

A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption

**Khan Muhammad¹, Jamil Ahmad¹, Haleem Farman², Zahoor Jan²,
Muhammad Sajjad² and Sung Wook Baik¹**

¹College of Electronics and Information Engineering, Department of Digital Contents, Sejong University, Seoul, South Korea

[e-mail: khan.muhammad.icp@gmail.com, {jamil.ahmad, zahoor.jan, haleem.farman, muhammad.sajjad}@icp.edu.pk]

²Department of Computer Science, Islamia College, Peshawar, Pakistan
[e-mail: {sbaik@sejong.ac.kr}]

*Corresponding author: Sung Wook Baik

*Received December 12, 2014; revised March 4, 2015; accepted April 29, 2015;
published May 31, 2015*

Abstract

Security of information during transmission is a major issue in this modern era. All of the communicating bodies want confidentiality, integrity, and authenticity of their secret information. Researchers have presented various schemes to cope with these Internet security issues. In this context, both steganography and cryptography can be used effectively. However, major limitation in the existing steganographic methods is the low-quality output stego images, which consequently results in the lack of security. To cope with these issues, we present an efficient method for RGB images based on gray level modification (GLM) and multi-level encryption (MLE). The secret key and secret data is encrypted using MLE algorithm before mapping it to the grey-levels of the cover image. Then, a transposition function is applied on cover image prior to data hiding. The usage of transpose, secret key, MLE, and GLM adds four different levels of security to the proposed algorithm, making it very difficult for a malicious user to extract the original secret information. The proposed method is evaluated both quantitatively and qualitatively. The experimental results, compared with several state-of-the-art algorithms, show that the proposed algorithm not only enhances the quality of stego images but also provides multiple levels of security, which can significantly misguide image steganalysis and makes the attack on this algorithm more challenging.

Keywords: Cryptography, Image Processing, Network Security, Steganography

1. Introduction

Steganography is a Greek word which means “Protected Writing”. It is an art and science of secret communication. It is the process during which secret information is embedded inside a carrier object (e.g. image, text, audio, and video) such that it cannot be detected by human visual system (HVS) [1-4]. The purpose of steganography is to hide secret data into a host media, protecting it from unauthorized persons. The main goals of steganography include high payload, improved robustness, and better imperceptibility. Payload shows the amount of data to be embedded in the cover image which is calculated in bits per pixel (bpp) such that the greater the bpp, the high the payload is and vice versa. Robustness shows the level of difficulty faced by attackers during extraction of secret data which protects it from grabbers' attacks. Imperceptibility means undetectability which is measured using different image quality assessment metrics (IQAMs) such as peak signal-to-noise ratio (PSNR)[5] and structural similarity index metric (SSIM)[6]. For instance, small obvious distortion between host and stego images results in higher PSNR score and hence represents high quality of stego images and vice versa[7].

Requirements of steganography include a carrier object (cover/host media), secret data, embedding algorithm, and sometimes a stego key and encryption algorithm to increase the security levels[1]. Applications of steganography involve the exchange of top secret information between government departments and defence organizations, medical imaging security, online banking security, smart identity card security, online voting security, and tamper proofing. In negative sense, it can be used for sending viruses and Trojan horses and provides a better method to be used by terrorists and criminals for their confidential communication as well[3, 8].

The steganographic techniques are categorized into two categories: (a). Spatial domain techniques directly modify the grey-levels of cover image for hiding secret data. These techniques possess high payload and result in high quality stego images. However, these techniques are not enough robust against image processing operations (cropping, scaling, rotations, and noise attacks) and statistical attacks (RS-analysis, chi-square attack) [9]. Spatial domain techniques include least significant bit (LSB) substitution method[10], pixel indicator technique (PIT)[11], edges based embedding (EBE) techniques [7], and pixel value differencing (PVD) techniques[12, 13]. (b). Transform domain techniques alter the image pixels via different transforms such as DWT[14], DFT[15], integer contour transform[16], and DCT[17] in order to hide secret information. These techniques are mostly used in watermarking systems and applications due to its better robustness against statistical steganalysis. On the other hand, these approaches have lower payload and result in stego images of low quality as compared to spatial domain approaches[3].

In this paper, we propose an efficient image steganographic approach based on GLM and MLE. Image has been used as a host object due to its low communication cost and availability of large number of redundant bits. The main contributions of this paper are: (i).Both the secret data and stego key is encrypted using MLEA which adds multiple

security levels to the proposed method. (ii). The proposed method is evaluated quantitatively by six different IQAMs including PSNR, SSIM, mean absolute error (MAE), mean consequential error (MCE), root mean-square-error (RMSE), and normalized mean error (NME). (iii). To deceive the attacker, image is transposed prior to embedding secret information. (iv). Qualitatively, this new approach is evaluated by both naked eye analysis and histogram changeability analysis using HVS. (v). The proposed scheme is experimentally tested by three different types of viewpoints: Embedding secret data of same size in different standard color images of same resolution, hiding cipher of different sizes in same images of same dimensions, and embedding cipher of equal sizes in same images of variable resolutions. Furthermore, the proposed method is compared with five classical and state-of-the-art methods.

The rest of the paper is structured as follows. Section 2 presents an overview of classical and latest steganographic approaches whose limitations led us towards current proposed work. In section 3, we present our proposed algorithm along with mathematical and graphical modelling. Section 4 presents experimental results and critical discussion and finally the work is concluded in section 5.

2. Related Work

The first attempt of steganography was taken by Greeks with the famous story of shaved head. Since that time, different methods have been used for information hiding such as tablets with wax, carrier pigeons, microdots, invisible inks, semagrams, and open codes [2, 3, 18, 19]. In this modern era, the most simple and classical method to hide secret data in an image is to replace the LSB of carrier image pixels with secret data. Suppose A is a cover 8-bit image with n pixels such that $A=A_0A_1\dots A_{n-1}$ where A_i is a pixel of A for $i=0, 1, 2, \dots, n-1$. Assume S is a secret message such that $S=S_0, S_1, \dots, S_{n-1}$ with S_i a k -bit string of message S for $i=0, 1, \dots, n-1$. To hide a secret bit S_i in the host image pixel A_i , the pixel A_i is divided into two parts; LSB_i and MSB_i such that $A_i=MSB_i \parallel LSB_i$ and LSB_i is replaced by S_i for $i=0, 1, \dots, n-1$. The stego image generated by this simple LSB method is B with pixels $B=B_0, B_1, \dots, B_{n-1}$ such that B_i is a pixel of B with $i=0, 1, \dots, n-1$. Payload capacity can be increased if more than 1 LSBs are used for message embedding but it brings noticeable changes in the stego image. This means that there is a trade-off between payload and visual quality of stego images.

F.A Jassim [20] proposed a secure method whose fundamental idea is based on the fact that adjacent pixels in images are strongly correlated with each other. In FMM scheme, the image is divided into a number of blocks, each of which contains $k \times k$ pixels where k shows the window size and each pixel represents a number in the range 0-255 divisible by 5 for 8-bit images. The proposed ST-FMM method is better in robustness and achieves good quality of stego images. However, there is a trade-off between the payload and window size such that increasing the window size decreases the payload and vice versa.

Bailey and Curran [21] proposed stego color cycle (SCC) method for color images that hides data in different channels of the cover image in a cyclic manner. i.e., the first secret bit is hidden in pixel1's red channel, the second secret bit is hidden in the green channel of pixel2 and the third secret bit is hidden in the blue channel of pixel3, and so on. The major limitation in SCC method is that the secret information is embedded in cover image pixels in a fixed cyclic and systematic way. So an attacker can easily discover this technique if secret information from a few pixels is successfully extracted.

