Enhanced Bandwidth Utilization in Image Steganography with Enhanced Data Security

Balkrishan
Department of CE, Yadavindra College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi Sabo-151302
District: Bathinda Punjab, India

Amar Partap Singh
Department of ECE, Sant Longowal Institute of Engineering and Technology,Longowal-148106
District: Sangrur, Punjab, India

ABSTRACT
In this paper, a new method is proposed for image steganography that involves double encryption as well as compression of a message followed by its subsequent hiding in a digital image. In the first instance, original data is encrypted using flexible matrix. Further, encrypted data is encrypted and compressed using Chinese Remainder Theorem (CRT) for extra layer of security and increased the data hiding capacity. The proposed method enhances bandwidth utilization besides ensuring three layered security to the message. The underlying principle of this method involves decomposition of each image-pixel into two blocks. One block is called Parity Reflecting Block (PRB) whereas other is known as Pixel Adjustment Block (PAB). The information about hidden bit is reflected by parity condition in the Parity Reflecting Block. The Pixel Adjustment Block is used to perform local pixel adjustment in order to reduce the degradation effect in the cover image produced as a result of alteration in the moderate bit. The performance of the proposed algorithm is evaluated in terms of Image Quality Measures (IQM) including Mean Square Error (MSE), Peak-Signal-to-Noise Ratio (PSNR), Entropy, Correlation, Mean Value and Standard Deviation. Security analysis is also carried by comparing the histograms of the cover and stego-images. The results of this study are quite promising.

General Terms
Information Security

Keywords
Data Hiding, Chinese Remainder Theorem, Crypto-Compressed-Data, Flexible Matrix, Parity

1. INTRODUCTION
Data encryption [1-4] & compression [2-4] are pivotal for proper storage and transmission of data. The rapid growth in the internet coupled with high bandwidth requirement has propelled the explosive growth of information communication. This type of advancement in the field of data communication has hiked the fear of getting the data snooped at the time of sending it from sender to the receiver. So, information security has already become an important part of data communication. In order to address this issue of information security, data-encryption as well as its hiding [5-16] plays an important role. Data hiding conceals the existence of secret message while cryptography protects its contents. The word steganography is derived from the Greek words- stegos meaning roof or cover and graphia meaning writing, i.e., it is an art of hiding information in such a way that communication takes place without any failure [5-7]. The objective of modern steganography is to keep the payload (embedded information) undetected, but the steganographic systems, because of their invasive nature, may leave behind somewhat traces in the cover image [8]. Steganography techniques use different carriers (cover medium in digital format) to hide data. These carriers may be network packets, floppy disk, hard drive, amateur radio waves [9] or general computer files such as text, image, audio, video, etc. [5, 9-12]. Data hiding capacity & invisibility are the two important parameters used to evaluate the effectiveness of the data hiding technique [14]. In [5] crypto data was embedded into the moderate significant bit of pixel of the cover image by parity condition of bits. The weakness of this method is that author used only lower bits for pixel adjustment and not used the upper bits for re-adjustment of the pixels of the stego image.

The simultaneous data encryption and compression technique is an attempt to provide a solution for optimal bandwidth utilization, space required for data storage and the encryption problems at the same time [2]. Number theory based data encryption and compression is an algorithm that employs Chinese Remainder Theorem (CRT) in order to generate and solve congruencies. However, several methods are available for data or image compression including JPEG-LS, SPIHT, JPEG2000, CALIC, etc. These are standards that use some kind of transform including Discrete Fourier Transformation (DFT), Discrete Cosine Transformation (DCT) & Discrete Wavelet Transformation (DWT) [3]. There are two main drawbacks of traditional transformation based compression methods: (a) In transform techniques, data is transformed from one domain to another, (b) Moreover, these techniques do not encrypt and compress image and/or data in single step [4]. However, such problems of traditional methods of compression are addressed in the proposed approach in which only basic mathematical operations are employed instead of transformation of the data. It also ensures encryption and compression of data in a single step.

