Information Sciences 609 (2022) 1451–1488

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Digital image steganography: A literature survey

Pratap Chandra Mandal [a,b], Imon Mukherjee [b,*], Goutam Paul [c], B.N. Chatterji [a,d]

[a] Computer Sc. & Engineering, B.P. Poddar Institute of Management & Technology, India
[b] Computer Sc. & Engineering, Indian Institute of Information Technology Kalyani, India
[c] R.C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, India
[d] Electronics and Electrical Communication Engineering (Retd.), IIT Kharagpur, India

ARTICLE INFO

Article history:
Received 20 November 2020
Received in revised form 22 May 2022
Accepted 22 July 2022
Available online 28 July 2022

Keyword:
Data hiding
Steganography
Spatial domain
Transform domain
Information security
Steganalysis

ABSTRACT

Steganography is the art of concealing information in a cover media in such a way that the presence of the information is unknown. Digital image steganography accomplishes the potential for protected communication that is crucial in most of the applications nowadays. Steganography has several beneficial applications. It has been driven to the frontrunner of present security systems by the amazing development in computational power, the rise in security consciousness. The main challenge in proposing a steganographic technique is to maintain a suitable balance among higher embedding capacity, imperceptibility, and security that separate it from correlated systems like cryptography and watermarking. This article offers an extensive state-of-the-art review and analysis of some recent steganographic techniques. Furthermore, we have discussed popular steganography tools in detail. Challenges in the recent deep learning based steganographic techniques have been addressed. To explore the domain, the article concludes with mentioning some future research directions.

1. Introduction

The internet revolution offers ease in digital communication; at the same time, it is also a challenge for us to secure the message over the open network. For addressing the security of information, several approaches are presented as shown in Fig. 1. The security system plays a vital role to restrict the messages from being seized by an unauthorized person. Cryptography [1] protects the content of the information that allows only the sender and intended beneficiary of communication to view its contents. Information hiding techniques include steganography [2,3] and watermarking [4]. Both watermarking and steganography are used to obscure the confidential information within the innocent media like image, video, audio, and text, but both have different purposes. Watermarking is used for authentication and copyright protection of digital data. In contrast, steganography [5] is the art of concealing information. Imperceptibility is of major importance for steganographic technique, whereas watermarking provides the maximum importance to robustness. On the basis of the capability of recovering the cover images, data hiding techniques are categorized into two groups: irreversible [6] and reversible data hiding (RDH) [7]. If the cover image can be obtained after removal of the confidential data the process is said to be reversible data hiding;

* Corresponding author.
E-mail addresses: pcmandal9@gmail.com (P.C. Mandal), imon@iiitkalyani.ac.in (I. Mukherjee), goutam.paul@isical.ac.in (G. Paul), bnchatterji@gmail.com (B.N. Chatterji).

https://doi.org/10.1016/j.ins.2022.07.120
0020-0255/

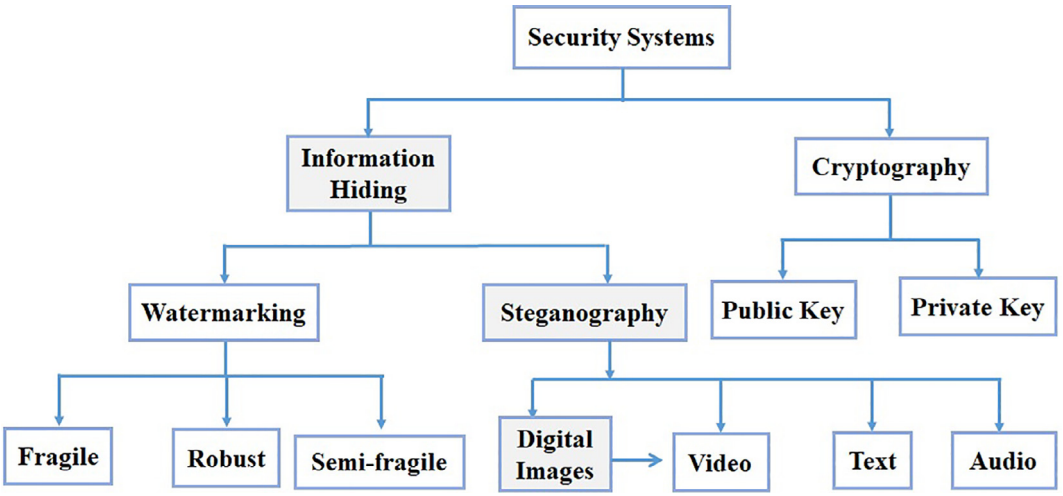

Fig. 1. Basic security system branches [3].

otherwise it is termed as irreversible data hiding. DE, histogram shifting, and Interpolation based techniques, etc., are the examples of reversible data hiding techniques whereas LSB, PVD, etc., are examples of irreversible data hiding techniques.

Conversely, steganalysis [8], is the art of identifying the hidden information embedded in digital media. After the heart-breaking incidents of 11^{th} September 2001, researchers have given great importance to the topic steganography and steganalysis [3]. It has also now become an important research topic due to the popularity of social media applications like Facebook, WhatsApp, etc. Both have several genuine applications and signify great research openings waiting to be addressed.

1.1. *Contributions*

1. An extensive review of steganographic techniques in different domains has been provided. Special emphasis has been given on the insightful analysis on the underdeveloped aspects or fail cases of the state-of-the-art works. We have also provided a comparative analysis of the recent state-of-the-art works.
2. Performance measurement criteria of a steganographic technique like capacity, quality, and security have been discussed in detail. Security of the techniques have been analyzed by various state-of-the art attacks like RS analysis, PDH attack, relative entropy, steganalysis tools like StegExpose, and benchmark tool like StirMark Benchmark 4.0, etc.
3. Applications of data hiding techniques have been mentioned.
4. Challenges in deep learning based steganography have been discussed.
5. The commonly used steganography tools are presented in detail. A comparative analysis and their weakness against the steganalysis tools have also been discussed.
6. Some recommendations have been given that can help to work in the right way.
7. Future research directions have been provided that can be promising in the coming days.

All the important abbreviations are listed in Table 1. To have a vibrant understanding of their functionalities a comparison among cryptography, watermarking, and steganography is shown in Table 2.

1.2. *A Glimpse of History*

The knowledge of data hiding can be found since the era of "Rig-Veda" (1500 – 1000 BCE). Most of the Sanskrit slokas have some apparent meanings, but deeper meanings are covered inside. The name steganography is derived from Greek words that literally mean "Covered Writing". At the early stage, it has been mainly used for military, diplomatic and for a rare case people used it for private purposes. From the documents it has been found that around 440 BC, Demaratus sent a caution about an upcoming attack to Greece on a wax tablet. The message was written on a wooden backing and then shielded by beewax. It seemed unused. In the 5^{th} century BC Histaiacus cut off a slave's hair, tattooed a message on his skull. The slave transferred the information after his hair grew back [9]. Italian mathematician Jerome Cardan discovered a Chinese ancient method of secret writing 500 years ago. Steganography became prevalent during World War II where there was an inadequate number of serviceable communication paths for resistance in Europe that created a perfect atmosphere for evolving techniques of secret communication. Key was ease of data exchange and high security. Data were transported through radio relay coded into name day wishes, birthday wishes or in promotional announcements. Because of that Nazi banned low

Table 1
List of important Abbreviations.

AEC	Average Embedding Capacity	NCC	Normalized Cross Correlation
ANN	Artificial Neural Networks	NN	Neural network
CIE	Codebook to Improve the EMD	OPAP	Optimal Pixel Adjustment Process
DCT	Discrete Cosine Transform	PDH	Pixel Difference Histogram
DFT	Discrete Fourier Transform	PEHS	Prediction Error Histogram shifting
DE	Difference Expansion	PRNG	Pseudo Random Number Generator
DH	Difference Histogram	PSNR	Peak Signal to Noise Ratio
DWT	Discrete Wavelet Transform	PVD	Pixel Value Differencing
DWTDM	Discrete Wavelet Transform Difference Modulation	PBPVD	Parity Bit Pixel Value Difference
		PVG	Pixel Value Grouping
ENMI	Enhanced Neighbor Mean Interpolation	QVD	Quotient Value Differencing
EMD	Exploiting Modification Direction	RDH	Reversible Data Hiding
GAN	Generative Adversarial Network	RIASIWT	Robust Image Adaptive Steganography using Integer Wavelet transform
HDWT	Haar Discrete Wavelet Transform		
HVS	Human Visual System	RDHEI	Reversible Data Hiding in Encrypted Images
HM	Histogram Modification	RDWT	Redundant Discrete Wavelet Transform
HS	Histogram Shifting	ROC	Receiver Operating Characteristic
HUGO	Highly Undetectable steGO	ROI	Region of Interest
IEMD	Improved EMD	RS	Regular and Singular
IRDH	Irreversible data hiding	SRM	Spatial Rich Model
iRMDR	improved Rightmost Digit Replacement	SSIM	Structural Similarity Index Metric
INP	Interpolation by Neighboring Pixel	SVD	Singular Value Decomposition
IWT	Integer Wavelet Transform	SVM	Support Vector Machine
JRM	JPEG Rich Model	SVR	Support vector regression
LSB	Least Significant Bit	STC	Syndrome Trellis Coding
MDLE	Multidirectional Line Encoding	UIQI	Universal Image Quality Index
MPE	Modification of Prediction Error	UED	Uniform Embedding Distortion metric
MPSO	Modified Particle Swarm Optimization	UNIWARD	UNIversal WAvelet Relative Distortion
MSE	Mean Squared Error	WOW	Wavelet Obtained Weights
NMI	Neighbor Mean Interpolation		

Table 2
Comparison among cryptography, watermarking, and steganography.

Characteristics	**Cryptography**	**Watermarking**	**Steganography**
Secret data	Plain text	Watermark	Payload
Carrier	Usually text based	image/audio files	Any digital media
Key constraint	Mandatory	Optional	Depends on application
Objective	Protection of content	Protection of copyright	Secret communication
Concern	Robustness	Robustness	Detectability/capacity
Visibility	Always	Sometimes	Never
Result	Cipher-text	Watermarked file	Stego file
Type of attacks	Cryptanalysis	Image processing	Steganalysis
Robustness	Depends on complexity of ciphering algorithm	Against removing or tampering secret data	Against detection of presence of secret data
Challenges	Key management, Encryption algorithm complexity	Robustness	Capacity, Imperceptibility, Security
Fails when	Deciphered	It is exchanged/eliminated	Secret data is detected

frequency radio headsets. Among several steganography methods applied in World War II one was the use of unnoticeable ink or microdots. Microdots are basically a text or an image significantly minimized to avoid exposure. In 1945, Morse code has been hidden in a drawing as shown in Fig. 2. The concealed data is encoded onto the extent of grass together with the river. The long grass signifies a line and the short grass specifies a point. The interpreted information is as: "Compliments of CPSA MA to our chief Col Harold R. Shaw on his visit to San Antonio May 11^{th} 1945" [10]. All stated approaches are termed as mechanical steganography that can still be applied today but the digital revolution in 21^{st} century has made secure techniques of data transfers for everyone.

The rest of the paper is framed as follows: Section 2 explains the fundamental concepts. Section 3 specifies the general model of steganography. Section 4 defines the evaluation criteria of any steganographic technique. Section 5 describes the application of steganography. Classification and discussion on steganographic technique is shown in Section 6. Section 7 explains adaptive steganography. Deep learning based steganography is discussed in Section 8. Analysis of performance of the recent state-of-the-art works is discussed in Section 9. Some popular steganographic tools have been described in Section 10. Comparison among steganography tools are provided in Section 11. Brief discussion on steganalysis is also presented

Fig. 2. Camouflage of Morse code (1945). The concealed data is encoded into the grass length together with the river [10].

in Section 12. Section 13 discusses the challenges in deep learning based steganography. Some future research directions are mentioned in Section 14 and the article is concluded in Section 15.

2. Fundamental Concepts

The study uses a few terms commonly specified by steganography groups. The image which is carrying the embedded message is termed as a "cover image". The term "stego image" means the image with a hidden message. The process by which secret information is embedded within the cover media is referred to as "steganography". The term "steganalysis" specifies different statistical analysis, which is used for attacking the steganographic methods.

3. General Model of Steganography

The modern steganography can be modeled by Simmons [11] in the famous prisoner's problem. The paper explains about the competencies and virtues of steganography in an insecure channel that involves three parties: Alice, Bob, and Wendy. Assume, Alice and Bob are the two prisoners who work together for an escape plan. Their communications are watched by a warden, Wendy. The general structure of a secure channel for steganography is depicted in Fig. 3. The sender (Alice) wants to send secret data (D) to the receiver (Bob), selects an innocuous cover image (C). Later, Alice hides the secret data (D) in the cover image (C) and applies a stego key (K) which is optional. At last, Alice gets a stego image (S) that must not be distinguished from the cover image (C). The stego image (S) specifies the cover image (C) along with the confidential data (D) concealed within the cover image with a secret key (K). The process is called the embedding process ($\mathscr{X}$). Then, Alice sends the stego image (S) to Bob through a communication channel. The aim of the system is to stop Wendy (unauthorized person) from detecting the concealed data (D). On the receiver end, during the extracting process ($\mathscr{X}'$), Bob retrieves the concealed data (D) using the extraction algorithm and the stego key (K) used in the embedding process. Then, the process can be formulated using the Eq. (1) and Eq. (2) as follows:

$$\mathscr{X} : (C, D, K) \rightarrow S \tag{1}$$

$$\mathscr{X}' : (S, K\prime) \rightarrow (D\prime, C\prime) \tag{2}$$

Ideally, the steganographic technique should guarantee $D = D\prime$ and it is not compulsory to have $C = C\prime$. When C and $C\prime$ are identical, the technique is termed as reversible data hiding (RDH), otherwise the technique is irreversible data hiding. Although the public key steganographic system [12] is described in various literatures, the private key steganographic system, where $K = K\prime$ is assumed, remains the utmost situation in the secret communication.

4. Evaluation Criteria of a Steganography Scheme

The performance of a steganography scheme is measured by three main criteria: capacity, imperceptibility, and security. Furthermore, these criteria help us to move in the right direction for enhancing the techniques.

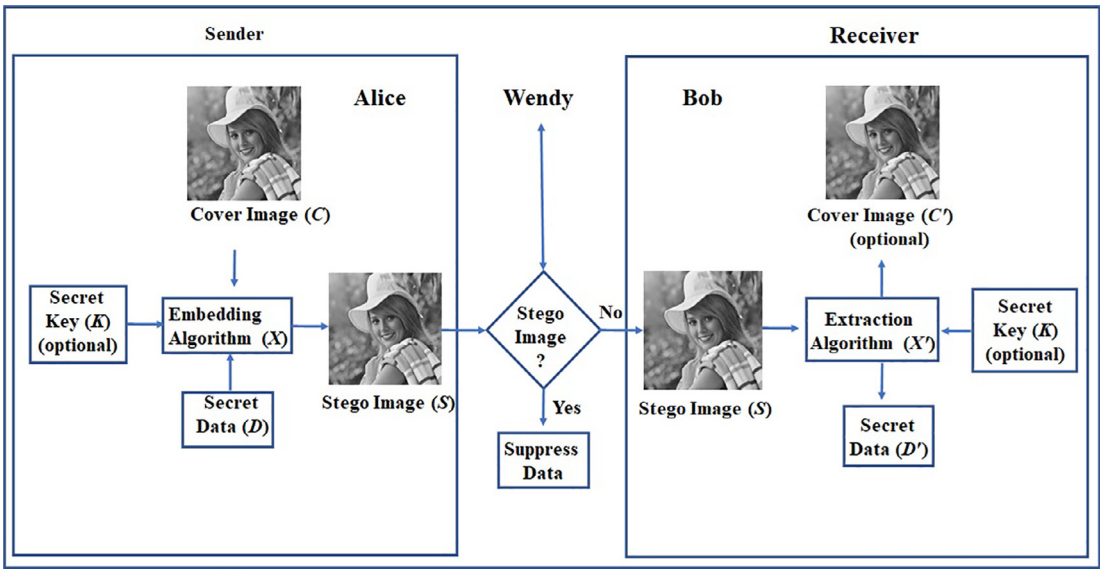

Fig. 3. General model of steganography.

4.1. *Embedding Capacity*

It is vital to find out how many bits a steganography scheme can embed imperceptibly in comparison to the other techniques. Assessing the capacity of a steganography method means to determine the highest number of bits that can be embedded imperceptibly. It is assessed by the bits per pixel (bpp). Average Embedding Capacity (AEC) is defined in image steganography as,

$$AEC(bpp) \triangleq \frac{\text{Total embedded bits}}{\text{Total number of pixels in the image}}.$$

4.2. *Imperceptibility/Stego Image Quality*

Quality is the major perceptual concern for most steganography methods to escape from detection. Several metrics are used for measuring the stego image quality. Let us consider, U and V refer to the cover and the stego images. P and Q be the rows and columns of an image.

Peak Signal to Noise Ratio (PSNR): PSNR [13,14] is defined as,

$$PSNR \triangleq 10 \log_{10} \frac{U_{max}^2}{MSE},$$

where U_{max} is the maximum pixel value and the Mean-Squared-Error (MSE) is computed by,

$$MSE \triangleq \frac{\sum_{e=1}^{P}\sum_{f=1}^{Q}[U(e,f) - V(e,f)]^2}{P \times Q},$$

Higher the PSNR value better the quality of the images. In that case both the cover and the stego images are very similar to each other.

Structural Similarity Index Metric (SSIM): In image steganography, SSIM [15] calculates the structural similarities between host and distorted images.

Let U and V specify the cover and distorted image. SSIM can be calculated as:

$$SSIM(U,V) \triangleq \frac{(2\mu_u\mu_v + x)(2\sigma_{uv} + y)}{(\mu_u^2 + \mu_v^2 + x)(\sigma_u^2 + \sigma_v^2 + y)}.$$

where, μ_u and μ_v imply the mean of U and V, σ_u^2 and σ_v^2 are the variance of U and V, σ_{uv} means the covariance of U and V. Two positive constants $x = (h_1.W)^2$ and $y = (h_2.W)^2$, where $W = 2^{\text{totalbits/pixel}} - 1$, $h_1 = 0.01$ and $h_2 = 0.03$. x and y are used here to avoid null denominator.

Universal Image Quality Index (UIQI): UIQI [16] between two images U and V, can the computed as,

$$UIQI \triangleq \frac{4\sigma_{uv}\mu_u\mu_v}{(\sigma_u^2+\sigma_v^2)(\mu_u^2+\mu_v^2)},$$

where, μ_u and μ_v imply the mean of U and V, σ_u^2 and σ_v^2 are the variance of U and V, σ_{uv} are the covariance between U and V. The values of UIQI vary from -1 to 1. UIQI is equal to 1 when two images are same.

Normalized Cross Correlation (NCC): NCC indicates the amount of similarity between two images. NCC [17] is calculated as,

$$NCC(U,V) \triangleq \frac{\frac{1}{P\times Q}\sum_{e=1}^{P}\sum_{f=1}^{Q}[U(e,f).V(e,f)]}{\sigma_u\sigma_v},$$

where, σ_u and σ_v are the standard deviations of U and V. NCC value is 0 for two dissimilar images and 1 for two identical images.

4.3. *Security*

Steganographic system faces several attacks (active/passive). The most vital assessment criterion in the steganographic system is security. The security of a technique can be measured with respect to the resistance against steganalysis attack, viz., StegExpose, pixel difference histogram (PDH), and standard tool, viz., StirMark benchmark 4.0. etc.

Receiver Operating Characteristic (ROC)

The steganalysis techniques usually attempt to identify or to excerpt the concealed message from the stego image deprived of any prior knowledge of embedding technique. When applying the steganalysis techniques on a test data set, the four situations may occur.

- True positive (*TP*) signifies number of stego images properly classified as stego.
- False negative (*FN*) signifies number of stego images incorrectly classified as cover.
- True negative (*TN*) signifies number of cover images properly classified as cover.
- False positive (*FP*) signifies number of cover images incorrectly classified as stego.

The confusion matrix (as shown in Table 3) is made to differentiate the test data set as cover or stego when a steganalysis technique is applied on it. Receiver operating characteristic (ROC) curve [18] is a graph to show the performance of a classifier at varying classification threshold. The ROC curve plots two parameters: FP rate and TP rate where,

Table 3
Confusion matrix.

	Predicted: No	**Predicted: Yes**
Actual: No	True negatives (TNs)	False positives (FPs)
Actual: Yes	False negatives (FNs)	True positives (TPs)

$$TP \text{ rate} = \frac{TP}{TP+FN}, FP \text{ rate} = \frac{FP}{FP+TN}.$$

The area under the curve (AUC) ROC is a common metric for calculating the test accuracy of a classifier. Reasonable tests should have $0.5 \leqslant \text{AUC} \leqslant 1$. AUC close to 1 means a very good diagnostic test. Random guessing generates the diagonal line between the points (0, 0) and (1, 1) which has an area of 0.5. Fig. 4 shows that Method A is closer to random guess line compared to Method B and Method B is closer to random guess line compared to Method C. Hence, AUC value of Method A is lower than the Method B and Method C. Therefore, Method A provides higher security than the Method B and method C.

Regular/Singular (RS) analysis

RS analysis [19] is used to verify the security of a steganographic scheme. It divides the stego-pixels into three groups, regular group R_M and R_{-M}, the singular group S_M and S_{-M} and the unusable group. The comparison between four parameters $(R_M, R_{-M}, S_M, S_{-M})$ are used to notice the presence of the hidden message. The steganographic technique beats the RS analysis when the condition $R_M \cong R_M > S_M \cong S_{-M}$ is satisfied.

