

A new method for locating data hiding in image steganography

Sabyasachi Pramanik¹ o

Received: 8 August 2022 / Revised: 15 May 2023 / Accepted: 31 August 2023 / Published online: 26 September 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

In the steganographic picture, it remains a challenging problem to determine the best place for inserting the hidden message with a minimum distortion of the host medium. However, there is a long way to go to select the right embedding position with less distortion. To accomplish this goal, we suggest a new high performance image steganography method in which extreme machine learning algorithms (ELM) are updated to build a supervised mathematical model. The ELM is initially checked in regression mode on a portion of the picture or host medium. This helped us to determine the best place to embed the message with the best values in the expected assessment measurements. For practicing on a new metric, contrast, homogeneity and other texture characteristics are used. In addition, the established ELM is used to tackle over fitting during workout. The findings are analyzed using the correlation, the structural similarity measure, fusion matrices and mean square error in the efficiency of the proposed steganography approach. In terms of imperceptibility, the adjusted ELM has been found to transcend current approaches. Excellent characteristics of the findings indicate that the proposed steganographic method is highly capable of retaining the visual image detail. In accordance with the current state of the art approaches, an increase of 28 per cent of imperceptibility is achieved.

Keywords Steganography \cdot Extreme machine learning \cdot Artificial neural network \cdot PSNR \cdot SSIM \cdot MSE

1 Introduction

In the scientific study, investigators concluded that three reasons for demonstrating that secure transmission of information is world - renowned with the help of that system could split the system by accessing the vulnerable available information in the remote server. In actuality, some questions were addressed vulnerable to criminal purpose held in certain computer systems being recognized by spywares [49]. These viruses or worms could



Sabyasachi Pramanik sabyalnt@gmail.com

Haldia Institute of Technology, Haldia, India

therefore be identified by using virus protection and a solution to this problem is strict rules obtained by firewall [7] discussed in steganography [19] techniques.

- An adverse effect on the transition of copyrights
- Internet-wide materials.
- Transfer of patents across the internet and storage.

The concept of embedding secret information inside other data is steganography. Text, photograph, audio, or video may be such information. The key goal of steganography is to mask classified data for secrecy in the host media. Steganography, therefore, offers safe communication via multimedia [68]. In addition, steganography may be used as a multimedia encapsulation technique where one medium is incorporated into another one. Multimedia encapsulation [62] thus allows a safe transition from one system to another of the metadata [72]. Over the decades, the continually growing advances in communication technologies have allowed sensitive information [71] to be openly transmitted and exchanged through the complex Internet network. Critical data exchange, as well as video/audio files [2], was a major security threat [57]. The security of consumer data is constantly jeopardized by sophisticated and disappointing attacks on phishing [20]. Unauthorized access or attack is then required to absolute security of sensitive data communication [48]. Currently, safe correspondence is accomplished by cryptographic and steganophical strategies backed by mathematical models. Ironically, it would not hide the presence of data when encrypting a plain-text [4] for the generation of cipher texts. It renders the data nonsensical to discourage assault or unwanted access to the hidden message. The shortcomings of cryptography [51] are solved with the implementation of a new technique called steganography for completely protected transmission of information. Nevertheless, most traditional techniques of steganography are subject to picking the right spots for message embedding with a minimum deformation in the host medium. Introduction of the steganographic technique based on the neural network (NN), where NN is used as a dispersed portrayal to accumulate the training [34] information, would resolve this shortage. Therefore, it is literally unfeasible to view the secret message beyond understanding the framework of the NN. While some researchers favor interpretable models, such as myth or predictive prototypes and heuristically [75] simulated frameworks like fuzzy [25], black box frameworks is shown to be more capable, in real-life, to capture complicated information and demonstrate their functionality. Different forensics experts are exploring data hiding techniques, and they have suggested several important steganographic algorithms to boost reliability and preserve the existence of the embedded data to prevent unintended parties from accessing the information. Goljan and Fridrich et al. [31] presented several original and prominent data embedding approaches, directly utilizing the digital image picture element and concealing secret message in the pixels. The approaches integrated secret constant amount secrets bits of message in the Least Significant Bits of the cover image's picture elements. But, constant Least Significant Bit embedding approaches for information are frail, and if its presence is suspected, the hidden information can be easily recovered. Therefore, for data hiding, it is good to utilize a varying LSB quantity. In such cases, if an attacker is doubtful of the existence of message, it is burdensome to retrieve the data. Steganography can be used in the

- Steganography can be a solution that allows for sending information and data whilst being blocked even without the possibility of transmitting and tracking the communications back to us.
- To store information about a venue, it is also possible to simply use steganography. For starters, it is possible to store many sources of knowledge, like our privatized banking



- information, several military agents, in a cover source. We will quickly disclose our banking details when we are asked to unhide the hidden message in our host file while it would be difficult to demonstrate the existence of the military activities.
- 3. To introduce watermarking, steganography can also be utilized. Although the principle for watermarking does not actually apply, there are several techniques in steganography, which are used for storing watermarks in files. The predominant distinction is on the basis of watermarking and the purpose of steganography is hiding the information. Watermarking is solely expanding the origins of the host having extra details. As individuals aren't going to consider noticeable improvements due to a watermark, steganographic pictures, audio or video files can be used.
- 4. A fascinating use of steganography is made possible by e-commerce. In most consumers of new e-commerce purchases, they are secured by a username and password, with no real means to check whether the username is the real card holder. Using biometric screening for finger printing, combined with fingerprint-embedded special session IDs steganographic photos allow for a very safe alternative to open authentication of e-commerce transactions.
- 5. Steganography together with existing methods of communication can be used to execute secret trades. Two types of secret messages are of concern to governments: those who support national communications security and the ones who don't. Digital steganography provides large quantities of data for both forms and opportunity. Companies may have comparable concerns regarding trade secrets or information regarding new goods.
- 6. Another main application of the transport of critical data is steganography. A possible cryptographic concern is that when they see it, eavesdroppers know they have an encrypted letter. Steganography enables critical data to be transferred without knowing some confidential details. The principle of using steganography in the transport of data which may be applied to just about every form of data transport, from e-mail to photos or blogs on the internet.

The advanced art in speech recognition [41], object recognition and various areas of knowledge is significantly illustrated in such black box models. The steganographic strategy uses information covering protocols to insert the data into a host media to avoid the discovery of secret information. Image steganography is the most common and commonly used of several steganographic techniques (concealing data into an image) since it enables the sharing of a large number of images through the internet. Furthermore, secret data provided by image steganography cannot be detected by visual analysis. The heuristic search optimization has been attractive to the steganography domain. Despite a great deal of study, it remains tough to achieve an effective steganographic algorithm to determine the best spot for embedding with lower computing time. Image steganographic techniques are classified into spatial and transform domain integration according to embedded positions. The later is also known as a transform domain embedding. The least important steganography of the spatial domain is the most commonly used approach in which steganography based on the LSB is used, and the LSB [52] carrier or host image is used to mask the hidden letter. By comparison, the concealed secret information can be discovered by the current steganalysis techniques in the least important bit replacement (LSBR)-constructed staganography. Therefore, visual and statistical attacks [37] are poor. The LSBM system also known as \pm embedding technique gives more protection related to LSBR. The LSBM method offers greater stability. But for most versions, steganographic techniques are incompatible. The spatial domain approaches aren't resilient against picture manipulation, noise attack [24],



and loss in compressing [27] in spite of their high power. In comparison, owing to the overall use of the BMP file, the mathematical properties of the image are compensated. As noted above, hidden details are hidden in the substantial regions of the host picture in frequency-based steganography. This domain includes multiple transformations like the DCT [60] and the DWT [54]. These transformations are used in concealing a message in a picture. Although the DWT and DCT make comparatively lower payload capacity, the earlier is more dominant to image recognition, statistical and noise tolerance. In addition to distortion and assaults steganographic strategies have a greater tolerance to attack in the frequency domain than in the spatial domain.

