SN Computer Science (2022) 3:153
https://doi.org/10.1007/s42979-022-01046-8

ORIGINAL RESEARCH

A Hybrid Secured Approach Combining LSB Steganography and AES Using Mosaic Images for Ensuring Data Security

Saralya Roy[1] · Md. Moinul Islam[1]

Received: 4 August 2021 / Accepted: 22 January 2022 / Published online: 3 February 2022

Abstract
Steganography is a technique of hiding information in digital media such as images, text, audio, etc. This digital media is used as the cover to make the private message invisible. Apparently, the attackers do not have any idea about the original message that is being hidden in the cover media. In this research, the proposed technique has focused on implementing the least significant bit (LSB) matching steganography algorithm. For ensuring better security, the advanced encryption standard (AES) technique is used before applying the steganography technique to ensure two-layer security of the private message. Another feature that is used in this research is using mosaic images as the cover media. Mosaic image is capable of hiding up to five LSB layers. Different survey papers show that the success rate of using mosaic images as the cover media is approximately 99% comparing with approximately 50% the success of normal image in case of data hiding. Our proposed approach overcomes the problem of stego image distortion using mosaic images. The improved LSB steganography algorithm also effectively handles mosaic images. Using a better version of LSB, Stego images were given more excellent peak signal-to-noise ratio (PSNR) value than other approaches when the hidden message was integrated into the mosaic image. Compared with different space domain strategies, the PSNR value of our proposed system is 85.65 dB for a maximum capacity of 32 bytes.

Keywords Steganography · Least significant bit · LSB matching · Mosaic image · PSNR · AES cryptography algorithm

Introduction

Today, the internet has become a necessity. Present information in the form of messages, images, videos, including sending data in the form of files, have become common place in today's sophisticated age. There are many electronic media nowadays such as e-mail, personal blog, chat application, and others for sending information. As internet usage is developing rapidly, internet users should pay more attention to the security and secrecy of data. The survey result of Norton Report 2013 shows that in 62% of cases, there is no online privacy in the world because of information being open on the internet [38].

There are many methods that can be used to ensure the security of electronic messages from being viewed by an unauthorized person. Steganography is a popular technique for securing messages. Steganography is the science and art of hiding secret messages in a cover media that can be either an image or audio or such like that to ensure that the existence of the confidential data is disguised [17, 36]. Steganalysis is a form of art and science that reveals the hidden messages as a counter-technology for steganography. Steganalysis reveals disadvantages of steganographic schemes by proof that a hidden message has been inserted in a cover, thus preventing criminal offenders from illegally transmitting hamrful messages using outstanding steganographic techniques. It is intended that the cover media does not create any suspicion that the file is containing any personal data. Steganography is a safe technique for sending a secret message. There are many techniques of Steganography. The least significant bit (LSB) is one of them, in which the data that is to be hidden is previously encrypted using the Advanced Encryption Standard algorithm (AES) [34].

This article is part of the topical collection "Cyber Security and Privacy in Communication Networks" guest edited by Rajiv Misra, R K Shyamsunder, Alexiei Dingli, Natalie Denk, Omer Rana, Alexander Pfeiffer, Ashok Patel and Nishtha Kesswani.

✉ Md. Moinul Islam
moinulislam7002@gmail.com

[1] Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, Chittagong 4349, Bangladesh

The entire message is invisible in Steganography to cover media such as text, audio or video, in which attackers have no knowledge of the original message contained in a media and which algorithms are used to insert it or remove it [4, 35].

In this paper, for better security, the AES encryption technique is used. Before applying the steganography technique, AES cryptography will change the secret message into ciphertext to ensure the two-layer safety of the news. The proposed method will hide extensive data in a single image retaining the advantages and discarding the disadvantages of the traditional LSB method. Various data sizes are stored inside the image, and the PSNR is also calculated for each of the images tested. Based on the PSNR value, the stego image has a higher PSNR value as compared to other methods [29]. Hence the proposed steganography technique is very efficient to hide the secret information inside an image. In addition to that, mosaic images are used to increase the efficiency of the process. Mosaic image approaches have been successfully proposed to solve different problems related to image processing. The contributions of our research can be summarized as follows:

- The main disadvantage of the traditional LSB steganography technique is it is easily cracked by unauthorized users. To overcome this disadvantage, the features of the mosaic image are used to increases the efficiency of the LSB steganographic algorithm.
- If a large amount of data is needed to embed in an image, a typical image usually distorts. It increases the chance of the attacker cracking the secret embedded message or data. To overcome this problem, mosaic images are used because smaller images are used to construct the bigger image. It becomes almost impossible to detect where changes in bits have been made. Enhancing the image quality keeping the data size same as previous.
- Mosaic image consists of RGBA channels. When the ciphertext is incorporated in the red and green channels of mosaic images, the intensity of the red and green channels becomes comparatively high, and the distortion between the cover and stego images increases. As a result, we have embedded the data in the blue channel, and the histogram shows that there's no significant distortion between the cover and stego images.

The rest of the paper is organized as follows: "Related Works" reviews related works of the system. We have presented our proposed method in "Methodology", including a brief discussion. Our experimental result was described in " Experimental Result and PerformanceEvaluation". Finally, "Conclusion and Future Work" concludes the paper and underlines the future work.

Related Works

A variety of strategies to improve safe data-hidden methods have been applied. They also managed to solve two key challenges, the amount of data obscured and data protection. Use of LSB algorithms to implement is the most common framework for hidden data. In the previous research papers, the researchers addressed how low LSB encoding can be implemented in the images [43], the audio file and the video file [2, 39]. It is concluded that in many cases, 4 LSB layers are possible that indicate the integration of 50% of the size of the cover file. However, due to texture issues, an approach implementing 5 LSB secret data layers was not present in the literature.

