Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 14 (8): 738-747, 2014
ISSN 1812-5654 / DOI: 10.3923/jas.2014.738.747

Image Steganography with Multilayer Security Using Moderate Bit Substitution

[1]Balkrishan Jindal and [2]Amar Partap Singh
[1]Yadavindra College of Engineering, Punjabi University, Guru Kashi Campus,
Talwandi Saboo, Dist Bathinda-151302, Punjab, India
[2]Sant Longowal Institute of Engineering and Technology, Longowal-148106,
District: Sangrur, (Punjab), India

Abstract: In this study, a novel method is proposed for hiding crypto data in digital images using moderate significant bit substitution with multilayer security to the hidden data for secure communication. Firstly, secret data is encrypted using a flexible-matrix based symmetric key to add first layer of security. Then another layer of security is added by again encrypting the ciphered data using Magic Square method. The payload bit stream produced after double encryption is then embedded into cover image in the spatial domain at 4th LSB position using moderate significant bit substitution. The three lower bits as well as upper 5th bit of the image pixel is used to perform post pixel adjustment so as to achieve minimum visual distortion between original cover image and stego-image. In order to examine the effectiveness of the proposed method, image quality measuring parameters are estimated including Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), entropy, correlation, mean value and Universal Image Quality Index (UIQI). In this study, T-test is also applied for validation of the proposed method at 0.2% level of significance. From experimental results it is observed that the proposed method has an ability to provide higher security as well as robustness for preventing the attacks on the stego-image including intentional removal of Least Significant Bit (LSB). In fact, the results of this study are quite promising.

Key words: Magic square, pixel adjustment, moderate significant bit, flexible matrix, T-test

INTRODUCTION

The transmission of data from one place to another place with the use of multimedia and internet technologies is very easy. But at the same time, the security of the transmitted data is a challenging task. In order to ensure the security of the data transmission over the internet, data encryption (Menezes *et al*., 1997; Forouzan, 2008) and data hiding (Bender *et al*., 1996; Johnson *et al*., 2001; Karzenbeisser and Perircolas, 2000; Wu and Hwang, 2007; Wang *et al*., 2000; Chan and Cheng, 2001, 2004; Chan *et al*., 2004; Chang *et al*., 2002, 2003, 2004; Wang *et al*., 2001; Balkrishan and Singh, 2010; Singh and Balkrishan, 2010) are two widely used techniques. Data encryption is a technique that is used to protect the data from illicit access. It transforms secret data into cipher text that looks like a stream of meaningless code. However it does not assure security and robustness because the hacker can obviously guess that there is a confidential message communication between sender and receiver. Steganography is the scientific approach of inserting the secret data within a cover media (image, audio, video, data or other media to distract the attention of the observer) such that the unauthorized viewers do not get an idea of any hidden information (Bender *et al*., 1996; Johnson *et al*., 2001; Karzenbeisser and Perircolas, 2000; Wu *et al*., 2007). Steganography is an alternative to data encryption. In steganography, the secrete data is embedded into the carrier in such a way that only carrier is visible which is sent from transmitter to receiver without scrambling data. Steganography is used when data encryption is not permitted. The concept of multiple encryptions of the data is also reported to provide the other encryption method. However, neither data encryption nor steganography ensures total security to the data or information uniquely as a standalone application. In order to overcome this drawback, modern trend is to integrate these two techniques to achieve essential security (Wang *et al*., 2000; Chan and Cheng, 2001; Balkrishan and Singh, 2010; Singh and Balkrishan, 2010). From the literature survey it is observed that various data techniques have been used in the last decay to embed hidden messages in images. LSB substitution is the first and the simplest method. It replaces LSB of the image pixels with the bits of message. In this method, the pixels of the cover image are chosen either sequentially (Wang *et al*., 2000; Chan and

Corresponding Author: Balkrishan Jindal, Yadavindra College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi Saboo, Dist Bathinda-151302, Punjab, India

Cheng, 2001; Chang *et al*., 2002; Chan and Cheng, 2004) or randomly (Singh and Balkrishan, 2010). Although, embedding data in LSB introduces small distortion in the cover image, but major drawback of this method is that the embedded message can easily be destructed by the attacker through interchanging and/or replacing either zero or one at the respective least significant bit positions. In order to circumvent these problems, Wang *et al.* (2000) developed a method to embed the secret data in the Moderately Significant Bit (MSB) of the cover image. A genetic algorithm was used to find the optimal substitution matrix for each pixel. In addition to this, Local Pixel Adjustment Process (LPAP) was also applied to improve the image quality of the stego-image (Wang *et al*., 2000). However, the local pixel adjustment process considers only first three Least Significant Bits (LSBs). The weakness of the local pixel adjustment process (Wang *et al*., 2000) was also pointed out by another group of researchers (Chan and Cheng, 2001). In this method, look up table was used for pixel adjustment after data embedding at 4th LSB or 5th MSB. They improved the LPAP method which significantly reduces the computational cost and improves the visual quality of stego-image as compared with the method reported in Wang *et al.* (2000).