Otherwise, the underlined steganography will be noticed by RS analysis.

Relative Entropy or Kullback–Leibler Divergence Test

To assess the security of a steganographic method, the relative entropy (E) [20] between the probability distributions of the cover image (C) and the stego image (S) can be computed by the Eq. (3),

$$E(S||C) = \sum s(x) log \frac{s(x)}{c(x)}. \tag{3}$$

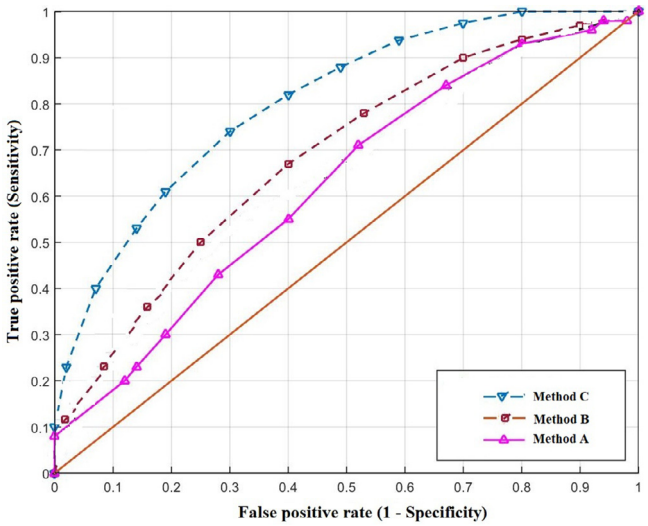

Fig. 4. ROC curve of a steganographic technique.

A technique is completely secured when the relative entropy between two probability distribution functions is zero. $E(S||C)$ is treated as a distance between the measures c and s. If the number of embedded bits increases, the relative entropy in the stego image increases.

Pixel Difference Histogram (PDH)

The security of a method can be tested by the PDH analysis [21]. The PDH is attained from the histogram of the difference between contiguous pixels. Fig. 5 specifies that the PDH curve of the cover and the stego images are similar, and no clear artifacts are exposed. Hence, it can be concluded that the method is secure for PDH analysis.

StirMark Benchmark 4.0

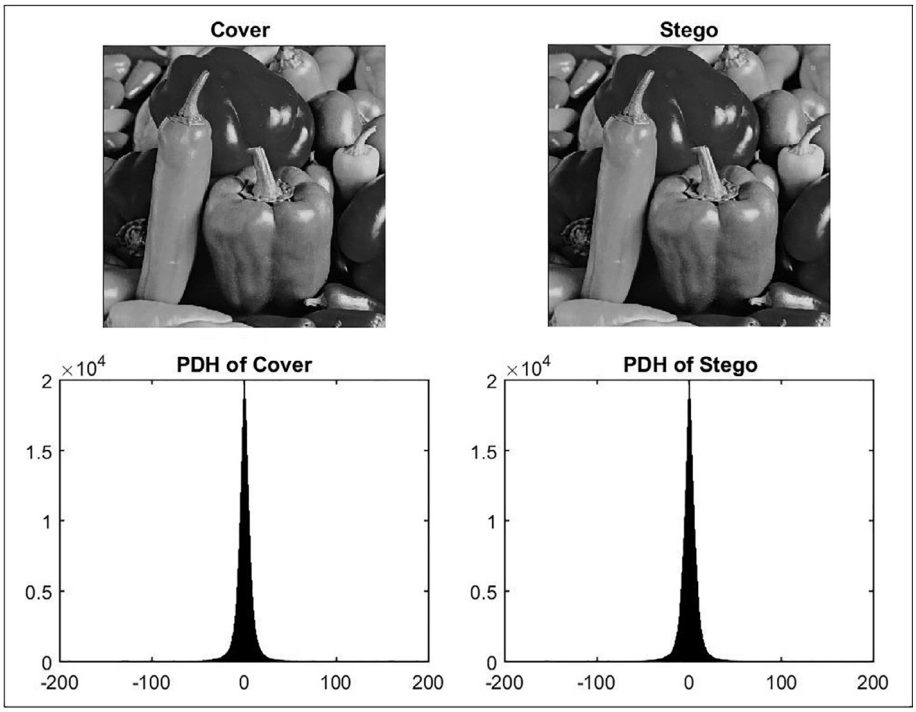

Fig. 5. PDH of Peppers image.

To measure the strength, the steganographic techniques can be verified using the benchmark tool, viz., StirMark benchmark 4.0 [22]. The StirMark benchmark has offered a series of attacks, common image processing tasks. These tasks are parameterized to obtain varying potency of the manipulation. Both cover and stego images are used as an input dataset to produce test data for evaluation of robustness. Common transformations are small random distortions, rotation, scaling, self-similarities and additive noise, etc. Test-AdditiveNoise places certain noise to the input image. The consequence is a certain degree of distortion to the image.An insignificant change in the cover and its corresponding stego version implies the strength of a scheme.

5. Applications of Data Hiding Techniques

Areas like medical, industry, multimedia, military, and many others need careful communication for security purposes. Data hiding technique is related to, but not limited to the following areas:

1. **General communication:** People may use these methods to deliver extra security in their day-to-day communications [23]. Numerous administration officials use this mechanism while interacting among themselves through the intranet, internet, etc.Criminals and dissidents also use steganography for their secret communication.
2. **Military agencies:** Militaries [24] need to communicate among themselves by passing stealthy data in such a manner that the enemies cannot understand or cannot perceive the presence of the concealed data. Hence, militaries use this technique in their communications.
3. **Medical Science:** It is also used in the medical field [25], for preserving the privacy of patients' data. A connection is preserved by hiding the patient's data within the image without decreasing its quality. The work [26] also has given new ideas about patients' data camouflage in digital images. The extra data should not degrade the image quality. One more encouraging research on DNA-steganography in medical science is going on. It can be utilized to store the particulars of a person into its DNA itself. The research in this area is not yet developed enough.
4. **TV Broadcasting:** One useful area is TV broadcasting, the safe transmission of secret data, video/audio synchronization, checksum embedding, and TCP/IP packets.
5. **Document Authentication:** Concealed data inside a digital document can comprise a digital signature that confirms its authenticity [23]. Steganography is used for embedding individual data in smart identity card.
6. **Copyright Information and Document Tracking:** Originators of digital content always use steganography/watermarking techniques to preserve the copyright information etc. inside it. By authenticating concealed data one can recognize the genuine proprietor of a document andprovides a safeguard of valuable properties [23].
7. **Electronic Money Transfer:** Electronic money is based on secret and unspecified communications systems. Experts of different money transfer controlling bodies can consider steganographic data transfer as a prospective and safe mechanism.
8. **Radar Systems:** Recent transit radar systems can assimilate messages composed in a radar base station, to avoid transmitting text files and images separately to the receiver's base stations.
9. **Remote Sensing:** Remote sensing [27] combines the vector maps and digital imagery of a site. It improves the analysis of the cultivated areas, including urban and natural locations among others.
10. **Digital Elections:** A massive amount of money is spent to complete the elections every year. The governmentsof different countries may think of a new idea of the digital election that needs lower cost. May even shrink the public harassment as everyone can cast his/her vote from home.

Some other applications include annotation and SmartSteg on mobile devices, thereby securing multimodal biometric data [28]. Steganography is not only popular for its ethical values but also for some dishonest issues, like spreading spam, mischievous viruses, and harmful links sent by the cyber-criminals.

6. Classification of Steganographhy

Image steganography can be categorized into two domains: spatial domain steganography and transform domain steganography as shown in Fig. 6.

6.1. *Spatial Domain based Steganography*

The easiest approach of message hiding in images is to embed the message in the cover image pixels in the spatial domain [29] itself. Here, pixel values are modified directly for embedding the stealthy message. Spatial domain techniques provide easiness in embedding and extraction compared to frequency domain techniques. Different spatial domain techniques are presented in Fig. 7.

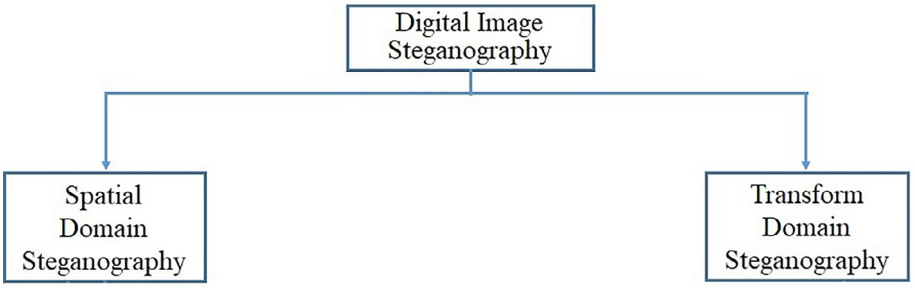

Fig. 6. Classification of digital image steganography techniques.

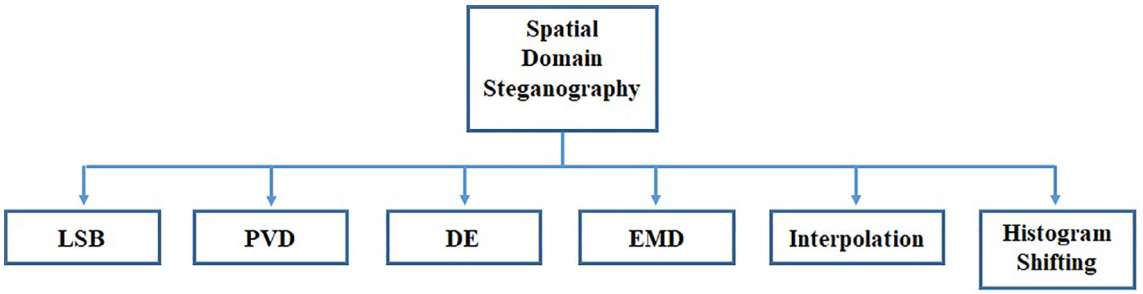

Fig. 7. Spatial domain steganography techniques.

6.1.1. *Least-Significant-Bit (LSB) Technique*

LSB based steganography [30] provides the simplest way of embedding secret data within the cover image. It normally substitutes the LSBs of chosen pixels of the cover image with stealthy data. LSB based approach uses LSB substitution and LSB matching techniques. LSB substitution works by embedding the secret information at the rightmost bits to keep the pixel distortion minimum as shown in Fig. 8. The mathematical illustration of LSB based data hiding technique can be defined using Eq. (4) as:

$$A' = A - A \bmod 2^n + d, \tag{4}$$

where A and A' specifies the pixel value of cover and stego images. n specifies the number of bits replacement. Message extraction is straight forward; just extract the n-LSBs from the pixel. Mathematical representation of the extraction process can be defined using Eq. (8) as:

$$d = A' \bmod 2^n. \tag{5}$$

In the beginning, LSB based steganography [31] simply has focussed on developing a system for increasing the embedding capacity only. Over the years, thesteganalysis arena has become more powerful to crack such atechnique using statistical analysis. After that researchers have given more concentration to present robust LSB schemes based on cryptography and steganography which can dodge such steganalysis attacks [32]. With time, also several variations of LSB based steganographic schemes have been developed to enhance the embedding capacity while keeping the good image quality. In sequen-

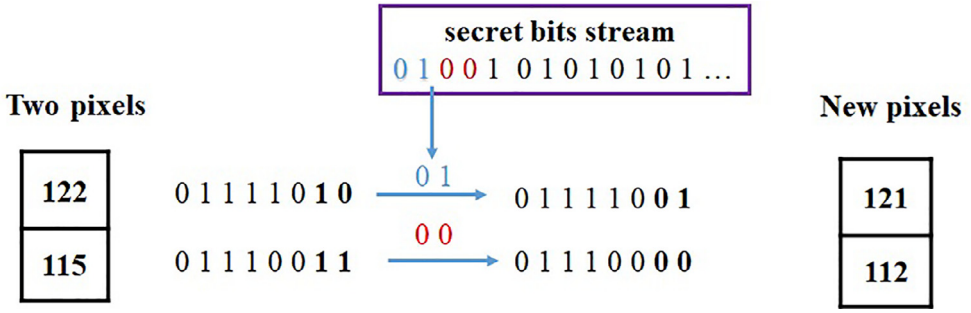

Fig. 8. An example of LSB substitution method.

tial embedding, stealthy bits are embedded in the LSBs of the adjacent pixels, while random embedding allocates the bits of the stealthy message randomly throughout the whole image [33]. In LSB matching [34], when the stealthy bit and LSB of the pixel are found identical, the concerned bit of the pixel remains unchanged, otherwise, 1 is subtracted or added at random. LSB substitution is easier to identify compared to LSB matching. A data hiding technique using interpolation followed by LSB substitution methods is presented by Jung and Yahoo [35].

The work [36] has developed a scheme for embedding a sequence of the stealthy messages in the cover pixel using the modulo three strategy. In each grayscale pixel, it can hide two ternary numbers by modifying the two LSBs. The embedding capacity of the method is 3.17 bpp. The security of the technique has not been tested by the standard tool like Stirmark benchmark 4.0. The work [34,37] recommends multi-bit steganography in the high energetic pixels using properly well-defined energy functions. The work allocates the data in chosen portions of a cover image using a variety of embedding techniques. The techniques do not share any key between the sender and the receiver. The algorithms keep no signature in the stego images with high payload. Jain [38] has developed a scheme using LSB and scrambling arnold method, to make the steganography safer.

Biswas et al. [39] have explored the multi-bit LSB (mLSB) steganography in color images. This algorithm withstands the test, StirMark Benchmark 4.0, ROC, dual statistical method, and histogram difference. The work [40] suggests a protected lip biometric framework. The work uses spatial steganography to hide the subject's identifier on the conforming lip image hiding identity. The accuracy of recognition of the framework is 92.8% which is comparatively low. A double-level reversible data hiding scheme utilizing the revised LSB matching approach has been presented in [41]. It shows security against steganalysis tests like RS analysis and PDH analysis. The security of the technique can be tested with the RS analysis, color frequency test, and standard tool Stirmark Benchmark 4.0. ROC curve shows the security of a technique which is missing in the article.

The LSB technique can be used with less computational complexity. It is very flexible to incorporate with other methods, but it directly affects the stego image quality. Steganalysis tool can easily detect the LSB based steganography [30]. The image quality can be improved by reducing the distortion in LSB based techniques. Distortion in the LSB based techniques can easily be minimized by the following 2^n correction method.

Let the cover pixel be $A = 31$, $L = 4$, and 4 bit confidential message $M = 0001$. The corresponding decimal value $d = 1$. Using Eq. (4), the stego pixel $A' = 17$. The original value 31 has been converted to 17. Hence, a massive alteration has happened for the n-LSB technique.

2^n Correction Method

It reduces the difference between the cover and stego pixels of the multi-bit LSB based embedding. The main purpose is to reduce the distortion in the stego image. It can be defined as:

$$R = A \bmod 2^n - d. \tag{6}$$

and

$$A' \leftarrow \begin{cases} A - R + 2^n, & \text{if } R > 2^{n-1} \text{ and } d < 255 - 2^{n-1}, \\ A - R - 2^n, & \text{if } R < -2^{n-1} \text{ and } A > 2^{n-1}, \\ A - R, & \text{Otherwise.} \end{cases} \tag{7}$$

Now, $R = 31 \bmod 2^4 - d = 15–1 = 14$. Using Eq. (6) and Eq. (7) of 2^n correction: $A' = A - R + 2^n = 31–14 + 16 = 33$. Now, the distortion becomes 2. Hence, a huge quality enhancement has happened using 2^n correction strategy over the n-LSB method. The extraction of the confidential message using the n-LSB method can be defined using Eq. (8) as:

$$d' = A' \bmod 2^n, \tag{8}$$

where A' reprsents the stego pixel and d' represents the decimal value of the n confidential message. Here, 2^n corrected stego pixel = 33 and $n = 4$. Now, $d' = 33 \bmod 2^n = 1$. Substituting 1 into n bits binary, the extracted message becomes 0001.

6.1.2. *Pixel Value Differencing (PVD) Technique*

Secret bits cannot be concealed enormously in the smooth areas in an image, but edge areas can tolerate immense modification. Based on this notion PVD based data hiding technique [42] is proposed. A cover image is divided into non-overlapping windows of two pixels.Stealthy messages are embedded in the difference between two pixels where the difference is evaluated as, $B_i = k_{i+1} - k_i, |B_i| \in [0,255]$. The pixel value range $R = [0,255]$, divided into contiguous sub-ranges. A probable sub-ranges can be [0, 7], [8, 15], [16, 31], [32, 63], [64, 127], [128, 255]. Width of the sub-ranges can be calculated as, W_i = Lower bound (U_a^i) - Upper bound (L_a^i) + 1. Maximum number of embeddable bits in a block is evaluated as, $C_i = \lfloor \lg (W_i) \rfloor$. After adding the lower bound of the sub-range with the integer value of the secret bits b, the new difference becomes B_i' = $L_a^i + b$ and $M_i = |B_i' - B_i|$. Finally, the new pixel pair (K_i', K_{i+1}') is calculated using Eq. (9) as:

$$(K_i', K_{i+1}') \leftarrow \begin{cases} K_i - \left\lceil \frac{M_i}{2} \right\rceil, K_{i+1} + \left\lfloor \frac{M_i}{2} \right\rfloor, & \text{if } B_i \text{ is odd number,} \\ K_i - \left\lfloor \frac{M_i}{2} \right\rfloor, K_{i+1} + \left\lceil \frac{M_i}{2} \right\rceil, & \text{if } B_i \text{ is even number.} \end{cases} \tag{9}$$

Fig. 9 displays the PVD based data embedding technique. Let us take two adjacent pixels (30,50). Their difference value is 20. Since, 20 lies within the range of 16 through 31. So, 4 bits can be concealed. After adding the integer value of 4 bits i.e., 10 with the lower bound of that range, the new difference becomes 26. The stego pixel pair calculated as (27, 53). In the extraction process, the lower bound of the corresponding range is subtracted from the difference of the two pixels.The extracted value will be $b = |27 - 53| - 16 = 10$. Many variations have been presented in the PVD based steganography method, by studying the correlation among pixels. Several region-based methods, from two to nine neighborhoods, have been applied to obtain the optimized level of data hiding. In literature, several mechanisms are proposed to solve the limitations of PVD and to improve embedding capacity. The overflow/underflow situation has not been discussed in the paper. To evaluate the security of the technique PDH analysis, color frequency test, and relative entropy can be applied.

For enhancing the payload, a try-way PVD scheme is presented in the works [43,44]. The original PVD method considers only one direction embedding using two neighboring pixels. Here, using four neighboring square pixels, three direction embedding is considered for enhancing the hiding capacity as shown in Fig. 10. In Chang et al. [43], an optimal approach and adaptive rules have been introduced for preventing the quality alteration of the images. Wang et al. [45] have presented a scheme for avoiding the falling-off-boundary problem. Optimal tactics have been taken to decrease image distortion. The technique is safe against the RS analysis. Lee et al. [6] have utilized the image compression concept with the already existing tri-way data hiding technique. After compressing the image by JPEG2000, the compressed image is embedded by tri-way PVD. In this multi-way embedding, pixel value changes to a great extent. Some of the pixel values might fall in overflow/underflow situations. However, the authors of the paper have not enlightened this matter. The work should have been evaluated by the pixel difference histogram, color frequency test, and relative entropy. For further advancement of the efficiency, some enhanced forms of PVD based technique have been researched. To enhance the data hiding capability, several mechanisms have been proposed by merging LSB with the PVD method. Jung [46] has developed a steganographic scheme applying PVD and LSB replacement technique. The main concept is to apply the PVD technique on the edge area and the LSB technique on the smooth area. Khodaei [47] et al. have presented an adaptive message embedding technique using LSB substitution and PVD method.

Hussain et al. [48] have projected a data hiding technique that enhances the security by two-layer embedding schemes, improved Rightmost Digit Replacement, and PBPVD. It enhances all three aspects of data hiding. To test the security of the technique, the work needs to be analysized by the standard tool Stirmark Benchmark 4.0. Hussain et al. [49] have enhanced the embedding capacity by combining the irreversible and reversible methods. Four steganographic methods: PVD, PVD shift, LSB substitution, and MPE have been merged to form a new data hiding scheme. Hence, the payload has increased significantly. This technique is robust against RS steganalysis. Due to the combination of four data hiding techniques, obviously the overflow/underflow situations may happen, but the topic has not been highlighted in the technique. An effective stenographic scheme is presented by Li et al. [50] that mixes PVD, modulus function, and PSO methods. PVD and modulus functions are used to hide the information. PSO method is to improve the quality of the images.