In [27], the authors suggested an advanced approach for message security in 3D cover images, with AES-256, edge detection and LSB steganography in the layers, with PSNR and MSE of roughly 70 dB and 0.0055, respectively. In another study [40], the authors used pixel locator sequence (PLS) to combine a random data distribution approach with LSB steganography . This approach distributes the data encrypted with AES to be infused into the image by randomly selecting pixels and modifying their LSB value and computed an MSE of 0.95186 and a PSNR of 48.34506 dB to quantify changes in image dynamics. Por et al. [32] illustrated the StegCure scheme is a combination of three steganography algorithms for the GIF image and the implementation of StegCure that conceals around 33% with high protection levels using PKI. Zaidan et al. [42] performed multi-cover steganographics with the help of remote sensing images and a general recursion neural crypto-system using a non-standard procedure to protect data until it is hidden, and they also develop a multi-cover methodology to ensure the strength of their solution. Naji et al. [28] stated that highly rated and highly protected data hidden by the AES encryption procedure with PE file assume that AES has an excellent data secure algorithm. Besides, the safest cover for multimedia files is the PE file. Hmood et al. in their research [13, 14] showed the relationship between the amount of data covered and the image quality using properties of the human vision system and pure steganography. These papers are mostly intended to assess the impact of increasing data volume and image quality. The first is that picturing photographs with a plain texture will only mask 33.3% of the image dimension. In the second place, up to 50% of the image size will hide images that do not have any clear texture. Hamid et al. [24] only used the complicated texture to mask the details and find a solution for the problem of simple texture by filtering images into a complex and simple texture. Taqa et al. [39] illustrated in their research that they have implemented a framework and it provides a mechanism for the safeguard of secret data in the video file and implements both LSB and AES via the MPEG video to make sure that the data are stable and stable.

The related works illustrated in this section have major limitations in certain areas. All steganographic approaches in the spatial domain have various difficulties and drawbacks. An unauthorised user may easily breach the LSB method. PVD technique has a high level of intricacy. It is not uncommon for the GLM method to lose vital data. This is due to the fact that the PCM method has an inadequate data storage capacity. As a result, this method has a higher payload capacity. As a result of the OPAP method, the image on the cover is distorted. This is due to the quality of the cover image that is utilized in these approaches.

Methodology

In this section, we have discussed our proposed method. To provide complete security of the system, we developed an approach that has different stages, as presented in Fig. 1.

At first, a secret message is taken as text and it is encrypted by AES cryptographic algorithm with a secret password. Then, the ciphertext is embedded with LSB matching (hide) steganographic algorithm into a mosaic image. This is the encryption and embedding process. Then, for retrieving the embedded ciphertext, LSB matching (unhide) algorithm is applied. And last of all, for retrieving the original secret message from ciphertext, AES decryption algorithm is applied. This is the extraction and decryption process. When using the conventional LSB steganography approach in [4, 34, 38], secret bits (ciphertext) are stored from the first pixel of an image to the last. There are no RGB channels taken into account. However, we investigated RGBA channels of mosaic images and observed that when the ciphertext is embedded in red and green channels, the intensity of red and green channels is comparably high, and the distortion between cover and stego images rises. As a result, we have explored working with the blue channel.

Encryption and Decryption with AES Cryptographic Algorithm

The cryptography methods give additional degree of security to steganography techniques, by increasing their resilience. There are several encryption algorithms such as, Data Encryption Standard (DES), Advanced Encryption Standard (AES), RSA, Triple DES, Blowfish, Towfish, etc [31]. In compared to other encryption techniques, AES provides

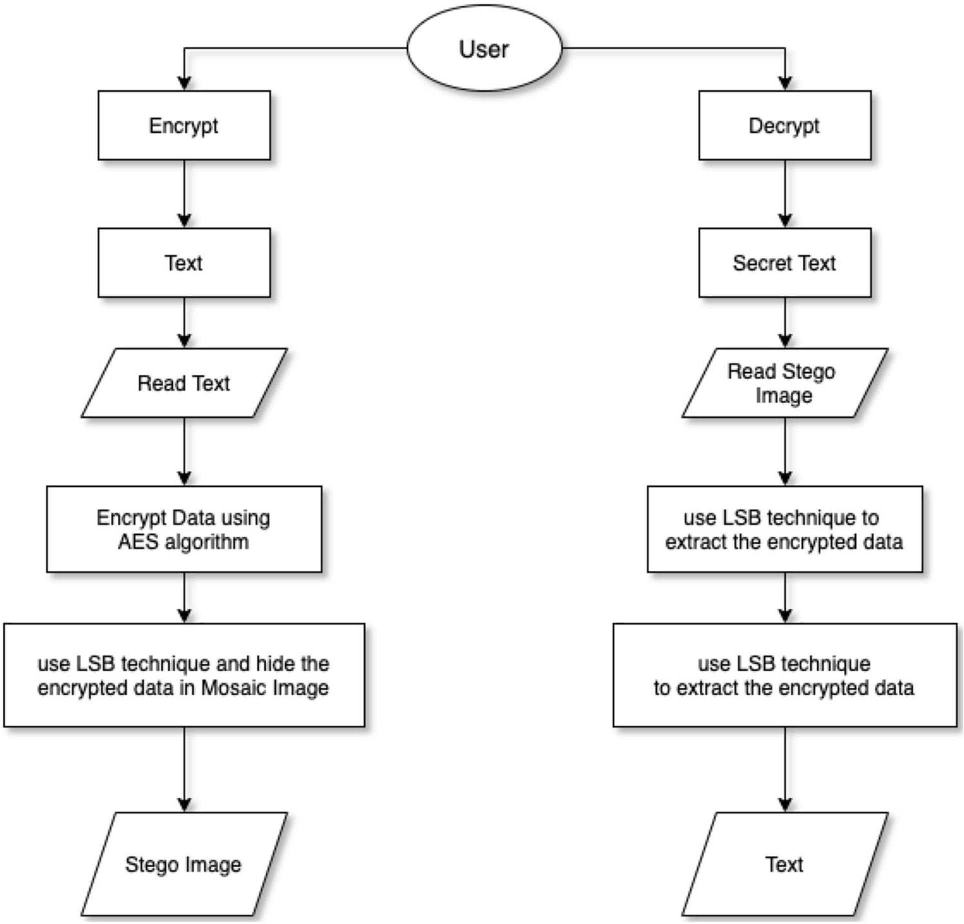

User
Encrypt
Text
Read Text
Encrypt Data using AES algorithm
use LSB technique and hide the encrypted data in Mosaic Image
Stego Image
Decrypt
Secret Text
Read Stego Image
use LSB technique to extract the encrypted data
use LSB technique to extract the encrypted data
Text

Fig. 1 The proposed methodology

greater secrecy, integrity, authenticity, and a balance of security and performance, and making it resistant to brute force assaults or hacking. To crack the encryption, around 2^{128} attempts are required for a key length of 128 bits. To improve the appropriateness for encrypting massive amounts of data, we employed AES. The technique is resistant to assaults such as content deletion, copy and paste attacks, and cryptographic attacks such as brute-force attacks [1].

AES has three cipher blocks: AES-128, AES-192, and AES-256. The ciphers encrypt and decrypt data in 128-bit chunks, using 128-bit, 192-bit, and 256-bit cryptographic keys. The Rijndael cipher [9] was designed for the use of additional block sizes and key lengths but was not used for AES. Symmetric ciphers are both encrypted and decrypted using the same token, which ensures that both the sender and the receiver would know and use the same private key [6].