Karim et.al [22] presented a new approach to enhance the security of existing LSB substitution method by adding one extra barrier of secret key. In the said method, secret key and red channel are used as an indicator while green and blue channels are data channels. On the basis of secret key bits and red channel LSBs, the secret data bits are embedded either in green channel or in blue channel. If either the bit of red channel LSB or secret key bit is 1, then the LSB of green channel is replaced with secret message bit, otherwise LSB of blue channel is replaced with secret bit. Although, this approach possesses the same payload as LSB based approaches but it increases the security by making use of secret key. An intruder cannot easily extract the secret information without the correct secret key.

Gutub proposed a high payload pixel indicator technique (PIT)[11] in which one channel is used as an indicator and the other two channels are data channels. The proposed method embeds the secret data in one or both of the data channels in a predefined cyclic manner. The experimental results show the high payload capacity and better imperceptibility of the proposed algorithm and also avoid the key exchange overhead. The major weak point of this method is that the payload capacity is totally dependent on host image and indicator bits which can result in low payload. Similarly this method hides fixed number of bits in each pixel which can bring more changes in the cover image if we embed more number of secret bits in each pixel. The major limitation in the proposed methods discussed so far is that the secret information can be extracted easily if an attacker finds out the algorithm being used for message hiding because secret data is in plain text form and not encrypted. Moreover, these methods result in stego images of low quality which can be detected using HVS.

In this paper, we propose a new method to handle these limitations by using GLM and MLE. The secret information is encrypted using MLEA before mapping it to the pixels of host image so that if an attacker finds out the algorithm being used, still the actual secret contents cannot be retrieved. A malicious user has to crack down the following barriers in order to retrieve the original secret data: (i).The color steganographic algorithm being used for data hiding. (ii).The secret key being used in encryption. (iii).The MLEA via which data is encrypted before embedding. (iv). Have the idea that image has been transposed before message hiding.

3. The Proposed Image Steganographic Algorithm

This section demonstrates the proposed algorithm, its embedding and extraction processes, and MLEA. The proposed steganographic scheme consists of three phases: encryption, data mapping and, extraction phase as shown in **Fig. 1**. These three phases are integrated with each other in order to develop an advanced steganographic system, having multiple security levels.

3.1 Mathematical Modeling of Proposed Scheme

Suppose M denotes the secret message that is to be embedded into the carrier image (C). T shows the transposed image, K is secret key and S is the stego image. Three functions named as α , β , and γ are used in the whole process of embedding as shown in equations 1-3.

$$T = \alpha(C) \quad (1)$$

$$M' = \beta(M, K) \quad (2)$$

$$S = \gamma(T, M') \quad (3)$$

The first function α takes C as an input and returns T which is the transposed image. M' is the resultant encrypted message returned by second function β after applying MLEA on message M using secret key K . Finally, the third function γ generates the stego image S after hiding the encrypted message M' in the transposed image T using the proposed steganographic scheme.

The recipient has to apply the reverse operations in order to extract the original hidden information. The following three functions are used for extracting the actual message as described in equations 4-6.

$$T = \alpha^{-1}(S) \quad (4)$$

$$M' = \gamma^{-1}(T) \quad (5)$$

$$M = \beta^{-1}(M', K) \quad (6)$$

In extraction process, function α^{-1} applies transposition on stego image S and returns T which is the resultant transposed image. Using eq. 5, the encrypted secret message M' is extracted from the image T by applying the extraction algorithm. At the end, original message M is achieved by using eq. 6 when encrypted message M' is decrypted by function β^{-1} using secret key K .

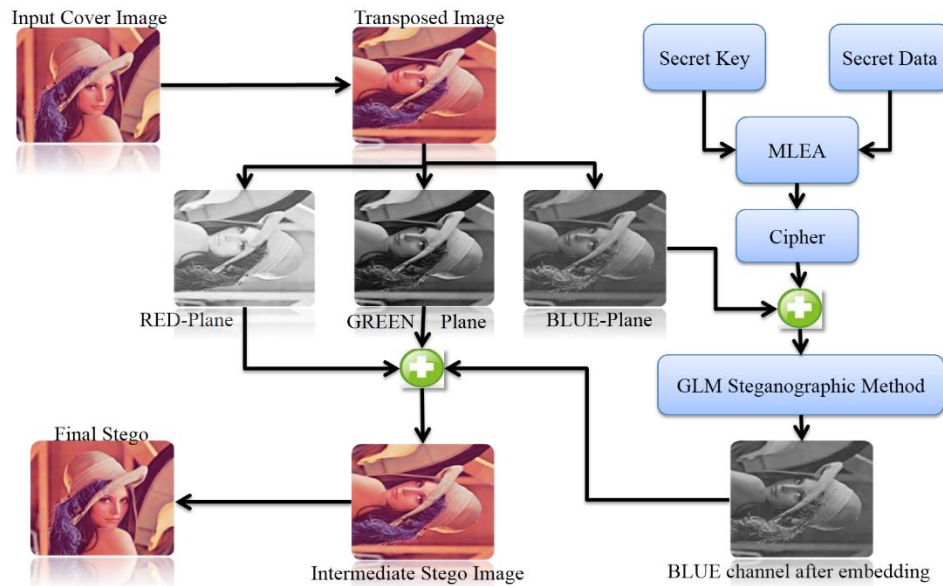


Fig. 1. Detailed pictorial representation of the proposed scheme

3.2 Encryption Phase

The encryption phase encrypts the secret information using MLEA, increasing the security and robustness of the proposed method which is its main motivational factor. The MLEA consists of the following three different operations.

- i. Bitxor operation of secret key and secret data bits with logical 1.
- ii. Bits shuffling algorithm which changes the positions of the secret bits such that the bits with even and odd indices are interchanged, hence increases the security and robustness.
- iii. Encrypted secret key based encryption which further modifies the shape of secret bits and increases the security of secret contents.

The end result of this phase is encrypted secret data in bits form. The main steps of encryption phase are flowcharted in [Fig. 2](#).

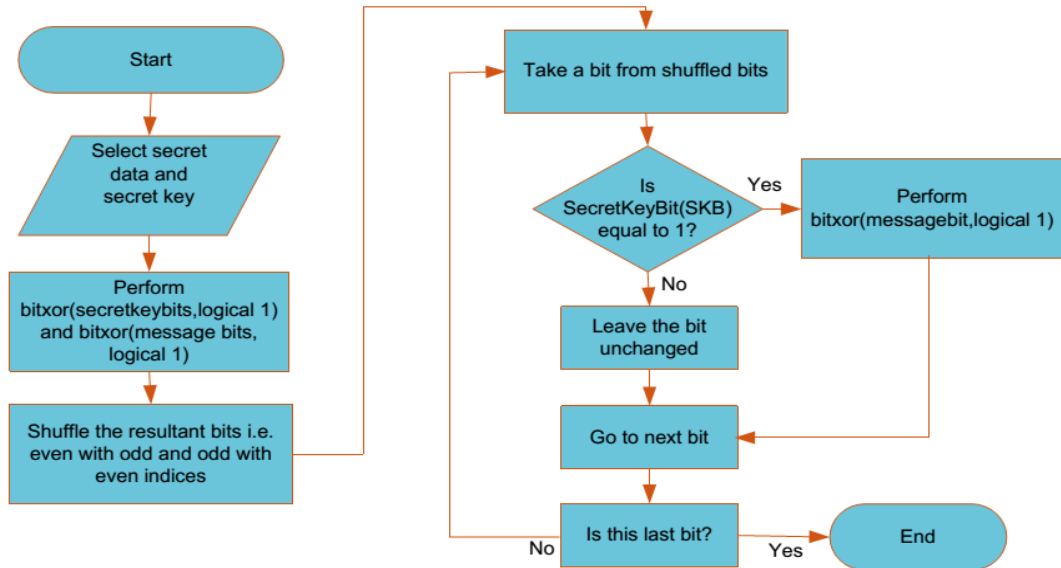


Fig. 2. Flowchart for multi-level encryption algorithm

To illustrate the MLEA, we present a simple example. Consider the secret message $M = "A"$ with bits stream $S = [01000001]$ and secret key with bit stream $K = [01010010]$. Apply the bitxor operations i.e. $ES = \text{bitxor}(01000001, 11111111) = 10111110$ and $EK = \text{bitxor}(01010010, 11111111) = 10101101$. Applying the bits shuffling algorithm on ES and EK we get $SS = \text{shufflebits}(ES) = \text{shufflebits}(10111110) = 01111101$ and $SK = \text{shufflebits}(EK) = \text{shufflebits}(10101101) = 01011110$. Finally we apply the secret key based encryption on shuffled bit stream (SS) using shuffled key bit stream (SK). It works as follows: If a bit in the key stream is 1, then we perform bitxor (shuffled message bit, logical 1) otherwise leave the message bit unchanged. As a result of this procedure, the final bits we get are: $S' = 00100011$ which is far most different than the original bits i.e. $S = 01000001$.

