then embedded into the pixels after applying the left data mapping (LDM) method. The scheme has increased security to the data and has authenticated its originality. However, with a high payload, the quality of an image can be enhanced by testing the method to color images also. In 2016, Parah et al. [89] have proposed a new information hiding technique based on a hybrid edge detection method. In this scheme, the color image is separated into three planes (red, green, blue). The data is embedded into edge regions and non-edge regions of green and blue planes by making use of a hybrid edge detector. Whereas, the red plane is used to hold the bit status of green and blue planes. In order to authenticate and detect tempering the data, a fragile watermark is embedded. Before embedding, the secret information is encrypted using the RC4 algorithm. The algorithm is able to increase capacity with good image quality. Further, the security of the method is provided to the data by encrypting it prior to embedding. However, the time complexity of the method can be reduced by reducing the data extraction time. In 2020, Delmi et al. [90] have discussed the image hiding approach using the edge adaptive method and chaos cryptography technique. In this technique, the data has been encrypted using the Arnold Cat Map function. Whereas, the data has been embedded into the edge region of an image located by a canny edge detector. The technique although has increased security to the data. However, can be enhanced to increase payload with good image quality. In 2021, Sharma et al. [91] have suggested crypto-stego approach

to prevent data from attacks. In this method, Rabin cryptosystem is used to encrypt the secret data, Arnold transform has been used to scramble the data, and the resulted data has been embedded into the edges of multiple images. The framework is able to provide better image quality with a considerable payload. However, the proposed approach is complex.

c) **Frequency domain crypto-stego techniques**

Different frequency domain based image steganography together with data encryption surveyed methods have been discussed in this subsection:

In 2016, Kaushik and Sheokand [92] have put forth a steganography scheme based on chaotic least significant bit (LSB) and discrete wavelet (DWT) approaches. In this method, the data is encrypted using a logistic map. Whereas, the encrypted data is embedded into frequency coefficients of the cover image using DWT by 3–3-2 LSB insertion scheme. The security of the proposed method has been increased by using the chaotic method. The method has good image quality but has less embedding capacity. In 2020, Panday [93] has suggested a new medical image steganography approach using a bit mask oriented generic algorithm (BMOGA). BMOGA has been used together with cryptographic features to encrypt data. In this approach, data has been embedded in the frequency coefficients of an image. Discrete wavelet transform (DWT) (1-level & 2-level) has been used to find frequency coefficients. The technique is secure and imperceptible, however, can be enhanced to gain a good payload. However, the scheme can be further modified to reduce the complexity of the algorithm. In 2018, Elhoseny et al. [94] have presented a secure medical data transmission model for internet of things (IoT) based healthcare systems. The method has used 2-D discrete wavelet transform (2D-DWT) to conceal data into both grayscale and color images. The secret information has been encrypted using a hybrid encryption scheme using advanced encryption standard (AES) and Rivest, Shamir, and Adleman (RSA) algorithms. The technique shows good image quality with good data security. However, the technique is complex.

In 2020, Duan et al. [95] have proposed a high-capacity image hiding scheme. In this method, the data have used encrypted with elliptic curve cryptography (ECC) approach. Discrete cosine transform (DCT) is applied to the secret image prior to encryption. A deep neural network has been used to increase the payload of the cover image. The method has been applied to both gray images as well as a color images. The method shows better security to the data. However, can be improved to reduce algorithm complexity. In 2018, Subhedar and Mankar [96] have presented image steganography using curvelet transform (CT) to embed secret information in the selected cover image. In order to obtain curvelet coefficients, level 6 CT has been applied to the cover image. Encryption data has been embedded into appropriate blocks by using standard deviation. Whereas, image block has been replaced with secret data block using spread spectrum when the deviation is higher than a threshold. The resulted stego image is obtained by applying inverse CT. In this technique, security has been heightened by encrypting the data using Arnold transform. However, it can be enhanced in payload and quality domain by testing it on the color image also. Further, the method is complex. In 2020, Eyssa et al. [97] have introduced an efficient image steganography method. In this approach, the data has been encrypted with the Baker map together with a discrete cosine map (DCT). The secret message in the presented method has been embedded into the values of the coefficients of an image. The security of the system has been increased. However, with a good amount of payload the image quality is less that needs to be enhanced. In 2021, Kaur and Singh [98] have introduced a new data hiding method based on discrete cosine transform (DCT) and coupled chaotic map. The secret data in this approach has been encrypted using coupled chaotic map of logistic and sine map. In this approach, the data has been embedded into the DCT coefficients of an image. The technique has a good payload, but, has been applied only on greyscale images and is complex.

d) **Medical image crypto-stego techniques**

The review of various medical image steganography together with data encryption has been discussed in this subsection:

In 2020, Hureib and Gutub [99] have proposed a combined cryptography and image steganography approach to enhance security in medical health data. In this method, Elliptic curve cryptography has been used to encrypt text before hiding. Then, the encrypted text is embedded into image pixels to hide its presence from the person who is not authorized. The technique has a good payload and image quality, however, it has not been tested for various attacks, like statistical attacks, etc. In 2020, another image steganography technique using elliptic curve cryptography has been presented [100]. The method has used 1-LSB and 2-LSB image steganography techniques to hide data into an image. The medical data has been embedded in the medical image after encrypting it with cryptography technique to improve data security. The method provides good image quality but has low embedding capacity. In 2019, Samkari and Gutub [101] have suggested a protecting mechanism for medical records against cybercrimes within the Hajj period. The method has used a 3-layer security system for medical record protection by encrypting data

using hybrid cryptography method and hiding encrypted data into an image to produce stego-image for sending through the internet. The presented approach has good image quality and is safe for data transmission, however, the method is complex. In 2021, Denis and Madhubala [102] have put forth hybrid data encryption and hiding model for medical data security over cloud-based healthcare systems. In this scheme, a hybrid encryption model using AES and RSA algorithms has been used to convert the original data into an encrypted form. Whereas, the 2D-DWT and Adaptive Genetic Algorithm (AGA) based optimal adjustment method to conceal encrypted medical data into an image for safe data transmission. The proposed technique provides good image quality and is secure. However, the approach is complex and has low hiding space. In 2021, Manikandan et al. [103] have proposed an image steganography technique to secure e-health. In this approach, the secret image is first encrypted with the XOR cipher encryption and is then embedded into the cove image using LSB method. The framework has considerable image quality but provides low embedding capacity. In 2021, Ogundokum et al. [104] have presented crypto-stego medical information securing model. This technique uses international data encryption algorithm (IDEA) and Matrix-XOR techniques for enhancing security to the internet of medical things (IoMT) for the medical records protection. In this method, secret data has been encrypted using IDEA and is then embedded into carrier image using XOR. The method provides good visual quality of an image and is secure for medical data transmission. However, space for transmitting data in a concealed manner should be increased. In 2021, Prasanalakshmi et al. [105] have recommended a secure clinical data transmission technique in the internet of things (IoT) using hyperelliptic curve (HECC) and cryptography techniques. This approach has used AES and Blowfish hybrid cryptography for medical data encryption and HECC for embedding encrypted medical data into a medical image. The generated embedded image is then compressed with the 5-level DWT to attain a good payload and better security. The technique provides good image quality with considerable payload, however, the technique is complex.