With the support of a frequency domain [36], the shortcomings of spatial domain technology can be addressed. Many DWT inquiries have been conducted for steganographic implementations that involve the appearance of rounding errors in the reverse DFT [3] drawbacks. Table 1 provides a short description of the inclusion in the space or frequency domain of hidden knowledge. Any physicists merged the space and frequency fields. The framework has been established to enhance the adaptive distortion mechanism in order to ensure minimum statistical detection [17]. The primary objective of steganographic approaches is to embed the undisclosed data in a host medium and its presence continues to be imperceptible. No noticeable variation is produced by the concealed data and does not fascinate the human vision (Human Visual System). As reported in the literature, the HVS has some limitations. The HVS is more sensitive compared to the complex region to alterations established in the smooth zone of the host image. The change introduced in the complex region is therefore difficult for HVS to detect and incorporates the complex zone of the host picture more favorable for information concealing.

With the classification of the complicated zone and smooth region pixels, hiding data in the complex region is initiated and complicated zone picture elements are detected. For data embedding, the complicated zone picture elements are utilized and the polished zone picture elements remain unaltered. In the literature review that can be used for this purpose, consists of several methods, e.g., canny edge detection, Deriche [39], differential [34], Sobel [10], Prewitt [22], Roberts cross, and others. These techniques are utilized in digital images to perceive complicated zone, but the execution of these approaches detects frail and detached peripheries and considers the communicating picture elements to be a constituent of the actual complicated periphery. Various picture elements that do not constitute the peripheries of the data concealing techniques are also subject to edge-based information hiding using these techniques. This makes such a technique of information hiding more sensitive to noise [74]. The motive underlying designing methods of image steganography is to help as per its use to interact in different organizations. It may also be used for contact with members of the military or security agents or agents of corporations to mask hidden correspondence or in the area of surveillance. The primary purpose of using steganography is to prevent attention being drawn to the transfer of secret knowledge. If doubt is aroused, so this aim to achieve the security of the secret messages has been prepared, and if the hackers noted some improvement in the received message, this investigator would want to know the hidden information within the message. One of the most common explanations that intruders can obtain unauthorized access to information and can use this information to damage, alter and assault someone for their own purposes. As technologies are increasingly growing due to the possibilities of hacking or un-authorizing information, contact often grows and requires specific kinds of protection from intruders in modern times. Not only is it restricted to information or correspondence, it often refers to the computer network, since the internet is only the medium for message sharing. Therefore, it is more important to provide the computer network with more protection since much of the data is transmitted over the internet. The



Author (s)Domain and ApproachAdvantagesDisadvantages[28]LSB and IWTCapable of hiding confidential text with an enormous payload capacity including an enhanced security level and an enhanced invisibilityNot applied to text or images[19]Hamming DistanceEnhanced hiding competency, enhanced capacity and lesserNot tested against image processing a computational costUnclear image quality[11]LSB and DCTCryptography encrypts the message making it more safeUnclear image quality[14]Batch SteganographyStoring secret data on multiple imagesNot tested against statistical attacks[15]DCT and ECCHigh PSNR and SSIMTheoretically implemented and not change is not conveyed[79]High Dimensional KL DivergenceSecurity measure is feasible and effectiveCapacity issue is not conveyed	Table 1 The en	Table 1 The embedding Methods for the current works	83	
LSB and IWT Capable of hiding confidential text with an enormous payload capacity including an enhanced security level and an enhanced invisibility Hamming Distance Enhanced hiding competency, enhanced capacity and lesser computational cost LSB and DCT Cryptography encrypts the message making it more safe Chaos encryption Safer and more imperceptible Safer and more imperceptible Storing secret data on multiple images DCT and ECC High PSNR and SSIM High Divergence Security measure is feasible and effective		Domain and Approach	Advantages	Disadvantages
Hamming Distance Enhanced hiding competency, enhanced capacity and lesser computational cost LSB and DCT Cryptography encrypts the message making it more safe Cryptography encrypts the message making it more safe Safer and more imperceptible Sater and more imperceptible Batch Steganography Storing secret data on multiple images DCT and ECC High PSNR and SSIM High Dimensional KL Divergence Security measure is feasible and effective	[28]	LSB and IWT	Capable of hiding confidential text with an enormous payload capacity including an enhanced security level and an enhanced invisibility	Not applied to text or images
LSB and DCT Cryptography encrypts the message making it more safe Chaos encryption Safer and more imperceptible Batch Steganography Storing secret data on multiple images DCT and ECC High PSNR and SSIM High Dimensional KL Divergence Security measure is feasible and effective	[19]	Hamming Distance	Enhanced hiding competency, enhanced capacity and lesser computational cost	Not tested against image processing attacks
Chaos encryption Safer and more imperceptible Batch Steganography Storing secret data on multiple images DCT and ECC High PSNR and SSIM High Dimensional KL Divergence Security measure is feasible and effective	[11]		Cryptography encrypts the message making it more safe	Unclear image quality
Batch Steganography Storing secret data on multiple images DCT and EC High PSNR and SSIM High Dimensional KL Divergence Security measure is feasible and effective	[58]	Chaos encryption	Safer and more imperceptible	Experiments does not include hiding text within image
DCT and ECC High PSNR and SSIM High Dimensional KL Divergence Security measure is feasible and effective	[14]	Batch Steganography	Storing secret data on multiple images	Not tested against statistical attacks
KL Divergence Security measure is feasible and effective	[23]	DCT and ECC	High PSNR and SSIM	Theoretically implemented and not checked by actual data such as text or pictures,
	[62]		Security measure is feasible and effective	Capacity issue is not conveyed



primary explanation for this is to protect secrecy, honesty, usability and also to avoid the illegal use of information. This can only be avoided by either concealing the presence of the data or preserving the information. Steganography and cryptography are the most effective means of avoiding this. These are also complimentary to another to have improved protection, anonymity and honesty for others. One of the main fields in the field of steganography is picture steganography. As the need for confidentiality and secrecy grows, there is a need to conceal sensitive information from them. If a client wants to give their confidential information by using image steganography to those individuals with protection and privacy who can send it. The value of steganography is that it can be used to relay messages anonymously without the knowledge that the transmission is revealed. Sometimes, the sender or recipient may be marked as someone with something to conceal when using cryptography. For instance, the photo might mask the plans for your company's next technological breakthrough. There are also a variety of drawbacks of steganography. It usually takes a lot of overhead to hide a comparatively few bits of information, unlike encryption. In addition, it is made obsolete until a steganographic method is found. If the secret data relies on some kind of key for its insertion and retrieval, this problem can be solved.

Increased steganographic results, including ANN [50] and genetic algorithm (GA) [53] or both depending on the spatial domain was used to eliminate distortion and in order to speed up training, GA and ANN are used. In order to increase the embedding power, the ANN frequency domain is used. In order to achieve good approximation capability, rapid convergence and stable surface performances, spatial sector-related ANN is used. In addition to increasing estimation capability and minimizing distortion, ANN form is used. The ANN is often used for the embedding of a message with steganography, which presumes the hidden message represented in an image. The steganography was therefore able to openly modify the message details provided that visual information is maintained. This presumption, however, does not extend to text data. ANN is also utilized to validate the picture for digital watermarking, where a hidden message is not needed. ANN is used to optimize power, to detect steganographic contents, to classify the hidden information in a picture while adding to steganalysis or as a classification, and to determine the upper and lower bound of the integrative capacity. GAs was also used for various applications of steganography. For quest and optimization [69], GA is used in modeling the steganography dilemma. In addition, the GAs can be optimized for minimally skewed used when a stego picture is collected similar to the cover picture. This introduces Discrete Cosine Transform [15] with Markov as identification and classification related to pictures. Table 2 shows numerous methods for hiding in combined areas of spatial [29] and frequency domain. Recent use of the learning resources of NNs is made of standard methods for data hiding to improve optimization. ANN is used in steganography either to identify the stego file, or to detect hidden information [64] in a picture. The authors are working to minimize the distortion [76] of the stego file, by choosing the image position for hiding messages as adequately as possible. Theoretically, at incredibly high learning speeds, an ELM shows strong generalization efficiency and universal approximation. It may be used for the purposes of either grouping or regression [8]. Inspired by some noteworthy ones we recommend an ELM-related supervised framework for image steganography also known as the Optimal Embedding Position Finder (OEPF). Moreover, during training in regression mode, an enhanced fusion criterion (fusion1) [9] is implemented to realize the best output metric for steganography. To assess the results, another novel fusion metric (fusion2) [42] has been created. And to the best of our understanding, we are using the unit for the first time.