In order to decrypt this message ($S' = 00100011$), we have to apply the reverse operations. i.e., the secret key ($K = 01010010$) is first encrypted using the above procedure and we get $EK = 01011110$. Now apply the reverse of secret key based encryption by the same way as discussed above. i.e., if secret key bit is 1, then apply bitxor (bit of S' , logical 1) otherwise leave it unchanged. So the intermediate result we get is $DS' = 01111101$. After applying the inverse of bits shuffling algorithm we get $SS' = 10111110$ and finally bitxor operation is applied i.e., $DM = \text{bitxor}(SS', \text{logical 1's}) = \text{bitxor}(10111110, 11111111) = 01000001$ which is the binary equivalent of secret character "A".

3.3 Data Mapping Phase

This phase maps the encrypted data into the carrier image pixels. Before data mapping, the carrier image is transposed, data is encrypted via MLEA, and then a 1-1 mapping between secret data bits and image pixels is maintained. The end result is a stego image of higher quality, containing secret information which is the main reason of its usage. This phase is illustrated by flowchart in Fig. 3.

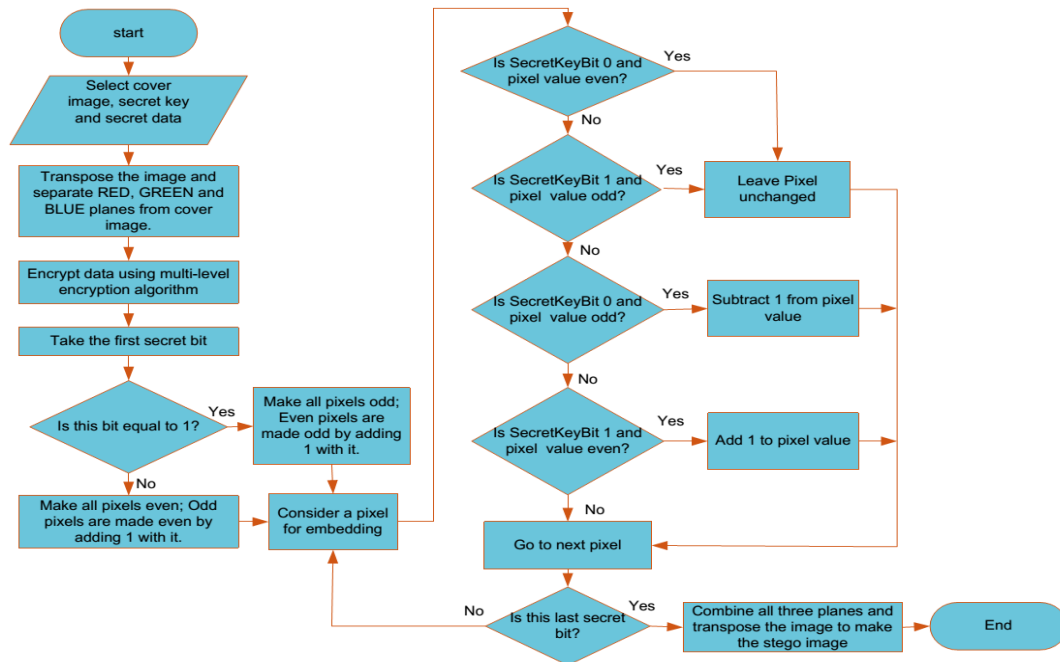


Fig. 3. Flowchart for embedding algorithm

For example, I represent an image containing eight pixels $P = [P1, P2, P3... P8]$ with values $P = [90, 36, 18, 27, 10, 25, 40, 63]$ and the secret message is $(S=01000001)$. We embed the encrypted message $(S' = 00100011)$ of encryption phase in these pixels. Since the first bit of S' is 0, so all the pixels are converted to even numbers by adding 1 to those pixels which are not even and we get the pixel values $[90, 36, 18, 28, 10, 26, 40, 64]$. After applying the flowchart operations on the resultant pixels, we get $P' = [P1', P2', P3'... P8'] = [90, 36, \mathbf{19}, \mathbf{28}, 10, \mathbf{26}, \mathbf{41}$ and 63]. The pixels shown in bold face are changed as a result of embedding which means approximately half of the pixels change only.

3.4 Extraction Phase

The extraction phase extracts the embedded secret bits from the stego image that is being sent by sender. The extracted bits are decrypted by applying the reverse operations of MLEA and then converted into its original form. By this way, the original secret message

is achieved based on which we can take further necessary actions. The major steps of this phase are depicted by flowchart in Fig. 4.

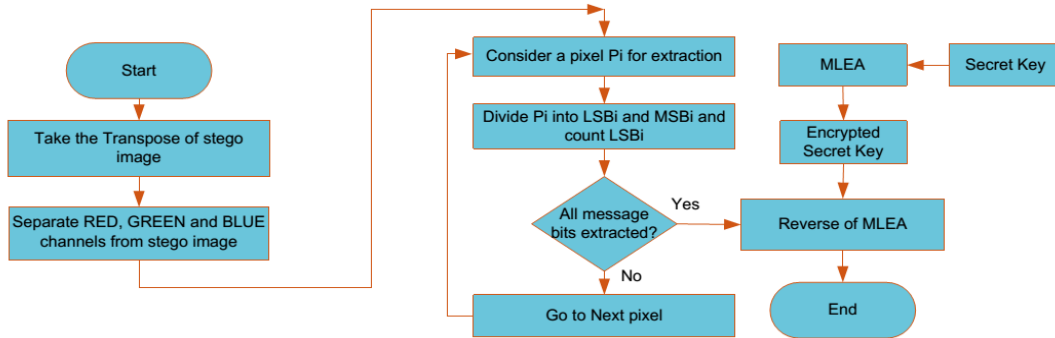


Fig. 4. Flowchart for extraction algorithm

For illustration of extraction process consider the pixels above $P' = [P1', P2', P3' \dots P8'] = [90, 36, 19, 28, 10, 26, 41 \text{ and } 63]$. In extraction process, we divide each pixel of blue channel into two parts i.e. LSB_i and MSB_i . we then store these LSBs into an array and get the encrypted secret bits i.e. $LSB(P1') = LSB(90) = 0$, $LSB(P2') = LSB(36) = 0$, $LSB(P3') = LSB(19) = 1$, $LSB(P4') = LSB(28) = 0$, $LSB(P5') = LSB(10) = 0$, $LSB(P6') = LSB(26) = 0$, $LSB(P7') = LSB(41) = 1$, $LSB(P8') = LSB(63) = 1$. By combining these LSBs, we get the bits stream $E = 00100011$ which is same as $S' = 00100011$ (Given in data mapping phase's example). The bits stream (E) is then decrypted using the reverse operations of MLEA and original secret message is achieved.