Mukherjee et al. [51] have shown a PVD based multi-bit embedding technique. Due to embedding in both high and low contrast pairs, the embedding capacity improved. The authors of the work [21] have presented a steganographic scheme using multi-way PVD (MPVD) and decreased difference expansion (DDE) methods. The security of the work is tested against several statistical attacks. It is also tested by the steganalysis tool, StegExpose. The Hussain et al. [52] have developed a steganography scheme using the adaptive LSB and PVD techniques. After embedding the confidential message, a readjustment strategy has been made to retrieve 100% of the secret message. The work has not shown the prevention of

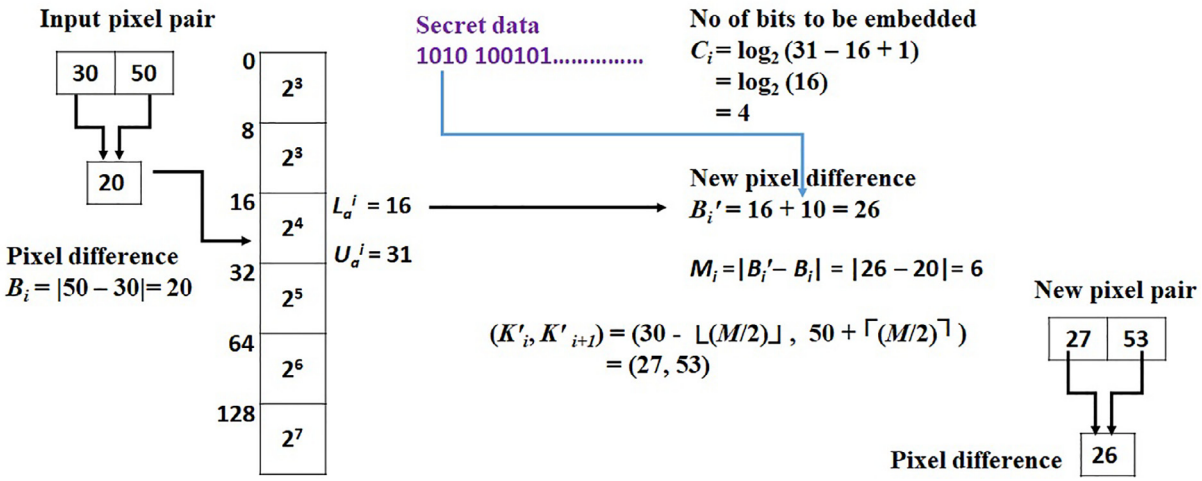

Fig. 9. Sample example of PVD method.

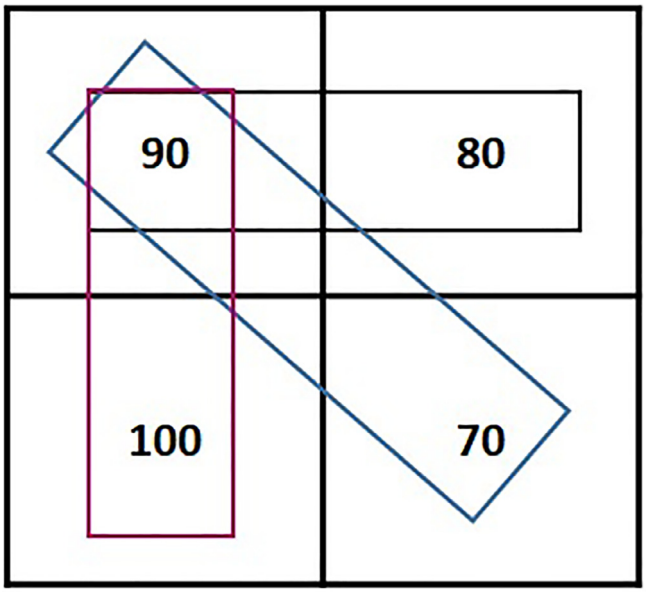

Fig. 10. An example of 3PVD method [43].

the overflow/underflow situation during embedding the secret message. The recent deep learning based steganalysis tools can be used to test the security of the technique.

6.1.3. ***Difference Expansion (DE) Technique***

In DE based data hiding [53], a cover image is divided into non-overlapping blocks of two pixels. Consider a pixel pair (U, V), their average value m and difference D can be obtained by Eq. (10),

$$m = \frac{U+V}{2}, D = U - V. \tag{10}$$

The inverse transform of Eq. (10) can be obtained from Eq. (11) as:

$$U = m + \lfloor \frac{D+1}{2} \rfloor, V = m - \lfloor \frac{D}{2} \rfloor. \tag{11}$$

Hu et al. [54] have presented a DE method that has used the vertical and horizontal difference images. This method has applied a modified histogram-based difference selection and shifting methods have been applied for making the scheme robust to different categories of images.Lee et al. [55] have presented a reversible message embedding method using prediction of difference expansion. Peng et al. [56] have developed an RDH technique on adaptive embedding and integer transform. The method can hide 2.17 bpp in Lena image with PSNR 20.71 dB. Location map is used in the technique to take the information about overflow/underflow condition. The location map reduces the embedding capacity and needs to be sent to the receiver. It also creates concern about security.

Most of the DE methods have tried to decrease the amount of secondary information for embedding into the cover images. This secondary information keeps only information about overflow/underflow problems. Gujjunoori et al. [57] have developed a DE method to decrease the secondary information, for enhancing the amount of hidden data. A layer-2 DE embedding method has been introduced for preserving the secondary information. Experimental results show the superiority of the work with existing similar state-of-the-art works. Wang et al. [58] have developed an RDH scheme based on bi-directional DE. At first, it converts the cover image into a 1D array in a *Z*-shaped style. After that, the difference between two adjoining pixels has been extended on both sides to conceal one bit into the left pixel. Al last, the 1D array has been transformed to a 2D array for accomplishing the stego image. During extraction, stego image is converted to a 1D array in the *Z*-shaped way. Then, the difference between two neighboring pixels is compressed towards both ways to retrieve the concealed message and to recover the cover 1D array. Finally, a 1D array is converted to a 2D array.

In DE based data hiding, payload is very low compared to other techniques. Image quality also degrades significantly. The limitation of the DE based techniques is that it distorts the visual quality of the images very much. To reduce the distortion during embedding the difference between two pixels needs to be reduced. This can be easily done by a logarithm function as shown in Fig. 11 and Fig. 12. In Fig. 11, the original difference between 37 and 64 is 27. Using a logarithm function the difference has been reduced to 11 to minimize the distortion. The extraction process works in the opposite way to obtain the original difference 27, using the logarithm function.

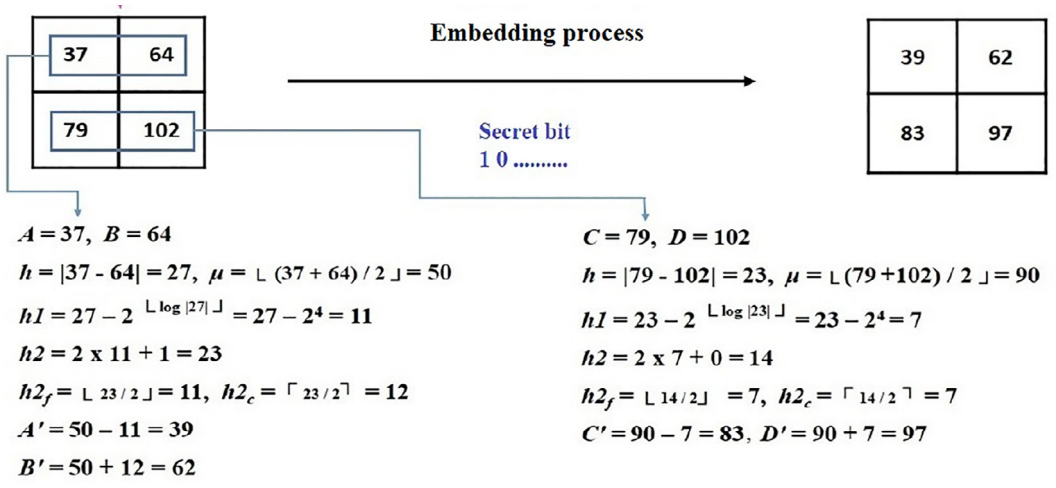

Fig. 11. Example of reduction of the difference strategy during DE based embedding process.

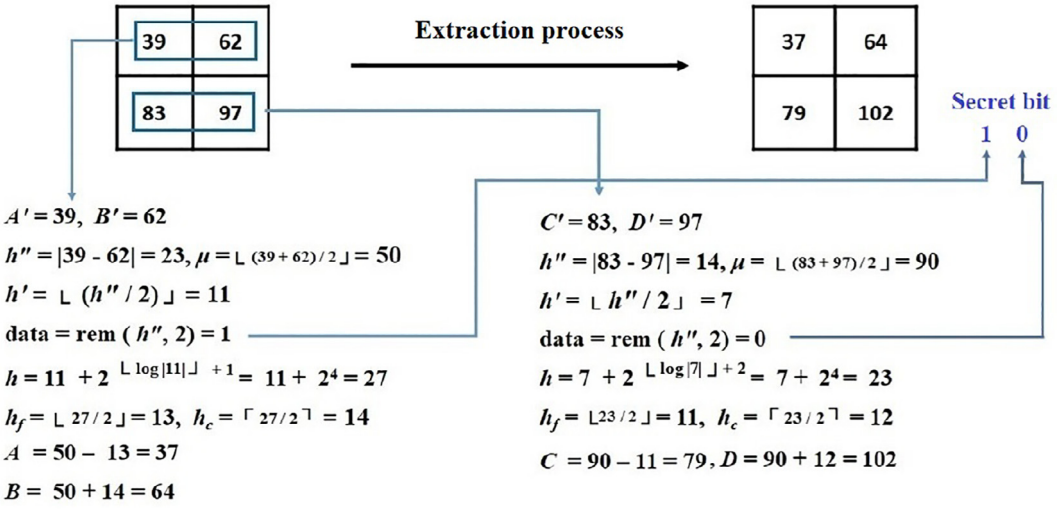

Fig. 12. Example of DE based extraction process using the reduction of the difference strategy.

6.1.4. *Exploiting Modification Direction (EMD) Technique*

In this technique [59] every stealthy digit in a 5-ary notational system is formed using 2 cover pixels. One pixel is enlarged or reduced by 1. For each group of 2 pixels, there are 5 different ways of modification. Let us consider a secret digit as x and a function using Eq. (12) as:

$$p = p(e_1, e_2, e_3, \ldots, e_m) = \left[\sum_{j=1}^{m}(e_j \times j)\right] \bmod (2m+1), \tag{12}$$

where $e_1, e_2, \ldots, e_m$ are cover pixels and $m = 2$.

If $p = x$, then pixel value will be unchanged. Let $s = x - p$. If $p \neq x$ and $s \leqslant m$, then increment e_s by 1. If $p \neq x$ and $s > m$, then decrement e_{2m+1-s} by 1. Let the stego pixels be $e'_1, e'_2, \ldots, e'_m$. In case of extraction, a secret digit is computed by Eq. (13),

$$y = p(e_1', e_2', \ldots, e_m') = \left[\sum_{j=1}^{m}(e_j' \times j)\right] \bmod (2m+1). \tag{13}$$

Example: Let $m = 2$, $e_1 = 102$, $e_2 = 19$ and x be the digit 0_5, then $p = p(102,19) = (102\times1 + 19\times2) \bmod 5 = 140 \bmod 5 = 0$. Since x and p are equal, e_1 and e_2 remain unchanged, i.e., $e'_1 = 102$ and $e'_2 = 19$. During extraction, $y = p(e'_1, e'_2) = (102\times1 + 19\times2) \bmod 5 = 140 \bmod 5 = 0$. So, 0_5 is extracted. Now let us consider, $x = 2_5$, $p = 0$, then $s = x - p = 2 - 0 = 2$. Here $x \neq p$ and $s \leqslant m$, so $e_s =$

$e_2 + 1 = 19 + 1 = 20$ and $e'_2 = 20$. In case of extraction, $y = p(e'_1, e'_2) = (102\times1 + 20\times2) \bmod 5 = 142 \bmod 5 = 2$. So, 2_5 is extracted. If x is 3_5, $p = 0$ and $s = x - p = 3–0 = 3$. Since $x \neq p$ and $s > m$, the new pixel becomes $e_{2m+1-s} - 1 = 19–1 = 18$. So, $e'_2 = 18$. In extraction, $y = p(102,18) = p(102\times1 + 18\times2) \bmod 5 = 138 \bmod 5 = 3$. So, 3_5 is extracted.

Zhang et al. [59] have fully exploited modification directions. One secret digit can be hidden for each pixel pair. The technique has low payload compared to other embedding techniques. There is a possibility of embedding more data without disclosing it to the human eye. Security against statistical attacks has not been discussed in the work. To enhance the payload, Chang et al. [60] have presented a 2-stage EMD method. Lee et al. [61] have proposed a 8-ary embedding EMD technique, but still, there is a chance to embed a more secret message. Wang et al. [62] have presented a scheme that hides $2n$ digits into each set of $(2n + 1)$ cover pixels. Maximum embedding capacity of the technique can be up to 2 bpp. PSNR is always more than 45 dB for all the images. For the different values of K, this technique has shown only the variations of embedding capacity and PSNR values. Resilient against the different steganalysis attacks which is an important criteria in steganography has not been explained in the work. Kim [18] has presented a method termed as CIE which has used a code book to enhance the performance of EMD technique. The technique shows the hiding rate, $R = \frac{log_2(2^{n+x}-1)}{n}$. It is superior to the original EMD method, where $R = \frac{log_2(2n+1)}{n}$ for $n \geqslant 2$. The method hides 3 times as many bits as the original EMD method if $n = 2$ and $x = 5$. Fig. 13 depicts the ROC curve of the CIE technique. The method shows good results against the HCF-COM detector. The work [63] has established an embedding scheme based on Modified Signed-Digit. For a group of n pixels only $\lceil \frac{n}{2} \rceil$ pixels is altered and the value is -1 or $+1$. Stego image quality is greater than 52 dB when each group contains more than 4 pixels. An Extended EMD based data hiding utilizing Hashed-Weightage Array is presented in [64]. The embedding capacity is entirely variable in this scheme. Data hiding is done using a dynamic weightage array. The scheme is resilient up to 3 bpp against RS steganalysis. The security of the technique is vulnerable for the embedding capacity near to 4 bpp. The AUC under the ROC curve is also high. Therefore, the security of the technique should be analyzed further by the pixel difference histogram, color frequency test, and relative entropy. It will be even better, if the security of the technique is tested with recent deep learning based steganalysis techniques.

6.1.5. ***Interpolation based Steganographic Technique***

Image interpolation normally generates a high-resolution image from its low resolution. The interpolation technique estimates values at unknown points with the values at a known point. Jung and Yoo [65] have presented an interpolation technique with a traditional scaling-up process which is known as neighbor mean interpolation (NMI). The scheme computes the value of an unknown pixel with its nearest neighboring pixels. First, theinput image is down-sampled to $\frac{1}{4}$ of its initial size. It then, up-sampled the image to get its original size and generates the unknown pixel values in alternate rows and columns. Then, the NMI method is used to enlarge this image to become a cover image as shown in Fig. 14. Stealthy data is hidden within the up-sampled cover image to generate stego image. The receiver extracts the hidden message from the stego image without using the cover image. Thetechnique offers a very low complexity. NMI technique hides the message into the difference between two pixels. The quantity of stealthy messages can be enhanced, if the difference between two pixels is increased. The scheme has utilized 2×2 non-overlapping blocks. So, the payload is limited. Considering the above limitation, the work [66] has proposed the interpolation by neighboring pixel (INP) technique. It has utilized 3×3 pixels for enhancing

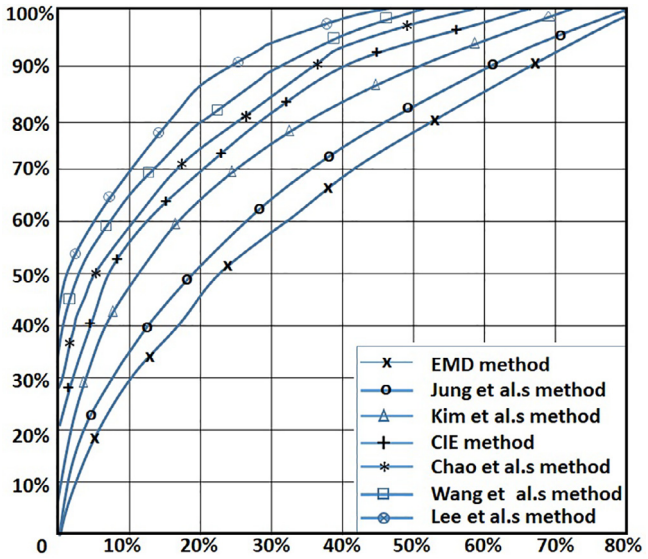

Fig. 13. ROC curve with a 100% payload [18].

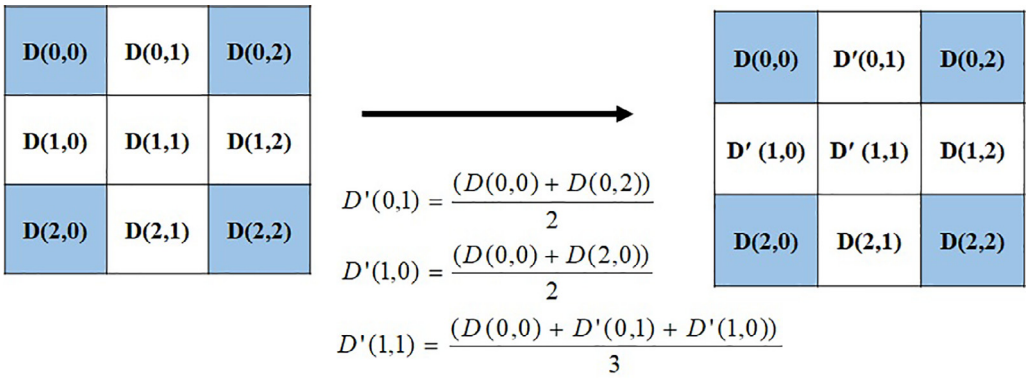

Fig. 14. NMI interpolation method [65].

the payload. The method provides a high payload with low computational time. It can embed up to 2.28 bpp and has achieved higher PSNR than NMI.

Chang et al. [67] have presented a two-stage data embedding technique using histogram modification and image interpolation method. PSNR value is improved by 43 % from its previous methods. The results show their superiority over NMI and INP methods. Malik et al. [68] have proposed a modified neighbor mean interpolation (MNMI) method based on the NMI method. MNMI has given extra weightage to the adjoining pixels. Though the authors have tested the technique using RS analysis, other standard statistical tests like color frequency test, kullback–leibler divergence test can be applied. The recent deep learning based steganalysis tools can also be used to test the security of the work. The work [69] has established a data embedding method based on enhanced EMD and interpolation with side-match prediction. Their method shows superiority over several previous state-of-the-art works. Lu et al. have [13] presented an interpolation based RDH technique applying the variance in the re-encoding approach. It uses a modulus function and a weighted matrix to calculate the modulus value to embed the stealthy information. Due to the use of re-encoding strategy and modulus function, it is required to calculate the computational complexity of the technique. The technique has only described the results of steganalysis attack by StegExpose, but has not presented the ROC curve which shows the security of a technique.

The work [70] has developed a data hiding technique using parabolic interpolation. They have used the 1D parabolic interpolation technique for data hiding. Their work is limited to 1D interpolation. So, it became unsuccessful to use the spatial redundancy of the cover image. The scheme not only suffers from lower embedding capacity, but also from visual quality. The security of the scheme needs to be tested by color frequency test, RS analysis, and relative entropy etc. Later, a high capacity RDH scheme with 2D parabolic interpolation has been proposed by the Shaik et al. [71]. It beats the previous interpolation based 1D parabolic methods in terms of PSNR and payload. However, the visual quality of the images in this method is very low. The security of the method has not been analyzed with RS analysis, χ^2 test and pixel difference etc. The technique ultimately remains computationally expensive.

The authors of the work [72] have presented a two-layer data hiding technique based on interpolation based data hiding and difference expansion that achieves high embedding capacity. Experimental results depict the usefulness of the developed technique. The limitation of the technique is the low PSNR value due to interpolation and difference expansion technique. The difference expansion technique increases the distortion within the images drastically. The visual quality of the images can be enhanced by reducing this difference with a logarithm function as shown in Fig. 11 and Fig. 12. Also the security of the technique can be analyzed by the recent deep learning based steganalysis techniques.

6.1.6. ***Histogram Shifting (HS)***

In histogram shifting [73], the histogram of the cover image is produced. After that, one or more pairs of peak and zero points are chosen as shown in Fig. 15. Here the peak point is at pixel value 152 and the zero point is a pixel value 249. Later, pixels between the zero and peak points are shifted towards the zero point, taking one step to free for message hiding. At the last stage, the stealthy data is hidden into pixels with the peak value in the histogram. The payload is decided by the number of pixels with the peak level [74]. Analyzed image retains a high quality since the alteration of pixels is regulated within one. It offers better quality images compared to most of the remaining RDH techniques. The embedding capacity is restricted by the number of peak points. Embedding capacity is low and for a flat histogram, this technique does not work well.