Learning to decide the best spot for embedding [55], with the least vulnerable location is a huge challenge. The current development of the World Wide Web (WWW) and the creation



 Table 2
 Frequency Domain Techniques with various embedding methods for the current approaches

Author (s)	Domain and Approach	Advantages	Disadvantages[]
[15]	DCT	Produces visually good texture images	Focus on payload aspects rather than embedding
[16]	Transform domain and GA	Strong against various steganalysis attacks	Concentrates on payload factor rather than hiding
[70]	DCT Domain	Significant changes in DCT domain	High complexity
[80]	Transform domain and Biometric data	Enhancing the security by minimizing deformation	The ideal number of blocks and their sizes were omitted
[81]	It constructs the problem of steganography as a problem of searching and optimization.	Increases the capability of encoding and promotes true color hidden image with share size limit.	Hiding small image into large image
[56]	Transform domain and PVD	Increases the approximation capacity.	MSE and PSNR aren't achieved and are not verified for various image processing attacks
[9]	Spatial LSB and ANN	Where the hiding level is poor, i.e. less than 15% It is applied in Steganalysis and not in encoding of various hidden message, this was particuter process. Various faulty levels are resolved whe larly difficult.	It is applied in Steganalysis and not in encoding process. Various faulty levels are resolved when removing the hidden information.



of the next-generation Web make it possible to send a huge amount of data through wireless networks [35]. In networking channels such as cellular networks, confidential information exchanged is inherently insecure. The true intent of the information being shared between legitimate users could theoretically intercept and adversely manipulate unauthorised users. Effective steganography approaches are very beneficial in avoiding such unwanted data interception. In stenography, there is a trade-off with image quality and implanting ability when implanting data within a picture. In fact, the further data is concealed within such a cover file, the more deterioration the image experiences, causing the resulting consistency of the stego image to decrease. It can be seen as an optimization challenge to integrate high data capacity into an image while maintaining the consistency of the carrier image.

2 Optimal Embedding Position Finder (OEPF) model

By avoiding the message in an image, more conventional steganographic approaches hide the secret information into a picture. The importance of the spatial characteristics of the photograph nevertheless, the message homogeneity characteristics of the image blocks critically assess the determination of the best embedding [21] place. A spot with the least image distortion is known to be the optimal one. Every type of distortion in the image must be used to shield the embedding mechanism from steganalysis [43].

After the payload [73] is inserted, in addition, both physically and objectively, the cover image and stego image have to be nearly similar. The primary factors that cause the distortion are the chosen region and the embedding process. ELM is recommended for locating the superior hidden position based on the OEPF model. It should be noted that because of its generalized estimation ability, ELM (Li, D. 2018) is advantageous, that makes speedy learning with a better over-fitting evasion compared to other contemporary Neural Network-oriented techniques. To train any separate-secret-level Neural Network consisting of a differing quantity of neurons, a modified ELM is thus used.

3 Legacy of modeling for steganography

As stated before, without affecting its visual features, OEPF recognizes the best appropriate window for hiding the hidden data in the picture. The picture is initially partitioned into (8 x 8) block picture elements, and each block inserts a single bit of the information. The picture is finally decomposed in alternating square frames to hide the information, based on the information length. Every square window's energy (E) [13], contrast (D) [33], homogeneity (Homo) [5], correlation (CRel) [67], mean (M) [18], entropy (Ent) [40], standard deviation (SD) [45], and are determined using:

$$D = \sum_{x,y} (x - y)^2 s(x, y)$$
 (1)

$$E = \sum_{x,y} s(x,y)^2 \tag{2}$$

$$J = \sum_{x,y} \frac{1}{1 - (x - y)^2} s(x, y) \tag{3}$$



(7)

$$Ent = -\sum_{x,y} s(x,y) \log(x,y)$$
 (4)

$$C \operatorname{Re} l = \frac{co(\operatorname{cov} er_picture, stego_picture)}{\|\operatorname{cov} er_picture\|\|stego_picture\|}$$
(5)

where x and y are the x-coordinate and y- coordinate picture element locations, respectively, and s is the picture element estimate.

$$co(i,j) = \frac{1}{M} \sum_{a=1}^{M} \left(i_a - K(i) \right) \left(j_a - L(j) \right) \tag{6}$$

$$SD = \sigma_{ii} = \sqrt{co(i,j)}$$

Where M is the value of the window picture elements

$$N = F(i) = \frac{1}{M} \sum_{x=1}^{M} i_x; N = F(j) = \frac{1}{M} \sum_{x=1}^{M} j_x;$$
(8)

The resulting imperceptibility is denoted by utilizing any one out of the three measurements, like SSIM [32], MSE [63], and correlation [26], after measuring the window characteristics and hiding the data into the identical window. The SSimInd and MSE expressions yield:

$$MSE = \frac{1}{MXN} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \left| picture_image(x, y) - stego_picture(x, y) \right|^2$$
 (9)

N & M are the length and breadth of the picture accordingly

$$SSimInd = \frac{\left(2\mu_i \mu_j + C_1\right) \left(\sigma_{ij}^2 + C_2\right)}{\left(\mu^2_i + \mu^2_j + C_1\right) \left(\sigma_i^2 + \sigma_j^2 + C_2\right)}$$
(10)

 μ_i and μ_j are the regional mean, σ_i and σ_j are the SD values, σ_{xy} denotes cross-covariance, C_1 and C_2 are constant values

4 Proposed method

The detailed technique, including the input in form of a host image, the information needed to be encoded [1] in the picture, the yield in the form of a stego image and the measurements of imperceptibility are defined in the following subsections. In order to examine the patterns related to the imperceptibility between the two images such as Baboon and Jet from the regular database are used. The correlation, MSE and SSIM is calculated with respect to two respective squared windows with regards to the extracted characteristics, the cover and the stego photos. The trends of the imperceptibility of the Baboon and Jet photos are seen in Figs. 1, 2, 3, 4, 5 and 6 after the hidden data is inserted in a squared window. It is obvious that most of the characteristics are closely correlated



(entropy, contrast, homogeneity, correlation, entropy, SD and energy). The presence of less uncertainty with respect to the collection of features in the imperceptibility association suggests their equal use in the paradigm of machine learning [59].

The imperceptibility patterns for the texture function are summarized in Table 3.

A thorough study of these patterns between the imperceptibility and the image's texture characteristics allotted the researchers to establish the potential difference between them. The machine learning (ML) [65] framework is then equipped for a better embedding.

5 Design of the model

To build the proposed model, the following steps have been taken:

- Partition of the (N X M) cover picture into non-overlapping (C X D) picture element sub-blocks, and (C = D = 8).
- Estimation of the block numbers required to hide the data in relation to the size of the information bits, m.
- Least square window size (SWS) determination against the picture which comprises the appropriate modules. The SWS is determined by way of:

$$SWS = 8 \left| \sqrt{m} \right| X 8 \left| \sqrt{m} \right|$$
 Pixels (11)

 Production of an unrefined data set of squared frames having a 4 pixel NOS scanning capability.