In this study, the present work reports on moderate-bit alteration technique for hiding data in a digital image without causing any appreciable distortion in the cover image with improved form of post pixel adjustment process. The proposed approach has two phases for post pixel adjustment. In the first phase lower three bits are considered for pixel adjustment while the second phase considers fifth bit. This scheme provides multilayer of security to the hidden data along with the better visual quality of the stego image. The two layer of security is provided by double encryption of secret message before its hiding. Firstly, secret data is encrypted using a flexible matrix based symmetric key to add first layer of security. Then encrypting the ciphered data using Magic Square method is added another layer of security. The third layer of security to the hidden data is achieved through the attainment of camouflage image. The experimental results are given to reveal the effectiveness of the proposed method. T-test is also applied for validation of the proposed method.

MATERIALS AND METHODS

In LSB substitution, the embedded secret data may be lost during post processing of stego image. To overcome this problem, the proposed method embeds crypto-data efficiently at the position of moderate significant bit of each pixel of the cover image with improved form of pixel adjustment. In the proposed approach, cryptography is integrated with steganography for secure communication. To provide additional layer of security, secret data is encrypted using flexible matrix proposed by the authors of the present study in their earlier work (Balkrishan and Singh, 2010) as shown in Table 1. Further encrypted data is again encrypted with proposed Magic Square method.

DATA ENCRYPTION METHODS

Flexible matrix: The proposed scheme uses a 16×16 size flexible matrix having entries ranging from 0 to 255 for encrypting data efficiently (Balkrishan and Singh, 2010). A modified form of the flexible matrix is again reproduced here with modified entries for the sake of illustration of the method explicitly. As an illustration, let data ABC is to be embedded in the cover image. First, data ABC is converted into ASCII equivalent. The ASCII value of each character's equivalent positions (row and column) is selected from the flexible matrix (Balkrishan and

Table 1: Pixel adjustment process after data embedding at 4th moderate significant bit

Column/row	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
1	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
2	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
3	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255
4	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
5	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
6	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
7	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
8	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
9	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
10	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
11	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
12	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
13	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
14	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
15	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95

Singh, 2010). Values of every position (row or column) are less than 16 and maximum 4 bits are required to represent the position. Then, values of each position are converted in to binary equivalent. Binary values of row and column are combining together to form an 8 bit encrypted character. All encrypted characters are obtained in 1-D array after using flexible matrix. The choice of flexible matrix to encrypt and decrypt the data provides additional layer of security.

Magic squares: In magic square method, A basic magic square of order n can be defined as an arrangement of numbers 1 to n^2 in an n x n matrix, such that each row, column and diagonal add up to the same number (Chang *et al*., 2009; Kaul and Singh, 2013; Adler's, 1996; Rouse-Ball, 1959). The magic sum, of each row, column and diagonal add up to can be found by the Equation:

$$\frac{1}{2}n\left(n^2+1\right)$$

Suppose, n is equal to 4. For n = 4, any instance of magic square is shown in Table 2. It is also called a diabolical magic square. In this magic square, sum is always 34 i.e., the sum of the four corners or the sum of any quadrant of the square or the sum of four nearest to the center is always 34. Such sum is obtained in 86 different ways. Thus data can be encrypted with 86 different ways. Each entry in magic square can be replaced by its square or cube. The ciphered data is obtained using Table 2. For obtaining the ciphered data from Magic Square Table (MST), 1-D array Y is taken. The Size of Y is [1, No. of rows of MST×No. of column of MST]. For given example, the size of Y is (Adler's, 1996; Menezes *et al*., 1997). The value at kth index of Y is obtained shown in Table 3 as follows:

- Find ith row and jth column from MST where k is located in MST. Values of every position (row or column) are less than 4 and maximum 2 bits are required to represent the position
- Convert I and j into two bit binary numbers i.e., Bi and Bj. Binary values of row and column are combining together to form an 4-bit ciphered data as shown in Table 3
- Y [1,k] = Combination of Bi Bj

Table 2: Look up table for magic square

Column/row	0	1	2	3
0	16	3	2	13
1	5	10	11	8
2	9	6	7	12
3	4	15	14	1

ILLUSTRATION

In order to understand the encryption process, consider an example illustrating the process of encryption of data using flexible matrix (Balkrishan and Singh, 2010) in combination with Magic square Method. In order to do so, assume the following inputs:

Message character, a = 97 = 0 1 1 0 0 0 0 1

As shown in the Flexible Matrix of Table 3, the row column numbers corresponding to location 97 are 10 and 1, respectively. The encrypted data 10 and 1 obtained in this manner is further ciphered using Magic square method of Table 2 thus, leading to 5, 15. The binary equivalent of (5, 15) is (0 1 0 1 1 1 1 1) with 5 being the upper byte and 15 being the lower byte, i.e., (5, 15) = (0 1 0 1 1 1 1 1).