4. Experimental Results and Analysis

The proposed technique, classical LSB technique, five modulus method (FMM) [20], stego color cycle (SCC) technique [21], pixel indicator technique (PIT) [11], and Karim's technique [22] are simulated using MATLAB R2014a. A number of different experiments were conducted in order to fully assess the effectiveness of the proposed scheme. The following sub-sections present a complete detailed study of experimental results and critical discussion.

4.1 Dataset

This sub-section describes the dataset of images that was used for experimental purposes. A dataset of 50 standard color images taken from database "The USC-SIPI Image Database Volume 3: Miscellaneous" and internet was used for comparative analysis of proposed method with other state-of-the-art methods. The dataset contains different edgy and smooth standard color images of different dimensions (128×128, 256×256, 512×512 and 1024×1024) including Lena, mandrill (baboon), peppers, trees, and house.

4.2 Quantitative Evaluation

This sub-section demonstrates the complete procedure of quantitative analysis that is used in this paper. All the mentioned techniques are coded using MATLAB R2014a and are tested by three different viewpoints: Using viewpoint1, a text file of 8KB is embedded in different edge and smooth color images having dimension 256×256 pixels. This process is applied on 50 images and its average PSNR value is calculated. The second viewpoint is about encoding text files of different sizes in the same images of uniform dimension (256×256). This type of experiment is applied on four standard color images. In viewpoint3, four color images with different resolutions (128×128, 256×256, 512×512 and 1024×1024) were used. The size of cipher in this type of experiment is same as viewpoint1 i.e. 8KB. The detailed experimental results of these three viewpoints and their datasets are shown in sub-section 4.2.2.

4.3 Image Quality Assessment Metrics

In this sub-section, we highlight different IQAMs that were used for comparison of existing five prominent data hiding schemes with the proposed scheme. Full-reference image-quality assessment method has been used in this paper in which the original cover images and distorted images are completely available to be compared with one another. Full-reference IQAMs include PSNR, SSIM, and MAE which are discussed one by one below and performance of all mentioned techniques is evaluated with them.

A. PSNR and MSE

PSNR is the ratio between the modified image and original cover image. It is used for calculating the observable deformation that occurs in stego images after intentionally embedding secret data. The PSNR is calculated in terms of decibels (dB). The higher the value of PSNR, the more the stego image is correlated with original cover image and vice versa[5]. Stego images with PSNR less than 30dB represent low quality. PSNR must strive for 40dB or higher values in order to fulfil the favourable demands of modern steganographic systems [23].

The mean-square-error (MSE) calculates the error between cover image and distorted stego image. When $C(x, y) = S(x, y)$, then $MSE=0$ and $PSNR= \infty$ i.e. both the images are identical[23]. The PSNR and MSE are calculated by equation (7) and equation (8).

$$PSNR = 10 \log_{10} \left(\frac{C_{max}^2}{MSE} \right) \quad (7)$$

$$MSE = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N (S_{xy} - C_{xy})^2 \quad (8)$$

Note that M and N show image dimensions, x and y are loop counters, C is cover image, S is stego image, and C_{max} is the maximum pixel intensity among both images.

B. Structural Similarity Index Metric (SSIM)

The full-reference IQAM (SSIM) is used to determine the quality of a stego image (Y) w.r.t original image (X). It was proposed by Wang [6]. It is calculated by taking the product of its three main components (luminance, contrast, and structural component) raised by an exponent, when required. Its value will be 1.0 if both the cover and stego images are indistinguishable. Generally, the SSIM between two images X and Y is defined as follows in (9):

$$SSIM(X, Y) = [l(x, y)]^\alpha \cdot [c(x, y)]^\beta \cdot [s(x, y)]^\gamma \quad (9)$$

Herein, α , β , and γ are parameters that represent the comparative consequence of its three components. By setting $\alpha = \beta = \gamma = 1$, we get the SSIM index as mentioned in (10).

$$SSIM(X, Y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (10)$$

Herein, μ_x , μ_y , σ_x , σ_y , and σ_{xy} are termed as local statistical parameters. C_1 , C_2 , and C_3 are small constants that handle the division by zero exception [24].

C. Mean Absolute Error (MAE) and Mean Consequential Error (MCE)

MAE is the average of the absolute value of each individual error that exists between the original and distorted image. This is the more preferable method to use when the amount by which numerical predictions are in error, is too much important [24]. MAE and MCE are calculated by equation 11 and equation 12.

$$MAE = \left(\frac{1}{N}\right) \sum_{x=1}^N |C_x - S_x| \quad (11)$$

$$MCE = \left(\frac{1}{N}\right) \sum_{C_x \neq S_x} 1 \quad (12)$$

D. Root Mean Square Error (RMSE)

RMSE is the square root of the average of the square of all errors that occurs between original and modified image [25]. Its usage is very common because it provides a better generic objective analysis error metric used in numerical predictions. RMSE amplifies and rigorously punishes large amount of errors as compared to MAE [24]. RMSE is calculated by equation (13).

$$RMSE = \sqrt{\left(\frac{1}{N}\right) \sum_{x=1}^N (C_x - S_x)^2} \quad (13)$$

4.3.1 Quantitative Results and Discussion

In this sub-section, we present the comparison of the proposed method with other five existing methods including classical LSB method, FMM[20], SCC[21], PIT[11], and Karim's method[22]. A few sample images from the datasets used for quantitative experiments are shown in Fig. 5-7. The incurred results of all mentioned algorithms based on PSNR, SSIM, NME, MCE, RMSE, and MAE from three different viewpoints are listed in Table 1-9 respectively.

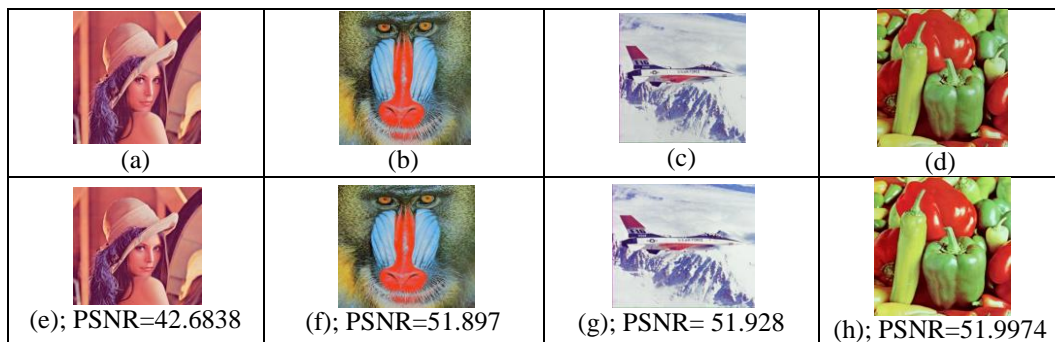


Fig. 5. Viewpoint1 dataset: cover images; (a) Lena (b) Baboon (c) F16jet (d) Peppers; Stego images; (e) Lena (f) Baboon (g) F16jet (h) Peppers

Table 1. Viewpoint1 Results; Comparison of the proposed method with existing five methods based on PSNR (dB) by hiding same amount of cipher (8KB) in different images of same resolution (256×256 pixels)

Serial#	Image Name	Classic LSB Method	SCC[21] Method	PIT[11]	FMM[20]	Karim's Method[22]	Proposed Method
1	Design1	46.3943	46.419	45.573	40.5802	46.4599	54.5235
2	Baboon	51.1648	46.5568	39.9997	48.9531	48.9536	51.897
3	House	51.1659	47.6956	40.2518	51.1776	51.1564	51.8654
4	Trees	39.0436	38.2702	39.5397	38.5418	38.5421	51.8989
5	Lena	42.5103	42.6036	42.3001	43.5786	42.5666	42.6838
6	Peppers	18.7241	16.079	19.4446	16.0755	16.0755	51.9974
7	Masjid	30.6466	28.5173	39.6331	28.5361	28.5363	52.577
8	Couple	48.4091	47.9157	46.582	46.25	47.9298	51.7058
9	Scene3	55.9381	55.9306	49.2724	40.244	55.9272	51.9283
10	Design2	38.1099	37.7652	37.7125	39.4414	37.7671	43.0306
Avg. of 50 images		43.1736	36.3208	34.7621	33.9232	36.3187	52.0931

