Computers, Materials & Continua CMC, vol.64, no.1, pp.31-61, 2020

A Novel Approach of Image Steganography for Secure Communication Based on LSB Substitution Technique

Shahid Rahman[1], Fahad Masood[2], Wajid Ullah Khan[2], Niamat Ullah[1], Fazal Qudus Khan[3], Georgios Tsaramirsis[3], Sadeeq Jan[4, *] and Majid Ashraf[5]

Abstract: Steganography aims to hide the messages from unauthorized persons for various purposes, e.g., military correspondence, financial transaction data. Securing the data during transmission is of utmost importance these days. The confidentiality, integrity, and availability of the data are at risk because of the emerging technologies and complexity in software applications, and therefore, there is a need to secure such systems and data. There are various methodologies to deal with security issues when utilizing an open system like the Internet. This research proposes a new technique in steganography within RGB shading space to achieve enhanced security compared with existing systems. We evaluate our approach with the help of diverse image quality evaluation techniques including MSE (Mean Square Error), RMSE (Root Mean Square Error), PSNR (Peak Signal-to-Noise Ratio), MAE (Mean Absolute Error), NCC (Normalized Cross-Correlation) and SSIM (Structural Similarity Index). Our experimental results demonstrate improved strength, intangibility, and security when contrasted with existing techniques and vindicate the effectiveness of this exploration work. The proposed approach achieved a 3.6701% average higher score for PSNR Correlation than the next best existing approach. Moreover, in PSNR with a variable amount of cipher embedded in the same images of the same dimensions, the proposed approach attained a 5.22% better score. Embedding the same size of cipher in images of different size resulted a 3.56% better score.

Keywords: Image steganography, least significant bits, MLEA and RGB color space.

[1] University of Buner, Buner, 19290, Pakistan.

[2] Abasyn University, Peshawar, 25000, Pakistan.

[3] Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21577, Saudi Arabia.

[4] National Center for Cyber Security-UETP, Department of CS & IT, University of Engineering & Technology, Peshawar, 25000, Pakistan.

[5] Department of Electrical Engineering, University of Engineering & Technology, Peshawar, 25000, Pakistan.

[*] Corresponding Author: Sadeeq Jan. Email: sadeeqjan@uetpeshawar.edu.pk.

Received: 19 November 2019; Accepted: 03 March 2020.

1 Introduction

Information hiding methods received attention from the research community due to the rapid use of information in modern technology. The two most common approaches for hiding information and securing data are the steganography and the cryptography. Steganography infers covered writing. It is one of the branches of "information stowing away or hiding". It is characterized as "the way toward composing secret message with the end goal that the proximity of the message is just known to the sender and receiver". It is the workmanship and study of undetectable communication and a push to cover the presence of the embedding data. Cover steganography is the art of conveying that cannot be distinguished or detected [Dunbar (2002); Anderson and Petitcolas (1998)]. The principal objective of steganography is to keep up an obscure correspondence between two social occasions. The best explanation behind steganography is to cover the specific closeness of correspondence by embedding messages into honest looking spread articles. Fig. 1 shows a fundamental plan of image steganography.

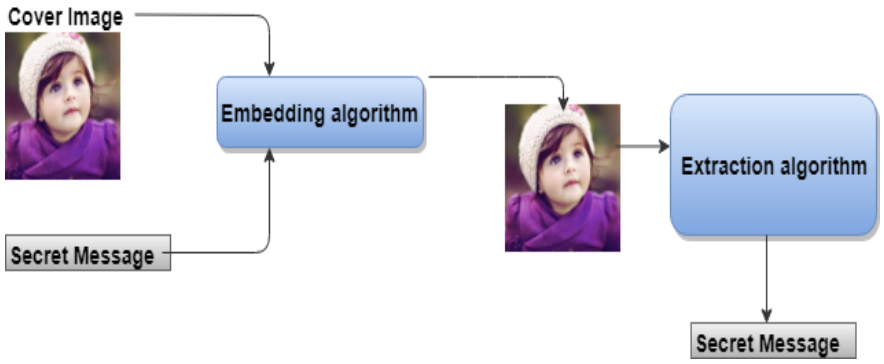


Figure 1: Fundamental plan of steganography

The secret message is hidden within the image in such a manner that the intended user is prevented to detect the hidden message. The stego-image is formed through an embedding algorithm. The stego-images, when formed, have a mirror distortion of the image which is negligible for the naked eye. The hidden message can be extracted algorithm from the stego-object. Steganography can be described as the examination of imperceptible data that customarily deals with the strategies for hiding the nearness of the passed-on message. In this technique, a piece of data covering is refined in correspondence, image, content, voice, or sight and sound substance for copyright, military correspondence, confirmation and other purposes [Lee and Chen (2000)]. Embedding a secret message into a digital medium is known as information hiding. A text, an image, an audio or any object that can be presented by some number of bits can be used as a secret message.

In the proposed strategy, the mystery information is expressed as a mystery message, mystery data or private data and will be utilized subsequently. The aim is to insert the mystery message in concealed objects. These items can be of numerous types, such as a picture, sound, video, document or another type that can convey data without reversing it. Therefore, it is avoided to cover pictures, sound and videos separately. By inserting a

mystery message into a cover question, we create what is called as a stego-object. The beneficiary should remove the message from the stego-object subsequent to sending the embedded object. Furthermore, numerous users utilized stego-key for security purposes, sending these keys to a recipient and after that concentrate the message utilizing these stego-keys. The extraction technique is the same as the inserting strategy. Recipient side concentrates on the message in the light of inverse encryption calculations [Zhang and Wang (2006); Kahn (1996)]. All fields are related to information hiding or covert communication such as cryptography, steganography, watermarking and covert channels. However, steganography is tied with making the messages/communication between two parties in such a way that the presence of embedding information of stego-question isn't obvious to anybody. In other words, the embedded message is secure against the intruder or aggressors. All algorithms need some desires which are essential for its calculation to work accurately. The essential and fundamental prerequisites or requirement of steganographic calculations is payload, imperceptibility, and robustness [Johnson and Jajodia (1998)]. These attributes will be taken into account in this research during the design of the new approach.

This paper is organized in the following way. Section 2, presents the state of the art, introducing the similar approaches that the proposed implementation will be compared against. Section 3 presents the proposed approach in detail. Section 4 presents the dataset, experiments and the evaluation results. Finally, Section 5 concludes this work by re-presenting the key findings, limitations and proposals for future work.

2 Related work

There are numerous methods and technologies created and utilized for steganography [Singh, Yadav, Raj et al. (2018); Darabkh, Dhamari and Jafar (2017); Prasad and Pal (2017); Ishaque, Khan and Sattar (2011)]. Every approach has its own advantages and disadvantages. A few methods have high payload limits and great softness and blurriness depend on the chose cover for covert or unknown information, concealing (Spatial space systems). However, they are more vulnerable against assaults (Noise tossing, rotation, revolution, resizing and so forth) while other approaches are stronger against factual or statistical assaults. This implies that there is a tradeoff between Payload, Imperceptibility, and Robustness [Ker (2005)].

Steganography utilize pictures, recordings, and system protocols, and sound for data camouflage. A few methodologies for advanced steganography have been proposed. These methodologies depend on LSB substitution, edge-based inserting, and pixel marker-based inserting. This section presents some existing methods based on LSB techniques and their advantages and disadvantages as well as comparisons to the proposed method.

2.1 LSB (Least significant bit algorithm)

Least Significant Bit (LSB) is one of the oldest steganography calculations that insert the message bits in the stego-image. It is notable information, concealing strategically utilized broadly due to its straightforwardness. It leads an adjustment to the minimum critical piece of the stego-picture pixels, which change just the quality of the covering.

This change is slight to the point that the human eye may not see it. The LSB conceals the message bits into the picture pixels either in a successive or randomized design. In the occurrence of RGB images in which every pixel has three channels or assets (Red, Green and Blue ranges from 0-255 every; Bit Depth=24 bits), we first separate the Red, Green and Blue channels from the cover picture and after that displace our covert message bits with the LSBs of one of the three channels and associate the three channels toward the end to make the stego picture [Zhang, Geng and Xiong (2009); Solanki, Chuahan and Desai (2015); Janakiraman, Amirtharajan, Thenmozhi et al. (2012)]. To clear up the possibility of LSB based steganography, let us consider the convoying eight pixels and secret letters in order "A" as shown in Tab. 1.

Table 1: LSB based embedding

Secret letter		**Binary**	
A		**01000001**	
Decimal	**Binary**	**Decimal**	**Binary**
141	1000110**1**	40	0010100**0**
130	1000001**0**	132	1000010**0**
118	0111011**0**	75	01001011
96	01100000	119	01110111
Decimal	**Binary**	**Decimal**	**Binary**
140	1000110**0**	40	00101000
131	1000001**1**	75	01001011
118	0111011**0**	74	01001011
97	01100001	119	01110111

After embedment, the changed bits are shown as bold in Tab. 1. The pixel values are 50% different. Converted information is normally covered up in the blue channel of RGB images which are less perceptible by the HVS (Human Visual System). LSB Replacement schemes have a high payload limit, better imperceptivity (in light of cover picture choice) however, they are more vulnerable against Steganalysis attacks [Karim, Rahman and Hossain (2011); Muhammad, Ahmad, Rehman et al. (2017); Grover and Mohapatra (2013); Akhtar, Johri and Khan (2013); Veena and Arivazhagan (2018), Chikouche and Noureddine (2017), Rahman, Masood, Khan et al. (2019), Nolkha, Kumar and Dhaka (2020), Rachael, Misra, Ahuja et al. (2020)]. Fig. 2 elaborates the concept of the LSB.

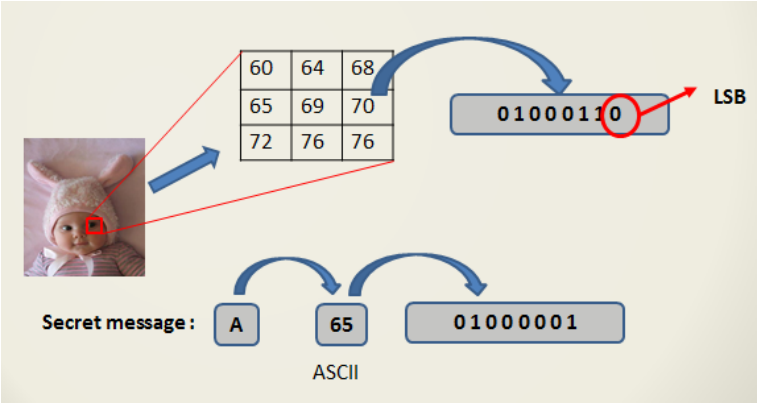


Figure 2: Least significant bits

Zhang et al. [Zhang, Geng and Xiong (2009)] proposed a new pixel esteem (value) differencing procedure; for data embedding near the goal pixel, it used the three pixels. It utilizes a crucial k-bit LSB technique for mystery information inserting with high refinement regard where the number of k-bit is assessed by pretty much three pixels. It basically uses a perfect pixel adjustment method on target pixels to hold better visual quality and high breaking point. Histogram of stego-picture and cover-picture is generally the same in the great position of the procedure, however, the dataset for tests is close to nothing [James (1990); USC (2019)].