From the literature, it has been observed that the use of cryptography and steganography together is able to provide double layer security to the data. Cryptography protects data from hacks, and in particular chaos based cryptography can be the better option for encryption because of its ergodicity and dependence on initial condition properties. And, incorporating a steganography approach with cryptography improves data security by concealing it into digital media. Data hiding using chaotic maps to locate and create a random sequence of pixels enhances data security. Also, concealing secret information in edge regions improves payload, can prevent cover image from noticeable distortion, and thus prevents attacks. Moreover, it has been observed that cryptography and steganography have widened their applications almost in all spheres of life, like in e-health, IoT, mobile devices, system login security, cloud, etc.

3 Evaluation parameters

Evaluation parameters are the tools used to check the efficiency, validity, and superiority of an algorithm. Outcomes of the analyzed scheme with various methods whose values lie between expected ranges prove the strength of the technique. The most common characteristics of image steganography and data encryption analysis are explained below in subsections.

3.1 Visual quality analysis

Steganography method alters the image by storing secret information inside pixels that affects the visual quality of an image. However, changes incorporated in an image should not be perceived by the invaders. There are various standard evaluating methods used to confirm the image quality strength, like, mean square error (MSE), peak signal to noise ratio (PSNR), structural similarity index (SSIM), etc. Table 5 summarizes the MSE, PSNR, NCC, NAE, and SSIM values achieved by different image steganography techniques in this study.

a) **Mean square error (MSE):**
MSE is the error measurement of the stego image with respect to its original image. It helps in comparing the difference between the pixel values of an original image and stego image. Lesser MSE value provides better quality of an image [106]. Therefore, the MSE value should be near '0'. MSE can be calculated as follows:

$$MSE = \frac{\sum_{i=1}^{n} (p_i - p_i^{'})^2}{n} \quad (1)$$

where p_i and $p_i^{'}$ respectively represent the pixel values of the original and stego image. And, n represents the image size.

b) **Peak signal to noise ratio (PSNR):**
PSNR is the visual quality measuring tool that measures the image alteration in the stego image compared to its original image. It estimates the difference in pixel

Table 5 Different parameter comparison of existing image steganography techniques

Technique	Embedding Capacity (bpp)	MSE	PSNR (dB)	NCC	NAE	SSIM
AbdelRaouf [35]	2.08	84.2420	43.95	-	-	0.8320
Hussain et al. [36]	4.05	-	34.05	-	-	-
Sahu and Swain [37]	6.00	-	47.64	-	-	0.9949
Hussain et al. [38]	3.00	-	38.84	-	-	-
Malik et al. [39]	1.51	-	49.95	-	-	-
Kumar et al. [40]	0.77	-	30.79	-	-	-
Chakraborty and Jalal [41]	3.36	-	56.91	-	-	-
Lin et al. [42]	0.15	-	40.01	-	-	-
Parah et al. [43]	2.25	-	39.25	1.0000	0.0147	0.9691
Li et al. [44]	3.16	7.0713	39.63	-	-	0.9908
Saha et al. [45]	3.00	-	40.82	-	-	-
Shen et al. [46]	1.60	-	39.62	-	-	-
Bairagi et al. [47]	1.24	-	54.77	0.9999	-	-
Hassan and Gutub [49]	1.82	-	26.63	-	-	-
Atta and Ghanbari [50]	3.37	-	49.87	-	-	0.9978
Dhargupta et al. [51]	2.39	-	37.02	-	-	-
Ahmadian and Amirmazlaghani [52]	0.25	-	49.74	-	-	-
Kich et al. [53]	0.30	-	52.53	-	-	-
He et al. [54]	2.25	-	37.38	-	-	-
Gaurav and Ghanekar [55]	1.23	3.4049	42.80	-	-	0.9980
Prasad and Pal [56]	3.17	-	35.92	1.0000	-	-
Mukherjee and Sanyal [57]	2.00	1.3800	46.78	0.9995	-	-
Kadhim et al. [58]	5.40	-	47.08	0.9750	-	0.9998
Ghosal et al. [59]	2.08	-	45.59	-	-	-
Ghosal et al. [60]	1.65	1.5300	46.39	-	-	0.9965
Banik et al. [62]	2.00	-	42.34	-	-	-
Tuncer and Sonmez [64]	3.12	-	39.28	-	-	-
Abdel-Aziz et al. [65]	2.50	0.0005	77.24	0.9577	-	0.9262
Yao et al. [66]	0.15	-	56.66	-	-	-
Mohamed et al. [70]	21.83	-	37.01	-	-	0.9998
Rabie et al. [71]	20.81	-	31.79	-	-	0.9757
Saidi et al. [72]	1.00	-	30.13	0.9800	-	0.8700
Miri and Faez [75]	0.26	0.2788	53.68	-	-	-
Kalita et al. [76]	0.50	-	44.06	0.9999	-	-
Ghosal et al. [77]	1.00	-	49.38	-	-	-
Ma et al. [78]	0.35	-	51.24	-	-	0.9984
Murugan and Subramaniyam [79]	1.00	0.9076	49.56	-	-	-
Maji et al. [80]	0.90	0.4469	51.62	0.9994	-	0.9976
Sharif et al. [81]	12.00	-	38.75	-	-	-
Prasad and Pal [83]	2.29	-	38.79	-	-	-
Alotaibi et al. [85]	2.00	-	39.91	-	-	-
Abdelwahab et al. [86]	1.58	0.1600	43.45	-	-	-
Parah et al. [88]	0.55	-	53.12	0.9994	0.0019	-
Parah et al. [89]	2.25	-	41.98			0.9693
Delmi et al. [90]	0.10	-	45.30	-	-	-
Kaushik and Sheokand [92]	0.01	0.0100	68.13	-	-	-
Elhoseny et al. [94]	0.01	0.1288	57.02	1.0000		1.0000
Duan et al. [95]	23.45	-	40.57	-	-	0.9602
Subhedar and Mankar [96]	0.25	-	50.08	0.9999	-	0.9996

Table 5 (continued)

Technique	Embedding Capacity (bpp)	MSE	PSNR (dB)	NCC	NAE	SSIM
Eyssa et al. [97]	0.75	-	40.46	-	-	-
Kaur and Singh [98]	0.50	-	34.86	-	-	-
Hureib and Gutub [99]	24.00	-	70.94	-	-	-
Hureib and Gutub [100]	1.00	-	74.61	-	-	-
Manikandan et al. [103]	1.00	-	48.94	-	-	0.9580

values of a stego image in relation to its original image. For better image quality, the PSNR value should be more than 39dB [107]. PSNR values of different existing methods for different payloads are shown in Graphs 1, 2, and 3 below. PSNR can be measured as follows:

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right) \tag{2}$$

where MSE can be measured with Eq. 1.

c) **Normalized cross correlation (NCC):**

NCC is the relation determination method of an image. It investigates the relationship between the original image and its corresponding stego image. A better correlation between images indicates better image visual quality. Hence, NCC near '1' is considered as the good steganography algorithm [108]. NCC can be analyzed as follows:

$$NCC = \frac{\sum_{i=1}^{m}\sum_{j}^{n} O(i,j)S(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n}\left[O(i,j)\right]^2} \tag{3}$$

where O and S respectively denote the original and stego image pixel values.