Table 2. Viewpoint1 Results; Comparison of the proposed method with other five methods based on SSIM

Serial#	Image Name	Classic LSB Method	SCC[21] Method	PIT[11]	FMM[20]	Karim's Method[22]	Proposed Method
1	Design1	0.997	0.9979	0.9977	0.9976	0.9984	0.9999
2	Baboon	0.9989	0.9993	0.9985	0.9925	0.9992	0.9998
3	House	0.9983	0.999	0.9974	0.986	0.9989	0.9995
4	Trees	0.9964	0.997	0.9956	0.9858	0.997	0.9995
5	Lena	0.9981	0.9989	0.9971	0.9822	0.9989	0.9994
Avg. of 50 images		0.9689	0.9560	0.9543	0.9751	0.9559	0.9995

Table 3. Viewpoint1 Results; Comparison of the proposed method with other five methods based on RMSE

Serial#	Image Name	Classic LSB Method	SCC[21] Method	PIT[11]	FMM[20]	Karim's Method[22]	Proposed Method
1	Design1	0.2359	0.3205	0.5599	1.7497	0.3165	0.0486
2	Parrot	0.2782	0.2769	0.595	1.7225	0.2751	0.0324
3	Laserlight	0.2767	0.2765	0.6009	1.7326	0.2768	0.0276
4	Kite	0.2759	0.2763	0.5894	1.7168	0.2735	0.0148
5	Rose	0.2778	0.2773	0.5975	1.7342	0.276	0.0365
Avg. of 50 images		0.2712	0.2746	0.5869	1.6958	0.2740	0.0339

Table 4. Viewpoint1 Results; Comparison of the proposed method with other five methods based on MAE

Serial#	Image Name	Classic LSB Method	SCC[21] Method	PIT[11]	FMM[20]	Karim's Method[22]	Proposed Method
1	Design1	0.0557	0.1027	0.1607	1.0205	0.1002	0.0024
2	Parrot	0.0774	0.0766	0.1883	0.9901	0.0757	0.0011
3	Laserlight	0.0766	0.0764	0.1914	1.0009	0.0766	0.0008
4	Kite	0.0761	0.0763	0.1851	0.9851	0.0748	0.0002
5	Rose	0.0772	0.0769	0.1904	1.0024	0.0762	0.0013
Avg. of 50 images		0.0740	0.0756	0.1843	0.9645	0.0752	0.0043

Table 5. Viewpoint1 Results; Comparison of the proposed method with other five methods based on NME

Serial#	Image Name	Classic LSB Method	SCC[21] Method	PIT[11]	FMM[20]	Karim's Method[22]	Proposed Method
1	Peppers	0.032	0.0782	0.0806	0.0666	0.0785	0.0046
2	F16jet	0.001	0.0009	0.0022	0.011	0.0009	0.0015
3	Building1	0.0037	0.0037	0.0054	0.0141	0.0037	0.0021
4	Baboon	0.0014	0.0014	0.0034	0.017	0.0015	0.0028
5	House	0.001	0.0011	0.0026	0.0128	0.0011	0.0021
Avg. of 50 images		0.0148	0.0522	0.0544	0.0341	0.0523	0.0030

Table 6. Viewpoint1 Results; Comparison of the proposed method with existing five methods based on MCE

Serial#	Image Name	Classic LSB Method	SCC[21] Method	PIT[11]	FMM[20]	Karim's Method[22]	Proposed Method
1	Design1	0.0557	0.1027	0.0973	0.3402	0.1002	0.0024
2	Parrot	0.0774	0.0766	0.1187	0.3311	0.0757	0.0011
3	Laserlight	0.0766	0.0764	0.1204	0.3339	0.0766	0.0008
4	Kite	0.0761	0.0763	0.1171	0.3311	0.0748	0.0002
5	Cake	0.0744	0.075	0.1211	0.3239	0.0739	0.0057
Avg. of 50 images		0.0740	0.0756	0.1167	0.3246	0.0752	0.0043

Tables 1-6 show the experimental results of the proposed scheme and other five schemes based on PSNR, SSIM, RMSE, MAE, NME, and MCE respectively for viewpoint1. According to viewpoint1, equal size of text (8KB) is encoded in different diverse images of same resolution (256×256). The anticipated scheme clearly dominates the existing five schemes by attaining highest values of all mentioned metrics. The last line of **Table 1-6** shows the average value of PSNR, SSIM, RMSE, MAE, NME, and MCE respectively computed over fifty images (50). The average results demonstrated at the last row of **Table 1-6** clearly shows the excellence of the proposed scheme as compared to other five mentioned approaches.

















 (a); Cipher=2KB PSNR=57.1945	 (b); Cipher=4KB PSNR=54.1715	 (c); Cipher=6KB PSNR=52.396	 (d); Cipher=8KB PSNR=51.3729
 (e); PSNR=57.1736	 (f); PSNR=54.147	 (g); PSNR=52.3881	 (h); PSNR=51.3841
 (i); PSNR=57.1817	 (j); PSNR=54.1715	 (k); PSNR=52.3731	 (l); PSNR=51.3596
 (m); PSNR=57.1943	 (n); PSNR=54.1346	 (o); PSNR=52.3789	 (p); PSNR=51.339

Fig. 6. Dataset of stego images for viewpoint2; (a), (b), (c), (d); Baboon images with 2KB, 4KB, 6KB, and 8KB of hidden text respectively. (e), (f), (g), (h); Lena images. (i), (j), (k), (l); Building images (m), (n), (o), (p); House images with 2KB, 4KB, 6KB, and 8KB of hidden text respectively

Table 7. Viewpoint2 results; Comparison of the proposed scheme with other 5 algorithms based on PSNR

Image Name	Secret data (KBs)	Cipher size in bytes	Classic LSB Method	SCC Method[21]	PIT[11]	FMM[20]	Karim's Method[22]	Proposed Method
Baboon image with dimension 256×256	2	2406	52.3875	49.6451	46.5568	40.0896	49.6407	57.1945
	4	4177	51.9039	49.3853	46.5301	40.0609	49.3783	54.1715
	6	6499	51.4696	49.1359	46.0068	40.0258	49.1352	52.3963
	8	8192	51.1648	48.9531	45.3508	39.9997	48.9536	51.3729
	Average		51.7315	49.2798	46.1111	40.044	49.277	53.7838
Lena with resolution	2	2406	45.8307	45.8314	49.2562	40.3354	45.8317	57.1736
	4	4177	45.7183	45.7193	49.2242	40.3033	45.7193	54.147

256×256	6	6499	45.6108	45.6128	49.2061	40.2696	45.61	52.3881
	8	8192	45.53	45.5296	49.2044	40.249	45.5267	51.3841
	Average		45.6725	45.6732	49.2227	40.2893	45.6719	53.7732
Building image with dimension 256×256	2	2406	28.8513	28.8513	28.8378	40.3785	28.8514	57.1817
	4	4177	28.8491	28.849	28.8315	40.3356	28.8491	54.1269
	6	6499	28.8468	28.8468	28.8253	40.3044	28.8468	52.3731
House image with resolution 256×256	8	8192	28.8451	28.8451	28.8213	40.2552	28.8451	51.3596
	Average		28.8481	28.8480	28.829	40.3184	28.8481	53.7603
	2	2406	52.3913	52.3894	48.0916	40.3448	52.3869	57.1943
House image with resolution 256×256	4	4177	51.9037	51.9059	47.6906	40.3061	51.9023	54.1346
	6	6499	51.483	51.4802	47.6823	40.2762	51.4774	52.3789
	8	8192	51.1659	51.1776	47.6956	40.2518	51.1564	51.339
Average		51.736	51.7382	47.79	40.2947	51.7308	53.7617	