The scale for the collection of information is

$$NOS = \left(\left(\frac{N - SWS}{4} \right) + 1 \right) X \left(\left(\frac{M - SWS}{4} \right) + 1 \right)$$
 (12)

The square window size is SWS and N & M are the length and breadth of the picture

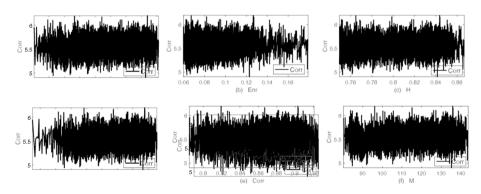


Fig. 1 Connection of the correlation measurement to the texture characteristic energy (E), contrast (D), homogeneity (Homo), correlation (CRel), mean (M), entropy (Ent), standard deviation (SD) for the picture of Baboon



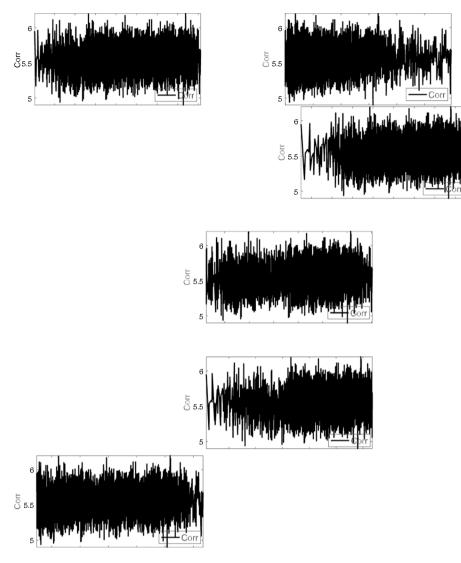


Fig 2 Connection of the MSE measurement to the texture characteristic energy (E), contrast (D), homogeneity (Homo), correlation (CRel), mean (M), entropy (Ent), standard deviation (SD) for the picture of Baboon

6 Preparation of data sets

Prior to ELM training ([18] and research, Fig. 7 shows the schematic structure in the development of the learning data array including the functional entity. For the construction of learning data array, texture attribute extraction, the metric measurement



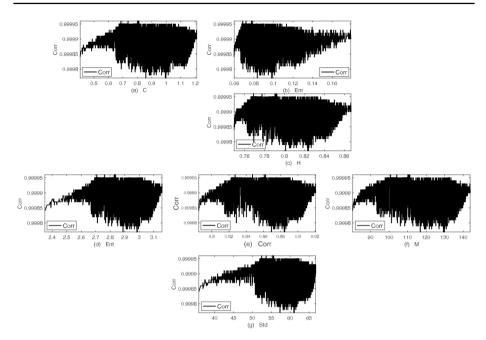


Fig. 3 Connection of the SSIM measurement to the texture characteristic energy (E), contrast (D), homogeneity (Homo), correlation (CRel), mean (M), entropy (Ent), standard deviation (SD) for the picture of Baboon

and the hiding are done. The hiding and the feature extrication process are customary to quickly Wavelet Dependent Embedding Transform. As previously mentioned, for each squared frame for the data set, the message must be inserted in the corresponding square window. Utilizing the hiding procedure and the estimation of the resulting visual

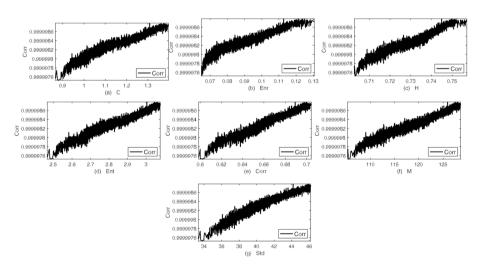


Fig. 4 Connection of the correlation measurement to the texture characteristic energy (E), contrast (D), homogeneity (Homo), correlation (CRel), mean (M), entropy (Ent), standard deviation (SD) for the picture of Baboon



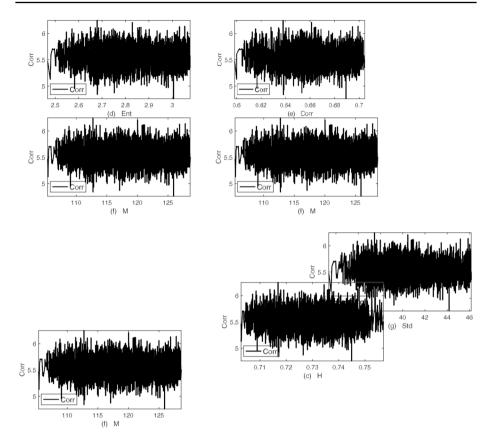


Fig. 5 Connection of the MSE measurement to the texture characteristic energy (E), contrast (D), homogeneity (Homo), correlation (CRel), mean (M), entropy (Ent), standard deviation (SD) for the picture of Baboon

imperceptibility measurements, data is derived from the raw data collection. The following steps will be taken to fulfill this objective:

- 1. The measure is quantized to the nearing even value having the indicator (8, 8) in the appropriate frame for the data bit 1. Otherwise, the odd number is approximated to the closest one.
- 2. For individual sub-section, the wavelet transform is calculated by reversing the wavelet.
- 3. Wavelet is translated into its relevant spatial level entity
- Before the final binary digit of the information is embedded, the embedding process is repeated.
- 5. The related visual metrics are determined for each square window. Correlation, MSE, SSIM, and fusion1 are part of these metrics. The Fusion1 expression yields:

$$Fusion1 = Correlationship X SSIM$$
 (13)



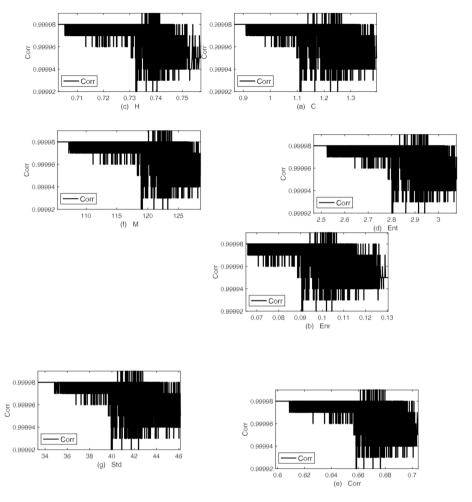


Fig. 6 Connection of the SSIM measurement to the texture characteristic energy (E), contrast (D), homogeneity (Homo), correlation (CRel), mean (M), entropy (Ent), standard deviation (SD) for the picture of Baboon

Table 3 Patterns for the Baboon and Jet photos of the imperceptibility to the texture element

Features	Measu res		
	Correlation	MSE	SSIM
Contrast	+ve	No pattern	-ve
Energy	+ve	No pattern	-ve
Homogeneity	+ve	No pattern	-ve
Correlation	+ve	No pattern	-ve
Mean	+ve	No pattern	-ve
SD	+ve	No pattern	-ve
Entropy	+ve	No pattern	-ve



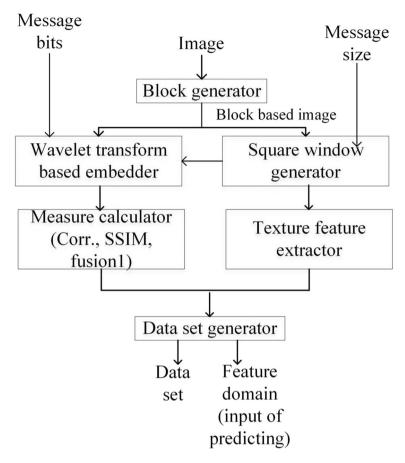


Fig. 7 Data set building and feature framework

Extraction of Texture Feature: Using the following steps, the texture features are extracted:

- For each squared frame whose sub-blocks are utilized to insert the information bits, the co-occurrence table is constructed.
- 2. In a square frame [77], the feature function [(energy (E), contrast (D), homogeneity (Homo), correlation (CRel), mean (M), entropy (Ent), standard deviation (SD)] for the co-occurrence table is determined. The expression in versatility gives

$$Features = (C, Enr, H, Ent, Corr, M, Std)$$
 (14)

Extreme Learning Machine Learning: The matrix structure is defined by

$$Y = (g_{1i}, g_{2i}, \dots, g_{7i}; f_{ij}), \text{ with } i=1,\dots,n$$

where n is the quantity of squared frames, $g_{1i}, g_{2i}, \ldots, g_{7i}$ are the extracted characteristics, f_{ij} is the related performance metrics, and the Correlation, MSE, SSIM, and fusion1 relevant to j = 1, 2, 3, 4.



To predict f_i , a neural network of n' concealed neurons are constructed and instructed on a portion of Y. In addition, before implementing the ELM-based model, the training and the testing stages are undergone by the use of RMSE. We are now shifting our attention to deciding the appropriate percentage of preparation and the possible quantity of neurons.