Amirtharajan et al. [Amirtharajan, Akila and Deepikachowdavarapu (2010)] performed a similar investigation of picture steganography in which singular sorts of techniques, like OPAP (Optimal Pixel Adjustment Procedure), IP (Inverted Pattern Approach), Mod10 were presented with their relating preferences and weaknesses. All the methodologies were incapable of authentic or factual assaults with the avoidance of DCT, which have some protection against some quantifiable ambushes [Dahiya (2017); Shehab, Elhoseny, Muhammad et al. (2018)].

Ibrahim et al [Ibrahim and Kuan (2011)] developed a system called Steganography Imaging System (SIS) which uses a secret key to enhance the security of the proposed technique. The creators have influenced the use of compacting to pack to the mystery or obscure key and secretive data to construct the payload. The pack record is then changed over into bits stream and concealed in the cover picture. The proposed calculation has a high payload cut-off and better nature of stego-pictures but this strategy is proposed only for BMP arrangement or configuration pictures.

Chatterjee et al. [Chatterjee and Das (2018)] showed that cryptography and steganography are two well-known techniques utilized for the reason. The proposed technique builds up another information concealing plan joining the ideas of cryptography and steganography to upgrade the security of correspondence. Such strategies are sound as the number of mystery keys utilized for encryption changes with the extent of the message. Meanwhile it produces keys that are autonomous of each other which anticipate hacking of all keys together. Therefore, greater security is achieved in the correspondence channel. The technique is assessed by estimating the contortion of the inventiveness of picture record figuring crest motion to-clamor proportion.

Babita et al. [Babita and Manprit (2009)] proposed a new image steganography method, to embed data bits using 4 LSB of each RGB channel. They focus on separating to improve the possibility of the stego-images. Further, they also encode the refinement of the cover and stego-picture as key information. To isolate the covered data in separating stage, the stego-picture is added with key data. The major demerit of the proposed scheme is the limitation on the size of the secret data/image.

Bailey et al. [Bailey and Curran (2006)] proposed a stego shading cycle (SCC) procedure for shading pictures that conceals information in various channels of the spread picture reliably. i.e., the basic riddle bit is disguised in pixel1's red channel, the second mystery piece is hidden in the green channel of pixel2 and the third puzzle bit is covered in the blue channel of pixel3, etc. The basic confinement in the SCC method is that the mystery data is presented in spread picture pixels in a settled cyclic and effective way. Therefore, attackers can, without a considerable amount of a stretch, find this methodology if stun data from a couple of pixels is suitably separated.

Gutub [Gutub (2010)] proposed a high payload pixel pointer procedure (PIT) in which one channel is used as a marker and the other two channels are data channels. The proposed procedure implored the riddle data in both of the data occupies in a predefined cyclic manner. The restrictive results exhibit as far as possible and better delicate nature of the organized figuring and keep up a vital separation from the key trade overhead. The major weakness behind this procedure is that it is possible for a subject to have a picture with pointer bits which can result in the low payload. Additionally, these strategies stow away settled quantities of bits in every pixel which can get more changes from the cover picture, if we install a greater number of mystery bits in every pixel. The sincere detention in the proposed technique is that the riddle information can be expelled adequately if an attacker finds the estimation being used for the message disguising. This is possible because the secret data is fitted as a fraud and not encoded. Moreover, this procedure results in stego pictures of a low quality which can be recognized using HVS.

Karim et al. [Karim, Rahman and Hossain (2011)] introduced another way to deal with the upgrade of the security of the existing LSB substitution technique by including one additional obstacle of mystery key. In this technique, the mystery key and red channel are utilized as a pointer while green and blue channels are information channels. Because of the verified key bits and red channel LSBs, the puzzle data bits are embedded either in green direct or in blue channel. In case either the bit of red channel LSB or riddle key piece is 1, then the LSB of green channel is supplanted with the mystery message bit. Generally, LSB of the blue channel is displaced with the mystery bit. This methodology has a similar payload as LSB based methodologies, yet it builds the security by utilizing the mystery key. An intruder has to invest significant effort to remove the mystery data without the right mystery key.

Muhammad et al. [Muhammad, Ahmad, Farman et al. (2015)] presented an ensured strategy for shading picture steganography using Grey-Level Modification and Multi-level Encryption. The security of information between two social gatherings is a huge issue in this exploiting edge of an area. To adjust these issues, the researchers proposed a procedure for RGB pictures in light of diminish or Grey-Level Modification (GLM) and Multi-level Encryption (MLE). The riddle key and mystery data are encoded using MLE

figuring before mapping it to the dull dimensions of the spread picture. By then, a transposition work is associated on spread pictures going before data stowing endlessly. The utilization of transpose, riddle key, MLE, and GLM incorporates four exceptional dimensions of security to the proposed figuring making it very troublesome for a malicious customer to remove the primary mystery information. The proposed plan gives a powerful, proficient and efficient approach to conceal mystery data inside the extent picture. The principal focal points of the proposed plan are improved nature of stego pictures, high subtlety, and upgraded power. The significant deficiency of this strategy is its defenselessness to various assaults (editing, scaling and clamor assaults) that exist in all spatial space methods including the current five plans. Since spatial space is utilized in the proposed methodology, the concealed information cannot be completely recouped if the picture is compacted, scaled or assaulted with commotions.

Grover et al. [Grover and Mohapatra (2013)] presented an adaptable or adaptive edge-based LSB substitution organism which covers up three (3) bits of covert information in edgy or tense pixel and two (2) covert bits in non-restless or non-edgy pixels in the blue channel of the RGB image. This approach has a high payload limit and is stronger when compared with the basic LSB substation technique. This is because the covered information is initially, separated into two sets and subsequently is embedded in the cover image, beginning from the pivotal pixel and navigating through the entire image increasing its strength and robustness. Rashid et al. [Rashid and Majeed (2019)] have identified the problems and solutions of edge-based image steganography.

Akhtar et al. [Akhtar, Johri and Khan (2013)] presented a unique variety of LSB based steganography approaches which enhances the nature of the stego image by bit-reversal technique. To randomly scatter the covert message bits inside the cover image pixels, the RC4 algorithm has been utilized as a part of the request to build the strength of the proposed approach. The utilization of RC4 calculation or algorithm for randomization makes it troublesome for an intruder to detach the covert message.

3 Proposed methods

All the conveying bodies need confidentiality, integrity, and authenticity of their secret data. Distinctive methodologies are utilized to adapt these security issues like digital certificates, digital signature, and cryptography. But these techniques alone cannot be traded off. Steganography is the best answer to these issues as it hides the presence of secret information. This research work presents a novel and enhanced technique in RGB color space.

3.1 Mathematical modeling of proposed methodology

Suppose the secret message is to be embedded is denoted by M in the carrier image (I). F demonstrate the flipped image, Mdv denotes differing values of the secret message. R is red, G is green and B denotes blue channels of the color image and the stego-image is S. In the entire procedure as a part of embedding in Eqs (1)-(6) six functions named as α, β, γ, Ω, δ and φ are utilized as given.

$$F = \alpha(I) \tag{1}$$

$$R, G, B = \beta(F) \tag{2}$$

$$\text{M dv} = \gamma(M, R) \tag{3}$$

$$\text{M dv}' = \Omega(\text{M dv}) \tag{4}$$

$$B' = \delta(B) \tag{5}$$

$$S = \varphi(M\ dv', B') \tag{6}$$

The principal work (α) accepts I as info and returns (F) which is the flipped picture. The second function (β) divides (F) into red, green and blue channels, in which red channel (R) is used to calculate the difference while the blue channel (B) for embedding. (γ) is the third function that calculates the difference between the pixel value of (R) and corresponding secret message (M), (ASCII code of a letter). For more robustness, the different values (Mdv) are encrypted using the fourth function (Ω) with the help of MLEA which returns (M dv′). Before embedding, the blue channel (B) is shuffled using a magic matrix (MatLab function) using the fifth function (δ) which gives (B'). Finally, the stego image (S) is generated using the sixth function (φ) by embedding encrypted difference values (M dv′) in the shuffled blue channel (B′) using the proposed steganographic algorithm. On the recipient side, the invert activity needs to apply so as to extricate the desired message. The following six functions are utilized to extract the original massage in Eqs (7)-(12) as described below.

$$F = \alpha^{-1}(S) \tag{7}$$

$$R, G, B = \beta^{-1}(F) \tag{8}$$

$$B' = \delta^{-1}(B) \tag{9}$$

$$\text{M dv}' = \varphi^{-1}(\text{B}') \tag{10}$$

$$\text{M dv} = \Omega^{-1}(\text{M dv}') \tag{11}$$

$$\text{M} = \gamma^{-1}(M^{dv}, R) \tag{12}$$

In the decoding procedure, function (α^{-1}) applies to the stego-image (S) and proceeds a flipped image (F). Eq. (8) divides (F) into red, green and blue channels. Using function (δ-1), the blue channel (B) is then shuffled using a magic matrix (MatLab function) to get the shuffled blue channel (B'). The encrypted difference values (M dv′) are then extracted from (B') by using Eq. (10). To get the original difference values (M dv), function (Ω-1) is used, which passes the encrypted difference values over MLEA in reverse order. Finally, the original message (M) is obtained by using Eq. (12) or function (γ^{-1}) by calculating the difference between the pixel value of the red channel (R) and corresponding message difference value (Mdv). Figs. 3 and 4 describe the whole method.

