scientific reports

Check for updates

OPEN

A novel and efficient digital image steganography technique using least significant bit substitution

Shahid Rahman[1], Jamal uddin[2], Hameed Hussain[1], Sabir Shah[1], Abdu Salam[3], Farhan Amin[4]✉, Isabel de la Torre Díez[5]✉, Debora Libertad Ramírez Vargas[6] & Julio César Martínez Espinosa[6]

Steganography is used to hide sensitive types of data including images, audio, text, and videos in an invisible way so that no one can detect it. Image-based steganography is a technique that uses images as a cover media for hiding and transmitting sensitive information over the internet. However, image-based steganography is a challenging task due to transparency, security, computational efficiency, tamper protection, payload, etc. Recently, different image steganography methods have been proposed but most of them have reliability issues. Therefore, to solve this issue, we propose an efficient technique based on the Least Significant Bit (LSB). The LSB substitution method minimizes the error rate in the embedding process and is used to achieve greater reliability. Our proposed image-based steganography algorithm incorporates LSB substitution with Magic Matrix, Multi-Level Encryption Algorithm (MLEA), Secret Key (SK), and transposition, flipping. We performed several experiments and the results show that our proposed technique is efficient and achieves efficient results. We tested a total of 165 different RGB images of various dimensions and sizes of hidden information, using various Quality Assessment Metrics (QAMs); A name of few are; Normalized Cross Correlation (NCC), Image Fidelity (IF), Peak Signal Noise Ratio (PSNR), Root Mean Square Error (RMSE), Quality Index (QI), Correlation Coefficient (CC), Structural Similarity Index (SSIM), Mean Square Error (MSE), Entropy, Contrast, and Homogeneity, Image Histogram (IH). We also conducted a comparative analysis with some existing methods as well as security analysis which showed better results. The achieved result demonstrates significant improvements over the current state-of-the-art methods.

Keywords Image steganography, LSB, Image quality assessment metrics, Histogram analysis, Image, Capacity, Robustness

During communication through different channels, information is more vulnerable to attackers, especially when transmission takes place over the internet[1]. Secure information sharing over communication channels is vital such as any leakage of private information may lead to persistent difficulties. The increasing need for protecting information as being transmitted over communication channels has led to the discovery of various mechanisms[2]. However, no single method can perfectly secure communication over the Internet, as each has its advantages and disadvantages. Steganography is a popular method that involves the embedding of secret data within cover objects like images, videos, audio, and text. The information hidden in such objects is not easily detectable to the naked eye because steganography is a procedure that conceals the secret information within the cover medium so that nobody can know about its existence[3,4]. In the abovementioned cover objects, images have remarkable performance in concealing information that's why it's the most widely used option for steganography. However, the basic research challenge in image steganography is achieving reliable criteria including capacity, computation, robustness, temper protection, and transparency, as shown in Fig. 1. It is worthwhile to define some key concepts relevant to image steganography. The payload; means a cipher text to be embedded within the cover object. Security; means how much the original and stego image is strong against some statistical attacks

[1]Department of Computer Science, University of Buner, Swari 19290, KP, Pakistan. [2]Riphah School of Computing & Innovation, Riphah International University Lahore, Lahore, Pakistan. [3]Department of Computer Science, Abdul Wali Khan University, Mardan 23200, Pakistan. [4]School of Computer Science and Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea. [5]Department of Signal Theory and Communications, University of Valladolid, Valladolid, Spain. [6]Universidad Europea del Atlántico. Isabel Torres 21, Santander 39011, Spain. ✉email: farhanamin10@hotmail.com; isator@uva.es

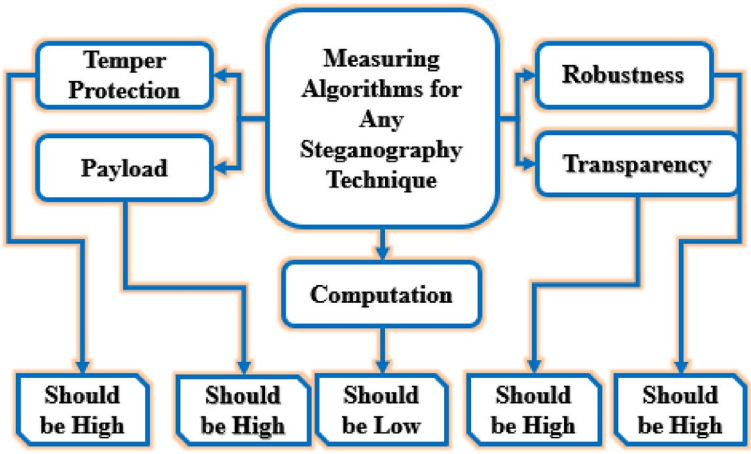

Fig. 1. Image steganography.

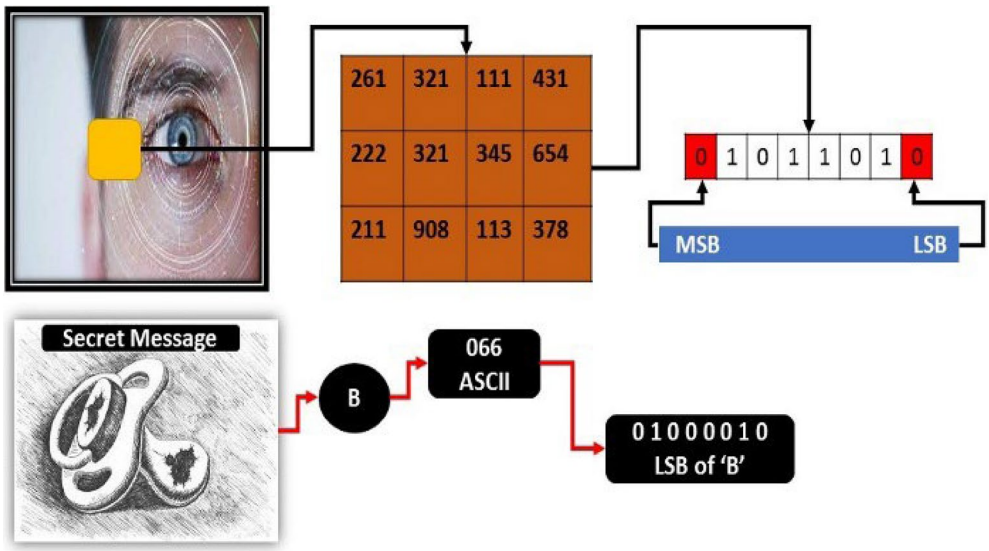

Fig. 2. Least significant bit (LSB).

such are cropping, tempering, scaling, etc. Perception; explains the nature of the cover picture after mounting the mystery message. Temper protection; is a critical issue after securing the secret information within the cover image because if someone tries to extract the message, temper protection; should be high enough to secure the stego image against attackers. The computation shows the time taken by the extracting and embedding process, and it should be minimized so the embedding and extracting process takes the least possible time[5]. The evaluation of existing research works based on these criteria is important as it can lead us to identify the research gap and suggest possible improvements. Most of the recent literature on image steganography is focused on one criterion, but some have broken down the other and every stenographic method needs reliability between them[6]. There is a tradeoff among different reliability criteria of steganography. Suppose we increase the limit of payload, it will degrade the quality of the image and also affect the robustness[7]. The research challenge is two-fold: not to decorate the quality of the cover object and to achieve reliable and best possible values for different parameters of image steganography criteria[8,9]. Furthermore, appropriate object selection and optimum size of image pixels and secret message size are vital.

These methods aim to hide a secret message within an image using a mysterious key. This ensures that the collector cannot decipher the message without having the same key. The algorithm used LSB substitution and value differencing concepts, resulting in a novel image steganography technique. The LSB technique is the most widely used and popular technique for image steganography as shown in Fig. 2. For security, the algorithm uses different concepts such as Magic Matrix and value differencing. Encrypting the message within the cover object it reduces the error rate. The proposed method achieves reliability between the criteria up to acceptable limits[6]. The outcomes show the significance and inspiration of the proposed calculation.