6.1 RMSE used in learning and checking

The OEPF is a supervised scheme involving the validation of the preparation and checking processes. In the current model, they play a determining role. OEPF is qualified for forecasting the visual imperceptibility (Correlation and SSIM) metrics and the fusion1 measurement here. To assess its predictability efficiency, the RSMEs for the suggested OEPF framework for the instruction and evaluation process are calculated. With each of the similarity metrics, Table 4 summarizes the RSME [38] measurements for the square window. For all the measurements of the training episode and the test episode for separate pictures, the measured RSMEs are perceived in roughly being zero, suggesting the appropriateness of the suggested framework.

6.2 Training building with extreme learning machine

When using ELM, a variety of problems is needed to be tackled. Next, to prevent overfitting for the use of a higher amount of trained variety and undermining the use of a lesser training variety, an acceptable training and testing ratio needs to be correctly calculated. Second, for the design of the network layout, the ELM [44] dosen't supplies the

Table 4 RMSEs with multiple images for the preparation process and research phase

Images	Measurement	Root Mean Square Error (Tutoring phase)	Root Mean Square Error (Assessing phase)
Lena	Correlation	0.0000003241	0.0000003357
	Mean Square Error	0.000237442	0.0002358761
	SSimInd	0.000005871	0.0000058271
	Fusion1	0.0000048943	0.0000087114
Plant	Correlation	0.0000023448	0.0000057449
	Mean Square Error	0.000354762	0.000321158
	SSimInd	0.0000082541	0.0000072345
	Fusion1	0.0020001300	0.0032000000
Baboon	Correlation	0.0000023116	0.0000035981
	Mean Square Error	0.000226973	0.0003122478
	SSimInd	0.0000051324	0.0000039871
	Fusion1	0.0000033128	0.0000031657
Mountain	Correlation	0.0000000286	0.0000000627
	Mean Square Error	0.000231157	0.0003788412
	SSimInd	0.00007782135	0.00008869412
	Fusion1	0.00006877432	0.0000756327



applicant with the correct value of neurons needed to be chosen. In addition, the model's output depends on the number of neurons calculated exactly, and a high (small) quantity of neurons contributes to over (or under) fitting. 50 percent instruction and 50 percent researches were split into the data collection used. Next, at stage five, the number of neurons is raised from 50 to 200. In each scenario, 80 percent for preparation and 20 percent for validation are partitioned into the data collection. Validation [30] is carried out on a component of the training results array because a monitoring data array is inaccessible in the usual device functioning mode. The number of neurons corresponding to the highest validation precision in the secret layer [46] is then chosen. If the optimum quantity of neurons is chosen, the hunt for the right training and testing ratio is conducted by allocating a confirmed testing data array amount.

In order to prevent partiality in the RSME with enlarging test data collection, allotment of a fixed amount of data for assessing is necessary. Afterwards, for the validation in each scenario, the percentage of training data is increased from 10 percent to 60 percent using the affirmation portion comprises of 20 percent of the tutoring data collection. 50 percent of the overall data collection is considered to be best for instruction. The training data collection (percent) of based accuracy standards for the images of Lena, Sails and Baboon is summarized in Table 5. The training data collection percentages of difference in the Corr, MSE, SSIM, and fusion1 estimates in relation with the host and stego pictures are seen in Fig. 8 (Lena, Sails, and Baboon) Fig. 9, 10 and 11.

Table 5 Calculations for the Lena, Sails and Baboon pictures are set by the precision extents of the various training data

Pictures	Tutoring (%)	Sample No.	Correlation	Mean Square Error	Structural Similarity Index Measure	fusion1
Lena	10	504	0.0000000415662	0.00023374	0.0000084457	0.0000083217
	20	1008	0.000000043215	0.00024713	0.0000071662	0.0000075231
	30	1512	0.0000000485231	0.00054217	0.0000075412	0.0000074238
	40	2016	0.000000042317	0.00021478	0.0000074235	0.0000074387
	50	2520	0.000000032578	0.00023180	0.0000078214	0.0000075413
	60	3025	0.000000047812	0.00023551	0.0000074268	0.0000074321
Jet	10	504	0.000000075412	0.00030854	0.0000215873	0.0000087412
	20	1008	0.000000072154	0.00023117	0.0000082357	0.0000082147
	30	1512	0.000000065412	0.00023314	0.0000081245	0.0000082147
	40	2016	0.000000065214	0.00023147	0.0000073542	0.0000075639
	50	2520	0.000000065491	0.00023941	0.0000073364	0.0000078853
	60	3025	0.000000056117	0.00018278	0.0000064654	0.0000065537
Baboon	10	504	0.000000064792	0.00020644	0.0000026758	0.0000021155
	20	1008	0.000000061951	0.00020515	0.0000019249	0.0000019248
	30	1512	0.000000061739	0.00020448	0.0000018580	0.0000019298
	40	2016	0.000000060180	0.00020039	0.0000020036	0.0000020270
	50	2520	0.000000059464	0.00019712	0.0000018142	0.0000018343
	60	3025	0.000000059567	0.00019783	0.0000019505	0.0000019876



Fig. 8 Lena, Sails, and Baboon photos, training data collection percentage based variance of Correlation

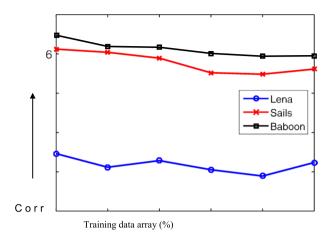


Fig. 9 Lena, Sails, and Baboon images, training data sets the percentage based variance of MSE

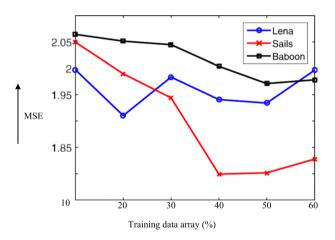


Fig. 10 Lena, Sails, and Baboon images, training data set the percentage based variance of SSIM

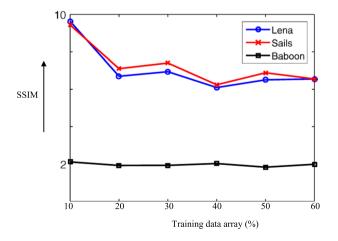
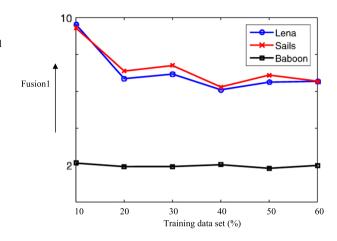




Fig. 11 Training data for the photos of Lena, Sails, and Baboon set the percentage based variance of fusion1



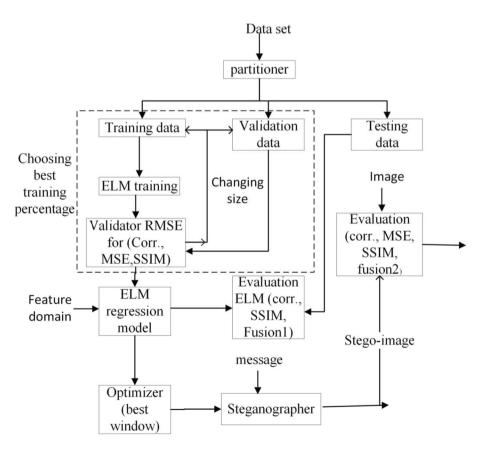


Fig. 12 Basic Framework of the suggested OLPF Approach



Fig. 13 Obtained cover and stego images



7 ELM's architecture and optimization

The structure of the suggested OEPF framework, that is accomplished utilizing the sequences below, is schematically outlined in Fig. 12:

- 1. For instruction as well as validation, the data collection is partitioned into 50 percent for training and 50 percent for checking.
- 2. Focused on the training data array, the ELM regression model is designed to be split into 80% for tutoring and 20% for verification.
- The Extreme Learning Machine regression framework is additionally utilized to anticipate the optimal square frame related to the fusion2 metric.
- 4. In order to produce the stego image, the data hiding process is carried out to embed the hidden information into the defined optimized square frame.