Therefore, in the present work, a new type of image steganography is described that combines three operations- cryptography, data compression and steganography in a simultaneous manner. In the first instance, the message is encrypted using flexible matrix [15] serving the purpose of a new type of symmetric key. The data byte is assigned a row number and column number from the flexible matrix itself. All row and column numbers are combined to form one dimensional (1-D) array. This process implements first layer of security to the data. It provides 256 combinations for data byte instead of single combination (remainder and quotients) when data byte is divided by 16 in the CRT. After this, enciphered data is again encrypted as well as compressed using Chinese Remainder Theorem (CRT). In addition to this, it also provides an additional layer of security to the original message and also increases the data hiding capacity of the cover image by compressing the secret data. At the end, crypto-compressed-data is embedded into the pixel of cover image using moderate-bit substitution thus providing third layer of security in the form of camouflage. Moderate bit substitution is achieved in such a way that no appreciable distortion is observed in the cover image. To improve the image quality further, a pixel adjustment process is also applied at each pixel of the cover image where alteration has occurred due to moderate significant bit substitution. This is done by slight adjustment of other bits in the image pixel without any damage to the secret data. To evaluate the visual quality of stego-image, Image Quality Measures (IQM) are evaluated including Mean Square Error (MSE), Peak-Signal-to-Noise Ratio (PSNR), Entropy, Correlation, Mean Value and Standard Deviation [17]. The proposed method is applied on different standard test-images of size 256×256 serving the purpose of good cover. Extensive experimental results proved that the hidden data remains invisible and there is no appreciable visual distortion in the image at all.

2. CHINESE REMAINDER THEOREM

The Chinese Remainder Theorem (CRT) is a good application of number theory to other fields. It is based on the algorithm of linear and modular congruencies. Congruence is nothing more than a statement about divisibility [4]. The Chinese Remainder Theorem is mainly based on the system of linear congruencies

$a = b(mod\ n)$which can be reduced to a set of $a = b(mod\ n_i)$, where$n_1, n_2 \dots n_k$ are prime factors of n.

(a) Theorem

Let $n_1, n_2 \dots n_k$ denote k positive integers which are relatively prime numbers, and let $a_1, a_2 \dots a_k$ denote any k integers. Then the congruencies $X = mod(a_i, n_i)$, where i = 1, 2,…., k have common solutions. Any two solutions are congruent Modulo $n_1, n_2 \dots n_k$.

$Y = X(mod\ P)\ Where\ P = n_1 * n_2 * \dots n_k$ (1)

$X = \big((a_1 * N_1 * x_1) + \cdots + (a_k * N_k * k)\big)(mod\ P)$

$i.e.\ \ X = \sum(a_i * N_i * x_i)\ \ (mod\ P)$ (2)

$Where,\ N_k = \frac{P}{n_k}\quad in\ which\ x_k\ satisfied$

$N_i * x_i = 1(mod\ n_i)$ (3)

The remainder of the solved congruencies X is transmitted. At the receiving end, a_i are found using $a_i = X(mod\ n_i)$ and the original data is reconstructed by row number and column number of flexible matrix.

(b) Numerical Example of data encryption and compression using CRT

$Let\ n_1 = 17, n_2 = 18, n_3 = 19\ \&\ n_4 = 23$
$which\ are\ relatively\ prime$
$Let\ a_1 = 10, a_2 = 14, a_3 = 9\ \&\ a_4 = 8$

Encryption:

$$P = 133722$$
$$N_1 = 7866, N_2 = 7429, N_3 = 7038\ \&\ N_4 = 5814$$
$$x_1 = 10, x_2 = 7, x_3 = 12\ \&\ x_4 = 9, X = 18914$$

Decryption:

$a_i = mod(X, n_i)$ (4)

$$a_1 = 10, a_2 = 14, a_3 = 9, a_4 = 8$$

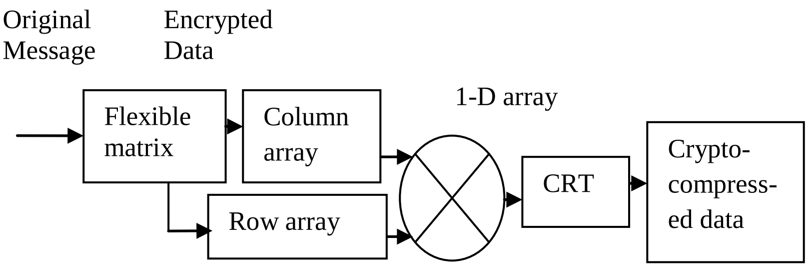


Fig.1 Proposed Method for Data Encryption and Compression

3. PROPOSED METHOD

The secret data is first encrypted using flexible matrix proposed by the authors of the present paper in their earlier work [15]. This matrix is reproduced in Table-1 with new entries for the sake of illustration [15]. The enciphered data is further re-encrypted & then compressed using CRT. The complete process is illustrated in Fig.1. The number theory based technique is applicable for encryption application by suitable selection of relatively prime numbers (n_i). Data compression depends on the block size used in CRT.