Histogram-based RDH is presented first in the work [75] where peak points with high frequencies in the histogram are used to hide the message. Each pixel is modified by 1 and a very good quality image is produced. The techniques mainly concentrate on exploiting inter-pixel associations to generate a 1-D histogram. For one pair of largest and smallest points, the entire image is scanned three times during embedding. It increases the computational complexity. Hence, the computational complexity of the technique needs to be measured. In work [76], a novel method applying 2-D DH is presented by considering all pixel-pair to originate a difference-pair. For enhancing the embedding capacity, many advancements for the HS-based techniques are developed. One approach is to fragment the cover image into multiple blocks, and then

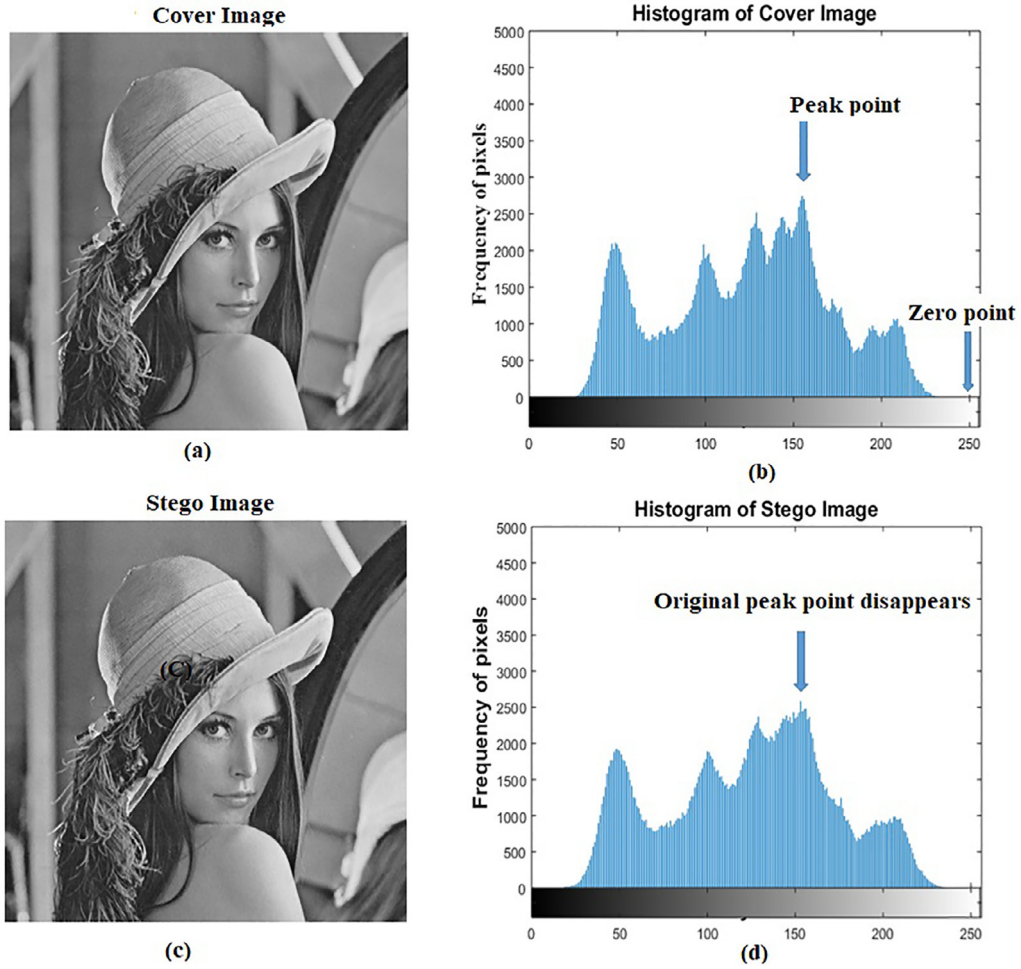

Fig. 15. (a) Lena image (b) Histogram of Lena image (c) Stego image (d) Histogram of stego image.

apply the HS technique of the work [75] distinctly. These techniques are called block-based histogram shifting (BHS) [77–79] techniques that can enhance the payload while dodging the underflow/overflow situation. In the work [79], the bad blocks are not utilized for embedding the data which reduces the embedding capacity. The discussion about computational complexity is missing in the paper. The recent learning based steganalysis techniques can be used to test the security of the work.

Another approach that is very popular in recent times for improving the HS based data hiding technique is prediction error histogram shifting (PEHS) [80,81]. In these techniques, prediction errors are achieved after processing the image by a prediction method. Stealthy messages are hidden into the prediction errors instead of the original image. For increasing the payload, a more advanced prediction for a more sharply distributed histogram is needed. Another approach to enhance payload is to spread the chosen bins for data hiding. Hsiao et al. [81] have stretched the technique from a 1-D to a 2-D histogram shifting. Since, image distortion occurs when the hiding bit is "1" in HS-based techniques. Xie et al. [82] have developed a signed-digit representation technique that surprisingly reduces the appearance of "1" and increases the appearance of "0". The experimental results depict that the presented technique offers a better payload than existing state-of-the-art works. Pixels in the first row are not utilized for embedding the confidential message. First row is used for storing the overhead data, viz., the values of n peak points. If the number of peak points increases the overhead information also increases and it reduces the embedding capacity as well. The security of the technique can be tested by the recent deep learning based steganalysis techniques.

Special domain steganography is weak against any small changes, due to some operations like scaling, rotation, and cropping, though they have achieved high data hiding capabilities. Also, these methods show poor robustness in image filtering and lossy compression. To increase the security and robustness of a scheme, transform domain becomes an alternative approach for steganography.

6.2. *Steganography in Transform Domain*

The transform domain [2] converts a cover image to obtain the frequency spectrum representation. Here, the secret bits are embedded within the frequency coefficients of the sub-band. Embedding and extraction are more complex here compared to the spatial domain, but it improves the safety of the system. Furthermore, the transform domain techniques are less affected by rotation, scaling, and compression. Therefore, the frequency domain methods are highly secured compared to spatial domain techniques. Several frequency domain techniques have been used in steganography and the most common methods are DCT, DFT, DWT, and IWT as shown in Fig. 16. Another transform domain based technique using First Fourier Transform (FFT) is demonstrated in the work [83].

6.2.1. *Discrete Cosine Transform (DCT) based Steganography*

DCT is an extensively used tool in frequency transformation. JPEG has applied the DCT [84,85] for image content transformation. The forward 2D-DCT [86] equation on 2D images can be written using Eq. (14) as:

$$F(x,y) = \frac{2}{M}C(x)C(y)\sum_{i=0}^{M-1}\sum_{j=0}^{M-1} f(i,j) \times \left[cos\left(\frac{\pi x(2i+1)}{2M}\right)cos\left(\frac{\pi y(2j+1)}{2M}\right)\right], \tag{14}$$

where $F(x,y)$ is the frequency coefficients of $M \times M$ blocks, $f(i,j)$ is the gray scale image and $C(x), C(y)$ are the constant scale factors, where,

$$C(x) = \begin{cases} \frac{1}{\sqrt{2}} & for \quad x = 0 \\ 0 & Otherwise \end{cases}.$$

and similarly for $C(y)$.

The inverse equation is obtained in Eq. (15) as,

$$f(i,j) = \frac{2}{M}\sum_{x=0}^{M-1}\sum_{y=0}^{M-1} C(x)C(y)F(x,y) \times \left[cos\left(\frac{\pi x(2i+1)}{2M}\right)cos\left(\frac{\pi y(2j+1)}{2M}\right)\right]. \tag{15}$$

Commonly used steganography tools like JSteg [87], OutGuess 0.1 [88], OutGuess 0.2 [88], F5 [89], nsF5 [90], and UED [91], based on DCT domain are discussed in Section 10. The work [84] has proposed a scheme on JPEG images where stealthy information is hidden within the quantized DCT coefficients. For enhancing the payload Tseng et al. [92] have offered a high payload scheme using the LSB substitution technique. The technique uses a capacity table for calculating embedded bits in each DCT component. After that, Chang et al. [93] have developed a lossless reversible steganographic method in quantized DCT components. This technique can only hides confidential message into consecutive zero coefficients in the medium area; non-zero coefficients in the medium area can not be utilized. Hence, the technique achieves low embedding capacity.

Lin et al. [94] have stretched Chang et al. [84,93] to form a steganographic technique using notation transformation concepts. For the better stego-image quality Lin [95] has used the idea of decomposition of images. Stealthy information is hidden into the high-frequency components. Integer mapping is used here to implement the 2D-DCT transformation. It shows higher PSNR and payload than the works in [84,93]. Again, Lin has used integer mapping for implementing their DCT transformation in the work [96]. Rabie and Kamel [97] have estimated the data hiding capacity limits in the color images. Their method has found the bonding between image quality and the embedding capacity. Hou et al. [98] have established an RDH technique, based on JPEG image quantified DCT coefficients with different frequencies. For decreasing the whole distortion for the analyzed image, coefficients from frequencies are selected. An advanced block selection approach is utilized that yields less simulated distortion. The embedding capacity of the technique is low. The security of the technique can be analyzed by several statistical attacks. The deep learning based steganalysis techniques can also be used to test the security of the technique.

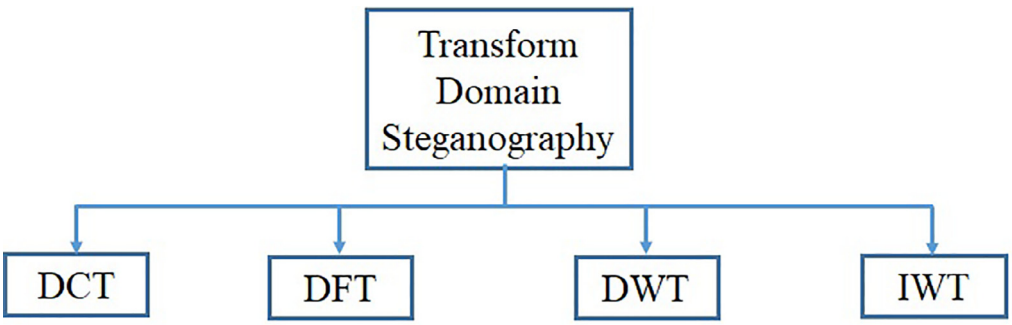

Fig. 16. Different Transform Domain steganography.

The main drawback of DCT based steganography is rounding errors. Also, DCT based steganography suffers from artifact problems and it has very little data hiding capacity [99].

6.2.2. *Discrete Fourier Transform (DFT) based Steganography*

2D-DFT is applied in various image processing schemes. An image is partitioned into corresponding sine and cosine frequency components. DFT [100] can be applied only on the real part of the data with an even symmetry. It can be defined using Eq. (16) as:

$$F(a,b) = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) e^{-j2\pi(\frac{ax}{M} + \frac{by}{N})}, \tag{16}$$

where $f(x,y)$ is the discrete signal and $F(a,b)$ is the spectrum of it. The reverse transformation can be defined using Eq. (17) as:

$$f(x,y) = \frac{1}{M \times N} \sum_{a=0}^{M-1} \sum_{b=0}^{N-1} F(a,b) e^{j2\pi(\frac{ax}{M} + \frac{by}{N})}, \tag{17}$$

where (x,y) is the pixel in the spatial domain and (a,b) is the frequency variable in frequency domain. Alturki and Mersereau [101] have developed a data hiding technique using quantization. Ramkumar et al. [102] have offered a competent scheme that is robust to lossy compression. Embedding capacity of the technique is low. Security of the technique can be analyzed with different statistical attacks as well as deep learning based steganalysis techniques. Liao et al. [100] have developed an embedding technique using Compressive Sensing (CS) and DFT. Steganography in DFT has very low data hiding capacity, less security, and low visual quality [2].

6.2.3. *Discrete Wavelet Transform (DWT) based Steganography*

2D-DWT [103] method transforms an image from the spatial domain to the transform domain. The commonly used and easiest transformation technique is Haar-DWT (HDWT). HDWT [103] can be constructed by horizontal and vertical operations on the images. Horizontal operation partitions an image into a low-frequency (L) and a high-frequency band (H). Then L and H further decompose into LL, LH, and HL, and HH of four sub-bands. LL corresponds to the low-frequency sub-band, LH and HL are middle-level frequency sub-bands, HH corresponds to the high-frequency sub-band. The LL coefficients are the chief component. If any modification is made to this sub-band, theobserver can easily notice the changes in the spatial domain, but any modification to the HH sub-band becomes imperceptible to human eyes. Wavelet-based transformation offers both frequency and spatial localization. Fig. 17 shows a 4-Level discrete wavelet transform of the Barbara image. Chan et al. [103] have developed a DWT based reversible message embedding technique that offers a high capacity and a high visual quality. Huffman encoding technique compresses the coefficients of the high-frequency band, then hides the stealthy message in the high-frequency part. The method uses the Huffman coding technique for recovering the cover image correctly. The embedding capacity is low. Security of the technique can be analyzed with several statistical attacks.

Sidhik et al. [104] have developed an improved scheme for color image steganography. The wavelet fusion technique has been used in this scheme. The security of the technique can be analyzed with recent deep learning based steganalysis tools. The technique has achieved low embedding capacity. Mukherjee et al. [105] have described the embedding of stealthy infor-

Fig. 17. 4-Level Discrete Wavelet Transform of Barbara Image.

mation by altering the neighboring pixels in the seed matrix. It withstands the statistical attacks as well as the StirMark benchmark attack. Subhedar et al. [106] have presented a data hiding technique with RDWT and QR factorization. In comparison to Singular Value Decomposition (SVD), QR factorization offers less computational complexity. Atawneh et al. [107] have introduced a steganographic technique on diamond encoding in the wavelet domain. The method increases an undesirable distortion to the images and reduces the security.

An improved digital image steganography schemehas been developed on DWT to confirm minimum alteration within the cover image [108]. The method has introduced two concepts; secret key computation concept and blocking concept. First one is used to make the scheme more robust and the second one is used to ensure minimum variation within the cover image. The work [109] has presented an embedding scheme based on the HVS model and a model for cover image statistics. The drawback of that technique is the perceptual characteristic degradation of the images. Embedding capacity of the technique has not been clearly discussed. The security of the technique can be analyzed by the recent deep learning based steganalysis techniques. The method fails to retrieve confidential messages accurately.

DWT is advantageous compared to other transform domain techniques like DFT and DCT. It is compatible with HVS which offers suitable perception quality. That is why the compression technique JPEG2000 uses DWT [104]. In comparison to DFT, DWT based methods offer both spatial and temporal information [99]. In contrast to DCT, they have a large hiding capacity. DWT based techniques are more secure against steganalysis attacks. However, steganographic methods using DWT have limitations in extracting accurate secret messages. That is why researchers use secret images instead of secret messages. The limitation has been overcome using steganography in the IWT domain.

6.2.4. ***Integer Wavelet Transform (IWT) based Steganography***

IWT [110] is suitable in data hiding techniques, where the cover medium needs integers. The lifting technique is used with floor and ceiling functions and integer coefficients are acquired without quantization. Simple filtering operation is used in lifting technique for modifying even and odd sample sequences. The modifications [111] are done by the Eq. (18) and Eq. (19) as follows:

$$O[i] = O_0[i] - \left\lfloor \frac{E_0[i+1] + E_0[i]}{2} \right\rfloor, \tag{18}$$

$$E[i] = E_0[i] + \left\lfloor \frac{O[i-1] + O[i] + 2}{4} \right\rfloor, \tag{19}$$

where $O[i]$ and $E[i]$ are odd and even samples respectively. Xuan et al. [112] have introduced an image steganographic technique on IWT which provides distortion less stego image and it hides much more information than the other existing state-of-the-art works. The work has used image histogram modification to overcome the possible grayscale overflow problem. The work [113] has established a steganographic method, RIASIWT, that embeds the confidential information in mid and low-frequency sections of the image where energies are high. The scheme also makes cover image tuning before embedding the stealthy message for confirming lossless recovery. The scheme confirms robustness against compression and filtering. The author of the paper [114] has developed a scheme based on the IWT and Munkres assignment technique. The assignment algorithm helps for the best matching between the blocks, to hide the stealthy image. It hides the stealthy image in different coefficients of cover image bands. High-quality stego image and extracted stealthy image looks perceptually alike with their corresponding original images.

An IWT based image steganography technique using PVD has been developed in the work [115] that embeds confidential data in all the subbands, but it suffers from low embedding capacity. Experimental results confirm the dominance of the scheme over other PVD based methods in terms of security and payload. Xiong et al. [116] have introduced a technique using IWT, histogram shifting, and orthogonal decomposition on encrypted images. Experimental results have revealed its superiority over state-of-the-art works, in terms of PSNR with the same payload. In the work [117], the confidential message has been concealed into the LSBs of the low-frequency coefficients. Due to this reason, the scheme achieves low embedding capacity. Kalita et al. [118] have developed an IWT based method using LSB technique. Only the high-frequency subbands are utilized to conceal the secret message. The scheme is secure against SPAM steganalysis, χ^2 test, and RS steganalysis successfully. The security of the method can even be analyzed with the recent deep learning based tools.

Ma and Wang [119] have presented an RDHEI method, based on IWT that provides complete reversibility. High-frequency coefficients are utilized for embedding the confidential data by pre-processing the images. For compression to become lossless, a ratio correction method has been introduced. Furthermore, the method implemented an adaptive correction scheme to improve the payload. IWT has been performed in multiple stages and embedding is performed on multiple levels. The experimentalresult shows their superiority over other existing methods. An effective steganographic method constructed on IWT and Multidirectional Line Encoding (MDLE) has been presented in the paper [120]. At first, the host image is decomposed into four sub-bands with Haar-IWT. Each sub-band is then partitioned into 3×3 non-overlapping windows. The center coefficients in each window are coupled with adjacent coefficients in eight directions. The MDLE-IWT method proves their security against common attacks. Muhuri et al. [121] have developed an IWT based steganographic scheme using particle swarm optimization (PSO). Optimal pixel adjustment process (OPAP) enhances perceptual transparency. It suppresses

other methods with a high computational time. Mandal et al. [122] have established an IWT based high capacity steganographic technique to overcome the low embedding capacity problem of the IWT methods.

A comparison between spatial domain and transform domain based steganography is shown in Table 4.

7. Adaptive Steganography

Adaptive steganography is used in spatial and frequency domains with an added layer [2]. Adaptive nature can be presented in the steganographic techniques: by choosing the target pixels in the cover image, nature of adjustment to be made, the number of bits hidden in a pixel, etc. Several fundamental works in steganography, are based on adaptive methods. It receives statistical characteristics of the images. The changes in the location of the images occur according to these statistical records [123]. Chang et al. [124] have proposed an adaptive method in the LSB substitution technique for index-based images. The relationship between adjacent pixels has been utilized to assess the amount of smoothness. The distortion becomes low and imperceptible to the human eye. The size of the image dataset is not mentioned. The security of the technique has not been tested by the steganalysis tools. Wu et al. [125] have developed a GA based robust steganographic technique in the frequency domain by artificially counterfeiting statistical characteristics to break the inspection of the steganalysis system. This technique enhances the payload of the hidden information and increases the stego-images quality.

Tseng et al. [126] have presented a steganography method using OPAP and GA to disrupt the steganalysis system. Moreover, GA based algorithm improves the stego image quality. Somepopular content adaptive steganographic techniques like HUGO [127], WOW [128], and UNIWARD [129] are discussed in Section 10. The work in [130] has applied the LSB substitution and GA to enhance visual quality and security. Likewise, Kanan and Nazeri [131] have presented a GA based steganographic technique, considering the hiding process as a search and optimization problem. Using this adaptive method, hiding capacity and visual quality has been enhanced, but the main drawback is the increased computational complexity. The security of the technique can be analyzed with deep learning based steganalysis tools. Wang et al. applied GA to optimize the hiding rate and image distortion with several histogram shifting [80]. Emam [132] has developed a steganographic algorithm applying five protection layers for data hiding in color images. It has applied an image segmentation algorithm for embedding data randomly. Combining adaptive neural networkand MPSO, the scheme has achieved good quality and high security. Region-based approach, embeds the message on the edge details and high texture regions [86]. Deviations in edge and texture regions have higher imperceptibility than smooth regions. This type of approach has a low embedding rate, but robustness and imperceptibility are quite high.

Rabie et al. [86] have presented a DCT based data hiding method for color image steganography. They have implemented a global adaptive region hiding method which permits high embedding capacities. To test the security of the technique, it can be analyzed by the statistical attacks. It is highly encouraging to test the security of the technique by the recent deep learning based steganalysis techniques. Miri et al. [133] have presented an embedding scheme using adaptive wavelet transform and genetic algorithm.Ma et al. [134] have developed a RDH technique based on CDM and ML algorithms. The work [135] is an attempt to modify the edge-based image steganography using AI algorithms. AI based optimization techniques are used to hide the confidential message over optimal cover image blocks with minimal extraction error. Hussein et al. [136] have developed a coverless image steganography technique based on OMR and rule-based machine learning (RBML) algorithms. It has achieved low embedding capacity, but high security.

8. Deep Learning based Steganography

The quick progress in the area of artificial intelligence prompted the researcher to change their mind in the direction of deep learning based steganography [137]. Researchers have established that it is possible for machines to embed the confidential data in the digital image. The number of such methods that practice deep learning based algorithms are relatively less. The work [138] has established LSBS and matrix coding based steganographic scheme with feed forward neural networks for attaining improved capacity. Hu et al. [139] have developed a steganography without embedding (SWE) technique on deep CNN. The work maps the confidential message into a noise vector and utilizes the trained generator NN model to

Table 4
Comparison between spatial and transform domain based steganography.

Characteristics	Spatial Domain	Transform Domain
Payload	High	Limited
Pixel Manipulation	Direct	Indirect
Quality	High	Less manageable
Statistical attacks	Easy to detect	Hard to detect
Security (against geometric attacks)	Vulnerable	Resistant
Robust (against noise, rotating, compression)	Highly susceptible	Less susceptible
Computational complexity	Less time	High time

produce the stego image based on the noise vector. No embedding process is necessary at the time of image generation, and the message residing in the image can be retrieved by another NN after training. The method can exact accurate data and has the ability to obstruct the detection by steganalysis tools.

Another deep learning based steganography technique has been presented in the work [140]. A secure steganographic technique based on generative adversarial network is presented in the paper [141]. The architecture of the model is shown in Fig. 18. A Tanh-simulator function has been used in scheme to fit the optimal embedding simulator. U-Net based compact generator architecture is presented as the generator. To repel the recent progressive steganalysis schemes maxSRMd2, and selection channel awareness are integrated into the discriminator. Implementation of this technique in the JPEG domain will be a good idea.

An imperceptible steganography method linking generative adversarial network and mixed loss function is presented [142]. Here, a secret image is concealed within the same size original color image. A U-Net CNN structure-based steganography that combines two different networks has been presented in [143]. Tang et al. [144] have developed a secure steganographic technique that has the capability of misleading a CNN based steganalyzer. Ma et al. [145] have developed a practical adversarial technique to improve the security of distortion-minimizing steganographic techniques. The work uses the gradients back-propagated from the deep-learning steganalyzer to regulate the varying path of the pixels. This type of steganographic revision helps to increase the security against steganalysis. Yang et al. [146] have developed an improved GAN based technique, UT-6HPF-GAN, to learn the hiding cost for image steganography. The work has projected a new double-tanh function optimization. A U-Net based structure is used as the generator. Several high pass filters are fused into the discriminator to further improve the adversary training.