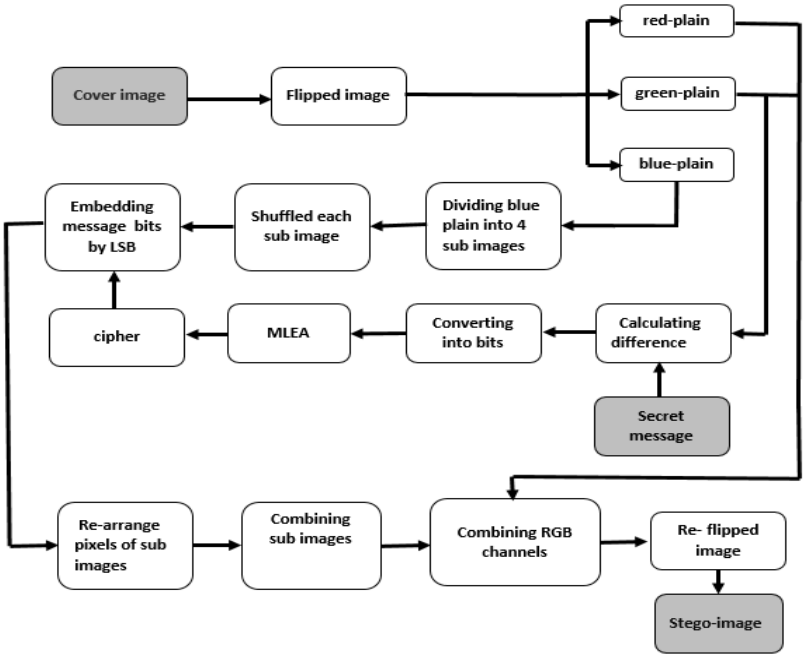


Figure 3: Overview of proposed steganographic approach

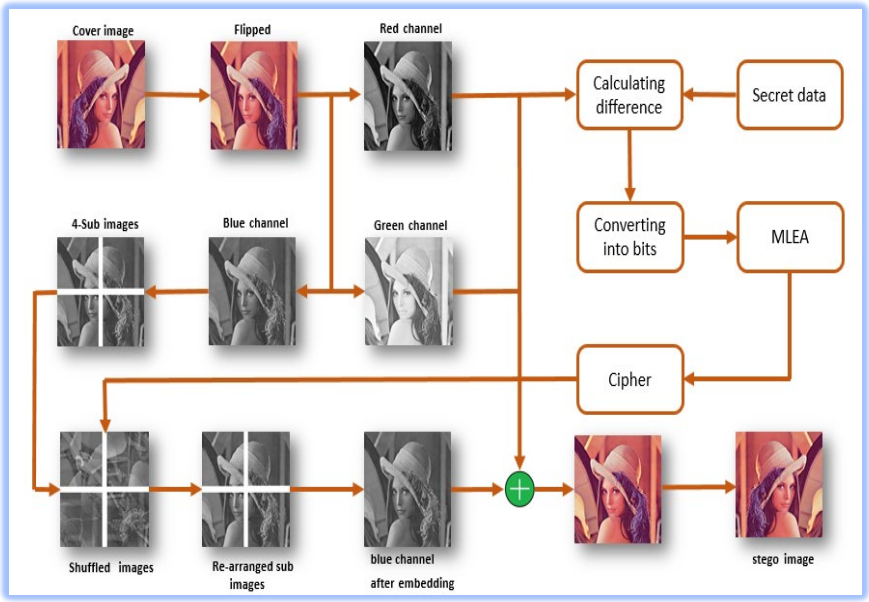


Figure 4: Detail graphical representation of proposed method

3.1.1 Flipping the cover image

We flip the cover image by 180o for enhancing the security layer and also to create confusion for attackers. Because we embed secret data in the flipped image and after

completing the embedding process, then convert the flipped image to its original form, i.e., the cover image. In such a case, if someone wants to attack the stage-image, he/she assumes that the embedding on the stage-image starts from 1st pixel, then 2nd and 3rd respectively. If the attacker attempts to extract the secret message, it will not be in its original form (secret data) as explained in Figs. 3-6. The following example also explains the whole process.

Consider the following cover image:

1	2	3
4	5	6
7	8	9

After flipping the image looks like:

9	8	7
6	5	4
3	2	1

Let us suppose the secret data to be embedded is 'hello', the resulting image is shown below:

9h	8e	7
6l	5l	4
30	2	1

After embedding the flipped image into its original form considered as a stego-image is:

1	2	3o
4	5l	6l
7	8e	9h

This image will be used by the attackers and the message they extract will be very different from the original message. Therefore, we flip the cover image to increase its security against assaults.

3.2 Shuffling by magic matrix

Magic matrix is a MatLab function that returns a matrix of a given size having the following properties.

- The magic matrix does not contain any repeated numbers.
- All the numbers inside the enchantment network are not exactly or equivalent to the result of lines (rows) and segments (columns).

- The sum of all rows, columns, and diagonals gives the same number.

Based on above properties, we can shuffle the pixels of a cover image in a way, which can easily then re-arrange in its proper order. This rearranging strategy is additionally clarified utilizing a straightforward precedent. Consider a cover picture (Ic) of size $3x3$, i.e., Ic={40,56,21,55,65,52,44,78, 79} to rearrange. For this purpose, we need to create an enchantment framework (Mm) of a size equivalent to the measure of the cover picture and let (Is) be the rearranged picture.

$$\text{Ic} = \begin{bmatrix} 40 & 56 & 21 \\ 55 & 65 & 52 \\ 44 & 78 & 79 \end{bmatrix} \quad \text{Mm} = \begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix} \quad \text{Is} = \begin{bmatrix} 78 & 40 & 52 \\ 21 & 65 & 44 \\ 55 & 79 & 56 \end{bmatrix}$$

The enchantment framework demonstrates the area where we need to move the pixel esteems i.e., the primary pixel esteems 40 moved to the area of 1 of magic matrix (row 1, column 2), 2nd, 56 to (row 3, column 3), 3rd, 21 to (row 2, column 1), 4th, 55 to (row 3, column 1), 5th, 65 to (row 2, column 2), and so on.

3.3 Embedding algorithm

The embedding algorithm is based on RGB color space. The cover image is first flipped horizontally and then divides into its red, green and blue channels. The blue channel is used to hide the secret data while the red channel is used for calculating the difference between the original message and pixel intensity. Before embedding, the blue channel is divided into four equal blocks and then every block is shuffled using a Magic matrix (MatLab functions which return a matrix that has not any repeated numbers and sum of all columns, rows, and diagonals are same). On the other hand, the secret data (ASCII codes) were subtracted from the corresponding pixel values of the red channel. These distinctions esteem at that point scrambled utilizing staggered encryption calculation (MLEA). In the last step, the scrambled distinction esteem in a cyclic mode (i.e., two bits for each square) are inserted into the rearranged blue channel. The primary strides of installing calculations are portrayed as a flowchart in Fig. 5.

We used the blue channel for embedding secret data which are divided into four equal blocks. We select 8 bits of secret data, embed the first two bits in the first block of the blue channels, 3rd and 4th bits into the 2nd block, and the last four bits into the fourth block of the blue channels respectively.

3.4 Extraction algorithm

In the extraction algorithm, the embedding algorithm is performed, but in reverse order. First, the stego-image is flipped and divided into the red, green and blue channels. The blue channel is then divided into 4 equal blocks and every block is shuffled by a magic matrix (MatLab function). The LSB of two pixels from each block is extracted cyclically up to the end of embedded data. The extracted data is then decrypted using MLEA (means apply different encryption operation i.e., replacing, combination, XOR on secret data for increasing its security) and convert every eight-bit combination into decimal. At the end, the difference is calculated, between corresponding red channel pixel values and extracted values. The process is depicted in Fig. 6.

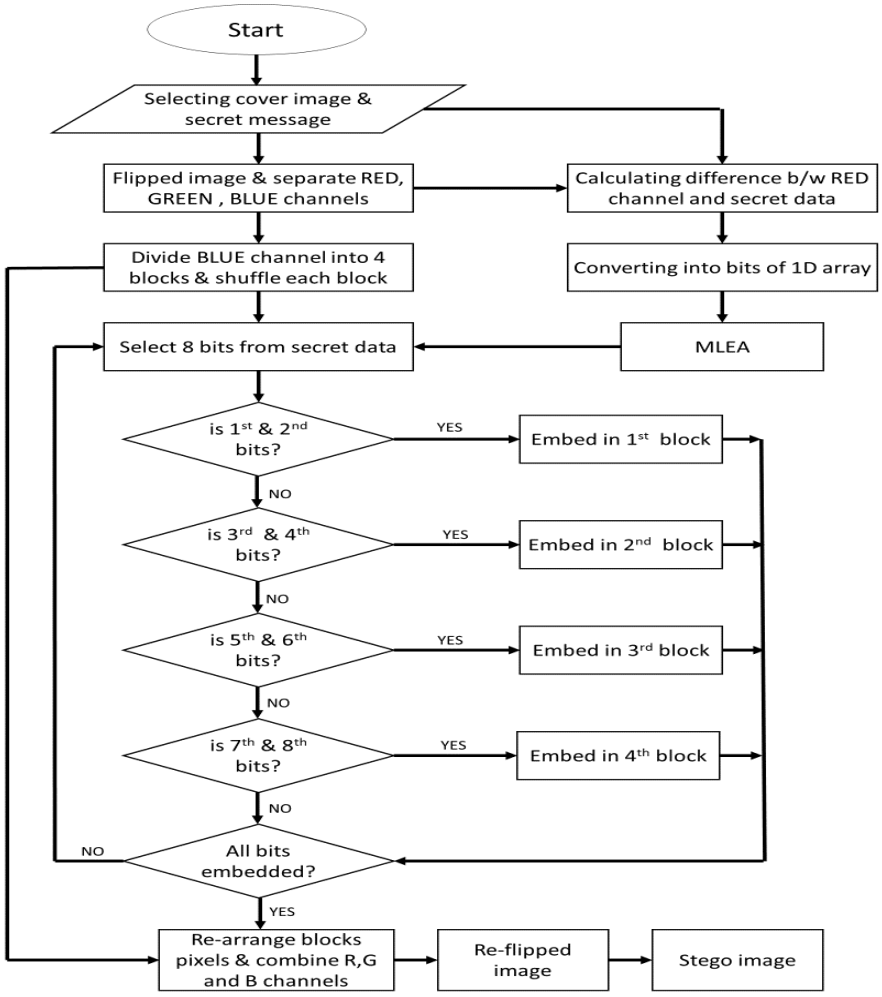


Figure 5: Brief description of embedding algorithm

3.5 MLEA (Multi-level encryption algorithm)

The MLEA encodes the mystery information before it is installed in the transporter picture. This calculation applies distinctive encryption activities on mystery information, expanding its security. The principle ventures of MLEA are given in the algorithm. In the decryption algorithm, all the steps of the encryption algorithm are used but in reverse order. The flowchart of MLEA is given in Fig. 7.

Step 1: Taking XOR of all bits by 1.

Step 2: Taking 8-bits combination & Replace first four bits by last four bits.

Step 3: Left circular shift to every 8-bits combination.

Step 4: Divide whole bits array into 2 blocks (i.e., b1 and b2) and then Taking XOR of on the base of b1 i.e., if b1 (i)= 1 then XOR b2 (i) by 1.

4 Experimental results and discussion

The proposed method, simple LSB method, Pixel Indicator Technique (PIT) [Gutub (2010)], Karim's scheme [Karim, Rahman and Hossain (2011)], Muhammad et al. [Muhammad, Ahmad, Farman et al. (2015)] are coded utilizing MATLAB R2014a. Various experiments were directed so as to completely survey the effectiveness of the proposed algorithm. The results of the experiments are presented in the following sub-sections.