Table 8. Viewpoint2 results; Comparison of the proposed scheme with other five algorithms based on SSIM

Image Name	Secret data (KBs)	Cipher size in bytes	Classic LSB Method	SCC Method[21]	PIT[11]	FMM[20]	Karim's Method[22]	Proposed Method
Baboon image with dimension 256×256	2	2406	0.9996	0.9996	0.9985	0.9925	0.9996	1
	4	4177	0.9993	0.9994	0.9984	0.9925	0.9994	0.9999
	6	6499	0.9991	0.9993	0.998	0.9925	0.9993	0.9998
	8	8192	0.9989	0.9993	0.9975	0.9925	0.9992	0.9997
	Average		0.9992	0.9994	0.9981	0.9925	0.9993	0.9998
Lena with resolution 256×256	2	2406	0.9991	0.9993	0.9971	0.9819	0.9993	0.9998
	4	4177	0.9987	0.9991	0.997	0.9818	0.9991	0.9996
	6	6499	0.9981	0.9988	0.9968	0.9818	0.9987	0.9995
	8	8192	0.9977	0.9985	0.9983	0.9818	0.9984	0.9994
	Average		0.9984	0.9989	0.9973	0.9818	0.9988	0.9995
Building image with dimension 256×256	2	2406	0.998	0.9983	0.9964	0.9765	0.9995	0.9996
	4	4177	0.9974	0.998	0.9952	0.9765	0.9991	0.9994
	6	6499	0.9968	0.9976	0.995	0.9766	0.9987	0.9992
	8	8192	0.9963	0.9973	0.9948	0.9765	0.9983	0.999
	Average		0.9971	0.9978	0.9953	0.9765	0.9989	0.9993
House	2	2406	0.9997	0.9998	0.9981	0.9859	0.9998	0.9997

image	4	4177	0.9992	0.9995	0.9978	0.986	0.9995	0.9997
with	6	6499	0.9987	0.9992	0.9975	0.9859	0.9991	0.9996
resolution	8	8192	0.9983	0.999	0.9974	0.9859	0.9989	0.9994
256×256								
	Average		0.9989	0.9993	0.9977	0.9859	0.9993	0.9996

The experimental results of all mentioned algorithms including the proposed approach using viewpoint2 are listed in [Table 7](#) and [Table 8](#). In this type of experiment, four well-known standard color images of dimension (256×256) are selected and different size of text is embedded inside it using all specified methods. These four images are chosen for this type of analysis because every new algorithm has to be evaluated by images of different natures (edgy and smooth). For example, the four images contain the smooth image (Lena) and an edgy image (Baboon). The average values of PSNR and SSIM shown in bold face in [Table 7](#) and [Table 8](#) respectively are larger than existing approaches. This distinction illustrates that the proposed approach out-performs in terms of PSNR and SSIM as compared to other five data hiding approaches in viewpoint2.

 (a); PSNR=60.4357	 (b); PSNR=51.3638	 (c); PSNR=57.4107	 (d); PSNR=63.4552
 (a); PSNR=60.3568	 (b); PSNR=51.4302	 (c); PSNR=57.4423	 (d); PSNR=63.3895
 (a); PSNR=60.3716	 (b); PSNR=51.3879	 (c); PSNR=57.4433	 (d); PSNR=63.6064
 (a); PSNR=60.7069	 (b); PSNR=51.4044	 (c); PSNR=63.2608	 (d); PSNR=63.2608

Fig. 7. Images dataset for viewpoint3 containing stego images of different dimensions with their corresponding PSNR values. Row1: Lena images; Row2: pepper images; Row3: house images; Row4: building images

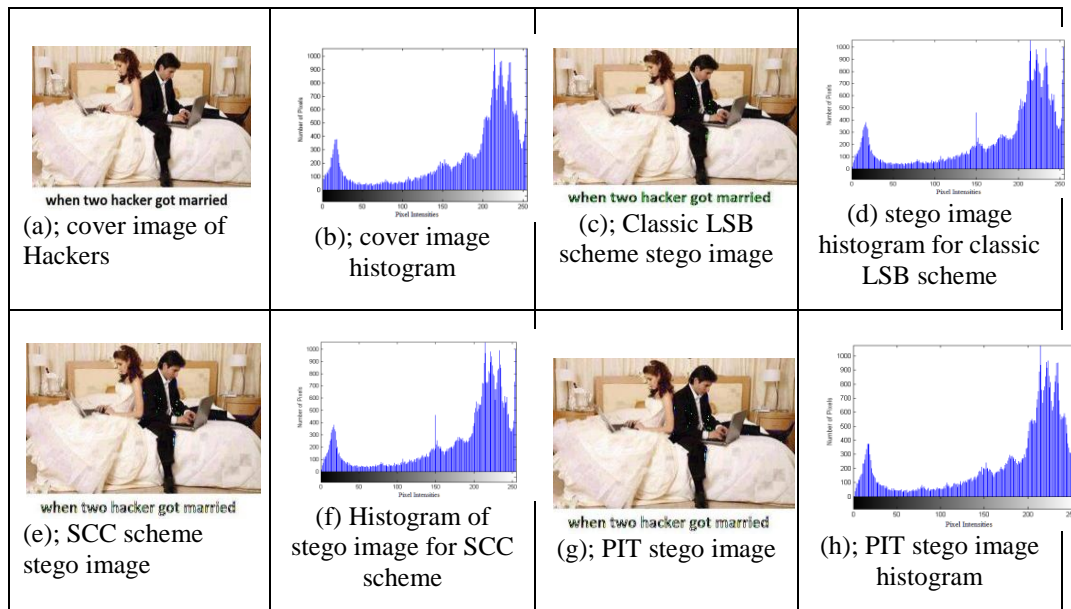
Table 9. Viewpoint3 results; comparison of the proposed method with other five methods based on PSNR

Image Name	Image dimensions (in pixels)	Classic LSB Method	SCC Method[21]	PIT[11]	FMM[20]	Karim's Method[22]	Proposed Method
Lena image	128×128	42.1208	42.1201	41.368	40.3257	42.121	60.4357
	256×256	45.531	45.5286	45.9463	40.2378	45.5343	51.3638
	512×512	47.0517	47.0523	47.1957	40.3152	47.0515	57.4107
	1024×1024	48.9022	48.9023	48.9566	40.3378	48.902	63.4552
	Average	45.9014	45.9008	45.8666	40.3041	45.9022	58.1663
Peppers image	128×128	19.1483	16.3692	16.3718	19.588	16.3692	60.3568
	256×256	19.8026	17.0126	17.0131	20.2123	17.0126	51.4302
	512×512	20.2429	17.4455	17.4457	20.6337	17.4455	57.4423
	1024×1024	20.2487	17.4413	17.4414	20.619	17.4413	63.3895
	Average	19.8606	17.0671	17.068	20.2632	17.0671	58.1547
House image	128×128	64.9052	64.8926	49.1782	40.3601	64.9305	60.3716
	256×256	44.8059	41.0315	41.1751	38.5233	41.0314	51.3879
	512×512	46.0551	42.1893	42.2356	38.927	42.189	57.4433
	1024×1024	47.3057	43.1444	43.1588	39.145	43.1444	63.6064
	Average	50.7679	47.8144	43.9369	39.2388	47.8238	58.2023
Building image	128×128	64.8137	64.656	49.1793	40.4385	64.72	60.7069
	256×256	46.3978	46.3994	46.9153	40.2848	46.3958	51.4044
	512×512	48.7443	48.7432	48.9566	40.4097	48.7425	57.7215
	1024×1024	49.0109	49.0109	49.0666	40.4239	49.0106	63.2608
	Average	52.2416	52.2023	48.5294	40.3892	52.2172	58.2734

Table 9 illustrates the experimental results of all mentioned approaches using viewpoint3. In this type of experiment, a text file of 8KB is embedded in four selected color images of different resolutions (128×128, 256×256, 512×512 and 1024×1024 pixels). The incurred results are tabulated in **Table 9**. By analysing the results in **Table 9**, it can be confirmed that the proposed scheme provide promising results in terms of PSNR in contrast to several existing classical and prominent (five) schemes.