The maximum data size can be varied to a maximum of 96 bytes for our research. Both key lengths are considered to be adequate for protecting sensitive data to the extent of the Secret, with "Top Secret" data needing a 192 or 256 bit key length. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys, a round consists of multiple processing steps that involve input plaintext replacement, translation, and combining, transforming it into a ciphertext final output. Figure 2 describes the flow diagram of AES encryption and Fig. 3 illustrates AES decryption technique.

The AES encryption algorithm defines several transformations that are to be performed on data stored in an array [10]. The cipher's first step is to put the data into an array, after which the cipher transformations are repeated over several encryption rounds. The round number is based on a key length, 10 rounds with 128-bit, 12 rounds with 192-bit, and 14 rounds with 256-bit. The first process in an AES encryption ciphers is to replace data by a substitution table; the second process changes data rows and the third mixes columns. A simple, exclusive (XOR) operation done with separate parts of the encryption key on each column requires longer keys to complete. The transition is a simple operation.

Solution to Image Distortion

Grayscale or standard RGB images are utilized in most situations mentioned in " Related Works" for the cover image. Please be aware that the photos are of a very low resolution (the pixel size of the images are not that high). Because of this, anytime a significant number of message bits need to be embedded, these images very readily get distorted. In other words, an intelligent attacker may readily determine that there is a secret message contained in the stego-image. In light of the low quality of the cover image, the resilience of the image rises if the image is significantly altered (the image is cropped or rotated). The majority of the approaches are sensitive to this issue. After a minor modification of an image, it is possible to lose important info. Because of the low quality of the cover photos, the distortion problem is of utmost importance.

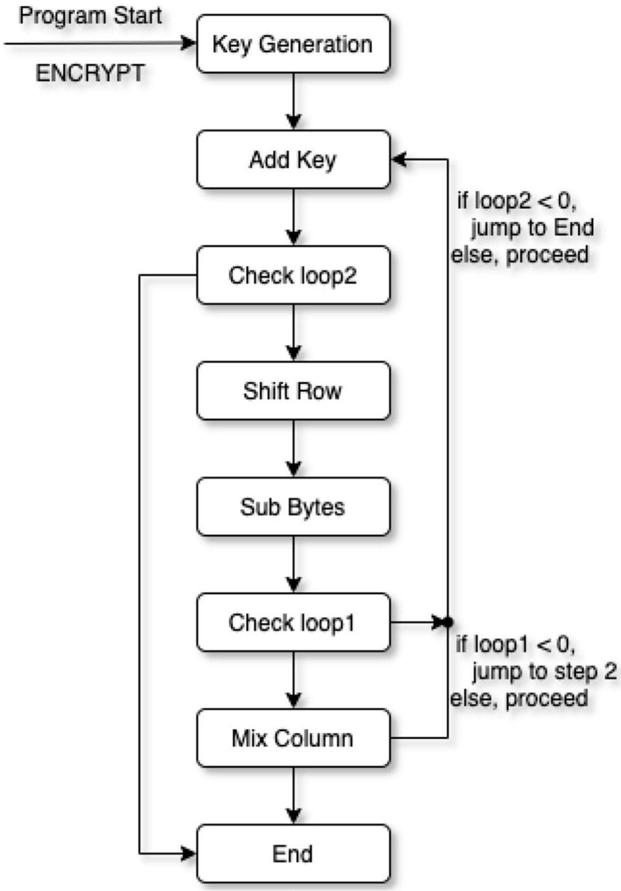


Fig. 2 Encryption technique of AES

When a large ciphertext is embedded in a conventional greyscale or RGB image, the cover image begins to distort. When the plaintext length grows longer, the ciphertext length grows as well. Anti-aliasing features are present in RGBA mosaic images utilized in the process. It does not deform the mosaic images as cover images, and it does not mislead these image formats. The mosaic images are created by picking one image and dividing it into smaller images (tiles) of sizes $8 * 8$, $16 * 16$, and $32 * 32$ pixels. These tiles are then compared to a huge number of similar-sized images. The user may then either insert a hidden image or a hidden text into them. The finished mosaic image contains secret information that is well-hidden and difficult to discover with the naked eye.

Mosaic Images

Mosaic image is a image consisting of hundreds or thousands of other images. Mosaic frames of mosaic pieces large and high with each piece of the same size are specified by

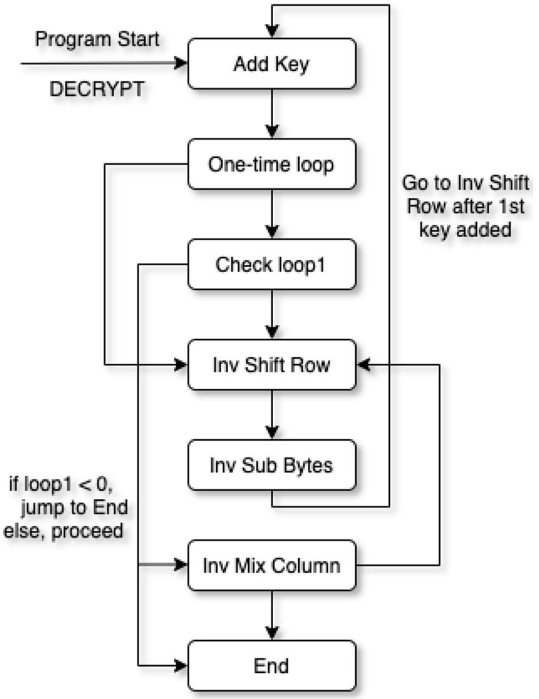


Fig. 3 Decryption technique of AES

user and created with a set of number [7]. The mosaic image is considered a piece of mosaic. To build a mosaic image, hundreds or thousands of images must be created, and these images are identical in scale. When a mosaic image is made, it is changed to the size of that segment. Each mosaic recalled a part of the overall image of the mosaic. The difference in scale is one of the most striking aspects of the mosaic images. The mosaic image was the right alternative to cover the secret data in this difference in scale. Mosaic image steganography is more effective and less prone. According to [7], the mosaic image with a resolution 324 MB, $12{,}000 * 9000$ pixel, other examples with an amount of pixels exceeding 9.4 gigabytes, having pixels of 3,366,400,000.

Usually, the ciphertext length increases if the plaintext is encrypted by the AES cryptography algorithm. As the plaintext length increases, the ciphertext length increases at the same time. The cover image begins to distort when incorporating this huge ciphertext in a standard greyscale or RGB image. *Mosaic images*, which are RGBA-type, are used in the proposed technique. It has anti-aliasing properties. This does not easily misrepresent these image forms.