4.1 Dataset

The Dataset (The USC-SIPI Image Database Volume 3: Miscellaneous) of standard color images downloaded from the website [USC (2019)], was utilized for evaluating the existing approaches against the proposed method. The database contains 50 edgy and smooth color images of size 512×512 including the images of "Lena", "baboon", "peppers", "house" and so on. In this paper, the experiment is conducted on fifty (50) images of various dimensions and formats.

4.2 Quantitative evaluation

In this sub-section, we present the entire procedure of quantitative investigation that is straggled by this examination work. Discussed strategies expressed in this paper are coded utilizing MATLAB R2014a and are tentatively surveyed by the given three distinct perspectives:

- **Perspective 1:** Embedding the same amount of data in different images of the same size.
- **Perspective 2:** Hiding a different amount of data in the same image of the same dimensions.
- **Perspective 3:** Embedding the same amount of data in the same image of distinct dimensions.

First of all, using perspective 1, in color images of different formats having size 256×256, a text of 8 KB is embedded; this experiment is conducted on 50 images, Secondly, in perspective 2, hiding four different sizes of text (i.e., 2 KB, 4 KB, 6 KB, 8 KB) in various images of the identical measurement (256×256). This analysis is directed to four standard shading pictures. In perspective3, we use similar pictures of perspective 2 with various resolutions (128×128, 256×256, 512×512 and 1024×1024) and the size of embedding secret text of 8 KB.

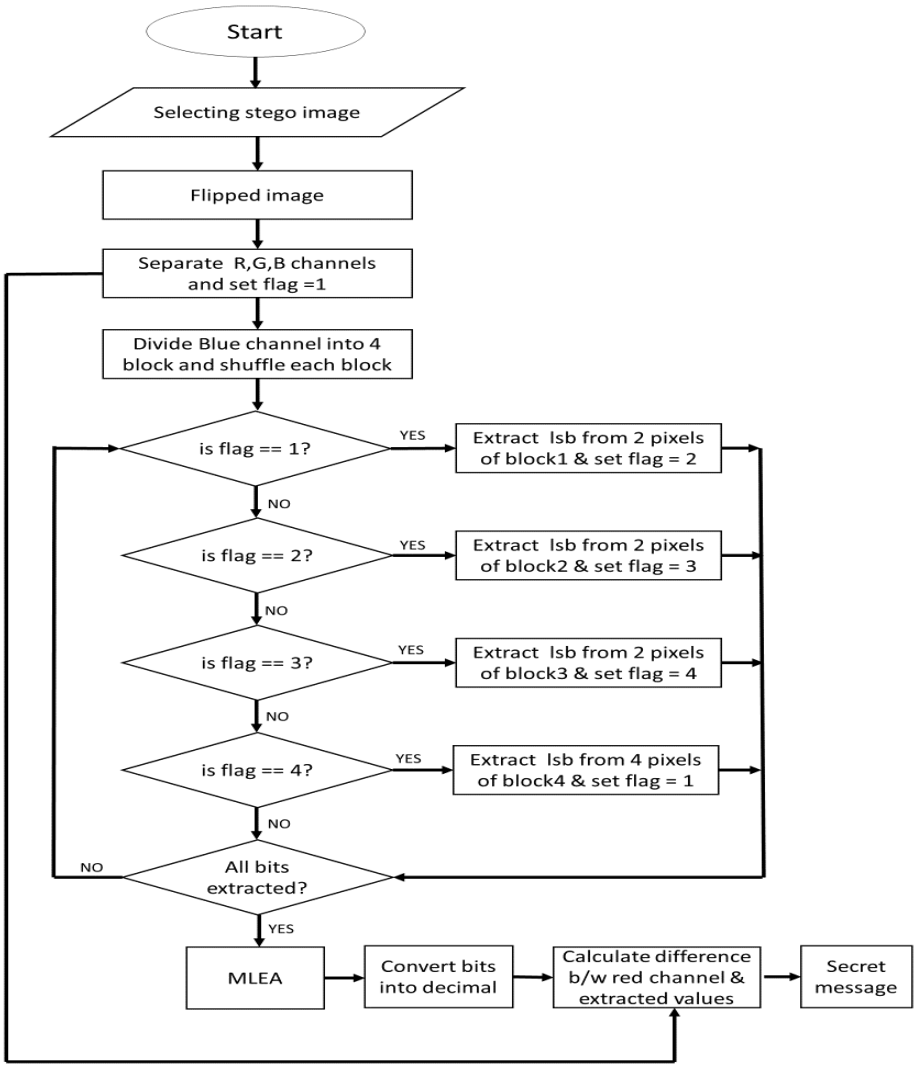


Figure 6: Brief description of extraction algorithm

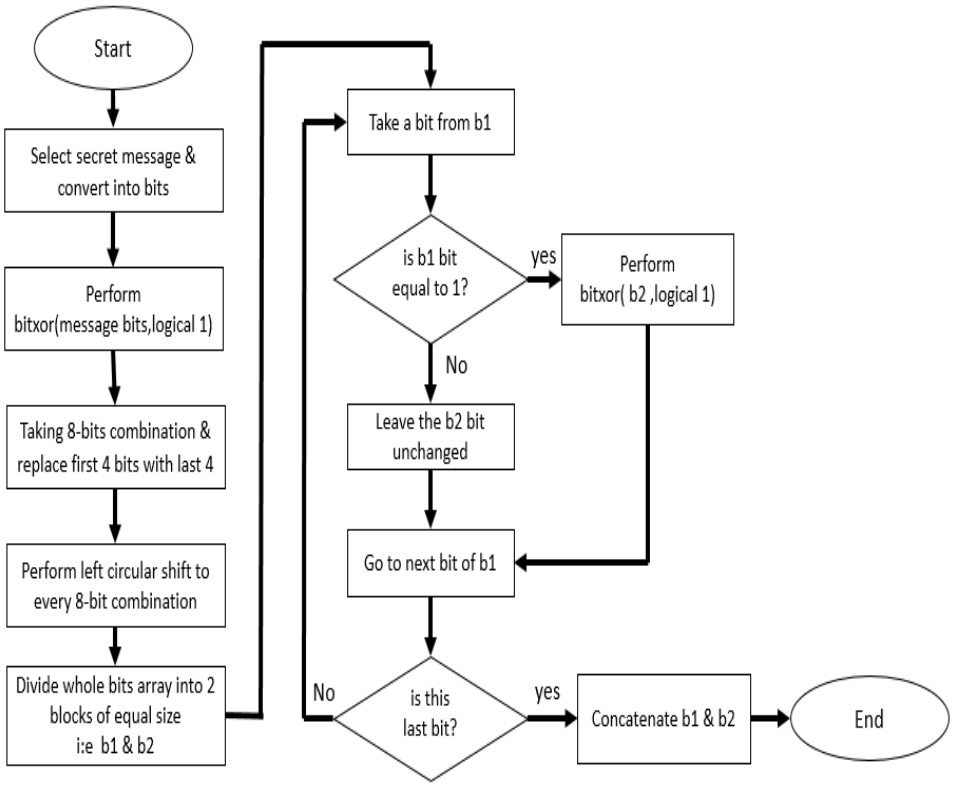
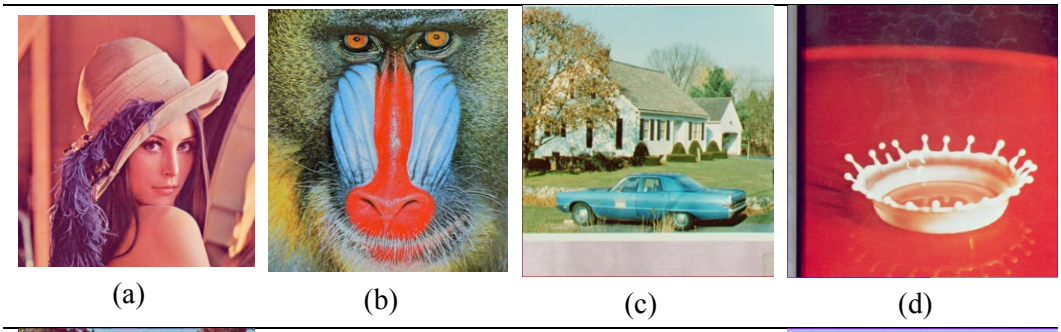


Figure 7: Description of multi-level encryption algorithm (MLEA)

4.3 Quantitative results and discussion

This section presents the comparison of proposed approach with other existing steganographic procedures such as Classical LSB [James (1990)], PIT [Gutub (2010)], Karim's approach [Karim, Rahman and Hossain (2011)] and Muhammad's et al. method [Muhammad, Ahmad Farman et al. (2015)]. Fig. 8 shows some of the famous images included in the dataset and used for experimental purposes. The overall results of proposed strategies and other existing techniques are specified in Tabs. 5, 6 and 7.

In Tab. 2, we present the experimental results of our planned work with other four existing steganographic techniques based on PSNR for perspective 1. As mentioned in perspective 1 same size of the text (8 KB) is embedded in the same dimension (256×256) of different images. The average value of PSNR over one hundred images (100) proves the edge of this research work over these existing mentioned schemes.