The data is then inserted in each square frame using Extreme Learning Machine training and all visual imperceptibility [12] measurements are calculated using the fusion2 measurement generated by:

$$fusion2 = \frac{CorrXSSIM}{MeanSquareError}$$
 (15)

7.1 Results and discussion

Experiments were performed on a 64-bit Intel1CoreTM computer. The suggested OEPF framework is tested utilizing 24 (512 x 512) pixels of grey scale images. A total of 5040 square windows were acquired in which square windows of size (232 x 232) were utilized. The data size of 100 bytes is used in embedding purposes. Figure 13 displays the photographs checked prior to embedding (the left block of every image) and after embedding (the right block of each picture).

Table 6 Root Mean Square Error measurements obtained using the Extreme Learning Method approach for various pictures

Image	Correlation	Mean Square Error	Structural Similarity Index	fusion2
Lena	0.000000028931	0.00019340	0.0000064897	6.2242
Baboon	0.000000054812	0.00018018	0.0000067782	5.9077
Cameraman	0.000000059464	0.00019712	0.0000018142	6.3427
Fruits	0.000000072910	0.00021492	0.0000897420	6.7471
Mountain	0.000000046185	0.00020671	0.0000038981	6.5776
Sea	0.000000046384	0.00018874	0.000014097	6.1217
Boat	0.000000036993	0.00018259	0.0002314300	5.8925
Tiger	0.000000037995	0.00018965	0.0000006518	6.0393
Leaves	0.000000034447	0.00019519	0.0000087432	6.3871
Tree	0.000000050114	0.00019526	0.0003784400	6.1066
Plant	0.000000074732	0.00017851	0.0000070962	5.7333
Eye	0.000000048013	0.00018282	0.0000011586	5.9634



 $\textbf{Table 7} \hspace{0.2cm} \textbf{Comparability of the OEPF technique measurements with other current methods} \\$

	Proposed OEPF mode	PF model			Mehdi [66]				Andres A. L. Hernandez et al. 2020	Hernandez et	al. 2020	
Image	Mean Square Error	Mean Square Correlation Error	Structural Similarity Index Meas- urement	Fusion2	Mean Square Error	Correlation Structura Similarity Index Me urement	Structural Similarity Index Meas- urement	Fusion2	Mean Square Error	Correlation	Structural Similarity Index Meas- urement	Fusion2
Lena	0.001133	0.999999	0.999989	881.8879 0.001384	0.001384	0.999999	9666660	722.1569	722.1569 0.012939	0.999998	0.999910	77.2759
Baboon	0.001130	0.999999	0.999996	884.8709 0.001388	0.001388	0.999999	0.999994	720.1871	720.1871 0.012329	0.999995	0.999957	81.1051
Cameraman	0.001126	0.999999	0.999997	887.8688	0.001372	0.999999	866666.0	728.1764	0.012512	0.999996	0.999994	79.9213
Fruits	0.001199	0.999999	0.999948	833.4831	0.001266	0.999999	0.999981	789.5758	0.013305	0.999997	0.999937	75.1510
Mountain	0.001205	0.999999	0.999994	829.5649	0.001380	0.999999	0.999995	724.1509	0.011779	0.999997	0.999972	84.8887
Sea	0.001109	0.999999	9666660	901.4161	0.001407	0.999999	0.999995	710.4141	0.012878	0.999997	0.999929	77.6436
Boat	0.001181	0.999999	0.999971	846.2843	0.001277	0.999999	0.999992	782.5134	0.012756	0.999998	0.999992	78.3917
Tiger	0.001064	0.999999	0.999998	939.5825	0.001399	0.999999	0.999994	714.2845	0.011908	0.999998	0.999988	84.0194
Leaves	0.001099	0.999999	0.999995	909.6258	0.001361	0.999999	0.999994	734.2930	0.013244	0.999998	0.999928	75.4968
Tree	0.001080	0.999999	0.999961	925.5033	0.001194	0.999999	0.999982	837.5063	0.010925	0.999997	0.999973	91.5281
Plant	0.001117	0.999999	0.999995	894.6849	0.001380	0.999999	0.999995	724.1515	0.012207	9666660	966666.0	81.9194
Eye	0.001239	0.999999	0.999995	806.5932	0.001377	0.999999	0.999995	726.1570 0.012451	0.012451	166666.0	0.999947	80.3092



For a 50 percent training data collection, Table 6 lists the Root Mean Square Errors [47] of the Extreme Learning Machine projection for the visible imperceptibility measurements for the cover and stego pictures.

The simulated outcomes acquired using the suggested OEPF model is contrasted with those of the current techniques related to the fusion2 measurement. In the context of imperceptibility and fusion2 calculation, that are approximately 31% and 109% respectively, the OEPF methodology is found to outperform the other methods. OEPF is thus seen to be a beneficial steganography method for hiding text in pictures having minimal deformation levels. In comparison, barely a limited tutoring portion of the cover picture [61] features is necessary. OEPF has been shown to be a convenient model for steganography to embed text data in pictures (Table 7).

8 Conclusion

Centered on ELM, to achieve high-performance picture steganography, we suggested an innovative OEPF model. An updated ELM algorithm is used in this method to set up the supervised computational framework to evaluate the optimized hiding picture position with a minimum distortion. The ELM is trained on a part of the image and checked in regression methodology to pick the optimum message hiding spot. It has permitted the supreme outcomes of the expected measurement indicators to be obtained. Training is carried out on the basis of a collection of extracted textures, statistical characteristics and their related visible imperceptibility metrics that use a portion of the graphic. For output enhancement, the learned model is further utilized. To surpass the current innovative frameworks, the proposed model is shown. The exceptional characteristics of the findings encourage that the current framework could be the justification for the progress of the approach for protected image steganography. By integrating a broader variety of functions, it is worth looking at the robustness [78] of the suggested approach against different image processing attacks. It is also good to further improve the model to provide more flexibility related to the exploration by analytically describing the region without regards to the explicit geometrical description. Another worthwhile invention is producing an index based on Pareto efficiency for rating the elucidation. Provided that there is presently no steganography framework that can survive all the steganalysis assaults, freshly producing an image and deleting it after producing the stego image is the safest way to provide protection for the secret images and remove the assault of contrasting the original image with the stego image.

Data availability My manuscript has associated data in a data repository

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

 Alanazi N, Khan E, Gutub A (2020) Efficient security and capacity techniques for Arabic text steganography via engaging Unicode standard encoding. Multimed Tools Appl 80:1403–1431. https://doi. org/10.1007/s11042-020-09667-y