In LSB-based image steganography, the selected image is divided into corresponding channels shown in Fig. 2. Each color intensity is then transformed into a corresponding binary representation. The secret message, represented as 'B', is converted into ASCII values and further coded into dual values. The method uses the Red, Green, Blue (RGB) color model because of its valuable properties. This model uses 24 depths per pixel, and each color has 8 8-bit representations in the range of 0-255[10]. RGB is suitable for embedding more information because having three colors and the combination of these colors can reproduce more possible colors[11]. Considering RGB, we are working with a binary image having a range of 0-255 of eight bits' representations where the left-most bit is LSB and the rightmost bit is considered MSB. In addition, consider the range from 0 to 255, if we change the MSB from 0, its impact is very high because it will change 99% intensity of the color. If we change LSB from one to 1 or 0 to 1 then its impact will be very low say up to 2% change. Therefore, the proposed algorithm used LSB concepts to embed the secret information, and according to the literature, up to 4 LSB bits, can be embedded as secret information which is less susceptible to any naked human eye[5,13]. As mentioned earlier state of art methods are not reliable because based on one or two parameters. So, this effort aims to develop a novel reliable method that ensures reliability. The proposed method was critically analyzed based on distinct perspectives and different formats to fulfill the basic criteria of image steganography. For the balance tradeoff, we used different concepts or facets (i.e. magic matrix, MLEA, Key, LSB up to 4 bit, etc.) to cover all the criteria of image steganography. Our proposed method ensures efficient Image format, dimension, and color that are necessary for spatial, and frequency domains including Machine learning (ML) and Deep learning (DL) models. The key contributions are given below.

- Herein, we design and propose a digital image steganography technique using the least significant bit substitution.
- Our proposed technique incorporates reliable image steganography parameters and appropriate cover image selection for achieving high security.
- Our proposed technique incorporates the random concepts for the selection of the cover image pixels by inserting the message bits to outperform.
- The experimental results show that the proposed method is efficient as compared to the state-of-the-art methods.

The rest of the paper is partitioned into four divisions. Division II presents the connected exploration works, Division III expounds on the proposed strategy, Division IV makes sense of the trial results and conversation and Division V finishes up the research work.

Related work

Steganography using cover objects is a growing field of research that involves hiding secret information within various objects. Recently, various methods of cover steganography have been developed, such as Most Significant Bits and Least Significant Bits (LSB) (MSB-LSB), Pixel Value Differencing (PVD), etc. Respectively every method has its pros and cons, subject to factors such as the implanting process of the hidden message, cover medium, size of the secret data to stand encrypted, and other parameters[7,8]. However, despite ongoing efforts to improve cover steganography, the error rates of these methods have not yet reached acceptable limits. Therefore, evaluating existing research is crucial to making progress and improving the significance and effectiveness of these methods. These limitations provide an opportunity for further advancement. This study focuses on LSB-based cover steganography, which is a commonly used method for concealing confidential data within a cover medium. Table 1 presents a security analysis of related works from the literature, Table 2 presents an acute exploration of different image steganography approaches by assessing algorithms which are the basic criteria of image steganography.

Tables 1 and 2 provide a detailed analysis of various research studies that focus on the security and quality parameters of image steganography. The experimental results section of the studies discusses different concepts for embedding secret messages within cover media using LSB-based methods. Additionally, the studies also emphasize the quality of the stego images. Since there is a tradeoff among the steganography evaluation criteria, some methods in the literature achieve good security but are unable to maintain good levels for other criteria which are crucial for some efficient Stenographic methods. The effectiveness of image steganography depends on the technique used to hide the secret message, as well as the choice of cover objects. Several different approaches have been used to encrypt messages and hide them in cover mediums. In this context, two tables have been created to critically analyze these methods based on quality assessment parameters and basic criteria. The analysis aims to identify the advantages and disadvantages of each existing method. Comparatively, the proposed algorithm has used a novel procedure of embedding the secret message and selecting the appropriate object to tackle the aforementioned issues to improve image steganography.

Proposed stenographic technique

In this section, we explain our proposed technique. In our proposed technique, First, we define certain notations that are utilized in the proposed algorithm. In Equations from 1 to 8, CI and FI represent the Cover image and Flipped image, while the transposed image is denoted as a FT and SM denotes the stealthy message. In addition, Skey and SIm denote the secret key and stego image used in the proposed method detailed explanation is used in Figs. 3 and 4 and Algorithm 1. We will provide more details about the algorithm in the following sections. We follow a series of steps to encode information into an image. First, we flip and transpose the cover image. Subsequently, we divided the transposed image into Red, Green, and Blue channels by Eq.3. The Blue channel is further divided into 4 equal blocks which are represented as BC1, BC2', BC3', and BC4' respectively and finally, the blue channel is shuffled by MGMx (Magic matrix). Then, the differencing values are calculated between the

Techniques [Ref]	Technique used	Quality assessment metrics (QAM)				
		MSE	RMSE	NCC	SSIM	PSNR
[14]	SCImage Steganography (IS)	0.789	0.999	0.998	1	50.04
[15]	Magic LSB IS	0.321	0.765	0.767	0.987	58.76
[16]	Secret Key	0.110	0.100	1	1	59.12
[17]	IS using DWT	0.999	0.977	0.789	0.899	61.11
[18]	Image S using DCT, OTP	0.001	0.112	0.989	0	65.23
[19]	IS based on Chaos theory	0.114	0.312	0.899	0.899	66.87
[20]	IS based on the Color Model	0.012	0.912	0.933	0.899	66.99
[21]	IS based histogram Analysis	0.963	0.678	0.923	0.987	68.98
[22]	IS based on Matching LSB	0.012	0.211	0	0.799	58.47
[23]	Pixel Indicator LSB based IS	0.889	0.999	1	0.788	65.36
[24]	GI and MLE based IS	0.889	0.889	0.989	0.887	69.01
[25]	IS using Modified LSB Approach	0.788	0.776	0.997	0.733	63.22
[26]	IS using an Adaptive pattern-based LSB Approach	1	0.222	0.899	0.897	67.66
[27]	IS Approach for variability based on Flipping LSB	0.978	0.733	0.922	0.945	68.98
[28]	A Secret IS method using Map LSB	0.999	0.876	0.999	0.999	69.99

Table 1. Summary of some previous research works for image steganography using QAM.

Technique used [Ref]	Basic criterion for steganographic techniques				
	Perception	Security	Temper protection	Payload	Computation
Ref[14]	Broke down quality	up to some Confines	Little	6, 8 KB	randomization
Ref[15]	Not dependable	Yes	Reliable	6-10KB	time consuming
Ref[16]	Only on RGB	consistent	Using key	10 kb	No
Ref[17]	Not reliable	trustworthy	Consider as a low ratio	Low payload	Time-consuming
Ref[18]	Cover object some level	commendable	Trustworthy	Squat	Reasonable
Ref[19]	Low image quality	Reasonable	Can be considered reliable	Low	Reasonable
Ref[20]	High	Reasonable	Moderate	High payload	Time is high
Ref[21]	Acceptable limit	High	Easiest for attackers	Low	Low time
Ref[22]	Reasonable	Low	Sensible	Great	High
Ref[23]	Enough	Sensible	Low error ratio	High	Sensible
Ref[24]	Not high	Sensible	Modest	Enough	Sensible
Ref[25]	Due modification	Enough	Sensible	Only up to 4 KB	Reasonable
Ref[26]	Low	Reasonable	High	Low level	Not time consuming
Ref[27]	Workable	High	Acceptable ratio	Low	Reasonable
Ref[28]	practical	High	Reasonable	Reasonable	Reasonable
Ref[29]	Low	Serviceable	High	Low	Low
Ref[30]	High	Serviceable	Low	Reasonable	Low
Ref[31]	Workable	Acceptable limit	High	Reasonable	High

Table 2. Analysis of previous research works grounded on QAM's.

secret message SM and the red channel by CalDiff. We then use a Multi-Level Encryption Algorithm (MLEA), based on CalDiff and a secret key, Skey, to obtain the cipher text, CText. Using this function, we encode the cover information into the shuffled Blue blocks using the secret key. Finally, we combine the three channels - Red, Green, and Blue - and the secret key to achieve the stego-image, SIm. We use MLEA to embed the secret message into the four shuffled blocks of the Blue channel, making it difficult for attackers to extract the information. The magic matrix also adds a layer of security by shuffling the blocks of the Blue channel. The complete process is illustrated in Fig. 5.