Relative prime numbers are chosen in such a way that these are larger than any value in one dimensional (1-D) array. During decoding**,** the same combination of n_i, that are selected for encoding should be applied correctly. To achieve safe transfer of data and obtain better results of embedding, moderate-bit substitution method is proposed in the present work for hiding crypto-compressed-data in a digital image. In this paper**,** for compression purpose**,** the block size (1×K) with K = 4 is taken. Depending on the amount of compression requirement, a large block size can also be considered.

3.1 Data Encryption and Compression using CRT

Consider a data of n characters and assign the row number and column number of n characters using flexible matrix [15]. The Row number and column number are combined to form 1- D array. Pad the 1-D array with zeros to make a block size of 10 or 8 or 4. Now, 1-D array is solved using the Chinese Remainder Theorem for block of 4. In equation (2) Ni and xi are pre-calculated as coefficients and these values need not be calculated for every X. All ai (i = 1, …, m, where m is the elements in 1-D array) are the 1-D array values after encryption using flexible matrix. The reason for using Chinese Remainder Theorem for solving the linear congruencies is to reduce a bigger number to a smaller representation. For data of size 1×3000 bytes and block size 4, all 1500 or less X are computed. After computing all X, the frequency of each distinct X and their counts are determined. All X are sorted in descending order of their count. A table of unique X and an equivalent smaller code is generated. Using this table, each X obtained is encoded into this smaller code. Data compression ratio was 1.35 for 3000 bytes. For the sake of clarification, the complete process is illustrated here.

3.2 Data Decryption and Decompression

Data decoding is performed at the receiving end. At the receiver, Ai is found for each X using the equation (4). Single 1-D array of all Ai is divided into two equal size arrays (Row number & Column number).The original pixel values are then reconstructed using the flexible matrix.

3.3 Illustration

Original message to be embedded	Image steganography
Data byte/ASCII value of character	105 109 97 103 101 32 115 116 101 103 97 110 111 103 114 97 112 104 121
Encrypt the message using flexible matrix	Column array = 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 10 9 10 Row array = 8 9 1 6 4 0 13 14 4 6 1 10 11 6 12 1 6 7 7
Combine the column and row array to get a 1-D array and pad with zeros such that total values in 1-D arrays divided by 4	1-D array = 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 10 9 10 8 9 1 6 4 0 13 14 4 6 1 10 11 6 12 1 6 7 7 0 0
Further encrypt and compress crypto data using Chinese Remainder Theorem	Calculate the values of X and assign the smaller code to each X
Data embedding into cover image to obtain stego-image	Data embedding at Moderate Significant Bit position

3.4 Crypto-compressed-data hiding

To understand the process of crypto-compressed-data hiding, it is assumed that a cover image is composed of pixels with odd or even number of one's. In the pixel of cover image, bit is altered at moderate position depending upon the parity condition of the bits counted from moderate position to the most significant bit (MSB). All the lower bits from moderate position to Least Significant Bit (LSB) are used for local pixel adjustment. The procedure used for moderate bit alteration followed by local pixel adjustment is narrated below:

I. If the PRB is of odd parity and message bit is 1, then there is no change in both the pixel blocks of the image pixel. The odd parity condition in the PRB reflects that the stored bit is 1 [16].

II. If the PRB is of odd parity and the message bit is 0, then complement the 4th moderate significant bit. Convert all the lower bits to 1 if moderate bit is changed to 0 or vice-versa otherwise [16].

III. If the PRB is of even parity and the message bit is also 0, then there is no change in both the pixel blocks of the image pixel. The even parity condition of the PRB reflects that image pixel stores 0 as the message bit [16].

IV. If the PRB is of even parity and the secret message bit is 1, then complement the 4th moderate significant bit. Convert all the lower bits to 1 if moderate bit is changed to 0 or vice-versa otherwise [16].

3.5 Pixel Adjustment Process

Following are the two steps used in pixel adjustment process.

Pixel Adjustment [16]

If crypto-bit to be embedded is equal to the 4th LSB, then there is no need for doing any pixel adjustment. However, if crypto-bit to be embedded is not equal to 4th LSB, pixel adjustment is performed by using first three LSBs. The underlying logic for the same is detailed below:

(a) If crypto-bit to be embedded is one, then pixel is adjusted by changing first three LSBs to zero.