d) **Normalized absolute error (NAE):**

NAE calculates the error between the original image and stego image to measure image quality after embedding. Error between the images should be less (near '0') to retain the image quality [88]. NAE can be expressed as follows:

$$NAE = \frac{\sum_{i=1}^{m}\sum_{j}^{n}\left(|O(i,j)S(i,j)|\right)}{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(O(i,j)\right)} \tag{4}$$

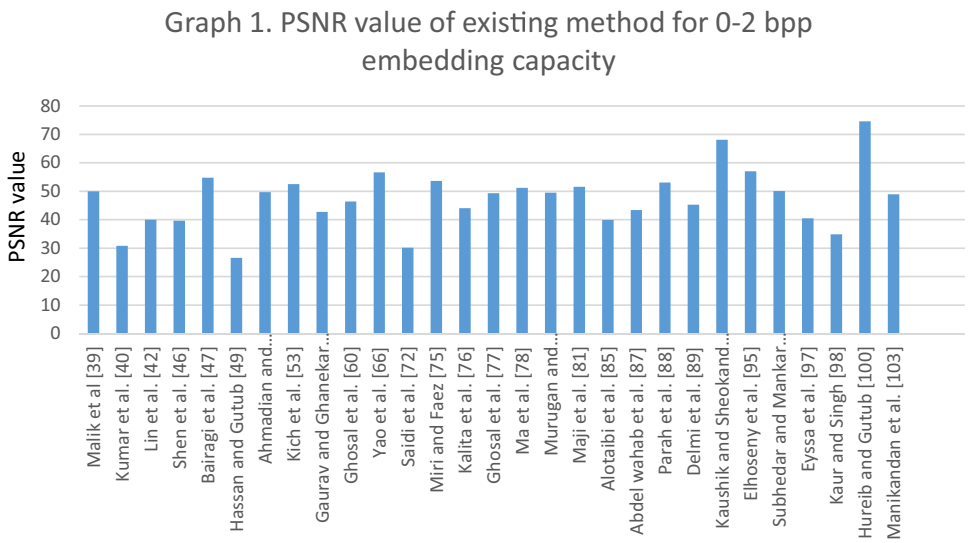
where O is the original image pixel value and S is the stego image pixel value.

e) **Structural similarity index (SSIM):**

SSIM is the visual quality measuring tool to checks the similarity between the original and stego image. The value of SSIM close to '1' (means 100%) represents the good image quality [109]. SSIM can be mathematically represented as follows:

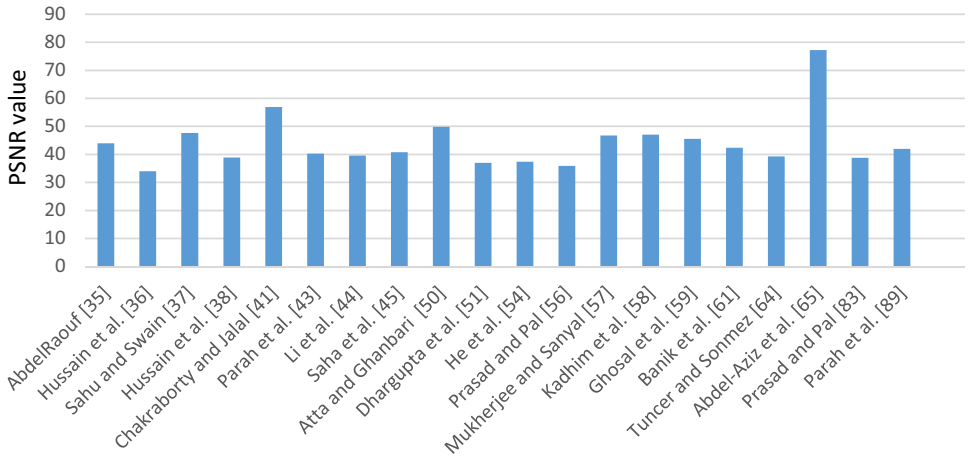
$$SSIM(i,j) = \frac{\left(2\mu_i\mu_j + C_1\right)\left(2\sigma_{ij} + C_2\right)}{\left(\mu_i^2 + \mu_j^2 + C_1\right)\left(\sigma_i^2 + \sigma_j^2 + C_2\right)} \tag{5}$$

where μ_i and μ_j are the mean intensity, σ_i and σ_j are the standard deviations, and σ_{ij} is the cross-covariance of images i and j respectively.



Graph 1 PSNR value of existing method for 0–2 bpp embedding capacity

Graph 2 PSNR value of exisitng method for 2–6 bpp embedding capacity



3.2 Embedding capacity analysis

Embedding capacity (EC) is another steganographic analysis parameter that calculates the number of secret data bits embedded into a per pixel of an image. The bits per pixel (bpp) should be more while preserving image imperceptivity. EC can be examined as follows:

$$EC(bpp) = \frac{number\ of\ embedding\ bits}{size\ of\ an\ image} \tag{6}$$

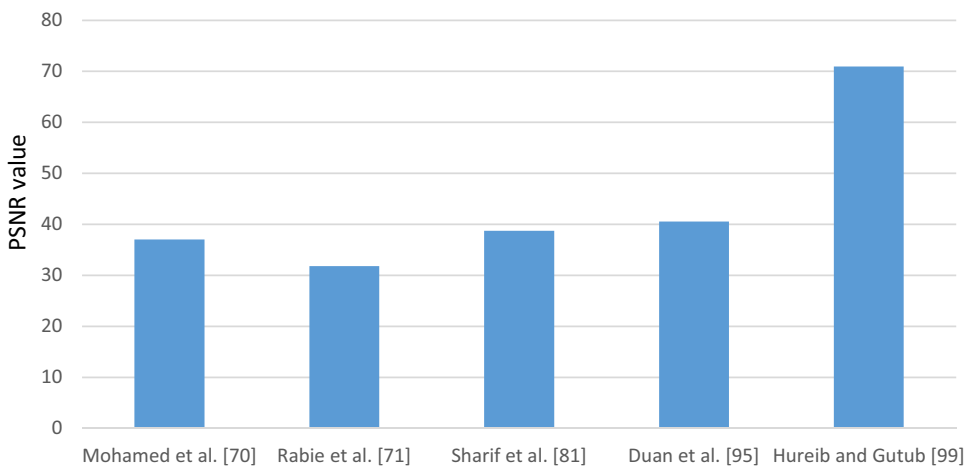
Here, size of an image is M × N × D, where M and N represents row and column of an image, and D represents the image pixel depth that can be either 1 or 3 depends upon the image selection (gray or color image). Therefore, maximum bpp for a grayscale image will be 8 and for color image it will be 24 (3 × 8 = 24). Embedding capacity for different image steganography techniques is shown in Table 5.

