

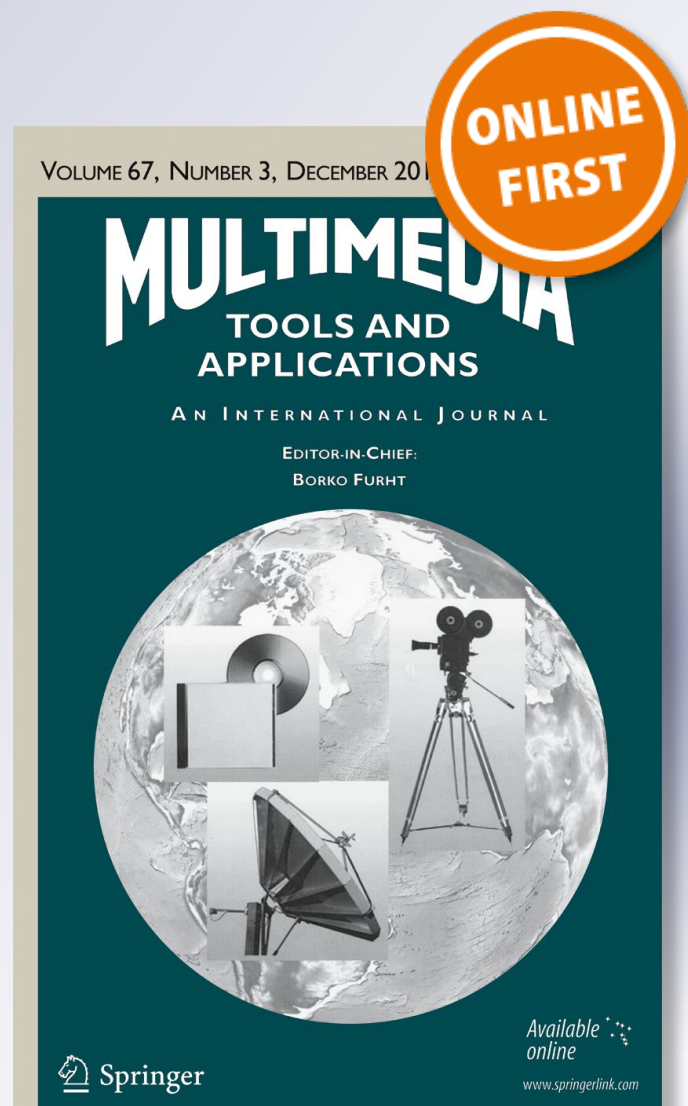
Image steganography for authenticity of visual contents in social networks

**Khan Muhammad, Jamil Ahmad,
Seungmin Rho & Sung Wook Baik**

Multimedia Tools and Applications
An International Journal

ISSN 1380-7501

Multimed Tools Appl
DOI 10.1007/s11042-017-4420-8



Your article is protected by copyright and all rights are held exclusively by Springer Science +Business Media New York. This e-offprint is for personal use only and shall not be self-archived in electronic repositories. If you wish to self-archive your article, please use the accepted manuscript version for posting on your own website. You may further deposit the accepted manuscript version in any repository, provided it is only made publicly available 12 months after official publication or later and provided acknowledgement is given to the original source of publication and a link is inserted to the published article on Springer's website. The link must be accompanied by the following text: "The final publication is available at link.springer.com".

Image steganography for authenticity of visual contents in social networks

Khan Muhammad¹  · Jamil Ahmad¹ · Seungmin Rho² ·
Sung Wook Baik¹

Received: 6 October 2016 / Revised: 25 December 2016 / Accepted: 20 January 2017
© Springer Science+Business Media New York 2017

Abstract Social networks are major sources of image sharing and secret messaging among the people. To date, such networks are not strictly bounded by copyright laws due to which image sharing, secret messaging, and its authentication is vulnerable to many risks. In addition to this, maintaining the confidentiality, integrity, and authenticity of secret messages is an open challenge of today's communication systems. Steganography is one of the solutions to tackle these problems. This paper proposes a secure cryptographic framework for authenticity of visual contents using image steganography, utilizing color model transformation, three-level encryption algorithm (TLEA), and Morton scanning (MS)-directed least significant bit (LSB) substitution. The method uses I-plane of the input image in HSI for secret data embedding using MS-directed LSB substitution method. Furthermore, the secret data is encrypted using TLEA prior to embedding, adding an additional level of security for secure authentication. The qualitative and quantitative results verify the better performance of the proposed scheme and provide one of the best mechanisms for authenticity of visual contents in social networks.

Keywords Information security · Authenticity of visual contents · Steganography · Multimedia security · Cryptography

✉ Sung Wook Baik
sbaik@sejong.ac.kr

Khan Muhammad
khan.muhammad.icp@gmail.com; khanmuhammad@sju.ac.kr; khan.muhammad@ieee.org

Jamil Ahmad
jamilahmad@sju.ac.kr

Seungmin Rho
smrho@sungkyul.edu

¹ Intelligent Media Laboratory, Digital Contents Research Institute, College of Electronics and Information Engineering, Sejong University, Seoul, Republic of Korea

² Department of Media Software, Sungkyul University, Anyang, Republic of Korea

1 Introduction

Steganography is a covert communication mechanism of secret messages between the sender and its recipient, deceiving the human visual system [7]. The main requirements of steganography include a cover object, secret data, and data hiding algorithm. Sometimes, an encryption mechanism is combined with steganography for better security of the secret data [42]. Steganography can be used for a number of useful applications including authenticity of images on social networking websites, secure national and international transmission of secret data, and securing online banking and voting systems [2, 3, 21]. It can also be quite nefarious as terrorists and criminals can use it for secret communication and sending Trojan horses and viruses to destroy systems [24, 39].

Steganographic techniques are divided into two categories: spatial domain techniques in which the pixels of the carrier image are directly altered for data embedding. For example, least significant bit (LSB) based techniques [7, 22, 24], pixel indicator techniques (PIT) [1, 14, 36], edges based techniques [9, 18, 22], and pixel value differencing (PVD) technique [44]. These techniques can carry large amount of data but are easily affected by image processing attacks such as rotation, scaling, and noise attacks. Transform domain techniques use the transformed co-efficients for information hiding such as discrete wavelength transform based methods, discrete Fourier transform based methods, and discrete cosine transform based techniques. These techniques are more resilience against image processing attacks but their payload is small and are computationally very complex [7]. Considering this reason, it is recommended to use spatial domain for applications requiring fast responses such as the current proposed work for authenticity in social networks.

1.1 Problem definition

Security of information during transmission is a major issue in this modern era. Almost, all social networking websites like Facebook, Instagram, and Twitter provide the basic facility of uploading and sharing our private images and secret communication via messages. The private images shared on these social websites are vulnerable to many risks [13, 38]. According to copyright laws of social networking, the person or website who uploads an image, keeps the ownership of that image. But these images can be easily modified by an intruder and can be used to perform illegal actions. Similarly if multiple users download a particular image, modify it and upload it back to its corresponding website/timeline, then it is relatively more difficult for a receiver to identify the actual owner of digital contents. Due to these reasons, authentication for top-secure systems and authenticity of visual contents on social networking websites become a major issue in today's challenging environment [10]. In this regard, the cryptographic methods can be used but they convert the appearance of visual contents into scrambled form. This makes the contents doubtful enough to draw the attackers' attention which in turn can result in decryption or modification of visual contents.