- Alhaddad MJ, Alkinani MH, Atoum MS, Alarood AA (2020) Evolutionary detection accuracy of secret data in audio steganography for securing 5G enabled internet of things. Symmetry 12:2071. https://doi.org/10.3390/sym12122071
- Alia AS, Al-Tamimib MSH, Abbood AA (2020) Secure image steganography through multilevel security. Int J Innov, Creat Change 11(1):80–103
- Al-Nofaie S, Gutub A, Al-Ghamdi M (2019) Enhancing Arabic text steganography for personal usage utilizing pseudo-spaces. J King Saud Univ-Comput Inform Sci. https://doi.org/10.1016/j.jksuci.2019. 06.010
- Amine K (2020) Steganographic techniques classification according to image format, international. Ann Sci 8(1):143–149. https://doi.org/10.21467/ias.8.1.143-149
- Ambika, Biradar RL (2020) Secure medical image steganography through optimal pixel selection by EH-MB pipelined optimization technique. Heal Technol issue 1
- Amsden ND, Chen L (2015) Analysis of Facebook steganographic capabilities. In: International conference on computing, networking and communications (ICNC), Garden Grove, CA, pp 67–71. https://doi.org/10.1109/ICCNC.2015.7069317
- Artiemjew P, Kislak-Malinowska A (2020) Indiscernibility mask key for image steganography. Computers 9(38). https://doi.org/10.3390/computers9020038
- Atee HA, Ahmad R, Noor NM, Rahma AM, Aljeroudi Y (2017) Extreme learning machine based optimal embedding location finder for image steganography. PLoS One 12(2):e0170329. https://doi.org/10.1371/journal.pone.0170329
- Ayub N, Selwal A (2020) An improved image steganography technique using edge based data hiding in DCT domain. J Interdisciplinary Math 23(2):357–366. https://doi.org/10.1080/09720502.2020. 1731949
- AlKhamese AY, Shabana WR, Hanafy IM (2019) Data security in cloud computing using steganography: a review. In: International conference on innovative trends in computer engineering (ITCE), Aswan, Egypt, pp 549–558. https://doi.org/10.1109/ITCE.2019.8646434
- Banik BG, Banik A (2020) Robust, Imperciptibleand blind video steganography using RGB secret, maximum likelihood estimation and Fibonacci encryption. Int J Electronic Sec Digital Forensics 12(2):147–199
- Baziyad M, Rabie T, Kamel I (2020) Toward stronger energy compaction for high capacity dctbased steganography: a region-growing approach. Multimed Tools Appl. https://doi.org/10.1007/ s11042-020-10008-2
- Benedict AG (2019) Improved file security system using multiple image steganography. Int Conf Data Sci Commun (IconDSC):1–5. https://doi.org/10.1109/IconDSC.2019.8816946
- Bikku T, Paturi R (2019) Frequency domain steganography with reversible texture combination. Traitement du Signal 36(1):109–117. https://doi.org/10.18280/ts.360114
- Biswas R, Bandyapadhay SK (2020) Random selection based GA optimization in 2D-DCT domain color image steganography. Multimed Tools Appl 79:7101–7120. https://doi.org/10.1007/ s11042-019-08497-x
- Cogranne R, Giboulot Q, Bas P (2020) Steganography by minimising statistical detectibility: the cases
 of JPEG and color images, IH&MMSec '20: Proceedings of the 2020 ACM Workshop on Information
 Hiding and Multimedia Security, pp 161–167. https://doi.org/10.1145/3369412.3395075
- Chaharlang J, Mosleh M, Rasouli-Heikalabad S (2020) A novel quantum steganography-Steganalysis system for audio signals. Multimed Tools Appl 79:17551–17577. https://doi.org/10.1007/ s11042-020-08694-z
- Cheng J, Chen Z, Yang R (2018) An efficient histogram-preserving steganography based on block. J Image Video Proc. 74. https://doi.org/10.1186/s13640-018-0306-6
- Dhivya N, Banupriya S (2020) Network security with cryptography and steganography. Int J Eng Res Technol (IJERT) ICATCT 8(03)
- Darbani A, Alyan Nezhadi MM, Forghani M (2019) A new steganography method for embedding message in JPEG images, 2019 5th conference on knowledge based engineering and innovation (KBEI), Tehran, Iran, pp 617-621, https://doi.org/10.1109/KBEI.2019.8735054.
- Deshmukh D, Kurundkar G (2020) Video steganography using Sobel edge detection technique. Int J Innovative Technol Exploring Eng 9(5). https://doi.org/10.35940/ijitee.E2856.039520
- Duan X, Guo D, Liu N, Li B, Gou M, Qin AC (2020a) A new high capacity image steganography method combined with image elliptic curve cryptography and deep learning network. IEEE Access 8. https://doi.org/10.1109/ACCESS.2020.2971528
- Duan X, Nao L, Mengxiao G, Yue D, Xie Z, Ma Y, Qin AC (2020b) High capacity image steganography based on improved FC-DenseNet. IEEE Access 8. https://doi.org/10.1109/ACCESS.2020.3024193



- El-Khamy SE, Korany NO, Mohamed AG (2020) A New Fuzzy-DNA Image Encryption and Steganography Technique. IEEE Access 8:148935–148951. https://doi.org/10.1109/ACCESS.2020. 3015687
- El-Khamy SE, Korany NO, El-Sherif MH (2017) Correlation based highly secure image hiding in audio signals using wavelet decomposition and chaotic maps hopping for 5G multimedia communications, XXXIInd general assembly and scientific symposium of the International Union of Radio Science (URSI GASS), pp 1-3. https://doi.org/10.23919/URSIGASS.2017.8105191
- Elmahi MY, Wahbi TM 2019 Multi-level steganography aided with compression, International conference on computer, control, electrical, and electronics engineering (ICCCEEE), Khartoum, Sudan, pp 1-6. https://doi.org/10.1109/ICCCEEE46830.2019.9071188
- Emad E, Safey A, Refaat A, Osama Z, Sayed E, Mohamed E (2018) A secure image steganography algorithm based on least significant bit and integer wavelet transform. J Syst Eng Electron 29(3):639–649. https://doi.org/10.21629/JSEE.2018.03.21
- Eyssa AA, Abdelsamie FE, Abdelnaiem AE (2020) An efficient image steganography approach over wireless communication system. Wireless Pers Commun 110:321–337. https://doi.org/10. 1007/s11277-019-06730-2
- Fu Z, Wang F, Cheng X (2020) The secure steganography for hiding images via GAN. EURASIP J Image Video Process 46. https://doi.org/10.1186/s13640-020-00534-2
- Goljan M, Fridrich JJ, Du R (2001) Distortion-free data embedding for images. In: Moskowitz IS (ed) IH 2001, LNCS 2137. Springer-Verlag, Berlin Heidelberg, pp 27–41
- Gutub A, Al-Ghamdi M (2020) Hiding shares by multimedia image steganography for optimized counting-based secret sharing. Multimed Tools Appl 79:7951–7985. https://doi.org/10.1007/ s11042-019-08427-x
- Horng J, Lee C, Yang S (2019) Image steganography using contrast enhancement technique. 8th Int Conf Innov, Commun Eng (ICICE) Zhengzhou, Henan Province, China 2019:169–173. https://doi. org/10.1109/ICICE49024.2019.9117372
- Jain T (2020) Spatial domain steganography techniques and neural network based Steganalysis with differential storagex. 2020 Int Conf Emerging Trends Inform Technol Eng (ic-ETITE):1–4. https:// doi.org/10.1109/ic-ETITE47903.2020.416
- Jin Z, Yang Y, Chen Y (2020) IAS-CNN: image adaptive Steganalysis via convolutional neural network combined with selection channel. Int J Distributed Sensor Networks 16(3). https://doi.org/10.1177/1550147720911002
- 36. Joshi SV, Bokil AA, Jain NA, Koshti D (2012) Image steganography combination of spatial and frequency domain. Int J Comput Appl 53(5)
- Kar DS, Nakka AM, Katangur AK (2018) A new statistical attack resilient steganography scheme for hiding message in audio files. Int J Inf Comput Secur 10(2/3):276–302. https://doi.org/10.1504/ IJICS.2018.091472
- Karakus S, Avci E (2020) A new image steganography method with optimum pixel similarity for data hiding in medical images. Med Hypoth 139. https://doi.org/10.1016/j.mehy.2020.109691
- Khan S, Irfan MA, Khan K, Khan M, Khan T, Khan RU, Ijaz MF (2020) ACO based variable least significant bits data hiding in edges using IDIBS algorithm. Symmetry 12(5):781. https://doi. org/10.3390/sym12050781
- Koptyra K, Ogiela MR (2020) Distributed steganography in PDF files—secrets hidden in modified pages. Entropy 22(6):600
- Kumar PM, Srinivas K (2019) Real time implementation of speech steganography. 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT). 365-369. https://doi.org/10.1109/ICSSIT46314.2019.8987785
- Priya L, Namitha KNM, Neela Niranjani Vengateshwaran NN (2019) Information hiding using LSB replacement technique and adaptive image fusion. Int J Comput Aided Eng Technol 11(2). https://doi.org/10.1504/IJCAET.2019.098153
- 43. Lee H, Lee HW (2020) New approach on Steganalysis: reverse-engineering based steganography SW analysis, proceedings of the 9th international conference on software and computer applications, pp 212-216. https://doi.org/10.1145/3384544.3384571
- Li D (2018) Automatic detection of cardiovascular disease using deep kernel extreme learning machine. Biomed Eng: Appl, Basis Comm 30(6). https://doi.org/10.4015/S1016237218500382
- Liu HH, Lee CM (2020) High-capacity reversible image steganography based on pixel value ordering. J Image Video Proc 54. https://doi.org/10.1186/s13640-019-0458-z
- Liu Q, Xiang X, Qin J et al (2020) Coverless image steganography based on DenseNet feature mapping. J Image Video Proc. 39:2020. https://doi.org/10.1186/s13640-020-00521-7