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 8: Perspective 1; Data set of cover images (a) Lena (b) Baboon (c) House (d) splash (e) Scene (f) peppers (g) F-16 (h) Building

Table 2: Results of perspective 1; PSNR correlation of proposed strategy with existing techniques

No.	Name of Image	ClassicLSB Method PSNR (dB)	PIT PSNR (dB)	Karim's Method PSNR (dB)	Muhammad Khan's Method PSNR (dB)	Planned Scheme PSNR (dB)
1	Peppers	55.8221	48.2451	50.2771	51.9974	59.4472
2	Baboon	54.7317	47.2843	48.0941	51.8975	62.3178
3	House	54.0623	52.3355	51.9792	51.8654	68.0819
4	Trees	55.2567	47.5473	50.3765	51.8989	56.4069
5	Lena	46.5303	43.0304	45.6554	45.8765	63.9871
6	Hackers	47.9587	42.4034	43.8334	50.5343	57.1400
7	Masjid	48.1246	45.2012	43.8094	52.5776	56.3665
8	Couple	47.4291	45.3525	46.2989	51.7058	55.3524
9	Design1	48.9282	46.8431	47.3121	54.5235	56.5353
10	Design2	39.1159	37.1625	38.6771	43.0396	56.3767
11	Baboon3	45.1242	37.7588	40.0142	51.3729	51.4163
12	F16jet	54.5341	51.9206	48.0898	53.5342	68.2059
13	Building1	42.4307	43.3105	43.3338	49.3452	58.4211
14	Moon	54.2198	48.9336	49.5265	53.4565	56.5115
15	Trees2	42.3737	39.5368	39.1645	50.4326	52.5408
Avg. of images	**100**	**49.1094**	**45.1234**	**45.7678**	**50.9370**	**54.6071**

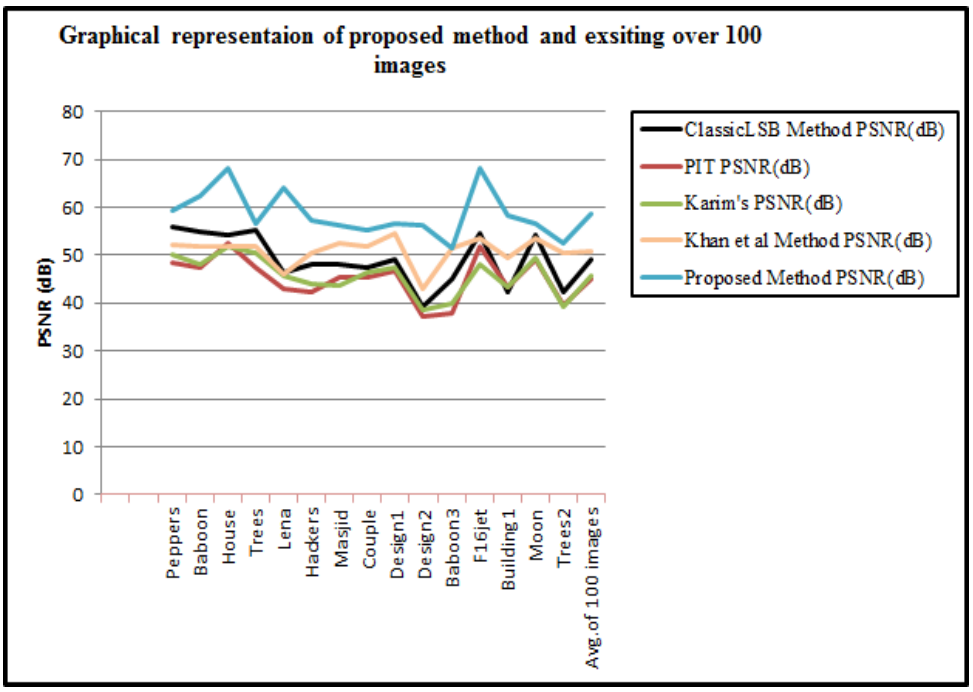
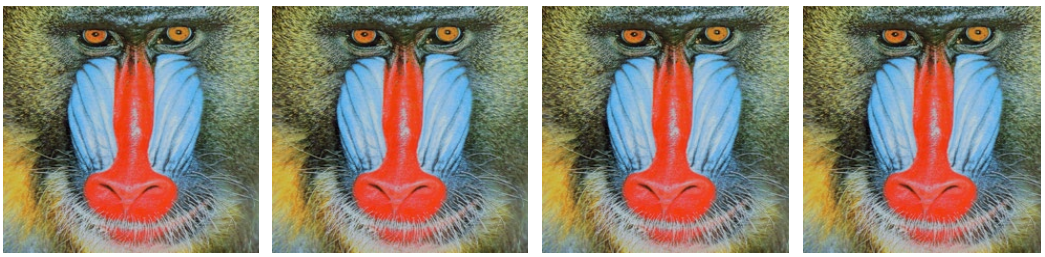
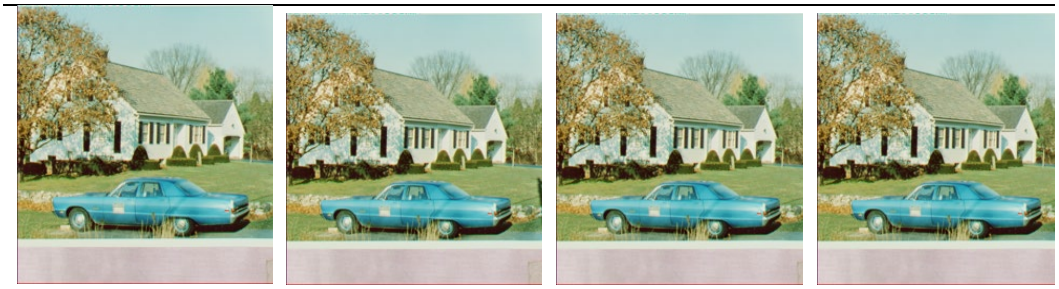


Figure 9: Graphical representations of proposed method and existing over 100 images

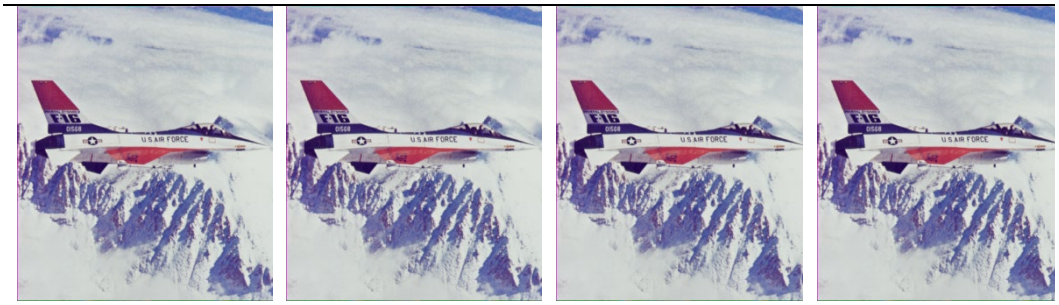


(a)	(b)	(c)	(d)
2 KB, PSNR= 68.8457	4 KB, PSNR= 65.9619	6 KB, PSNR= 63.4316	8 KB, PSNR= 62.9988



(e) 2 KB, PSNR= 74.4506 | (f) 4 KB, PSNR= 71.8292 | (g) 6 KB, PSNR= 65.8933 | (h) 8 KB, PSNR= 68.8379

(i) 2 KB, PSNR= 68.6201 | (j) 4 KB, PSNR= 66.0118 | (k) 6 KB, PSNR= 65.8076 | (l) 8 KB, PSNR= 63.1719



(m) 2 KB, PSNR= 74.4506 | (n) 4 KB, PSNR= 71.8292 | (o) 6 KB, PSNR= 65.8933 | (p) 8 KB, PSNR= 68.8379

Figure 10: Data set for perspective 2; (a-d) Baboon (e-h) House (i-l) Lena (m-p) F-16

According to perspective 2; different sizes of text (2 KB, 4 KB, 6 KB and 8 KB) are embedded into four standard smooth and edgy images (Lena, baboon, house, and F-16) of the same size of (256×256) from the dataset. In Tab. 3, the average PSNR of the same stego image of different text size is given where our proposed method is clearly dominating over other mentioned four approaches with a 5.217225% higher score.

Table 3: Results of perspective 2; Comparison of proposed method with other mentioned algorithms based on PSNR with variable amount of cipher embedded in same images of same dimensions (256×256)

Images Name & Dimensions	Secret Msg (KBs)	Cipher bytes	Simple LSB Method	PIT	Karim et al. [Karim, Rahman and Hossain (2011)] Method	Muhammad et al. [Muhammad, Ahmad, Farman et al. (2015)] Method	Planned Scheme
Lena 256×256	2	2410	45.0324	44.3201	46.2742	56.6989	68.6201
	4	4160	49.3832	44.0721	49.8405	54.6276	66.0118
	6	6500	49.3293	43.9245	49.6874	53.2954	65.8076
	8	8120	47.2003	42.3001	49.5747	52.4265	63.1719
	Average		**47.7363**	**43.6542**	**48.8442**	**52.2556**	**65.9028**
Baboon 256×256	2	2410	60.46	48.5814	48.3915	77.5866	76.9997
	4	4160	57.4258	47.8021	48.2189	75.5843	76.9919
	6	6500	55.6814	45.9804	48.0371	75.7645	75.9716
	8	8120	54.7317	46.8912	47.9014	74.7645	75.9988
	Average		**57.0747**	**47.5635**	**48.1372**	**75.9247**	**76.4978**
House 256×256	2	2410	53.4359	53.3206	53.7158	75.4476	75.5506
	4	4160	47.7961	53.8402	53.3388	71.3254	72.8292
	6	6500	52.3782	53.0132	53.0278	65.4332	66.8933
	8	8120	52.0423	51.0755	52.7929	68.5476	69.8379
	Average		**51.4131**	**52.8124**	**53.2188**	**70.1884**	**71.2777**
Peppers 256×256	2	2410	53.5459	54.7359	53.3206	70.7158	75.4476
	4	4160	47.6561	47.6961	53.8402	68.3388	71.3254
	6	6500	54.6582	54.4782	53.0132	57.0278	65.4332
	8	8120	53.7623	53.6423	51.0755	63.7929	68.5476
	Average		**51.4131**	**52.8124**	**53.2188**	**64.9684**	**70.5277**