3.3 Differential analysis

The strength of an algorithm is tested by checking the sensitivity of an encrypted image with its original image and secret key. The strength of an encryption algorithm should be strong enough to resist attacks. The well-known differential analysis is a number of pixel change rate (NPCR) and unified average change intensity (UACI).

a) **Number of pixel change rate (NPCR):**
NPCR is the security evaluating method that analysis the single pixel changes in the original image. It checks

Graph 3 PSNR value of exisitng methods for 12–24 bpp embedding capacity



the sensitivity of the encrypted image compared to its original image and secret key. The acceptable NPCR value is 99.61% and closer to 100% is considered as the best encryption algorithm [110]. NPCR can be analyzed by the equation as follows:

$$NPCR = \frac{1}{mn}\sum_{i,j=1}^{mn} E_T(i,j) \times 100\% \tag{7}$$

$$Where, E_T = \begin{cases} 0, if I_o = I_e \\ 1, if I_o \neq I_e \end{cases} \tag{8}$$

where m and n are the image measurements. E_T is the total number of unequal units. And, I_o and I_e are the original image and encrypted image respectively.

b) **Unified average change intensity (UACI):**

UACI is the other encrypted image strength checking method. It calculates the average intensity of the difference between the original image and encrypted image. More percentage difference in intensities ensures a good UACI value and the lowest acceptable UACI value is 33.44% [110]. UACI can be calculated by the equation as follows:

$$UACI = \frac{1}{mn}\left(\sum_{i,j=1}^{mn} \frac{\left|I_o(i,j) - I_e(i,j)\right|}{255}\right) \times 100\% \tag{9}$$

where I_o and I_e are respectively the original and encrypted images. And, m and n are the image measurements.

3.4 Entropy analysis

Entropy is the average information per bit existing in an image. It checks the pixel randomness of an encrypted image. The average range of entropy is between 0 to 8 and close to 8 for 8 bit is considered as the best entropy value [111]. Entropy can be computed as follows:

$$E(S) = -\sum_{i=1}^{n} P(c_i)\log_2 P(c_i) \tag{10}$$

where S represents symbol collections, $c_i \in S$, $P(c_i)$ represents probability and n is the symbol number.

3.5 Key analysis

The key analysis is the main tool of an encryption algorithm for checking algorithm strength. The algorithm strength depends on key analysis. It can be checked in two ways: key space and key sensitivity analysis. Key space checks the size of the secret key used for encrypting an image. The larger size of the secret key makes the system secure against attacks, as it will be difficult for the unauthorized user to get the exact same key. Key sensitivity checks the sensitivity of the secret key to the changes made. Even a single bit change in the original key results in an altogether different image or unrecoverable image.

3.6 Statistical analysis

Statistical analysis checks the robustness of an encrypted image against attacks. The commonly used statistical analyses are histogram analysis and correlation coefficient for testing its robustness against attacks.

a) **Histogram:**

Histogram analysis represents the image by the number of data points within a definite range. The histogram gives the pixel distribution or uncommon forms of an image. Histogram analysis can be checked on stego image or encrypted image in comparison to the original image. In the steganography approach, the histogram deviations of the stego image with respect to its original image can suspect the presence of data in an image. Therefore, for histogram comparison of stego image, the stego image histogram should resemble the original image histogram to avoid statistical attacks. Whereas, the histogram of an encrypted image should be uniform to show its random behavior. Histogram uniformity among pixels claims the robustness of the encryption method. Thus, the histogram of an encrypted image should be uniform to prevent the data from statistical attacks.

b) **Correlation coefficient (CC):**

The correlation coefficient (CC) checks the relationship between the original image and the encrypted image. In the original image, the pixels are interconnected with each other in three different directions: horizontal, vertical, and diagonal. However, for encrypted images, the correlation range between the pixels is [1, 1] and near 0 (lesser correlated) is considered as the good encryption technique [112]. The correlation coefficient can be expressed as follows:

$$CC_{i,j} = \frac{C(i,j)}{\sqrt{\sigma(i)}.\sqrt{\sigma(j)}} \tag{11}$$

$$where, C(i,j) = \frac{\sum_{n=1}^{m}\left(i_n - x(i)\right)\left(j_n - x(j)\right)}{m} \tag{12}$$

$$\sigma(i) = \frac{1}{m}\sum_{n=1}^{m}\left(i_n - x(i)\right)^2 \tag{13}$$

$$\sigma(j) = \frac{1}{m}\sum_{n=1}^{m}\left(j_n - x(j)\right)^2 \tag{14}$$

Here, i and j represent image coordinates and $C(i, j)$ represents the covariance between them. $\sigma(i)$ and $\sigma(j)$ are the standard deviations of their respective image coordinates. m is the pixel pairs (i_n, j_n) number. And, $x(i)$ and $x(j)$ are the mean deviations of i_n and j_n respectively.

3.7 Randomness analysis

Randomness analysis checks the pixel haphazardness of an encrypted image. National Institute of Standards and Technology (NIST) [113] has developed a statistical test suite to find out the algorithm strength by analyzing several tests on an encrypted image. The NIST statistical test suite consists of almost 15 calculable tests. These tests include frequency test, frequency within block test, run test, longest run of ones in a block test, binary matrix rank test, discrete fourier transform (DCT) test, non-overlapping template matching test, overlapping template matching test, etc. This test is helpful in identifying deviations of a binary sequence of an encrypted image.

3.8 Speed analysis

Scheme efficacy is analyzed by the execution time of an algorithm to complete its task [114]. The execution time of a method depends upon the system configuration and the algorithm complexity. This analysis can be examined for different processing steps of a program, like, embedding process, encryption process, the extraction process, decryption process, etc. The execution time for any of the program steps should be as small as possible to make the method computationally efficient. The embedding and extraction of some image steganography techniques are shown in Table 6.

Table 6 Embedding and extraction of some image steganography techniques

Technique	Embedding Time (sec)	Extraction Time (sec)
Sahu and Swain [37]	9.0000	11.0000
Parah et al. [43]	8.2633	-
Shen et al. [46]	6.7300	-
Hassan and Gutub [49]	3.7870	-
Ghosal et al. [77]	1.5400	1.4100
Parah et al. [88]	0.9804	0.0547
Parah et al. [89]	0.3481	2.3270

3.9 Steganography effect on medical image accuracy analysis

Medical image accuracy analysis checks the accuracy and precision of resulted medical image after treating with the steganography method. The commonly used methods are accuracy, specificity, sensitivity, and precision, [115] for analyzing the performance and quality contents of an image after steganography.

a) **Accuracy:**

Accuracy is the medical image quality content and prediction accuracy measuring tool. It is the ratio between all correct predictions (positive or negative) and the entire test set [115, 116]. Accuracy can be measured by the Equation as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{15}$$

where TP is true positive, TN is true negative, FP is false positive, and FN is false negative.

b) **Specificity:**

Specificity is also called as true negative rate (TNR). It is the ratio between the number of correctly predicted normal people and the total number of normal people [115]. Specificity can be calculated by the Equation as follows:

$$Specificity = \frac{TN}{TN + FP} \tag{16}$$

where TN is true negative and FP is false positive.

c) **Sensitivity:**

Sensitivity is also called true positive rate (TPR) and recall. It is the ratio between the correctly predicted people with a disease and the total number of actual diseased people [115]. Sensitivity can be computed as follows:

$$Sensitivity = \frac{TP}{TP + FN} \tag{17}$$

where TP is true positive and FN is false negative.

d) **Precision:**

Precision is also called a positive prediction value (PPV). It is the ratio between the total number of positive predictions people with a disease and the total number of positive predicted people [115]. Precision can be expressed as follows:

$$Precision = \frac{TP}{TP + FP} \tag{18}$$

where TP is true positive and FP is false positive.