Shang et al. [147] have proposed a steganographic technique that produces the stego image through a GAN based model and adversarial example methods to let stego images escape from discovery. Three modules are working in the technique. The encoder module generates the stego image. Steganalyzer module checks the stego image whether they comprise the confidential data. Decoder module retrieves the confidential data from stego image. Ray et al. [148] have proposed a deep learning-based steganography to embed confidential messages. Deep supervision based edge detectors have been used with CNN for capturing more edge pixels. In the work [149], a CNN-based classifier is used to predict images that have high imperceptibility after data hiding. The CNN is based on SqueezeNet design, and trained on transfer learning and learned from scratch. The testing accuracy is not as good as training accuracy. The performance can be improved by considering a bigger dataset. The main problem with the deep learning based steganographic techniques is that these techniques are computationally expensive to train and execute the dataset for achieving the expected accuracy. GPU and large size RAM are required which are very expensive.

9. Performance Analysis and Recommendations

Performance of the recent state-of-the-art works have been analyzed in Table 5. The parameters that have been chosen for comparison are the advantages of a technique, drawback of the technique, embedding capacity, visual quality, and resistance against statistical attacks/steganalysis.

Some Recommendations

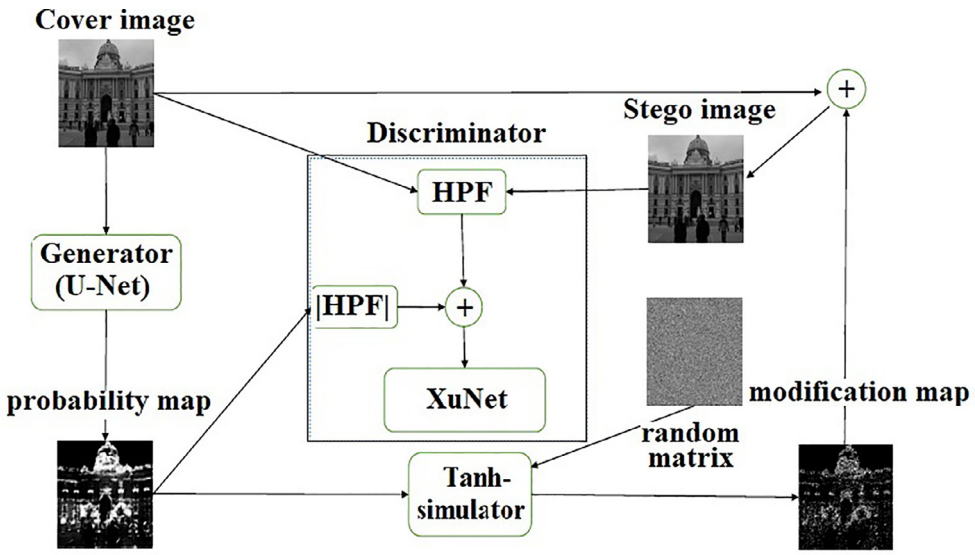

Fig. 18. Architecture of the UT-SCA-GAN [141] model.

Table 5
Performance analysis of recent state-of-the-art works.

Method & Reference	**Advantage**	**Limitation**	**Embedding capacity**	**Visual Quality** (PSNR)	**Resistance against statistical attacks/ steganalysis**
LSB [35]	Combination of interpolation and LSB technique improves the security	Weak against geometrical attacks or lossy compression.	2.25 bpp	37.5 dB	Security against Steganalysis test is required.
LSB [41]	Double-layer embedding provides security and high payload	Execution time is high.	6 bpp	48 dB	Withstands RS and PDH steganalysis.
PVD [21]	It provides higher embedding capacity with good visual quality	It is not reversible	2.88 bpp	38.50 dB	Deep learning based steganalysis test is required
PVD [50]	PSO method improves the quality of the images	Execution time is quite high	2.14 bpp	42.74 dB	Withstands RS Steganalysis
DE [57]	Decreases the volume of secondary data. Two-layer data hiding scheme. Used edge detection procedure.	SSIM index is low. Visual quality is low.	1 bpp	30.4 dB	Only precision and recall values are evaluated.
DE [58]	A RDH technique based on bi-directional DE. Decreases the image distortion rate by two-way difference extensions.	For embedding capacity of 1 bpp, visual quality decreases drastically.	0.7 bpp	32 dB	It shows strength against several Gaussian noises.
EMD [63]	For a group of n pixels only $\lceil \frac{n}{2} \rceil$ pixels are altered. Only ± 1 ranges variations.	Limited payload	1 bpp	$>$ 52 dB	Strong against RS Bit plane attacks.
EMD [64]	Utilized Hashed-Weightage Array. The array is created as pseudo random.	Tested only on RS steganalysis. Modern steganalysis test is required. Security lapses above 3 bpp.	4 bpp	35 dB	Resilient against RS steganalysis up to 3 bpp.
Interpolation [13]	Interpolation based RDH technique. It uses differences in re-encoding strategy. It uses modulus function and weighted matrix.	Execution time is higher than other state-of-the art works.	3 bpp	36 dB	It withstands the steganalysis tool, viz., StegExpose. Resilient against RS analysis.
Interpolation [71]	High payload RDH scheme applying 2-D parabolic interpolation.	Embedding capacity and PSNR is low. Execution time is slightly high.	1.7 bpp	27.4 dB	Steganalysis test is required.
HS [77]	It applies Multi-layer HM based RDH technique. A new difference generation algorithm, viz., PVG is used to generate sharper difference histogram.	Embedding capacity is low.	0.6 bpp	35 bpp	Statistical test is required for confirming the resistance power.
HS[82]	It has used signed-digit representation for enhancing the visual quality. Block-wise prediction is made to generate a sharp prediction error histogram	Embedding capacity is low.	0.312 bpp	34.96 dB	Security against Steganalysis test is needed.

Table 5 (*continued*)

Method & Reference	Advantage	Limitation	Embedding capacity	Visual Quality (PSNR)	Resistance against statistical attacks/ steganalysis
Hybrid [49]	Enhanced the embedding capacity by combining the irreversible and reversible methods. Merging of 4 method also enhances the security of the scheme	It should be evaluated by non-structural analysis like, ML.	3.1 bpp	37.1 dB	It is robust against RS steganalysis.
DCN [98]	It chooses coefficients from frequencies that decreases the whole distortion. An advanced block selection approach is utilized that yields less simulated distortion.	Payload is not clearly mentioned. Robustness against statistical attack is absent.	-	$>$ 52 dB	Robustness test absent.
DFT [100]	Implement separable message embedding in encrypted images using Computer Sensing and DFT.	Complexity is high.	2 bpp	40 dB	Steganalysis test is required. Bit error rate $<$ 0.1
DWT [109]	HVS is the core of this model. DWT coefficients are utilized as the carrier.	Perceptual characteristic is degraded.	1500 bits	$>$ 59 dB	Steganalysis test is required.
IWT [119]	Cover image is encrypted. Location maps are lossless compressed for reducing the secondary data. Ratio correction is used in the pre-processing stage. Multi-phase IWT and multi-stage data hiding is used.	Image quality is not discussed properly. PSNR value is mentioned as nearly $+\infty$, which is doubtful.	0.77 bpp	$+\infty$	Steganalysis test is required.
IWT [120]	Multidirectional line encoding (MDLE) enhances the usage of coefficients.	Low embedding capacity	1.83 bpp	42.73 dB	Secure against image processing attacks. Secure against RS analysis PDH attack
IWT [121]	Uses particle swarm optimization, optimal pixel adjustment technique.	High computational time	2.25 bpp	41.41 dB	Secure against RS analysis, χ^2 test. and KL divergence. test
Adaptive [80]	Problem of HS-based numerous data hiding is framed as rate and distortion optimization problem. GA is applied to resolve the optimization problem.	Resilient against statistical attacks need to be addressed	0.76 bpp	$>$42 dB	Staganalysis test is missing.
Adaptive [132]	It has 5 layers safeguard. It uses ML for fine tuning the pixels value.	Processing time is high.	up to 12 bpp (color)	55 dB	Strong against several statistical attacks.
Adaptive [133]	Genetic algorithm is used here to search the optimal frequency transformation. Non-linear data hiding technique enhances the overall security of the system.	Weak against geometric or compression attacks.	2 bpp	55 dB	Steganalysis test is absent.
Deep [139]	Steganography without embedding (SWE) technique	Huge volume of dataset and high	$\geqslant$37.5 bytes/ image	-	Capable of obstructing steganalysis attack

(*continued on next page*)

Table 5 (*continued*)

Method & Reference	Advantage	Limitation	Embedding capacity	Visual Quality (PSNR)	Resistance against statistical attacks/ steganalysis
	on deep CNN. Message resides in the image can be retrieved by another NN	computational power is required.			
Deep [142]	Hides and retrieves stealthy data in the Y channel of the cover image. Imperceptibility is strengthened.	Huge volume of dataset is required. Limited by computing power.	8 bpp (color)	34.1 dB	Steganalysis test is absent.
Deep [136]	Database is not required for cover images. Confidential message is not required for sharing	Huge volume of dataset is required. Computational complexity is high.	120 bits/ carrier	-	secure against image processing attacks. Steganalysis test is required.

The following are the recommendations based on the analysis of the recent state-of-the-art works:

- Steganalysis tool can easily detect the LSB based steganography [30], but the method is very flexible to incorporate with other methods. Hence, this method can be mixed with other approaches. After LSB based embedding, 2^n correction method should be added to reduce the distortion and to increase the image quality.
- Reversibility is crucial in certain areas such as military and medical image processing. The system can use any of the methods like, DE, EMD, HS, etc.
- Embedding capacity of the steganographic technique can be enhanced by mixing several techniques. Fusion of the techniques puzzles the steganalysis attacks.
- Steganographic techniques that are implemented in spatial domain accomplish higher embedding capacity than that of transform domain. However, transform domain based steganographic techniques are more protected against statistical attacks. Hence, effort in the transform domain is highly encouraged if the application demands high security.
- In case of transform domain-based steganography, the wavelet domain is more promising than the other domains. Because, DFT based techniques does not provide the information about timing; it only gives frequency information. DCT based methods suffer from artifact problems. It also suffers from rounding-errors. Embedding capacity of the technique is also low.
- In the case of wavelet domain, the IWT domain outperforms DWT based steganography. Because, the DWT [108] produces floating-points as wavelet coefficients which are utilized to hide the secret information. It fails to recover the accurate information if any truncation error occurs during image construction. IWT overcome this problem by using the lifting scheme to achieve the exact removal of the embedded information.
- Embedding in the edge region provides an outstanding distortion free result whether it is used in the spatial, or frequency domains. However, the disadvantage is the low embedding capacity.
- Adaptive nature can be incorporated by some optimization techniques in the steganography to achieve high imperceptibility.
- Steganography without embedding (SWE) technique can be applied using deep CNN that resolves the problem of detection of the hidden data. No embedding process is necessary at the time of image generation, and the message residing in the image can be retrieved by another NN, after training. The approach can extract accurate data and has the ability to obstruct the detection by steganalysis tools.
- Most of the deep learning based steganographic techniques implement the encoder-decoder model which are based on CNNs. Other methods combine an adversarial component applying a GAN based framework. Several variations are available based on the GAN model which provide better security, high quality and high capacity steganography. Hence, working on the GAN framework is highly encouraging.

10. Some Popular Steganography Tools

A steganography software tool permits a user to embed secret message in a carrier media.

10.1. ***JSteg***

The JSteg algorithm [87] is one of the leading algorithms to use JPEG images, developed by Derek Upham. Fig. 19 shows the embedding process of the algorithm within the DCT coefficient. In the cover image, all disjoint blocks of 8×8 pixels are converted using the DCT. Subsequently, the DCT coefficients are scaled according to the default JPEG quantization table. This

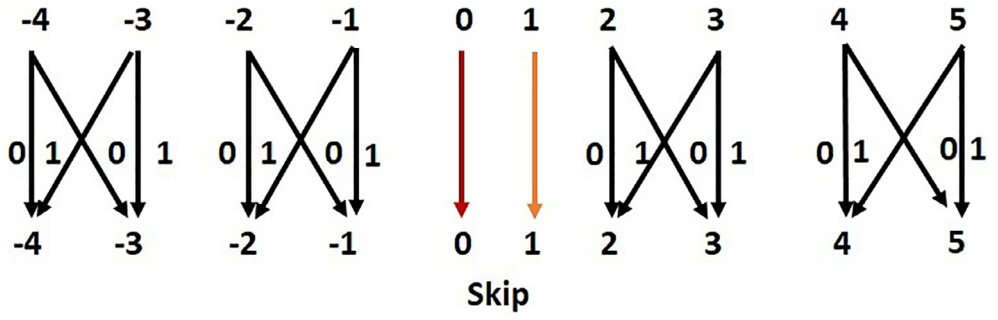

Fig. 19. Embedding process using JSteg algorithm.

method replaces the LSB of the quantized DCT coefficients in a sequence with message bits and skips the coefficients whose magnitudes are 1 or 0. JSteg embeds the stealthy bits in the whole cover image in a zigzag fashion. The embedding capacity of this technique is very low since DCT coefficients have a large number of zero-values. JSteg is resilient against visual attacks, but the presence of embedded data in the stego images using the JSteg algorithm can be easily identified by the χ^2 attack [150]. Algorithm 1 and Algorithm 2 provide the pseudocode for the encoding and decoding process of the JSteg algorithm.

Algorithm 1: The encoding process of the JSteg algorithm.

Input: A cover image component $\mathcal{C}$, a message $M_1, ..., M_m$ of known length m.
Output: The stego image component $\mathcal{S}$.

Split the image component into 8×8 non-overlapping blocks and convert the spatial domain intensities of each block into corresponding DCT values using Equation (14) ;
for *i from 1 to m* **do**
  $p \leftarrow$ next DCT coefficient;
  if $p =$ *DC component* **then**
    Goto step 3 ;
  end
  else
    if $p \neq 0$ *or* $p \neq 1$ **then**
      Replace LSB(p) with $\mathcal{M}_i$;
    end
  end
end
convert each 8×8 block back to spatial domain;
Output the transformed image component;

Algorithm 2: The decoding process of the JSteg algorithm.

Input: A stego image component $\mathcal{S}$.
Output: The embedded message of length m.

Split the image component into 8×8 non-overlapping blocks and convert the spatial domain intensities of each block into corresponding DCT values using Equation (14) ;
for *i from 1 to m* **do**
  $p \leftarrow$ next DCT coefficient;
  if $p =$ *DC component* **then**
    Goto Step 3 ;
  end
  else
    if $p \neq 0$ *or* $p \neq 1$ **then**
      $M_i' \leftarrow c_i \mod 2$,;
    end
  end
end
Output the embedded message;

10.2. ***OutGuess 0.1***.

The first version of OutGuess (i.e., OutGuess 0.1), developed by Provos [88], is an enhanced version of the JSteg algorithm. It scatters the embedding locations over the whole image with the help of a PRNG. The embedding process of the OutGuess 0.1 algorithm is basically a mixture of both randomized Hide & Seek algorithm [151] and JSteg algorithm. The coefficients are shuffled into a seemingly random order using a PRNG. The secret bits are then embedded using the same method as for JSteg before finally inverting the shuffle such that the coefficients are back in the exact positions. The image is then transformed back to the spatial domain. The algorithm avoids hiding within the DC coefficient, and any AC coefficient equal to either 1 or 0. Algorithm 3 and Algorithm 4 provide the encoding and decoding process of the OutGuess 0.1 algorithm.

Algorithm 3: The encoding process of the OutGuess 0.1 algorithm.

Input: A cover image component $\mathcal{C}$, a message $M_1, ..., M_m$ of known length m and seed k.
Output: The stego image component $\mathcal{S}$ containing the embedded message.

Split the image component into 8×8 non-overlapping blocks and convert the spatial domain intensities of each block into corresponding DCT values using Equation (14) ;
Generate randomized DCT sequence $Z_1, Z_2, ..., Z_m$ from cover image with seed k;
for *i from 1 to m* **do**
    $p \leftarrow$ next DCT coefficient;
    if $p =$ *DC component* **then**
        Goto step 4 ;
    end
    else
        if $p \neq 0$ *or* $p \neq 1$ **then**
            $q \leftarrow LSB(R_{Z_i})$;
            if $q \neq \mathcal{M}_i$ **then**
                Replace $LSB(p_{Z_i})$ with $\mathcal{M}_i$;
            end
        end
    end
end
convert each 8×8 block back to spatial domain ;
Output the stego-image component;

Algorithm 4: The decoding process of the OutGuess 0.1 algorithm.

Input: A stego image component $\mathcal{S}$ and seed k.
Output: The embedded message of length m.

Split the image component into 8×8 non-overlapping blocks and convert the spatial domain intensities of each block into corresponding DCT values using Equation (14);
Generate randomized DCT sequence $Z_1, Z_2, ..., Z_m$ using cover with seed k;
for *i from 1 to m* **do**
    $p \leftarrow$ next DCT coefficient;
    if $p =$ *DC component* **then**
        Goto step 4;
    end
    else
        if $p \neq 0$ *or* $p \neq 1$ **then**
            $M'_i \leftarrow LSB(p_{Z_i})$;
        end
    end
end
Output the embedded message;

10.3. ***OutGuess 0.2***.

The embedding algorithm of OutGuess 0.2 [88] is the same as that of OutGuess 0.1. The only difference is introduced after the information has been embedded. The technique retains the first-order statistics of DCT coefficients in stego images to resist the χ^2 attack [150]. Furthermore, it cautiously uses the LSB method to avoid causing statistical attacks. Outguess

and JSteg are nearly alike methods. The embedding is spread randomly throughout the image by using a PRNG. To choose the subsequent coefficient, OutGuess calculates a random offset and adds the offset to the current coefficient location. The random offsets are calculated by a PRNG. This embedding will cause the image statistics (i.e., the distribution of the coefficients) to diverge, hence some coefficients are kept to correct the statistical deviation. The modification is carried out to make the distributions of cover and stego images alike in terms of frequencies of the values.The impact of these modifications becomes much more apparent when statistical steganalysis is applied to it.

10.4. ***F3***

Fig. 20 shows the embedding process of the algorithm within the DCT coefficient. A. Westfeld et al. have developed the F3 algorithm [89], which provides better security than the OutGuess 0.2 algorithm. The reason for this is that it did not instantiate the same embedding procedure as the JSteg and OutGuess algorithms did. Instead of avoiding embedding in DCT coefficients equal to 1, the F3 algorithm permits embedding in these areas, though it does not embed in the zeros and the DC coefficients. The algorithm still embeds the secret message sequentially within the cover image. One more modification with this algorithm is that it does not embed directly in the LSB of the DCT coefficients. It takes the absolute value of the coefficients first, before comparing them with the secret message. If the absolute value of the coefficient and the secret bits areidentical, no changes are made. If they are dissimilar, the absolute value of the DCT coefficient is reduced by one. Algorithm 5 and Algorithm 6 provide the encoding and decoding process of the F3 algorithm.

Algorithm 5: The encoding process of the **F3** algorithm.

Input: A cover image component $\mathcal{C}$, a message M of length m.
Output: The stego image component $\mathcal{S}$ containing the embedded message.

1 Split the image component into 8×8 non-overlapping blocks and convert the spatial domain intensities of each block into corresponding DCT values using Equation (14) ;
2 **for** *i from 1 to m* **do**
3 $p \leftarrow$ next DCT coefficient;
4 **if** $p = DC\ component$ **then**
5 Goto step 3 ;
end
6 **else**
7 **if** $p \neq 1$ **then**
8 **if** $absolute(p) \neq \mathcal{M}_i$ **then**
9 Replace $absolute(p)$ with $absolute(p) - 1$;
end
end
end
end
10 convert each 8×8 block back to spatial domain ;
11 Output the stego-image component;

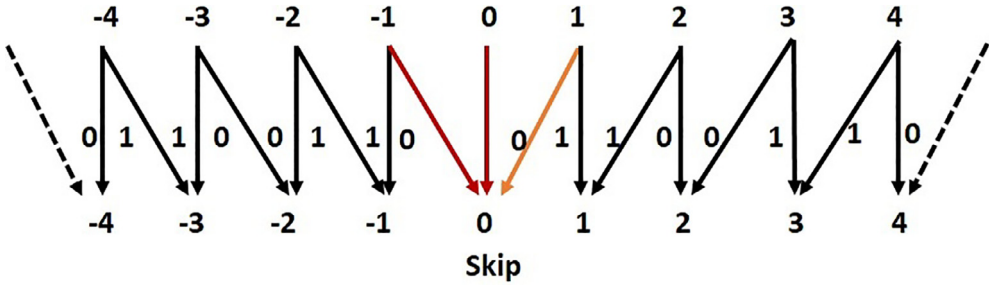

Fig. 20. Embedding process using F3 algorithm.

Algorithm 6: The decoding process of the **F3** algorithm.

Input: A stego image component $\mathcal{S}$.
Output: The embedded message of length m.