Embedding algorithm

Algorithm 1, First, we select the cover image and then flip and transpose it respectively. After dividing the FT image into RGB channels, the Blue channel is again divided into 4 equal blocks for encrypting messages. In addition, a magic matrix is used for shuffling the blue channel for security purposes. While red channel and secret message bits are used for calculating the differing values. Now to generate cipher text, MLEA is applied on bits using a secret key. Finally, using LSB the cipher text will be inserted into Blue channel sub 4 blocks. However,

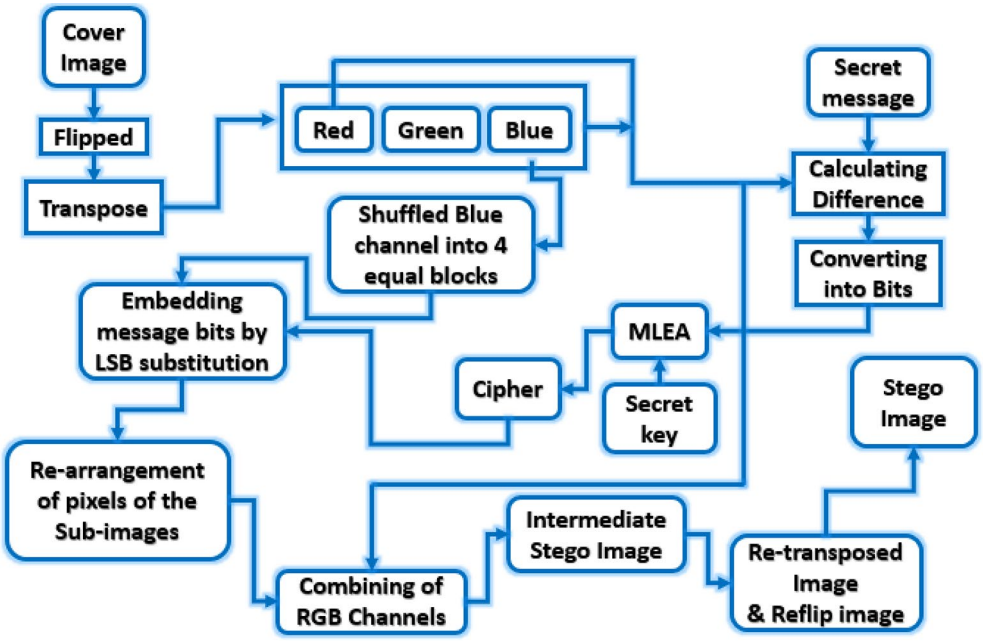

Fig. 3. Proposed method.

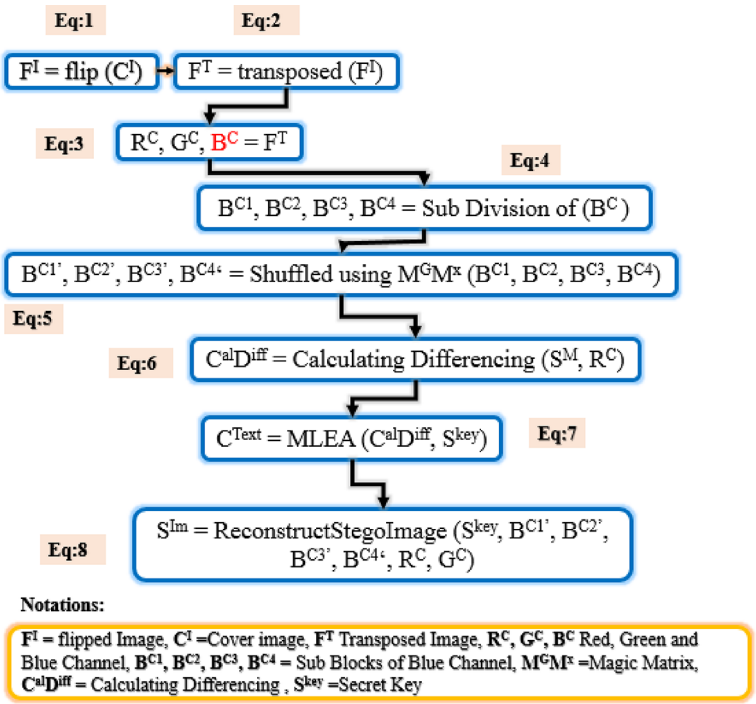

Fig. 4. Mathematical Notations used in Proposed method (Eqs:1-8).

for shuffling the message bits we used magic matrix as a MATLAB function having some unique properties such as rotation, reflection, etc., and having no repeated values as a result. The sum of this matrix row and column, diagonal remains the same and this activity is placed for security purposes. For tamper and robustness, MLEA and Key are utilized which are placed before the encrypted secret message to cover the image. MLEA has some better operations which are usually applied before encoding secret messages into cover images. MLEA used XOR operations for all bits at once which take 8 bits combination and replace 1st four bits with the last bits like a flipping property. So the left circular shift operation is performed on every 8 bits and makes two equal blocks array namely B1 and B2 in this way. IF B1 i == 1, and XOR B2 by 1. Shown in Fig. 5.

Input: C^I, S^M, S^{key}
Output: S^{Im}
Procedure

1. First, initialize the CI, SM, and Skey
2. Cover image CI flipped as FI and then FT as transposed image.
3. Then FT transposed the image converting to RGB channels.
4. After that BC blue channel is separated into sub-locks as a B-C1', C2', C3', and C4' and also shuffled by Magic Matrix MGMx.
5. Calculation between SM and Red channel of differencing values (CalDiff) will performed into bits.
6. MLEA was applied on converted bits of RC and SM and for CText we used Skey.
7. Select 8 bits from the secret data and verify if they meet the specified conditions.
8. **IF**
   a. Embed block one BC1' into the blue channel if the 1st&2nd bits are yes, otherwise doing nothing.
   b. Embed into Blue Channel Block One BC2' if the 3rd & 4th bits are yes, else skip.
   c. If the 5th and 6th bits are set, embed in block one BC2' of the blue channel. If not, do nothing.
   d. If the 7th and 8th bits are set, embed them into block one BC2's blue channel. If not, do not embed.
   e. "If all bits are embedded, proceed to step 9."
   f. Increase the counter value by one: Counter = counter + 1;

   End IF
9. To encrypt the secret message bits in blue channels, you need to repeat step 8 until it is done.
10. First, we need to reorder the sub-image pixels, and after that combine RGB channels.
11. Flip the image horizontally first and then transpose it vertically. to recover the original Stego-Image.

End Procedure

Algorithm. 1. Embedding algorithm.

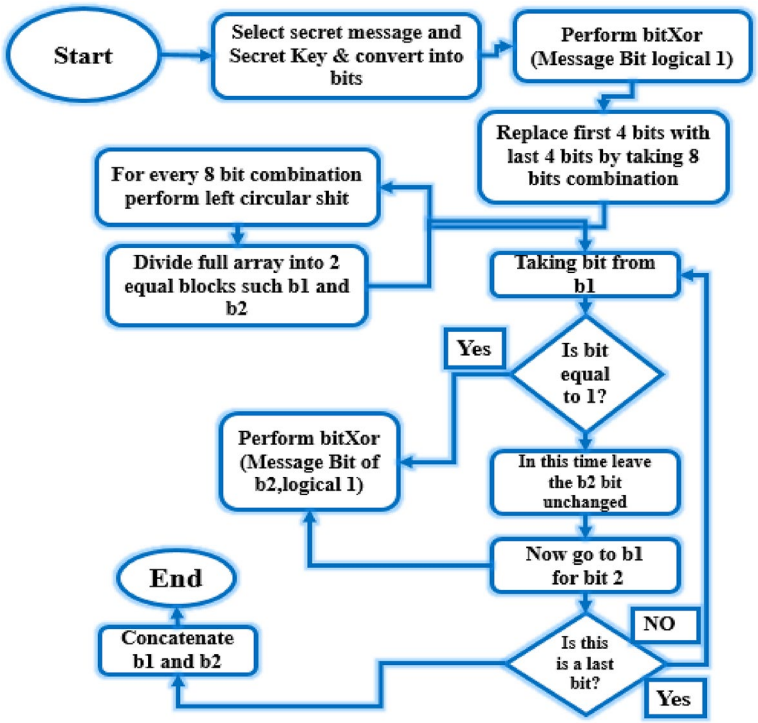

Fig. 5. Mlea for proposed stenographic method.