4 Discussions and future research directions

For secure information transmission, the image steganographic technique is used to restrict intrusion. It embeds the secret data bits into the image pixels to hide the data from unauthorized extraction. Numerous image steganography techniques have been developed by researchers to ensure data security. New trends in image steganography are discussed in this comprehensive review. From the literature, it can be observed that most of the techniques have been able to provide security and safety to the data. The security of data has been enhanced by some of the crypto-stego techniques discussed to provide double layer security to the data. From the survey of the existing image steganography and crypto-stego techniques, it can be noticed that each algorithm has its advantages and disadvantages. A few of the important issues as future directions are highlighted below:

- Using smooth regions for hiding data creates more distortion in an image and thus suspects the presence of data. Hiding data into the edge regions not only provides good image quality but increases the embedding capacity of an image. Therefore, edge based image steganography technique could be used to increase the hiding space and visual quality of an image.
- Most of the image steganography methods discussed have taken grayscale images as a cover medium. Therefore, there is a need for developing and applying steganography methods also on color images to prove its versatility and to further increase payload.
- Hiding data into the frequency coefficients of an image provides security to the data but provides less capacity and is a complex method. Therefore, robust algorithms should be developed in spatial domain to improve data security with less complexity for which the encryption of data together with steganography can be helpful.
- Many of the existing image steganography approaches have tried to either improve payload, image quality, or security of the algorithm. Therefore, a good tradeoff between these parameters should be created to improve the overall performance of the method in all dimensions. For this, edge based image steganography and chaos based encryption methods could be used together. Although, the research in this field has been done by the researchers. Though, it is still an underdeveloped field that needs to be explored in various image steganography schemes and different chaotic maps.
- A survey of the literature leads us to conclude that computational complexity is still an open area of research in the area of the image steganography method.
- Experimental analysis of different reviewed techniques has not used all the evaluation parameters for analyzing the scheme. It can be observed from the survey that image steganography algorithms that encrypt data before embedding have not tested the technique for basic NPCR, UACI, and other security tools. To ensure strong security to the encrypted data. Therefore, every encryption method should be tested for different security tools.
- The steganography approach should resist geometrical attacks, signal processing attacks, and noise attacks to ensure its reliability, so development of robust steganographic systems is an open area of research.
- Several methods have been tested only on few image formats. Therefore, an effort should be done to create a benchmark dataset to compile the algorithm for different image formats.

5 Conclusion

Technological advancement is increasing exponentially to ease daily activities and for a fast service delivery system. For todays' efficient communication system, the internet acts as a central pillar and reduces overconsumption of resources like time and cost. However, the internet is an open environment for data thefts, data modifications, etc. Therefore, to protect data/information from getting into the wrong hands, the image steganography method is used for ensuring data security. The purpose of this review paper is to present a comprehensive review of various image steganography and crypto-stego techniques with their pros and cons to help the reader understand different image crypto-stego techniques. This paper also gives insight into the evaluation parameters being used for steganography and cryptography analysis. This review is significantly highlights the grey areas in the area of the image steganography. Most of the existing image steganography approaches still suffer in terms of less security, low payload, poor image quality, and complexity. Therefore, it is a necessity to develop efficient image steganographic schemes along with data encryption to improve image embedding capacity, image imperceptibility, security with less complexity and should be resistant to different attacks.

Funding This work is not supported by any funding.

Declarations

Informed consent NA

Research involving human participants and/or animals. NA

Conflicts of interest The authors do not have any conflict of interest.

