Sādhanā (2019) 44:119
https://doi.org/10.1007/s12046-019-1106-0

Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment

R SHANTHAKUMARI[1,*] and S MALLIGA[2]

[1]Department of Information Technology, Kongu Engineering College, Erode 638 060, India
[2]Department of Computer Science and Engineering, Kongu Engineering College, Erode 638 060, India
e-mail: shanabiraki@gmail.com; mallinishanth72@gmail.com

MS received 23 August 2018; revised 20 February 2019; accepted 11 March 2019; published online 20 April 2019

Abstract. The architecture development of cloud computing technology is growing tremendously in recent times, which leads to improvement of scalability, accessibility and cost reduction measures in the IT sectors of all enterprises. In this service, the data storage without reviewing security policies and procedures is a challenging task and probabilities of extracting secret information by an unauthorized intervention are more. However, to prevent the breaches of security in the cloud service, the steganography art plays an essential role in the data communication medium to improve the security measures, and it is an indispensable technique for hiding the secret information into a cover object. This paper describes the implementation of new steganography method with International Data Encryption Standard Algorithm (IDEA) and Least Significant Bit Grouping (LSBG) algorithm for embedding the secret information into an original image and extracting the same. The result shows the improvement of data embedding capacity and reduces the issues related to data security by effective utilization of this new approach, which reveals the remarkable achievement of the combinational execution of steganography and cryptography technique. The IDEA and LSBG have some vital qualities such as data confidentiality, integrity verification, capacity and robustness, which are crucial factors to achieve successful implementation of steganography process in data security system. The effectiveness and properties of the stego image can be evaluated by some specific measures like mean squared error, root mean squared error, peak signal to noise ratio and structural similarity index matrix to analyse the image quality. The results show that the proposed technique outperforms the existing methodologies and resolves the data security problem in data transmission and storage system of cloud computing services.

Keywords. Cloud storage; cryptography; confidentiality; data integrity; encryption; steganography.

1. Introduction

The potential technological growth with significant economies revenue of cloud computing makes a dramatic change in the computing service. This development has received considerable attention from businesses, media and academics in addition to IT industries to achieve their trouble-free network service and improved cost-saving measures. This cloud technology creates revolutionary changes and bounteous growth in the IT sectors through its reliable service. The architecture of this computing essentially comprises the abstraction of three layer constructs such as Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) in such a way that all the enterprises deploy the cloud computing services. Even though this technology has certainly benefitted many enterprises by reducing cost and meeting their stated goals within schedule, some problems related to data security issues still persist and remain in the unsolved state, since most of the potential users store their information in the unencrypted text file and the threats are more on security issues about data storage and transmission part in cloud computing. This issue can be overcome by enciphering and embedding data in images before storing it in cloud storage and retrieving it by deciphering method.

Generally, there are two techniques, cryptography and steganography, which are followed to protect secret message from unauthorized intervention at the time of data transmission. Cryptography is defined as an action to transform the primary information to different patterns in a way that is senseless to others by appropriate encoding process and ensure to decode the same with a unique authentication key. Steganography is another dynamic approach to conceal the secret data into a cover object so that it becomes unidentified and remains inattentive. Data embedding capacity and indistinctness are the reference points for the steganography process to implement the same successfully. The Simmons' Prisoners' Problem [1]

*For correspondence

proposed an elementary plan of steganography to escape from prison by a smart way of picture message communication between two persons, and there is a valuable explanation about steganography methodology in [2]. Studies [3–6] proposed an approach for the attainment of high-level preservation in steganography sequences [7]; digital file formats such as image and audio more suitable because of their characteristics of higher redundancy, which provides effective implementation of data hiding method. The process of image steganography defined an algorithm that embeds the secret information in a digital image with the aid of a powerful authentication code and then the outcome image is communicated to the intended recipient, who is responsible for extracting the secret information with the help of the same code.

Image steganography is commonly categorized into two parts as spatial domain and transform domain. Out of these two, the spatial domain is the most successful one for hiding information at cover image through the process of direct pixel manipulation method. The spatial domain contains some outstanding properties like transparency, minimum realization time and lesser complexity time [8]. During the implementation of image steganography techniques, the significant parameters such as data security, location of secret data in the cover object and high invisibility of hidden data must be focused upon to achieve the remarkable result through effective utilization of this technique.

In recent years, cloud computing systems have been developed and applied to scientific computations, web-based mail services, document sharing and so on. Among them, online-storage service is a very essential utility form as regards cloud computing systems. In general, authentication clients have their own independent directory and other users are not allowed to access these directories without prior authentication. However, in certain cases, the files stored in the cloud servers use cyber-attack techniques to read/write information through third parties. This is regarded as a great security threat or issue in cloud computing. This has motivated the present study to improve the security of image data in cloud using steganography.

In this paper, the authors have proposed a technique using the concept of International Data Encryption Standard Algorithm (IDEA) that is combined with Least Significant Bit Grouping (LSBG) algorithm in image steganography process for inserting the secret information into host image and provides an improved embedding capacity, adequate security and minimum distortion effect of the steganographic image.

The study is motivated by the idea from Saleh *et al* [28], which operates on the basis of AES; however the proposed method uses a new improved technique, which is discussed as follows.

The author proposes an approach based on steganography and cryptography techniques for secret data transfer in cloud environment. This combined technique attains data confidentiality, integrity verification, capacity and robustness that prove effective for the performance of the proposed method. Firstly, cryptography explains the execution of IDEA to encrypt the secret information in the form of text/file to attain high-level security. Secondly, LSBG algorithm and grey code procedure are used for embedding the encrypted data in image pixels to protect the secret information within the cover medium that forms one more single layer of security. Finally, the primary target of dual-layer protection is achieved through the combined techniques in the data transmission field. The concept of IDEA and LSBG algorithm provides the two-tier protection for secured data transmission process over an optimal communication channel and it is divided into two phases. The first phase performs the encryption and embeds the payload in the cover media and the second one defines the extraction of secret data followed by decryption method.

The rest of the paper is arranged as follows. Section 2 studies related work, section 3 describes the projected technique, section 4 analyses the diagnostic results and section 5 concludes the paper.