The construction of mosaic images is done by selecting a target image, splitting it into smaller images (tiles) of sizes $8 * 8$, $16 * 16$, $32 * 32$ [30]. These tiles are then compared with thousands of equal sized tiles stored in a database. Tiles from the original images are then replaced by similar sized tiles from the database. These images are named as Mosaic Images because they are being constructed with thousand of similar sized tiles (smaller images).

The quality of image steganography is assessed using a variety of metrics. Each measure evaluates a distinct component of the outcome. mean square error (MSE), peak signal to noise ratio (PSNR), structured similarity index measure (SSIM), payload capacity, cross correlation coefficient, entropy, quality index, correlation, and the signal-to-noise ratio are only a few examples of well-known metrics. Regardless of various measuring techniques, according to [4] the peak signal-to-noise ratio (PSNR) and mean square error (MSE) provide a more objective approach to assess an algorithm's performance. As a result, we computed the performance of our suggested approach using PSNR and MSE. PSNR (peak signal-to-noise ratio) is used to measure the distortion between cover and stego images. The higher the PSNR value, the lower is the distortion. The mathematical equation of PSNR is illustrated as:

$$\mathrm{PSNR} = 10 * \log_{10} \frac{255^2}{\mathrm{MSE}}, \tag{1}$$

where MSE is the mean-square error. MSE is defined as:

$$\frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} (I_c(i,j) - I_s(i,j))^2, \tag{2}$$

where $I_c(i,j)$ and $I_s(i,j)$ represent the pixel values of cover image and stego image, respectively, and m, n are the width and height of the original image. The MSE is the total squared error between the compressed and the original image, and the PSNR is a measured maximum error, whereas, mean absolute error (MAE) represents the mean absolute error between the stego image and the original image.

$$\frac{1}{nm} \sum_{i=1}^{n} \sum_{j=1}^{m} |f(i,j) - y(i,j)| \tag{3}$$

In Eq. 3, the mean absolute error is the mean value of the total errors. Where $f(i, j)$ is the pixel value of the original image and $y(i, j)$ is the actual value of the stego image. The size of a monochrome image is $m * n$. For coloured images, the size of an image is $m * n * 3$.

Least Significant Bit (LSB)

Since digital images are proliferating particularly online and because of the wide quantity of redundant bits in the digital image representation, images are the most common steganography cover items [26]. Different steganographic algorithms exist for these various image file formats [20]. Based on embedding method, image steganography techniques are classified into 3 categories: spatial doamin, transform domain, and distortion technique. Image pixel values are translated into binary values in steganographical spatial domain techniques and certain bits shift for hidden data hiding.

The least significant bit (LSB) technique is one of the most basic and most commonly used techniques for inserting or dissimulating the hidden message of pixel values in the LSBs, without any significant visual distortion. It is the most common technique for hiding secret data with an image with large payloads, whereas the human visual system is unable to see distortions in the resulting stego image [3, 12]. Insertion by LSB is a popular and easy approach to insert data into a coverage image. Any of the bytes in an image are changed into the least relevant bit (in other words, the 8th bit). A 24-bit image uses a little of red, green, and blue color component, as each component is represented by a byte. Three bits in each pixel can be stored. A total of 144,000 bits (or 180,0000 bytes of embedded data) can be stored in an 800 * 600 pixels image. The steganographic methods for LSB can be divided into two categories: LSB substitution and LSB matching, which are often referred to as ±1 embedding [25]. The strategies of LSB matching discover hidden messages found in digital Media with LSB matching steganography. The LSB matching, a complement of the LSB replacement [21], maintains the favours of the LSB replacement and is harder to spot from the mathematical point of view. If a bit needs to be adjusted, in the LSB match, the pixel value will be set to ±1. Usage of + or − is randomly selected and would not affect the secret code. The detectors function in the same manner, with both LSB substitution and ±1 incorporation. The LSB is the secret bit, for any chosen pixel.

Solution to LSB Substitution Method

As mosaic images are of RGBA type and they have greater resolution and size than normal RGB or greyscale images, not all techniques of spatial domain steganography work efficiently with mosaic images. LSB substitution technique works very slowly with mosaic images. That's why, a new and improved version of LSB technique is proposed in this study. The process of embedding message bits into pixel's RGBA bits is made faster by taking the modulus of pixel values of blue channel. This improved technique *LSB Matching* [15] works very efficiently with mosaic images.

Data Embedding and Extraction Using LSB Matching Steganography

The LSB substitution method is not suitable for working with embedding and extracting data from mosaic images as it takes a longer execution time. So, to get better performance, we have used LSB matching method [15] for data embedding and extraction process. By taking the modulus of the pixel values of blue channel of mosaic images, the embedding and extracting process is being improved and this improved method works efficiently with mosaic images. Both the embedding and extraction processes are illustrated in Algorithms 1 and 2, respectively.

Algorithm 1 Data Embedding using LSB Matching Steganography

```
1:  Input: Ciphertext
2:  Output: Stego images
3:  procedure DATA EMBEDDING
4:      Read ciphertext from file
5:      Take ASCII value of each character of ciphertext
6:      Convert the ASCII values to bytes
7:      SET $i = 0$
8:      if $i < 8$ then
9:          DO $message\_bits >> i$ and SET $i++$
10:         RETURN $messagebits$
11:         if $messagebits$ not checked then
12:             Generate a random variable $K$
13:             SET $K = 1$ or $-1$
14:             if colorpixel (B/W) checked then
15:                 SET $K = 1$ for Black and $K = -1$ for White
16:                 Take Modulus of $pixel\_val$ to Blue channel
17:                 if $Modulus\ != message\_bit$ then
18:                     $pixelVal += K$
19:                 else: go to Step 10
20:             else: RETURN previous value of $K$
21:         else: go to Step 14
22:     else: EXIT
23: end procedure
```

Algorithm 2 Data Extraction using LSB Matching Steganography

```
1:  Input: Stego Images
2:  Output: Ciphertext
3:  procedure DATA EXTRACTION
4:      Read the stego image
5:      if $messagebits$ not checked then
6:          SET $bitVal = 0$ and $bitIdx = 0$
7:          Take Modulus of pixel value of Blue channel
8:          SET $bitVal \mid= Modulus << bitIdx$
9:          SET $bitIdx++$
10:         if $bitIdx == 8$ then
11:             go to Step 4
12:         else: go to Step 5
13:     else: EXIT
14: end procedure
```

Experimental Result and Performance Evaluation

In this section, we have described all the performance metrics used in this work to test our proposed method. Here for different parameter of k, capacity and payload PSNR (dB) value was calculated. All tests were performed on an 8 GB RAM Intel Core i5 2.50GHz CPU. The proposed method is implemented in Python 3.7 under OS Windows 10.