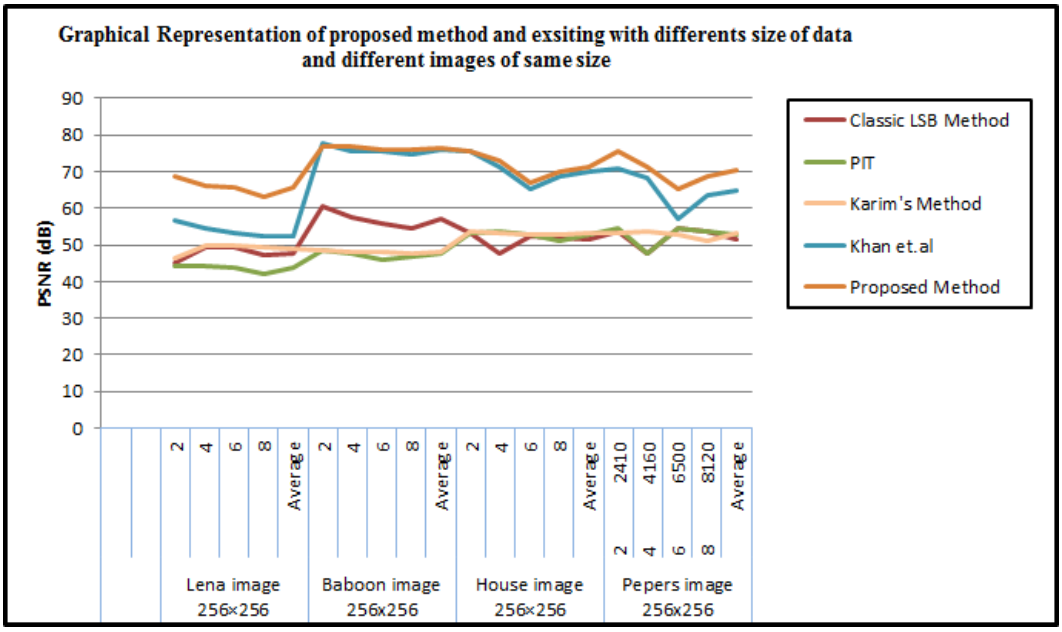
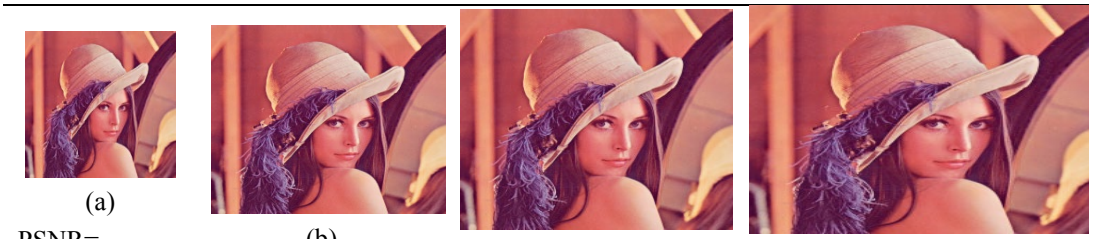
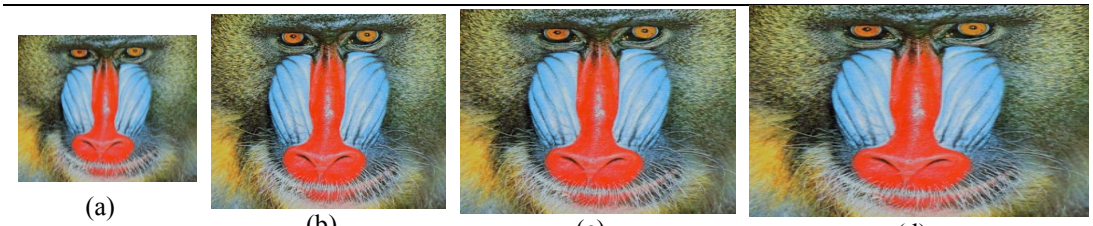


Figure 11: Graphical represntaion of proposed method and exsiting with different size of data and different images of same size

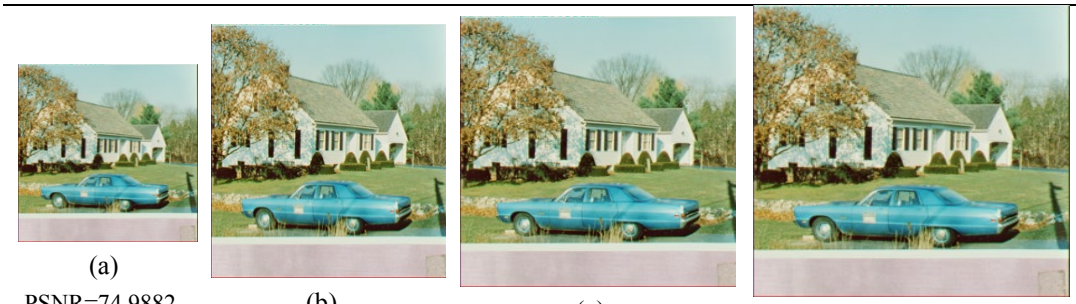


(a) PSNR= 67.6532 (b) PSNR=64.1323 (c) PSNR=60.3323 (d) PSNR=61.1322



(a) PSNR=75.1022 (b) PSNR=56.9587 (c) PSNR=62.8478 (d) PSNR=68.9636

(a) PSNR=62.7678 (b) PSNR=62.7678 (c) PSNR=74.6757 (d) PSNR=75.7527



(a) PSNR=74.9882 (b) PSNR=64.9790 (c) PSNR=64.6510 (d) PSNR=72.567

Figure 12: Images for perspective 3; row wise representation of Lena, Baboon, and House and Building images of different sizes

Tab. 4 shows a comparison based on PSNR between the proposed method and other mentioned approaches using perspective 3. According to perspective 3, same size (8 KB) of text is embedded in different sizes (128×128, 256×256, 512×512 and 1024×1024) of the same images. The results clearly demonstrate that the proposed scheme has better performance compare to other existing schemes with an average of 3.561475% better score.

Table 4: Results according to perspective 3; PSNR based comparison of proposed method with other mention methods, embedding same size of cipher in selected standard images of different size

Image Name	Image dimensions (in pixels)	Classic LSB Method	PIT	Karim's Method	Muhammad et al. [Muhammad, Ahmad, Farman et al. (2015)] Mehtod	Planned Scheme
Baboon Image	128×128	64.9939	48.6326	50.2716	65.6754	75.1022
	256×256	55.8862	50.2321	49.6829	62.4044	62.6587
	512×512	61.882	50.1906	50.0517	59.4242	62.8478
	1024×1024	67.8306	50.2001	50.1669	65.5012	68.9636
	Average	**62.6482**	**49.81385**	**50.0433**	**63.2513**	**65.9681**
Lena Image	128×128	42.4947	45.3316	42.502	58.3332	67.6532
	256×256	49.1185	50.1136	49.5582	52.4134	64.1323
	512×512	49.8277	50.0932	49.9546	57.0021	60.3323
	1024×1024	50.0299	50.1004	50.0645	59.7532	61.1322
	Average	**47.8677**	**48.9097**	**48.0198**	**56.8725**	**60.3125**
House Image 1	128×128	43.5487	44.34547	47.5464	63.6754	62.9882
	256×256	49.4532	49.2130	50.4567	62.4044	62.9790
	512×512	48.8743	50.1110	51.5643	59.3032	74.9110
	1024×1024	51.8974	50.4311	52.4531	65.3212	75.0467
	Average	**48.4434**	**48.5251**	**50.5051**	**62.6760**	**68.9812**
House Image 2	128×128	62.7293	67.5132	62.7137	69.3076	74.8999
	256×256	56.6697	54.7702	53.3682	64.8565	64.9701
	512×512	62.7405	54.754	54.3691	63.3443	64.6510
	1024×1024	68.8288	54.7901	54.6877	72.4734	72.5676
	Average	**62.7421**	**57.95688**	**56.2847**	**67.4932**	**69.2771**

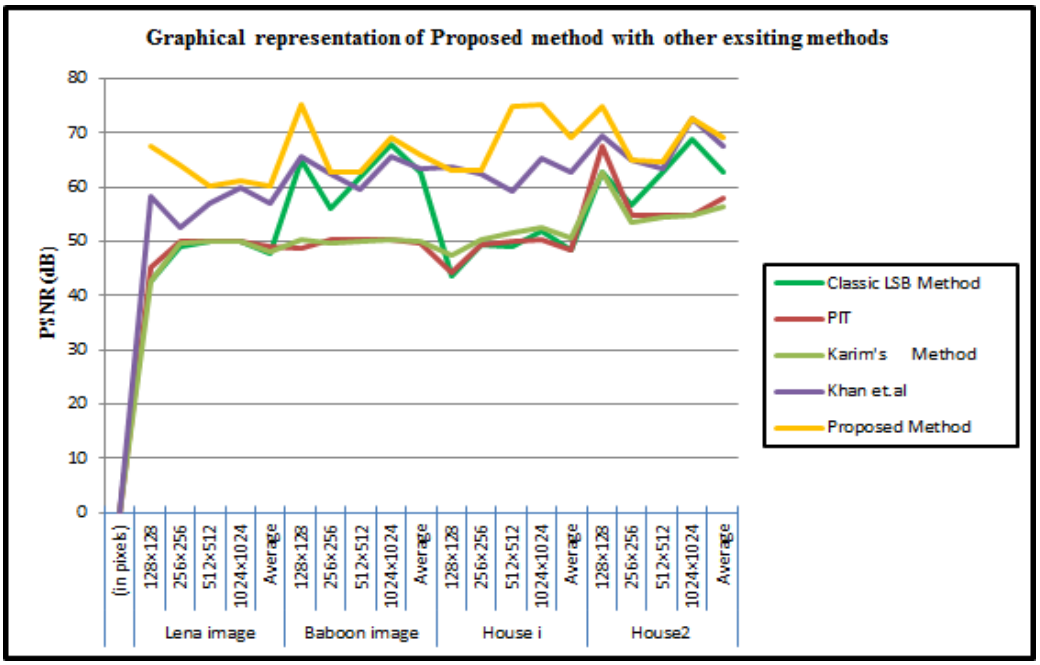


Figure 13: Graphical representation of proposed method with other existing methods with different size of same images

Exploratory impacts of the proposed technique based on image quality assessment metrics including MSE, RMSE, SSIM, and NCC according to perspective 1, perspective 2 and perspective 3 are given in Tabs. 5, 6, and 7 respectively.

Table 5: Experimental results based on MSE, RMSE, NCC and SSIM of proposed method according to perspective 1

Serial No	Image Name	MSE	RMSE	NCC	SSIM
1	Lena	0.6668	0.0395	0.9999	0.9997
2	Baboon	0.0053	0.0482	0.9999	0.9997
3	House	0.667	0.0497	1	0.9999

Table 6: Experimental results based on MSE, RMSE, NCC and SSIM of proposed method according to perspective 2

Image Name& dimensions	Secret message (KBs)	MSE	RMSE	NCC	SSIM
Lena 256×256	2	0.0208	0.0046	1	0.9998
	4	0.0464	0.0095	0.9999	0.9999
	6	0.0664	0.0127	0.9999	0.9997
	8	0.0912	0.0174	0.9998	0.9990

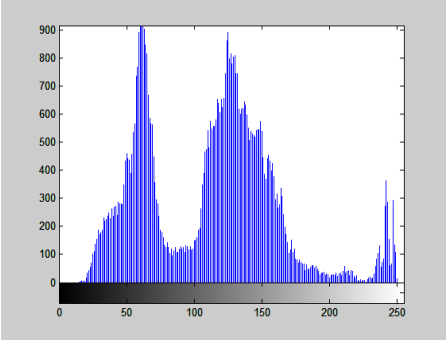
Baboon 256×256	2	0.0203	0.0032	1	0.9999
	4	0.0446	0.0064	1	0.9999
	6	0.0646	0.0087	0.9999	0.9998
	8	0.0893	0.0122	0.9999	0.9997
House 256×256	2	0.0201	0.0027	1	0.9999
	4	0.0453	0.0071	1	0.9996
	6	0.0653	0.0103	0.9999	0.9994
	8	0.0903	0.0150	0.9999	0.9992

Table 7: Experimental results based on MSE, RMSE, NCC and SSIM of proposed method according to perspective 3