To surmount the aforementioned problems, we propose a new cryptographic framework based on steganography in this paper. Our major research contributions are highlighted as follows:

- i. A secure cryptographic framework assisted by steganography is proposed for authenticity of visual contents, and security of secret messages in social networks. To the best of our knowledge, we identify the problem of authenticity of visual contents in social networks for the first time and propose a steganography based framework which can be an effective solution.

- ii. Improved quality of stego images using HSI color space for better authenticity of visual contents, and security of secret data. The choice of HSI for steganography is inspired from its cost-effectiveness, suitability for steganographic techniques, and de-correlation property.
- iii. Encryption of secret key and secret data prior to data hiding using TLEA, increasing the security of proposed approach, hence making the extraction of embedded data more challenging for adversaries.
- iv. Data hiding using MS-directed LSB substitution method for random distribution of secret data in different regions of the cover image, leaving various distortions on cover image randomly, hence disturbing the steganalysis' estimation, making its identification less feasible by steganalysis methods.

The remaining of the paper is structured as follows. Related work is given in Section 2. The proposed work is illustrated in Section 3. The details of experiments and results are provided in Section 4. Section 5 highlights the key findings of the paper in conclusion.

2 Related work

LSB is the simplest method of data hiding with default payload of 1 bits per pixel (bpp). This payload can be increased if more than 1 LSBs are used for message embedding subject to compromising on image quality. LSB method is quite simple but it is easily detectable using different steganalysis detectors [9, 20].

To make these steganalysis approaches ineffective, a new method LSB matching (LSB-M) was proposed in [22]. LSB-M randomly adds 1 to the pixel of the image if the secret bit to be embedded does not match with the LSB of the pixel. This process reduces the asymmetric artifacts caused by simple LSB method. For better quality and less detection rate, the authors in [24] proposed LSB-M revisited (LSB-MR) by hiding two bits of data in a pixels pair. The first bit of secret data is embedded in the first pixel and second bit in the relationship between the given two pixels of the host image. LSB, LSB-M, and LSB-MR embed data in cover images using fixed pattern and hence its extraction is relatively easy for adversary. To distribute secret data in image, the authors in [5] proposed stego color cycle (SCC) method by using different channels in turn i.e. red, green, and blue. The SCC method is further improved by authors in [27] using randomization which makes the extraction of secret data more difficult comparing to SCC and methods using LSB as a baseline mechanism.

The LSB and cyclic LSB based methods use a cyclic systematic pattern for data hiding. This enables the attacker to extract the actual data if data from a few pixels is accurately extracted. Furthermore, the payload of these approaches is limited i.e. 1 bpp. To resolve these two problems, the authors in [36] suggested pixel indicator technique (PIT) which hides data in cover images by logically dividing the input image's channels into data channels and indicator channel. The payload of PIT can be lower in some cases due to its dependency on indicator channel. To overcome this limitation, the authors in [12] proposed a new scheme which hides secret data based on the pixel intensities. They introduced the usage of secret key in deciding the indicator channel to increase the security of [36]. The payload and security is further improved by the authors in [37] using partition schemes. Some other pixel indicator based methods can be found in [4, 41] that aim to increase the payload and security of existing PIT based methods.

The aforementioned methods manipulate every pixel of the cover image independently without taking into account the fact that whether a pixel lies at edge area or smooth area of the host image. The

authors in [9] investigated for the first time that edge area's pixels can carry more secret bits than smooth area's pixels. The payload of [9] is increased by authors in [8] using hybrid edge detectors. The authors in [22] merged the LSB-MR method [24] with edges based data hiding approach which resulted in larger payload and improved image quality. The authors in [16] nominated the 1st edges based approach for RGB images, resulting in payload three times larger than the mentioned edges based methods. The authors in [11] proposed a new edges based scheme that improves the payload as well as security. The existing mentioned edge based algorithms produce marked images of fixed quality which is their major limitation. The authors in [18] nominated a novel approach which resolves this limitation and can tune the quality of stego images as per requirement.

Majority of the methods discussed so far in literature result in low quality of stego images, increasing its detection chances by human vision system. Moreover, the existing methods embed data directly inside the image pixels in plain form which is much easier to extract if the steganographic algorithm is compromised. As a result, the attackers can easily hack the hidden secret data and hence cannot be used for authenticity in top-secret security systems. To solve these problems, we propose a secure cryptographic framework, utilizing HSI color space, TLEA, and MS-directed LSB substitution method, which can provide one of the best mechanisms for authenticity of visual contents on social media networks and secret communication of private messages.

3 The proposed cryptographic framework

The proposed framework uses cryptography to authenticate the visual contents and maintain the security of secret messages in social networking. Cryptography is the combination of cryptography and steganography. For cryptography, a new encryption algorithm termed as "TLEA" is used in the proposed framework. For steganography, MS-directed LSB substitution method is used, exploring HSI color space by hiding data in the achromatic component. HSI color space has been used for information hiding instead of RGB color space because of three main reasons mentioned in [30].

3.1 Problem solution

All the communicating bodies want the confidentiality, integrity, and authenticity of their secret information. Different approaches are used to cope with these security issues like digital certificate, digital signature, and cryptography but these methods alone cannot be used due to their limited security and suspiciousness of attackers. Steganography is one of the solutions to these problems due to its covert nature of communication. In the proposed solution, the login information of the actual owner, current date and time, and any other authenticity related secrets are first encrypted using TLEA and then embedded in the image that is to be uploaded to a social media network. This facilitates the actual user to authenticate the actual shared images as if someone modifies the actual image, it will not contain the embedded information.

3.2 Proposed method

The proposed technique is a new color image cryptographic technique, basing on RGB-to-HSI color model conversion, TLEA, and MS-directed LSB method. The secret data is encrypted using multiple levels of encryption (TLEA) such as BITXOR, bits shuffling, message blocks

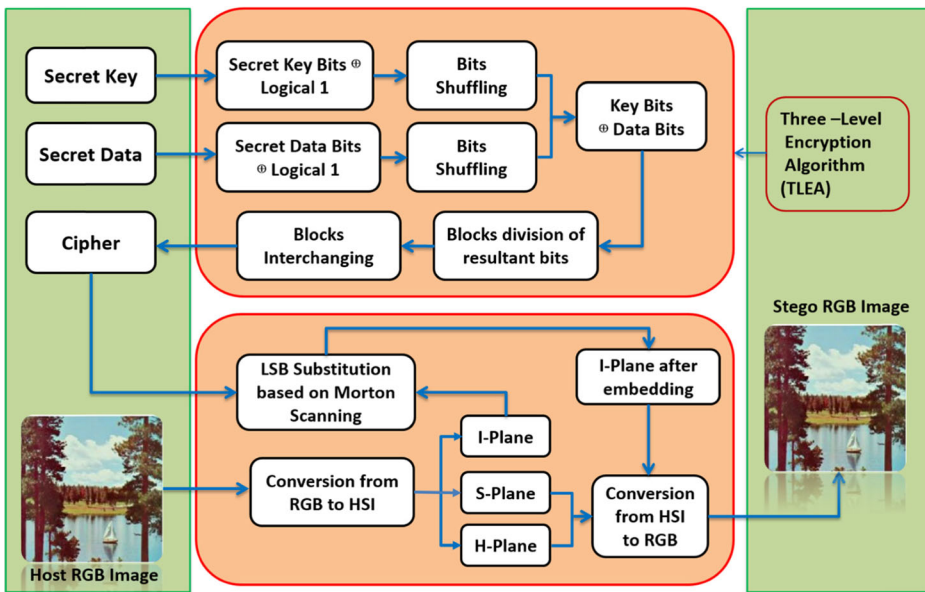


Fig. 1 Overall flow-diagram of the proposed cryptographic framework

division, and blocks interchanging using secret key. The encrypted data is then embedded in the I-plane of HSI color model using MS-directed LSB substitution method. Finally, the resultant image is re-transformed to RGB color model to make the stego image. The overall flow-diagram of the proposed system is depicted in Fig. 1. A summary of all the terminologies and input/output symbols used in the proposed cryptographic model are given in Table 1.

