J Med Syst (2016) 40:114
DOI 10.1007/s10916-016-0473-x

MOBILE SYSTEMS

Dual-Level Security based Cyclic18 Steganographic Method and its Application for Secure Transmission of Keyframes during Wireless Capsule Endoscopy

Khan Muhammad[1] · **Muhammad Sajjad**[2] · **Sung Wook Baik**[1]

Received: 9 January 2016 / Accepted: 7 March 2016

Abstract In this paper, the problem of secure transmission of sensitive contents over the public network *Internet* is addressed by proposing a novel data hiding method in encrypted images with dual-level security. The secret information is divided into three blocks using a specific pattern, followed by an encryption mechanism based on the three-level encryption algorithm (TLEA). The input image is scrambled using a secret key, and the encrypted sub-message blocks are then embedded in the scrambled image by cyclic18 least significant bit (LSB) substitution method, utilizing LSBs and intermediate LSB planes. Furthermore, the cover image and its planes are rotated at different angles using a secret key prior to embedding, deceiving the attacker during data extraction. The usage of message blocks division, TLEA, image scrambling, and the cyclic18 LSB method results in an advanced security system, maintaining the visual transparency of resultant images and increasing the security of embedded data. In addition, employing various secret keys for image scrambling, data encryption, and data hiding using the cyclic18 LSB method makes the data recovery comparatively more challenging for attackers. Experimental results not only validate the effectiveness of the proposed framework in terms of visual quality and security compared to other state-of-the-art methods, but also suggest its feasibility for secure transmission of diagnostically important keyframes to healthcare centers and gastroenterologists during wireless capsule endoscopy.

Keywords Information security · Wireless capsule endoscopy · Image encryption · Steganography · Video summarization · Medical image analysis

This article is part of the Topical Collection on *Mobile Systems*

✉ Sung Wook Baik
sbaik@sejong.ac.kr

Khan Muhammad
khanmuhammad@sju.ac.kr

Muhammad Sajjad
muhammad.sajjad@icp.edu.pk

[1] Digital Contents Research Institute, Sejong University, Seoul, Republic of Korea

[2] Digital Image Processing Laboratory, Islamia College Peshawar, Peshawar, Pakistan

Introduction

Cryptography is one of the most well-known methods of secure communication, converting secret data into unreadable forms before transmission, ensuring its integrity, confidentiality, and authenticity. The encrypted unreadable data transmitted over the Internet usually diverts the attention of adversaries who intend to decrypt or modify it and thereby instigate a beach of sensitive data [1]. To address this issue, the idea of steganography is proposed, which provides a secure channel for covert communication over the Internet. It enables users to embed their secret messages inside innocent carriers including text, images, videos, audio, and network packets such that its existence is undetectable by human visual system (HVS) and is known only to the communicating bodies [2].

Over the past decade, numerous steganographic methods have been proposed by researchers focusing on payload, imperceptibility, and security. These methods are applicable in various applications including tamper-proofing, online voting security, copyright protection, and covert communication [3]. Steganographic techniques can be classified into two classes:

Published online: 19 March 2016

spatial domain techniques (direct modification of host image pixels) and frequency domain techniques (host image is transformed into frequency domain, and a secret message is embedded inside its co-efficients) [1]. Spatial domain techniques have a higher payload and better imperceptibility but can be easily affected by different normal and geometric attacks such as cropping, compression, rotations, and noise attacks. Spatial domain approaches include LSB based methods [4–6], edges based approaches [7–9], pixel indicator techniques (PIT) [10–12], and pixel value differencing (PVD) methods [1]. On the other hand, frequency domain techniques are computationally complex in nature and lack the larger embedding capacity but are comparatively resilient against different attacks. Transform domain approaches include discrete wavelet transform, Arnold transform techniques, integer contour transform, and discrete cosine transform based methods [13–18]. Higher payload, good image quality, and less computational complexity make spatial domain schemes more feasible for medical security applications such as secure transmission of electronic patient records (EPR) and keyframes of wireless capsule endoscopy (WCE) to healthcare centers [19].

The limited capacity along with extensive computations of transform domain techniques make them less suitable for various security applications. Therefore, our security framework uses spatial domain for data hiding, and the literature presented here is related to spatial domain. The basic method of spatial domain data hiding is LSB substitution, wherein the LSBs of any input image are substituted with secret information. This method is quite simple and can be easily detected. Keeping in view this shortcoming, various improved versions of the LSB method have been proposed in literature [20, 21], focusing on its payload, visual quality, and security [22]. Wang [23] integrated the LSB method with a genetic algorithm for improving the visual quality but with extra computational complexity, which was reduced by Chang [24] using dynamic programming based LSB substitution. Chan [25] presented pixel adjustment based data hiding approach increasing the perceptual transparency. Thien [26] combined the LSB method with modulus functions, obtaining an acceptable visual quality. Wu [27] integrated the LSB approach with pixel value differencing, resulting in a relatively higher payload and better visual quality.

The LSB based methods are easy to implement but can be easily compromised using different steganalysis detectors [25, 28]. To handle this issue, the authors in [7] presented the LSB matching (LSBM) technique by randomly adding/subtracting 1 to/from the pixel value based on the bits of secret information producing minimal artifacts in host images. Mielikainen [6] nominated LSBM revisited (LSBMR) method by embedding two bits in a pair of pixels, thus reducing the modification rate from 0.5 to 0.375 per pixel. To increase the payload of LSB based techniques, Parvez [29] presented PIT where data is embedded in one or two channels, selected based on fixed indicator channel. Adnan [11] nominated secret key based indicator selection technique by considering the channel intensity, increasing the payload. To increase the security and further improve the payload, various pixel indicator based techniques have been proposed by researchers in the literature [11, 30–34].

The techniques discussed earlier use the concept of pixel indicator and LSB, not considering the pixels' relationship during data hiding. Tsai [28] took into consideration the pixels' relationship by hiding more bits in edge area pixels that are less detectable by HVS, providing a higher payload. Chen [35] utilized hybrid edge detectors, further improving the payload. Lue [7] integrated LSBMR with Tsai's technique [28], resulting in a higher payload as well as better visual quality. Ioannidou [8] extended the edge based technique to RGB images, providing a threefold higher payload as compared to grayscale images. Grover [36] divided the secret data into edge and non-edgy blocks and embedded 3 bits per edgy pixels and 2 bits per smooth pixel, traversing the image from center, increasing the security and payload with a fixed quality. Kanan [9] presented a new edge based approach by tuning the quality and payload, increasing its feasibility of usage for various applications.

The aforementioned techniques directly embed secret data in images without shuffling and encryption. This limitation makes the extraction of secret data easy for attackers subject to successful discovery of the embedding algorithm. In addition, the host image is not scrambled prior to data hiding, decreasing the level of security. Furthermore, some of the existing techniques produce low quality stego images with visible visual artifacts, hence reflecting the attention of the adversaries during transmission.

In this paper, we propose an imperceptible steganographic technique to overcome the mentioned limitations. The main contributions of this work are summarized as follows:

1. A novel crystographic framework by combining the strengths of image scrambling, cryptography, and steganography for secure transmission of secret information and especially for electronic patient records to healthcare centers.
2. Encrypting the secret information prior to data hiding using a three-level-encryption algorithm (TLEA), introducing an extra layer of security. In addition, the host

image is scrambled before data embedding, increasing the complexity of data extraction, and hence making the brute force attack less feasible.
3. A novel data hiding scheme called "cyclic18 LSB substitution" is proposed, producing visually high quality stego images and scattering the secret data/EPR in different channels of the host image, hence making the extraction more challenging for attackers.
4. An important application of the proposed framework for secure transmission of keyframes extracted from WCE videos using video summarization to remote patient monitoring centers and gastroenterologists. The application has many advantages to healthcare centers such as preservation of patients' privacy, reduction in transmission cost, saving the gastroenterologists' time of browsing and analysis, and improved diagnosis.

The rest of the paper is organized as follows. The proposed framework is detailed in Section 2, followed by experimental results and discussion in Section 3. Section 4 explains the application of the proposed framework in secure wireless capsule endoscopy. Section 5 concludes the paper and suggests future work.

The proposed security framework

In this section, we describe the main components of the proposed framework along with simple examples, clarifying its conceptual novelty. First, the input image is rotated at 180° and then scrambled based on a secret key, resulting in scramble planes. The motivational factor behind rotation and image scrambling is to increase the complexity of data recovery for attackers, making the brute force attack less feasible. Next, the secret information is divided into three sub-blocks based on a secret pattern in the ratio 4:3:1 and are encrypted using TLEA. For ease of understanding, the proposed division mechanism is illustrated using the following example.

Consider a message M with S characters where each character can be represented by an ASCII value of 8 bits. Suppose N contains the binary bits of M. For division of "N" into three blocks m_1, m_2, and m_3 in the ratio 4:3:1, we have used the mechanism of Eq. 1 as follows:

$$\left\{\begin{array}{l} m_1 = \frac{N}{2} \\ m_2 = \frac{3 \times N}{8} \\ m_3 = \frac{N}{8} \end{array}\right\} \quad (1)$$

The reason for this data division is twofold: i) to embed the largest portion of data m_1 into the LSB plane, the second larger block m_2 into second LSB plane, and finally the smallest block m_3 into the third LSB plane and ii) to keep the modification rate at the lowest possible minimum. Finally, the encrypted blocks are embedded within the scrambled image using an extension of the LSB substitution method known as cyclic18 LSB substitution. The major steps of the proposed framework are shown in Fig. 1.