To evaluate the performance of our research, we have collected mosaic images from online sources and used more than 100 mosaic images of different resolutions and sizes. Among them, first one (Baby) is of $1000 * 750$ pixels, Lenna is of $900 * 900$ pixels, third one (Girl) is of $3000 * 3000$ pixels, Chaplin is of $204 * 247$ pixels, and the last one (Hand) is of $300 * 168$ pixels. A secret message of 32 bytes was encrypted and then embedded into these mosaic images and then the PSNR value of the stego images were compared with the cover images as shown in Fig. 4. The stego-images generated indicate that human eyes cannot distinguish any distortion in comparison with the actual images.

As we stated earlier in "Methodology", we preprocessed raw dataset for fitting into our proposed model. At first, a hidden message was taken as text, and encrypted with a secret password by the cryptographic AES algorithm. The ciphertext was then integrated into the mosaic image with an LSB matching (hidden). This is the method of coding and incorporation. LSB matching (unhide) algorithm is then implemented for the recovery of the embedded ciphertext. And last but not least, the AES Decryption Algorithm is used to retrieve the original hidden message from ciphertext. This is the method of extraction and decoding.

The length of a key is the number of bits in the key of an encryption technique. Key lengths are determined by the maximum number of combinations necessary to crack an encryption scheme. Because 256 bit keys need 14 rounds of numerous processing steps to convert plaintext to ciphertext, we selected 256 bit keys to ensure the security of our proposed approach.

Here, we have compared the histogram of cover images and stego images. An image histogram is a type of histogram that is used to show how a digital images' colors are distributed. The number of pixels for each tonal value is plotted on a graph. It allows a person to see the complete distribution of a image in only a few glances. A histogram is a graphical representation of discrete or continuous data. A histogram is a visual depiction of the distribution of data. A histogram shows a huge amount of data as well as the frequency with which the data values occur. It also highlights any anomalies or gaps in the data. It shows data points that fall inside a specific range, in this example the total pixel value of the cover and stego images, to provide a visual interpretation

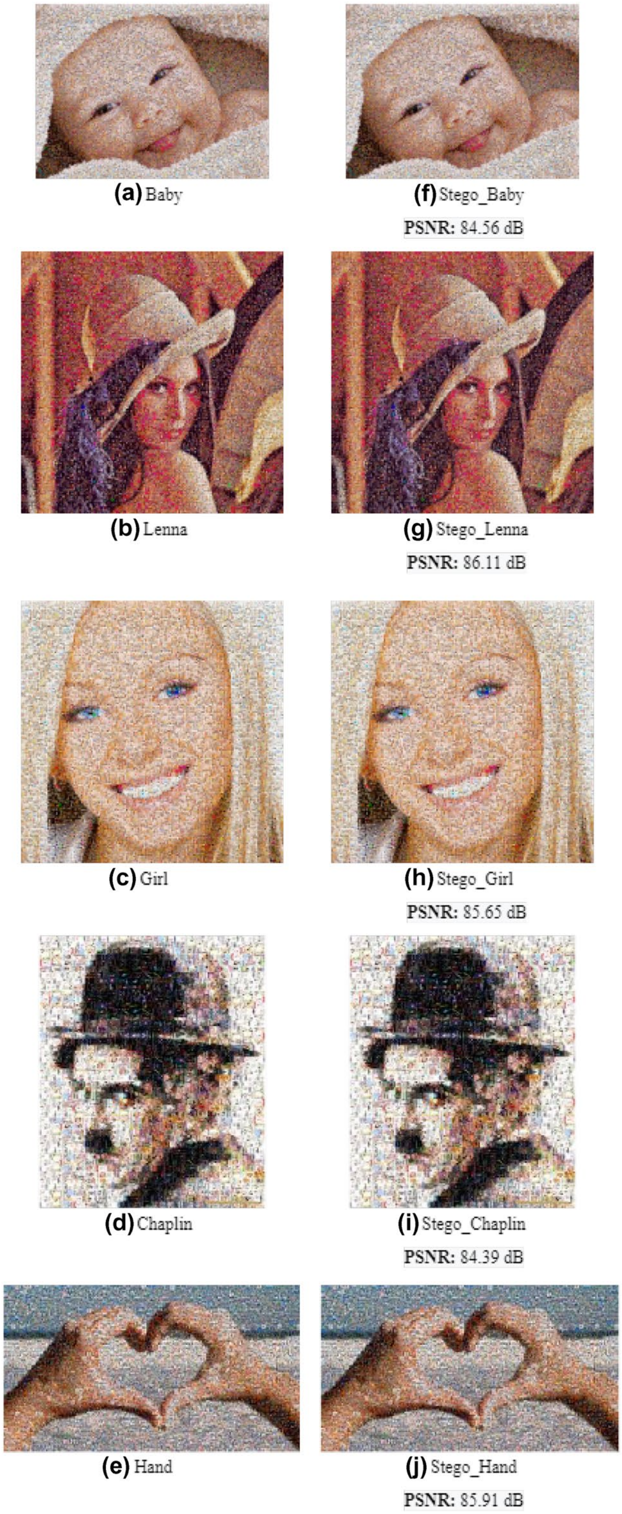


Fig. 4 Cover images (**a–e**) and stego images (**f–j**) produced with PSNR when $k = 6$

of data. The histograms of the cover and stego images were evaluated and compared in Fig. 5, and no outliers or gaps in distinct co-ordinates were observed. We can see from these histograms that the distortion between the cover and stego images is minimal and not clearly detectable by human eyes.

Each tone is represented by a horizontal axis, while the vertical axis shows how many pixels make up that particular tone. Right side of horizontal axis indicates light and pure white regions, left side represents black and dark parts, middle represents blue areas, right hand side represents blue areas. For each zone, the vertical axis indicates its respective capture area. If a image is really black, the histogram will contain the most data points on the left and center. Most of the data points in a histogram for a highly bright image with minimal black regions and shadows will be on the graph's left-hand side or in the middle. From the histogram, we can see that the differences between the cover images and stego images are negligible and are not easily detected by human eyes.