Table 1 Brief description of terminologies and input/output symbols

Serial#	Terminology/Symbol	Description
1	Host Image (I^H)	The host/cover/input image in which data will be embedded
2	I^{RGB}	The input image in RGB color model
3	I^{HSI}	The image converted to HSI color space
4	Stego Image ($I^{(RGB-S)}$)	The output image in RGB color space, containing secret data
5	TLEA	Three Level Encryption Algorithm
6	M	M shows the secret information which will be embedded in I^H
7	MT	An array containing the binary bits of secret message (M)
8	K	The secret key used in TLEA
9	T	An array containing the binary representation of secret key
10	M_1, M_2, M_3, M_4	The intermediate sub-blocks of the message bits.
11	MM	An array containing the final encrypted bits of secret data
12	$I^{I-plane}$	Intensity component i.e. the achromatic plane of I^{HSI}
13	$S^{S-plane}$	Saturation component i.e. the chromatic plane of I^{HSI}
14	$H^{H-plane}$	Hue component i.e. the chromatic plane of I^{HSI}
15	I^{MS}	The $I^{I-plane}$ after arranging its pixels using MS.
16	I^{MS-S}	The stego $I^{I-plane}$ after data hiding
17	I^{HSI-S}	The intermediate stego image in HSI color space
18	I^{RGB-S}	The final stego image in RGB color space

3.3 Three-level encryption algorithm (TLEA)

The TLEA encrypts the secret information before embedding it into the host image. TLEA consists of multiple encryption operations, increasing the security of embedded data for authentication and makes its extraction difficult for attackers, which is the major motivational factor behind its usage. The key steps of TLEA are presented in Algorithm 1.

Algorithm 1. Three-Level Encryption Algorithm (TLEA)

Input: Secret Message (M) and Secret Key (K)

1. **Initialize** $K \leftarrow \text{key}$, $M \leftarrow \text{secret message}$, $\text{temp (T)} \leftarrow \text{uint8}(\text{zeros}(1, (\text{length}(K) * 8)))$,
 $F \leftarrow T$, $j = 8$, $MT \leftarrow \text{uint8}(\text{zeros}(1, \text{length}(M) * 8))$
2. **for** each character $K(i)$ in secret key K and $M(i)$ in message M **do**
 - a. Convert $K(i)$ into 8-bits and concatenate it with T .
 - b. Convert $M(i)$ into 8-bits and concatenate it with MT .**end for**
3. **for** all bits in $T(i)$ and $MT(i)$, **do**
 - a. $T(i) \leftarrow (T(i) \oplus \text{logical } 1)$;
 - b. $MT(i) \leftarrow (MT(i) \oplus \text{logical } 1)$;**end for**
4. **Repeat** for each 8-bits combination in T and MT
 - for** $i = 1$ to 4 **do**
 - a. $t1 \leftarrow T(i)$ and $t2 \leftarrow MT(i)$;
 - b. $T(i) \leftarrow T(j)$ and $MT(i) \leftarrow MT(j)$;
 - c. $T(j) \leftarrow t1$ and $MT(j) \leftarrow t2$;
 - d. $j \leftarrow j - 1$;**end for**
 - $j \leftarrow 8$;**Until** (end of bits streams (T and MT))
5. **for** each bit $T(i)$ and $MT(i)$ **do**
 - $F(i) \leftarrow (T(i) \oplus MT(i))$**end for**
6. **for** each 8-bits block (B) in F **do**
 - a. $M_1 \leftarrow B(1)$ and $B(2)$; $M_2 \leftarrow B(3)$ and $B(4)$;
 - b. $M_3 \leftarrow B(5)$ and $B(6)$; $M_4 \leftarrow B(7)$ and $B(8)$;**end for**
7. Concatenate the resultant blocks in the order [M_4 , M_2 , M_1 and M_3] and assign it to MM which is the final array of bits.

Output: Encrypted secret data (MM)

For better explanation of the TLEA, consider a secret message with binary bits $M = (01000001, 01011011)_2$ and secret key bits $K = (11010010, 10110010)_2$. First the XOR operation between the bits of M and K is performed with logical 1. i.e. $[M \oplus \text{logical } 1] = [(01000001, 01011011)] \oplus [11111111, 11111111] = (10111110, 10100100)_2$ and $[K \oplus \text{logical } 1] = [(11010010, 10110010)] \oplus [11111111, 11111111] = (00101101, 01001101)_2$. Next, the resultant bits are shuffled based on a specific pattern as given in Fig. 2.

After applying this pattern on each byte of K and M , the resultant bits are $M = (01111101, 00100101)_2$ and $K = (10110100, 10110010)_2$. The third step is to apply the XOR operation between the resultant bits of M and K i.e. $(M \oplus K) = [(01111101, 00100101)] \oplus [(10110100, 10110010)] = [(11001001, 10010111)]$. The next step is to divide the whole cipher bits into 4 distinct blocks as follows:

Block Division Procedure

Input: Steam of bits

- a. Collect the 1st and 2nd bit of every byte and name it as M_1
- b. Collect the 3rd and 4th bit of every byte and store it in an array with name M_2
- c. Collect the 5th and 6th bit of every byte and store it in an array with name M_3
- d. Finally the 7th and 8th bit of every byte are stored in M_4

Output: Four blocks ($M_1, M_2, M_3,$ and M_4)

After applying this procedure on resultant bits, the 4 distinct blocks are $M_1 = (1110)_2$, $M_2 = (0001)_2$, $M_3 = (1001)_2$, and $M_4 = (0111)_2$. Lastly, the blocks are interchanged based on the pattern $P = [M_4, M_2, M_1, M_3]$ to form the final cipher bits. The final bit stream obtained as a result of TLEA is $M = [(01110001, 11101001)]_2$ which is absolutely different from the original bits stream i.e. $M = (01000001, 01011011)_2$.

3.4 Embedding algorithm

The embedding algorithm is a two-step process: HSI-to-RGB conversion and LSB substitution using MS. The input image of interest is converted into HSI and the secret information, encrypted by TLEA, is embedded in the achromatic component of HSI image using LSB substitution method. To increase the security and make the extraction of data more difficult for adversary, MS has been used in embedding process which is the motivational reason for its

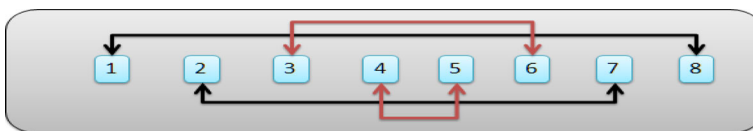


Fig. 2 Pattern for bits shuffling

usage. The major steps of embedding mechanism incorporated in the current framework are illustrated in Algorithm 2.