DATA EMBEDDING AND PIXEL ADJUSTMENT

In the proposed method, important data bits are embedded into the moderate significant bit position of pixel of the cover image. One bit of ciphered message is substituted with 4th LSB of pixel of cover image. To lower the degradation of the image quality, first post pixel adjustment at lower bits of the pixel is used to increase the visual quality of stego image. Let Z (i, j) be the pixel of cover image. If secret data bit is equal to the 4th LSB, then no pixel adjustment is required. If secret data bit is not equal to the 4th LSB, then modify the pixel by Z (i, 1-3) = 0 or 1 depends upon the hiding of ciphered data bit. Further, for improving the visual quality of the stego image 2nd post pixel adjustment at 5th upper bit of the pixel is also performed. Figure 1 shows the process of proposed data encryption and data embedding method. Figure 2 shows the 1st and 2nd post pixel adjustment of bits of pixel of the cover image after embedding the data bit at 4th MSB. The advantages of the proposed method are (a) Attacks on stego-image are very less. (2) The quality of the cover image is not affected appreciably. The procedure used for first post pixel adjustment and 2nd post pixel adjustment process of the selected pixel is summarized below.

First post pixel adjustment: If the embedded crypto-data bit is equal to the 4th LSB of the image pixel, then no pixel-adjustment is required and go to the next pixel. However, if crypto-bit to be embedded is not equal to 4th LSB, pixel adjustment is performed involving first three LSBs. The underlying logic for the same is detailed below:

- If the embedded crypto-data bit is one as well as not equal to the 4th LSB of the image-pixel, then modify the pixel by making first three LSBs equal to zero, i.e., Z (i, 1 to 3) = 0

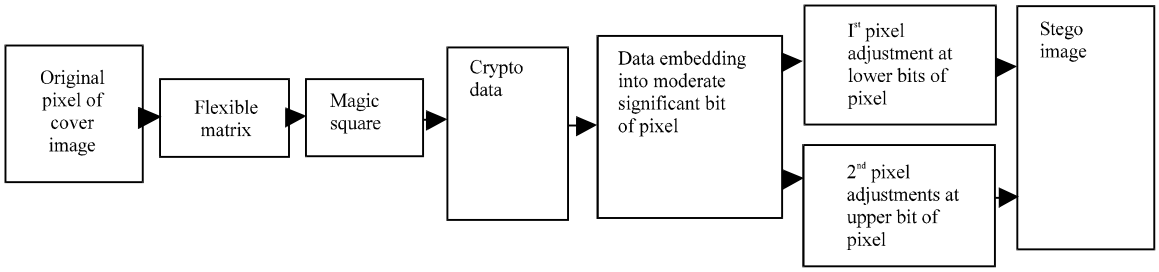

Fig. 1: Proposed data encryption and data embedding method

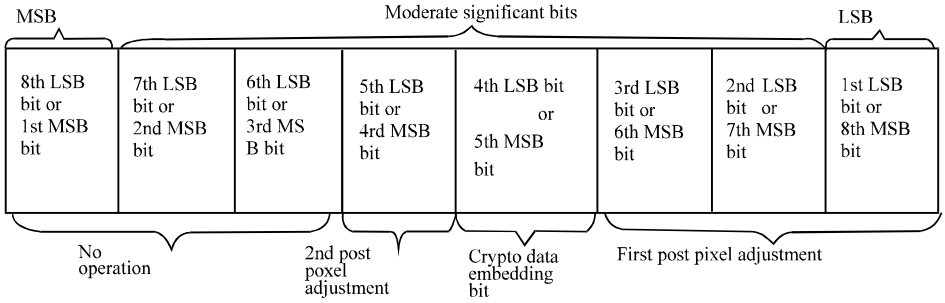

Fig. 2: Shows the 1st and 2nd post pixel adjustment of bits of pixel of the cover image after embedding the data bit at 4th MSB

Table 3: Ciphered data obtained from MST

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Ciphered data = Y[1,k]	15	2	1	12	4	9	10	7	8	5	6	11	3	14	13	0

- If the embedded crypto-data bit is zero as well as not equal to the 4th LSB of the image-pixel, then modify the pixel by making first three LSBs equal to 1, i.e., Z (i, 1-3) = 1

2nd post pixel adjustment: In this section, 2nd post pixel adjustment process is proposed to enhance the visual quality of stego image obtained by embedding the crypto data bit into the moderate significant bit (4th LSB) substitution method. Let P, P' and P" be the corresponding pixel values of the ith pixel in the cover-image, the stego-image obtained by the proposed method and the modified stego-image obtained after the 2nd post pixel adjustment. Following are the steps of 2nd post pixel adjustment:

Step 1: If 5th and 4th LSBs are equal after embedding crypto-bit, then perform 2nd post pixel adjustment using the following steps:

- After embedding the crypto data bit into 4th LSB of the pixel, calculate the error (D1) between modified pixel and original pixel. D1 = abs (P-P'). If D1>4, then complement the 5th LSB bit and Z (i, 1 to 3) bits, otherwise no need for optimal pixel adjustment, i. e., P' replaced with P". If D1<4, then no need for 2nd post pixel adjustment after embedding the crypto data bit and go to next pixel for embedding next crypto-data bit

Moreover, 2nd post pixel adjustment process only requires error (D1) between the original cover-image and the stego-image obtained by embedding the crypto data bit into the moderate significant bit (4th LSB) substitution method. If the error value is greater than 4 (D1>4), 2nd post pixel re-adjustment is used to modify the pixel of stego image. The value of D1>4 is chosen in such a way that it gives better visual quality as compared to its other values including D = 1, 2, 3, 5, 6, 7 or 8.