Secret key based image scrambling

In this sub-section, we briefly describe the proposed image scrambling method. Four different sub-keys have been used to complete the whole process of image scrambling. Sub-key$_1$ is used for scrambling the eight planes of green channel, sub-key$_2$ is used for scrambling the eight planes of red channel, sub-key$_3$ is utilized for scrambling of blue channel, and finally sub-key$_4$ is used to combine the three encrypted channels, resulting in a scrambled image. The proposed keys play two important roles in image scrambling: rotating each plane of a channel on a different angle and swapping the eight planes of a given channel. Each sub-key consist of eight digits except sub-key$_4$, which is 3 digits long. These sub-keys are combined for making a scrambling secret key, controlling the entire process of image scrambling.

Three-level encryption algorithm (TLEA)

The TLEA encrypts the three message blocks of secret information prior to applying the cyclic18 LSB substitution algorithm. This newly designed algorithm contains three different sub-procedures including bitxor of stego key bits and message bits with 1, bits shuffling procedure, and encrypted secret key based encryption. The motivational reason behind its usage is to increase the security of embedded data, introducing extra barriers in the way of an attacker, hence making data recovery more challenging. The main steps are depicted by flowchart in Fig. 2.

To briefly explain the proposed encryption scheme, consider M as a secret message such that M="*C*" with binary equivalent B= $(01000011)_2$ and K as a stego key with binary K= $(01011011)_2$. First of all, the bitXOR operation is applied on the stego key and message bits such that B_1= $(01000011 \oplus 11111111) = (10111100)_2$ and K_1= $(01011011 \oplus 11111111) = (10100100)_2$. The second sub-procedure is to apply the bits shuffling scheme on both of the resultant bits i.e. B_2=shufflingScheme (B_1) = shufflingScheme $(10111100)_2 = (01111100)_2$ and K_2=

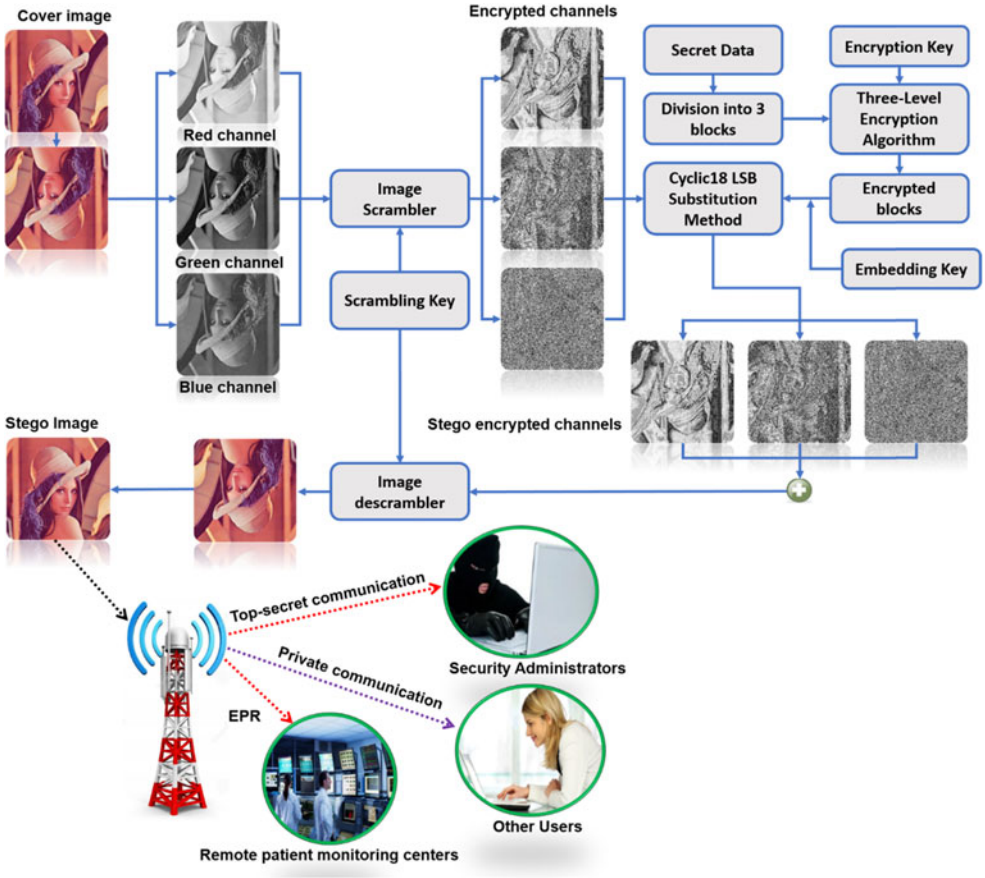

Fig. 1 Detailed pictorial representation of the proposed framework

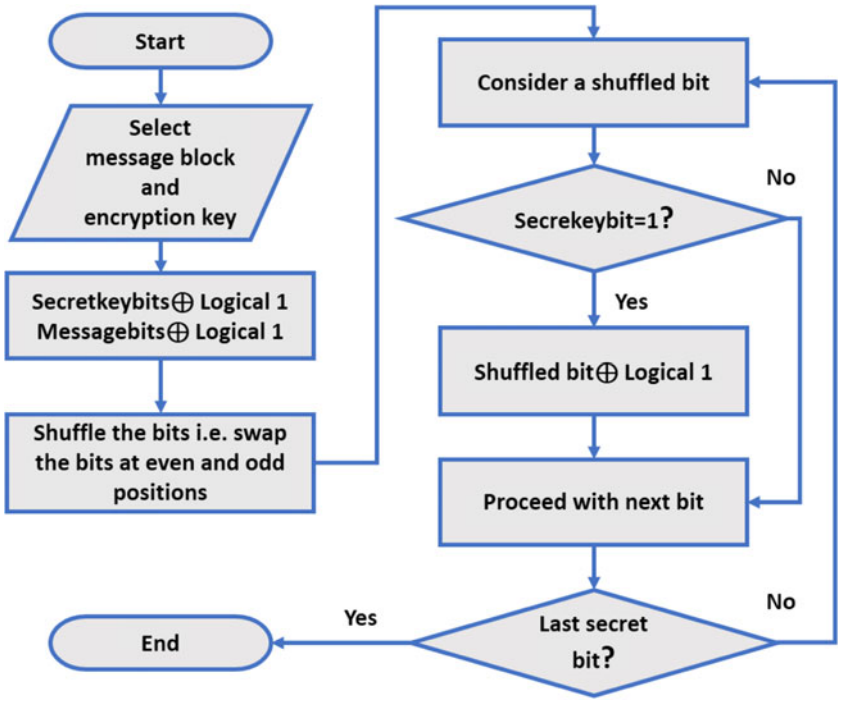

Fig. 2 Flowchart of three-level encryption algorithm

shufflingScheme (K_1) = shufflingScheme $(10100100)_2$ = $(01011000)_2$. The final sub-procedure is encrypted stego key based encryption that is applied on B_2 using K_2. The third procedure works as follows:

Encrypted stego key based encryption	
i.	Set finalBits=[ ] % Empty
ii.	If a shuffled and encrypted bit in K_2= 1 Then apply bitXOR (B_2 bit, logical 1) and append the resultant bit with finalBits array. Else Append B_2 bit with finalBits array without bitXOR operation.
iii.	Repeat step 2 until all bits are encrypted

Applying this procedure on B_2 bits using K_2 results in finalBits= $(00100100)_2$, which is completely different from the actual sequence of secret bits B= $(01000011)_2$. For decryption, the reverse operations are applied, i.e. bitXOR of stego key bits with logical 1, bits shuffling of resultant stego key, shuffled key based decryption of original encrypted bits, and finally bitXOR of message bits with logical 1.

Cyclic18 LSB embedding algorithm

The proposed embedding algorithm hides the encrypted secret bits in the LSBs of the host image in a randomized pattern, increasing its security. The pattern in which the message bits are embedded in different channels of the carrier image is RGB, RBG, GRB, GBR, BRG, BGR, and so on. These six pairs each of three planes, result in eighteen channels. That is why the proposed scheme is termed as cyclic18 LSB method. The motivational reason behind using cyclic18 LSB substitution is to scatter the secret information in the LSBs and intermediate LSBs of the host image, making the data recovery more challenging for malicious users, hence increasing the security of steganographically hidden data. The main steps of cyclic18 LSB approach are depicted by the flowchart in Fig. 3.

The embedding cyclic18 LSB method is further clarified using the following example. Consider a 24-bit image with pixels $\{p_1 - p_{18}\}$ where each pixel is represented by 24 bits i.e. eight bits for the red channel, eight bits for the green channel, and eight bits for the blue channel. (Syntax: [pixel number: red, green, blue]). For the sake of ease of understanding, we present only the LSB part of the cyclic18 LSB substitution method with an example.