Algorithm 2. Embedding Algorithm

Input: Host Colour Image (I^H), Secret data (D) and Secret key (K)

1. **Initialize** $I^H \leftarrow$ RGB image, $D \leftarrow$ secret data, $K \leftarrow$ secret key
2. Apply TLEA using Algorithm 1 on D to get the encrypted bits stream MM.
3. Apply transformation on I^H to convert it from RGB to HSI color space i.e. $I^{RGB} \rightarrow I^{HSI}$
4. Split the converted image I^{HSI} into its three planes i.e. $I^{H-Plane}$, $I^{S-Plane}$ and $I^{I-Plane}$.
5. Arrange the pixels of $I^{I-Plane}$ based on MS to get I^{MS} as depicted in Fig. 3.
6. **While** counter \leq size of D **do**
 - a. Consider $I^{MS}(x, y)$ in the I-plane;
 - b. $t1 \leftarrow I^{MS}(x, y)$;
 - c. $t2 \leftarrow$ conversion of t1 to 8-bits binary format;
 - d. $t2(8) \leftarrow$ MM (counter);
 - e. counter \leftarrow counter + 1;
- end while**
7. Re-arrange the pixels of I^{MS} after embedding process to its original form to get I^{MS-S}
8. Combine $I^{H-Plane}$, $I^{S-Plane}$ and I^{MS-S} to get I^{HSI-S} which is the stego image in HSI color space.
9. Transform I^{HSI-S} into RGB color space to get I^{RGB-S} as a final stego image.

Output: Stego Image (I^{RGB-S})

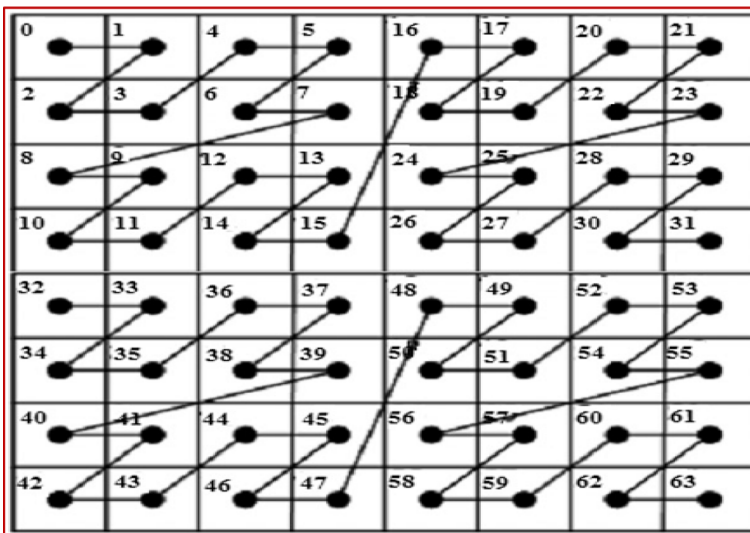


Fig. 3 Morton Scanning of a typical 8×8 image [17]

3.5 Extraction algorithm

The extraction algorithm transforms the stego RGB image into HSI color space and extracts the LSBs of I-plane based on MS. The extracted secret bits are then decrypted using the reverse operations of TLEA to get the actual hidden data which can then be used in authenticity of visual contents.

Algorithm 3. Extraction Algorithm

Input: Stego Image (I^{RGB-S}), Secret key (K)

1. **Initialize** $I^{RGB-S} \leftarrow$ stego RGB image, $K \leftarrow$ secret key
2. Apply transformation on I^{RGB-S} to convert it from RGB to HSI color space i.e. $I^{RGB-S} \rightarrow I^{HSI-S}$
3. Split the converted image I^{HSI-S} into its three planes i.e. $I^{H-Plane}$, $I^{S-Plane}$ and $I^{I-Plane}$.
4. Arrange the pixels of $I^{I-Plane}$ based on MS to get I^{MS} as depicted in Fig. 3.
5. **While** message size \geq counter **do**
 - a. $t \leftarrow$ conversion of I^{MS} (counter) to 8-bits representation;
 - b. $D(\text{counter}) \leftarrow t(8)$; % 8th bit i.e. LSB

End

6. Decrypt the resultant bits using the reverse operations of TLEA to get the original bits
7. Re-construct the original data from the achieved bits

Output: Secret data (D)

4 Experimental results and discussion

The performance of our method is evaluated using both quantitative and qualitative analysis based on various IQAMs and the results are compared with six state-of-the-art methods including LSB, LSB-M [22], LSB-MR [24], SCC [5], PIT [12], and Karim's method [19]. MATLAB R2013a has been used as a simulation tool. The test images have been taken from LIVE datasets [40], having TIFF format with dimension (256×256) and (512×512) pixels. These datasets are globally acceptable as a benchmark for evaluation of steganographic algorithms. Furthermore, they are used for benchmarking purposes. Due to these reasons, the selected images have been used for evaluation purposes in this paper including some well-known test images such as Lena, peppers, baboon, building, parrot, and trees. The following sub-sections explain the detail of experimental results and performance analysis.

4.1 Quantitative evaluation

In this section, the detail about various experiments conducted for performance evaluation is described. We conducted our experiments using three main perspectives as follows: 1) hiding the same amount of secret information (8 KB) in different images of the same dimensions (256×256) [perspective1], 2) hiding variable amount of cipher (2 KB, 4 KB, 6 KB, 8 KB) in the same image of the same dimension (256×256) [perspective2], and 3) hiding same amount of cipher (8 KB) in the same image of different dimensions $(128 \times 128, 256 \times 256, 512 \times 512,$

and 1024×1024) [perspective3]. The evaluation metrics include PSNR, NCC, MAE, SSIM, and RMSE which can be calculated using Eqs. 1–5 as follows [25, 31]:

$$PSNR = 10\log_{10}\left(\frac{C_{\max}^2}{MSE}\right) \tag{1}$$

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

$$NCC = \frac{\sum_{x=1}^M \sum_{y=1}^N (S(x,y) \times C(x,y))}{\sum_{x=1}^M \sum_{y=1}^N (S(x,y))^2} \tag{3}$$

$$MAE = \left(\frac{1}{N}\right) \sum_{x=1}^N |C_x-S_x| \tag{4}$$

$$SSIM(C, S) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{5}$$

PSNR computes the obvious distortion that is caused due to intentional embedding of secret data in host images for assessing the quality of stego images. The relationship between quality of stego image and PSNR is described as: "The higher is the PSNR; the better is the quality of stego image and vice versa" [32]. Figure 4 shows the individual PSNR score of each mentioned scheme for 10 standard color images based on perspective 1.