The above mentioned procedure is also illustrated in Table 4 by assuming hypothetical data in the image pixel. The complete data hiding procedure is illustrated in Fig. 1. In fact, the proposed method provides three layers of security to protect the hidden data. In the first instance, cryptography technique is used to protect the information. Then another layer of security is added to the secret data by encrypting the ciphered data using Magic square method. The ciphered data produced after double encryption is then embedded in the cover image in an attempt to achieve camouflage.

Table 4: Pixel adjustment process after data embedding at 4th moderate significant bit

Original pixel			Stego-pixel		Stego-pixel after first pixel adjustment			Stego-pixel after 2nd pixel adjustment	
Bit details	Value (p)	Message bit	Bit details	Value	Bit details	Value (P')	D = p-p'	Bit details	Value (P")
1 0 1 0 0 1 0 0	164	0	1 0 1 0 0 1 0 0	164	Not Applicable	-	0	Not applicable	-
1 0 1 0 1 1 1 0	174	1	1 0 1 0 1 1 1 0	174	Not Applicable	-	0	Not applicable	-
0 0 1 1 1 0 0 1	57	0	0 0 1 1 0 0 0 1	49	0 0 0 1 0 1 1 1	55	2	Not applicable	-
1 0 1 0 0 1 0 0	164	1	1 0 1 0 1 1 0 0	172	1 0 1 0 1 0 0 0	168	4	Not applicable	-
0 1 1 0 1 1 1 1	111	0	0 1 1 0 0 1 1 1	103	0 1 1 0 0 1 1 1	103	8	0 1 1 1 0 0 0 0	112
0 0 1 1 0 0 1 0	50	1	0 0 1 1 1 0 1 0	58	0 0 1 1 1 0 0 0	56	7	0 0 1 0 1 1 1 1	47

PROPOSED ALGORITHM

Message ciphering and embedding module:

- **Step 1:** Commencing with first character, read secret message character-wise from saved text file
- **Step 2:** Encrypt each character into row number and column number using Flexible Matrix
- **Step 3:** Repeat step 2 for all characters of the saved text file to obtain row number and column number i.e., A(Row number, Column number), where A is a flexible matrix
- **Step 4:** Combine all the row numbers and column numbers into 1-D array
- **Step 5:** Commencing with first number, read the data from 1-D array
- **Step 6:** Apply magic square on 1-D array and compute k (i, j), i.e., ith row and jth column, for every value of 1-D array using Table 1
- **Step 7:** Combine the row number and column number obtained from Table 1, for 1-D array, data and get a ciphered data as shown in Table 2 equivalent to 1-D array element k
- **Step 8:** Repeat steps 6 to 7 for ciphering all the elements of 1-D array. Save the ciphered data into another 1-D array
- **Step 9:** Convert the 1-D array into equivalent binary bitstream
- **Step 10:** Read each pixel of the cover image commencing with first pixel Z(i, j) where i and j = 1: 256
- **Step 11:** Convert each pixel into equivalent eight-bit binary number
- **Step 12:** Embed one cipher-data-bit of message into the 4th LSB of pixel of cover image and go to next pixel
- **Step 13:** Repeat step 11 to 13 until all the cipher message bits are embedded into the cover image
- **Step 14:** Use the first post pixel adjustment process or first post pixel adjustment process with 2nd post pixel adjustment process to improve the visual quality of the stego image

Message extraction and decrypting module:

- **Step 1:** Read the pixel of the stego-image starting from first pixel
- **Step 2:** Convert each pixel value into equivalent binary number
- **Step 3:** Extract crypto-bit from 4th LSB of pixel of the stego image commencing with first pixel Z (i, j) where i = 1: 256 and j = 1: 256
- **Step 4:** Go to next pixel and repeat steps from 2 to 3
- **Step 5:** Repeat steps 2 to 4 until all the crypto-bits of the secret message are extracted
- **Step 6:** Convert every four bits into equivalent decimal number and store into 1-D array
- **Step 7:** All values in 1-D array are replaced with original numbers (k) using Table 2 and stored into 1-D array
- **Step 8:** The decrypted 1-D array divided into two equal parts, first part taken as a row numbers and second part taken as a column numbers for decrypting the data using flexible matrix
- **Step 9:** First number form the row and first number form the column for reading the decimal value from the selected flexible matrix i.e., A (Row, Column), where A is a flexible matrix
- **Step 10:** Convert all decimal values into characters and the characters are then combined together to form the secret message which are saved into text file

VALIDATION OF THE PROPOSED METHOD USING T-TEST

The difference between mean gray level values of Cover Image and Stego Image obtained with the proposed method shown in Table 5.