2. Related work

There are many techniques that are popular in the field of steganography. Mostly the Least Significant Bit (LSB) plane substitution method can be implemented effectively by changing the LSB of the cover media with the hidden information. Sharp [9] introduced a newly developed approach of key-based digital signal steganography to reduce the security threats while exchanging the secret information between two ends over an existing communication channel. In this technique, the sampled image format is a more convenient one compared with others such as video and audio signals to be selected as a cover image. The sequence of this method begins from the generation of symmetrical pre-shared key inclusive of actual random data for extracting the secret information by encoding and decoding algorithms. The performance of this technique is proved by the way it reveals the powerful resistance towards brute force attack.

Further improving on steganography methods, Wu and Tsai [10] introduced a new method for image steganography by embedding hidden information on the basis of consecutive pixel value difference into a greyscale as cover medium. In this method, a cover medium is split into non-overlapping parts of two consecutive pixels; later each piece of pixel value is verified to find the difference values. Finally, all difference values are segregated into many ranges for determining the data embedding capacity. This approach provides a robust imperceptible ability of stego image compared with the usual LSB method, attains improved data security and prevents the extraction of the secret information by illicit users

To overcome the problem of limited hiding capacity of existing methods, Wang *et al* [11] developed a new approach to embed the secret message into host media by optimal LSB replacement procedure, which proved that it attained an excellent embedding efficiency and was utilized even in the worst case, but the system performance was affected by the drawback of huge computation time, which led to introduction of another new technique to execute steganography of image with genetic algorithm. The outcome of this process is that an improved embedded data capacity is obtained and there is no sign of degradation in the quality of the embedding sequence. However, this also meets the same problem of large computation time.

Chan and Cheng [12] proposed an LSB replacement with pixel adjustment process, which delivers the stego image with enhanced image quality, and provides lower worst mean square error (WMSE) value compared with that of the usual LSB substitution method. The practical implementation of this system is attained by periodic verification of embedded error between cover media and final output of stego image and with minimum computational complexity. Chang and Tseng [13] presented a new steganography technique based on pixel-side information matching concept for execution of secret data embedding process and the correlation between very nearby pixels has the most important one to determine the input pixel location, which leads to finalization of the data embedding capacity. The data embedding in the pixel edge area attains higher value compared with the flat region, and this approach reveals that it provides an improved data hiding capacity with minimum distortion level.

Wu *et al* [14] initiated a novel steganography method of image established by way of Pixel Value Differencing (PVD) and LSB substitution technique. For implementing this, initially, the PVD method is applied to attain a dissimilar value from two continuous pixels of the host image. The pixel value difference is classified into two types – smaller and bigger – and according to this value range, it can be positioned on the smooth and edge area of cover media, respectively. The secret information is concealed in the flat area of a still image by LSB replacement scheme and the PVD method is utilized to obscure the secret information into edge area. The final evolution of this method achieves significant improvements in undercover data capacity to be embedded into cover media and higher level imperceptibility of stego image. Mielikainen [15] proposed an enhanced steganography method to embed the information into grey variation host image by LSB matching technique, which applies a binary operation to embed 2 bits of the secret message into 2 pixels of host media. The outcome of the scheme shows lower mean square error (MSE) value 0.375 per pixel than the expected MSE value of 0.5 per pixel of LSB algorithm with confirmed minimum distortion level and provides powerful opposition against current attacks.

Kekre *et al* [16] introduced a new improved LSB technique for the execution of steganography of greyscale image and 24-bit colour image. The end result of this method shows higher level of embedding capacity and imperceptibility than the LSB method. Zhang *et al* [17] presented a steganography approach based on PVD technique where the cover image is divided into non-overlapping parts including two linking pixels and the pixel difference in every region is converted to embed the data into a cover image. The same sequences are followed to the next target pixel for retaining higher imperceptibility capacity with good visual properties to the stego image. The improved histogram efficiency of cover media and stego image is one of the achievements of this approach, but the dataset capacity for experiments is minimal.

Zhang [18] presented a novel reversible data hiding scheme for an encrypted image. First, the whole information of an uncompressed image is encrypted to embed the additional data into the image through simple alteration in a small portion of encrypted data, but in this technique, there are some possibilities to decrypt the image by an intruder who knows about the encryption code and to extract the private content in the cover media. Jain and Ahirwal [19] described that based on the range stego code generation, the image pixel is divided into ranges that are five different grey level ranges of an image in private stego-key, and in which each range indicates embed data in the LSBs of the image by substituting the fixed number of bits. The capability of this process is a high virtue of secret information in stego image and it is not discernible to an observer. Researches show that to improve the integrity of confidential data, the extra bits of the witness are to be obscured with secret information, and deformities in the image are possible.

Chung-Li Hou proposed and developed a new technique [20], which focuses mainly on reducing the distortion level between host and stego image by effective implementation of tree-based parity check method for concealing the secret information into cover media. This process describes that all the pixels in each row of an image matrix are used for embedding the data bits, without considering whether pixels are in the smooth region or edge region of the cover image. There are some drawbacks to this system, which lead to asymmetry between cover and stego. At the same time, distortion is also increased due to hidden information bits that are inserted in the pixels without considering the nearby pixel values. Hussain and Hussain [21] set forth a new steganography method of an image by embedding secret data in the horizontal edges of the host image. In this process, initially, the horizontal edge length is measured by the computation of the cover image edges to embed data close to margin pixel. Finally, the identical edge properties of cover and stego are verified to attain improved PSNR value, but the limited data embedding capacity reduces the efficiency of this method. Luo *et al* [22] also presented an edge-adaptive method for image steganography process in

which the size of the embedded message and difference of two continuous pixels in the host object are analysed to choose the right portion for inserting the hidden information into the cover media. The security of hidden message gets improved in an excellent way compared with common LSB-based strategy. This scheme is examined with various cover media, and finally it reveals that greyscale images are more convenient to edge-adaptive technique.

Shanthakumari and Malliga [23] introduced a new scheme to insert the private content into the cover image by tree-based parity check with LSBMR and build the stego image with lower deformation compared with a cover medium. Secret data are inserted into the edge portion of a cover image and this achieves minimum distortion level with improved security. However, this plan contains one more drawback—with tree level expansion it is not possible to obtain more than two levels. Liao *et al* [24] proposed a new approach of steganography based on digital picture with 4-pixel differencing and revised LSB replacement method for embedding the data into cover media. To precisely predict the level that the particular pixel block lays, the pixel values get readjusted by the readjustment procedure. In the readjustment procedure, each pixel block is needed to be worked out with 81 possible combinations for reaching the final resultant block. Thus, the determination of higher or lower level is done in a sophisticated manner, and the distortion between cover and stego image is also increased. To overcome this, Shanthakumari and Malliga [25] proposed a technique of multi-pixel differencing and HL code for execution of LSB-based digital image steganography scheme to attain the high-level embedding capacity with minimum distortion between host and stego image. In this, the concept of HL code is used to make all the pixels of those blocks as an embedding unit for hiding the secret bits by directly predicting the higher and the lower order blocks.