- Lopez-Hernandez AA, Martinez-Gonzalez RF, Hernandez-Reyes JA, Palacios-Luengas L, Vazquez-Medina R (2020) A steganography method using neural networks. IEEE Lat Am Trans 18(03):495– 506. https://doi.org/10.1109/TLA.2020.9082720
- Malathi M, Praveen RK, Thandapani (2020) An efficient steganography for data hiding using DWT and IWT. Int J Grid Disribut Comput 13(1):524–531
- Park J, Cho Y (2020) Design and implementation of automated steganography image-detection system for the KakaoTalk instant messenger. Computers 9:103. https://doi.org/10.3390/computers9040103
- Pichardo-Méndez JL, Palacios-Luengas L, Martínez-González RF et al (2020) LSB pseudorandom algorithm for image steganography using skew tent map. Arab J Sci Eng 45:3055–3074. https://doi. org/10.1007/s13369-019-04272-0
- 51. Pramanik S, Singh RP, Ghosh R (2019) A new encrypted method in image steganography, Indonesian journal of electrical engineering and computer. Science 14(3):1412–1419. https://doi.org/10.11591/ijeecs.v13.i3.pp1412-1419
- Pramanik S, Bandyopadhyay SK (2014) Hiding secret message in an image, international journal of innovative science. Eng Technol 1(3):553–559
- Pramanik S, Raja SS (2020) A secured image steganography using genetic algorithm. Advan Math: Sci J 9(7):4533–4541. https://doi.org/10.37418/amsj.9.7.22
- Pramanik S, Singh RP, Ghosh R (2020) Application of bi-orthogonal wavelet transform and genetic algorithm using image steganography. Multimed Tools Appl 79:17463–17482. https://doi.org/10.1007/ s11042-020-08676-1
- Pramanik S, Bandyopadhyay SK (2013) Application of steganography in symmetry cryptography with genetic algorithm. Int J Comput Technol 10(7):1791–1799
- Prasad S, Pal AK (2017) An RGB color image steganography scheme using overlapping block-based pixel value differencing. R Soc Open Sci:4161066. https://doi.org/10.1098/rsos.161066
- Ramya G, Janarthanan PP. Mohanapriya D (2018) Steganography based data hiding for security applications, International Conference on Intelligent Computing and Communication for Smart World (I2C2SW). 131-135. https://doi.org/10.1109/I2C2SW45816.2018.8997153
- Rachmawanto EH, Setiadi DRIM, Sari CA, Andono PN, Farooq O, Pradita N (2019) Spread embedding technique in LSB image steganography based on chaos theory, International seminar on application for Technology of Information and Communication (iSemantic), Semarang, Indonesia, pp 1-6. https://doi.org/10.1109/ISEMANTIC.2019.8884266
- Ruan F, Zhang X, Zhu D et al (2019) Deep learning for real-time image steganalysis: a survey. J Real-Time Image Proc 17:149–160. https://doi.org/10.1007/s11554-019-00915-5
- Rashid M, Arora B (2020) Image steganography using bit differencing technique. Am J Comp Sci Inform Technol 8(2). https://doi.org/10.36648/2349-3917.8.2.51
- Shah PD, Bichkar RS (2020) Genetic algorithm based approach to select suitable cover image for image steganography. Int Conf Emerg Technol (INCET):1–5. https://doi.org/10.1109/INCET49848. 2020.9154032
- Sharma S, Kaur J (2020) Improved image steganography technique using AES cryptography for data security. Int J Advanc Eng Res Dev 7(6)
- Siddiqui GF, Iqbal MZ, Saleem K, Saeed Z, Ahmed A, Hameed IA, Khan MF (2020) A dynamic three-bit image steganography algorithm for medical and e-health systems. IEEE Access 8. https://doi. org/10.1109/ACCESS.2020.3028315
- Sindhu R, Singh P (2020) Information hiding using steganography. Int J Eng AdvancTechnol 9(4). https://doi.org/10.35940/ijeat.D8760.049420
- Shang Y, Jiang S, Ye D, Huang J (2020) Enhancing the security of deep learning steganography via adversarial examples. Mathematics 8(9). https://doi.org/10.3390/math8091446
- Sharifzadeh M, Aloraini M, Schonfeld D (2020) Adaptive batch size image merging steganography and quantized Gaussian image steganography. IEEE Trans Inform Foren Sec 15:867–879. https://doi. org/10.1109/TIFS.2019.2929441
- 67. Stoyanov B, Stoyanov B (2020) BOOST: medical image steganography using nuclear spin generator. Entropy 22:501. https://doi.org/10.3390/e22050501
- Sukumar A, Subramaniyaswamy V, Vijayakumar V et al (2020) A secure multimedia steganography scheme using hybrid transform and support vector machine for cloud-based storage. Multimed Tools Appl 79:10825–10849. https://doi.org/10.1007/s11042-019-08476-2
- Suresh M, Sam S (2020) Optimized interesting region identification for video steganography using fractional gray wolf optimization along with multi-objective cost function. J King Saud Univ-Comput InformSci. https://doi.org/10.1016/j.jksuci.2020.08.007
- Suryawanshi GR, Mali SN (2018) Analysis of effect of spatial domain steganography technique on DCT domain using statistical features for digital images. Int J Appl Eng Res 13(1):634–640



- Tiwari A, Vashistha P, Sharma AK (2020) Information hiding using steganography and LSB technique. Int J Advanc Sci Technol 29(5):3900–3906
- Uday KK, Navya P, Dinakar R, Santhi H (2020) Implementation of quantum steganography based encryption using Grover search. Int J Advanc Sci Technol 29(12s):304–313 Retrieved from http:// sersc.org/journals/index.php/IJAST/article/view/21938
- Verma V, Muttoo SK, Singh VB (2020) Enhanced payload and trade-off for image steganography via a novel pixel digits alteration. Multimed Tools Appl 79:7471–7490. https://doi.org/10.1007/ s11042-019-08283-9
- Xue B, Li X, Guo Z (2015) A new SDCS-based content-adaptive steganography using iterative noiselevel estimation, 2015 international conference on intelligent information hiding and multimedia signal processing (IIH-MSP), Adelaide, pp. 68–71. https://doi.org/10.1109/IIH-MSP.2015.80
- Yang J, Zheng H, Kang X, Shi Y (2020) Approaching optimal embedding in audio steganography with GAN, IEEE international conference on acoustics, speech and signal processing (ICASSP), Barcelona, Spain, pp 2827–2831. https://doi.org/10.1109/ICASSP40776.2020.9054397
- Yeung Y, Lu W, Xue Y, Huang J, Shi Y (2020) Secure binary image steganography with distortion measurement based on prediction. IEEE Trans Circ Syst Video Technol 30(5):1423–1434. https://doi. org/10.1109/TCSVT.2019.2903432
- Younus ZS, Younus GT (2019) Video steganography using knight tour algorithm and LSB method for encrypted data 29, issue 1. https://doi.org/10.1515/jisys-2018-0225
- Zhang Y, Luo X, Guo Y, Qin C, Liu F (2020) Multiple robustness enhancements for image adaptive steganography in Lossy channels. IEEE Trans Circ Syst Video Technol 30(8):2750–2764. https://doi. org/10.1109/TCSVT.2019.2923980
- Song H, Tang G, Sun Y, Gao Z (2019) Security measure for image steganography based on high dimensional KL divergence. Secur Commun Netw. https://doi.org/10.1155/2019/3546367
- Douglas M, Bailey K, Leeney M et al (2018) An overview of steganography techniques applied to the protection of biometric data. Multimed Tools Appl 77:17333–17373. https://doi.org/10.1007/ s11042-017-5308-3
- Kumar V, Kumar D (2018) A modified DWT-based image steganography technique. Multimed Tools Appl 77:13279–13308. https://doi.org/10.1007/s11042-017-4947-8

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