Split the image component into 8×8 non-overlapping blocks and convert the spatial domain intensities of each block into corresponding DCT values using Equation (14) ;
for *i from 1 to m* **do**
  $p \leftarrow$ next DCT coefficient;
  if $p =$ *DC component or* $p = 0$ **then**
    Goto step 3;
  end
  else
    if $p \neq 1$ **then**
      $M_i' \leftarrow absolute(p)$;
    end
  end
end
Output the embedded message;

10.5. *F4*

The foremost problem with the F3 algorithm is that it efficiently embeds more zeros than ones as a consequence of the shrinkage mechanism. This means that when the statistical properties of the stegogram are inspected through its histogram, some artifacts of embedding become discernible. This is similar to the JSteg implementation except a little dissimilar pattern is obtained. Fig. 21 shows the embedding procedure within the DCT coefficient of the cover image. Adding with this, steganalysis also finds that more odd coefficients existed in F3 stegograms than even coefficients. This leads to two lacks that can be observed while viewing the histogram of a doubtful image. The F4 algorithm [89] is presented to eliminate these properties such that the histogram would look similar to that of a fresh image. Algorithm 7 and Algorithm 8 provide the encoding and decoding process of the F4 algorithm.

Algorithm 7: The encoding process of the **F4** algorithm.

Input: A cover image component $\mathcal{C}$, a message $M_1, \ldots, M_m$ of known length m.
Output: The stego image component $\mathcal{S}$ containing the embedded message.

Split the image component into 8×8 non-overlapping blocks and convert the spatial domain intensities of each block into corresponding DCT values using Equation (14) ;
for *i from 1 to m* **do**
  $p \leftarrow$ next DCT coefficient;
  if $p =$ *DC component* **then**
    Goto step 3;
  end
  else
    if $p \neq 1$ **then**
      if $absolute(p) = \mathcal{M}_i$ *and* $absolute(p) > 0$ **then**
        Replace $absolute(p)$ with $absolute(p) + 1$;
      end
      else if $absolute(p) \neq \mathcal{M}_i$ *and* $absolute(p) < 0$ **then**
        Replace $absolute(p)$ with $absolute(p) - 1$;
      end
      else
        Goto Step 3;
      end
    end
  end
end
convert each 8×8 block back to spatial domain;
Output the stego-image component;

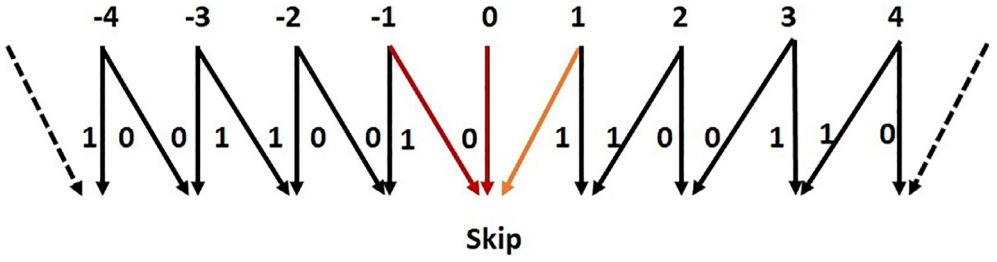

Fig. 21. Embedding process using F4 algorithm.

Algorithm 8: The decoding process of the **F4** algorithm.

Input: A stego image component $\mathcal{S}$.
Output: The embedded message of length m.

1 Split the image component into 8×8 non-overlapping blocks and convert the spatial domain intensities of each block into corresponding DCT values using Equation (14) ;
2 **for** i *from 1 to* m **do**
3 $p \leftarrow$ next DCT coefficient;
4 **if** $p =$ *DC component or* $p = 0$ **then**
5 Goto step 3;
end
6 **else**
7 **if** $absolute(p) > 0$ **then**
8 $M_i' \leftarrow absolute(p) - 1$;
end
9 **else**
10 $M_i' \leftarrow absolute(p) + 1$;
end
end
end
11 Output the embedded message;

10.6. ***F5***

F5 algorithm was presented by Westfeld in 2001 to enhance the embedding capacity of JPEG images deprived of forfeiting security. Furthermore, the objective of establishing the F5 algorithm was to retain the histogram shape of DCT coefficients. The F5 algorithm skips the AC and DC coefficients whose magnitudes are zeros, so it does not use them for embedding. The embedding procedure of the F5 algorithm [89] is principally identical to the F4 algorithm. The F5 algorithm encompasses two important strategies. One strategy is that the absolute value of the DCT coefficient is always reduced by one. F5 simply embeds into non-zero AC DCT coefficients. If a coefficient turns into zero after embedding, which can only occur for coefficients equal to 1 or -1, i.e., shrinkage happens and the identical bit is re-embedded at the next coefficient. To lessen the effect of embedding on the DCT histogram, F5 hops over 50% of all DCT coefficients equal to 1 or -1. The second vital constituent of F5 is the introduction of matrix embedding using binary Hamming codes. Matrix embedding allows embedding additional bits per one embedding change and thus improves embedding efficiency. Algorithm 9 offers the encoding process of the F5 algorithm.

Algorithm 9: The encoding process of the **F5** algorithm.

Input: A cover image component $\mathcal{C}$, a message $M_1, \ldots, M_m$ of known length m.
Output: The stego image component $\mathcal{S}$ containing the embedded message.

1 Split the image component into 8×8 non-overlapping blocks and convert the spatial domain intensities of each block into corresponding DCT values using Equation (14) ;
2 Determine the parameter n from the message length (i.e. m) and the capacity of the carrier medium (say, f') where, $f' = \frac{63}{64} f_{DCT} - f(0) - \frac{51}{100} f(1)$. Here f_{DCT} is the number of all DCT coefficients, $f(0)$ is the number of AC DCT coefficients equal to zero, $f(1)$ is the number of AC DCT coefficients with absolute value 1;
3 Generate randomised sequence $Z_1, Z_2, ..., Z_m$ using cover data according to seed k;
4 Perform XOR operation between Z_i and $\mathcal{M}_i$ to obtain $\mathcal{M}_i^{new}$ where $0 \leq i \leq m$;
5 $\mathcal{M}^{new} = ||_i^m \mathcal{M}_i^{new}$;
6 The message $\mathcal{M}^{new}$ is divided into segments of n bits for embedding into a group G of $2^n - 1$ AC DCT coefficients along the random walk.
7 **for** *i from 1 to m* **do**
8 $p \leftarrow$ next G;
9 Set $flag$=1;
10 **else**
11 **if** *flag=1* **then**
12 $q \leftarrow h(G)$, where $h(.)$ denotes the hash function;
13 **for** *j from 1 to n* **do**
14 **if** $q_j \neq \mathcal{M}_{n\cdot(i-1)+j}^{new}$ *and* $absolute(p_j) \neq 0$ **then**
15 Replace $absolute(p_{Z_i})$ with $absolute(p_{Z_i}) - 1$;
16 **if** $absolute(p_{Z_i}) = 0$ **then**
17 $flag$=0;
end
end
end
18 **if** *flag=0* **then**
19 $p \leftarrow$ next G;
20 Set $flag$=1;
21 Goto Step 11;
end
end
end
end
22 convert each 8×8 block back to spatial domain;
23 Output the stego-image component;

10.7. ***nsF5***

nsF5 [90] is non-shrinkage F5, a modification of Westfeld's F5 Algorithm [89] with enhanced coding. It changes DCT coefficients only in the direction of zero. The F5 without shrinkage (nsF5) performs steadily and considerably superior to the original F5. It is the best-verified algorithm that embeds directly into the DCT coefficients deprived of depending on any side information at the sender.

10.8. ***Highly Undetectable steGO (HUGO)***.

It is the first modern spatial domain content-adaptive steganographic algorithm [127] that applies STC. It was planned to minimize the embedding distortion in a high dimensional feature space calculated from differences of four adjacent pixels. The steps of this algorithm are shown in Fig. 22. The security of HUGO was confirmed and compared to previous state-of-the-art (LSB matching) on a high embedding capacity for four different feature sets. In the difference with LSB matching, HUGO permits embedding 7 $\times$ longer messages with the same security level.

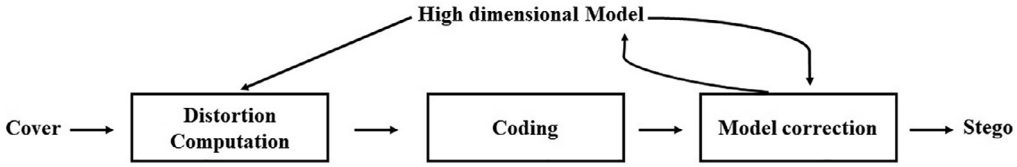

Fig. 22. High level diagram of HUGO [127].

10.9. *Uniform Embedding Distortion (UED)*

UED [91] is a competent JPEG steganographic technique based on STC and a uniform embedding approach. It modifies nonzero quantized DCT coefficients of diverse magnitude with the identical probability that gives probable least artifacts for statistics of DCT coefficients as a whole.

10.10. *Wavelet Obtained Weights (WOW)*

WOW [128] is a model-free spatial domain content adaptive steganographic method that uses a bank of directional high-pass filters to achieve the directional residuals. By computing the effect of embedding on each directional residual and by appropriately accumulating these impacts, it makes the distortion become high in case of smooth areas and low in case of texture areas. Consequently, the algorithm becomes extremely adaptive and has been shown enhanced resistance compared to HUGO [127] when the Spatial Rich Model (SRM) is used for detection.

10.11. *UNIversal WAvelet Relative Distortion (UNIWARD)*

UNIWARD [129] is another spatial domain content adaptive steganographic technique that uses a universal distortion function. UNIWARD can be used for embedding in an arbitrary domain. The embedding distortion is calculated as a totality of relative variations of coefficients in a directional filter bank decomposition of the cover image. Because of directionality, the embedding alterations have occurred in the areas of the cover image that are hard to model in multiple directions like textures or noisy areas, while side-stepping smooth areas. From experimental results the spatial JPEG, and side-informed JPEG versions of UNIWARD have shown the maximum level of security when verified empirically with rich models.

11. Comparison Among SteganographyTools

A comparison has been made on the steganography tools in Table 6. In case of nsF5, HUGO, WOW, UED, S-UNIWARD, and J-UNIWARD, there are no implementations of the algorithms for public use. Thus, none of them has any encryption. In fact, researchers mostly work with embedding simulators and not real embedding algorithms. The actual embedding, which

Table 6
Comparison among steganographic tools.

Tools	Format	Domain	Encryption Support	Random Bit Selection	Weak against
JSteg [87]	JPEG	DCT	No	No	χ^2 test [150] StegDetect Fridrich et al. [152]
OutGuess 0.1 [88]	JPEG	DCT	RC4	Yes	χ^2 test [150] StegDetect
OutGuess 0.2 [88]	JPEG	DCT	RC4	Yes	Fridrich et al. [152]
S-Tools [9]	BMP, GIF	Spatial	IDEA, DES, 3DES, MPJ2, NSEA	No	χ^2 test [150]
EZStego	BMP, GIF	Spatial	IDEA, DES, 3DES, MPJ2, NSEA	No	χ^2 test [150] RS steganalysis [19]
F5 [89]	JPEG	DCT	RC4	Yes	Fridrich et al. [152]
nsF5 [90]	JPEG	DCT	Not provided	Yes	JRM [153]
UED [91]	JPEG	DCT	Not provided	No	Chen et al. [154]
HUGO [127]	Any raster format	Spatial	Not provided	Yes	SRM [155]
WOW [128]	Any rater format	Spatial	Not provided	Yes	SCA-TLU-CNN [156] Yedroudj-Net [157]
S-UNIWARD [129]	Any raster format	Spatial	Not provided	Yes	Xu's CNN [158] SCA-TLU-CNN [156] PSRM [159]
J-UNIWARD [129]	JPEG	Spatial	Not provided	Yes	PSRM [159] Chen et al. [154]

would include possible encryption, would have been done on top of these. Then, it is up to the researcher what encryption they want to use.

12. Steganalysis

Steganalysis technique tries to find the stealthy message concealed using steganography [160,161]. The purpose of steganography will be failedif the steganalysis system identifies the existence of concealed data in the cover media. The significance of steganalysis is increasing day-by-day. It is used in cyber warfare, tracking criminal activities over the internet, and in computer forensics [162]. It is also used to improve the safety of steganographic techniques by finding and estimating their weaknesses. According to the basics of detection procedure, steganalysis is divided into signature steganalysis and statistical steganalysis [8]. Signature steganalysis searches for specific patterns of any steganographic scheme. Statistical steganalysis exploits statistical parameters to identify any secret information within the analyzed image. It extracts the statistical features from clean and stego images. After comparing the statistical features, clean images are separated from stego images. Some of the steganalysis techniques that are intended for specific steganographic techniques like, LSB matching, LSB embedding, BPCS steganography, JPEG-compression, etc.Other types of statistical steganalysis are RS analysis [19], χ^2 test [163], and histogram analysis, etc. All these methods can easily depict the presence of a hidden messageand even calculate secret message size.

Machine learning techniques have been employed in the modern steganalysis approach. Here, features are extracted from both clean and stego images. A classifier is trained, and finally unknown images are placed on the evaluation model. SVM [164] and ANN [165] have been used mostly as classifiers. CNN [166] based techniques can be proficiently exploited as the steganalysis tools to investigate the concealed data within the image [167]. They can capture the convoluted dependencies among the pixels to analyze and recognize the existence of stealthy data. Therefore, these ML-based steganalysis methods bear a big challenge to the orthodox techniques. The orthodox techniques are handcrafted, but they are heuristic where a certain level of knowledge is essential to recognize where and how precisely to hide the stealthy data. Contrarily, deep learning based CNNs can achieve this with very less effort. We have to design the architecture of the model. For example, the artificial neural network can efficiently detect the ideal embedding position in an image. The trained AI models do the embedding and extraction automatically once they are trained with the provided essential features. Nowadays, deep learning via CNN [168,169] is widely used as a steganalysis tool.

In deep learning, feature representations can be learned automatically. Ye et al. [156] have developed a deep CNN (as shown in Fig. 23) with a truncated linear unit (TLU) for boosting the detection process. The efficiency of the CNN model has been further enhanced by introducing the selection channel. The authors of the paper [170] have applied quantization and truncation into deep learning for the first time. It has shown its dominance over hand-crafted JPEG steganalytic features. Wu et al. [171] have presented a relatively higher deep CNN (DRN) than existing CNNs at that time. Accuracy of the model is fairly higher than the other models. Zhang et al. [172] have proposed a CNN model in larger JPEG images. Experimental results exhibited the improved revealing correctness and quicker convergence rate for large images. A custom-made CNN framework has been designed in the paper [161] for steganalysis. Strength of the model is the 4 HPF for residual noise removal. Detection error of the model is 15.2% which is a good result. Encouraged by the fractal network, a novel steganalysis technique, SFNet, has been presented in the work [173]. It is an end-to-end network that does not include any pre-processing filters to reveal stego noise. The experimental results show the superiority of the work with other existing steganalysis techniques. The efficiency of the model can be tested for JPEG-domain steganalysis.

13. Challenges in Deep Learning based Steganography

Recent progress in deep learning has made noteworthy improvement in steganography and steganalysis. Several deep learning based steganography and steganalysis techniques have gained extensive attention to the researchers. Although, this technology is still facing some problems and challenges. Further study is required to develop more strong and correct deep learning based techniques that can light on real world applications.

Data availability: Deep learning based steganographic techniques require a huge number of images to obtain expected accuracy. There are very few proper benchmark datasets available except BOSSBase 1.01 [174]. The total number of images in BOSSBase is 10000, but the images in BOSSBase 1.01 are of grayscale in tiff format. Collecting the huge number of images for generating the dataset can be a challenging task.

Training and execution efficiency: The deep learning models work well on a larger dataset. Hence, deep learning based steganographic techniques are computationally expensive to train and execute the dataset. It needs the resources like GPU, bulky size RAM etc. which are very expensive.

Real-time steganography: Deep learning based steganographic models are trained on a massive quantity of datasets. In the case of real-time steganography, it faces difficulty. The stego images are transmitted from the sender to the receiver through an untrusted channel. The real time live images may comprise blurring, skewing, and noises. The competency of the trained model in dealing with the real time live images is still questionable.

Problem of GAN: Sometimes GAN [175] based frameworks suffer from convergence problems. The model does not converge regardless of the parameters selected. During training the network, a vanishing gradient problem happens. The dis-

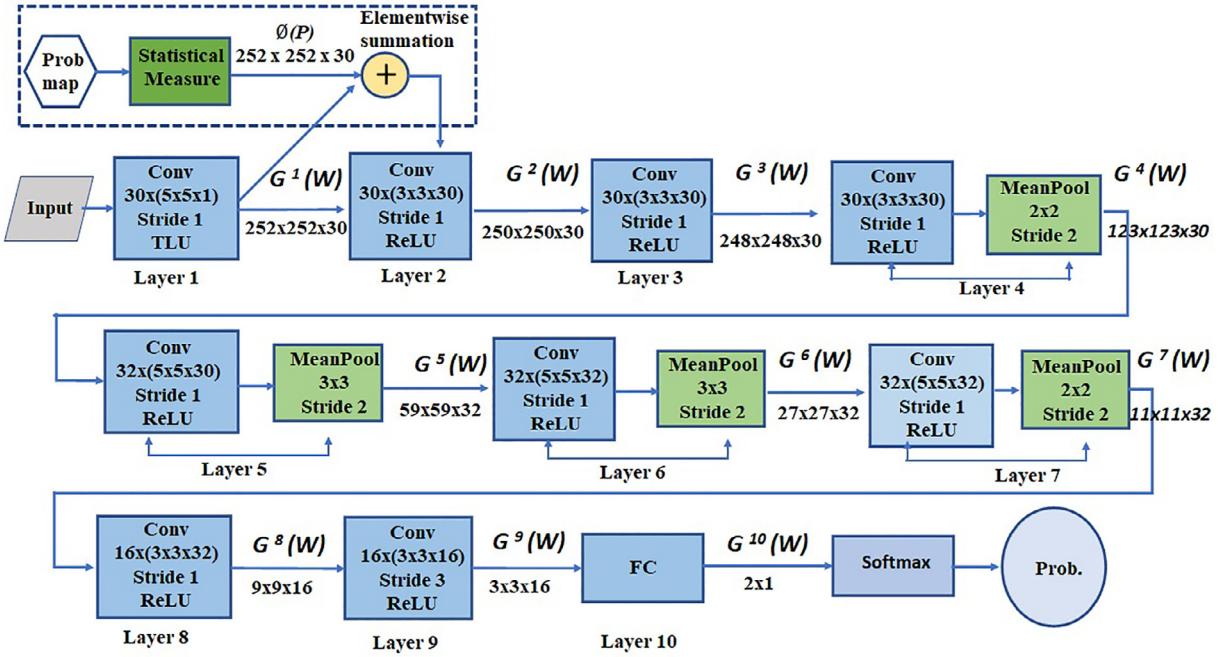

Fig. 23. The structure of the 10-layer CNN model [156].

criminator network performs very well but the generator network experiences gradient vanishing problems and it learns nothing. So, overfitting problems occur. Mode collapse also occurs frequently as the generator and discriminator are interdependent.

14. Future Research Directions

The following are the aspects that can be considered for future research directions:

- Adaptive steganographic techniques can be applied for reducing distortion and increasing the security. High imperceptibility also can be achieved by incorporating some optimization techniques.
- Hybrid techniques using both the spatial and transform domain approaches, may be used for incorporating the benefits of these two types of approaches.
- Transform domain based techniques provide higher security than that of spatial domain. However, to increase the embedding capacity in the transform domain is a much more difficult and challenging task. High capacity steganographic technique with minimized distortion in the transform domain is highly encouraged.
- The steganography techniques can be implemented using video as a cover media to hide huge amount of secret data.
- Since sequential embedding is weak against statistical attacks. The non-sequential embedding technique can be improved by different seed generation algorithms using the PRNG. It is even better to implement the non-sequential embedding based on the image feature.
- Quantum steganography is an emerging research direction where reversible and non-reversible steganography techniques can be implemented.
- From the state-of-the-art deep learning methods discussed so far, it appears that the GAN based framework is the most hopeful. Further variations of the GAN based framework, like Wasserstein GANs (WGANs), CycleGANs, etc., can be proposed for steganography.
- In addition, applications of GAN based steganography technique in the JPEG domain are also a research route yet to explore.

15. Conclusions

In this paper, the taxonomy, the basic idea, and the performance assessment criteria have been discussed for image steganography. An attempt has been made to provide an extensive review of steganographic techniques in different domains. The performance of recent state-of-the-art works has been described. Similarities and dissimilarities among spatial domain, transform domain, and adaptive steganography have been discussed. A good steganographic method should, not

only be capable of high payload but also should be able to yield stego images that are invisible to the human eye. Also, a good steganographic method should have the capability to repel several steganalysis attacks. Hiding capacity in spatial domain based techniques are better than the transform domain-based techniques, but they are less secure than transform domain techniques. In adaptive steganography, to build a statistical analysis in the edges and irregular texture areas is tough. The steganalysis system fails to make a true decision. Hence, choosing places adaptively for hiding is still an encouraging solution in steganography. Recently, deep learning based steganography has appeared as a promising research topic. It can be used for enhancing the security and visual quality of steganographic techniques.