Mandal and Das [26] proposed a new adaptive PVD system for grey image steganography to reduce the occurrence of inappropriate visualization of the stego image when the pixel value exceeds the greyscale order. This method results in identical payload and visual fidelity. Shanthakumari *et al* [27] proposed the Least Significant Bit Inversion (LSBI) algorithm, one of the most reliable techniques for execution of steganography process in data communication, and it provides higher degree of embedding capacity, with much lower distortion level between the original and the stego images. In this technique, security of secret information embedding by grey code standard obtained adequate protection, which conforms to the formation of protection layer at cover image and the hidden data are not discernible to the observer. An outcome of some studies mentioned earlier is that even though the way of effective implementations of the data embedding technique is easy, some inconveniences such as embedding capacity, security and deformation of the original image are the crucial factors considered to get more improvements. However, the proposed scheme of IDEA and LSBG algorithm can resolve all the issues, and there would be sufficient improvement in the embedding capacity, adequate protection and minimization of the distortion between cover and stego images.

3. Proposed method

In this part, the author proposes an improved new approach based on a combination of steganography and cryptography techniques for concealing the secret content into a carrier medium to provide adequate protection for secret data transfer over a typical communication medium. This blend of technology has successfully reached the benchmark level of some essential properties known as data confidentiality, capacity and robustness, which are the evidence to prove the excellent performance and effective implementation of this steganography process. Cryptography explains the execution of IDEA to encrypt the secret information in the form of text/file to attain high-level security. Another one is LSBG algorithm, and grey code procedure to hide encrypted messages in image pixels to protect the secret information within the cover medium that forms one more single layer of security. Finally, the primary target of dual-layer protection is achieved through the combined techniques in the data transmission field. Figure 1 shows an overall block diagram of the proposed method; it explains that the specific combinational concept of IDEA and LSBG algorithm provides the two-tier protection for secured data transmission process over an optimal communication channel, and the detailed explanations are divided into two phases, namely phases I and II as shown in figure 2. The first phase performs the encryption and embeds the payload in the cover media and the second one defines the extraction of secret data followed by decryption method.

The cloud computing system is constructed in the local network for investigating the safety and security of image data. The proposed system constructs the cloud using two servers, and several clients are used for several services and implemented on server-side and client-side applications. The main prototype for the cloud model in the proposed method is as follows.

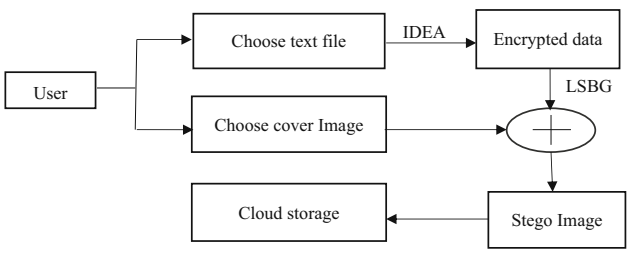

Figure 1. Overall block diagram of proposed method.

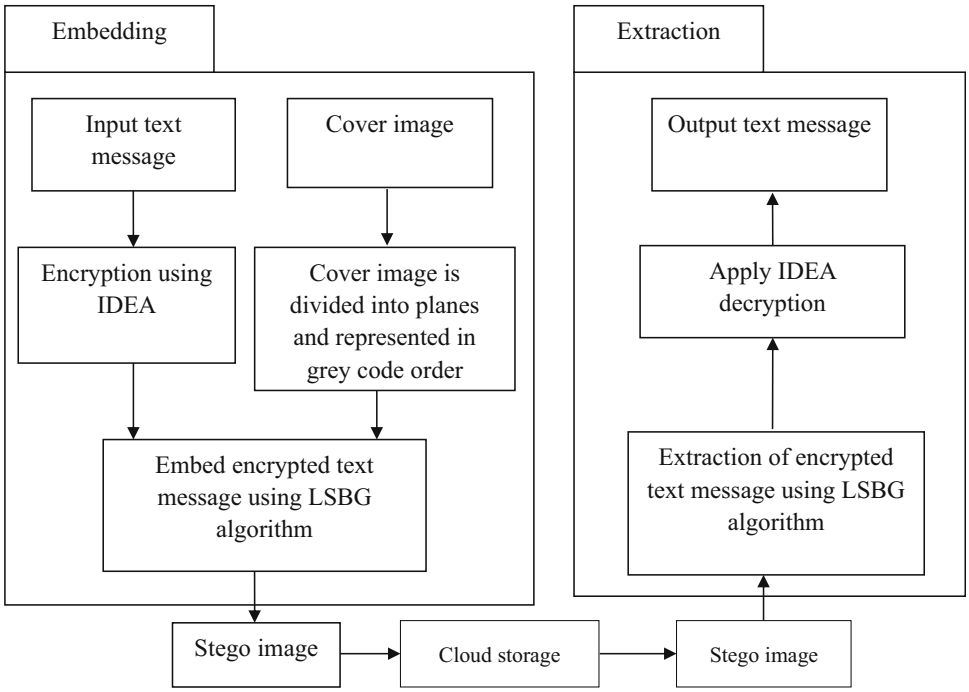

Figure 2. Proposed method.

- Cover data generator: dynamic generation of steganographic image.
- Storage server: store the steganographic image that is uploaded from the client.
- Client: Input the message, hide it into steganographic image and upload it to the storage server.

3.1 *Phase I*

The secret data embedding procedure of proposed method is explained as follows:

1. Select the input-obscure text file that is ready to be hidden in the cover object.
2. Finalize the cover object from the source files.
3. First, encrypt the obscure text data by IDEA procedure explained in section 3.2a.
4. The encrypted confidential data from step 3 to cover object by LSBG algorithm as explained in section 3.2b.
5. Upload the resultant stego image obtained from step 4 on cloud.

3.2 *Phase II*

The Secret data extraction procedure from stego image is explained as follows:

1. Select the stego image that is to be downloaded.
2. Download the stego image from the cloud.
3. Extract the secret text message from stego image using LSBG algorithm as defined in section 3.3a.
4. Apply IDEA decryption process explained in section 3.3b.