Figure 5 shows the average PSNR score of each mentioned method including the proposed method computed over 50 standard color images using perspective 1. The performance of SCC, PIT, and Karim’s method is almost same while classic LSB and LSB-M get better results

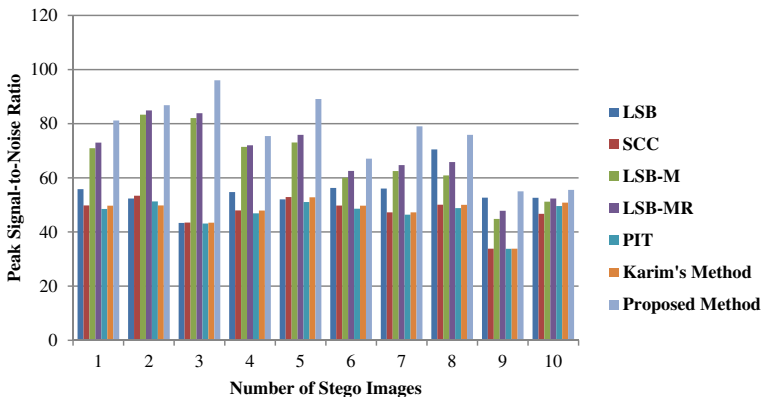
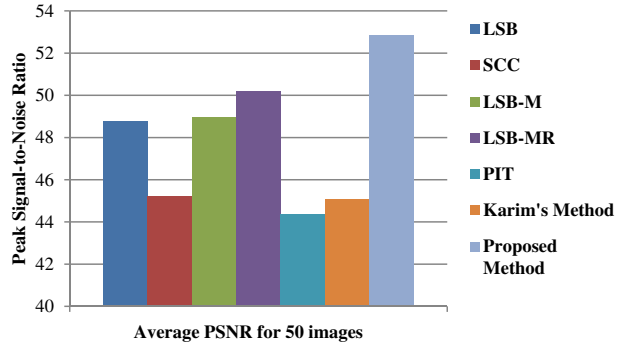


Fig. 4 PSNR versus number of images. PSNR score of each mentioned technique for 10 standard images

Fig. 5 Average value of PSNR computed over 50 images



as compared to SCC, PIT, and Karim’s method. The average PSNR score of LSB-MR is higher than other five competing methods. From Fig. 5, it is clear that our method dominates the other methods by getting the highest score of PSNR and hence validates its effectiveness.

NCC is calculated to determine how much the stego image is correlated to the original reference image. NCC closer to 1 shows the better quality of stego image. Figure 6 shows the NCC statistics of the proposed method and other steganographic methods for 50 images using perspective 1. From Fig. 6, it can be seen that the PIT and SCC methods have the lowest scores of NCC. LSB-MR and Karim’s method achieve higher score of NCC among other competing algorithms. Our method presents better results in terms of NCC also and hence shows its superiority over other methods.

RMSE is the simplest metric among all available IQAMs and is used to measure the root-mean-squared error between host and stego images. A smaller value of RMSE indicates the effectiveness of a given steganographic scheme [28]. Figure 7 shows the statistics of RMSE for each scheme computed over 50 images based on perspective 1. PIT gives worse results based on RMSE as its payload is higher compared to other competing methods. The average score of RMSE in our proposed method is the lowest and hence demonstrates better image quality over other methods.

MAE is also calculated to analyze the error range between input image and output stego image. The higher score of MAE shows the in-effectiveness of a given steganographic method. Figures 8 and 9 show the experimental results of all mentioned methods based on MAE using perspective 1. In Fig. 8, the MAE score of each method is mentioned for 5 standard images. The performance of SCC, LSB, and Karim’s method is approximately same. The results of LSB-M and LSB-MR in terms of MAE are worse as compared to SCC, LSB, and Karim’s method. PIT

Fig. 6 Average value of NCC computed over 50 standard color images

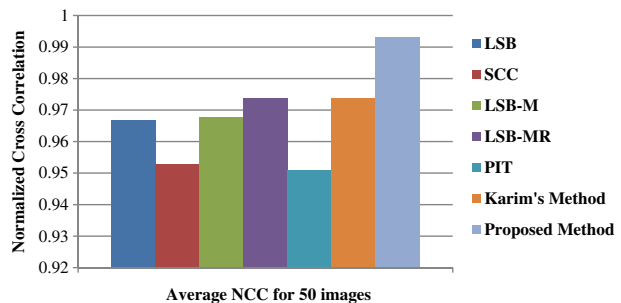
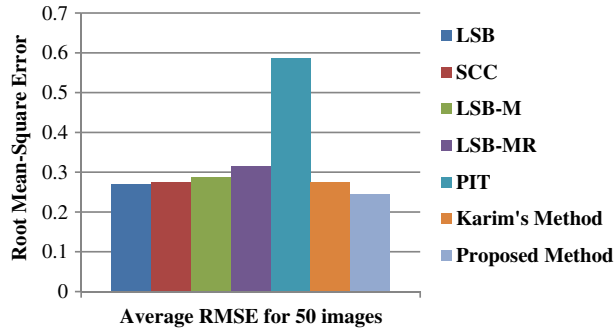


Fig. 7 Average value of RMSE computed over 50 standard color images



is the most in-effective method based on MAE over other competing methods. The MAE score in Fig. 9 for the proposed method in all five cases is the smallest and hence shows its better performance. Figure 9 shows the MAE statistics computed over 50 images. It is also clear from Fig. 9 that our proposed technique produces small amount of error due to intentional embedding of secret data in cover images in contrast to other state-of-the-art methods.

As human visual perception is mostly incorporated to extract the structural information from a given image, therefore, we measure the quality of stego images via degradation of structural information. In addition, the previous IQAMs ignore some of the structural information that is distorted during data hiding. Furthermore, PSNR with its corresponding RMSE produces wrong results in certain circumstances as proved by Wang [45]. Keeping in view these points, another metric SSIM is considered for evaluation. Figure 10 shows the average score of SSIM for each mentioned technique computed over 50 images using perspective 1. The SSIM score of SCC, PIT, and Karim’s method is approximately same. LSB and LSB-M have the 2nd highest score. LSB-MR obtains better results than other 5 competing algorithms. The proposed scheme leads the existing six schemes by achieving the highest score of SSIM. All the quantitative evaluation discussed so far validates that our method maintains the quality of marked images and hence can provide one of the best ways for authentication of secret images in social networks.

Figures 11 and 12 show the statistics of all mentioned schemes based on PSNR using perspective 2 for two standard images (Baboon and Lena). These two images have been selected for this type of evaluation because every newly designed algorithm needs to be tested with edgy and smooth images. In this case, Lena is a smooth image while baboon is an edgy image. The performance of other methods is different for smooth and edgy images. For instance, PIT method gives worse results for edgy image over other methods while it gives better results than

Fig. 8 MAE score for each mentioned scheme computed over 5 images

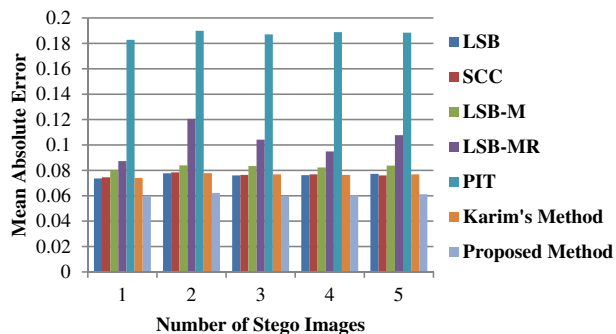
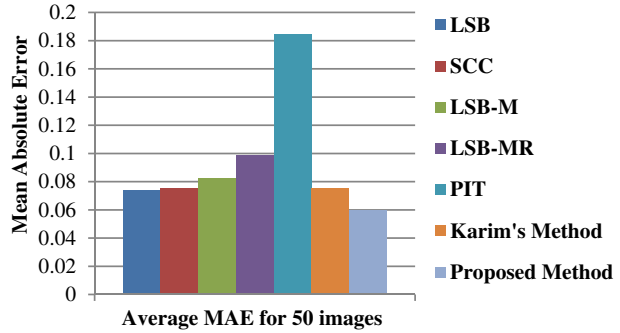


Fig. 9 Average score of all mentioned schemes for 50 images based on MAE



other competing methods for smooth image. The proposed method results in high score of PSNR for both edge and smooth images and hence validates its better performance.