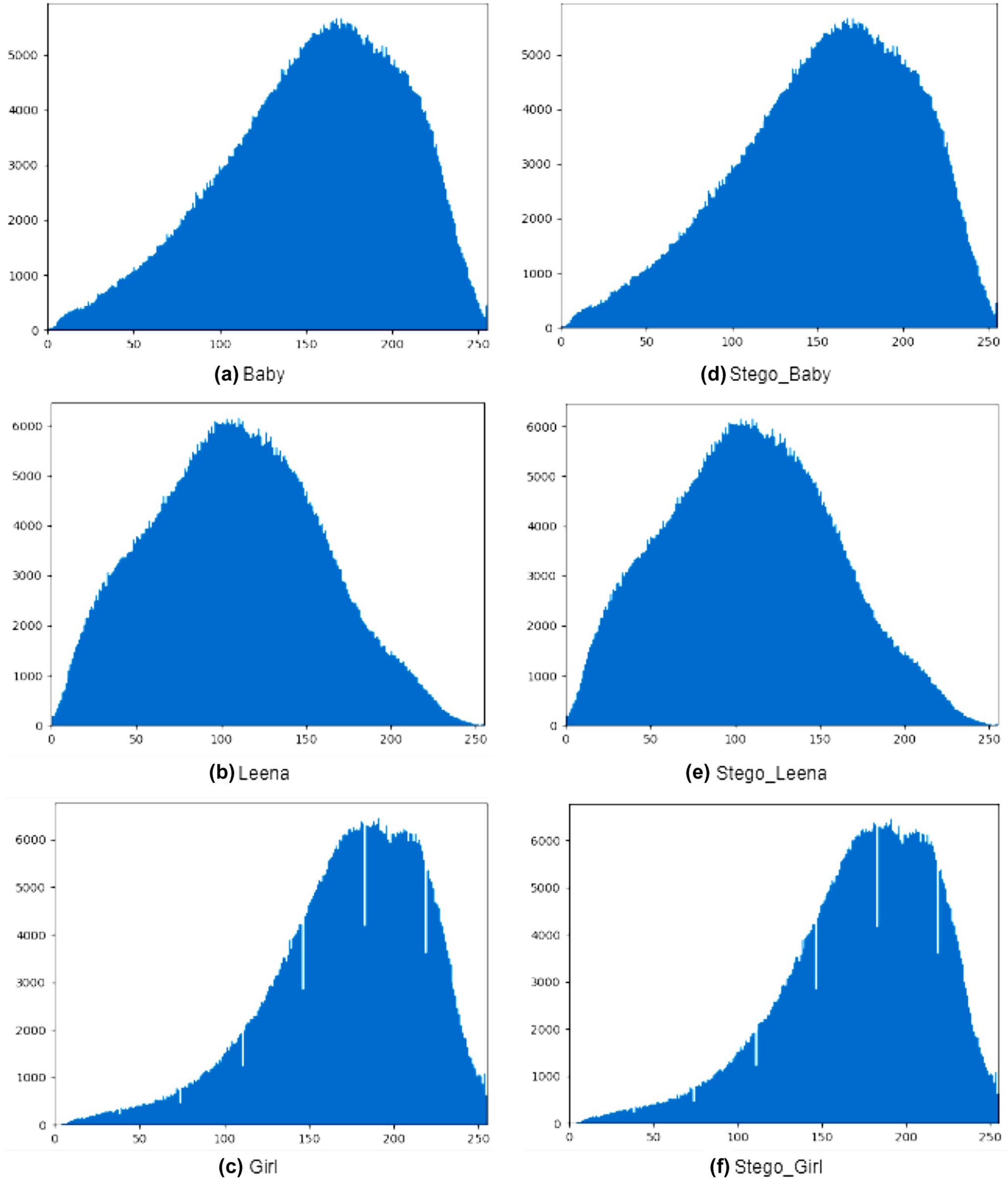
From Table 1, it is stated that, with increasing capacity and payload, the value of PSNR decreases. For a total of 5 bytes of capacity and 1.16 payload bits per pixel, PSNR gives 90.36 dB as the highest and for 96 bytes of capacity and 5.36 payload bits per pixel, the proposed model gives 79.98 dB as the lowest value. There are different spatial domain techniques available and for efficiency measurement of the proposed method, we have compared our model with other spatial techniques in terms of capacity (bytes), average PSNR (dB) and MSE.

In the existing methods, traditional LSB steganography technique is used in which the secret bits are stored in consecutive pixels starting from the first one. No channels are considered in those methods. That's why, whenever the secret bits are being embedded into the red or green channels, the possibility of image distortion becomes higher as the intensity of red and green channel is higher. Considering this, we have taken the channels into consideration in our proposed method. We have taken the modulus of pixel value of the blue channel and embedded the secret bits into blue channel as the intensity of Blue channel is moderated. So, we have managed to reduce the possibility of image distortion in our proposed method compared to other existing methods. From Tables 2 and 3, we observe that the proposed method has higher efficiency than the other spatial domain techniques while using mosaic image as the cover image. The PSNR (peak signal-to-noise ratio) and MSE (mean square error) metrics are used to determine accuracy. PSNR (peak signal to noise ratio) is used to measure the distortion between cover and stego images. The higher the PSNR value, the higher the accuracy and the lower is the distortion. As we have stated earlier that we have managed to reduce the possibility of image distortion in our proposed method by considering Blue channel for embedding the secret bits, we have got higher PSNR value while embedding 32 bytes of secret data using our proposed method comparing with other existing methods.

Conclusion and Future Work

In this study, the method of image steganography has been developed. The proposed approach overcomes the issue of image distortion in stego through the use of mosaic images. An encrypted message of much larger length can easily be integrated without visible distortion using the mosaic image. In addition, the improved version of the LSB steganography algorithm can deal with the mosaic images effectively. The procedure of embedding and extraction has been quicker than other current spatial domain approaches. After embedding the secret message into the mosaic image using the better version of LSB, stego images were given a higher PSNR values than other methods. We experimented with and showed PSNR values with a maximum data size of 96 bytes. The location of the data to be concealed, as well as the image size, may be varied. The greater the image size, the more effectively the information may be hidden inside the image. The time complexity of our proposed approach is $O(n)$ and unaffected by the size of the images. For a maximum data size of 96 bytes, we experimented with and exhibited a PSNR value of 79.98 dB. The PSNR value drops significantly as the data size exceeds 96 bytes. The PSNR value for 128 bytes of data size with a payload of 6.04 bits per pixel is 67.59 dB.