The projected method of IDEA and LSBG algorithm consists of the two segments, as shown in figure 2.

3.1a *P1: procedure for encryption algorithm*: The protection process of secret data is done by implementing a symmetric encryption algorithm named IDEA, and the same authentication code is used for secret data insertion and retrieval. The process of decryption is executed using the concept of the same encryption algorithm for extraction of private content from cover object except that sub-keys are derived using a different algorithm that would be improved by modifying the size of a secret key used in the encryption and decryption operation on the data. The block cipher IDEA operates with 16-bit plaintext and cipher text blocks and is controlled by a 32-bit key.

The Plain IDEA technique describes that there are four identical cycles and a "half cycle" end transformation and mixes three algebraic operations on nibbles (4-bit blocks): bitwise XOR, addition modulo 2^4(= 16) and multiplication modulo $2^4 + 1$(= 17). There are 16 possible nibbles, among which 14 steps of a complete cycle are given here.

The following steps illustrate the algorithm.

Input: secret data, key

Output: cipher text

Let the plaintext bits be stored in $A1$–$A4$ and the 28 sub-keys be named as $Y1$–$Y28$.

a. Make multiplication of $A1$ and sub-key $Y1$.
b. Make addition of $A2$ and sub-key $Y2$.
c. Make addition of $A3$ and sub-key $Y3$.
d. Make multiplication of $A4$ and sub-key $Y4$.
e. XOR the results of actions a and c.
f. XOR the results of actions b and d.
g. Make multiplication of the result of action e and sub-key $Y5$.
h. Make addition of the actions f and g.
i. Make multiplication of the result of action h and sub-key $Y6$.
j. Make addition of actions g and i.
m. Make XOR the result of actions a and i.
n. Make XOR the results of actions c and i.
o. Make XOR the results of actions b and j.
p. Make XOR the results of actions d and j.

The process is repeated from step a to step p for the remaining three cycles, but with different sub-keys. After the completion of series 4, the final transformation occurs, which consists of the following steps.

q1: Make multiplication of $A1$ and the sub-key $Y25$.
q2: Make addition of $A2$ and the sub-key $Y26$.
q3: Make addition of $A3$ and the sub-key $Y27$.
q4: Make multiplication of $A4$ and the fourth sub-key $Y28$.

After these steps are performed, the resultant bits are grouped into 7 bits and their corresponding characters are found, which represent the encrypted message. The encoded data are stored in a file.

3.1b *P2: procedure for data embedding*: The following details explain the procedure of information embedding algorithm.

Input: cover object, cipher text.
Output: stego image.

1. Choose the appropriated cover object from source.
2. The cover object is split into 4 8-bit planes and they represent the grey code order (group1 represents the value 00, group2 represents the value 01, group3 represents the value 11 and group4 represents the value 10).
3. Read the encrypted data as a result of encryption algorithm and the same is converted into ASCII code form as much as the final text.
4. The result of the afore-mentioned step is converted into a binary bit, and if its total counting is an odd figure, then one more bit '0' is to be inserted in the end. Otherwise, there is no change in the process.

4a. Finally the total binary bit is split into 2-bit blocks for a primary input of the projected algorithm.
4b. The 2-bit blocks are verified with grey code group specified in step 2 to match it with bit value. If the result of this verification is true, the corresponding pixel is selected and the 1st LSB bit is changed as '1' and remaining pixel's 1st LSB positions are marked as '0'up to its final pixel. The step 4b procedure is repeated for second and third LSB bits, and finally stego image is obtained.

3.2a *P3: procedure for data extraction using LSBG algorithm*: The same sequences of embedding process are followed in the reverse direction to extract the private content in the stego image by utilizing the decoding procedure received from the sender. The detailed data retrieving algorithm is presented here.

Input: stego image.
Output: cipher text.

1. Study the received stego image.
2. The received format is split into 4 8-bit planes, and the planes represent the grey code order.
3. Retrieve the pixels that have the value '1' in their LSB position. The step 3 procedure is repeated for second and third LSB bits.
4. Draw out the group valuation in line with the used location.
5. The superior outcome is split into 7-bit block up to its final pixel, and this block is converted into a decimal system that represents the particular ASCII value of the coded data.
6. The ASCII values are transformed into their equal identity to achieve the coded content material.

3.2b *P4: procedure for decryption algorithm*: The same process sequences of encryption are followed to implement the decryption method with a generation of the new decryption code. IDEA decryption procedure consists of applying the same concept of encryption; fresh codes must be produced for retrieval; A_j^i supplies the j^{th} decryption code of decryption cycle i. Y_j^i supplies the p^{th} encryption code of encryption cycle i. For the 1st decryption cycle, $A_1^1 = (Y_1^5)^{-1}$, where $(Y_1^5)^{-1}$ supplies the multiplicative inverse of the 1st encryption code of encryption cycle 5 modulo 17, $A_1^2 = -Y_2^5$, where $-Y_2^5$ supplies the additive inverse of the second encryption code of encryption cycle 5 modulo 16, $A_1^3 = -Y_3^5$; $A_1^4 = (Y_4^5)^{-1}$; $A_1^5 = A_5^4$ and $A_1^6 = Y_6^4$. The same decryption codes are produced in the remaining complete decryption cycle. The decryption code for the last conversion "half cycle" is $A_1^5 = (Y_1^1)^{-1}$, $A_2^5 = -Y_2^1$, $A_3^5 = -Y_3^1$ and $A_4^5 = (Y_4^1)^{-1}$.

The decryption algorithm works in the following way.

Input: cipher text.
Output: secret data.

Let the cipher text bits be stored in $C1$–$C4$, and the 28 sub-keys be named as $Y1$–$Y28$.

a. Make multiplication of $C1$ and sub-key $Y1$.
b. Make addition of $C2$ and sub-key $Y2$.
c. Make addition of $C3$ and sub-key $Y3$.

d. Make multiplication of $C4$ and sub-key $Y4$.
e. XOR the results of actions a and c
f. XOR the results of actions b and d.
g. Make multiplication of the result of action e and sub-key $Y5$.
h. Make addition of actions f and g.
i. Make multiplication of the result of action h and sub-key $Y6$.
j. Make addition of actions g and i.
m. Make XOR the result of actions a and i
n. Make XOR the results of actions c and i.
o. Make XOR the results of actions b and j.
p. Make XOR the results of actions d and j.