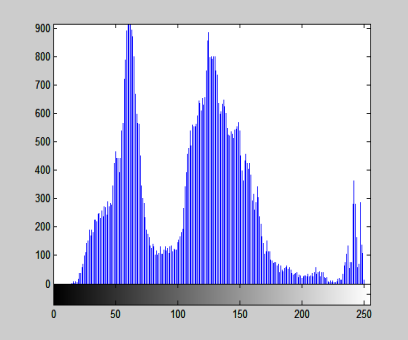
Image Name	Image dimensions (in pixels)	MSE	RMSE	NCC	SSIM
Lena Image	128×128	0.0012	0.0003	1	1
	256×256	0.0724	0.0152	0.9998	0.9998
	512×512	0.0189	0.0046	1	0.9995
	1024×1024	0.0047	0.0011	1	1
Baboon Image	128×128	0.0011	0.0002	1	1
	256×256	0.0660	0.0069	0.9999	0.9997
	512×512	0.0180	0.0032	1	0.9999
	1024×1024	0.0044	0.0009	1	1
House Image	128×128	0.0011	0.0002	1	1
	256×256	0.0700	0.0123	0.9999	0.9994
	512×512	0.0176	0.0027	1	0.9999
	1024×1024	0.0045	0.0010	1	1

Cover image(a)

Stego image(b)



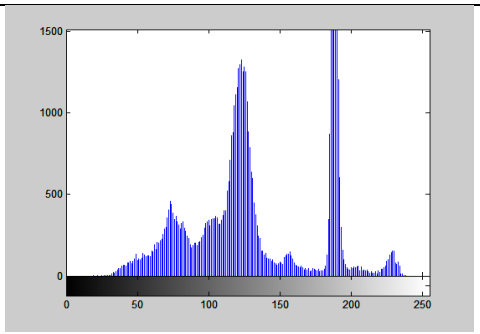
Cover image Histogram



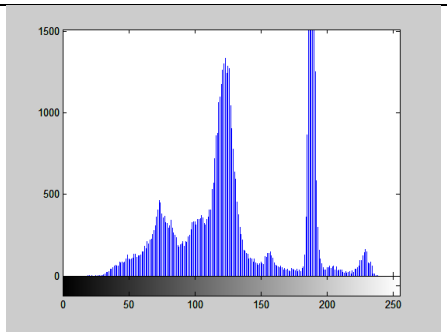
Stego-image Histogram

Cover image (c)

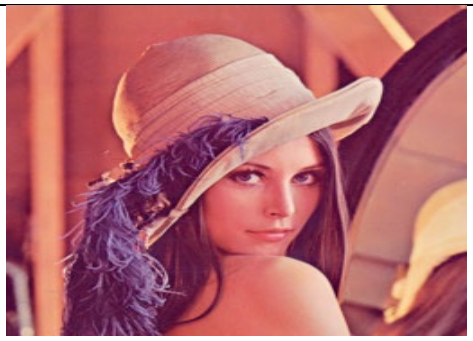
Stego-image (d)



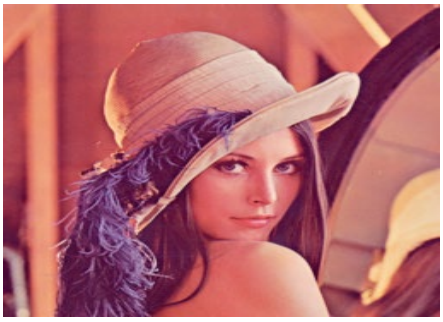
Stego-image Histogram



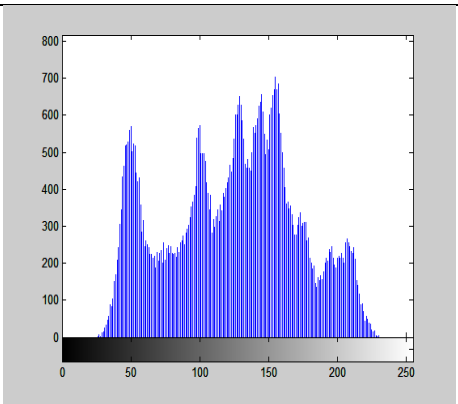
Stego-image Histogram



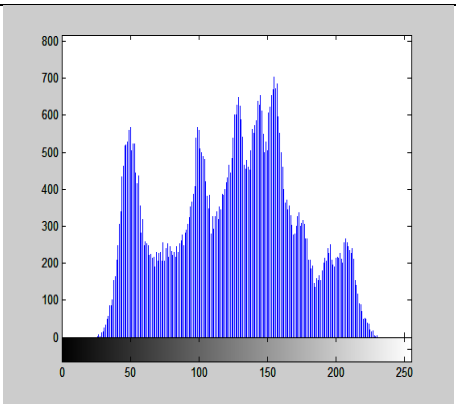
Cover image (e)



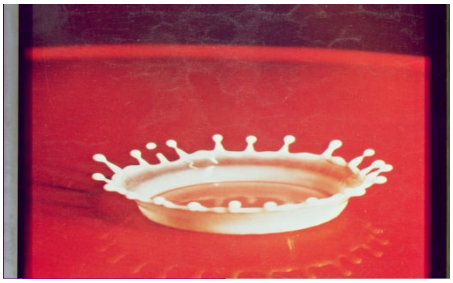
Stego-image (f)



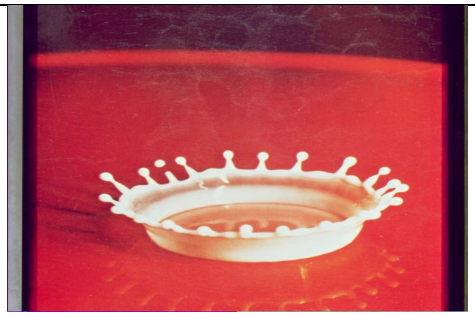
Cover image Histogram



Stego-image Histogram



Cover image (g)



Stego-image (h)

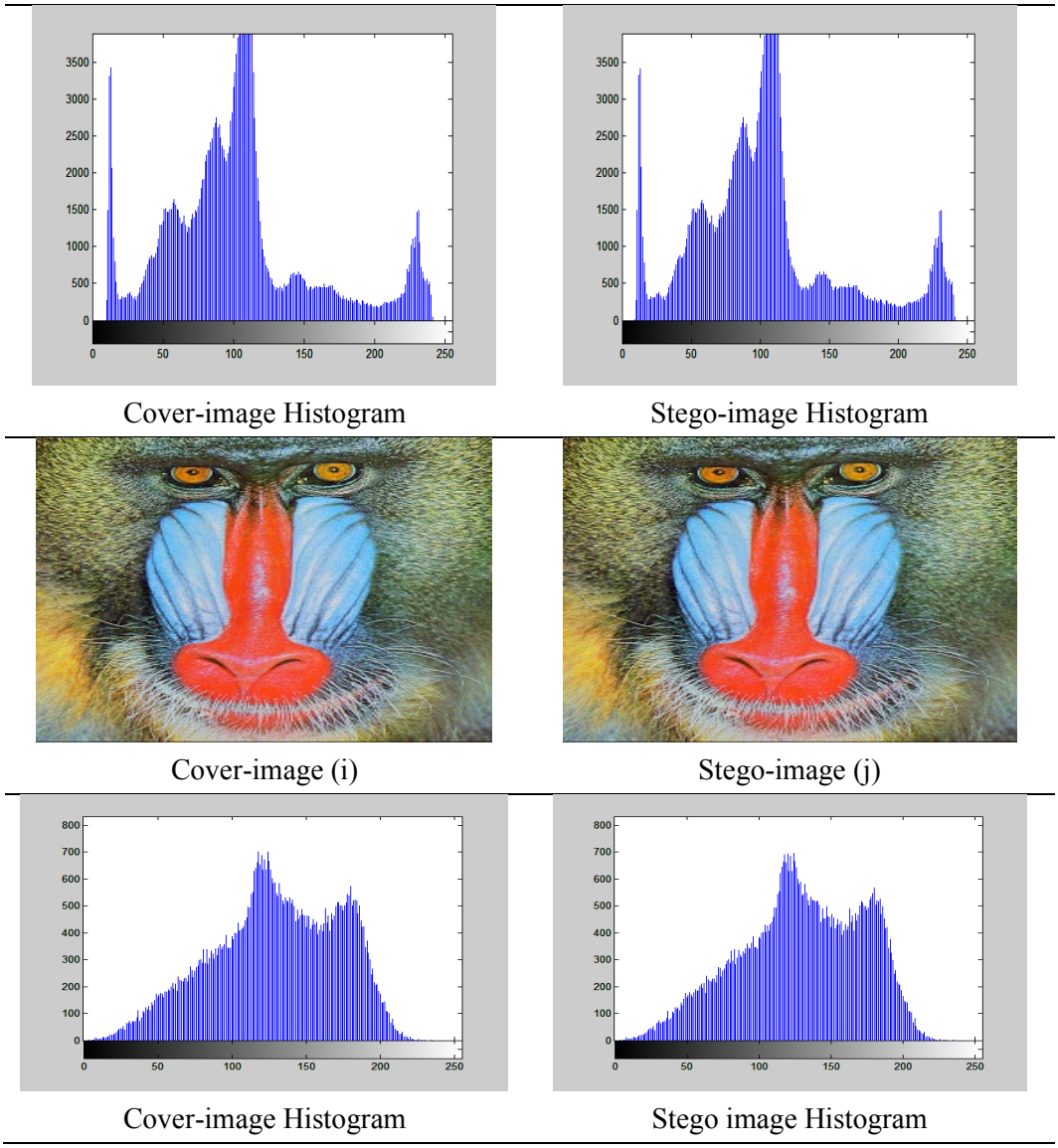


Figure 14: Performance anlysis of a proposed scheme of different images of the same size (256×256) using HVS based on quality of stego images with their Histogram

5 Conclusion and future work

This research proposed an improved steganographic procedure in RGB color space. The implementation was evaluated against the state of the art and achieved 3.6701% average higher score for PSNR correlation and 5.217225% in PSNR with variable amount of cipher embedded in same images than the next best existing approach. Embedding same size of cipher in images of different size, resulted to a 3.561475% better score. The new approach increase the strenght of steganography and expel the reiteration of most normal

letters. The work aims to enhance the security of the existing methods for hiding information. We have demonstrated a new and upgraded procedure in RGB shading space, to make it more powerful and secure than existing approaches. A limited number of statistical analysis metrics were used in the evaluation section. A future extension could include more statistical metrics such as Weighted Mean Absolute prediction Error (WMAE), Mean SSIM (MSSIM), Outlier Ratio (OR), Image Fidelity (IF), Normalized Absolute Error (NAE), Normalized MSE (NMSE), Difference Mean Opinion Score (DMOS) and Histogram Error (HE) to analyze the results. There are many image quality assessment metrics, but during the evaluation, we found various limitations in each quality assessment scheme. Other significant limitations of this work include its weakness in various assaults such as decoration, scaling and clamor assaults. Future work can focus on the elaborating steganography in the context of image quality assessment. Also, an advanced encryption algorithm can be investigated to make this work more effective and powerful. Furthermore to prevent the stego-images from various attacks and improvements to current algorithm, they can be presented in frequency domain.