Null hypothesis:

- H_0: The difference between mean gray level values of original Cover Image and Stego Image is not significant i.e., Mean gray level values of both images are equal
- H_1: The difference between mean gray level values of original Cover Image and Stego Image is significant i.e., Mean gray level values of both images are not equal

Table 5: Observation table for Lena cover image with and without post pixel adjustment process

		Stego image without post pixel adjustment			Stego image with first and 2nd post pixel adjustment		
No. of pixels for block of image	Mean of original image X block-wise	Mean of stego image Y block-wise without post pixel adjustment	d = Y-X	d^2	Mean of stego image block-wise with post pixel adjustment	d = Y-X	d^2
1-6553	128.4758	130.4523	1.9765	3.9065	129.6035	1.1277	1.2718
6554-12106	102.5323	103.6128	1.0806	1.1676	103.2255	0.6933	0.4806
12107-19659	102.7516	103.9448	1.1932	1.4237	103.372	0.6205	0.3850
19660-26212	99.5222	101.0304	1.5082	2.2746	100.3766	0.8544	0.7300
26213-32765	121.1346	121.0745	-0.0601	0.0036	121.1239	-0.0107	0.0001
32766-39318	151.4633	153.2049	1.7416	3.0333	152.2875	0.8242	0.6793
39319-45871	145.5338	124.2489	0.4166	0.1736	145.673	0.1392	0.0194
45872-52424	125.3163	126.2468	0.9304	0.8657	125.4296	0.1132	0.0128
52425-58977	130.4018	132.2516	1.8498	3.4219	131.0169	0.6151	0.33784
58978-65530	133.8218	134.1857	0.3640	0.1325	133.7778	-0.0439	0.0019
			Sum of d = 11.0008	Sum = 16.4030		Sum = 4.9330	Sum =3.9594
n = 10			Mean of d = 1.10001			Mean of d = 0.4933	

$$S = \frac{\sqrt{\sum d^2 - n(d)^2}}{\sqrt{n-1}} \quad (1)$$

Where $\bar{d}$ is the mean of the differences between mean gray level values of cover image and stego image and S is the standard deviation of the differences between mean gray level values of cover image and stego image. t is based on n-1 degree of freedom. Table value of t (Degree of freedom 9) for 0.2% = 4.297. For stego image obtained after without post pixel adjustment, S is 0.6913 using Eq. 1 and t is 5.0320 using Eq. 2. Hence, the calculated value of t is:

$$t = \bar{d} * \frac{\sqrt{n}}{s} \quad (2)$$

5.0320 that is greater than table value of t = 4.297 at 0. 2% level of significant. Thus it is concluded that the difference between mean gray values of cover image and stego image is significant. Hence, H_0 (Null hypothesis) is rejected and H_1 is accepted for stego images obtained with without pixel adjustment.

For stego image obtained with the proposed method S = 0.4118 using Eq. 1, t = 3.7885 using Eq. 2, since calculated values of t = 3.7885 which is less than table value = 4.297 at 0. 2% level of significant. Hence it may be conclude that the difference between means is not significant. Thus H_0 (Null hypothesis) is accepted and H_1 is rejected. From this we conclude that difference between mean of values of original cover image and stego image is significant. Hence it is concluded that mean of gray level values of cover images and stego images obtained with the proposed method is approximately equal and visual quality of stego image is good.

RESULTS AND DISCUSSION

In this section, experimental results are presented and discussed of the proposed method. Four gray-scale images (Goldhill, Mandril, Lena and Jet) with size 256×256 are used in the experiments as cover images shown in Fig. 3a. Simulation results are performed by hiding 8192 bytes (65536 bits) of secret message into the cover images (one bit per pixel) in MATLAB software. The results of simulation study are included in Fig. 3b without pixel adjustment, Fig. 3c with first post pixel adjustment and Fig. 3d with first and 2nd post pixel adjustment (proposed method). As the results, there are not any visual artifacts present. It means that such distortions will be less noticeable because changes are small. After completing the simulation study. Image Quality Measuring (IQM) parameters including Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), entropy, correlation, mean value and Universal Image Quality Index (UIQI) are recorded and summarized in Table 6-8 (Gonzalez and Woods, 2008; Wang and Bovik, 2002). Experimental results have shown that the proposed method not only has an acceptable image quality but also achieved reasonably good values of IQM parameters. The PSNR of the four cover images in Fig. 3d are 38.9779, 39.0124, 38.9344 and 38.8432, respectively better than 38.75 for Lena image reported in Wang *et al*. (2000). The extra computational cost is very small as compared to the method reported in the work (Wang *et al*., 2000, 2001) which requires huge computations for the genetic algorithm and an optimal substitution matrix.

The histogram analysis is performed on both cover image and stego image shown in Fig. 4. The stego image Fig. 4b, c, d shows minimum changes in the histogram compared to the cover image histogram Fig. 4a. From these minimum changes in the histogram of the stego image it is difficult to infer that secret data is hidden.