(b) If crypto-bit to be embedded is zero, then pixel is adjusted by changing first three LSBs to one.

Post pixel adjustment

In this step, post pixel adjustment is applied further improve the visual quality of stego image obtained after pixel adjustment. This process involves only two bits, i.e., 5th and 6th bits. Let P, P' and P" are the values of ith pixel in the cover-image, modified pixel of stego-image after pixel adjustment and modified pixel of stego image after post pixel adjustment, respectively. Calculate the error (D1) between modified pixel of stego-image after pixel adjustment and original pixel of cover image, i.e., D1 = abs (P-P'). If D1 > 4, then post pixel adjustment is required otherwise there is no need of doing post pixel adjustment. 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 underlying logic for the same is detailed below:

(a) If after the process of embedding, 4th & 5th LSBs are unequal and 4th & 6th LSBs are equal, then post pixel adjustment is performed by complementing 1st, 2nd , 3rd, 5th and 6th bits of p'.

In fact, the proposed method provides a three layered security to protect the hidden data. First, cryptography technique is used to protect the information. Secondly, data hiding capacity of cover image is increased by encrypting and compressing the crypto data using CRT. Then, the cipher information so obtained is embedded in the cover image. The data hiding procedure is illustrated in Fig.2.

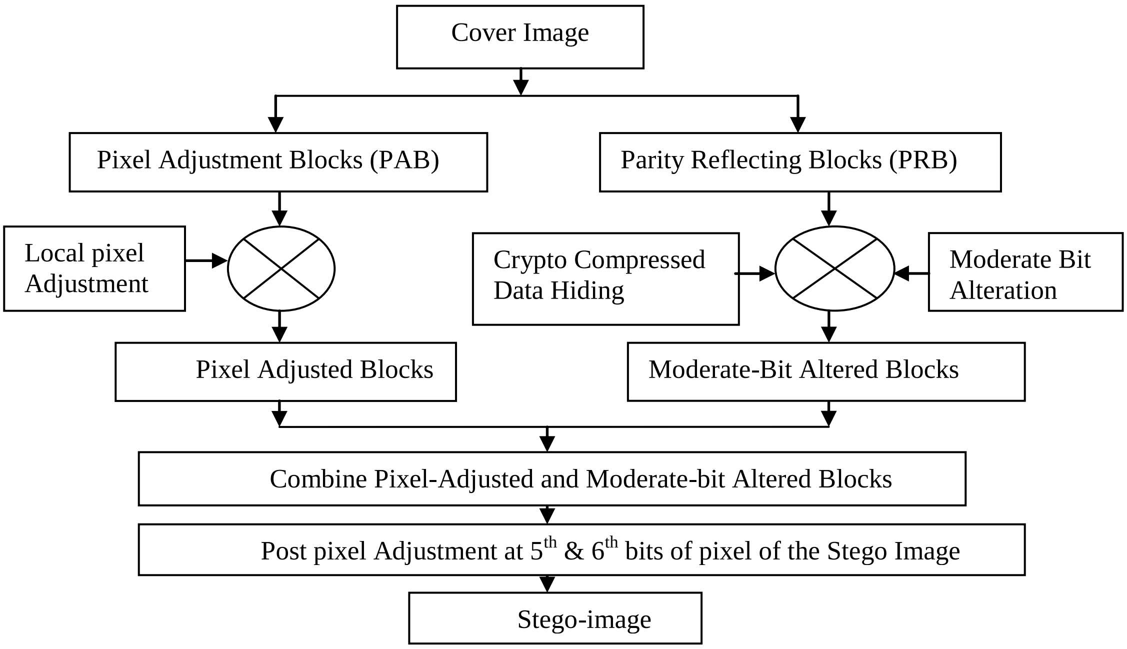


Fig 2: Moderate-Bit Altered Image Steganography

4. PROPOSED ALGORITHM FOR HIDING CRYPTO COMPRESSED DATA

4.1 Message Ciphering & Embedding

Step-1: Save secret message as a text file.

Step-2: Commencing with first character, read secret message character-wise from saved text file.

Step-3: Encrypt each character into row and column numbers using flexible matrix.

Step-4: Repeat Step-3 for all characters in the saved text file to obtain a row and column numbers.