The process is repeated from step 2 to step 15 for the remaining three cycles, but with different sub-keys. After round 4, the final transformation occurs, which consists of the following steps.

q1: Make multiplication of $C1$ and the sub-key $Y25$.
q2: Make addition of $C2$ and the sub-key $Y26$.
q3: Make addition of $C3$ and the sub-key $Y27$.
q4: Make multiplication of $C4$ and the fourth sub-key $Y28$.

The obtained bits are grouped into 7 bits, and the ASCII value of the hidden information is represented by the corresponding decimal values evaluated from this group. After completion of these step processes, confidential data are extracted correctly from stego image.

4. Experimental results and analysis of the proposed method

4.1 *Security analysis*

The security attribute of IDEA and LSBG technique is presented with various factors.

Confidentiality	The proposed approach ensures that sensitive information is protected from illegal users by revealing only encrypted file information to cloud service provider
IDEA	To crack an IDEA-encrypted message using a brute force approach, it would take longer than the age of universe of approximately 10^{13} years. Hence, IDEA encryption algorithm is considered to be a secure cipher

4.2 *Evaluation assessment*

Steganography assessments are made on three aspects.

Assessment I – imperceptibility/quality.
Assessment II – capacity or payload.
Assessment III – robustness or resistance to attacks.

4.2a *Assessment I: imperceptibility/stego-image quality*: It is the measurement of the indistinct level of hidden information embedded in the cover media and used to quantify the obscurity of secret data in a stego image. The properties of an image could be evaluated by comparing them with the precise quality of a stego image, and the perceptual quality of an image is assessed by the measures of similarity between original and stego images. There are simple statistic error metrics of objective quality or distortion assessment approach. Some of the existing measuring standards such as MSE, root mean squared error (RMSE), peak signal to noise ratio (PSNR), structural similarity index matrix (SSIM), image fidelity (IF), absolute error (AE), normalized cross–correlation (NCC), average difference (AD) and structural content (SC) are followed for scaling image quality.

4.2a1 *MSE*: MSE defines the squared difference between the quality of estimated and observed stego image. It is a more convenient method to measure the quality of the full stego image. MSE calculation is used in image processing and defined as in Eq. (1):

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(Y_{i,j} - Y'_{i,j})^2. \tag{1}$$

Equation(1) expresses that m and n are the numbers of rows and columns, respectively, of the cover media, while $Y_{i,j}$ and $Y'_{i,j}$ refer to pixel value from the cover image and stego image, respectively.

4.2a2 *RMSE*: RMSE is one of the ways to quantify the difference between cover image and stego image and defined as follows:

$$\mathrm{RMSE} = \mathrm{MSE}^{\frac{1}{2}} \tag{2}$$

4.2a3 *PSNR*: PSNR is evaluated in decibels and inversely proportional to the MSE. It is used as metrics to verify the perceptual quality of stego image. It is given by Eq. (3):

$$\mathrm{PSNR} = 10\log 10(255 \wedge 2/\mathrm{MSE}). \tag{3}$$

4.2a4 *SSIM*: SSIM is an evaluation of the similarity between input and output images of steganography technique and used to quantify the SSIM index based on an initial defect-free image as a reference of stego image. It is given by Eq. (4):

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{4}$$

where μ_x, μ_y are, respectively, the average values of x, y and σ_x^2, σ_y^2 are the variances of x and y.

4.2a5 *IF*: Fidelity is the perceptual similarity between images before and after processing. IF is as given in Eq. (5):

Table 1. MSE, RMSE, PSNR, SSIM, IF, AE, NCC, AD and SC for test images.

		Quality metrics				
Embedding capacity (bits)	Test images	Mean Squared Error (MSE)	Root Mean Squared Error (RMSE)	Peak Signal to Noise Ratio (PSNR)	Structural Similarity Index Matrix (SSIM)	Image Fidelity (IF)
7,86,432	Lena	0.856470	0.925456	54.85	0.996780	1.000000
7,86,432	Baboon	0.904756	0.951186	54.62	0.996525	1.000000
7,86,432	Peppers	0.881097	0.938667	54.73	0.987959	1.000000

		Quality metrics			
Embedding capacity (bits)	Test images	Absolute error (AE)	Normalized cross correlation (NCC)	Average difference (AD)	Structural content (SC)
7,86,432	Lena	0.008015	1.000000	0.441864	1.000000
7,86,432	Baboon	0.007599	1.000000	0.459389	1.000000
7,86,432	Peppers	0.006939	1.000000	0.547024	1.000000

$$\mathrm{IF} = 1 - \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(y(i,j) - y'^{(i,j)}\right)^2}{\sum_{i=1}^{m}\sum_{j=1}^{n} y(i,j)^2}. \quad (5)$$

4.2a6 *AE*: AE is the absolute difference between the original and the stego images. It is given by Eq. (6):

$$\mathrm{AE} = |y(i,j) - y'(i,j)| \quad (6)$$

where matrix y corresponds to the original image and matrix y' corresponds to the after-image steganography.

4.2a7 *NCC*: NCC has been commonly used as a metric to evaluate the degree of similarity or dissimilarity between two compared images and defined as follows:

$$\mathrm{NCC} = \sum_{\mathrm{i}=1}^{m}\sum_{j=1}^{n}\frac{(y(i,j)y'(i,j))}{\sum_{i=1}^{m}\sum_{j=1}^{n}(y(i,j))^2}. \quad (7)$$

4.2a8 *AD*: AD is the average difference between the stego image and the test image and defined as follows:

$$\mathrm{AD} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(y(i,j) - y'(i,j)). \quad (8)$$

4.2a9 *SC*: SC is also a correlation-based measure and it measures the similarity between two images. SC is given by Eq. (9):

$$\mathrm{SC} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(y(i,j))^2}{\sum_{i=1}^{m}\sum_{j=1}^{n}(y'(i,j))^2}. \quad (9)$$

4.2b *Assessment II: capacity/payload*: Capacity or payload defines the cover media capacity to hide the confidential information with high indistinct level. It provides a measure of the maximum number of bits that can be hidden into the cover image with an acceptable stego image quality.

4.2c *Assessment III: robustness/resistance to attacks*: Robustness defines the quantity that determines effective implementation of a steganography technique and maintenance of high-level stability against breach of security. There are some crucial factors such as imperceptibility (PSNR), payload and robustness (immunity to visual analysis, histogram analysis and chi-square) that are involved in determining successful execution of the steganography process in the data communication system. This new approach is intensely tested through several steganalysis attacks, visual analysis, histogram and chi-square. The outcome of the experimental result shows that the stego image has delivered strong opposition force against all attacks.