Funding Statement: This research is supported by the Higher Education Commission (HEC), Pakistan through its initiative of National Center for Cyber Security for the affiliated Security Testing- Innovative Secured Systems Lab (ISSL) established at University of Engineering & Technology (UET) Peshawar, Grant No. 2 (1078)/HEC/M&E/2018/707.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Abraham, A.; Paprzycki, M. (2004): Significance of steganography on data security. *International Conference on Information Technology: Coding and Computing*, vol. 2, pp. 347-351.

Ahuja, B.; Kaur, M. (2009): High capacity filter-based steganography. *International Journal of Recent Trends in Engineering*, vol. 1, pp. 672-674.

Akhtar, N.; Johri, P.; Khan, S. (2013): Enhancing the security and quality of LSB based image steganography. *5th International Conference and Computational Intelligence and Communication Networks*, pp. 385-390.

Amirtharajan, R.; Akila, R.; Deepikachowdavarapu, P. (2010): A comparative analysis of image steganography. *International Journal of Computer Applications*, vol. 2, no. 3, pp. 41-47.

Anderson, R. J.; Petitcolas, F. A. (1998): On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, vol. 16, no. 4, pp. 474-481.

Babu, K. S.; Raja, K. B.; Kiran, K. K.; Devi, T. H.; Venugopal, K. R. et al. (2008): Authentication of secret information in image steganography. *TENCON IEEE Region 10 Conference*, pp. 1-6.

Baby, A.; Krishnan, H. (2017): Combined strength of steganography and cryptography-a literature survey. *International Journal of Advanced Research in Computer Science*, vol. 8,

no. 3, pp. 1007-1010.

Bailey, K.; Curran, K. (2006): An evaluation of image-based steganography methods. *Multimedia Tools and Applications*, vol. 30, pp. 55-88.

Chandramouli, R.; Memon, N. (2001): Analysis of LSB based image steganography techniques. *Proceedings of International Conference on Image Processing*, vol. 3, pp. 1019-1022.

Chatterjee, A.; Das, A. K. (2018): Secret communication combining cryptography and steganography. *Progress in Advanced Computing and Intelligent Engineering*, pp. 281-291.

Chikouche, S. L.; Noureddine, C. (2017): An improved approach for LSB-based image steganography using AES algorithm. *5th IEEE International Conference on Electrical Engineering-Boumerdes*, pp. 1-6.

Dahiya, S. (2017): Data encryption-based image steganography: a review. *International Journal of Engineering Development and Research*, vol. 5, no. 1.

Darabkh, K. A.; Al-Dhamari, A. K.; Jafar, I. F. (2017): A new steganographic algorithm based on multi directional PVD and modified LSB. *Information Technology & Control*, vol. 46, no. 1, pp. 16-36.

Dunbar, B. (2002): A detailed look at steganographic techniques and their use in an open-systems environment. *Sans Institute InfoSec Reading Room.*

Grover, N.; Mohapatra, A. K. (2013): Digital image authentication model based on edge adaptive steganography. *The 2nd International Conference on Advanced Computing, Networking and Security*, pp. 238-242.

Gutub, A. A. (2010): Pixel indicator technique for RGB image steganography. *Journal of Emerging Technologies in Web Intelligence*, vol. 2, no. 1, pp. 56-64.

Halder, T.; Karforma, S.; Mandal, R. (2019): A block-based adaptive data hiding approach using pixel value difference and LSB substitution to secure e-governance documents. *Journal of Information Processing Systems*, vol. 15, no. 2, pp. 261-270.

Ibrahim, R.; Kuan, T. S. (2011): Steganography algorithm to hide secret message inside an image. *Computer Technology and Application*, vol. 2, pp. 102-108.

Ishaque, E. M.; Khan, E. F.; Sattar, D. S. (2011): Investigation of steganalysis algorithms for multiple cover media. *Ubiquitous Computing and Communication Journal*, vol. 6, no. 5, pp. 9-20.

James, F. (1990): A review of pseudorandom number generators. *Computer Physics Communications*, vol. 60, pp. 329-344.

Jan, Z.; Mirza, A. M. (2012): Genetic programming-based perceptual shaping of a digital watermark in the wavelet domain using Morton scanning. *Journal of the Chinese Institute of Engineers*, vol. 35, pp. 85-99.

Janakiraman, S.; Amirtharajan, R.; Thenmozhi, K.; Rayappan, J. B. (2012): Pixel forefinger for gray in color: a layer by layer stego. *Information Technology Journal*, vol. 11, pp. 9-19.

Johnson, N. F.; Jajodia, S. (1998): Exploring steganography: seeing the unseen. *Computer*, vol. 31, pp. 26-34.

Juneja, M.; Sandhu, P. S. (2009): Designing of robust image steganography technique based on LSB insertion and encryption. *International Conference on Advances in Recent Technologies in Communication and Computing*, pp. 302-305.

Juneja, M.; Sandhu, P. S.; Walia, E. (2009): Application of LSB based steganographic technique for 8-bit color images. *World Academy of Science, Engineering and Technology*, pp. 423-425.

Kahn, D. (1996): The history of steganography. *International Workshop on Information Hiding*, pp. 1-5.

Karim, S. M.; Rahman, M. S.; Hossain, M. I. (2011): A new approach for LSB based image steganography using secret key. *14th International Conference on Computer and Information Technology*, pp. 286-291.

Ker, A. D. (2005): Steganalysis of LSB matching in grayscale images. *IEEE Signal Processing Letters*, vol. 12, pp. 441-444.

Kumar, M. V.; Mamatha, E.; Reddy, C. S.; Mukesh, V.; Reddy, R. D. (2017): Data hiding with dual based reversible image using sudoku technique. *International Conference on Advances in Computing, Communications and Informatics*, pp. 2166-2172.

Kumar, V.; Kumar, D. (2010): Performance evaluation of DWT based image steganography. *IEEE 2nd International Advance Computing Conference*, pp. 223-228.

Lee, Y. K.; Chen, L. H. (2000): High capacity image steganographic model. *IEEE Proceedings-Vision, Image and Signal Processing*, vol. 147, no. 3, pp. 288-294.

Muhammad, K.; Ahmad, J.; Farman, H.; Jan, Z.; Sajjad, M. et al. (2015): A secure method for color image steganography using gray-level modification and multi-level encryption. *Transactions on Internet and Information Systems*, vol. 9, no. 5, pp. 1938-1962.

Muhammad, K.; Ahmad, J.; Rehman, N. U.; Jan, Z.; Sajjad, M. (2017): CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8597-8626.

Nabavian, N. (2007): CPSC 350 data structures: image steganography.

Nolkha, A.; Kumar, S.; Dhaka, V. S. (2020): Image steganography using LSB substitution: a comparative analysis on different color models. *Springer Smart Systems and IoT: Innovations in Computing*, pp. 711-718.

Parvez, M. T.; Gutub, A. A. (2008): RGB intensity-based variable-bits image steganography. *IEEE Asia-Pacific Services Computing Conference*, pp. 1322-1327.

Prasad, S.; Pal, A. K. (2017): An RGB colour image steganography scheme using overlapping block-based pixel-value differencing. *Royal Society Open Science*, vol. 4.

Rachael, O.; Misra, S.; Ahuja, R.; Adewumi, A.; Ayeni, F. et al. (2019): Image steganography and steganalysis based on least significant bit. *Proceedings of International Conference on Emerging Trends in Information Technology, Emerging Trends in Information Technology*, pp. 1100-1111.

Rashid, R. D.; Majeed, T. F. (2019): Edge based image steganography: problems and solution. *IEEE International Conference on Communications, Signal Processing, and Their Applications*, pp. 1-5.

Rahman, S.; Masood, F.; Khan, W. U.; Salam, A.; Ullah, S. I. (2019): The investigation of LSB based image steganographic techniques in spatial domain for secure communication. *Sukkur IBA Journal of Emerging Technologies*, vol. 2, no. 1, pp. 1-12.

Sahu, A. K.; Swain, G. (2018): An improved data hiding technique using bit differencing and LSB matching. *Internetworking Indonesia Journal*, vol. 10, no. 1, pp. 17-21.

Sahu, A. K.; Swain, G. (2019): An optimal information hiding approach based on pixel value differencing and modulus function. *Wireless Personal Communications*, pp. 1-16.

Sahu, N.; Peng, D.; Sharif, H. (2017): Unequal steganography with unequal error protection for wireless physiological signal transmission. *IEEE International Conference on Communications*, pp. 1-6.

Shehab, A.; Elhoseny, M.; Muhammad, K.; Sangaiah, A. K.; Yang, P. et al. (2018): Secure and robust fragile watermarking scheme for medical images. *IEEE Access*, vol. 6, pp. 10269-10278.

Singh, N.; Bhardwaj, J. (2019): Comparative analysis for steganographic LSB variants. *Computing, Communication and Signal Processing*, pp. 827-835.

Singh, S. K.; Yadav, S.; Raj, A.; Gupta, P. (2018): A survey paper on different steganography techniques. *Proceedings on International Conference on Emerg*, vol. 2, pp. 103-108.

Solanki, R.; Chuahan, M.; Desai, M. (2015): Survey of image steganography techniques. *International Journal of Advanced Research in Engineering, Science & Management*. Retrieved from

https://pdfs.semanticscholar.org/d4f3/81047f0e6fb3fadcd0a4a2201563686836bd.pdf.

Swain, G. (2018): High capacity image steganography using modified LSB substitution and PVD against pixel difference histogram analysis. *Security and Communication Networks*.

Swain, G. (2018): A data hiding technique by mixing MFPVD and LSB substitution in a pixel. *Information Technology and Control*, vol. 47, no. 4, pp. 714-727.

Thakur, L.; Chokkar, R. L. (2017): Comparison of cryptographic techniques. *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 3, no. 2. Retrieved from https://www.IJARIIT.com.

USC. (2019): SIPI Image Database. (US. California, Ed.) Retrieved from

http://sipi.usc.edu/database/database.php?volume=misc#top.

Veena, S. T.; Arivazhagan, S. (2018): Quantitative steganalysis of spatial LSB based stego images using reduced instances and features. *Pattern Recognition Letters*, vol. 105, pp. 39-49.

Zhang, H.; Geng, G.; Xiong, C. (2009): Image steganography using pixel-value differencing. *Second International Symposium on Electronic Commerce and Security*, pp. 109-112.

Zhang, X.; Wang, S. (2006): Efficient steganographic embedding by exploiting modification direction. *IEEE Communications Letters*, vol. 10, pp. 781-783.