Step-5: Combine all the row and column numbers into 1-D array.

Step-6: Pad the 1-D array with zeros such that total values in array must be divided by 4 for a block size of 4.

Step-7: Further encrypt and compress the ciphered data by applying the CRT using block of 4 values of 1-D array to calculate the value of X.

Step-8: Repeat step 7 for all values in 1-D array to obtain the values of X.

Step-9: After computing all X, the frequency of each distinct X and their counts are determined. All X are sorted in descending order of their count. A table of unique X and an equivalent smaller code is generated. Using this table, each X obtained is encoded into this smaller code.

Step-10: All value of X and smaller codes are converted into equivalent binary number (all X and smaller codes have equal number of bits by padding with zeros from left side) and make a binary string.

Step-11: Read each pixel of the cover image commencing with first pixel.

Step-12: Convert each pixel into equivalent eight-bit binary number called image byte.

Table 1. Proposed 16×16 Matrix for Enciphering Data [15]

Column Number Row Number	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	143	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
5	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
6	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
7	64	55	66	67	68	69	70	73	72	71	74	75	76	77	78	79
8	80	81	82	87	84	85	86	83	88	89	90	91	92	93	94	95
9	32	97	99	100	101	102	103	104	105	109	110	111	114	115	116	117
10	46	98	106	107	108	113	112	121	118	119	120	122	124	125	126	127
11	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	144
12	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
13	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
14	123	33	34	35	36	37	38	39	40	41	42	43	44	45	96	47
15	48	49	50	51	52	53	54	65	56	57	58	59	60	61	62	63

Step-13: Convert image byte into two blocks-Pixel Adjustment Block and Parity Reflecting Block.

Step-14: Determine the parity of the Parity Reflecting Block (PRB) & read first crypto-compressed-bit.

a) If the PRB is of odd parity and message bit is 1, then there is no change in both the pixel blocks of the image pixel. The odd parity condition in the PRB reflects that the stored bit is 1.

b) If the PRB is of odd parity and the message bit is 0, then complement the 4^{th} moderate significant bit. Convert all the lower bits to 1 if moderate bit is changed to 0 or vice-versa otherwise.

c) If the PRB is of even parity and the message bit is also 0, then there is no change in both the pixel blocks of the image pixel. The even parity condition of the PRB reflects that image pixel stores 0 as the message bit.

d) If the PRB is of even parity and the secret message bit is 1, then complement the 4^{th} moderate significant bit. Convert all the lower bits to 1 if moderate bit is changed to 0 or vice-versa otherwise.

Step-15: Go to next image byte and next crypto-compressed-bit and repeat the Steps-12 to 14 until all the crypto-compressed bits of the secret message are embedded into the PRBs of the cover image.

4.2 Message Extraction & Decryption

Step-1: Read the pixel of stego-image starting from first pixel.

Step-2: Convert each pixel value into equivalent binary number called image byte.

Step-3: Extract first crypto-compressed-bit by determining the parity condition of the Parity Reflecting Block. If it is odd parity then embedded crypto-bit is 1 otherwise it is 0.

Step-4: Repeat steps 2 to 3 until all the crypto-compressed-bits of the secret message are extracted.

Step-5: Divide the crypto-compressed-bits for values of X and smaller codes.

Step-6: Smaller codes are also replaced with X values.

Step-7: Apply the equation (4) and A_i of each X using the equation.

Step-8: Repeat step 7 for all values of X.

Step-9: Combine all A_i to form a single 1-D array. Divide the 1-D array into two equal sized arrays (Row & Column). The original pixel values are then reconstructed using the flexible matrix.

Step-10: Save all characters in the form of text file.

5. RESULTS AND DISCUSSION

In this section, simulation results of the proposed algorithm are presented by embedding 3000 bytes of crypto-compressed data at moderate significant bit positions of the pixels in the cover image. For experiments, four standard gray scale test images with 256×256 pixel size are employed as cover images (Lena, Mandrill, Pepper and Cameraman). MATLAB software is used to implement the algorithm and validate the results. Original cover images are shown in Fig. 3(a) along with their corresponding stego-images are shown in Fig. 3 (b) & (c) that are generated as a result of proposed algorithm. The proposed technique embeds crypto-compressed-data into moderate-significant-bit positions in the image-pixels without causing any appreciable distortion in the cover image. Visual quality of a stego image is an important parameter in evaluating the performance of the proposed algorithm. It is expressed in terms of Image Quality Measure (IQM) parameters including Mean Square Error (MSE), Peak-Signal-to-Noise Ratio (PSNR), Entropy, Correlation, Mean Value and Standard Deviation. The performance of the proposed algorithm is summarized in terms of IQM parameters. These results are tabulated in Table-2, Table-3 and Table-4. The results in these tables indicate that PSNR, Entropy, correlation, Mean value and Standard Deviation are decreasing whereas the MSE is increasing as the hidden message bit moves from LSB towards moderate significant bit position. The performance of the proposed method is better than [16] in terms of IQM parameters shown in Tables 2, 3 and 4.