4.3 *Results for Assessments I and II*

To appraise the fulfillment of the proposed method over some existing systems, some experimental results are shown in the tables. Matlab is used to implement the proposed method and the program is run using a 2.67-GHz processor with 4.0-GB RAM. More than 50 images are tested using the proposed method. The experiment is carried out on the images named "Lena", "Baboon" and "Peppers" collected from the benchmark datasets.

In table 1, embedding capacity refers to the amount of concealed information inside a cover image. With our proposed approach, all images are of resolution 512 × 512; we take 4 pixels in a group to embed 12 bits at a time. Therefore, the embedding capacity of our scheme is 7,86,432 bits. The results for various evaluation factors like MSE, RMSE, PSNR, SSIM, IF, AE, NCC, AD and SC are presented in table 1, which shows different parameter values for different types of cover media, which is completed by the text embedding process.

From table 1, it is proved that the MSE value is very low for all the images and the PNSR value ranges between 54.62 and 54.85 dB, which implies good performance. The

utilization of the IDEA to provide security to the images on the basis of cryptography and steganography leads to good performance in terms of PSNR. NCC and SC have attained the value of 1, which implies that there is high similarity between cover image and the retrieved stego image. The AD is calculated between cover and stego images; the best value close to 0 is achieved if there is no major change in pixel values of stego image after embedding message bit. AE is the statistical difference between the cover and the stego image. The small value indicates the high quality of host and stego image.

4.3a *Evaluation of Assessments I and II of the proposed and existing techniques*: Comparison of existing techniques with the proposed approach on the basis of PSNR and embedding capacity is shown in table 2. In view of the capacity of embedding, the steganographer can minimize the detection risk by better selection of a secure cover image for a certain payload. Embedded capacity is considered as the maximum embedded rate limit, where the stego image can be recognized by a steganalyser when the size of hidden data exceeds the limit. The experimental result (table 2) of high embedding capacity ensures that the image is embedded in a secure way.

The evaluation of Assessments I and II shows improvement of imperceptibility and capacity with higher data hiding level when compared with other methods. An image with a PSNR value above 30 dB is widely accepted as an image of good quality. The proposed approach provides high PSNR results in addition to doubling the hidden data payload compared with its classical counterparts. The proposed approach is able to maintain a good PSNR value for a sufficiently large payload of 7,86,432 bits.

Table 2 shows the embedding capacity of different approaches and the proposed method provides good PSNR value with better image quality. For "Lena" image with payload of 7,86,432 bits, the PSNR obtained is 54.85, which is better when compared with that of the values obtained with PVD, side match, adaptive LSB, colour PVD and crypto-stegno algorithm with minimum payload, whose PSNR values are 59.81, 41.2, 59.1, 42.3 and 44.96, respectively.

In all the cases, the proposed work yields better results in terms of PSNR. On an average, a PSNR value of 54.73 is obtained with the proposed method, which is a significant improvement.

4.4 *Results for Assessment III: robustness/ resistance to attacks*

4.4a Statistical analysis: visual analysis: Visual analysis is simply analysing the image visually and looking for anomalies or artefacts of embedding. Figure 3 reveals the result of the visual analysis of the proposed method on

Table 2. Capacity and PSNR value comparison of existing techniques.

Techniques	PVD		Side match		Adaptive LSB		Colour PVD		Crypto_stegno algorithm		Proposed technique	
Author	Wu *et al*'s scheme (2003)		Chang *et al*'s scheme (2004)		Kekre *et al*'s scheme (2008)		Mandal *et al*'s scheme (2012)		Saleh *et al*'s scheme (2016)		LSBG	
Test Images	Embedding capacity (bits)	PSNR (dB)	Embedding capacity (bits)	PSNR (dB)	Embedding capacity (bits)	PSNR (dB)	Embedding capacity (bits)	PSNR (dB)	Embedding capacity (bytes)	PSNR (dB)	Embedding capacity (bits)	PSNR (dB)
Lena	35,827	59.1	48,626	41.2	35,827	59.1	1,45,787	42.3	62,208	44.96	7,86,432	54.85
Baboon	34,235	59.4	57,146	37.2	34,235	59.4	1,44,916	38.4	63,408	42.81	7,86,432	54.62
Peppers	60,317	56.2	50,907	40.8	50,907	40.8	1,45,995	42.3	62,000	44.83	7,86,432	54.73

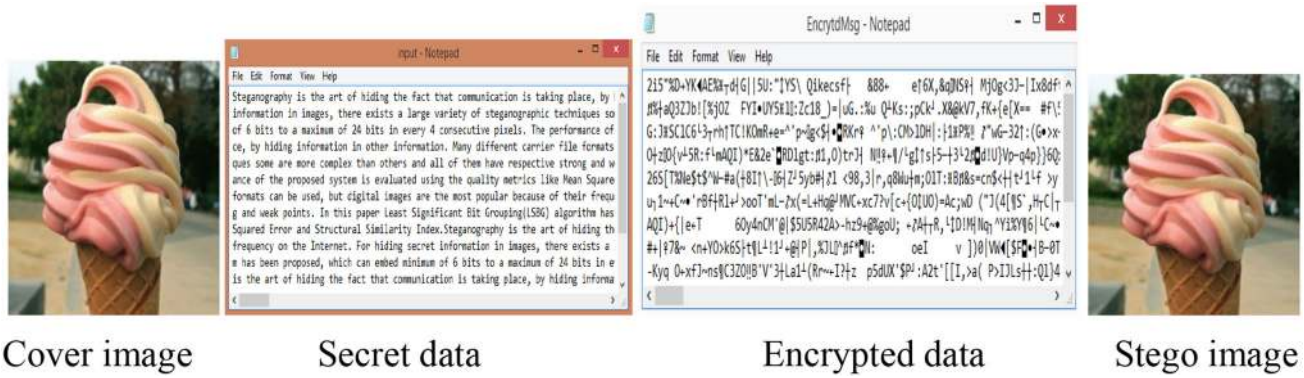

Figure 3. Visual analysis.