This proposed method utilizes the human visual system's limitations (HVS). Color vectors at a cluster of color pixels cannot be detected by HVS. This strategy can be used to conceal sensitive data. There are various reasons to hide data, but they all boil down to preventing unauthorized parties from discovering a message. In the corporate realm, steganography might conceal a secret formula or new innovation plans and also be used for corporate espionage to communicate confidential information without the organization knowing. Cartographers occasionally add a little fictional street to their maps, allowing them to punish copycats. To prevent unauthorized re-sellers, add fictional names to mailing lists. Also, governments are interested in two sorts of covert data communication: security-related and non-security-related. Business has comparable worries about trade secrets for innovative technology or product knowledge. This technique decreases the danger of information leaking. This techniques allows us to convey news and information without worry of being filtered or intercepted and traced back to us. A cover source can hold, for example, our personal financial information or military secrets [19, 37]. We can readily divulge our financial data without revealing our cover source's military secrets.



(a) Baby

(d) Stego_Baby

(b) Leena

(e) Stego_Leena

(c) Girl

(f) Stego_Girl

Fig. 5 Histogram analysis of cover images and stego images

Table 1 Experiment result of the proposed method

Embedding parameter (*k*)	Capacity (bytes)	Payload (bits per pixel)	PSNR (dB)
1	5	1.16	**90.36**
2	19	1.85	88.87
3	28	2.31	85.52
4	45	3.45	83.21
5	64	4.23	81.87
6	96	5.36	79.98

Bold indicates the highest PSNR value in terms of embedding parameter of 1 with a message capacity of 5 bytes

Table 2 Comparison between various spatial domain techniques

Author(s)	Method
Khodaei et al. [22]	LSB substitution
Jung et al. [18]	LSB substitution
Zakaria et al. [44]	LSB substitution
Joshi et al. [16]	LSB substitution
Yang et al. [41]	Adaptive LSB substitution
Liao et al. [23]	Modified LSB substitution
Mokammel et al. [11]	Diamond encoding
Prasad et al. [33]	Optimal pixel adjustment
Proposed	LSB matching + AES

Table 3 Comparison of average PSNR values and MSE of our proposed model with previous state-of-the-art data security approaches

References	Message capacity (bytes)	Average PSNR (dB)	Average MSE
[22]	–	39.30	–
[18]	–	43.94	–
[44]	–	43.17	–
[16]	–	54.15	0.25003
[41]	24	41.70	–
[23]	–	40.20	–
[11]	32	57.3	0.0235
[33]	32	70.40	0.0195
Proposed	32	**85.65**	0.0097

Bold indicates the highest PSNR value in terms of embedding parameter of 1 with a message capacity of 5 bytes

Moreover, our primary focus was only with mosaic images that are commonly used in the creation of three-dimensional images, medical imaging, computer vision, satellite data, and military automated target recognition. But we are also planning to implement our approach on other types of images. We strongly believe that the proposed LSB Matching steganography with AES approach can be applied to greyscale or RGB color images as proposed in [5, 8, 34]. According to [4], upto five LSB layers can be hidden using the mosaic image texture. Their findings suggest that the mosaic images' complex texture aids in the creation of an extremely high rate of data hidden using five LSB layers without any detectable distortion, and that their experiment demonstrated the mosaic images' ability to hide a high rate of data hidden with a success rate of 99 percent for the mosaic images as cover, whereas, in our proposed technique, only one LSB layer is used for embedding process. Although the highest PSNR value of our proposed method has come to 90.36 dB, further study could assess the efficiency of our proposed model by collecting large test sets with more dimensions of security features as well as by including more layers in the embedding phase and improving the PSNR with the increase in LSB layers of mosaic images for greater than 96 bytes of data and the efficiency of our proposed technique on a cyber security implementation basis.

Author contributions These authors contributed equally to this work.

Funding Not applicable.

Availability of data and material Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Abdullah A. Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptogr Netw Secur. 2017;16:1–11.
2. Ahmed MA, Mat Kiah ML, Bahaa B, Zaidan A. A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J Appl Sci. 2010. https://doi.org/10.3923/jas.2010.59.64.
3. Al-Aidroos NM, Bahamish HA. Image steganography based on LSB matching and image enlargement. In: 2019 First International Conference of Intelligent Computing and Engineering (ICOICE); 2019. p. 1–6 . https://doi.org/10.1109/ICOICE48418.2019.9035172.
4. Alam GM, Mat Kiah ML, Bahaa B, Zaidan A, Alanazi H. Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: analytical study. Sci Res Essays. 2010;5:3254–60.
5. Anwar F, Rachmawanto EH, Atika Sari C, Ignatius Moses Setiadi DR. Stegocrypt scheme using LSB-AES base64. In: 2019 International Conference on Information and Communications Technology (ICOIACT); 2019. p. 85–90 . https://doi.org/10.1109/ICOIACT46704.2019.8938567.