Figures 13 and 14 show the quantitative results based on PSNR using perspective 3 for two standard images i.e. peppers and house. Figure 13 demonstrates that the performance of LSB, LSB-M, and LSB-MR is almost same. Similarly PIT, SCC, and Karim’s method produce approximately the same results. The proposed method obtains higher score of PSNR and shows its superiority over other methods. From Fig. 14 too, it is evident that our technique gives better results than other methods.

4.2 Qualitative evaluation

The visual quality of marked images for our method after intentional embedding is evaluated by comparison with other methods including LSB, SCC, LSB-M, LSB-MR, PIT, and Karim’s method. The image quality is considered to be better if detecting the existence of data inside it using HVS is difficult. Figure 15 shows the qualitative evaluation for our method and other mentioned schemes.

In Fig. 15, the top-left most image is a standard cover image “peppers” while the remaining are stego images of different steganographic techniques as written below each image. All the stego images contain 8 KB text embedded through various mentioned methods. From stego images, one can note the obvious distortion in peppers image for LSB, SCC, PIT, and Karim’s Method. Although, the stego images generated by LSB-M and LSB-MR do not contain visible distortion, yet its quality is lower than the proposed method as validated by various experiments. It is clear from above assessment that the stego images of our method are indistinguishable and are of high quality compared to other methods. Consequently, the better quality reduces detection

Fig. 10 Average value of SSIM computed over 50 standard color images

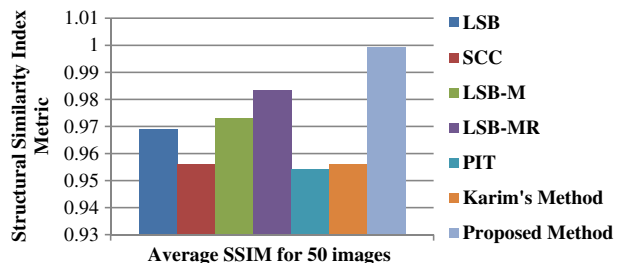
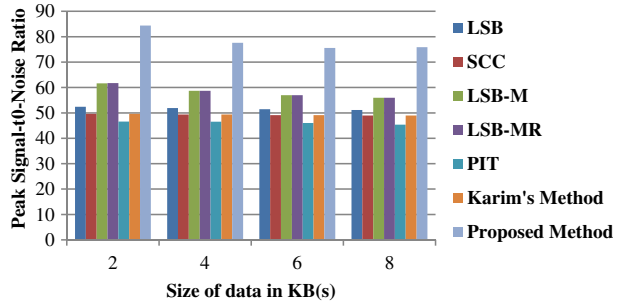


Fig. 11 Perspective 2 results: PSNR scores for baboon image



chances by adversaries, making our technique more suitable for visual contents authenticity and secure private communication.

4.3 Performance analysis of our scheme

This sub-section analyses the performance of our technique in contrast to other related techniques. In the area of steganography, three metrics of magic triangle are used to assess the performance of a given algorithm, which are payload, imperceptibility, and security [28]. Payload is the amount of hidden data in an image and is measured in bpp. Imperceptibility shows the quality of stego images and is measured using different IQAMs. Security determines the difficulty level in extraction of actual hidden data from the marked image. The first property (payload) is same for all mentioned methods except PIT while the other two properties are different. Classical LSB method results in good quality of stego image but it lacks security as the data can be easily hacked by just extracting LSB of each pixel. SCC method is better than LSB as it disperses the data in red, green, and blue channels of the host image but still the data can be extracted as data is in plain form. Karim’s method introduces the usage of secret key during embedding process and hides data in blue or green channel depending on the XOR result of secret key bits and LSBs of red channel, producing low-quality stego images compared to other methods and hence the hidden data is easily detectable using HVS. LSB-M and LSB-MR produce better results but they are less imperceptible compared to our method. PIT results in low quality stego images in most cases, having no security consideration but its payload is higher than all mentioned methods including the proposed scheme.

The proposed method dominates the existing mentioned methods in imperceptibility and security. The stego images generated using the proposed scheme demonstrates that it is a highly imperceptible algorithm and hence cannot be detected by the HVS. Furthermore, the proposed

Fig. 12 Perspective 2 results: PSNR scores for Lena image

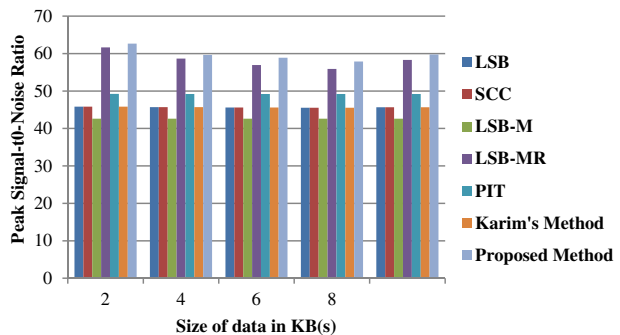
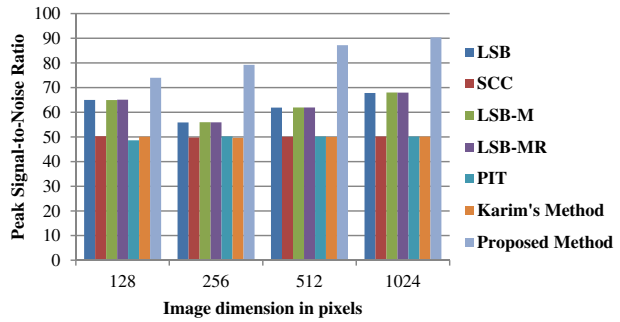


Fig. 13 Perspective 3 results; PSNR score for peppers image

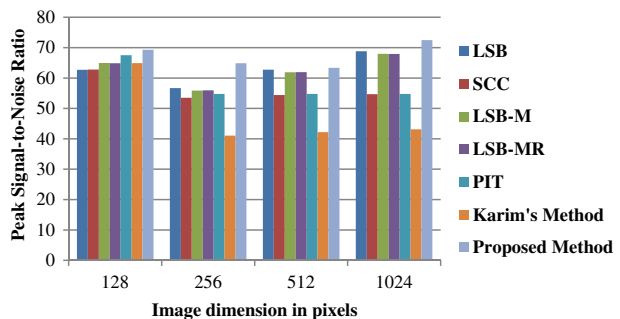


scheme provides multiple levels of security and hence makes the extraction of data more difficult for adversary. The attacker has to crack the stego key, the encryption scheme used for secret key and secret data, and steganographic algorithm to extract the concealed data. In addition to this, the usage of achromatic component (I-plane) can easily deceive the attacker. This results in an algorithm which has good imperceptibility, better quality of stego images, and multiple levels of security. Also, according to Wu's principle [43], it is considered a contribution of any steganographic method if it improves the stego image quality while keeping the payload unchanged or improve the payload with an acceptable image quality or improve both of them. Since, the proposed method improves the security and imperceptibility, therefore, according to Wu's principle, it is one of the contributions in the area of steganography.