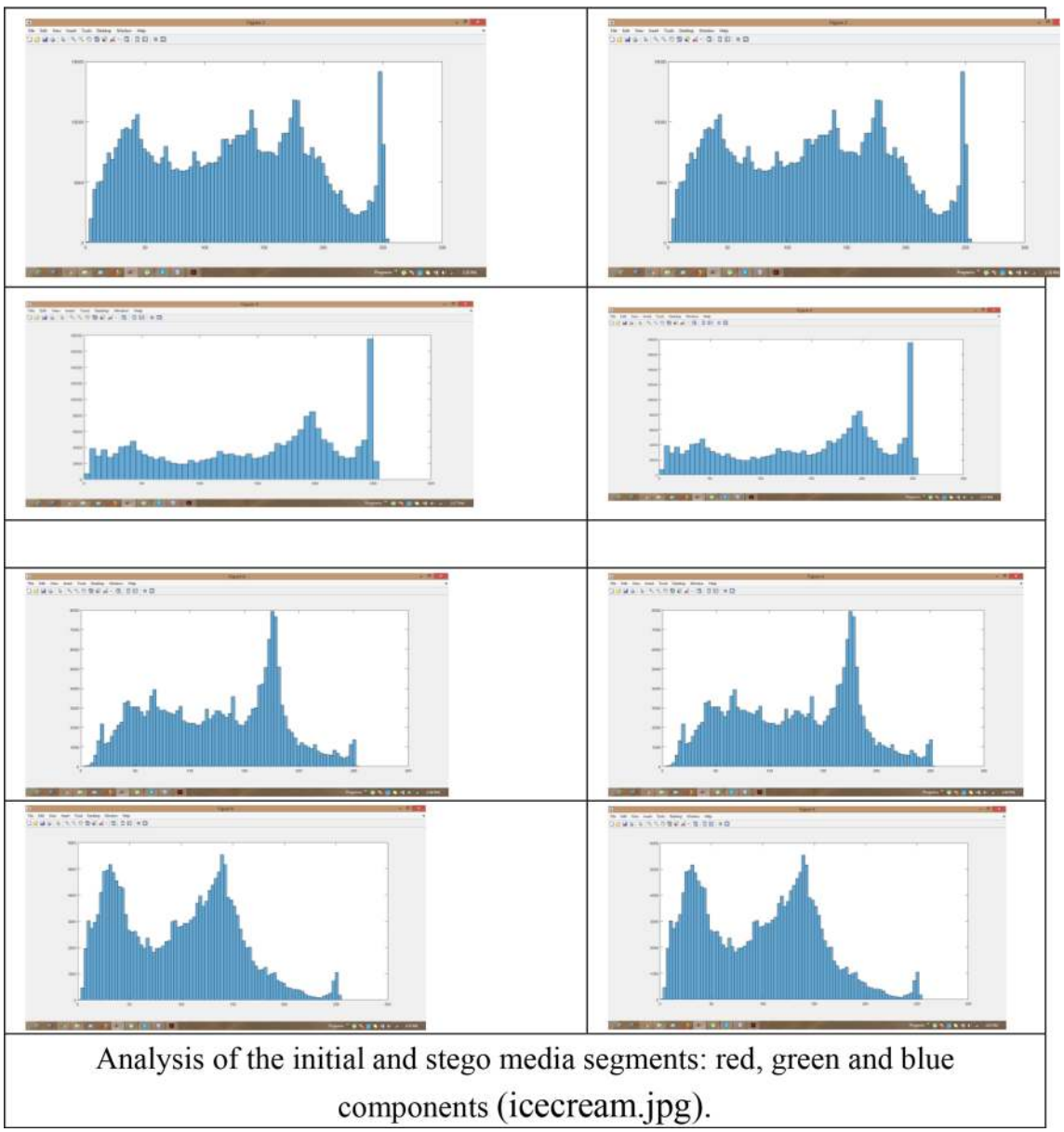

Figure 4. Histogram analysis.

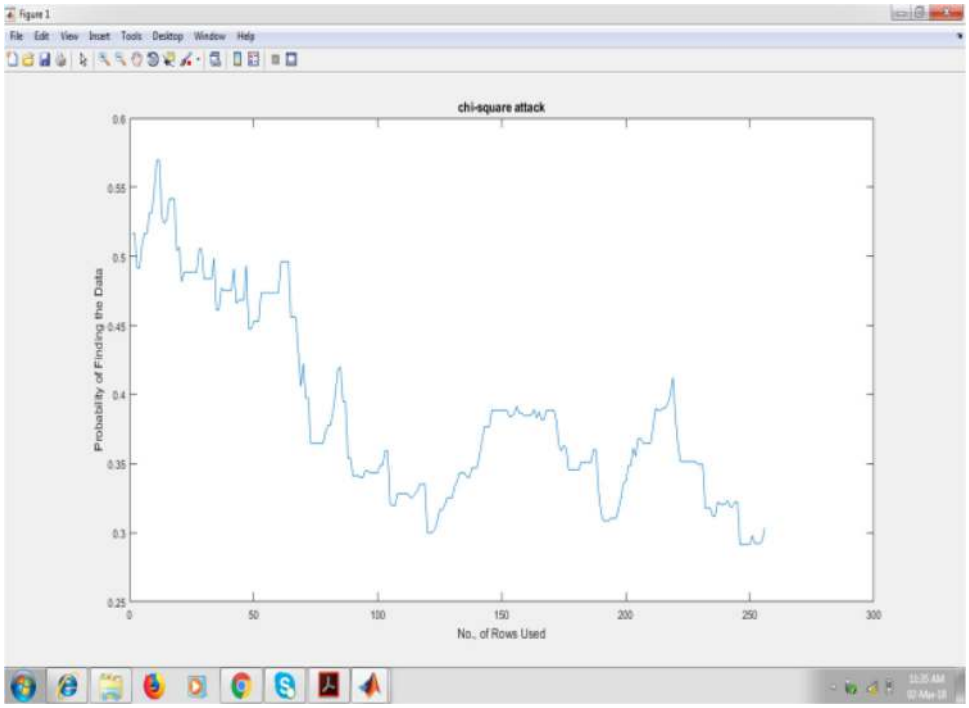

Figure 5. Chi-square attack.

colour image (icecream.jpg), and it does not clearly define the visual difference between input and output images. This technique successfully withstands visible attacks also.

4.4b *Statistical analysis: histogram analysis*: Histogram is a graphical representation of intensity values in an image. The *X*- and *Y*-axes of the plots represent pixel values and number of pixels, respectively, to evaluate the visual image quality. Figure 4 presents the result of the histogram analysis; both the images are the same. It does not clearly define susceptible attacks.