CRediT authorship contribution statement

Pratap Chandra Mandal: Conceptualization, Methodology, Formal analysis, Investigation, Resources, Data curation, Writing - original draft, Visualization. **Imon Mukherjee:** Methodology, Formal analysis, Validation, Writing - review & editing, Supervision, Project administration. **Goutam Paul:** Validation, Writing - review & editing, Supervision. **B.N. Chatterji:** Validation, Writing - review & editing, Supervision.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] F. Dachselt, W. Schwarz, Chaos and Cryptography, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48 (12) (2001) 1498–1509, https://doi.org/10.1109/TCSI.2001.972857.
[2] A. Cheddad, J. Condell, K. Curran, P.M. Kevitt, Digital Image Steganography: Survey and Analysis of Current Methods, Signal Processing 90 (3) (2010) 727–752, https://doi.org/10.1016/j.sigpro.2009.08.010.
[3] M.S. Subhedar, V.H. Mankar, Current Status and Key Issues in Image Steganography: A Survey, Computer Science Review 13 (2014) 95–113, https://doi.org/10.1016/j.cosrev.2014.09.001.
[4] L. Luo, Z. Chen, M. Chen, X. Zeng, Z. Xiong, Reversible Image Watermarking using Interpolation Technique, IEEE Transactions on Information Forensics and Security 5 (1) (2009) 187–193, https:// doi.org/10.1109/TIFS.2009.2035975.
[5] V. Sedighi, R. Cogranne, J. Fridrich, Content-adaptive Steganography by Minimizing Statistical Detectability, IEEE Transactions on Information Forensics and Security 11 (2) (2015) 221–234, https://doi.org/10.1109/TIFS.2015.2486744.
[6] Y.P. Lee, J.C. Lee, W.K. Chen, K.C. Chang, J. Su, C.P. Chang, High Payload Image Hiding with Quality Recovery using Tri-way Pixel Value Differencing, Information Sciences 191 (2012) 214–225, https://doi.org/10.1016/j.ins.2012.01.002.
[7] C. Qin, X. Qian, W. Hong, X. Zhang, An Efficient Coding Scheme for Reversible Data Hiding in Encrypted Image with Redundancy Transfer, Information Sciences 487 (2019) 176–192, https://doi.org/10.1016/j.ins.2019.03.008.
[8] A. Nissar, A.H. Mir, Classification of Steganalysis Techniques: A Study, Digital Signal Processing 20 (6) (2010) 1758–1770, https://doi.org/10.1016/j.dsp.2010.02.003.
[9] N.F. Johnson, S. Jajodia, Exploring Steganography: Seeing the Unseen, Computer 31 (2) (1998) 26–34, https://doi.org/ 10.1109/MC.1998.4655281.
[10] L. Stéganographie, Information Noyée, Information Cachée, Pour La, Science 229 (1996) 142–146.
[11] G.J. Simmons, The Prisoners' Problem and the Subliminal Channel, in: Advances in Cryptology, Springer, 1984, pp. 51–67.
[12] V.A. Luis, N.J. Hopper, Public-key Steganography, in: Eurocrypt, 2004, pp. 323–341, doi: 10.1007/978-3-540-24676-3-20.
[13] T.C. Lu, Interpolation based Hiding Scheme using the modulus Function and Re-encoding Strategy, Signal Processing 142 (2018) 244–259, https://doi.org/10.1016/j.sigpro.2017.07.025.
[14] D.R.I.M. Setiadi, PSNR vs SSIM: Imperceptibility Quality Assessment for Image Steganography, Multimedia Tools and Applications 80 (6) (2021) 8423–8444, https://doi.org/10.1007/s11042-020-10035-z.
[15] A.A. Mohammad, A.A. Haj, M. Farfoura, An Improved Capacity Data Hiding Technique based on Image Interpolation, Multimedia Tools and Applications 78 (6) (2019) 7181–7205, https://doi.org/10.1007/s11042-018-6465-8.
[16] A. Toet, M.A. Hogervorst, Performance Comparison of Different Gray Level Image Fusion Schemes Through a Universal Image Quality Index, in: Signal Processing, Sensor Fusion, and Target Recognition XII, Vol. 5096, International Society for Optics and Photonics, 2003, pp. 552–561, doi: 10.1117/12.484886.
[17] J. Luo, E.E. Konofagou, A. Fast, Normalized Cross Correlation Calculation Method for Motion Estimation, IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control 57 (6) (2010) 1347–1357, https://doi.org/10.1109/TUFFC.2010.1554.
[18] C. Kim, Data Hiding by an Improved Exploiting Modification Direction, Multimedia Tools and Applications 69 (3) (2014) 569–584, https://doi.org/10.1007/s11042-012-1114-0.
[19] J. Fridrich, M. Goljan, R. Du, Reliable Detection of LSB Steganography in Color and Grayscale Images, in: Proceedings of the 2001 Workshop on Multimedia and Security: New Challenges, 2001, pp. 27–30, doi: 10.1145/1232454.1232466.
[20] R. Agrawal, Finite Sample Concentration of the Multinomial in Relative Entropy, IEEE Transactions on Information Theory 66 (10) (2020) 6297–6302, https:// 10.1109/TIT.2020.2996134.
[21] P.C. Mandal, I. Mukherjee, High Capacity Data Hiding based on Multi-directional Pixel Value Differencing and Decreased Difference Expansion, Multimedia Tools and Applications (2021) 1–23, https://doi.org/10.1007/s11042-021-11605-5.
[22] F.A. Petitcolas, R.J. Anderson, M.G. Kuhn, Attacks on Copyright Marking Systems, in: International Workshop on Information Hiding, Springer, 1998, pp. 218–238, doi: 10.1007/3-540-49380-8-16.
[23] P. Wayner, Disappearing Cryptography - Information Hiding, in: Steganography & Watermarking (Second Edition), A volume in The Morgan Kaufmann Series in Software Engineering and Programming, Morgan Kaufmann, Elsevier, 2002, pp. 1–397.
[24] K. Raja, K. Kumar, S. Kumar, M. Lakshmi, H. Preeti, K. Venugopal, L.M. Patnaik, Genetic Algorithm based Steganography using Wavelets, in: International Conference on Information Systems Security, Springer, 2007, pp. 51–63, https://doi.org/10.1007/978-3-540-77086-2-5.
[25] F.A. Petitcolas, Watermarking Schemes Evaluation, IEEE Signal Processing Magazine 17 (5) (2000) 58–64, https://doi.org/10.1109/79.879339.
[26] D. Anand, U. Niranjan, Watermarking Medical Images with Patient Information, in: Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Vol. 2, IEEE, 1998, pp. 703–706, https://doi.org/ 10.1109/IEMBS.1998.745518.
[27] B. Carpentieri, A. Castiglione, A. De Santis, F. Palmieri, R. Pizzolante, One Pass Lossless Data Hiding and Compression of Remote Sensing Data, Future Generation Computer Systems 90 (2019) 222–239, https://doi.org/10.1016/j.future.2018.07.051.

[28] M. Wu, B. Liu, Data Hiding in Image and Video: Part I-Fundamental Issues and Solutions, IEEE Transactions on Image Processing 12 (6) (2003) 685–695.
[29] N. Mukherjee, G. Paul, S.K. Saha, An Efficient Multi-bit Steganography Algorithm in Spatial Domain with Two-layer Security, Multimedia Tools and Applications 77 (14) (2018) 18451–18481, https://doi.org/10.1007/s11042-018-5720-3.
[30] C.K. Chan, L.M. Cheng, Hiding Data in Images by Simple LSB Substitution, Pattern Recognition 37 (3) (2004) 469–474, https://doi.org/10.1016/j.patcog.2003.08.007.
[31] R. Chandramouli, N. Memon, Analysis of LSB based Image Steganography Techniques, in: Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205), Vol. 3, IEEE, 2001, pp. 1019–1022, https://doi.org/ 10.1109/ICIP.2001.958299.
[32] X. Zhou, W. Gong, W. Fu, L. Jin, An Improved Method for LSB based Color Image Steganography Combined with Cryptography, in: 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), IEEE, 2016, pp. 1–4, https://doi.org/10.1109/ICIS.2016.7550955.
[33] S. Atawneh, A. Almomani, P. Sumari, Steganography in Digital Images: Common Approaches and Tools, IETE Technical Review 30 (4) (2013) 344–358.
[34] G. Paul, I. Davidson, I. Mukherjee, S. Ravi, Keyless Steganography in Spatial Domain using Energetic Pixels, in: International Conference on Information Systems Security, Springer, 2012, pp. 134–148, https://doi.org/10.1007/978-3-642-35130-3_10.
[35] K.H. Jung, K.Y. Yoo, Steganographic Method based on Interpolation and LSB Substitution of Digital Images, Multimedia Tools and Applications 74 (6) (2015) 2143–2155, https://doi.org/10.1007/s11042-013-1832-y.
[36] W.L. Xu, C.C. Chang, T.S. Chen, L.M. Wang, An Improved Least Significant Bit Substitution Method using the Modulo Three Strategy, Displays 42 (2016) 36–42, https://doi.org/10.1016/j.displa.2016.03.002.
[37] G. Paul, I. Davidson, I. Mukherjee, S. Ravi, Keyless Dynamic Optimal Multi-bit Image Steganography using Eergetic Pixels, Multimedia Tools and Applications 76 (5) (2017) 7445–7471, https://doi.org/10.1007/s11042-016-3319-0.
[38] A. Jain, A Secured Steganography Technique for Hiding Multiple Images in an Image using Least Significant Bit Algorithm and Arnold Transformation, in: International Conference on Intelligent Data Communication Technologies and Internet of Things, Springer, 2019, pp. 373–380, https://doi.org/10.1007/978-3-030-34080-3-42.
[39] R. Biswas, I. Mukherjee, S.K. Bandyopadhyay, Image Feature based High Capacity Steganographic Algorithm, Multimedia Tools and Applications 78 (14) (2019) 20019–20036, https://doi.org/10.1007/s11042-019-7369-y.
[40] S. Das, K. Muhammad, S. Bakshi, I. Mukherjee, P.K. Sa, A.K. Sangaiah, A. Bruno, Lip Biometric Template Security Framework using Spatial Steganography, Pattern Recognition Letters 126 (2019) 102–110, https://doi.org/10.1016/j.patrec.2018.06.026.
[41] A.K. Sahu, G. Swain, Reversible Image Steganography using Dual-layer LSB Matching, Sensing and Imaging 21 (1) (2020) 1–21, https://doi.org/10.1007/s11220-019-0262-y.
[42] D.C. Wu, W.H. Tsai, A Steganographic Method for Images by Pixel Value Differencing, Pattern Recognition Letters 24 (9–10) (2003) 1613–1626, https://doi.org/10.1016/S0167-8655(02)00402-6.
[43] K.C. Chang, C.P. Chang, P.S. Huang, T.M. Tu, A Novel Image Steganographic Method using Tri-way Pixel Value Differencing, Journal of Multimedia 3 (2) (2008) 37–45.
[44] P.C. Mandal, I. Mukherjee, Index-Based Improved High Capacity Data Hiding Technique, in: Evolution in Computational Intelligence, Springer, 2022, pp. 491–500, doi: 10.1007/978-981-16-6616-2_48.
[45] C.M. Wang, N.I. Wu, C.S. Tsai, M.S. Hwang, A High Quality Steganographic Method with Pixel Value Differencing and Modulus Function, Journal of Systems and Software 81 (1) (2008) 150–158, https://doi.org/10.1016/j.jss.2007.01.049.
[46] K.H. Jung, High Capacity Steganographic Method based on Pixel Value Differencing and LSB Replacement Methods, The Imaging Science Journal 58 (4) (2010) 213–221, https://doi.org/10.1179/136821910X12651933390584.
[47] M. Khodaei, K. Faez, New Adaptive Steganographic Method using Least Significant Bit Substitution and Pixel Value Differencing, IET Image Processing 6 (6) (2012) 677–686, https://doi.org/ 10.1049/iet-ipr.2011.0059.
[48] M. Hussain, A.W.A. Wahab, A.T. Ho, N. Javed, K.H. Jung, A Data Hiding Scheme using Parity bit Pixel Value Differencing and Improved Rightmost Digit Replacement, Signal Processing: Image Communication 50 (2017) 44–57, https://doi.org/10.1016/j.image.2016.10.005.
[49] M. Hussain, A.W.A. Wahab, N. Javed, K.H. Jung, Recursive Information Hiding Scheme Through LSB, PVD Shift, and MPE, IETE Technical Review 35 (1) (2018) 53–63, https://doi.org/10.1080/02564602.2016.1244496.
[50] Z. Li, Y. He, Steganography with pixel-value differencing and modulus function based on pso, Journal of information security and applications 43 (2018) 47–52, https://doi.org/10.1016/j.jisa.2018.10.006.
[51] N. Mukherjee, G. Paul, S.K. Saha, D. Burman, A pvd based High Capacity Steganography Algorithm with Embedding in Non-sequential Position, Multimedia Tools and Applications 79 (19) (2020) 13449–13479, https://doi.org/10.1007/s11042-019-08178-9.
[52] M. Hussain, Q. Riaz, S. Saleem, A. Ghafoor, K.H. Jung, Enhanced Adaptive Data Hiding Method using LSB and Pixel Value Differencing, Multimedia Tools and Applications 80 (13) (2021) 20381–20401, https://doi.org/10.1007/s11042-021-10652-2.
[53] J. Tian, Reversible Data Embedding using a Difference Expansion, IEEE Transactions on Circuits and Systems for Video Technology 13 (8) (2003) 890–896, https://doi.org/10.1109/TCSVT.2003.815962.
[54] Y. Hu, H.K. Lee, K. Chen, J. Li, Difference Expansion based Reversible Data Hiding using Two Embedding Directions, IEEE Transactions on Multimedia 10 (8) (2008) 1500–1512, https:/10.1109/TMM.2008.2007341.
[55] C.F. Lee, H.L. Chen, H.K. Tso, Embedding Capacity Raising in Reversible Data Hiding based on Prediction of Difference Expansion, Journal of Systems and Software 83 (10) (2010) 1864–1872, https://doi.org/10.1016/j.jss.2010.05.078.
[56] F. Peng, X. Li, B. Yang, Adaptive Reversible Data Hiding Scheme based on Integer Transform, Signal Processing 92 (1) (2012) 54–62, https://doi.org/10.1016/j.sigpro.2011.06.006.
[57] S. Gujjunoori, M. Oruganti, Difference Expansion based Reversible Data Embedding and Edge Detection, Multimedia Tools and Applications (2019) 1–29, https://doi.org/10.1007/s11042-019-07767-y.
[58] W. Wang, A Reversible Data Hiding Algorithm based on Bidirectional Difference Expansion, Multimedia Tools and Applications 79 (9) (2020) 5965–5988, https://doi.org/10.1007/s11042-019-08255-z.
[59] X. Zhang, S. Wang, Efficient Steganographic Embedding by Exploiting Modification Direction, IEEE Communications Letters 10 (11) (2006) 781–783, https://doi.org/10.1109/LCOMM.2006.060863.
[60] C.C. Chang, W.L. Tai, K.N. Chen, Improvements of EMD Embedding for Large Payloads, in: Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007), Vol. 1, IEEE, 2007, pp. 473–476, https://doi.org/ 10.1109/IIHMSP.2007.4457590.
[61] C.F. Lee, C.C. Chang, K.H. Wang, An Improvement of EMD Embedding Method for Large Payloads by Pixel Segmentation Strategy, Image and Vision Computing 26 (12) (2008) 1670–1676, https://doi.org/10.1016/j.imavis.2008.05.005.
[62] Z.H. Wang, T. Kieu, C. Chang, M. Li, A Novel Information Concealing Method based on Exploiting Modification Direction, Journal of Information Hiding and Multimedia Signal Processing 1 (1) (2010) 1–9.
[63] W.C. Kuo, C.C. Wang, H.C. Hou, Signed Digit Data Hiding Scheme, Information Processing Letters 116 (2) (2016) 183–191, https://doi.org/10.1016/j.ipl.2015.08.003.
[64] S. Saha, A. Chakraborty, A. Chatterjee, S. Dhargupta, S.K. Ghosal, R. Sarkar, Extended Exploiting Modification Direction based Steganography using Hashed-weightage Array, Multimedia Tools and Applications (2020) 1–21, https://doi.org/10.1007/s11042-020-08951-1.
[65] K.H. Jung, K.Y. Yoo, Data Hiding Method using Image Interpolation, Computer Standards & Interfaces 31 (2) (2009) 465–470, https://doi.org/10.1016/j.csi.2008.06.001.
[66] C.F. Lee, Y.L. Huang, An Efficient Image Interpolation Increasing Payload in Reversible Data Hiding, Expert Systems with Applications 39 (8) (2012) 6712–6719, https://doi.org/10.1016/j.eswa.2011.12.019.

[67] Y.T. Chang, C.T. Huang, C.F. Lee, S.J. Wang, Image Interpolating based Data Hiding in Conjunction with Pixel Shifting of Histogram, The Journal of Supercomputing 66 (2) (2013) 1093–1110, https://doi.org/10.1007/s11227-013-1016-6.
[68] A. Malik, G. Sikka, H.K. Verma, Image Interpolation based High Capacity Reversible Data Hiding Scheme, Multimedia Tools and Applications 76 (22) (2017) 24107–24123, https://doi.org/10.1007/s11042-016-4186-4.
[69] S.Y. Shen, L.H. Huang, S.S. Yu, A Novel Adaptive Data Hiding based on Improved EMD and Interpolation, Multimedia Tools and Applications 77 (10) (2018) 12563–12579, https://doi.org/10.1007/s11042-017-4905-5.
[70] X. Zhang, Z. Sun, Z. Tang, C. Yu, X. Wang, High Capacity Data Hiding based on Interpolated Image, Multimedia Tools and Applications 76 (7) (2017) 9195–9218, https://doi.org/10.1007/s11042-016-3521-0.
[71] A. Shaik, V. Thanikaiselvan, High Capacity Reversible Data Hiding using 2D Parabolic Interpolation, Multimedia Tools and Applications 78 (8) (2019) 9717–9735, https://doi.org/10.1007/s11042-018-6544-x.
[72] P.C. Mandal, I. Mukherjee, B.N. Chatterji, High Capacity Reversible and Secured Data Hiding in Images using Interpolation and Difference Expansion Technique, Multimedia Tools and Applications (2021) 1–22, https://doi.org/10.1007/s11042-020-09341-3.
[73] C. Qin, C.C. Chang, Y.H. Huang, L.T. Liao, An Inpainting-assisted Reversible Steganographic Scheme using a Histogram Shifting Mechanism, IEEE Transactions on Circuits and Systems for Video Technology 23 (7) (2012) 1109–1118, https://doi.org/10.1109/TCSVT.2012.2224052.
[74] C.L. Liu, H.H. Liu, Reliable Detection of Histogram Shift-based Steganography using Payload Invariant Features, in: Applied Mechanics and Materials, Vol. 284, Trans Tech Publ, 2013, pp. 3517–3521, doi: 10.4028/www.scientific.net/AMM.284-287.3517.
[75] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, Reversible Data Hiding, IEEE Transactions on Circuits and Systems for Video Technology 16 (3) (2006) 354–362, https://doi.org/10.1109/TCSVT.2006.869964.
[76] X. Li, W. Zhang, X. Gui, B. Yang, A Novel Reversible Data Hiding Scheme based on Two-dimensional Difference-histogram modification, IEEE Transactions on Information Forensics and Security 8 (7) (2013) 1091–1100, https://doi.org/10.1109/TIFS.2013.2261062.
[77] W. He, G. Xiong, K. Zhou, J. Cai, Reversible Data Hiding based on Multilevel Histogram Modification and Pixel Value Grouping, Journal of Visual Communication and Image Representation 40 (2016) 459–469, https://doi.org/10.1016/j.jvcir.2016.07.014.
[78] L. Liu, C.C. Chang, A. Wang, Reversible Data Hiding Scheme based on Histogram Shifting of n-bit planes, Multimedia Tools and Applications 75 (18) (2016) 11311–11326, https://doi.org/10.1007/s11042-015-2855-3.
[79] Z. Tang, S. Xu, D. Ye, J. Wang, X. Zhang, C. Yu, Real-time Reversible Data Hiding with shifting block histogram of pixel differences in encrypted image, Journal of Real-Time Image Processing 16 (3) (2019) 709–724, https://doi.org/10.1007/s11554-018-0838-0.
[80] J. Wang, J. Ni, X. Zhang, Y.Q. Shi, Rate and distortion optimization for Reversible Data Hiding using Multiple Histogram Shifting, IEEE Transactions on Cybernetics 47 (2) (2016) 315–326, https://doi.org/10.1109/TCYB.2015.2514110.
[81] J.Y. Hsiao, Z.Y. Lin, P.Y. Chen, Reversible Data Hiding Based on Pairwise Prediction Error Histogram, Journal of Information Science & Engineering 33 (2).
[82] X.Z. Xie, C.C. Chang, Y.C. Hu, An Adaptive Reversible Data Hiding Scheme based on Prediction Error Histogram Shifting by Exploiting Signed Digit Representation, Multimedia Tools and Applications (2020) 1–18, https://doi.org/10.1007/s11042-019-08402-6.
[83] N. Mukherjee, G. Paul, S.K. Saha, Two-point fft-based High Capacity Image Steganography using Calendar based Message Encoding, Information Sciences 552 (2021) 278–290, https://doi.org/10.1016/j.ins.2020.11.044.
[84] C.C. Chang, T.S. Chen, L.Z. Chung, A Steganographic Method based upon JPEG and Quantization Table Modification, Information Sciences 141 (1–2) (2002) 123–138, https://doi.org/10.1016/S0020-0255(01)00194-3.
[85] Q. Giboulot, R. Cogranne, P. Bas, Detectability-based jpeg Steganography Modeling the Processing Pipeline: the Noise-content Trade-off, IEEE Transactions on Information Forensics and Security 16 (2021) 2202–2217, https://doi.org/10.1007 10.1109/TIFS.2021.3050063.
[86] T. Rabie, I. Kamel, High Capacity Steganography: A Global Adaptive Region Discrete Cosine Transform Approach, Multimedia Tools and Applications 76 (5) (2017) 6473–6493, https://doi.org/10.1007/s11042-016-3301-x.
[87] D. Upham, Jsteg, http://www.tiac.net/users/korejwa/jsteg.htm (1997).
[88] N. Provos, Defending Against Statistical Steganalysis., in: Usenix Security Symposium, Vol. 10, 2001, pp. 323–336.
[89] A. Westfeld, F5-A Steganographic Algorithm, Information Hiding (2001) 289–302.
[90] J. Fridrich, T. Pevný, J. Kodovský, Statistically Undetectable JPEG Steganography: Dead Ends Challenges, and Opportunities, in, in: Proceedings of the 9th Workshop on Multimedia & Security, 2007, pp. 3–14, https://doi.org/10.1145/1288869.1288872.
[91] L. Guo, J. Ni, Y.Q. Shi, An Efficient JPEG Steganographic Scheme using Uniform Embedding, in: 2012 IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, 2012, pp. 169–174, https://dx.doi.org/ 10.1109/WIFS.2012.6412644.
[92] H.W. Tseng, C.C. Chang, High Capacity Data Hiding in JPEG Compressed Images, Informatica 15 (1) (2004) 127–142.
[93] C.C. Chang, C.C. Lin, C.S. Tseng, W.L. Tai, Reversible Hiding in DCT-based Compressed Images, Information Sciences 177 (13) (2007) 2768–2786, https://doi.org/10.1016/j.ins.2007.02.019.
[94] C.C. Lin, P.F. Shiu, High Capacity Data Hiding Scheme for DCT-based Images, Journal of Information Hiding and Multimedia Signal Processing 1 (3) (2010) 220–240.
[95] Y.K. Lin, High Capacity Reversible Data Hiding Scheme based upon Discrete Cosine Transformation, Journal of Systems and Software 85 (10) (2012) 2395–2404, https://doi.org/10.1016/j.jss.2012.05.032.
[96] Y.K. Lin, A Data Hiding Scheme based upon DCT Coefficient Mmodification, Computer Standards & Interfaces 36 (5) (2014) 855–862, https://doi.org/10.1016/j.csi.2013.12.013.
[97] T. Rabie, I. Kamel, On the Embedding Limits of the Discrete Cosine Transform, Multimedia Tools and Applications 75 (10) (2016) 5939–5957, https://doi.org/10.1007/s11042-015-2557-x.
[98] D. Hou, H. Wang, W. Zhang, N. Yu, Reversible Data Hiding in JPEG Image based on DCT Frequency and Block Selection, Signal Processing 148 (2018) 41–47, https://doi.org/10.1016/j.sigpro.2018.02.002.
[99] V. Kumar, D. Kumar, Performance Evaluation of Modified Color Image Steganography using Discrete Wavelet Transform, Journal of Intelligent Systems 28 (5) (2017) 749–758, https://doi.org/10.1515/jisys-2017-0134.
[100] X. Liao, K. Li, J. Yin, Separable Data Hiding in Encrypted Image based on Compressive Sensing and Discrete Fourier Transform, Multimedia Tools and Applications 76 (20) (2017) 20739–20753, https://doi.org/10.1007/s11042-016-3971-4.
[101] F. Alturki, R. Mersereau, Secure Blind Image Steganographic Technique using Discrete Fourier Transformation, in: Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205), Vol. 2, IEEE, 2001, pp. 542–545, https://doi.org/ 10.1109/ICIP.2001.958548.
[102] M. Ramkumar, A.N. Akansu, On the Design of Data Hiding Methods Robust to Lossy Compression, IEEE Transactions on Multimedia 6 (6) (2004) 947–951, https://doi.org/10.1109/TMM.2004.837254.
[103] Y.K. Chan, W.T. Chen, S.S. Yu, Y.A. Ho, C.S. Tsai, Y.P. Chu, A HDWT-based Reversible Data Hiding Method, Journal of Systems and Software 82 (3) (2009) 411–421, https://doi.org/10.1016/j.jss.2008.07.008.
[104] S. Sidhik, S. Sudheer, V.M. Pillai, Performance and Analysis of High Capacity Steganography of Color Images Involving Wavelet Transform, Optik 126 (23) (2015) 3755–3760, https://doi.org/10.1016/j.ijleo.2015.08.208.
[105] I. Mukherjee, B. Datta, R. Banerjee, S. Das, DWT Difference Modulation based Novel Steganographic Algorithm, in, in: International Conference on Information Systems Security, Springer, 2015, pp. 573–582, https://doi.org/10.1007/978-3-319-26961-0-36.
[106] M.S. Subhedar, V.H. Mankar, Image Steganography using Redundant Discrete Wavelet Transform and QR Factorization, Computers & Electrical Engineering 54 (2016) 406–422, https://doi.org/10.1016/j.compeleceng.2016.04.017.
[107] S. Atawneh, A. Almomani, H.A. Bazar, P. Sumari, B. Gupta, Secure and Imperceptible Digital Image Steganographic Algorithm based on Diamond Encoding in DWT Domain, Multimedia Tools and Applications 76 (18) (2017) 18451–18472, https://doi.org/10.1007/s11042-016-3930-0.