[p_1: 11010110, 10000110, 11010110], [p_2: 11000110, 10110110, 11010100],
[p_3: 11000111, 11100110, 11110110], [p_4: 10010110, 10101110, 11010111],
[p_5: 11011110, 00000111, 01010110], [p_6: 11011110, 10110110, 11010111],
[p_7: 11010101, 10000101, 00010110], [p_8: 11011111, 11010110, 11000110]
[p_9: 11010110, 10000110, 11010111], [p_{10}: 11000110, 10110110, 11010100],
[p_{11}: 11000111, 11100110, 11110111], [p_{12}: 10010110, 10101110, 11010111],
[p_{13}: 11011110, 00000111, 01010110], [p_{14}: 11011110, 10110110, 11010111],
[p_{15}: 11010101, 10000101, 00010110], [p_{16}: 11011111, 11010110, 11000110].
[p_{17}: 11011101, 10000101, 01010110], [p_{18}: 11011011, 10010110, 11010110]

Consider a secret message M= "*ABC*" whose binary equivalent is B= (01000001 01000010 010000011)$_2$ and stego key bits K= (01011011)$_2$. After applying TLEA using stego key K, the bits obtained are given as finalBits= (00100101 00100110 00100100)$_2$. Now follow the pattern RGB, RBG, GRB, GBR, BRG, and BGR cyclically and embed data in different channels of the host image using the LSB method. The pattern shows that the secret bits are embedded in the host image's pixels as follows: Embed the 1st secret bit of block$_1$ in pixel$_1$'s red channel, 2nd bit of block$_1$ in pixel$_2$'s green channel, 3rd bit of block$_1$ in pixel$_3$'s blue channel, 4th bit of block$_1$ in pixel$_4$'s red channel, 5th bit of block$_1$ in pixel$_5$'s blue channel, 6th bit of block$_1$ in pixel$_6$'s green channel, 7th bit of block$_1$ in pixel$_7$'s green channel, 8th bit of block$_1$ in pixel$_8$'s red channel, 9th bit of block$_1$ in pixel$_9$'s blue channel, 10th bit of block$_1$ in pixel$_{10}$'s green channel, and so on. The embedding sequence is shown in Table 1.

Using Table 1 and the LSB substitution scheme, we embed the encrypted message bits finalBits= (00100101 00100110 00100100)$_2$ in the pixels (p_1-p_{18}) and get the pixels (p_1'-p_{18}') as follows:

[p$_1$': 1101011**0**, 10000110, 11010110], [p$_2$': 11000110, 1011011**0**, 11010100],
[p$_3$': 11000111, 11100110, 1111011**1**], [p$_4$': 1001011**0**, 10101110, 11010111],
[p$_5$': 11011110, 00000110, 0101011**0**], [p$_6$': 11011110, 1011011**1**, 11010110],
[p$_7$': 11010101, 1000010**0**, 00010110], [p$_8$': 1101111**1**, 11010110, 11000110],
[p$_9$': 11010110, 10000110, 1101011**0**], [p$_{10}$': 11000110, 1011011**0**, 11010100],
[p$_{11}$': 11000111, 11100110, 1111011**1**], [p$_{12}$': 1001011**0**, 10101110, 11010111],
[p$_{13}$': 11011110, 00000110, 0101011**0**], [p$_{14}$': 1101111**1**, 10110111, 11010110],
[p$_{15}$': 11010101, 1000010**1**, 00010110], [p$_{16}$': 11011110, 11010110, 1100011**0**],
[p$_{17}$': 11011101, 1000010**0**, 01010110], [p$_{18}$': 1101101**0**, 10010110, 11010110]

Herein, the bold face black color LSBs represent the locations where secret bits are embedded, and the bold face underlined black color indicates the altered LSBs as a result of message embedding.

Data recovery algorithm

The data recovery algorithm extracts the hidden secret data from the stego image by applying the reverse operation of the embedding algorithm. The same pattern of the embedding algorithm is also used in the extraction process i.e. RGB, RBG, GRB, GBR, BRG, BGR, and so on. The extracted bits are then decrypted using the reverse operations of the three-level encryption algorithm to get the original secret message. The main steps of the extraction algorithm are depicted in the flowchart in Fig. 4.

Experimental results and discussion

In this section, we present the complete experimental setup for evaluating the performance of the proposed method in terms of payload, security, and perceptual transparency of the resultant stego images. The proposed method is compared with ten state-of-the-art techniques, belonging to three different categories including LSB and cyclic LSB based techniques [6, 7, 21, 37], pixel indicator based techniques [11, 38, 39], and color model exchange based techniques [40, 41]. MATLAB R2014a is used for simulation and conducting a variety of experiments based on various image quality assessment metrics (IQAMs) [42–44]. In the next sub-sections, the detail of experiments and comparison is presented along with a security analysis, illustrating the strength of the proposed scheme.

Dataset

In this section, we briefly describe the images dataset and their sources. We have used a dataset of 50 standard images, selected from various standard databases including USC-SIPI-ID [45], LIVE [46], and COREL [47]. The dataset contains images of different nature such as smooth and edgy images which is the criteria for selecting images for the performance evaluation of steganographic schemes. Some of the famous standard images used for evaluation of steganographic algorithms are Lena, baboon, trees, house, peppers, f16jet, and building, which are included in the dataset. To fully evaluate the performance of all

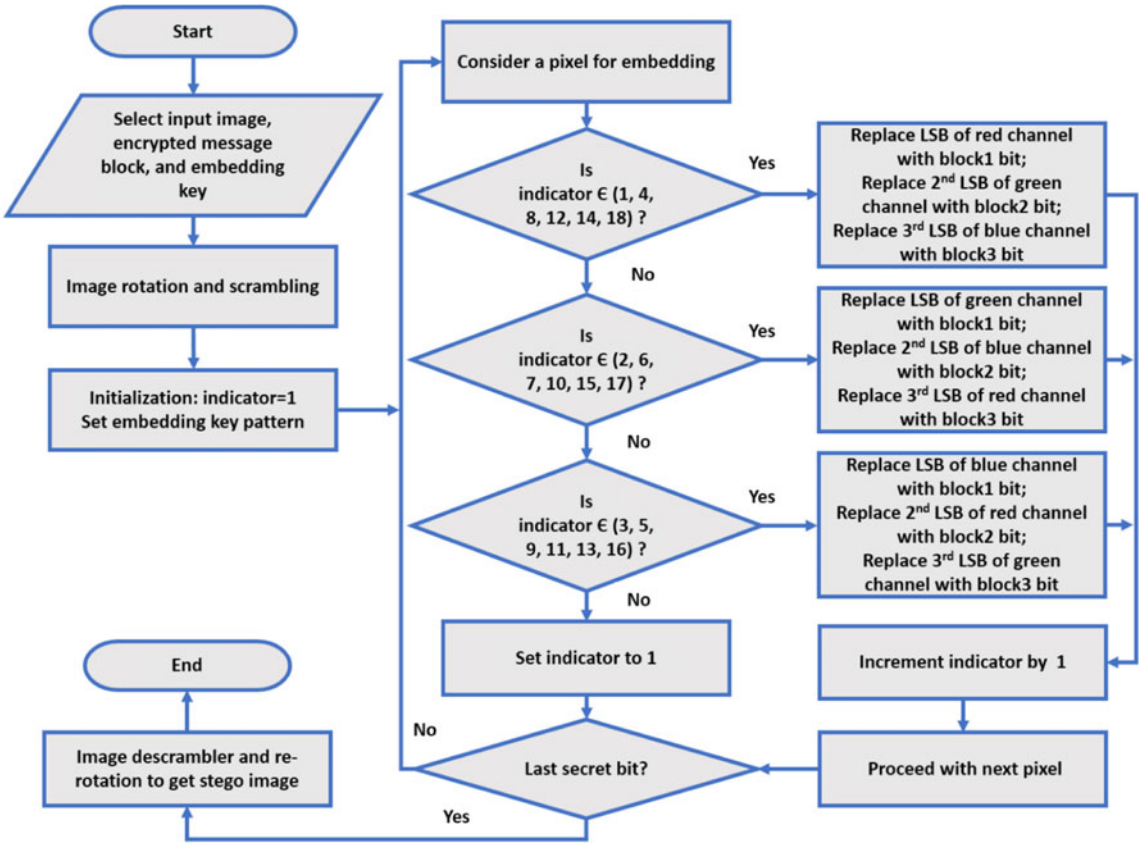

Fig. 3 Flowchart for the embedding algorithm

methods and make the comparison unbiased, the images are adjusted to different resolutions depending on the requirements.

Quantitative evaluation

This sub-section explains the quantitative evaluation of the proposed scheme and other competing techniques. All the techniques are tested using three different experiments. Experiment 1 hides a message file of 8KB in different images with equal dimensions (256×256 pixels). Experiment 2 embeds message files of different sizes (2KB, 4KB, 6KB, and 8KB) in same images of same resolution. Experiment 3 makes use of same images with the same size cipher but different dimensions. The performance evaluation is based on various IQAMs such as peak signal-to-noise ratio (PSNR) [48], normalized cross correlation (NCC), and structural similarity index metric (SSIM) [49]. These metrics can be calculated using equations 2–5 as follows:

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

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy}-C_{xy}\right)^2 \tag{3}$$

$$NCC = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy}\times C_{xy}\right)}{\sum_{x=1}^{M}\sum_{y=1}^{N}S_{xy}^2} \tag{4}$$

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

Table 1 Sequence for embedding process

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
R	G	B	R	B	G	G	R	B	G	B	R	B	R	G	B	G	R