The histograms of cover and stego-images give clear idea of the security of the transmitted data, i.e., if change in the cover is minimal, then stego system is considered secure. In this context, the effectiveness of the proposed algorithm is also determined in terms of having a comparison of the histograms of cover and stego images as show in Fig.4. The histogram analysis of the stego-images proves that these images look exactly similar to that of the original image. Further, this process provides two additional layers of security to the hidden message. First, cryptography technique is used to protect the information and it requires less computational overhead as compared to other steganographic techniques which transforms cover images into frequency domain. Secondly data hiding capacity of cover image is increased by encrypting and compressing the ciphered data using CRT. It also provides 256 combinations for data byte instead of single combination (remainder and quotients) when data byte is divided by 16 in CRT.

Table 2. Mean Square Error and Peak Signal-to-Noise Ratio resulted from hiding 3000 bytes of Crypto-Compressed data

Test Image (256×256)	Peak Signal-to-Noise Ratio (PSNR)		Mean Square Error (MSE)	
	With [16]	Proposed Method	With [16]	Proposed Method
Lena	42.7959	43.6624	3.4158	2.7980
Goldhill	42.7764	43.3040	3.4312	3.0387
Mandrill	42.5498	43.2155	3.6150	3.1012
Camera	41.7003	42.2161	4.3959	3.9036

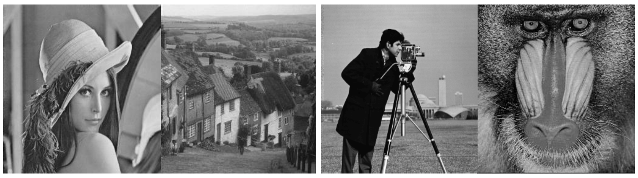
Table 3. Entropy and Correlation resulted from hiding 3000 bytes of Crypto-Compressed data

Test Image (256×256)	Entropy		Correlation	
	With [16]	Proposed Method	With [16]	Proposed Method
Lena	5.1151	5.1239	0.9993	0.9994
Goldhill	5.1016	5.1090	0.9993	0.9994
Mandrill	5.1695	5.1748	0.9992	0.9993
Camera	4.8165	4.8258	0.9995	0.9995

Table 4. Mean Value and Standard Deviation resulted from hiding 3000 bytes of Crypto-Compressed data

Test Image (256×256)	Mean Value			Standard Deviation		
	Cover image	With [16]	Proposed Method	Cover image	With [16]	Proposed Method
Lena	124.0923	124.1127	124.0150	47.8448	47.9462	47.9539
Goldhill	112.0349	112.2391	112.2100	48.5952	48.6440	48.5932
Mandrill	102.7616	102.7898	102.7715	48.7939	48.7962	48.7911
Camera	118.7228	118.6388	118.4387	62.3434	62.6854	62.5541

Lena Goldhill Cameraman Mandrill



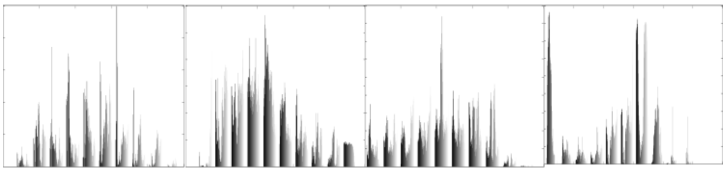
(a) Original cover images

(b) Stego images obtained with the proposed method in [16]

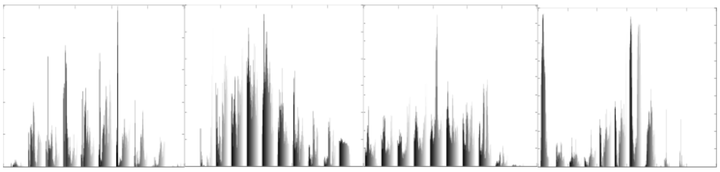
(c) Stego images obtained with the proposed method