6. Arora R, Parashar A, Transforming CCI. Secure user data in cloud computing using encryption algorithms. Int J Eng Res Appl. 2013;3(4):1922–6.
7. Bahaa B, Zaidan A, Taqa A, Alam GM, Mat Kiah ML, Jalab A. Stegomos: a secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem. Int J Phys Sci. 2010;5:1796–806.
8. Chikouche SL, Chikouche N. An improved approach for LSB-based image steganography using AES algorithm. In: 2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B); 2017. p. 1–6 . https://doi.org/10.1109/ICEE-B.2017.8192077.
9. Daemen J, Rijmen V. The block cipher rijndael. In: Quisquater JJ, Schneier B, editors. Smart card research and applications. Berlin: Springer; 2000. p. 277–84.
10. Fathy A, Tarrad IF, Hamed HFA, Awad AI. Advanced encryption standard algorithm: issues and implementation aspects. In: Hassanien AE, Salem ABM, Ramadan R, Kim TH, editors. Advanced machine learning technologies and applications. Berlin: Springer; 2012. p. 516–23.
11. Haque MM, Sheikh J, Rashid MJA. An improved steganographic technique based on diamond encoding method. In: 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE); 2017. p. 583–588 . https://doi.org/10.1109/ECACE.2017.7912972.
12. Hemalatha S, Renuka A, Acharya UD, Kamath PR. A secure image steganography technique using integer wavelet transform. In: 2012 World Congress on Information and Communication Technologies. IEEE; 2012. p. 755–758.
13. Hmood A, Bahaa B, Zaidan A, Jalab H. An overview on hiding information technique in images. J Appl Sci. 2010. https://doi.org/10.3923/jas.2010.2094.2100.
14. Hmood A, Jalab H, Mk Z, Bahaa B, Zaidan A. On the capacity and security of steganography approaches: an overview. J Appl Sci. 2010. https://doi.org/10.3923/jas.2010.1825.1833.
15. Jiaohua Q, Xuyu X, Wang M. A review on detection of LSB matching steganography. Inf Technol J. 2010. https://doi.org/10.3923/itj.2010.1725.1738.
16. Joshi K, Yadav R, Allwadhi S. PSNR and MSE based investigation of LSB. In: 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT); 2016. p. 280–285.
17. Juneja M, Sandhu P. Improved LSB based steganography techniques for color images in spatial domain. Int J Netw Secur. 2014;16:452–62.
18. Jung KH, Kee-Young Y. Steganographic method based on interpolation and LSB substitution of digital images. Multimed Tools Appl. 2014. https://doi.org/10.1007/s11042-013-1832-y.
19. Kadhim IJ, Premaratne P, Vial PJ, Halloran B. Comprehensive survey of image steganography: techniques, evaluations, and trends in future research. Neurocomputing. 2019;335:299–326.
20. Kaur J. A new steganography technique based on layers of image and sensitivity vectors acquiring HVS. 2011.
21. Kekre HB, Mishra D, Khanna R, Khanna S, Hussaini A. Comparison between the basic LSB replacement technique and increased capacity of information hiding in LSB's method for images. Int J Comput Appl. 2012;45(1):33–8 (**Full text available**).
22. Khodaei M, Sadeghi Bigham B, Faez K. Adaptive data hiding, using pixel-value-differencing and LSB substitution. Cybern Syst. 2016;47(8):617–28.
23. Liao X, Wen QY, Zhang J. A steganographic method for digital images with four-pixel differencing and modified LSB substitution. J Vis Commun Image Represent. 2011;22(1):1–8.
24. Majeed A, Mat Kiah ML, Madhloom HT, Zaidan B, Zaidan A. Novel approach for high secure and high rate data hidden in the image using image texture analysis. Int J Eng Technol. 2009;1(2):63–9.
25. Mielikainen J. LSB matching revisited. IEEE Signal Process Lett. 2006;13(5):285–7. https://doi.org/10.1109/LSP.2006.870357.
26. Morkel T, Eloff JH, Olivier MS. An overview of image steganography, vol. 1. In: ISSA; 2005. p. 1–11.
27. Moussa Y, Alexan W. Message security through AES and LSB embedding in edge detected pixels of 3D images. In: 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES); 2020. p. 224–229. https://doi.org/10.1109/NILES50944.2020.9257937.
28. Naji AW, Hameed SA, Zaidan BB, Al-Khateeb WF, Khalifa OO, Zaidan AA, Gunawan TS. Novel framework for hidden data in the image page within executable file using computation between advanced encryption standard and distortion techniques. 2009. http://arxiv.org/abs/0908.0216.
29. Nurhayati, Ahmad SS. Steganography for inserting message on digital image using least significant bit and AES cryptographic algorithm. In: 2016 4th International Conference on Cyber and IT Service Management; 2016. p. 1–6. https://doi.org/10.1109/CITSM.2016.7577468.
30. Pascaline AH, Christopher LCF, Khan MHM, Pudaruth S. Using photomosaic and steganographic techniques for hiding information inside image mosaics. In: 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI); 2015. p. 1893–1897. https://doi.org/10.1109/ICACCI.2015.7275894.
31. Patil P, Narayankar P, Narayan DG, Meena SM. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish. Procedia Comput Sci. 2016;78:617–24. https://doi.org/10.1016/j.procs.2016.02.108. In: 1st International Conference on Information Security and Privacy, 2015.
32. Por LY, Lai WK, Alireza Z, Ang TF, Su MT, Delina B. Stegcure: a comprehensive steganographic tool using enhanced LSB scheme. WSEAS Trans Comput. 2008;7:1309–18.
33. Prasad G, Varadarajan D, Jilani SA, Kodandaramaiah D. Image steganography based on optimal LSB pixel adjustment method. Int J Comput Technol. 2006;5:1–6. https://doi.org/10.24297/ijct.v5i1.4380.
34. Rachmawanto EH, Amin RS, Setiadi DRIM, Sari CA. A performance analysis stegocrypt algorithm based on LSB-AES 128 bit in various image size. In: 2017 International Seminar on Application for Technology of Information and Communication (iSemantic); 2017. p. 16–21. https://doi.org/10.1109/ISEMANTIC.2017.8251836.
35. Saračević M, Adamović S, Miškovic V, Maček N, Šarac M. A novel approach to steganography based on the properties of Catalan numbers and Dyck words. Future Gener Comput Syst. 2019;100:186–97. https://doi.org/10.1016/j.future.2019.05.010.
36. Selimovic F, Stanimirovic P, Saračević M, Selim A, Krtolica P. Authentication based on the image encryption using Delaunay triangulation and Catalan objects. Acta Polytechnica Hungarica. 2020;17:207–24. https://doi.org/10.12700/APH.17.6.2020.6.12.
37. Serpa-Andrade L, Garcia-Velez R, Pinos-Velez E, Flores-Urgilez C. Analysis of the application of steganography applied in the field of cybersecurity. In: International Conference on Applied Human Factors and Ergonomics. Springer; 2021. p. 366–371.
38. Sheth U, Saxena S. Image steganography using AES encryption and least significant nibble. In: 2016 International Conference on Communication and Signal Processing (ICCSP); 2016. p. 0876–0879. https://doi.org/10.1109/ICCSP.2016.7754272.
39. Taqa A, Zaidan A, Bahaa B. New framework for high secure data hidden in the mpeg using AES encryption algorithm. Int J Comput Electr Eng. 2009. https://doi.org/10.7763/IJCEE.2009.V1.87.
40. Tiwari K, Gangurde SJ. LSB steganography using pixel locator sequence with AES. In: 2021 2nd International Conference on

Secure Cyber Computing and Communications (ICSCCC); 2021. p. 302–307. https://doi.org/10.1109/ICSCCC51823.2021.9478162.

41. Yang H, Sun X, Sun G. A high-capacity image data hiding scheme using adaptive LSB substitution. Radioengineering. 2009;18(4):509–16.
42. Zaidan A, Bahaa B, Taqa A, Sami K, Alam GM, Jalab A. Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. Int J Phys Sci. 2010;5:1776–86.
43. Zaidan B, Zaidan A, Taqa A, Othman F. Stego-image vs stego-analysis system. Int J Comput Electr Eng. 2009;1(5):572.
44. Zakaria AA, Hussain M, Wahab AWA, Idris MYI, Abdullah NA, Jung KH. High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution. Appl Sci. 2018;8(11). https://doi.org/10.3390/app8112199. https://www.mdpi.com/2076-3417/8/11/2199.

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