Extraction algorithm

Decoded message is the opposite of encoded by taking the stego image as input flipped and transposed respectively. For getting the respective red, Green, and Blue channels set flag 1; and check the condition for getting the secret message pixels from equals sub 4 blocks BC1', BC2', BC3', and BC4'of blue channel. The complete steps of the extraction algorithm are presented in Algorithm 2.

Input: S^{Im} Secret Message, S^{key} Secret Key
Output: S^{M} Secret Message

1. Begin by initializing SIm and Skey.
2. To obtain FI, and FT images apply flip and transposed functions.
3. Set Flag 1, when FT image converted into RGB channels.
4. Now Blue channel BC converted as B-C1'-C4', and to set the condition it is shuffled using Magic Matrix MGMx.
5. **IF**
6. Check if Flag equals 1. If so, extract the least significant bit from two pixels of BC1' and set Flag to 2.
7. Check if Flag is equal to 2. If it's true, then extract the least significant bit from two pixels of BC2'. After that, set Flag to 3.
8. Is Flag equal to 3? If yes, extract the least significant bit from two pixels of BC3 and set Flag equal to 4.
9. If Flag is equal to 4, then extract the least significant bit (LSB) from two pixels of BC4 and set Flag equal to 1.
10. Have all the bits been extracted?
11. It seems like step 5 needs to be repeated till the successfully extraction of message bits from blue channel sub blocks. Once the answer is yes, we can proceed to step 6.
12. **End IF**
13. After performing the inverse operations of MLEA, the output is generated based on a secret key Skey.
14. Converting the differencing values (CalDiff) inn to bits which is the calculated values between SM and RC.
15. **End Procedure**

Algorithm. 2. EA (Extraction algorithm).

Fig. 6. Dataset.

Simulation and experimental results

To highlight the significance and importance of this research work, we have conducted a critical analysis of some related works. After critical analysis the results in[12] LSB sub-based[15], , LSB-GLM[21], LSB-RGB[22], LSB-Inverted based[23,25,27], and Robust LSB[28], compared with proposed method. A dataset of 165 different images was downloaded from Image Processing Place (IPP) and the University of Southern California-Signal and Image Processing Institute (USC-SIPI-2022) for proposed method testing[32,33] shown in Fig. 6. The results of the tests indicate that the proposed algorithm successfully embeds secret messages without any suspicious activity, noise, or distortion. More details are provided below.

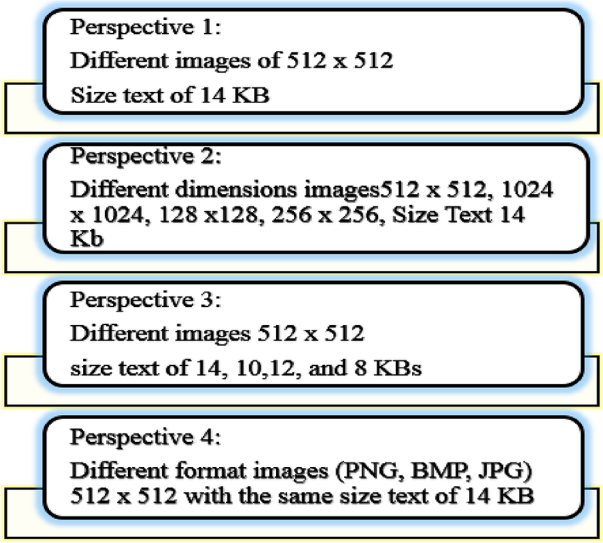

Fig. 7. Multiple viewpoints to analyze Stenographic algorithm's performance.

Img's	M- Size	Resulted PSNR
Baboon	14KB	81.32
Girl1		79.98
Tree		80.98
Lake		82.09
House		80.85
Peppers		78.00
Splash		86.06
Average on 165 images		81.32

Table 3. Persp-1 Images of size 512 × 512 pixels with 14 KB text.

Images	Baboon		Peppers		Lake		House		Splash		Flowers	
Dimensions and Resulted PSNR	128x	69.3	128x	74.2	128x	70.0	128x	71.2	128x	69.2	128x	77
	256x	77.1	256x	79.1	256x	75.2	256x	77.2	256x	73.2	256x	82.1
	512x	78.3	512x	81.3	512x	77.3	512x	82.3	512x	75.3	512x	83.3
	1024x	81.3	1024x	83.9	1024x	85.9	1024x	84.9	1024x	80.9	1024x	87.9
Average of 165 images	Average resulted PSNR on different dimension: D- dimensions D-128 = 71.81, D-256 = 77.31, D-512 = 79.63, and D-1024 = 84.133											

Table 4. Persp-2: Resulted PSNR values on different images using P2.

Performance

The proposed technique is assessed in light of distinct viewpoints with some color images to show the significance and inspiration of this work. So, the basic assessment parameter for analyzing both cover and Stego images is the Peak Signal Noise Ratio (PSNR). PSNR value determines both image quality. If PSNR is > 30dB, the image is high-quality. Equation (9) finds PSNR value[34]. Different analysis perspectives are given in Fig. 7.

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{C}_{\max}{}^{2}}{\mathrm{MSE}}\right) \tag{9}$$

The algorithm underwent thorough analysis, and the results are in Tables 3, 4, 5 and 6 respectively.

The results obtained from different angles demonstrate the superior quality of the proposed algorithm in comparison to existing strategies. A crucial aspect to consider is determining the optimal size of message bits embedded in an image of a particular size to ensure efficient steganography. Hence, before embedding the secret message into the image it is important to compute the message and image pixels to point out the best dimension and format images for which size of the text. Consequently, the proposed strategy is assessed

Images 512 × 512	Baboon		Peppers		Lake		House		Splash		Flowers	
Different Size of Text and Resulted PSNR	8KB	77.2	8KB	69.0	8KB	65.1	8KB	70.1	8KB	89.0	8KB	75.3
	10KB	79.1	10KB	72.1	10KB	69.2	10KB	73.2	10KB	85.2	10KB	81.3
	12KB	80.1	12KB	77.3	12KB	70.2	12KB	74.4	12KB	83.0	12KB	76.2
	14KB	82.2	14KB	81.9	14KB	76.2	14KB	79.6	14KB	77.9	14KB	78.1
Average of 120 images	Average resulted PSNR on different size of text: ST (Size text) ST-8 = 74.28, ST-10 = 76.68, ST-12 = 7686, and ST-14 = 79.81											

Table 5. Persp-3: Resulted PSNR on 512 × 512 embedded 14, 10, 12, and 8 KB size of text.

Images	Message Size	PSNR values			
		PNG	TIFF	BMP	JPG
Baboon	14KB	79.321	73.123	69.212	82.212
Girl		81.223	77.765	80.121	82.918
Peppers		86.189	71.554	68.876	82.887
Lake		83.098	79.986	75.097	82.643
House		80.854	79.654	87.001	80.087
Flowers		84.001	87.009	87.091	85.098
Splash		86.065	87.112	83.087	86.076
An average of 150 images		82.82	79.33	78.78	83.00

Table 6. Persp-4: Resulted PSNR on (PNG, BMP, JPG, D-512 × 512) using 14 KB text.

Image	Comparison with some existing methods						
	Baboon	Flowers	Peppers	Lake	House	Tree	Splash
GLM [21]	78.34	79.09	74.00	79.86	69.00	77.32	80.22
Secure RGB [22]	77.99	81.00	75.00	81.31	78.98	82.10	80.00
Inverted LSB [23]	70.91	88.00	71.98	79.99	79.00	80.00	82.07
LSB IMST [24]	73.04	80.00	80.32	82.98	83.09	84.32	83.32
IMST [27]	76.99	84.02	83.87	80.09	80.87	82.98	82.97
Robust ST [28]	77.32	78.43	79.22	76.66	78.32	79.97	79.97
Proposed method	79.34	87.98	85.01	84.01	83.89	84.98	88.12

Table 7. PSNR values-based state-of-the-art methods with proposed method.

utilizing different viewpoints. It is also important as a principle perspective to distinguish which cover object is the most appropriate for encrypting the secret messages to pledge secure transmission over the web. To solve this issue, that's why the proposed work has tried to utilize different image formats, including PNG, JPG, and BMP, dimensions, and viewpoints in light of PSNR values to show the method performance. Using various QAMs the proposed work is comparatively analyzed for security purposes in the following section.