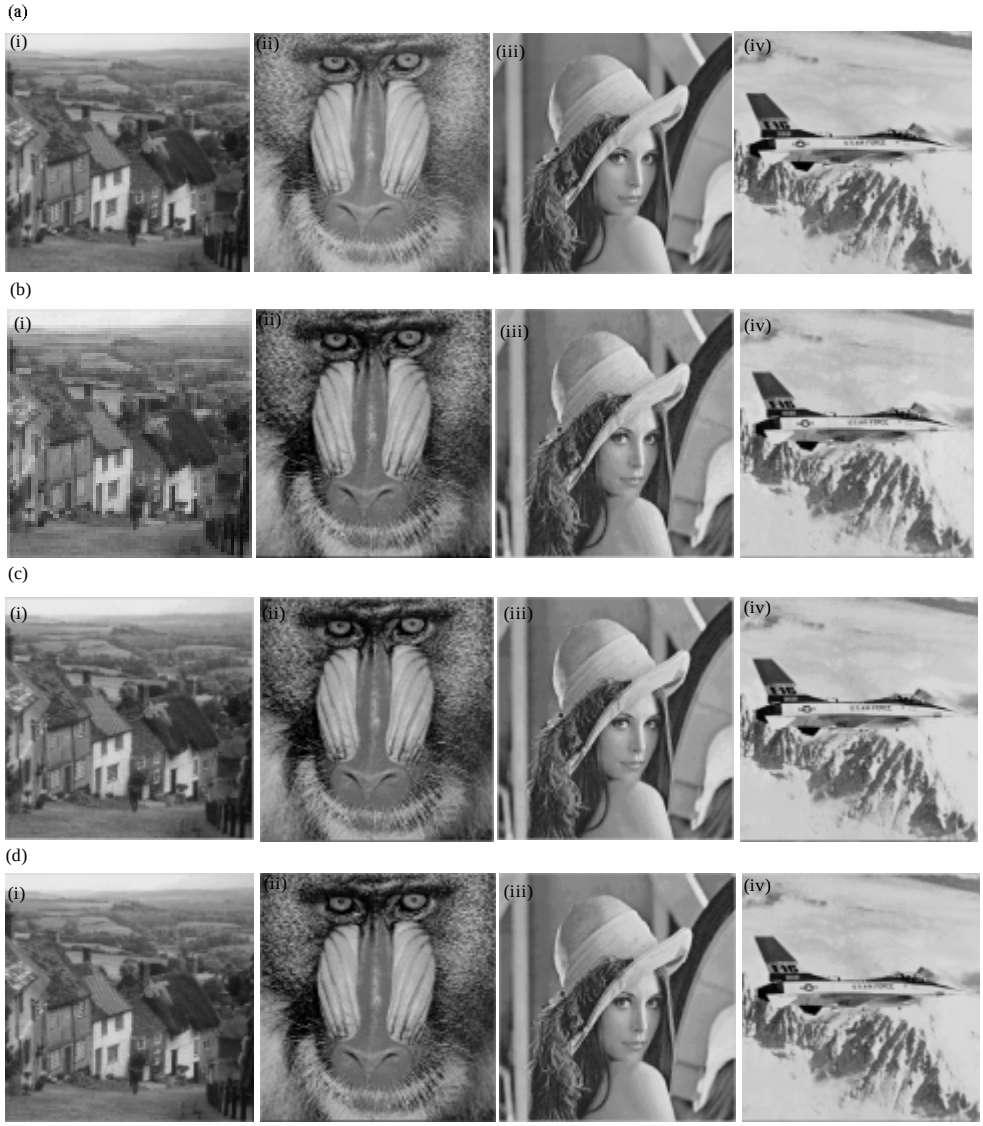

Fig. 3(a-d): Cover and stego-images obtained by proposed method (a) Original cover images (i) Golhill, (ii) Mandrill, (iii) Lena, (iv) Jet (b) Stego-images obtained without post pixel adjustment process, (c) Stego-images obtained after first post pixel adjustment process and (d) Stego-images obtained after 2nd post pixel adjustment process

Moreover it is again clear that the histograms of cover and stego images did not release any identifiable visual difference. Steganalysis is performed in terms of security analysis using the concept of histogram comparison. Statistical analysis is also performed on proposed stego image. Statistical parameters like mean values are calculated from the image before and after embedding of secret message tabulated in Table 7. The universal image quality index (Q) is used to measure the quality of the stego image tabulated in Table 7. This UIQI is based on statistical measurements and it's dynamic range is [-1, 1]. From Table 5 it is concluded that the differences between mean gray level values of original Cover Image and Stego Image obtained after first and 2nd post pixel adjustment of pixels of stego image is small as compared to the differences between mean gray level values of original Cover Image and Stego Image obtained after without pixel adjustment of pixels of stego image. Due to page constraints, T-test is performed on Lena cover image only. Similarly, T-test can be performed on