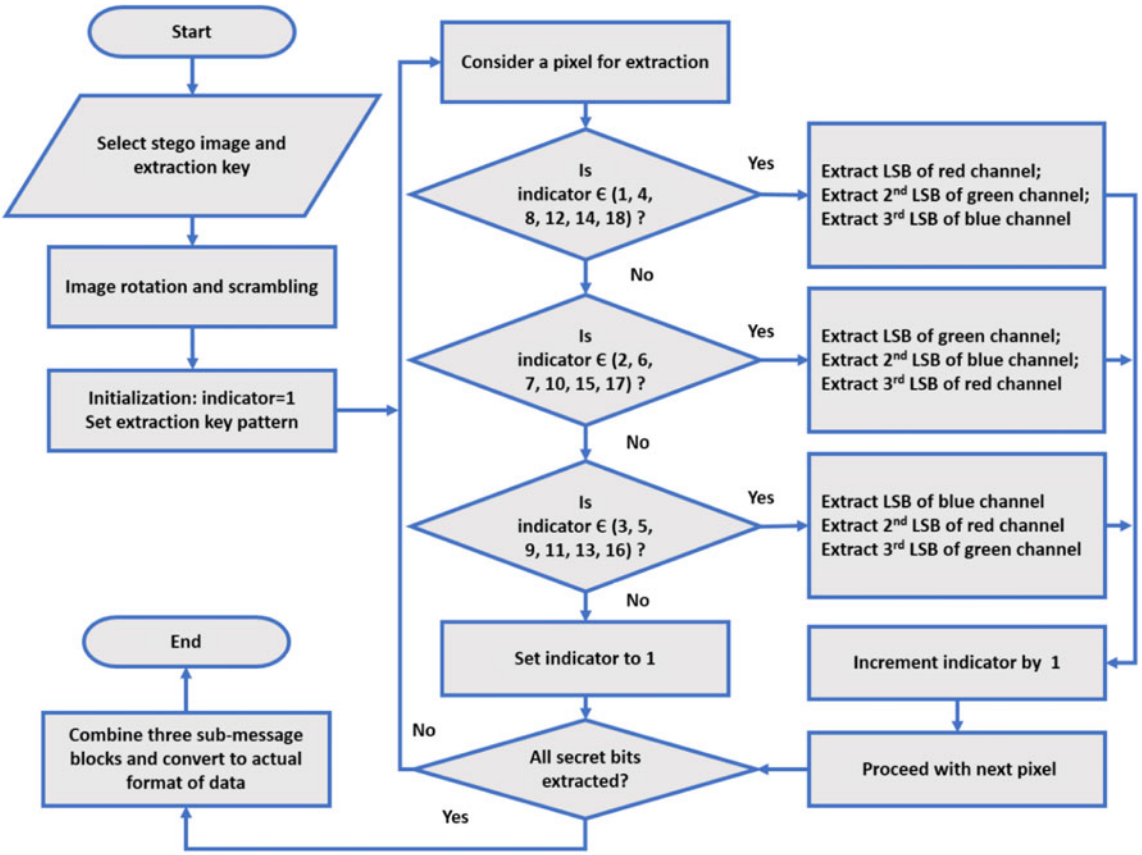

Fig. 4 Flowchart for the data recovery algorithm

Here, C and S show the cover image and output stego image, respectively, M and N represent image dimensions, x and y are counter variables, and μ_x, σ_x, μ_y, σ_y, σ_{xy} show statistical terms [50, 51].

Quantitative results and discussion

The quantitative results and comparison of all implemented methods including the proposed method are detailed in this section. Figure 5 shows a set of cover and stego images from the dataset. Figures 6, 7 and 8 show the quantitative experimental results of the existing methods and the proposed method using various IQAMs.

Table 2 shows the results of experiment 1 using an average score of PSNR over fifty images for the proposed method and the other five methods. These five methods belong to the category of LSB and cyclic LSB based methods. Table 3 presents the results of experiment 1 using NCC for the proposed method and other five methods. The methods included for comparison in Table 3 belong to the category of pixel indicator and color model exchange based methods. Figure 6 demonstrates the performance of the proposed scheme in comparison with all ten mentioned methods using SSIM. The graph is constructed using the average score of SSIM, calculated over fifty images. Table 2, Table 3, and Fig. 6 show that the FFM technique gives worse results in terms of NCC and SSIM; the performance of LSB-M, LSB-MR, CST, and SHSI is almost same, and MLSB-HIS method is approaching the proposed method. It is clear from Table 2, Table 3, and Fig. 6 that the proposed method achieves the highest average score of PSNR, NCC, and SSIM over fifty images, hence validating its better performance in contrast to the other ten methods.

Figure 7 shows experiment 2 results of the proposed framework and other competing methods by hiding secret data of various sizes (2KB, 4KB, 6KB, and 8KB) in different standard images, keeping the image dimensions the same. Each sub-graph represents the comparison of the proposed method with three competing methods, each of which is selected from the given three categories of techniques based on varying size of secret information, i.e. 2KB, 4KB, 6KB, and 8KB, respectively. By analyzing the results of Fig. 7, we can see that the proposed method dominates all the mentioned schemes by achieving the highest score of PSNR in all cases, hence validating its better performance.

Figure 8a and b show the performance evaluation of the proposed method with the other ten techniques using PSNR for experiment 3. In this experiment, the message size and tested image is kept the same, while the image dimension varies, i.e. 128×128, 256×256, 512×512, and 1024×1024

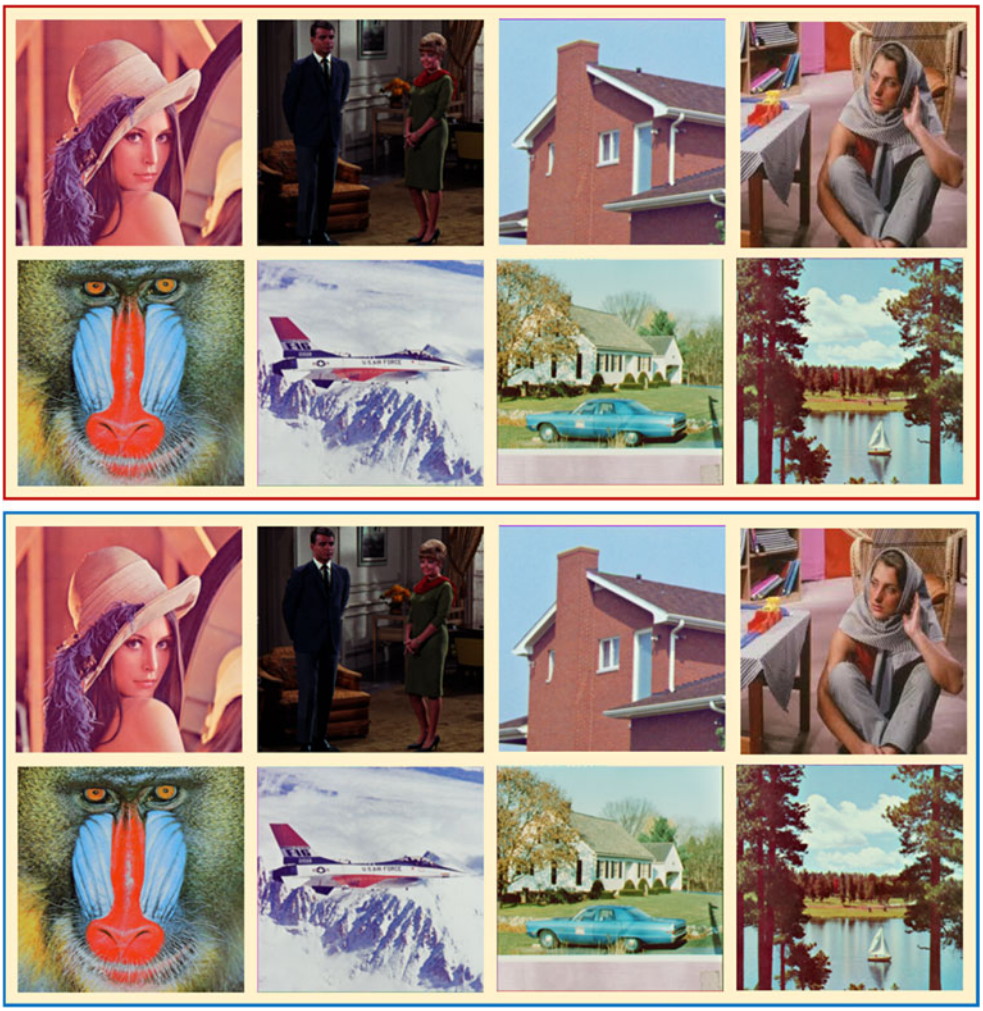

Fig. 5 A set of input cover and output stego images of the proposed method. The first two rows show cover images from left to right including Lena, couple, Barbara, scene, baboon, airplane, home, and trees. The 3rd and 4th rows show the resultant stego images of the proposed method with their corresponding PSNR scores including Lena=55.8865dB, couple=53.9442dB, Barbara=45.3401dB, scene=43.8451dB, baboon=49.9442dB, airplane=54.1581dB, home=52.9981dB, and trees=41.9458dB

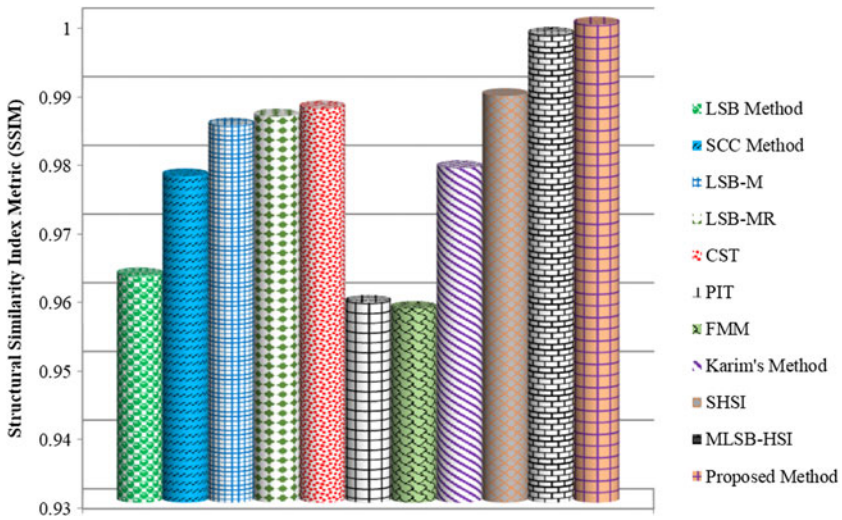

Fig. 6 Experiment 1 results: comparison of the proposed method with other ten competing methods using average score of SSIM computed over fifty images