Analysis of the proposed steganography technique

To show the viability and significance of the proposed work against different facts, such as trimming and scaling, it was tested using several quality assessment metrics outlined in this section. The results indicate significant improvements and better performance of the proposed algorithm.

Performance analysis

This section provides a detailed explanation of the results obtained from the suggested algorithm. These results are also compared with previous research studies based on metrics such as MSE, RMSE, NCC, SSIM, and PSNR. Table 7; Fig. 8 present the experimental outcomes of the proposed technique based on these assessment metrics, demonstrating the enhancements made by this method. Here are some important assessment metrics that need to be elaborated for the experimental results of any steganographic method. So, to measure the difference between both input and resulting images, Root Mean Square Error (RMSE) is usually used. One more significant quality metric that is utilized to examine the connection between an input and results from media is Normalized Cross Correlation (NCC). If the value of the NCC is equal to 1, then both cover and stego images are considered

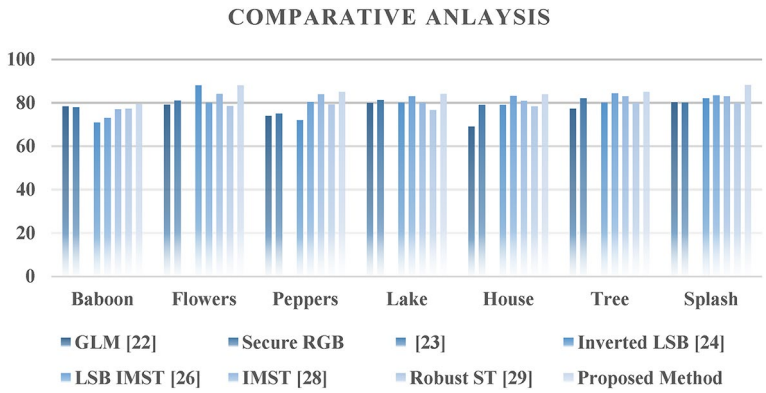

Fig. 8. Comparison with State of the art models.

identical. On the other hand, if this value becomes 0, it indicates that there is a complete difference between both images. The Structural Similarity Index (SSIM) is a significant quality metric used to evaluate the quality of cover and stego images. It consists of three parts followed by Luminance, Contrast, and Structural and it determines the quality of the image. An image will be considered a quality image if the value of SSIM is 1 while 1 < presents the difference between the cover and stego image. Equation 13 elaborates on the formulas for each segment. If measuring the contrast between both cover and stego image Mean Squared Error (MSE) is usually used and both images will be considered if the value of MSE is 0. To obtain quality and robust images MSE value should be low[35,36] Formulas of each are elaborated in Eqs. 10–13.

$$\mathrm{RMSE} = \sqrt{\left(\frac{1}{\mathrm{N}}\right)\sum{}_{\mathrm{x}=1}^{\mathrm{N}}(\mathrm{C_x} - \mathrm{S_x})^2} \tag{10}$$

$$\mathrm{RMSE} = \sqrt{\left(\frac{1}{\mathrm{N}}\right)\sum{}_{\mathrm{x}=1}^{\mathrm{N}}(\mathrm{C_x} - \mathrm{S_x})^2} \tag{11}$$

$$\mathrm{NCC} = \frac{\sum_{\mathrm{x}=1}^{\mathrm{M}}\sum_{\mathrm{y}=1}^{\mathrm{N}}(\mathrm{S}(\mathrm{x},\mathrm{y}) * \mathrm{C}(\mathrm{x},\mathrm{y}))}{\sum_{\mathrm{x}=1}^{\mathrm{M}}\sum_{\mathrm{y}=1}^{\mathrm{N}}\mathrm{S}(\mathrm{x},\mathrm{y})^2} \tag{12}$$

$$\mathrm{SSIM}(\mathrm{X},\mathrm{Y}) = \frac{\left(2\mu_{\mathrm{x}}\mu_{\mathrm{y}} + \mathrm{C}_1\right)\left(2\sigma_{\mathrm{xy}} + \mathrm{C}_2\right)}{\left(\mu_{\mathrm{x}}{}^2 + \mu_{\mathrm{y}}{}^2 + \mathrm{C}_1\right)\left(\sigma_{\mathrm{x}}{}^2 + \sigma_{\mathrm{y}}{}^2 + \mathrm{C}_2\right)} \tag{13}$$

This section elaborated on the results of the proposed method using some security measures and QAMs to ensure the work's importance and resistance. Before continuing to the outcomes, making sense of these concepts is significant and explained below.

The Relationship Coefficient (CC) is utilized to track down the linearity (degree and heading) of two irregular factors. It assumes an imperative part because of its estimation qualities[37]. If the CC value is equal to 1, the two factors are supposed to be somewhat similar or firmly related. Equation 14 shows the formula for CC.

$$I = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sum_i \sqrt{\sum_i (x_i - x_m)^2}\sqrt{\sum_i (y_i - y_m)^2}} \tag{14}$$

Image fidelity (IF) is also a more significant metric that tracks down the picture quality. Equation 15 shows the formula for IF calculation where P and S address the Cover and Stego picture, and "I" and "j" address beginning and finishing values.

$$IF = 1 - \frac{\sum_{i,j}(P(i,j) - S(i,j))^2}{\sum_{i,j}(P(i,j) \times S(i,j))} \tag{15}$$

To measure the quality of stego images Quality Index is also used on different perspective. Equation 16 elaborates the detailed formula that how to calculate the stego images. T and H represent both stego and cover images and n shows the pixel quantity in an image while the value scope of QI is in the range of -1 to 1. Both input and resulting images will be identical if the value is = 1, otherwise, the images will show the difference between the images.

$$Q = \frac{4\sigma_{HT} H' T'}{\left(\sigma_{H+}^2 \sigma_T^2\right)\left(H'^2 + T'^2\right)}$$

Image	Resulted Values		
	Correlation coefficient	IF	QI
Lake	0.999	0.999	1
Flowers	0.999	1	1
Peppers	1	1	0.999
Baboon	0.998	0.998	1
Splash	0.999	0.999	1
Tree	0.999	0.999	0.998
House	0.998	1	1

Table 8. Cumulative QAM results of the Proposed Method.

Analysis Parameter	Images	Effect on red, green, and blue statistical analysis					
		Cover Image			Stego Image		
		Red	Green	Blue	Red	Green	Blue
Contrast	Baboon	2.666 1e+03	2.4447e+03	1.23478e+03	2.666 1e+03	2.4447e+03	1.23478e+03
	Girl	7.2324e+08	8.2721e+05	7.3514e+08	7.2324e+08	8.2721e+05	7.3514e+08
	Peppers	2.5134e+08	2.7042e+08	8.1540e+06	2.5134e+08	2.7042e+08	8.1440e+07
Homogeneity	Baboon	1.2334e+06	1.3234+07	2.7244e+05	1.2334e+06	1.3234+07	2.7244e+05
	Girl	7.3224e+07	7.2440e+08	5.4152e+08	7.3314e+07	7.2440e+08	5.4152e+08
	Peppers	1.7453e+07	1.3462e+07	2.3638e+09	1.7453e+07	1.4462e+07	2.3638e+09
Entropy	Baboon	6.6632	5.4632	6.5345	6.6632	5.4632	6.5345
	Girl	8.5857	8.6634	5.1457	8.5857	8.6634	5.1457
	Peppers	7.4865	9.3251	7.3735	7.4865	9.3251	7.3735

Table 9. Effect analysis of red, green, and blue channels while embedding message bits.