4.4 Advantages, applications, and limitations of the proposed method

The main advantages of the proposed method is better quality of stego images, better imperceptibility, and improved security which provide better authenticity of secret data in context of social networking. Better quality of stego images and imperceptibility minimizes the chance of detectability by HVS. As a result, the chances to modify the uploaded stego image on social media reduces and hence results in better authenticity of secret data. Security shows how much difficult it is to extract the hidden data from stego image. In the proposed method, the use of I-plane instead of RGB, TLEA, MS based data hiding, and secret key make the extraction of secret information extremely difficult for attackers and hence increases its security. The proposed method is a good combination of better imperceptibility and security and can be adopted by social networking users for authenticity of their visual contents and security of private messages. Furthermore, individuals can also adopt it for only secret communication of sensitive information over the Internet.

Fig. 14 Perspective 3 results; PSNR score for house image







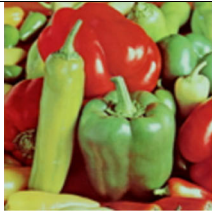



			
Peppers test image	LSB Method	SCC Method	LSB-M Method
			
LSB-MR Method	PIT	Karim's Technique	Our Scheme

Fig. 15 Visual quality assessment of our scheme and other methods for a test image

The proposed method can also provide various potential applications in medical field i.e. secure medical diagnosis for remote patient’s monitoring centers. In this context, we present here two possible applications including secure gait analysis and sleep monitoring. In gait analysis, a set of wearable sensors are used by clinicians to measure different gait parameters, which are helpful in the diagnostic procedure of numerous diseases including Huntington and Parkinson’s disease [6]. The transmission of these parameters to healthcare centers is quite sensitive and minor modification by attackers in such parameters can lead specialists to incorrect diagnosis. In this context, the proposed steganographic method can be incorporated for secure transmission of these parameters to healthcare centers, preserving patient’s privacy as well as improved diagnosis. In the same way, the proposed method can be used in secure remote sleep monitoring by sending various sensed parameters such as sleep deepness, duration, and sleep regularity to healthcare centers securely.

Although, the proposed method provides better security and authenticity for the secret data uploaded on social media, yet there is also a minor limitation in the proposed method and all the existing methods of spatial domain. The embedded secret data in stego images cannot be recovered fully if the stego image is affected with image processing attacks such as cropping, scaling, rotations, and noise attacks. In order to make the stego image resilience against image processing attacks, the steganographic technique must be implemented using transform domain which are computationally expensive with limited payload and hence are not preferable for security applications requiring real-time response.

5 Conclusions

In this paper, a new cryptographic framework for authenticity of visual contents in social networks is proposed based on HSI color space, MS-directed LSB substitution, secret key, and TLEA. The secret information is encrypted using TLEA before embedding, increasing the security of secret

data. The achromatic component (I-Plane) of HSI color model is used for message concealment based on MS, increasing the security and imperceptibility. An average PSNR of 65.57 dB is achieved with the proposed approach, demonstrating the high quality of stego images. Our method results in better imperceptibility and security which in turn provide better authenticity of visual contents in social networks. The qualitative and quantitative evaluation based on multiple IQAMs using three perspectives validate the superiority claimed by the proposed method. Our method can be potentially used in medical field for secure sleep monitoring and secure gait analysis.

In future, we plan to work on the practical implementation of the suggested applications for medical field by considering a real-world scenario. We also tend to combine the current work with image encryption algorithms [15] and other steganographic methods [26, 29] for further improvement in security. Further, the proposed work can be merged with video summarization techniques for authentication of medical videos such as wireless capsule endoscopy [23, 33] and diagnostic hysteroscopy [34, 35].

Acknowledgement This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2016R1D1A1A09919551).

References

1. Abu-Marie W, Gutub A, Abu-Mansour H (2010) Image based steganography using truth table based and determinate array on RGB indicator. *International Journal of Signal and Image Processing* 1:196–204
2. Al-Otaibi NA, Gutub AA (2014a) 2-Layer security system for hiding sensitive text data on personal computers. *Lecture Notes on Information Theory* 2:151–157
3. Al-Otaibi NA, Gutub AA (2014b) Flexible Stego-System for Hiding Text in Images of Personal Computers Based on User Security Priority. In: *Proceedings of 2014 International Conference on Advanced Engineering Technologies (AET-2014)*, pp 250–256
4. Amirtharajan R, Archana P, Rajesh V, Devipriya G, Rayappan J, (2013) Standard deviation converges for random image steganography. In: *Information & Communication Technologies (ICT), 2013 I.E. Conference on*, 2013, pp 1064–1069
5. Bailey K, Curran K (2006) An evaluation of image based steganography methods. *Multimedia Tools and Applications* 30:55–88
6. Buke A, Gaoli F, Yongcai W, Lei S, Zhiqi Y (2015) Healthcare algorithms by wearable inertial sensors: a survey. *Communications, China* 12:1–12
7. Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: survey and analysis of current methods. *Signal Process* 90:727–752
8. Chen W-J, Chang C-C, Le THN (2010) High payload steganography mechanism using hybrid edge detector. *Expert Syst Appl* 37:3292–3301
9. Dumitrescu S, Wu X, Wang Z (2003) Detection of LSB steganography via sample pair analysis. *IEEE Trans Signal Process* 51:1995–2007
10. Grover N, Mohapatra A, (2013a) Digital Image Authentication Model Based on Edge Adaptive Steganography. In: *Advanced Computing, Networking and Security (ADCONS), 2013 2nd International Conference on*, 2013, pp 238–242
11. Grover N, Mohapatra A, (2013b) Digital image authentication model based on edge adaptive steganography. In: *2013 2nd International Conference on Advanced Computing, Networking and Security*, pp 238–242
12. Gutub AA-A (2010) Pixel indicator technique for RGB image steganography. *Journal of Emerging Technologies in Web Intelligence* 2:56–64
13. Gutub A, (2015) Social Media & its Impact on e-governance. *ME Smart Cities 2015-4th Middle East Smart Cities Summit*
14. Gutub A, Ankeer M, Abu-Ghalioun M, Shaheen A, Alvi A, (2008) Pixel indicator high capacity technique for RGB image based Steganography. In *WoSPA 2008-5th IEEE International Workshop on Signal Processing and its Applications*