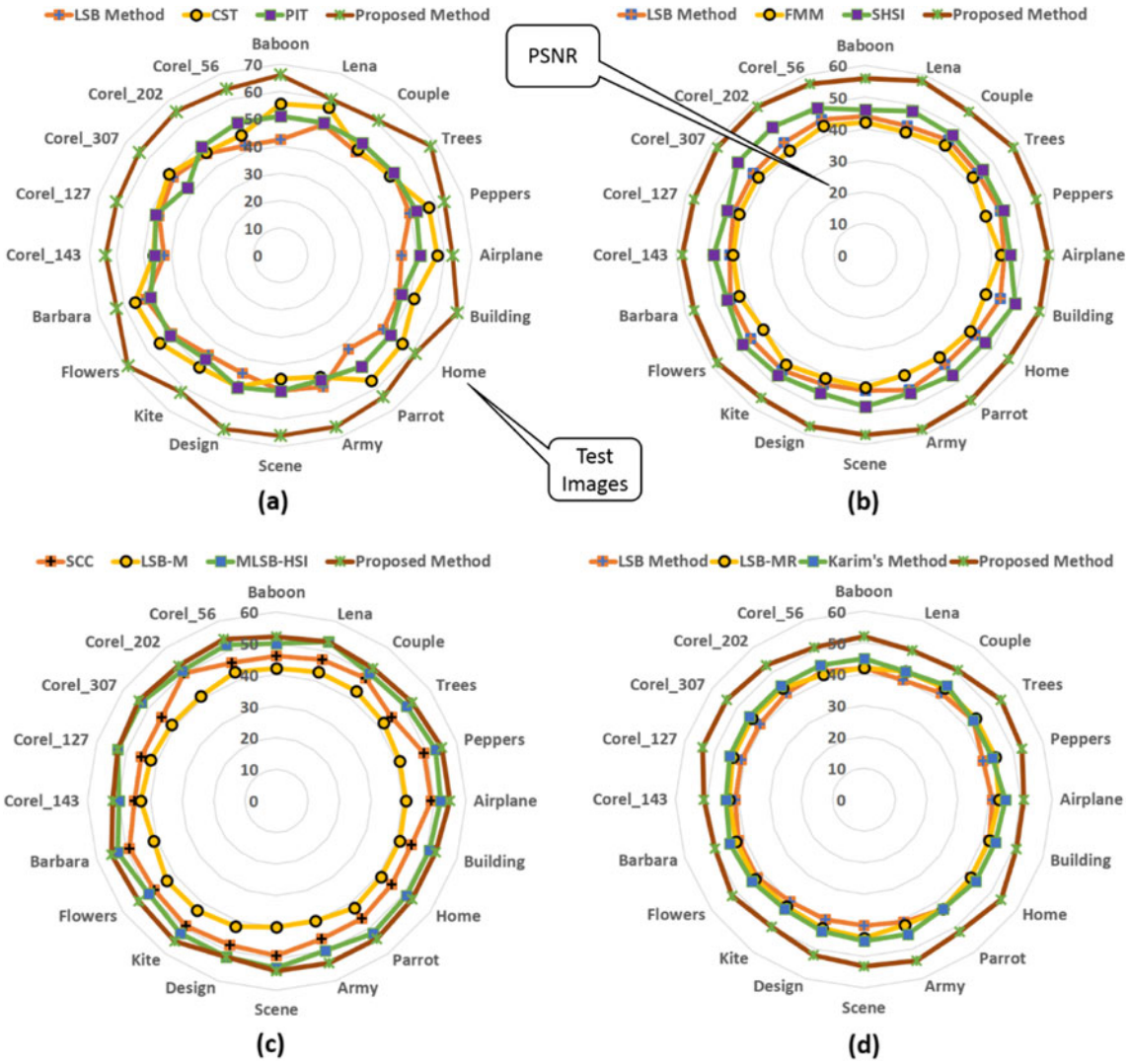

Fig. 7 Experiment 2 results: comparison of the proposed scheme with other methods of three categories using PSNR over 20 standard test images by varying amount of embedded data (2KB, 4KB, 6KB, and 8KB). (**a**) PSNR based performance evaluation of proposed method with LSB, CST, and PIT by hiding 2KB data in all the given images as shown in the shape of circle. (**b**) Evaluation based on 4KB data. (**c**) Evaluation based on data of size 6KB and (d), PSNR based comparison when the data size is 8KB

pixels. This experiment analyzes the effect of image size on the performance of each mentioned method. By analyzing Fig. 8a and b, we can see that the performance of certain methods gradually increases with increases in image dimension such as CST, SCC, PIT, and MLSB-HSI. On the other hand, there is variation in the PSNR score of other competing methods with an increase in image dimension. The proposed method achieves the highest PSNR score in all cases, keeping its performance consistent, hence validating its better performance in contrast to the ten given methods.

Qualitative evaluation

In this section, we evaluate the performance of the proposed framework and other competing methods using qualitative evaluation, which is one of the performance evaluation methods for steganographic techniques. In this evaluation strategy, we have used mean opinion score (MOS) [52] and visual histogram changeability [41] as metrics for evaluation. In the case of MOS, we requested five professors and five PhD students to rate the visual quality of stego images generated by the proposed scheme and other mentioned approaches using a scale of 0 (unsatisfactory quality) to 5 (highest quality). The quality evaluators include five male and five female researchers within the age range of 25–50 years, working in image and video processing. They were trained for 1 hour about the evaluation process and importance of this security application. A total of ten standard test images were rated during this assessment method, and the MOS scores were averaged as shown in Table 4.

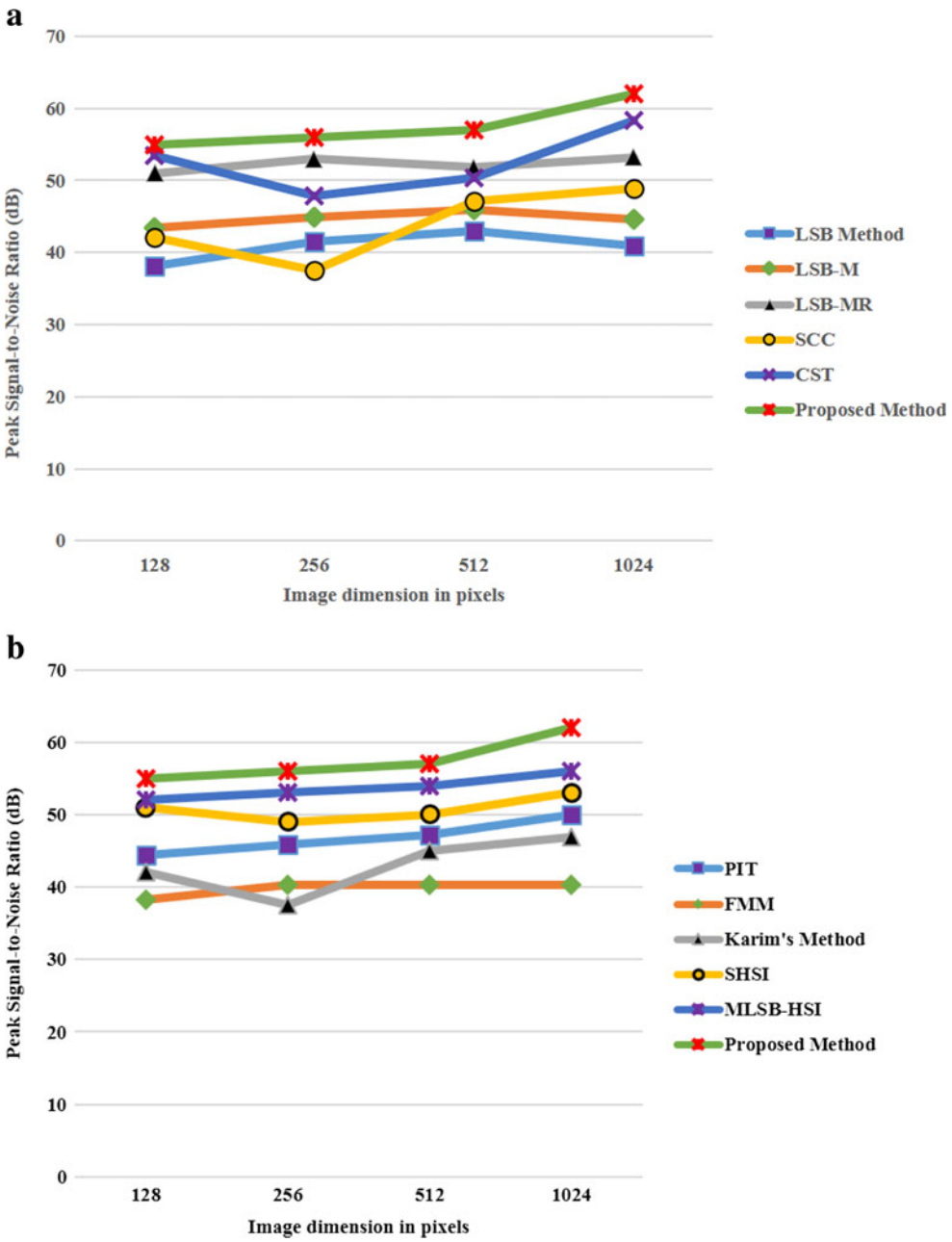

Fig. 8 (**a**) Experiment 3 results: comparison of the proposed method with five competing methods, belonging to the category of LSB and cyclic LSB based approaches using PSNR. (**b**) Experiment 3 results: comparison of the proposed scheme with the other five competing methods, belonging to the category of pixel indicator and color model exchange based methods using PSNR

By interpreting the MOS based results in Table 4, we observed that the proposed framework generates visually high quality stego images in contrast to all other techniques under consideration. Thus, it reduces the chances of detection by HVS, preserving the security of the embedded information. To further evaluate the visual quality, we have considered histogram changeability of the resultant stego images. The sample test image "Lena" and its corresponding histograms of three channels for cover and stego image are shown in Fig. 9.