References

1. Jan A, Parah SA, Malik BA, Rashid M. Secure data transmission in IoTs based on CLoG edge detection. Future Generation Computer system. 2021. https://doi.org/10.1016/j.future.2021.03.005.
2. Alsaidi A, lehaibi KA, Alzahrani H, Ghamdi MA, Gutub A. Compression multi-level crypto stego security of texts utilizing colored email forwarding. J Comp Sci Computational Math (JCSCM). 2018;8(3). https://doi.org/10.20967/jcscm.2018.03.002.
3. Khan WZ, Aalsalem MY, Khan MK, Arshad Q. Data and Privacy: getting consumers to trust products enabled by the Internet of Things. IEEE Consumer Electronics Magazine. 2019;8:35–8. https://doi.org/10.1109/MCE.2018.2880807.
4. Singh AK, Kumar B, Singh SK, Ghrera SP, Mohan A. Multiple watermarking technique for securing online social network contents using back propagation neural network. Futur Gener Comput Syst. 2016. https://doi.org/10.1016/j.future.2016.11.023.
5. Alanazi N, Alanizy A, Baghoza N, Ghamdi MA, Gutub A. 3-Layer PC text security via combining compression, aes cryptography 2LSB image steganography. J Res Eng Appl Sci. 2018;3(4):118–124. https://doi.org/10.46565/jreas.2018.v03i04.001.
6. Parah SA, Sheikh JA, Assad UI, Bhat GM. Hiding in Encrypted Images: A three tier security data hiding technique. Multidim Syst Sign Process. 2017;28(2):549–72.
7. Al-Roithy BO, Gutub A. Remodeling randomness prioritization to boost-up security of rgb image encryption. Multimed Tools Appl. 2021;80:28521–81. https://doi.org/10.1007/s11042-021-11051-3.
8. Jan A, Parah SA, Malik BA. A novel laplacian of gaussian and chaotic encryption based image steganography technique. 2020 Int Conf Emerg Technol (INCET) Belgaum. 2020;1–4. https://doi.org/10.1109/INCET49848.2020.9154173.
9. Luo Y, Yu J, Lai W, Liu L. A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimed Tools Appl. 2019;78:2023–22043. https://doi.org/10.1007/s11042-019-7453-3.
10. Jan A, Parah SA, Malik BA. Logistic map-based image steganography using edge detection. Adv Intell Syst Comput. 2021;1189. https://doi.org/10.1007/978-981-15-6067-5_50.
11. Patro KAK, Acharya B. A novel multi-dimensional multiple image encryption technique. Multimed Tools Appl. 2020. https://doi.org/10.1007/s11042-019-08470-8.
12. Li C, Feng B, Li S, Kurths J, Chen G. Dynamic analysis of digital chaotic maps via state-mapping networks. IEEE Transaction on Circuits and Systems-I: Regular Papers. 2019;66(6):2322–35. https://doi.org/10.1109/TCSI.2018.2888688.
13. Hua Z, Jin F, Xu B, Huang H. 2D Logistic-Sine-Coupling map for image encryption. Elsevier Signal Process. 2018;149:148–61.
14. Khan M, Sajjad M, Mehmood I, Rho S, Baik SW. image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Futur Gener Comput Syst. 2016. https://doi.org/10.1016/j.future.2016.11.029.
15. Kim C, Yang CN, Leng L. High-capacity data hiding for ABTC-EQ based compressed image. Electronics. 2020;9(4):644.
16. Hussan FS, Gutub A. Improving data hiding within colour images using hue component of HSV colour space, CAAI Transactions on Intelligence Technology. IET (IEE). 2021. https://doi.org/10.1049/cit2.12053.
17. Hassan FS, Gutub A. Novel embedding secrecy within images utilizing an improved interpolation-based reversible data hiding scheme. J King Saud University - Comp Information Sci. 2020;ISSN:1319–1578. https://doi.org/10.1016/j.jksuci.2020.07.008.
18. Hussan M, Parah SA, Gull S, Qureshi GJ. Temper detection and self-recovery of medical imagery for smart health. Arab J Sci Eng. 2021. https://doi.org/10.1007/s13369-020-05135-9.
19. Loan NA, Hurrah NN, Parah SA, Lee JW, Sheikh JA, Bhat GM. Secure and robust digital image watermarking using coefficient differencing and Chaotic encryption. IEEE transection. 2018. https://doi.org/10.1109/ACCESS.2018.2808172.
20. Biswas R, Mukherjee I, Bandyopadhyay SK. Image feature based high capacity steganographic algorithm. Multimed Tools Appl. 2019. https://doi.org/10.1007/s11042-019-7369-y.
21. Hussain M, Wahab AWA, Idris YIB, Ho ATS, Jung KH. Image steganography in special domain: A survey. Signal Process Image Commun. 2018;65:46–66. https://doi.org/10.1016/j.image.2018.03.012.
22. Wang J, Yang C, Wang P, Song X, Lu J. Payload location for JPEG image steganography based on co-frequency sub-image filtering. International J Distributed Sensor Networks 2020;16(1).
23. Ayub N, Selwal A. An improved image steganography technique using edge based data hiding in DCT domain. J Int Math. 2020;23(2):357–66.
24. Patel SK, Saravanam C. Performance analysis of hybrid edge detector scheme and magic cube based scheme for steganography application. IEEE transection. 2018.
25. Jiang S, Ye D, Huang J, Shang Y, Zheng Z. SmartSteganography: Light-weight generative audio steganography model for smart embedding applications. J Netw Comput Appl. 2020;165:102689. https://doi.org/10.1016/j.jnca.2020.102689.
26. Prasad S, Pal AK. An RGB colour image steganography scheme using overlapping block-based pixel-value differencing. Royal Soc Open Sci. 2017;4.
27. Alkhudaydi M, Gutub A. Securing data via cryptography and Arabic text steganography. SN Computer Sci. 2021;2(46). https://doi.org/10.1007/s42979-020-00438-y.
28. Alkhudaydi MG, Gutub AA. Integrating light-weight cryptography with diacritics Arabic text steganography improved for practical security applications. J Information Security Cybercrimes Res 2020;3(1), 13–30, https://doi.org/10.26735/FMIT1649.
29. Gutub A, Al-Ghamdi M. Image based steganography to facilitate improving counting-based secret sharing, 3D Research. 2019;10(6). https://doi.org/10.1007/s13319-019-0216-0.
30. Gutub A, Al-Juaid N. Multi-bits stego-system for hiding text in multimedia images based on user security priority. J Comp Hardware Eng. 2018;1(2):1–9. https://doi.org/10.63019/jche.v1i2.513.
31. Al-Juaid N, Gutub A. Combining RSA and audio steganography on personal computers for enhancing security. SN Appl Sci. 2019;1:830. https://doi.org/10.1007/s42452-019-0875-8.
32. Atty BAE, Iliyasu AM, Alaskar H, Latif AAAE. A Robust Quasi quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. Sensors. 2020;20:3108. https://doi.org/10.3390/s20113108.
33. Parah SA, Sheikh JA, Assad UI, Bhat GM. Realisation and robustness evaluation of a blind spatial domain watermarking technique. Int J Electron. 2017;104(4):659–72.
34. Pattanaik B, Chitra P, Lakhmi HR, Selvi T, Nagraj V. Contrasting the performance of discrete transformations on digital image steganography using artificial intelligence. Materials Today: Proceedings. 2021. https://doi.org/10.1016/j.matpr.2020.12.076.
35. AbdelRaouf A. A new hiding approach for image steganography based on visual color sensitivity. Multimed Tools Appl. 2021. https://doi.org/10.1007/s11042-020-10224-w.
36. Hussain M, Riaz Q, Saleem S, Ghafoor A, Jung KH. Enhanced adaptive data hiding method using LSB and pixel value differencing. Multimed Tools Appl. 2021. https://doi.org/10.1007/s11042-021-10652-2.