4.4 Qualitative Analysis

In this sub-section, we briefly illustrate the qualitative analysis that has been used in this paper. The visual quality of stego images produced by the proposed method and other mentioned state-of-the-art methods are evaluated based on HVS and histogram changeability. A sample of cover and stego images taken from the dataset and their histograms are shown in Fig. 8. All these images contain 8KB text except the image with label (a). Using naked eye analysis of stego images, it can be confirmed that there is noticeable distortion in the stego images generated by existing methods except FMM (slightly distorted) and the proposed scheme. The distortion can be noted by comparing the black areas (black writing and black dress of man) of cover and stego images in Fig. 8. On the other hand, the stego image with label (m) generated by our proposed algorithm is almost same to the given cover image with label (a) and there is no obvious distortion between these two images. Furthermore, the histogram of stego image for our proposed scheme and cover image is almost same while the histograms of stego images generated by other methods are slightly modified. These points clearly show the excellence of the proposed method in contrast to existing five prominent methods.



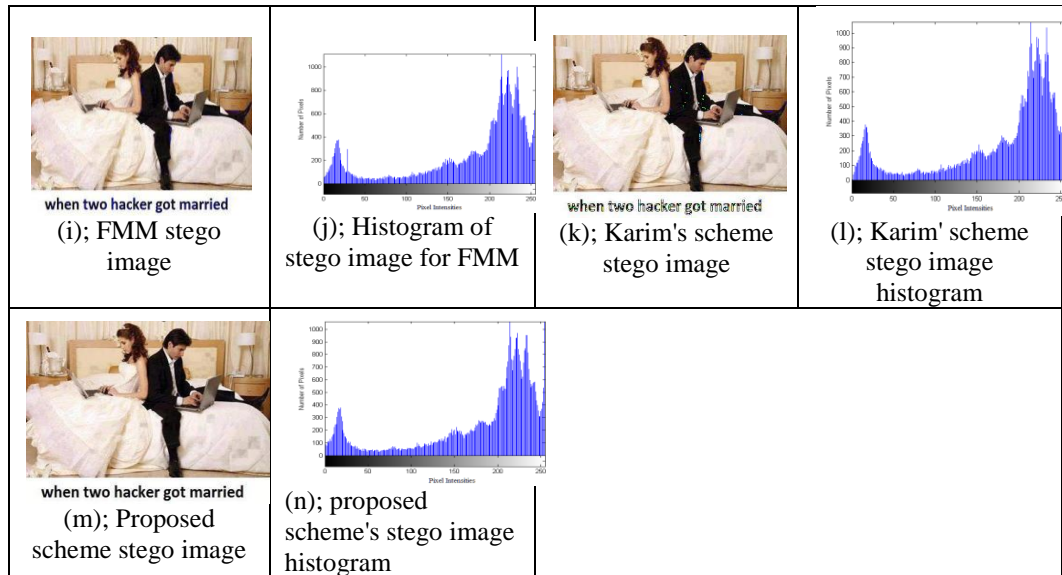


Fig. 8. Qualitative analysis of all discussed schemes using HVS based on quality of stego images with dimension (256×256) and their histograms

4.5 Performance Evaluation

The performance of any newly designed method is evaluated using three metrics named as payload, imperceptibility, and robustness[7]. An algorithm is considered to be best if it has high payload, better imperceptibility and robustness. But there is always a trade-off between these three factors. Bit per pixel (bpp) is used to indicate the payload of a given method which is 1bpp for all mentioned algorithms except FMM and PIT. FMM is window size dependent algorithm which can lead towards lower payload even less than 1bpp and hence cannot be used in payload-demanding security applications. PIT method has high payload capacity among other competing methods but it is time consuming and cannot be used in real-time security applications, requiring fast processing. SCC disperses the secret data in red, green, and blue channels to improve security but still data can be easily extracted if some pixels are compromised as the data hiding pattern is fixed and data is in plain form. Karim's technique makes use of secret key during embedding process, increasing the security as compared to PIT, FMM, LSB, and SCC but compromising the key will enable the attacker to extract the actual data as data is not encrypted.

The robustness of all mentioned schemes including the proposed scheme is evaluated based on a dataset of 50 standard color images. A color secret image of dimension (64×64 pixels) is embedded in different cover images of dimension (512×512 pixels) and the

resultant stego images are attacked based on *salt & pepper* noise with noise density $D=0.05$. The embedded secret image is then extracted from the noisy stego images and its quality is evaluated using PSNR. This process is repeated for 50 images using the proposed method and other five state-of-the-art methods. The incurred results for robustness evaluation are listed in [Table 10](#).

Table 10. Robustness evaluation using PSNR based on “salt & pepper” noise with noise density ($D=0.05$)

Serial#	Image Name	Classic LSB Method	SCC[21] Method	PIT[11]	FMM[20]	Karim's Method[22]	Proposed Method
1	Lena	34.5886	30.1284	28.4031	26.9048	26.918	34.6448
2	Baboon	34.6121	26.4387	25.6398	26.7673	26.9407	34.7728
3	House	34.7114	29.4317	29.1023	27.0404	26.9328	34.6403
4	Fjet16	34.6595	25.3821	28.5631	26.914	26.9504	34.6382
5	Peppers	34.7114	30.0124	32.4389	26.7176	27.1899	34.6222
Avg. of 50 images		35.0131	28.6666	29.1458	27.1272	27.1321	34.7452

[Table 10](#) shows the quality of secret image extracted from noisy stego images based on PSNR. The PSNR score of classic LSB method is higher than all mentioned methods but it has the lowest security. The proposed scheme clearly dominates the other competing methods and provides good results in terms of robustness and imperceptibility. The proposed technique increases the robustness by encrypting the secret key as well as secret data using MLE which consist of BITXOR operation, bits shuffling procedure and secret key-based encryption. Furthermore, the usage of transposition adds an additional level of security and can deceive the attacker. These steps create multiple barriers in the way of an attacker and hence increase the robustness of proposed scheme which can be confirmed from [Table 10](#). In addition to this, the proposed method results in stego images whose quality is much more better than the existing five methods and hence cannot be easily detected using HVS. These properties conclude that the proposed technique out-performs the existing methods in terms of robustness, security and imperceptibility.

4.6 Advantages and limitations of the proposed method

The proposed scheme provides a robust, efficient and time saving way to hide secret information inside the cover image. The main advantages of the proposed scheme are improved quality of stego images, high imperceptibility, cost-effectiveness, and enhanced robustness. Moreover, the utilization of MLE and image transposition add multiple security levels to the said technique. The major shortcoming of this method is its vulnerability to different attacks (cropping, scaling and noise attacks) which exist in all spatial domain techniques including the existing five schemes. Since spatial domain is

used in the proposed approach, the hidden data cannot be fully recovered if image is compressed, scaled or attacked with noises as discussed in section 4.4.

5. Conclusion and Future Directions

A new faster and efficient color image steganographic method has been proposed to map secret data to the grey-levels of the carrier image using MLE and GLM without causing any noticeable distortion with high imperceptibility and security. An acceptable average PSNR score above 50dB is achieved using the proposed method which shows the high quality of stego images. The payload capacity of all mentioned algorithms is same i.e. 1bpp (bits per pixel) except FMM and PIT. The capacity of FMM is dependent on the window size but its running time is near to our proposed scheme. The PIT method is the most time consuming algorithm however it has payload capacity much more than existing five methods. By experimental results, we conclude that our proposed scheme provide better security, imperceptibility and robustness and require short processing time as compared to existing five schemes.