4.4c *Statistical analysis: chi-square attack*: The chi-square attack is a method to test the robustness of the security system against the attacks. Chi-square attack tests even the proposed approach, which successfully withstands this attack as shown in figure 5. After phase I, the stego image is examined by the chi-square attack to check the degree of imperceptibility of the proposed approach. The highest probability of finding the secret information in the tested stego image is found to be 57%. Thus, it is evident that the intruder cannot alter the proposed scheme.

5. Conclusion

The intention of this paper is achieved by the successful execution of the new steganography approach for an image and this process is integrated into two techniques: IDEA and LSBG algorithm. Compared with other methods, it attained higher imperceptibility (PSNR) with lower MSE. The hiding capacity also got improved by the utilization of lower side 6 bits to a higher side 12 bits of data embedded in every 4 pixels. The grey code procedure is followed to obscure the secret information into the cover media to make a formation of the single layer of security and encrypting the secret data before embedding using IDEA, which provides the second layer of protection.

It can be observed from the results of the proposed scheme that the efficiency of this technique is higher than that of the other methods and high embedding capacity is achieved. As it is integrated with IDEA, the robustness of the proposed technique is high and the same is subjected to several tests such as visual analysis, histogram analysis and chi-square analysis. Finally, the outcomes of this technique are satisfactory, and future intention is to implement this method in audio and video steganography.

References

[1] Simmons G J 1984 The prisoners' problem and the subliminal channel. In: Chaum D (Ed.) *Advances in Cryptology, Proceedings of CRYPTO '83*. New York: Plenum Press, pp. 51–67

[2] Johnson N F and Jajodia S 1998 Steganography: seeing the unseen. *IEEE Computer* 16: 26–34

[3] Bhattacharyya S and Sanyal G 2008 Study of secure steganography model. In: *Proceedings of the International*

Conference on Advanced Computing and Communication Technologies, Panipat, India

[4] Bhattacharyya S and Gautam Sanyal G 2009 An image based steganography model for promoting global cyber security. In: *Proceedings of the International Conference on Systemics, Cybernetics and Informatics*, Hyderabad, India

[5] Bhattacharyya S and Sanyal G 2009 Implementation and design of an image based steganographic model. In: *Proceedings of the IEEE International Advanced Computing Conference*, Patiala, India

[6] Bhattacharyya S, Prasad A and Sanyal K G 2010 A novel approach to develop a secure image based steganographic model using integer wavelet transform. In: *Proceedings of the International Conference on Recent Trends in Information Telecommunication and Computing*

[7] Morkel T, Eloff J H P and Olivier M S 2005 An overview of image steganography. In: *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandton, South Africa, June/July

[8] Brainos A C 2004 A study of steganography and the art of hiding information. *Security Writer*, East Carolina University

[9] Sharp T 2001 An implementation of key-based digital signal steganography. In: *Proceedings of the Information Hiding Workshop*, Springer LNCS 2137, pp. 13–26

[10] Wu D C and Tsai W H 2003 A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters* 24(9): 1613–1626

[11] Wang R Z, Lin C F and Lin J C 2001 Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition* 34: 671–683

[12] Chan C K and Cheng L M 2004 Hiding data in images by simple LSB substitution. *Pattern Recognition* 37: 469–474

[13] Chang C C and Tseng H W 2004 A steganographic method for digital images using side match. *Pattern Recognition Letters* 25: 1431–1437

[14] Wu H C, Wu N I, Tsai C S and Hwang M S 2005 Image steganographic scheme based on pixel-value differencing and LSB replacement methods. In: *IEE Proceedings – Vision, Image and Signal Processing* 152(5): 611–615

[15] Mielikainen J 2006 LSB matching revisited. *IEEE Signal Processing Letters* 13(5): 285–287

[16] Kekre H, Athawale A and Halarnkar P N 2008 Increased capacity of information hiding in LSB's method for text and image. *International Journal of Computer and Information Engineering* 2(5): 1497–1500

[17] Zhang H, Geng G and Xiong C 2009 Image steganography using pixel-value differencing. In: *Proceedings of the Second International Symposium on Electronic Commerce and Security*, vol. 2, pp. 109–112, https://doi.org/10.1109/isecs.2009.139

[18] Zhang X 2010 Reversible data hiding in encrypted image. *IEEE Signal Processing Letters* 18(4): 255–258

[19] Jain Y K and Ahirwal R R 2010 A novel image steganography method with adaptive number of least significant bits modification based on private stego-keys. *International Journal of Computer Science and Security* 4(1): 40–49

[20] Hou C L, Lu C C, Tsai S C and Tzeng W G 2011 An optimal data hiding scheme with tree-based parity check. *IEEE Transaction on Image Processing* 20(3): 880–886

[21] Hussain M and Hussain M 2011 Embedding data in edge boundaries with high PSNR. In: *Proceedings of the Conference on Emerging Technologies*, https://doi.org/10.1109/icet.2011.6048469

[22] Luo W, Huang F and Huang J 2010 Edge adaptive image steganography based on LSB matching revisited. *IEEE Transactions on Information Forensics and Security* 5(2): 201–214

[23] Shanthakumari R and Malliga S 2015 Data hiding in image using tree based parity check with LSB matching revisited algorithm. *International Journal of Innovative Research in Computer and Communication Engineering* 3(6): 5472–5479

[24] Liao X, Wen Q and Zhang J 2011 A steganographic method for digital images with four-pixel differencing and modified LSB substitution. *Journal of Visual Communication and Image Representation* 22(1): 1–8

[25] Shanthakumari R and Malliga S 2017 Information hiding in digital images using modified LSB substitution with multi-pixel differencing and HL code. *Asian Journal of Research in Social Sciences and Humanities* 7(1): 198–207

[26] Mandal J K and Das D 2012 Steganography using adaptive pixel value differencing (APVD) for gray images through exclusion of underflow/overflow. *Computer Science & Information Technology, CSCP Series*, pp. 93–102, ISBN: 978-1-921987-03-8

[27] Shanthakumari R, Malliga S and Dheepika S 2014 Data hiding scheme in spatial domain. *International Journal of Computer Science Engineering and Technology* 4(12): 400–403

[28] Saleh M E, Aly A A and Omara F A 2016 Data security using cryptography and steganography techniques. *International Journal of Advanced Computer Science and Applications* 7(6): 390–397