15. Hamza R, Titouna F, (2016) A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. *Information Security Journal: A Global Perspective* 1–18. doi:10.1080/19393555.2016.1212954
16. Ioannidou A, Halkidis ST, Stephanides G (2012) A novel technique for image steganography based on a high payload method and edge detection. *Expert Syst Appl* 39:11517–11524
17. Jan Z, Mirza AM (2012) Genetic programming-based perceptual shaping of a digital watermark in the wavelet domain using Morton scanning. *J Chin Inst Eng* 35:85–99
18. Kanan HR, Nazeri B (2014) A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. *Expert Syst Appl* 41:6123–6130
19. Karim M, (2011) 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
20. Ker AD (2005) A general framework for structural steganalysis of LSB replacement. *Information Hiding* 2005:296–311
21. Liu Z, Zhang F, Wang J, Wang H, Huang J (2015) Authentication and recovery algorithm for speech signal based on digital watermarking. *Signal Process* 123:157–166
22. Luo W, Huang F, Huang J (2010) Edge adaptive image steganography based on LSB matching revisited. *IEEE Trans Inf Forensics Secur* 5:201–214
23. Mehmood I, Sajjad M, Baik SW (2014) Mobile-cloud assisted video summarization framework for efficient Management of Remote Sensing Data Generated by wireless capsule sensors. *Sensors* 14:17112–17145
24. Mielikainen J (2006) LSB matching revisited. *IEEE Signal Process Lett* 13:285–287
25. Mstafa RJ, Elleithy KM (2016a) A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes. *Multimedia Tools and Applications* 75:10311–10333
26. Mstafa RJ, Elleithy KM, (2016b) Compressed and raw video steganography techniques: a comprehensive survey and analysis. *Multimedia Tools and Applications* 1–38. doi:10.1007/s11042-016-4055-1
27. Muhammad K, Ahmad J, Rehman NU, Jan Z, Qureshi RJ (2015a) A secure cyclic steganographic technique for color images using randomization. *Technical Journal, University of Engineering and Technology Taxila* 19:57–64
28. Muhammad K, Ahmad J, Farman H, Jan Z, Sajjad M, Baik SW (2015b) A secure method for color image steganography using gray-level modification and multi-level encryption. *KSII Transactions on Internet and Information Systems (TIIS)* 9:1938–1962
29. Muhammad K, Ahmad J, Sajjad M, Zubair M (2015c) Secure image steganography using cryptography and image transposition. *NED Univ J Res* 12:81–91
30. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW (2016a) A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. *Multimedia Tools and Applications* 75:14867–14893
31. Muhammad K, Ahmad J, Rehman NU, Jan Z, Sajjad M, (2016b) CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. *Multimedia Tools and Applications* 1–30. doi:10.1007/s11042-016-3383-5
32. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW, (2016c) Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems*. doi:10.1016/j.future.2016.11.029
33. Muhammad K, Sajjad M, Baik SW (2016d) Dual-level security based Cyclic18 steganographic method and its application for secure transmission of Keyframes during wireless capsule endoscopy. *J Med Syst* 40:1–16
34. Muhammad K, Ahmad J, Sajjad M, Baik SW (2016e) Visual saliency models for summarization of diagnostic hysteroscopy videos in healthcare systems. *Springer Plus* 5:1495
35. Muhammad K, Sajjad M, Lee MY, Baik SW (2017) Efficient visual attention driven framework for key frames extraction from hysteroscopy videos. *Biomed Signal Process Control* 33:161–168
36. Parvez MT and Gutub AA-A (2008) RGB intensity based variable-bits image steganography. In *Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE*, pp 1322–1327
37. Parvez MT, Gutub AA-A (2011) Vibrant color image steganography using channel differences and secret data distribution. *Kuwait J Sci Eng* 38:127–142
38. Patsakis C, Zigomitos A, Papageorgiou A, Solanas A (2015) Privacy and security for multimedia content shared on OSNs: issues and countermeasures. *Comput J* 58:518–535
39. Qazanfari K, Safabakhsh R (2014) A new steganography method which preserves histogram: generalization of LSB $\llbracket \sup \gg \llbracket \sup \gg$. *Inf Sci* 277:90–101
40. Sheikh HR, Wang Z, Bovik AC, Cormack L (2003) Image and video quality assessment research at LIVE
41. Swain G, Lenka SK (2012) A novel approach to RGB Channel based image steganography technique. *Int Arab J e-Technol* 2:181–186
42. Tang M, Hu J, Song W (2014) A high capacity image steganography using multi-layer embedding. *Optik-International Journal for Light and Electron Optics* 125(15):3972–3976. doi:10.1016/j.ijleo.2014.01.149
43. Wu N-I, Hwang M-S (2007) Data hiding: current status and key issues. *IJ Network Security* 4:1–9

44. Wu D-C, Tsai W-H (2003) A steganographic method for images by pixel-value differencing. *Pattern Recogn Lett* 24:1613–1626
45. Zhou W, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. *IEEE Trans Image Process* 13:600–612



Khan Muhammad received his BS degree in computer science from Islamia College, Peshawar, Pakistan with research in information security. Currently, he is pursuing MS leading to Ph.D. degree in digitals contents from College of Electronics and Information Engineering, Sejong University, Seoul, Republic of Korea. He is working as a researcher at Intelligent Media Laboratory (IM Lab) since 2015 under the supervision of Prof. Sung Wook Baik. His research interests include image and video processing, data hiding, image and video steganography, video summarization, diagnostic hysteroscopy, wireless capsule endoscopy, CCTV video analytics, and deep learning. He has published 18+ papers in peer-reviewed international journals and conferences such as Future Generation Computer Systems, Biomedical Signal Processing and Control, IEEE Access, Journal of Medical Systems, Multimedia Tools and Applications, SpringerPlus, KSII Transactions on Internet and Information Systems, International Journal of Applied Pattern Recognition, Journal of Korean Institute of Next Generation Computing, NED University Journal of Research, Technical Journal, Sindh University Research Journal, Middle-East Journal of Scientific Research, MITA 2015, PlatCon 2016, and FIT 2016. He is a student member of IEEE.



Jamil Ahmad received his BCS and MS degree in Computer Science from the University of Peshawar, and Islamia College, Peshawar, Pakistan, respectively. Currently, he is pursuing PhD degree in digital contents from Sejong University, Seoul, South Korea. His research interests include image analysis, semantic image representation, and content based multimedia retrieval. He is a student member of IEEE.



Seungmin Rho is a faculty of Department of Media Software at Sungkyul University in Korea. In 2012, he was an assistant professor at Division of Information and Communication in Baekseok University. In 2009-2011, he had been working as a Research Professor at School of Electrical Engineering in Korea University. In 2008-2009, he was a Postdoctoral Research Fellow at the Computer Music Lab of the School of Computer Science in Carnegie Mellon University. He gained his B.S degree in Computer Science from Ajou University. He received his MS and PhD degrees in Information and Communication Technology from the Graduate School of Information and Communication at Ajou University, South Korea. He visited Multimedia Systems and Networking Lab in University of Texas at Dallas from Dec. 2003 to March 2004. Before he joined the Computer Sciences Department of Ajou University, he spent two years in industry. His current research interests include database, big data analysis, music retrieval, multimedia systems, machine learning, knowledge management as well as computational intelligence.



Sung Wook Baik received the B.S degree in computer science from Seoul National University, Seoul, Korea, in 1987, the M.S. degree in computer science from Northern Illinois University, Dekalb, in 1992, and the Ph.D. degree in information technology engineering from George Mason University, Fairfax, VA, in 1999. He worked at Datamat Systems Research Inc. as a senior scientist of the Intelligent Systems Group from 1997 to 2002. In 2002, he joined the faculty of the College of Electronics and Information Engineering, Sejong University, Seoul, Korea, where he is currently a Full Professor and Dean of Digital Contents. He is also the head of Intelligent Media Laboratory (IM Lab) at Sejong University. His research interests include computer vision, multimedia, pattern recognition, machine learning, data mining, virtual reality, and computer games. He is a professional member of IEEE.