From Fig. 9, we can confirm that there are no obvious changes in the histograms of cover and stego image, resulting in less histogram changeability, hence validating the better performance of the proposed method.

Secret key sensitivity analysis

In this section, we describe the sensitivity of the secret key in context of security for the proposed framework. The secret key is generally expected to be of maximum

Table 2 Results of experiment 1: PSNR (dB) based comparison of the proposed technique with other five state-of-the-art methods, belonging to LSB substitution and cyclic LSB substitution based methods, including the simple LSB method, the cyclic LSB method, the LSB matching technique, the LSB matching revisited technique, and the cyclic steganographic technique with an embedding capacity=1 bits per pixel

Serial number	Image name	LSB method	CLSB [37] method	LSB-M [7]	LSB-MR [6]	CST [21]	Proposed method
1	Peppers	55.9251	53.0445	49.3252	40.3691	52.9717	56.0235
2	Airplane	53.4882	47.4852	45.6879	49.2347	47.4902	54.1581
3	Couple	52.8935	48.9459	46.5598	47.9971	48.9446	53.9442
4	Corel_205	50.9353	48.9508	46.5779	48.8077	48.9559	50.9525
5	Trees	39.0436	38.5418	38.2702	39.5397	38.5421	41.9458
6	Corel_300	47.1757	47.4921	45.6642	39.7967	47.4941	48.4874
7	Corel_118	38.8939	36.0779	35.9214	34.7013	36.0779	40.0780
8	Home	50.1659	51.1776	47.6956	40.2518	51.1564	52.9981
9	Baboon	48.1648	48.9531	46.5568	39.9997	48.9536	49.9442
10	Lena	54.8865	54.9211	49.2562	40.2340	54.8384	55.8865
Avg. of 50 images		**51.9589**	**47.9390**	**45.1515**	**43.4931**	**47.9474**	**53.9516**

length so that it can survive against brute force attack where the attacker applies all possible combinations of characters to crack it, which leads to breakage of the security algorithm [41, 53].

Keeping this concern in view, we have used three different keys: scrambling key, encryption key, and embedding key. These keys are combined to make a single master key which has been utilized in the proposed framework. For simplicity and ease of calculation, we have kept the size of these keys small i.e. 27 digits for the scrambling key and 64 bits for the embedding key as well as the encryption key. One can increase the length of these keys to further increase the security, depending on the requirement and type of application. A small change in any of the used keys results in a significant change in the decryption process, leading to an invalid hidden message.

Security strength of the proposed framework

The security strength of the proposed framework is analyzed using Kirchhoff's principle [54], assuming that the procedure of data hiding is known to attackers. In this case, the security of the whole system depends on secret key selection, i.e. the system is considered enough secure if the adversaries cannot detect/extract

Table 3 Results of experiment 1: NCC based comparison of the proposed technique with other five state-of-the-art methods, belonging to pixel indicator based techniques and color model exchange based approaches, including the PIT method, Karim's method, the simple HSI method, and the magic LSB based HSI method with an embedding capacity=1 bits per pixel

Serial number	Image name	SHSI method [40]	MLSB-HSI method [41]	PIT [11]	FMM method [38]	Karim's method [39]	Proposed method
1	Scene	0.9897	0.9997	0.9896	0.9796	0.9887	0.9998
2	Couple	0.9775	0.9795	0.9785	0.9695	0.9796	0.9882
3	Baboon3	0.9898	0.9898	0.9794	0.9597	0.9889	0.9998
4	Design	0.9987	0.9988	0.9990	0.9798	0.9909	0.9995
5	Competition	0.9919	0.9980	0.9981	0.9889	0.9989	0.9997
6	Corel_338	0.9845	0.9934	0.9960	0.9797	0.9888	0.9983
7	Corel_141	0.9551	0.9519	0.9021	0.9202	0.9719	0.9821
8	Corel_301	0.9876	0.9878	0.9798	0.9598	0.9799	0.9998
9	Corel_205	0.9972	0.9975	0.9891	0.9791	0.9959	0.9991
10	Corel_134	0.9935	0.9940	0.9894	0.9799	0.9993	0.9996
Avg. of 50 images		**0.9768**	**0.9829**	**0.9669**	**0.9652**	**0.9729**	**0.9932**

Table 4 MOS score based evaluation of the proposed method with other schemes

Image Name	LSB	SCC	CST	LSB-M	LSB-MR	PIT	FMM	KM	MLSB-HSI	Proposed Method
Lena	3.5	3.4	3.3	3.2	3.8	3.1	3	3.9	4.4	4.5
Baboon	3.8	3.6	3.5	3.3	3.6	3.2	3.2	3.7	4.1	4.2
Airplane	4.1	3.8	3.9	3.7	3.8	3.5	3.4	4.1	4.3	4.4
Home	3.9	3.4	3.2	3.2	3.5	3.3	3.1	3.8	4.0	4.2
Couple	4.2	3.7	3.5	3.4	3.6	3.2	3	4.1	4.3	4.3
Barbara	3.4	3.1	3.2	3.1	3.3	3	3.2	3.7	3.7	3.9
Peppers	3.2	3	3.2	3	3.4	3.1	3.3	3.6	3.8	4.1
Trees	3.3	3.1	3	3.1	3	3.2	3	3.5	3.7	4
Army	3.7	3.4	3.2	3.4	3.5	3	3.1	3.7	3.8	4.2
Scene	3.6	3.2	3.3	3.5	3.4	3.3	3.4	4	4.2	4.3
Average of 10 images	**3.67**	**3.37**	**3.33**	**3.29**	**3.49**	**3.19**	**3.17**	**3.81**	**4.03**	**4.21**

the embedded information despite knowing the data embedding procedure. This makes the secret key selection very crucial for securing the system. Based on this, we have used three different keys including a scrambling key (216 bits), an encryption key (64 bits), and an embedding key (64 bits), producing a master key of 344 bits, and thus providing enough key space to resist the brute-force attack. A brief analysis for the security strength of the proposed scheme is illustrated as follows:

$$\textit{Master key length} = 344\ \textit{bits}$$
$$\textit{Possible number of keys} = 2^{344}$$

If the attacker is generating 1 million keys per second, then the total time required for finding the actual key can be calculated as follows:

$$\textit{Key generating speed} = 10^6$$
$$\textit{Number of years required} = \frac{2^{344}}{10^6 \times 365 \times 86400} = 1.1363 \times 10^{90}$$
$$\textit{Average number of years required} = 5.68 \times 10^{89}$$

According to this analysis, we can conclude that the proposed framework provides enough security to remain resilient against a brute-force attack, hence validating its effectiveness.

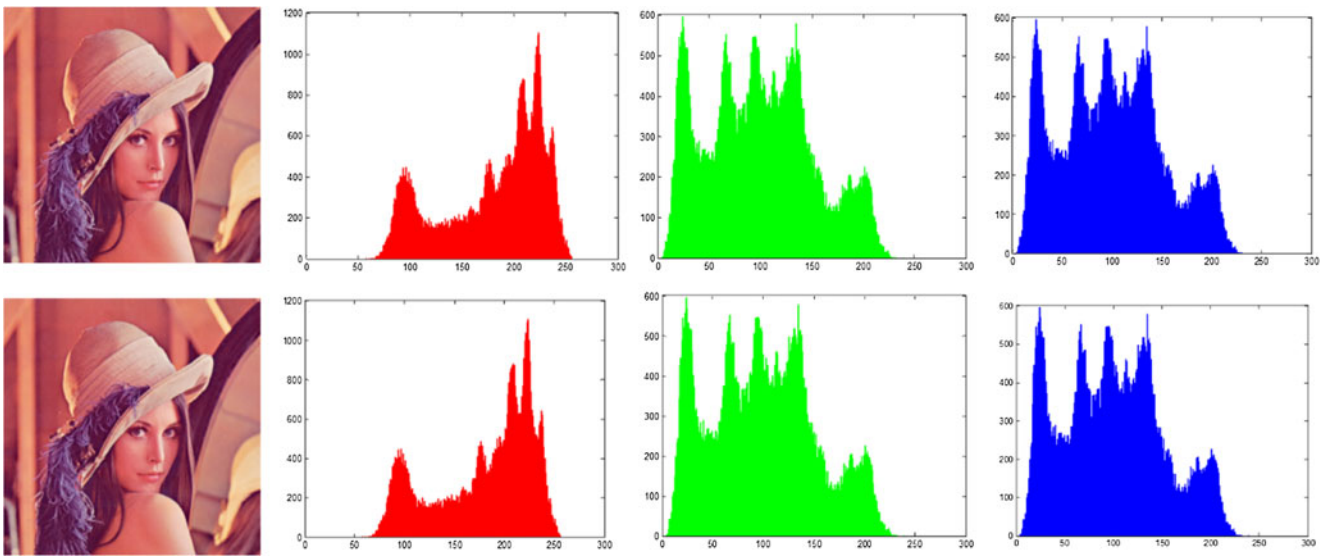

Fig. 9 Visual quality assessment: The first line shows the standard Lena test image along with histograms of its three channels i.e. *red*, *green*, and *blue* (left to right). The second line illustrates the stego Lena image and histograms of three channels after embedding 8KB text using the proposed method