37. Sahu AK, Swain G. Reversible image steganography using dual-layer LSB matching. Sens Imaging. 2020;21:1. https://doi.org/10.1007/s11220-019-0262-y.
38. Hussain M, Wahab AWA, Ho ATS, Javed N, Jung KH. A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. Signal Process Image Commun. 2017. https://doi.org/10.1016/j.image.2016.10.005.
39. Malik A, Sikka G, Verma HK. An AMBTC compression based data hiding scheme using pixel value adjusting strategy. Multidim Syst Sign Process. 2018;29(4):1801–18.
40. Kumar R, Kim DS, Jung KH. Enhanced AMBTC based data hiding method using hamming distance and pixel value differencing. J Inf Secur Appl. 2019;47:94–103.
41. Chakraborty S, Jalal AS. A novel local binary pattern based feature image steganography. Multimed Tools Appl. 2020;79:19561–74.
42. Lin J, Qian Z, Wang Z, Zhang X, Feng G. A new steganography method for dynamic GIF images based on palette sort. Wirel Commun Mobile Comput. 2020;2020:8812087.
43. Parah SA, Sheikh JA, Akhoon JA, Loan NA. Electronic Health Record Hiding in Images for Smart City Applications: A Computationally Efficient and Reversible Information Hiding Technique for Secure Communication. Future Generation Comp Sys. 2018. https://doi.org/10.1016/j.future.2018.02.023.
44. Li X, Luo Y, Bian W. Retracing extended sudoku matrix for high-capacity image steganography. Multimed Tools Appl. 2021 https://doi.org/10.1007/s11042-021-10675-9.
45. Saha S, Chakraborty A, Chatterjee A, Dhargupta S, Ghosal SK, Sarkar R. Extended exploiting modification direction based steganography using hashed-weightage array. Multimed Tools Appl. 2020;79:20973–93.
46. Shen SY, Huang LH, Yu SS. A novel adaptive data hiding based on improved EMD and interpolation. Multimed Tools Appl. 2018;77:131–41.
47. Bairagi AK, Khondoker R, Islam R. An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. Information Security J: A Global Perspective Taylor & Francis. 25 2016;4(6):197–212. https://doi.org/10.1080/19393555.2016.1206640.
48. Rim Z, Afef A, Ridha E, Mourad Z. Beta chaotic map based image steganography. Springer Nature. 2020. https://doi.org/10.1007/978-3-030-20005-3_10.
49. Hassan FS, Gutub A. Efficient image reversible data hiding technique based on interpolation optimization. Arab J Sci Eng. 2021. https://doi.org/10.1007/s13369-021-05529-3.
50. Atta R, Ghanbari M. 2021 A high payload data hiding scheme based on dual tree complex wavelet transform. Optik. 2021;226. https://doi.org/10.1016/j.ijleo.2020.165786.
51. Dhargupta S, Chakraborty A, Ghosal SK, Saha S, Sarkar R. Fuzzy edge detection based steganography using modified Gaussian distribution. Multimed Tools Appl. 2019. https://doi.org/10.1007/s11042-018-7123-x.
52. Ahmadian AM, Amirmazlaghani M. A novel secret image sharing with steganography scheme utilizing Optimal Asymmetric Encryption Padding and Information Dispersal Algorithms. Signal Process Image Commun. 2019. https://doi.org/10.1016/j.image.2019.01.006.
53. Kich I, Ameur EB, Taouil. Image Steganography Based on Edge Detection Algorithm, IEEE transection. 2018.
54. He X, Zhang W, Zhang H, Ma L, Li Y. Reversible data hiding for high dynamic range images using edge information. Multimed Tools Appl. 2018. https://doi.org/10.1007/s11042-018-6589-x.
55. Garav K, Ghanekar U. Image steganography algorithm based on edge region detection and hybrid coding. Comput Model Technol. 2018;22(1):40–56.
56. Prasad S, Pal AK. Stego-key-based image steganography scheme using edge detector and modulus function. Int J Computational Vision and Robotics. 2020;10(3):223–40.
57. Mukherjee S, Sanyal G. Edge based image steganography with variable threshold. Multimed Tools Appl. 2019;78:16363–88. https://doi.org/10.1007/s11042-018-6975-4.
58. Kadhim IJ, Premaratne P, Vial PJ. Adaptive Image Steganography Based on Edge Detection Over Dual-Tree Complex Wavelet Transform Springer Nature International Publishing. 2018;544–550. https://doi.org/10.1007/978-3-319-95957-3_57.
59. Ghosal SK, Mandal JK, Sarkar R. High payload image steganography based on Laplacian of Gaussian (LoG) edge detector. Multimed Tools Appl. 2018;77:30403–18.
60. Ghosal SK, Chatterjee A, Sarkar R. Image steganography based on Kirsch edge detection. Multimed Syst. 2021;27:73–87.
61. Banik BG, Poddar MK, Bandyopadhyay SK. Image steganography using edge detection by Kirsch operator and flexible replacement technique. Emerg Technol Data Mining Inf Sec Adv Intel Syst Comput. 2019;814:175–87. https://doi.org/10.1007/978-981-13-1501-5_15.
62. Wang Y, Tang M, Wang Z. High-capacity adaptive steganography based on LSB and hamming code. Optik. 2020;213. https://doi.org/10.1016/j.ijleo.2020.164685https://doi.org/10.1016/j.ijleo.2020.164685.
63. Tripathy SK, Srivastava R. An Edge-Based Image Steganography Method Using Modulus-3. Strategy and Comparative Analysis Springer Nature. 2020;485–494. https://doi.org/10.1007/978-981-15-4018-9_43.
64. Tuncer T, Sonmez Y. A Novel Data Hiding Method based on Edge Detection and 2k Correction with High Payload and High Visual Quality. Balkan J Electrical & Comp Eng. 2019;7(3):311–318. https://doi.org/10.17694/bajece.573514.
65. Abdel-Aziz MM, Hosny KM, Lashin NA. Improved data hiding method for security color images. Multimed Tools Appl. 2021;50:12641–70. https://doi.org/10.1007/s11042-020-10217-9.
66. Yao H, Fanyu M, Chuan Q, Tang Z. Dual-JPEG-image reversible data hiding. Inf Sci. 2021;563:130–49. https://doi.org/10.1016/j.ins.2021.02.015.
67. Liu Y, Chang CC. Reversible data hiding for JPEG images employing all quantized non-zero AC coefficients. Displays. 2018;51:51–6. https://doi.org/10.1016/j.displa.2018.01.004.
68. Attaby AA, Ahmed MFMM, Alsammak AK. Data hiding inside JPEG images with high resistance to Steganalysis using a novel technique: DCT-M3. Ain Shams Engineering Journal. 2018;9:1966–74. https://doi.org/10.1016/j.asej.2017.02.003.
69. El-Rahman SA. A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information. Comput Electr Eng. 2016;1–20. https://doi.org/10.1016/j.compeleceng.2016.09.001.
70. Mohamed N, Baziyad M, Rabie T, Kamel I. L*a*b color space high capacity steganography utilizing quad-trees. Multimed Tools Appl. 2020;79:25089–113. https://doi.org/10.1007/s11042-020-09129-5.
71. Rabie T, Kamel I, Baziyad M. Maximizing embedding capacity and stego quality: curve-fitting in the transform domain. Multimed Tools Appl. 2018;77:8295–326. https://doi.org/10.1007/s11042-017-4727-5.
72. Saidi M, Hermassi H, Rhouma R, Belghith S. A new adaptive image steganography scheme based on DCT and chaotic map. Multimed Tools Appl. 2017;76(11):13493–510. https://doi.org/10.1007/s11042-016-3722-6.
73. Nipanikar SI, Deepthi VH, Kulkarni N. A sparse representation based image steganography using particle swarm optimization and wavelet transform. Alex Eng J. 2018;57:2343–56. https://doi.org/10.1016/j.aej.2017.09.005.