$$\sigma_H^2 = \frac{1}{N-1}\sum_{i=1}^{N}\left(H_i - H'\right)^2$$
$$H' = \frac{1}{N}\sum_{i=1}^{N}H_i - T = \frac{1}{N}\sum_{i=1}^{N}T_i$$
$$\sigma_H^2 = \frac{1}{N-1}\sum_{i=1}^{N}\left(T_i - T'\right)^2 \tag{16}$$

Contrast analysis is widely used to quantify the intensity dissimilarity between pixels and their neighbors throughout the image. It also helps in the main texture area of the image and can be calculated as under in eq. 17.

$$Q = \frac{4\sigma_{HT}H'T'}{\left(\sigma_{H+}^2\sigma_T^2\right)\left(H'^2 + T'^2\right)} \tag{17}$$

To measure the security of any steganographic method Information Entropy (IE) is usually used. Suppose e1…. em, as m shows the measure of potential components and from P(e)… P(em) will be considered as a probability for thesis components. The formula in eq. 18 elaborated on the calculation of Entropy. In view of the recurrence of the image, the condition is the assessment of the typical number of pieces expected to implant a series of pieces.

$$\sigma_H^2 = \frac{1}{N-1}\sum_{i=1}^{N}\left(H_i - H'\right)^2 \tag{18}$$

For gray level diagonal and co-occurrences, Homogeneity (H) is widely used to find the closest level of element distribution[38,39]. Eq.19 shows the whole calculation. So i,j show lists of line and segment numbers, and p (i, j) represent pixel's values ith column and jth section.

$$H' = \frac{1}{N}\sum_{i=1}^{N}H_i - T = \frac{1}{N}\sum_{i=1}^{N}T_i \tag{19}$$

The proposed calculation has been demonstrated critical in light of observational outcomes from QAMs. The investigation depends on differentiation, homogeneity, and entropy to recognize the specific distinctions between the embedded medium's relating channels (red, green, blue) after embedding the cipher message shown in Tables 8 and 9.

The results of our proposed method were better than those of the techniques described in[27,29]. According to Table 10, our method has a relatively high hiding capacity compared to existing techniques, with a normal PSNR. The average bpp value of our method for more than eight test images is 5.025.

Security analysis

The section expounded on the security of the proposed technique has been talked about concerning Pixel Difference Histogram (PDH), and RS steganalysis. The PDH and RS analysis is the normal and powerful measurable steganalysis to recognize the presence of the restricted data in the stego-picture for the LSB based techniques[40]. The LSB replacement methods experience the ill effects of RS investigation and PVD methods experience the ill effects of PDH investigation. The proposed method utilizes ideas like adjusted LSB replacement, also value differencing, so both RS investigation and PDH should dissect it. Here, RS steganalysis is used to break down the effectiveness of the extended procedure[41]. Consequently, the RS plot applied more than 500 implanted pictures to check or hack the secret-covered picture. So, both RS and PDH considerations is proceeded according to the structure talked about in[42,43]. RS analysis of two standard images Lena, baboon, Pepper, and house are presented in Fig. 9a-c respectively. The x-axis and y-axis describe the ratio of the concealing capability and ratio of the singular and regular groups. To plot four arcs/curves, four factors S-m, Sm, R-m, Rm as described in[41,44,45]. RS analysis identifies the presence of implanted bits based on the condition if R_m-S_m < R-2^m-S. While the steganographic-based method is unnoticeable by RS analysis if $S_m \approx S_{-m} < R_m \approx R_{-m}$.

Figure 10a, b indicate that the condition $Sm \approx S - m < Rm \approx R - m$ holds because the curves of R − m and Rm are positioned above the curves of R − m and Rm, while the curves of S − m and Sm are equal in length to each other. Additionally, the curves of R − m and Rm are also of equal length. This leads to the conclusion that the intended method is highly resistant in terms of RS analysis. To validate the effectiveness of the proposed method, we need to use the concepts of LSB and value differencing to examine its success through PDH analysis and RS analysis. To show the difference on both axis's for frequency and pixel difference PDH graph is used. The PDH analysis of some standard images namely Lena, pepper images presented in Fig. 10a,b respectively. The dotted and solid lines indicate the PDH analysis of both stego and cover image respectively. It very well may be seen that the step impact or crisscross presence is tiniest. While the arcs/curve show the smooth nature of the stego image. Hence, it very well may be presumed that the proposed strategy is pitifully impervious to PDH check.

Proposed method histogram analysis

The proposed method also conducted histogram analysis using some images. As we know that histogram is utilized to decide the specific frequencies of every pixel in the picture and to uncover point-by-point contrasts between the cover and stego pictures. We fundamentally assess the proposed technique by breaking down the histograms of a few pictures, including Strawberry, Peppers, Mandrill, and House. The outcomes exhibit the viability of the proposed work, as shown in Fig. 11[46].

Conclusion and future work

In this research, we propose a secret key-based LSB substitution image steganography technique. Our proposed technique incorporates reliable image steganography parameters and appropriate cover image selection for achieving high security. Our proposed method utilized some random concepts for the selection of the cover image pixels for inserting the message bits to get outperformance. To demonstrate the effectiveness and enactment, we performed experimentation. The experimental results show that the proposed method is critically analyzed based on various steganography and different statistical metrics. The achieved results show our proposed method performs in terms of various QAMs such as MSE, RMSE, SSIM, NCC, PSNR, correlation coefficient, image fidelity, quality index, contrast, entropy, and homogeneity. Moreover, it has been confirmed that the given method weakly endures PDH analysis and very strongly endures RS analysis. In addition, the empirical results show a high level of robustness, acceptable limits of payload, imperceptibility, and resistance against attacks scaling, cropping, tempering, etc. Time complexity, limited payload, and RGB color model are demerits of the work. Combining image steganography with cryptography to achieve a better steganography scheme, may be investigated as future work. In the spatial domain, compression methods such as Huffman code,

Image 512 × 512	Comparison results of the proposed and existing methods								
	Kamil, S [27]			Ray [25]			Proposed Method		
	bpp	Hiding Capacity	PSNR	bpp	Hiding Capacity	PSNR	bpp	Hiding Capacity	PSNR
Baboon	928,000	3.21	43.32	881,383	3.01	44.59	1,152,683	4.21	56.12
Girl	821,344	3.22	43.18	851,343	3.22	44.21	1,032,421	4.12	55.01
Peppers	946,722	3.11	43.18	851,348	3.12	44.33	1,187,381	4.21	51.32
Lake	884,783	3.82	44.18	811,211	2.92	44.33	8,513,432	4.12	52.11
House	883,247	3.21	43.18	741,311	2.89	44.23	8,513,483	4.12	50.31
Tree	928,374	3.41	44.18	844,665	2.76	43.88	1,188,778	4.22	50.11
Lena	851,343	3.51	43.38	854,654	3.20	44.89	1,109,887	4.22	59.11
Splash	851,348	3.51	43.38	745,334	2.98	44.01	1,176,767	4.22	50.32
Average	886,895	3.37	43.49	764,138	3.01	44.30	12,459,962	4.31	52.17

Table 10. Comparison of proposed method with state-of-the-art methods.