In future work, the authors plan to increase the payload of the proposed scheme by taking into consideration the relationship between nearby pixels i.e. edge and smooth area's pixels. In addition, MLEA will be further improved to make it more secure.

References

- [1] C. Qin, C.-C. Chang, and Y.-P. Chiu, "A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image Inpainting," *Image Processing, IEEE Transactions on*, vol. 23, pp. 969-978, 2014. [Article \(CrossRef Link\)](#)
- [2] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing*, vol. 90, pp. 727-752, 2010. [Article \(CrossRef Link\)](#)
- [3] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: an overview," *International Journal of Computer Science and Security (IJCSS)*, vol. 6, pp. 168-187, 2012. [Article \(CrossRef Link\)](#)
- [4] X. Liao and C. Shu, "Reversible Data Hiding in Encrypted Images Based on Absolute Mean Difference of Multiple Neighboring Pixels," *Journal of Visual Communication and Image Representation*, 2015. [Article \(CrossRef Link\)](#)
- [5] N. U. R. Jamil Ahmad, Zahoor Jan, Khan Muhammad, "A Secure Cyclic Steganographic Technique for Color Images using Randomization," *Technical Journal, University of Engineering and Technology Taxila, Pakistan*, vol. 19, pp. 57-64, 2014. [Article \(CrossRef Link\)](#)
- [6] W. Zhou, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *Image Processing, IEEE Transactions on*, vol. 13, pp. 600-612, 2004. [Article \(CrossRef Link\)](#)

- [7] W.-J. Chen, C.-C. Chang, and T. Le, "High payload steganography mechanism using hybrid edge detector," *Expert Systems with applications*, vol. 37, pp. 3292-3301, 2010. [Article \(CrossRef Link\)](#)
- [8] K. Muhammad, J. Ahmad, H. Farman, and M. Zubair, "A Novel Image Steganographic Approach for Hiding Text in Color Images Using HSI Color Model," *Middle-East Journal of Scientific Research*, vol. 22, pp. 647-654, 2014. [Article \(CrossRef Link\)](#)
- [9] H. R. Kanan and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm," *Expert Systems with Applications*, vol. 41, pp. 6123-6130, 2014. [Article \(CrossRef Link\)](#)
- [10] J. Mielikainen, "LSB matching revisited," *Signal Processing Letters, IEEE*, vol. 13, pp. 285-287, 2006. [Article \(CrossRef Link\)](#)
- [11] A. A.-A. Gutub, "Pixel indicator technique for RGB image steganography," *Journal of Emerging Technologies in Web Intelligence*, vol. 2, pp. 56-64, 2010. [Article \(CrossRef Link\)](#)
- [12] C.-M. Wang, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," *Journal of Systems and Software*, vol. 81, pp. 150-158, 2008. [Article \(CrossRef Link\)](#)
- [13] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, pp. 1613-1626, 2003. [Article \(CrossRef Link\)](#)
- [14] P.-Y. Chen and H.-J. Lin, "A DWT based approach for image steganography," *International Journal of Applied Science and Engineering*, vol. 4, pp. 275-290, 2006. [Article \(CrossRef Link\)](#)
- [15] W.-Y. Chen, "Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques," *Applied Mathematics and computation*, vol. 196, pp. 40-54, 2008. [Article \(CrossRef Link\)](#)
- [16] M. Fakhredanesh, M. Rahmati, and R. Safabakhsh, "Adaptive image steganography using contourlet transform," *Journal of Electronic Imaging*, vol. 22, pp. 043007-043007, 2013. [Article \(CrossRef Link\)](#)
- [17] H. Noda, M. Niimi, and E. Kawaguchi, "High-performance JPEG steganography using quantization index modulation in DCT domain," *Pattern Recognition Letters*, vol. 27, pp. 455-461, 2006. [Article \(CrossRef Link\)](#)
- [18] M. Hussain and M. Hussain, "A Survey of Image Steganography Techniques," *International Journal of Advanced Science & Technology*, vol. 54, 2013. [Article \(CrossRef Link\)](#)
- [19] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, pp. 142-172, 2011. [Article \(CrossRef Link\)](#)
- [20] F. A. Jassim, "A novel steganography algorithm for hiding text in image using five modulus method," *arXiv preprint arXiv:1307.0642*, 2013. [Article \(CrossRef Link\)](#)
- [21] K. Bailey and K. Curran, "An evaluation of image based steganography methods," *Multimedia Tools and Applications*, vol. 30, pp. 55-88, 2006. [Article \(CrossRef Link\)](#)
- [22] M. Karim, "A new approach for LSB based image steganography using secret key," in *14th International Conference on Computer and Information Technology (ICCIT 2011)*, pp. 286-291, 2011. [Article \(CrossRef Link\)](#)

- [23] T. Na and M. Kim, "A Novel No-Reference PSNR Estimation Method With Regard to Deblocking Filtering Effect in H. 264/AVC Bitstreams," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 24, pp. 320-330, 2014. [Article \(CrossRef Link\)](#)
- [24] Y. Fang, K. Zeng, Z. Wang, W. Lin, Z. Fang, and C.-W. Lin, "Objective Quality Assessment for Image Retargeting Based on Structural Similarity," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 4, pp. 95-105, 2014. [Article \(CrossRef Link\)](#)
- [25] M. Sajjad, I. Mehmood, and S. W. Baik, "Image super-resolution using sparse coding over redundant dictionary based on effective image representations," *Journal of Visual Communication and Image Representation*, vol. 26, pp. 50-65, 2015. [Article \(CrossRef Link\)](#)



Khan Muhammad received his BCS degree in Computer Science from Islamia College, Peshawar, Pakistan in 2014 with research in image processing. Currently, he is pursuing Joint Master-PhD degree in digital contents from Sejong University, Seoul, South Korea. His research interests include image processing, data hiding, steganography, watermarking, and video summarization.



Jamil Ahmad received his BCS degree in Computer Science from the University of Peshawar, Pakistan in 2008. He received his Master's degree in Computer Science with specialization in image processing from Islamia College, Peshawar, Pakistan. Currently, he is pursuing PhD degree in digital contents from Sejong University, Seoul, Korea. His research interests include image analysis, semantic image representation and content based multimedia retrieval.



Haleem Farman is a lecturer in the Department of Computer Science, Islamia College Peshawar Pakistan and PhD Scholar in the Department of Computer Sciences, University of Peshawar, Pakistan. His fields of interest include Wireless Sensor Networks, Mobile Ad-hoc Networks, and Image Processing



Zahoor Jan is currently holding the rank of an associate professor in computer science at Islamia College Peshawar, Pakistan. He received his MS and PHD degree from FAST University Islamabad in 2007 and 2011 respectively. He is also the chairman of Department of Computer Science at Islamia College Peshawar, Pakistan. His areas of interests include image processing, machine learning, computer vision, artificial intelligence and medical image processing, biologically inspired ideas like genetic algorithms and artificial neural networks, and their soft-computing applications, biometrics, and solving image/video restoration problems using combination of classifiers using genetic programming.



Muhammad Sajjad received his PhD degree in Digital Contents from Sejong University, Seoul, South Korea. He is now working as a research associate at Islamia College Peshawar, Pakistan. His research interests include digital image super-resolution and reconstruction, sparse coding, video summarization and prioritization, image/video quality assessment, and image/video retrieval.



Sung Wook Baik is a professor in the Department of Digital Contents at Sejong University. His research interests include Computer vision, Pattern recognition, Computer game and AI. He has a PhD degree in Information Technology and Engineering from George Mason University.