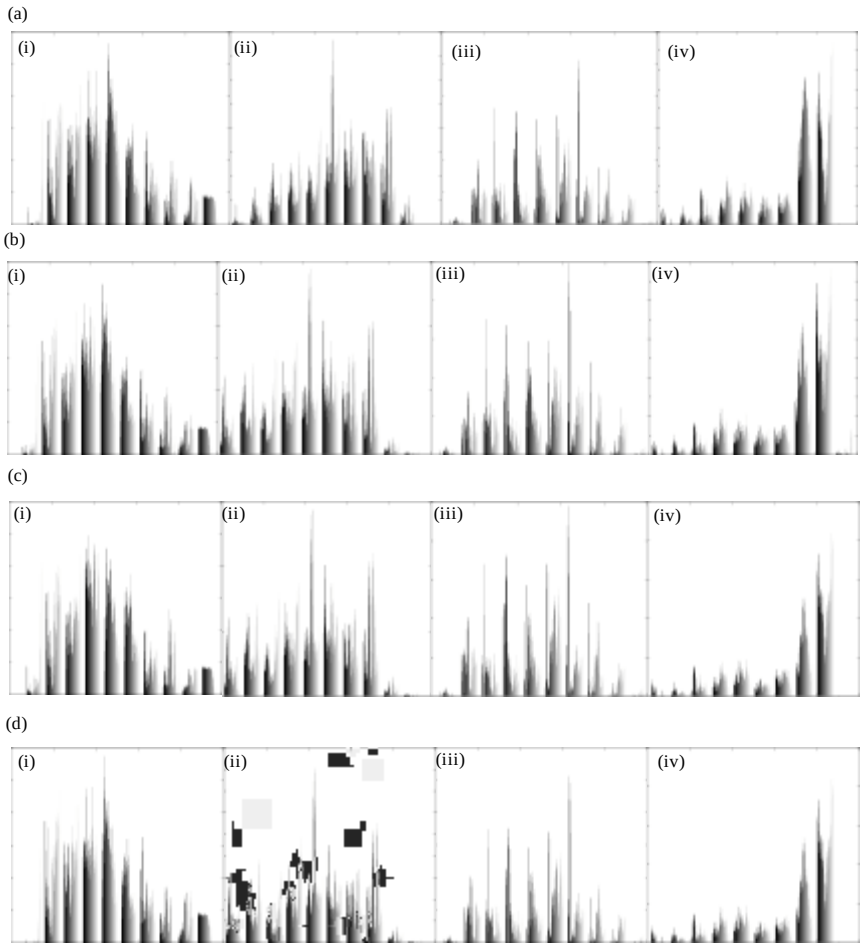

Fig. 4(a-d): Histogram of cover and Stego images obtained by proposed (a) Histogram of original cover image, (i) Goldhil (ii) Mandrill (iii) Lena and (iv) Jet (b) Histogram of stego images obtained without post pixel adjustment process, (c) Histogram of stego images obtained after first post pixel adjustment process and (d) Histogram of stego images obtained after 2nd post pixel adjustment process

Table 6: Peak signal-to-noise ratio and mean squared error resulted after hiding 8192 crypto-data bytes using proposed methods

	PSNR			MSE		
Test image (256×256)	Without pixel adjustment	With first post pixel adjustment	With First and 2nd post pixel adjustment (proposed method)	Without pixel adjustment	With first post pixel adjustment	With first and 2nd post pixel adjustment (proposed method)
Lena	33.0545	36.9136	38.9344	32.1836	13.2348	8.3108
Jet	32.8365	37.0744	38.8432	33.8398	12.7537	8.4871
Baboon	33.0897	37.1328	39.0124	31.9238	12.5835	8.228
Goldhill	33.0859	37.1605	38.9779	31.9512	12.5033	8.1628

Table 7: Entropy and correlation resulted after hiding 8192 crypto-data bytes using proposed method

	Entropy			Correlation		
Test image (256×256)	Without pixel adjustment	With first post pixel adjustment	With First and 2nd post pixel adjustment (proposed method)	Without pixel adjustment	With first post pixel adjustment	With First and 2nd post pixel adjustment (proposed method)
Lena	5.0855	4.5271	4.6395	0.9938	0.9974	0.9982
Jet	4.6038	3.952	4.0954	0.9937	0.9975	0.9982
Baboon	5.1258	4.5834	4.56924	0.9941	0.9976	0.9984
Goldhill	5.0941	4.5214	4.631	0.9942	0.9976	0.9983

Table 8: Mean value and universal image quality index resulted after hiding 8192 crypto-data bytes using proposed method

		Mean value			Universal image quality index		
Test image (256×256)	Original image	Without pixel adjustment	With first post pixel adjustment	With first and 2nd post pixel adjustment (proposed method)	Without pixel adjustment	With first post pixel adjustment	With first and 2nd post pixel adjustment (proposed method)
Lena	124.0923	125.9378	125.1564	124.5561	0.7934	0.8742	0.9032
Jet	170.6822	172.9803	171.8288	171.3068	0.7054	0.8366	0.8712
Baboon	102.7616	104.6449	103.8195	103.3353	0.9558	0.9802	0.9856
Goldhill	112.0349	113.9097	113.057	112.5317	0.8913	0.9437	0.9559

all other cover and stego images. Experimental results show the effectiveness of the proposed algorithm.