74. Navriyanto A, Sutarno S, Erwin E, Siswanti SD. Image steganography using combine of discrete wavelet transform and singular value decomposition for more robustness and higher peak signal noise ratio. IEEE Transection. 2018;147–152.
75. Miri A, Faez K. An image steganography method based on integer wavelet transform. Multimed Tools Appl. 2018;77:13133–44. https://doi.org/10.1007/s11042-017-4935-z.
76. Kalita M, Tuithung T, Majumdar S. A new steganography method using integer wavelet transform and least significant bit substitution. Comput J. 2019. https://doi.org/10.1093/comjnl/bxz014.
77. Ghosal SK, Mukhopadhyay S, Hossain S, Sarkar R. Exploiting Laguerre transform in image steganography. Comput Electr Eng. 2021;89. https://doi.org/10.1016/j.compeleceng.2020.106964.
78. Ma B, Li B, Wang XY, Wang CP, Li J, Shi YQ. A code division multiplexing an block classification-based real-time reversible data-hiding algorithm for medical images. J Real-Time Image Proc. 2019. https://doi.org/10.1007/s11554-019-00884-9.
79. Murugan GVK, Subramaniyam RU. Performance analysis of image steganography using wavelet transform for safe and secured transaction. Multimed Tools Appl. 2020;79:9101–15. https://doi.org/10.1007/s11042-019-7507-6.
80. Maji G, Mandal S, Sen S. Cover independent image steganography in spatial domain using higher order pixel bits. Multimed Tools Appl. 2021;80:15977–6006. https://doi.org/10.1007/s11042-020-10298-6.
81. Sharif A, Mollaeefar M, Nzari M. A novel method for digital image steganography based on a new three-dimensional chaotic map. Multimed Tools Appl. 2017;76:7849–67. https://doi.org/10.1007/s11042-016-3398-y.
82. Gambhir G, Mandal JK. Multicore implementation and performance analysis of a chaos based LSB steganography technique. Microsyst Technol. 2020. https://doi.org/10.1007/s00542-020-04762-4.
83. Prasad S, Pal AK. Logistic map-based image steganography scheme using combined LSB and PVD for security Enhancement. Springer Nature Adv Intel Comput. 2019. https://doi.org/10.1007/978-981-13-1501-5_17.
84. Mohammad K, Ahamd j, Rho S, Baik SW. Image steganography for authenticity of visual contents in social networks. Multimed Tools Appl. 2017. https://doi.org/10.1007/s11042-017-4420-8.
85. Alotaibi M, Al-Hendi D, Alroithy B, Alghamdi M, Gutub A. Secure mobile computing authentication utilizing hash, cryptography and steganography combination. J Inf Sec Cybercrimes Res (JISCR). 2019;2(1):9–20.
86. Mathivanan P, Balaji GA. QR code base color image stego-crypto technique using dynamic bit replacement and logistic map. Optik. 2021;225: 165838. https://doi.org/10.1016/j.ijleo.2020.165838.
87. Abdelwahab OF, Hussein AI, Hamed HFA, Kelash HM, Khalaf AAM. Efficient combination of RSA cryptography, lossy and lossless compression steganography techniques to hide data. Comput Sci. 2021;183:5–12. https://doi.org/10.1016/j.procs.2021.02.002.
88. Parah SA, Kaw JA, Bellavista P, Loan NA, Bhat GM, Muhammad K, Victor A. Efficient security and authentication for edge-based Internet of Medical Things. IEEE Internet Things J. 2021. https://doi.org/10.1109/JIOT.2020.3038009.
89. Parah SA, Sheikh JA, Akhoon JA, Loan NA, Bhat GM. Information Hiding in Edges: A high capacity information hiding technique using hybrid edge detection. Springer Multimedia Tools Appl. 2016;77(1):185–207.
90. Delmi A, Suryadi S, Satria Y. Digital image steganography by using edge adaptive based chaos cryptography. J Phys. 2017;1442. https://doi.org/10.1088/1742-6596/1442/1/012041.
91. Sharma H, Mishra DC, Sharma RK, Kumar N. Multi-image steganography and authentication using crypto-stego techniques. Multimed Tools Appl. 2021;80:29067–93. https://doi.org/10.1007/s11042-021-11068-8.
92. Kaushik N, Sheokand K. A steganography technique based on chaotic LSB and DWT. International J Innov Res Comp Comm Eng. 2016;4(6):10420–10426. https://doi.org/10.15680/IJIRCCE.2016.0405028.
93. Panday HM. Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography. Futur Gener Comput Syst. 2020;111:213–25. https://doi.org/10.1016/j.future.2020.04.034.
94. Elhoseny M, Gonzalez GR, Elnasr OMA, Shawkat SA, Arunkumar A, Farouk A. Secure Medical Data Transmission Model for IoT-Based Healthcare Systems. IEEE Transection, Special Section on Information Security Solutions for Telemedicine Applications. 2018;6(2018):20596–608. https://doi.org/10.1109/ACCESS.2018.2817615.
95. Duan X, Guo D, Liu N, Li B, Gou M, Qin C. A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. IEEE Transection. 2020;8. https://doi.org/10.1109/ACCESS.2020.2971528.
96. Subhedar MS, Mankar VH. Curvelet transform and cover selection for secure steganography. Multimed Tools Appl. 2018;77:8115–38. https://doi.org/10.1007/s11042-017-4706-x.
97. Eyssa AA, Abdelsamie FE, Abdelnaiem AE. An efficient image steganography approach over wireless communication system. Wireless Pers Commun. 2020;110:321–37. https://doi.org/10.1007/s11277-019-06730-2.
98. Kaur R, Singh B. A hybrid algorithm for image steganography. Multidimens Syst Signal Process. 2021;32:1–23. https://doi.org/10.1007/s11045-020-00725-0.
99. Hureib ESB, Gutub AA. Enhancing medical data security via combining elliptic curve cryptography and image steganography. International J Comp Sci Network Security (IJCSNS). 2020;20(8):1–8. https://doi.org/10.22937/IJCSNS.2020.20.08.1.
100. Hureib ESB, Gutub AA. Enhancing medical data security via combining elliptic curve cryptography with 1-LSB and 2-LSB image steganography. International J Comp Sci Network Security (IJCSNS). 2020;20(12):232–241. https://doi.org/10.22937/IJCSNS.2020.20.12.26.
101. Samkari H, Gutub A. Protecting medical records against cybercrimes within hajj period by 3-layer security. Recent Trends Inf Technol Appl. 2019;2(3):1–21. https://doi.org/10.5281/zenodo.3543455.
102. Denis R, Madhubala P. Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare system. Multimed Tools Appl. 2021;80:21165–202. https://doi.org/10.1007/s11042-021-10723-4.
103. Manikandan T, Muruganandham A, Babuji R, Nandalal V, Iqbal JIM. Secure E-Health using image steganography. J Phys. 2021;1917:012016. https://doi.org/10.1088/1742-6596/1917/1/012016.
104. Ogundokun RO, Awotunde JB, Adeniyi EA, Ayo FE. Crypto-stego based model for securing medical information on IOMT platform. Multimed Tools Appl. 2021. https://doi.org/10.1007/s11042-021-11125-2.
105. Prasanalakshmi B, Murugan K, Srinivasan K, Shridevi S, Shamsudheen S, Hu YC. Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography. J Supercomput. 2021. https://doi.org/10.1007/s11227-021-03861.
106. Karakus S, Avci E. A new image steganography method with optimum pixel similarity for data hiding in medical images. Med

Hypotheses. 2020;139. https://doi.org/10.1016/j.mehy.2020.109691.
107. Sukumar AK, Subramaniyaswamy V, Vijayakumar V, Ravi L. A secure multimedia steganography scheme using hybrid transform and support vector machine for cloud-based storage. Multimed Tools Appl. 2020. https://doi.org/10.1007/s11042-019-08476-2.
108. Gutub A, Al-Shaarani F. Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons. Arab J Sci Eng. 2020. https://doi.org/10.1007/s13369-020-04413-w.
109. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW. Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Futur Gener Comput Syst. 2016. https://doi.org/10.1016/j.future.2016.11.029.
110. Khan MF, Ahmed A, Saleem K. A novel cryptographic substitution box design using gaussian distribution. IEEE Access. 2019;7:15999–6007.
111. Sneha PS, Sankar S, Kumar AS. A chaotic colour image encryption scheme combining Walsh-Hadamard transform and Arnold-Tent maps. J Ambient Intell Humaniz Comput. 2020;11:1289–308. https://doi.org/10.1007/s12652-019-01385-0.
112. Shah D, Shah T. Anovel discrete image encryption algorithm based o n finite algebraic structures. Multimed Tools Appl. 2020. https://doi.org/10.1007/s11042-020-09182-0.
113. Cicek I, Pusane AE, Dundar G. An Integrated Dual Entropy Core True Random Number Generator. IEEE Transaction Circuits-II. 2017;64:329–33.
114. Njitacke ZT, Isaac SD, Nestor T, Kengne J. Window of Multistability and Control in a Simple 3D Hopfield Neural Network: Application to Biomedical Image Encryption. Springer Neural Comput Appl. 2020. https://doi.org/10.1007/s00521-020-05451-z.
115. Eze P, Parampalli U, Evans R, Liu D. Evaluation of the effect of steganography on medical image classification accuracy. J Bioinforma Comput Biol. 2020;9(4). https://doi.org/10.1007/s11042-021.
116. Eze P, Parampalli U, Evans R, Liu D. A new evaluation method for medical image information hiding techniques. IEEE Transection. 2020;6119–6122. https://doi.org/10.1109/EMBC44109.2020.9176066.