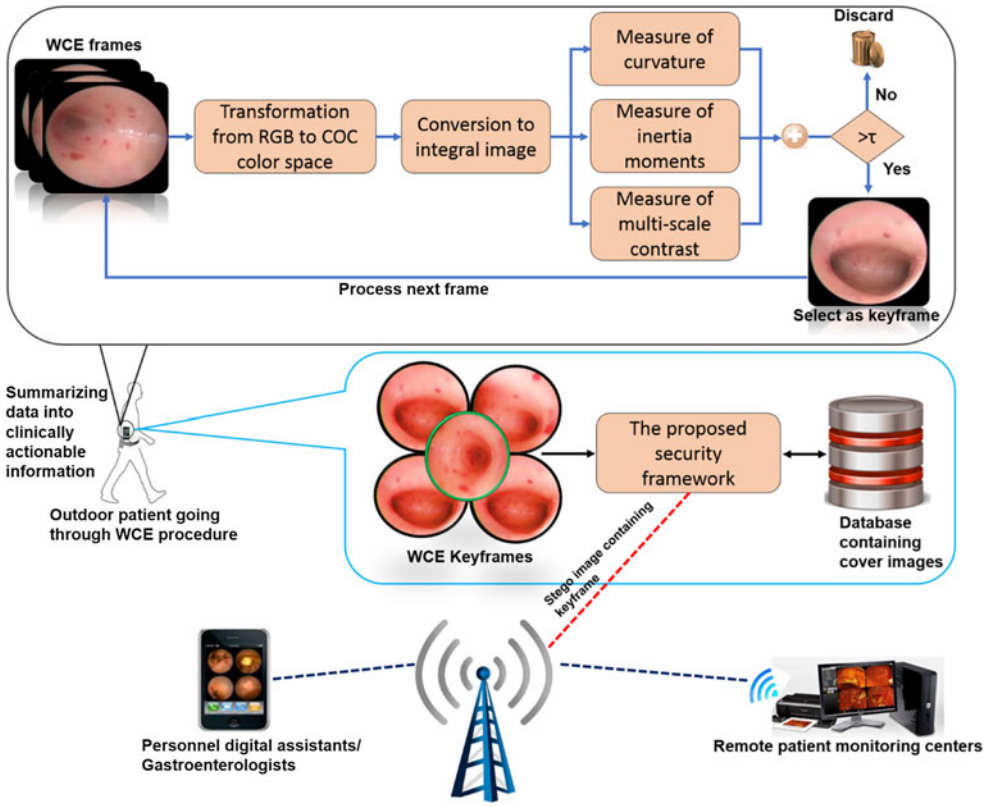

Fig. 10 Secure transmission of diagnostically important keyframes extracted using video summarization during wireless capsule endoscopy to gastroenterologists and healthcare centers

Applications of the proposed framework

In this section, we describe several general and one specific application of the proposed framework regarding security and privacy. The general applications of the proposed framework include copyright protection, TV broadcasting, top-secret communication, feature tagging, and improving the performance of search engines. The special application of the proposed method is briefly explained in the coming sub-section.

Secure and efficient wireless capsule endoscopy using the proposed method

Wireless capsule endoscopy (WCE) is the process of identifying the causes of diseases by visualizing the inaccessible portions of the human body by gastroenterologists. The system consists of three major components including a one-time usable wireless capsule, a battery along with an image recording unit (IRU), and a sensing system [55]. During the WCE process, the patient wears the IRU and swallows the disposable capsule, which transmits the video frames to IRU wirelessly when passing through the patient's gastrointestinal tract. The detailed explanation of the entire process can be found in Ref [56]. A huge amount of video frames are generated during WCE, but only a limited set of keyframes are used for actual diagnostic process. Therefore, sending all the video data to gastroenterologists for analysis is the wastage of several resources such as battery, energy, and bandwidth [55]. In addition, analyzing this enormous amount of gastrointestinal video data wastes the valuable time of gastroenterologists. Furthermore, sending such large amount of video data to remote patient monitoring centers and gastroenterologists securely is also a challenging task. To address these problems, video prioritization combined with the proposed security framework can be used as shown in Fig. 10.

In this scenario, keyframes can be extracted from the huge WCE video using the video summarization technology by taking decisions based on the saliency map, computed by fusing the various features of video frames such as multi-scale contrast, curvature, and image moments as done in our recent work [55]. A detailed overview of the proposed system is illustrated in Fig. 10. For further detailed study, the reader is referred to [57–62], and [63–65] for video summarization, WCE, and image steganography, respectively. The summarized sequence of keyframes can be then sent securely using the proposed steganographic method to gastroenterologists and remote patient monitoring centers, ensuring the patient's privacy and maintaining the accuracy and security of summarized WCE information. Unlike traditional endoscopy methods, which require special medical staff and proper hospitalization, this application will result in five main advantages including patient's privacy, minimizing transmission

cost, bandwidth, and storage costs, saving the precious time of gastroenterologists, and secure transmission of summarized WCE keyframes.

Conclusion and future work

In this paper, an imperceptible image steganographic scheme with dual-level security is proposed. The secret information encrypted by TLEA is embedded into the cover image, scrambled by the proposed image scrambler using cyclic18 LSB substitution method. The utilization of LSB and intermediate LSBs for data hiding using the proposed method preserves the visual transparency of stego images, hence minimizes the chances of detection by HVS. The proposed system introduces multiple security barriers for attackers by incorporating message blocks division, TLEA, image scrambling, and rotating the sub-images at various angles, hence making data extraction very challenging for adversaries. Furthermore, the system provides enough security to resist the brute-force attack. The qualitative and quantitative experimental results conclude that the proposed scheme provides better imperceptibility and security along with an improved visual quality of the stego images, making it one of the best candidates for secure communication in general and secure transmission of EPR and keyframes to healthcare centers in specific.

In the future, we will tend to use sparse representation combining with visual attention models to effectively represent the cover image and hide data based on the saliency information. This will result in larger payload as well as better visual quality. We also plan to further increase the security of the proposed system and extend its applications to wireless multimedia surveillance networks and medical imaging based areas.

Acknowledgments This research is supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A2012904).

References

1. Cheddad, J., Condell, K., Curran, and Mc Kevitt, P., "Digital image steganography: Survey and analysis of current methods,". *Signal Process.* 90:727–752, 2010.
2. Liu, J., Tang, G., and Sun, Y., A secure steganography for privacy protection in healthcare system. *J. Med. Syst.* 37:1–10, 2013.
3. Yang, C.-Y., and Wang, W.-F., Effective electrocardiogram steganography based on coefficient alignment. *J. Med. Syst.* 40:1–15, 2016.
4. Khan, F. and Gutub, A. A.-A., "*Message Concealment Techniques using Image based Steganography,*" *in The 4th IEEE GCC Conference and Exhibition*, 2007.
5. Al-Otaibi, N. A. and Gutub, A. A., "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)*, 2014, pp. 243–250.
6. Mielikainen, J., "LSB matching revisited,". *SigN. ProcesS. Lett., IEEE* 13:285–287, 2006.
7. Luo, W., Huang, F., and Huang, J., "Edge adaptive image steganography based on LSB matching revisited,". *Inform. Forensics Secur., IEEE Trans.* 5:201–214, 2010.
8. Ioannidou, Halkidis, S. T., and Stephanides, G., A novel technique for image steganography based on a high payload method and edge detection. *Expert Syst. Applic.* 39:11517–11524, 2012.
9. Kanan, H. R., and Nazeri, B., A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. *Expert Syst. Applic.* 41:6123–6130, 2014.
10. Gutub, M., Ankeer, M., Abu-Ghalioun, A., Shaheen, and Alvi A., "Pixel indicator high capacity technique for RGB image based Steganography," in *WoSPA 2008–5th IEEE International Workshop on Signal Processing and its Applications*, 2008, pp. 1-3.
11. Gutub, A.-A., Pixel indicator technique for RGB image steganography. *J. Emerg. Technol. Web Intell.* 2:56–64, 2010.
12. Abu-Marie, W., Gutub, A., and Abu-Mansour, H., Image based steganography using truth table based and determinate array on RGB indicator. *Int. J. Sign. Imag. Process.* 1:196–204, 2010.
13. Fakhredanesh, M., Rahmati, M., and Safabakhsh, R., Adaptive image steganography using contourlet transform. *J. Electron. Imag.* 22:043007–043007, 2013.
14. Chen, W.-Y., Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. *Appl. Math. Comput.* 196:40–54, 2008.
15. Noda, H., Niimi, M., and Kawaguchi, E., High-performance JPEG steganography using quantization index modulation in DCT domain. *Pattern Recogn. Lett.* 27:455–461, 2006.
16. Jafari, R., Ziou, D., and Rashidi, M. M., Increasing image compression rate using steganography. *Expert Syst. Applic.* 40:6918–6927, 2013.
17. Raeiatibanadkooki, M., Quchani, S. R., KhalilZade, M., and Bahaadinbeigy, K., Compression and encryption of ECG signal using wavelet and chaotically Huffman code in telemedicine application. *J. Med. Syst.* 40:1–8, 2016.
18. Chen, S.-T., Guo, Y.-J., Huang, H.-N., Kung, W.-M., Tseng, K.-K., and Tu, S.-Y., Hiding patients confidential Datainthe ECG signal via transform-domain quantization scheme. *J. Med. Syst.* 38:1–8, 2014.
19. Martínez-Pérez, I., De La Torre-Díez, and López-Coronado, M., "Privacy and security in mobile health apps: a review and recommendations,". *J. Med. Syst.* 39:1–8, 2015.
20. Muhammad, K., Ahmad, J., Farman, H., and Jan, Z., A new image steganographic technique using pattern based bits shuffling and magic LSB for grayscale images. *Sindh Univ. Res. J.-SURJ (Sci. Ser.)* 47:723–728, 2016.
21. Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., and Qureshi, R. J., "A secure cyclic steganographic technique for color images using randomization,". *Tech. J., Univ. Eng. Technol. Taxila* 19:57–64, 2015.
22. Al-Otaibi, N. A., and Gutub, A. A., "2-Leyer security system for hiding sensitive text data on personal computers,". *Lect. NoteS Inform. Theory.* 2, 2014.
23. Wang, R.-Z., Lin, C.-F., and Lin, J.-C., Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recogn.* 34:671–683, 2001.
24. Chang, C.-C., Hsiao, J.-Y., and Chan, C.-S., Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recogn.* 36:1583–1595, 2003.