[108] V. Kumar, D. Kumar, A Modified DWT-based Image Steganography Technique, Multimedia Tools and Applications 77 (11) (2018) 13279–13308, https://doi.org/10.1007/s11042-017-4947-8.
[109] M. Fakhredanesh, M. Rahmati, R. Safabakhsh, Steganography in Discrete Wavelet Transform based on Human Visual System and Cover Model, Multimedia Tools and Applications 78 (13) (2019) 18475–18502, https://doi.org/10.1007/s11042-019-7238-8.
[110] P.C. Mandal, I. Mukherjee, Integer Wavelet Transform based Secured Image Steganography using LSB and Coefficient Value Differencing, in: 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), IEEE, 2021, pp. 332–337, https://doi.org/10.1109/ICSCCC51823.2021.9478095.
[111] M.D. Adams, F. Kossentni, Reversible Integer-to-Integer Wavelet Transforms for Image Compression: Performance Evaluation and Analysis, IEEE Transactions on Image Processing 9 (6) (2000) 1010–1024, https://doi.org/10.1109/83.846244.
[112] G. Xuan, J. Zhu, J. Chen, Y.Q. Shi, Z. Ni, W. Su, Distortionless Data Hiding based on Integer Wavelet Transform, Electronics Letters 38 (25) (2002) 1646–1648, https://doi.org/10.1049/el:20021131.
[113] K. Raja, S. Sindhu, T. Mahalakshmi, S. Akshatha, B. Nithin, M. Sarvajith, K. Venugopal, L.M. Patnaik, Robust Image Adaptive Steganography using Integer Wavelets, in: 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08), IEEE, 2008, pp. 614–621, https://doi.org/10.1109/COMSWA.2008.4554484.
[114] N. Raftari, A.M.E. Moghadam, Digital Image Steganography based on Integer Wavelet Transform and Assignment Algorithm, in: 2012 Sixth Asia Modelling Symposium, IEEE, 2012, pp. 87–92, https://doi.org/ 10.1109/AMS.2012.15.
[115] A.K. Gulve, M.S. Joshi, An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform using Pixel Value Differencing Approach, Mathematical Problems in Engineering 2015 (2015) 1–14, https://doi.org/10.1155/2015/684824.
[116] L. Xiong, Z. Xu, Y.Q. Shi, An Integer Wavelet Transform based Scheme for Reversible Data Hiding in Encrypted Images, Multidimensional Systems and Signal Processing 29 (3) (2018) 1191–1202, https://doi.org/10.1007/s11045-017-0497-5.
[117] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, E. Mohamed, A Secure Image Steganography Algorithm based on Least Significant Bit and Integer Wavelet Transform, Journal of Systems Engineering and Electronics 29 (3) (2018) 639–649, https://doi.org/10.21629/JSEE.2018.03.21.
[118] M. Kalita, T. Tuithung, S. Majumder, A New Steganography Method Using Integer Wavelet Transform and Least Significant Bit Substitution, The Computer Journal 62 (11) (2019) 1639–1655, https://doi.org/10.1093/comjnl/bxz014.
[119] G. Ma, J. Wang, Efficient Reversible Data Hiding in Encrypted Images based on Multi-stage Integer Wavelet Transform, Signal Processing: Image Communication 75 (2019) 55–63, https://doi.org/10.1016/j.image.2019.03.013.
[120] H. Zhang, L. Hu, A Data Hiding Scheme based on Multidirectional Line Encoding and Integer Wavelet Transform, Signal Processing: Image Communication 78 (2019) 331–344, https://doi.org/10.1016/j.image.2019.07.019.
[121] P.K. Muhuri, Z. Ashraf, S. Goel, A Novel Image Steganographic Method based on Integer Wavelet Transformation and Particle Swarm Optimization, Applied Soft Computing (2020) 106257–106300, https://doi.org/10.1016/j.asoc.2020.106257.
[122] P.C. Mandal, I. Mukherjee, B. Chatterji, High Capacity Steganography based on IWT using Eight-way CVD and n-LSB Ensuring Secure Communication, Optik 247 (2021) 1–16, https://doi.org/10.1016/j.ijleo.2021.167804.
[123] M. Kharrazi, H.T. Sencar, N.D. Memon, Performance Study of Common Image Steganography and Steganalysis Techniques, Journal of Electronic Imaging 15 (4) (2006) 041104–041120, https://doi.org/10.1117/1.2400672.
[124] C.C. Chang, P. Tsai, M.H. Lin, An Adaptive Steganography for Index based Images using Codeword Grouping, in: Pacific Rim Conference on Multimedia, Springer, 2004, pp. 731–738, https://doi.org/10.1007/978-3-540-30543-9-91.
[125] Y.T. Wu, F.Y. Shih, Genetic Algorithm based Methodology for Breaking the Steganalytic Systems, IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics) 36 (1) (2006) 24–31, https://doi.org/10.1109/TSMCB.2005.852474.
[126] L.Y. Tseng, Y.K. Chan, Y.A. Ho, Y.P. Chu, Image Hiding with an Improved Genetic Algorithm and an Optimal Pixel Adjustment Process, in: 2008 Eighth International Conference on Intelligent Systems Design and Applications, Vol. 3, IEEE, 2008, pp. 320–325, https://doi.org/ 10.1109/ISDA.2008.235.
[127] T. Pevný, T. Filler, P. Bas, Using High-dimensional Image Models to Perform Highly Undetectable Steganography, in: International Workshop on Information Hiding, Springer, 2010, pp. 161–177, https://doi.org/10.1007/978-3-642-16435-4-13.
[128] V. Holub, J. Fridrich, Designing Steganographic Distortion using Directional Filters, in: 2012 IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, 2012, pp. 234–239, https://doi.org/ 10.1109/WIFS.2012.6412655.
[129] V. Holub, J. Fridrich, Digital Image Steganography using Universal Distortion, in: Proceedings of the First ACM Workshop on Information Hiding and Multimedia Mecurity, 2013, pp. 59–68, doi: 10.1145/2482513.2482514.
[130] M. Khodaei, K. Faez, Image Hiding by using Genetic Algorithm and LSB Substitution, in: International Conference on Image and Signal Processing, Springer, 2010, pp. 404–411, https://doi.org/10.1007/978-3-642-13681-8-47.
[131] H.R. Kanan, B. Nazeri, A Novel Image Steganography Scheme with High Embedding Capacity and Tunable Visual Image Quality based on a Genetic Algorithm, Expert Systems with Applications 41 (14) (2014) 6123–6130, https://doi.org/10.1016/j.eswa.2014.04.022.
[132] N.N.E. Emam, New Data Hiding Algorithm based on Adaptive Neural Networks with Modified Particle Swarm Optimization, Computers & Security 55 (2015) 21–45, https://doi.org/10.1016/j.cose.2015.06.012.
[133] A. Miri, K. Faez, Adaptive Image Steganography based on Transform Domain via Genetic Algorithm, Optik 145 (2017) 158–168, https://doi.org/10.1016/j.ijleo.2017.07.043.
[134] B. Ma, B. Li, X.Y. Wang, C.P. Wang, J. Li, Y.Q. Shi, Code Division Multiplexing and Machine Learning based Reversible Data Hiding Scheme for Medical Image, Security and Communication Networks 2019 (2019) 1–14, https://doi.org/10.1155/2019/4732632.
[135] I.J. Kadhim, P. Premaratne, P.J. Vial, High Capacity Adaptive Image Steganography with Cover Region Selection using Dual-tree Complex Wavelet Transform, Cognitive Systems Research 60 (2020) 20–32.
[136] S.S. Al Hussien, M. Mohamed, E.H. Hafez, Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning, IEEE Access 9 (2021) 16522–16531, https://doi.org/10.1109/ACCESS.2021.3050737.
[137] S. Ghamizi, M. Cordy, M. Papadakis, Y.L. Traon, Adversarial Embedding: A Robust and Elusive Steganography and Watermarking Technique, arXiv preprint arXiv:1912.01487.
[138] S. Baluja, Hiding Images in Plain Sight: Deep Steganography, Advances in Neural Information Processing Systems (2017) 2069–2079.
[139] D. Hu, L. Wang, W. Jiang, S. Zheng, B. Li, A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks, IEEE Access 6 (2018) 38303–38314, https://doi.org/10.1109/ACCESS.2018.2852771.
[140] C. Li, Y. Jiang, M. Cheslyar, Embedding Image Through Generated Intermediate Medium using Deep Convolutional Generative Adversarial Network, Computers, Materials & Continua 56 (2) (2018) 313–324.
[141] J. Yang, K. Liu, X. Kang, E.K. Wong, Y.Q. Shi, Spatial Image Steganography based on Generative Adversarial Network, arXiv preprint arXiv:1804.07939.
[142] R. Zhang, S. Dong, J. Liu, Invisible Steganography via Generative Adversarial Networks, Multimedia Tools and Applications 78 (7) (2019) 8559–8575, https://doi.org/10.1007/s11042-018-6951-z.
[143] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, C. Qin, Reversible Image Steganography Scheme based on a U-Net Structure, IEEE Access 7 (2019) 9314–9323, https://doi.org/10.1109/ACCESS.2019.2891247.
[144] W. Tang, B. Li, S. Tan, M. Barni, J. Huang, CNN-based Adversarial Embedding for Image Steganography, IEEE Transactions on Information Forensics and Security 14 (8) (2019) 2074–2087, https://doi.org/10.1109/TIFS.2019.2891237.
[145] S. Ma, X. Zhao, Y. Liu, Adaptive Spatial Steganography based on Adversarial Examples, Multimedia Tools and Applications 78 (22) (2019) 32503–32522, https://doi.org/10.1007/s11042-019-07994-3.
[146] J. Yang, D. Ruan, J. Huang, X. Kang, Y.Q. Shi, An Embedding Cost Learning Framework using GAN, IEEE Transactions on Information Forensics and Security 15 (2019) 839–851, https://doi.org/10.1109/TIFS.2019.2922229.

[147] Y. Shang, S. Jiang, D. Ye, J. Huang, Enhancing the Security of Deep Learning Steganography via Adversarial Examples, Mathematics 8 (9) (2020) 1446–1454, https://doi.org/10.3390/math8091446.
[148] B. Ray, S. Mukhopadhyay, S. Hossain, S.K. Ghosal, R. Sarkar, Image Steganography using Deep Learning based Edge Detection, Multimedia Tools and Applications 80 (24) (2021) 33475–33503, https://doi.org/10.1007/s11042-021-11177-4.
[149] N. Hamid, B.S. Sumait, B.I. Bakri, O. Al Qershi, Enhancing Visual Quality of Spatial Image Steganography using Squeezenet Deep Learning Network, Multimedia Tools and Applications 80 (28) (2021) 36093–36109, doi: 10.1007/s11042-021-11315-y.
[150] A. Westfeld, A. Pfitzmann, Attacks on Steganographic Systems, Information Hiding (1999) 61–76, https://doi.org/10.1007/10719724-5.
[151] N. Provos, P. Honeyman, Hide and Seek: An Introduction to Steganography, IEEE Security & Privacy 1 (3) (2003) 32–44, https://doi.org/10.1109/MSECP.2003.1203220.
[152] J. Fridrich, M. Goljan, D. Hogea, Attacking the Outguess, ACM Workshop on Multimedia and Security (2002) 3–6.
[153] J. Kodovský, J. Fridrich, Steganalysis of JPEG Images using Rich Models, in: Media Watermarking, Security, and Forensics 2012, Vol. 8303, International Society for Optics and Photonics, 2012, pp. 1–13, doi: 10.1117/12.907495.
[154] M. Chen, V. Sedighi, M. Boroumand, J. Fridrich, JPEG-phase-aware Convolutional Neural Network for Steganalysis of JPEG Images, in, in: Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security, 2017, pp. 75–84, https://doi.org/10.1145/3082031.3083248.
[155] J. Fridrich, J. Kodovsky, Rich Models for Steganalysis of Digital Images, IEEE Transactions on Information Forensics and Security 7 (3) (2012) 868–882, https://doi.org/10.1109/TIFS.2012.2190402.
[156] J. Ye, J. Ni, Y. Yi, Deep Learning Hierarchical Representations for Image Steganalysis, IEEE Transactions on Information Forensics and Security 12 (11) (2017) 2545–2557, https://doi.org/10.1109/TIFS.2017.2710946.
[157] M. Yedroudj, M. Chaumont, F. Comby, How to Augment a Small Learning Set for Improving the Performances of a CNN-based Steganalyzer?, Electronic Imaging 2018 (7) (2018) 317–329, https://doiorg/10.2352/ISSN.2470-1173.2018.07.MWSF-317.
[158] G. Xu, H.-Z. Wu, Y.-Q. Shi, Structural Design of Convolutional Neural Networks for Steganalysis, IEEE Signal Processing Letters 23 (5) (2016) 708–712, https://doi.org/10.1109/LSP.2016.2548421.
[159] V. Holub, J. Fridrich, Random Projections of Residuals for Digital Image Steganalysis, IEEE Transactions on Information Forensics and Security 8 (12) (2013) 1996–2006, https://doi.org/10.1109/TIFS.2013.2286682.
[160] M. Hussain, A.W.A. Wahab, Y.I.B. Idris, A.T. Ho, K.H. Jung, Image Steganography in Spatial Domain: A Survey, Signal Processing: Image Communication 65 (2018) 46–66, https://doi.org/10.1016/j.image.2018.03.012.
[161] P.C. Mandal, Structural Design of Convolutional Neural Network Based Steganalysis, in: Computational Intelligence and Machine Learning, Springer, 2021, pp. 39–45, doi: 10.1007/978-981-15-8610-1_5.
[162] J. Fridrich, M. Goljan, R. Du, Detecting LSB Steganography in Color, and Gray Scale Images, IEEE Multimedia 8 (4) (2001) 22–28, https://doi.org/10.1109/93.959097.
[163] A. Westfeld, A. Pfitzmann, Attacks on Steganographic Systems, in: International Workshop on Information Hiding, Springer, 1999, pp. 61–76, doi: 10.1007/10719724-5.
[164] O.J. Sandoval, M.C. Hernandez, G.S. Perez, K.T. Medina, H.P. Meana, M.N. Miyatake, Compact Image Steganalysis for LSB Matching Steganography, in: 2017 5th International Workshop on Biometrics and Forensics (IWBF), IEEE, 2017, pp. 1–6, https://doi.org/ 10.1109/IWBF.2017.7935103.
[165] V. Sabeti, S. Samavi, M. Mahdavi, S. Shirani, Steganalysis and Payload Estimation of Embedding in Pixel Differences using Neural Networks, Pattern Recognition 43 (1) (2010) 405–415, https://doi.org/10.1016/j.patcog.2009.06.006.
[166] Y. Qian, J. Dong, W. Wang, T. Tan, Deep Learning for Steganalysis via Convolutional Neural Networks, in: Media Watermarking, Security, and Forensics 2015, Vol. 9409, International Society for Optics and Photonics, 2015, pp. 171–180, doi: 10.1117/12.2083479.
[167] J. Kim, H. Park, J.I. Park, CNN-based Image Steganalysis using Additional Data Embedding, Multimedia Tools and Applications 79 (1–2) (2020) 1355–1372, https://doi.org/10.1007/s11042-019-08251-3.
[168] Y. Qian, J. Dong, W. Wang, T. Tan, Feature Learning for Steganalysis using Convolutional Neural Networks, Multimedia Tools and Applications 77 (15) (2018) 19633–19657, https://doi.org/10.1007/s11042-017-5326-1.
[169] Y. Zou, G. Zhang, L. Liu, Research on Image Steganography Analysis based on Deep Learning, Journal of Visual Communication and Image Representation 60 (2019) 266–275, https://doi.org/10.1016/j.jvcir.2019.02.034.
[170] J. Zeng, S. Tan, B. Li, J. Huang, Large-scale JPEG Image Steganalysis using Hybrid Ddeep Learning Framework, IEEE Transactions on Information Forensics and Security 13 (5) (2018) 1200–1214, https://doi.org/10.1109/TIFS.2017.2779446.
[171] S. Wu, S. Zhong, Y. Liu, Deep Residual Learning for Image Steganalysis, Multimedia Tools and Applications 77 (9) (2018) 10437–10453, https://doi.org/10.1007/s11042-017-4440-4.
[172] Q. Zhang, X. Zhao, C. Liu, Convolutional Neural Network for Larger JPEG Images Steganalysis, International Workshop on Digital Watermarking, Springer (2018) 14–28, https://doi.org/10.1007/978-3-030-11389-6-2.
[173] B. Singh, A. Sur, P. Mitra, Steganalysis of Digital Images Using Deep Fractal Network, IEEE Transactions on Computational Social Systems 8 (3) (2021) 599–606, https://doi.org/10.1109/TCSS.2021.3052520.
[174] Images, The BOSSbase-1.01 Database, Binghamton University, available from: http://dde.binghamton.edu/download/.
[175] Z. Pan, W. Yu, X. Yi, A. Khan, F. Yuan, Y. Zheng, Recent Progress on Generative Adversarial Networks (GANs): A Survey, IEEE Access 7 (2019) 36322–36333, https://doi.org/10.1109/ACCESS.2019.2905015.