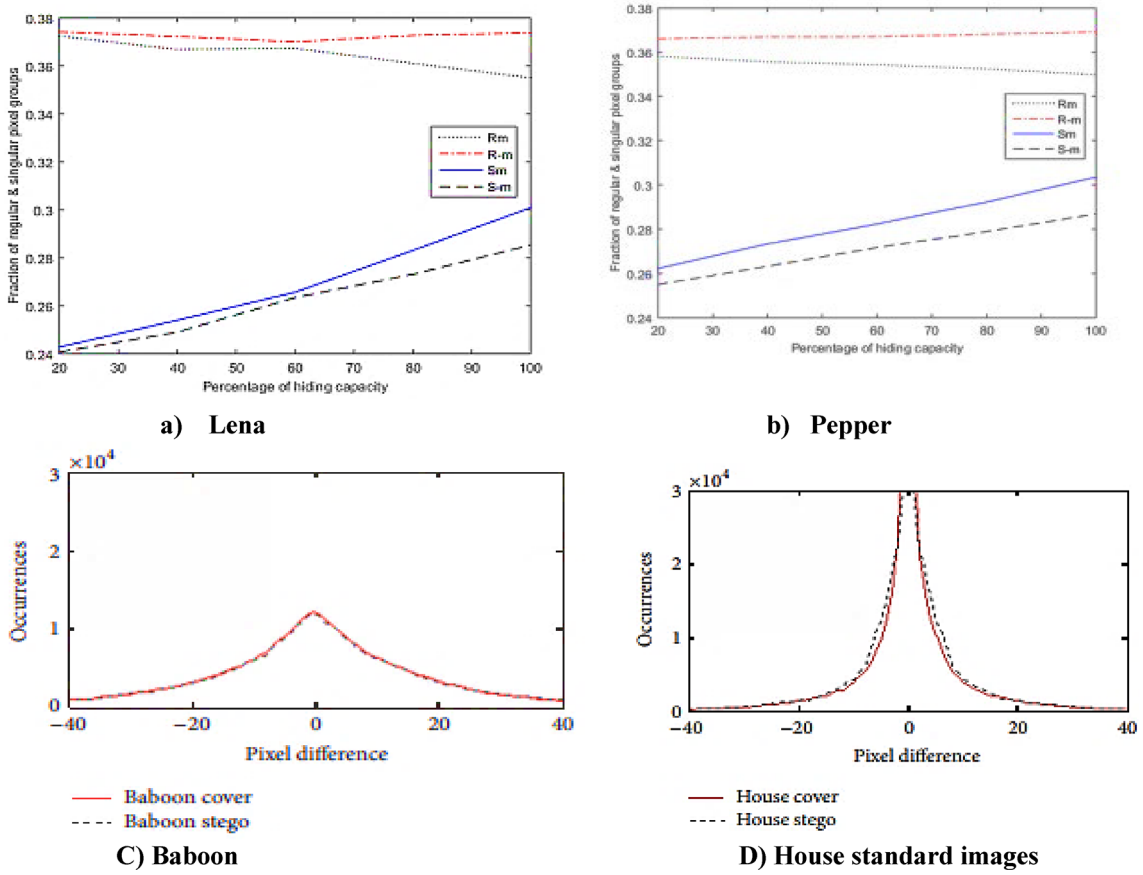

Fig. 9. RS Plot of Lena, pepper, Baboon, and House standard images.

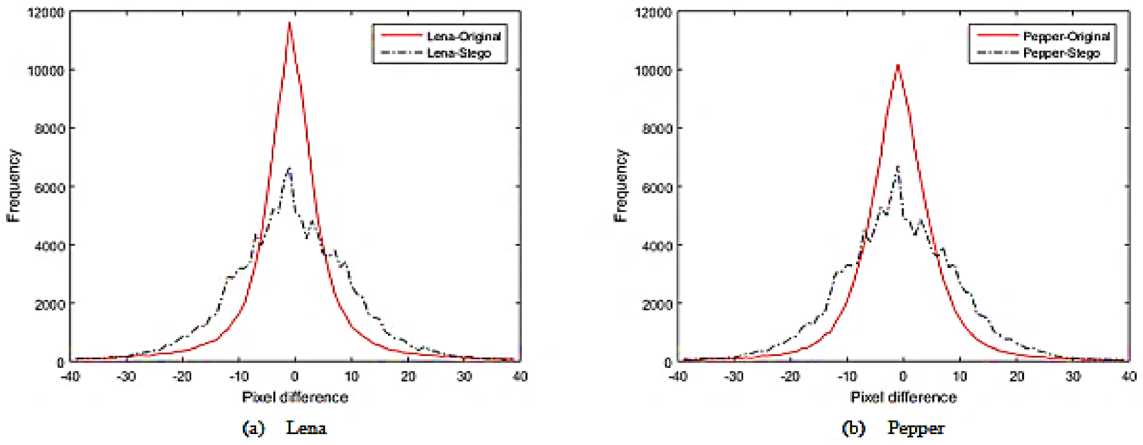

Fig. 10. PDH Plot of Two standard images namely Lena and Pepper.

HSI model, and acronoment method are also best for future work. Also, some machine learning techniques such as different deep learning architecture or unsupervised learning may be utilized for obtaining efficient steganography for secure communication between the sender and the receiver. Now GAN GAN-based models are also can be used for better and secure communication.

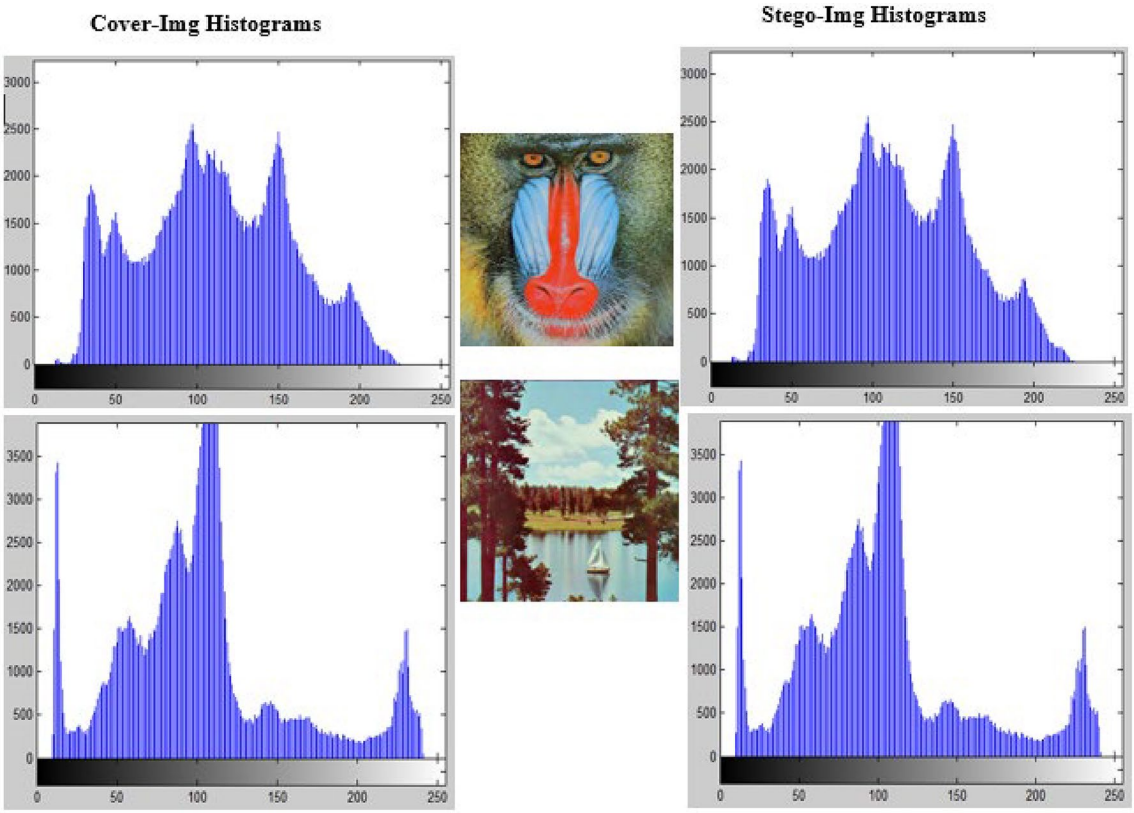

Fig. 11. Histogram analysis of various cover and stego images.

Data availability

Data is provided within the manuscript or supplementary information files.