25. Chan, C.-K., and Cheng, L.-M., Hiding data in images by simple LSB substitution. *Pattern Recogn.* 37:469–474, 2004.
26. Thien, C.-C., and Lin, J.-C., A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. *Pattern Recogn.* 36:2875–2881, 2003.
27. Wu, H.-C., Wu, N.-I., Tsai, C.-S., and Hwang, M.-S., "Image steganographic scheme based on pixel-value differencing and LSB replacement methods,". *IEE Proc.-Vision, Imag. Sign. Process.* 152: 611–615, 2005.
28. Dumitrescu, S., Wu, X., and Wang, Z., "Detection of LSB steganography via sample pair analysis,". *Sign. Process., IEEE Trans.* 51:1995–2007, 2003.
29. Parvez, M. T. and Gutub, A.-A., "RGB intensity based variable-bits image steganography," in *Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE*. 1322-1327, 2008.
30. Parvez, M. T., and Gutub, A. A.-A., Vibrant color image steganography using channel differences and secret data distribution. *Kuwait J. Sci. Eng.* 38:127–142, 2011.
31. Amirtharajan, R., Behera, S. K., Swarup, M. A., and Rayappan, J. B. B., "Colour guided colour image steganography," *arXiv preprint arXiv:1010.4007,* 2010.
32. Swain, G., and Lenka, S. K., A novel approach to RGB channel based image steganography technique. *Int. Arab J. e-Technol.* 2: 181–186, 2012.
33. Amirtharajan, R., Archana, P., Rajesh, V., Devipriya, G., and Rayappan, J., "Standard deviation converges for random image steganography," in *Information & Communication Technologies (ICT), 2013 I.E. Conference on*. 1064-1069, 2013.
34. Amirtharajan, R., Mahalakshmi, V., Nandhini, J., Kavitha, R., and Rayappan, J., Key decided cover for random image steganography. *Res. J. Inf. Technol.* 5:171–180, 2013.
35. Chen, W.-J., Chang, C.-C., and Le, T. H. N., High payload steganography mechanism using hybrid edge detector. *Expert Syst. Applic.* 37:3292–3301, 2010.
36. Grover, N., and Mohapatra, A., "Digital image authentication model based on edge adaptive steganography," in *Advanced Computing, Networking and Security (ADCONS), 2013 2nd International Conference on*. 238-242, 2013.
37. Bailey, K., and Curran, K., An evaluation of image based steganography methods. *Multimed Tools Applic.* 30:55–88, 2006.
38. Jassim, F. A., "A novel steganography algorithm for hiding text in image using five modulus method," *Int. J. Comput. Applic*. 72, 2013.
39. Karim, M., "A new approach for LSB based image steganography using secret key," *14th Int. Conf. Comput. Inform. Technol. (ICCIT 2011)*. 286–291, 2011.
40. Muhammad, K., Ahmad, J., Farman, H., and Zubair, M., A novel image steganographic approach for hiding text in color images using HSI color model. *Middle-East J. Sci. Res.* 22:647–654, 2014.
41. Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., and Baik, S., "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimed. Tools Applic*. 1–27, 2015/05/24 2015.
42. Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M., and Baik, S. W., A secure method for color image steganography using gray-level modification and multi-level encryption. *KSII Trans. Internet Inform. Syst. (TIIS)* 9:1938–1962, 2015.
43. Sajjad, M., Mehmood, I., and Baik, S. W., Image super-resolution using sparse coding over redundant dictionary based on effective image representations. *J. Vis. Commun. Image Represent.* 26:50–65, 2015.
44. Muhammad, K., Mehmood, I., Lee, M. Y., Ji, S. M., and Baik, S. W., Ontology-based secure retrieval of semantically significant visual contents. *J. Korean Instit. Next Gen. Comput.* 11:87–96, 2015.
45. The USC-SIPI Image Database. http://sipi.usc.edu/services/database/Database.html. 2003.
46. Sheikh, H. R., Sabir, M. F., and Bovik, A. C., "A statistical evaluation of recent full reference image quality assessment algorithms,". *Imag. Process., IEEE Trans.* 15:3440–3451, 2006.
47. Wang, J. Z., Li, J., and Wiederhold, G., "SIMPLIcity: Semantics-sensitive integrated matching for picture libraries,". *Pattern Anal. Mach. Intell., IEEE Trans.* 23:947–963, 2001.
48. Muhammad, K., Ahmad, J., Sajjad, M., and Zubair, M., "Secure image steganography using cryptography and image transposition,". *NED Univ. J. Res*. 12:81–91, 2015.
49. Dogan, S., Tuncer, T., Avci, E., and Gulten, A., A new watermarking system based on discrete cosine transform (DCT) in color biometric images. *J. Med. Syst.* 36:2379–2385, 2012.
50. Sajjad, M., Ejaz, N., and Baik, S. W., Multi-kernel based adaptive interpolation for image super-resolution. *Multimed. Tools Applic.* 72:2063–2085, 2014.
51. Mstafa, R. J., and Elleithy, K. M., "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes,". *Multimed. Tools Applic*. 1–23, 2015.
52. Ejaz, N., Mehmood, I., and Baik, S. W., Efficient visual attention based framework for extracting key frames from videos. *Signal Process. Image Commun.* 28:34–44, 2013.
53. Sun, Y., Chen, L., Xu, R., and Kong, R., An image encryption algorithm utilizing Julia Sets and Hilbert Curves. *PLoS One* 9: e84655, 2014.
54. Parah, S. A., Sheikh, J. A., Hafiz, A. M., and Bhat, G., Data hiding in scrambled images: A new double layer security data hiding technique. *Comput. Electrical Eng.* 40:70–82, 2014.
55. Mehmood, M., Sajjad, and Baik, S. W., Video summarization based tele-endoscopy: A service to efficiently manage visual data generated during wireless capsule endoscopy procedure. *J. Med. Syst.* 38: 1–9, 2014.
56. Wang, S., Banerjee, B. A., Barth, Y. M., Bhat, S., Chauhan, K. T., and Gottlieb, Wireless capsule endoscopy. *Gastrointest. Endosc.* 78:805–815, 2013.
57. De Avila, S. E. F., Lopes, A. P. B., da Luz, A., and de Albuquerque Araújo, A., VSUMM: A mechanism designed to produce static video summaries and a novel evaluation method. *Pattern Recogn. Lett.* 32:56–68, 2011.
58. Almeida, J., Leite, N. J., and Torres, R. D. S., Vison: Video summarization for online applications. *Pattern Recogn. Lett.* 33:397–409, 2012.
59. De Avila, S. E., da Luz, A., de Araujo, A., and Cord, M., "VSUMM: An approach for automatic video summarization and quantitative evaluation,". *Comput. Graph. Imag. Process. 2008. SIBGRAPI'08. XXI Brazilian Sympos.* 103–110, 2008.
60. Almeida, N. J., Leite, A., and Torres, R. D. S., Online video summarization on compressed domain. *J. Vis. Commun. Image Represent.* 24:729–738, 2013.
61. Lee, H.-G., Choi, M.-K., Shin, B.-S., and Lee, S.-C., Reducing redundancy in wireless capsule endoscopy videos. *Comput. Biol. Med.* 43:670–682, 2013.
62. Chen, Y., and Lee, J., "A review of machine-vision-based analysis of wireless capsule endoscopy video,". *Diagnos. Therapeut. Endoscopy.* 2012, 2012.
63. Chih-Yang, C.-C., Chang, and Yu-Zheng, W., Reversible steganographic method with high payload for JPEG images. *IEICE Trans. Inf. Syst.* 91:836–845, 2008.
64. Zhao, H., Wang, H., and Khan, M. K., Statistical analysis of several reversible data hiding algorithms. *Multimed. Tools Applic.* 52:277–290, 2011.
65. Wu, H., and Wang, H., "Multibit color-mapping steganography using depth-first search,". *Biomet. Sec. Technol. (ISBAST), 2013 Int. Sympos*. 224–229, 2013.