The experimental results thus reveal that: (a) Histogram of the stego image looks alike to that of the histogram of original image, (b) Statistical parameter values of the cover image are merely equal to the stego-image, (c) The achievement of good values of IQM parameters and T-test validates that stego-images obtained with proposed method have maintained excellent visual quality.

CONCLUSION

In this study, an attempt is made to overcome the problem of post-processing of stego-image obtained with simple LSB substitution method. In the proposed method, we integrate cryptography with steganography to achieve essential security for the secret data. The proposed method embeds crypto-data efficiently at the position of moderate significant bit of each pixel of the cover image and provides three layers of security to the hidden data. The proposed method significantly improves the visual quality of stego images as compared with first post pixel adjustment process, without post pixel adjustment process of the stego image and the method reported in Wang *et al*. (2000). T-test validate the proposed method the proposed method as compared with the without post pixel adjustment. Hence, pixels of cover image and stego image are merely equal. For data extraction, the original cover image as well as no other extra information is required for data extraction. In addition to this, the hidden data can be extracted correctly without any error as quantization error from the stego-image, even if its LSB is removed intentionally or unintentionally. The proposed method provides a higher security as well as robustness to the attacks on stego image as compared to simple LSB substitution method. Extensive experimentation proves the effectiveness of the proposed method. Experimental results show that the stego image is visually indistinguishable from the original cover image with acceptable image quality.

REFERENCES

Adler's, A., 1996. What is a magic square? http://mathforum.org /alejandre/magic.square /adler/ adler.whatsquare.html

Balkrishan and A.P. Singh, 2010. Hiding encrypted data using randomly chosen moderate bit insertion in digital image steganography. J. Comput. Sci. Eng., 1: 21-27.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.

Chan, C.K. and L.M. Cheng, 2001. Improved hiding data in images by optimal moderately significant-bit replacement. Electron. Lett., 37: 1017-1018.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. Pattern Recognit., 37: 469-474.

Chan, C.K., L.M. Cheng, K.C. Leung and S.L. Li, 2004. Image hiding based on block difference. Proceedings of the International Conference on Control Automation, Robotics and Vision, December 6-9, 2004, Kunming, China, pp: 968-972.

Chang, C.C., M.H. Lin and Y.C. Hu, 2002. A fast and secure image hiding scheme based on LSB substitution. Int. J. Pattern Recogn. Artif. Intell., 16: 399-416.

Chang, C.C., J.Y. Hsiao and C.S. Chan, 2003. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. Pattern Recogn., 36: 1583-1595.

Chang, C.C., G.M. Chen and M.H. Lin, 2004. Information hiding based on search-order coding for VQ indices. Pattern Recognit. Lett., 25: 1253-1261.

Chang, C.C., K.T. Duc, Z.H. Wang and M.C. Li, 2009. An image authentication scheme using magic square. Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology, August 8-11, 2009, Beijing, China, pp: 1-4.

Forouzan, B.A., 2008. Cryptography and Network Security. 4th Edn., McGraw-Hill Higher Education, USA.

Gonzalez, R.C. and R.E. Woods, 2008. Digital Image Processing. 3rd Edn., Pearson Education, India.

Johnson, N.F., Z. Duric and S. Jajodia, 2001. Information Hiding: Steganography and Watermarking Attacks and Countermeasures. Kluwer Academic Publishers, USA.

Karzenbeisser, S. and F.A. Perircolas, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, UK., ISBN: 9781580530354, Pages: 220.

Kaul, B.L. and R. Singh, 2013. Generalization of magic square (numerical logic) 3×3 and its multiples (3×3) × (3×3). Int. J. Intell. Syst. Appl., 1: 90-97.

Menezes, A.J., P.C. van Oorschot and S.A. Vanstone, 1997. Handbook of Applied Cryptography. CRC Press, New York, USA.

Rouse-Ball, W.W., 1959. Mathematical Recreations and Essays. Macmillan and Co. Ltd., London, UK.

Singh, A.P. and Balkrishan, 2010. Secure data communication using moderate bit substitution for data hiding with three layer security. J. ET, 91: 45-50.

Wang, R.Z., C.F. Lin and J.C. Lin, 2000. Hiding data in images by optimal moderately significant-bit replacement. IEE Electron. Lett., 36: 2069-2070.

Wang, R.Z., C.F. Lin and J.C. Lin, 2001. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recogn., 34: 671-683.

Wang, Z. and A.C. Bovik, 2002. A universal image quality index. IEEE Sig. Process. Lett., 9: 81-84.

Wu, N.I. and M.S. Hwang, 2007. Data hiding: Current status and key issues. Int. J. Network Sec., 4: 1-9.