Received: 7 October 2024; Accepted: 11 December 2024
Published online: 02 January 2025

References

1. Subramanian, N., Elharrouss, O., Al-Maadeed, S. & Bouridane, A. Image steganography: A review of the recent advances. *IEEE access*. **9**, 23409–23423 (2023).
2. Hemeida, F., Alexan, W. & Mamdouh, S. A comparative study of audio steganography schemes. *Int. J. Comput. Digit. Syst.* **10**, 555–562 (2021).
3. Lakshmi Sirisha, B. & Chandra Mohan, B. Review on spatial domain image steganography techniques. *J. Discrete Math. Sci. Crypt.* **24** (6), 1873–1883 (2021).
4. Singh, K. U. A survey on image steganography techniques. *Int. J. Comput. Appl.*, **97**(18). (2014).
5. Menon, N. A survey on image steganography. In *2017 International Conference on Technological Advancements in Power and Energy (TAP Energy)* (pp. 1–5). IEEE. (2017), December.
6. Kaur, S., Singh, S., Kaur, M. & Lee, H. N. A Systematic Review of Computational Image Steganography Approaches. *Arch. Comput. Methods Eng.*, 1–23. (2022).
7. Ejidokun, T., Omitola, O. O., Nnamah, I. & Adeniji, K. Implementation and Comparative Analysis of Variants of LSB Stenographic Method. In *2022 30th Southern African Universities Power Engineering Conference (SAUPEC)* (pp. 1–4). IEEE. (2022), January.
8. Ansari, A. S., Mohammadi, M. S. & Parvez, M. T. A multiple-format steganography algorithm for color images. *IEEE Access.* **8**, 83926–83939 (2020).
9. Bhavani, Y., Kamakshi, P., Kavya Sri, E. & Sindhu Sai, Y. A Survey on Image Steganography Techniques Using Least Significant Bit. In Intelligent Data Communication Technologies and Internet of Things (281–290). Springer, Singapore. (2022).
10. Sahu, A. K. & Gutub, A. Improving grayscale steganography to protect personal information disclosure within hotel services. *Multimedia Tools Appl.*, 1–21. (2022).
11. Hussain, M. & Hussain, M. A survey of image steganography techniques. (2013).
12. Mohamed, M. M., Ghoniemy, S. & Ghali, N. I. A Survey on Image Data Hiding Techniques. *Int. J. Intell. Comput. Inform. Sci.*, 1–25. (2022).
13. Nabi, S. T., Kumar, M., Singh, P., Aggarwal, N. & Kumar, K. A comprehensive survey of image and video forgery techniques: variants, challenges, and future directions. *Multimedia Syst.*, 1–54. (2022).
14. Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z. & Qureshi, R. J. A secure cyclic Stenographic technique for color images using randomization. *arXiv preprint arXiv:1502.07808*. (2015).
15. Alanzy, M., Alomrani, R., Alqarni, B. & Almutairi, S. Image steganography using LSB and hybrid encryption algorithms. *Appl. Sci.* **13** (21), 11771 (2023).
16. Karim, S. M., Rahman, M. S. & Hossain, M. I. A new approach for LSB based image steganography using secret key. In *14th international conference on computer and information technology (ICCIT 2011)* (pp. 286–291). IEEE. (2011), December.

17. Baby, D., Thomas, J., Augustine, G., George, E. & Michael, N. R. A novel DWT based image securing method using steganography. *Procedia Comput. Sci.* **46**, 612–618 (2015).
18. Rachmawanto, E. H. & Sari, C. A. Secure image steganography algorithm based on dct with otp encryption. *J. Appl. Intell. Syst.* **2** (1), 1–11 (2017).
19. Naima, S. et al. Secure and imperceptible frequency-based watermarking for medical images. *Circuits, Systems, and Signal Processing*, 1–22. (2024).
20. Çataltaş, Ö. & Tütüncü, K. Comparison of LSB image steganography technique in different color spaces. In *2017 international artificial intelligence and data processing symposium (IDAP)* (pp. 1–6). IEEE. (2017), September.
21. Huang, R., Lian, C., Dai, Z., Li, Z. & Ma, Z. A novel hybrid image synthesis-mapping framework for steganography without embedding. *IEEE Access*. (2023).
22. Dhar, S. & Sahu, A. K. Digital to quantum watermarking: A journey from past to present and into the future. *Comput. Sci. Rev.* **54**, 100679 (2024).
23. Dhar, P. K., Kaium, A. & Shimamura, T. Image steganography based on modified lsb substitution method and data mapping. *Int. J. Comput. Sci. Netw. Secur.* **18** (3), 155–160 (2018).
24. Gutub, A. A. A. Pixel indicator technique for RGB image steganography. *J. Emerg. Technol. web Intell.* **2** (1), 56–64 (2010).
25. Ray, A. M., Pramanik, S., Das, B. & Khanna, A. Hybrid cryptography and steganography method to provide safe data transmission in IoT. In *International Conference on Data Analytics & Management* (pp. 513–524). Singapore: Springer Nature Singapore., June. (2023).
26. Sahu, A. K. & Sahu, M. Digital image steganography and steganalysis: A journey of the past three decades. *Open. Comput. Sci.* **10** (1), 296–342 (2020).
27. Sharma, D. & Prabha, C. Hybrid security of EMI using edge-based steganography and three-layered cryptography. In *Appl, Data Sci. Smart Syst.* (pp. 278–290). CRC.
28. Venkata Krishna, G. P. C. & Vivekananda Reddy, D. Machine learning-enhanced hybrid cryptography and image steganography algorithm for securing cloud data. *J. Intell. Fuzzy Syst.*, (Preprint), 1–11. (2024).
29. Almazaydeh, L. Secure RGB image steganography based on modified LSB substitution. *Int. J. Embed. Syst.* **12** (4), 453–457 (2020).
30. Rustad, S., Syukur, A. & Andono, P. N. Inverted LSB image steganography using adaptive pattern to improve imperceptibility. *Journal of King Saud University-Computer and Information Sciences*. (2021).
31. Kamil, S., Abdullah, S. N. H. S., Hasan, M. K. & Bohani, F. A. Enhanced flipping technique to reduce variability in image steganography. *IEEE Access*. **9**, 168981–168998 (2021).
32. ALabaichi, A., Al-Dabbas, M. A., A. A., K. & Salih, A. Image steganography using least significant bit and secret map techniques. *International journal of electrical & computer engineering (2088–8708)*, *10*(1). (2020).
33. Liu, X. et al. Robust coverless steganography using limited mapping images. *J. King Saud University-Computer and Information Sci.*. (2022).
34. Naz, M. T. S. A. & Zade, S. *A new approach for image steganography using* (Inter Pixel Value Difference and Quantized Range Table Method, 2022).
35. Xu, Y., Mou, C., Hu, Y., Xie, J. & Zhang, J. Robust invertible image steganography. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 7875–7884). (2022).
36. https://sipi.usc.edu/database
37. https://www.imageprocessingplace.com/root_files_V3/image_databases.htm
38. Alatiyyat, B. F. & Narmatha, C. Survey on image steganography techniques. In *2022 2nd International Conference on Computing and Information Technology (ICCIT)* (pp. 57–64). IEEE, January. (2022).
39. Nabi, S. T., Kumar, M., Singh, P., Aggarwal, N. & Kumar, K. A comprehensive survey of image and video forgery techniques: variants, challenges, and future directions. *Multimedia Syst.* **1**, 54 (2022).
40. Wang, Z., Zhou, M., Liu, B. & Li, T. Deep image steganography using transformer and recursive permutation. *Entropy* **24** (7), 878 (2022).
41. Sharif, A., Mollaeefar, M. & Nazari, M. A novel method for digital image steganography based on a new three dimensional chaotic map. *Multimedia Tools Appl.* **76**, 7849–7867 (2017).
42. Zhang, W. et al. Continual learning for blind image quality assessment. *IEEE Trans. Pattern Anal. Mach. Intell.* (2022).
43. Swain, G. Two new steganography techniques based on quotient value differencing with addition-subtraction logic and PVD with modulus function. *Optik* **180**, 807–823 (2019).
44. Pradhan, A., Sahu, A. K., Swain, G. & Sekhar, K. R. Performance evaluation parameters of image steganography techniques. In *2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS)* (pp. 1–8). IEEE. (2016), May.
45. Sahu, M., Padhy, N., Gantayat, S. S. & Sahu, A. K. Performance analysis of various image steganography techniques. In *2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)* (pp. 1–6). IEEE. (2022), September.
46. Mileva, A., Velinov, A., Dimitrova, V., Caviglione, L. & Wendzel, S. Information hiding in the DICOM message service and upper layer service with entropy-based detection. *Entropy* **24** (2), 176 (2022).

Acknowledgements

This research is funded by the European University of Atlantic.

Author contributions

"Shahid Rahman.Jamal uddin. and Farhan Amin.Hameed Hussain. wrote the main manuscript text and Sabir Shah.Abdu Salam. Isabel de la Torre Díez. Debora Libertad Ramírez Vargas and Julio César Martínez Espinosa prepared Figs. 1-3. All authors reviewed the manuscript."

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to F.A. or I.T.D.