Fig 3: Results of Experimental Validation

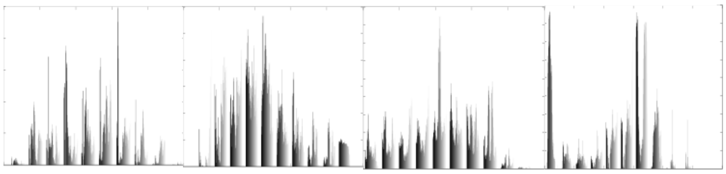
Lena Goldhill Cameraman Mandrill



(a) Histograms of original cover images



(b) Histograms of stego images obtained with the proposed method [16]



(c) Histograms of stego images obtained with the proposed method

Fig 4: Histograms of cover & stego-images

6. CONCLUSION

In this study, an attempt is made to develop a new approach for data hiding in grey scale images in which data encryption, compression and hiding are combined to enhance bandwidth utilization and achieve secure communication. First layer of security is achieved by using a symmetric key based on the concept of a flexible matrix. The data hiding capacity of the cover image is enhanced by encrypting as well as compressing the ciphered data using CRT. In this algorithm, upper 5^{th} & 6^{th} bits of the image pixel are also used for post pixel adjustment to further improve the visual perception of the stego image. In fact, by doing so, an additional layer of security to the original message is also provided besides increasing data hiding capacity of the cover image. The proposed algorithm requires less computational overhead as compared to other steganographic techniques which transform the cover image into frequency domain. Experiment results have demonstrated that the proposed scheme for data hiding works satisfactorily for different gray level digital images. Moreover, the proposed method provides acceptable image quality with very little distortion in the cover image.

7. REFERENCES

[1] Forouzan. B. A., Cryptography and Network Security. 4^{th} ed. Publisher: McGraw-Hill Higher Education, 2008.

[2] Vinoly Seromony, “Image encryption and compression using number theoretic paradigm”, GSPx Conference, (April 2003).

[3] W.B. Pennebaker, J. Mitchell, “JPEG still image compression standard”, New York, Van Nostrand Reinhold, edition (2001).

[4] V. Jagannathan, A. Mahadevan, R. Hariharan and E. Srinivasan, “Number Theory Based Image Compression Encryption and Application to Image Multiplexing”, IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. Feb. 22-24, (2007), pp.59-64.

[5] Neil F. Johnson and Sushil Jajodia, “Exploring steganography seeing the unseen”, IEEE Computer, (February 1998), pp. 26-34.

[6] R.J. Anderson and F. A. P. Petitcolas, “On the limits of the steganography”, IEEE Journal Selected Areas in Communications, (2001), 16(4), pp. 474-481.

[7] F. A. P. Petitcolas, R.J. Anderson and M. G. Kuhn, "Information Hiding–A Survey", Proceedings of IEEE, (July 1999), vol. 87 pp. 1062-1078.

[8] K. B. Raja, C. R. Chowdary, R. K. Venugopal, L. M. Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", Proceedings of IEEE, (2005), pp. 171-176.

[9] Westfeld A., "Steganography for Radio Amateurs-A DSSS Based Approach for Slow Scan Television", LNCS 4437, Springer-Verlag Berlin Heidelberg, 2007, pp. 201-215.

[10] Y. K. Lee and L. H. Chen, "A high capacity image steganographic model", In IEE Vision, Image and Signal Processing, (2000), 147(3), pp. 288-294.

[11] Michael Backes, "A cryptographically sound Dolev Yao style security proof of the Otway-Rees protocol", In Proceedings of the 9th European Symposium on Research in Computer Security (ESORICS), vol. 3193, Springer Verlag, Berlin Germany, (September 2004), pp. 89-108.

[12] L. M. Marvel, C. G. Boncelet, and C. T. Retter, "Spread spectrum image steganography", IEEE Transactions on Image Processing, vol. 8, Aug. (1999), pp. 1075–1083.

[13] Xin Li, Hong-heather Yu, "Transparent and Robust Audio Data Hiding in Spectrum Domain", IEEE International Conference on Multimedia and Expo (ICME), NY, USA, (2 August 2000).

[14] Chin-Chen Chang, Chi-Shiang Chan,Yi-Hsuan Fan, "Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels," Pattern Recognition, vol. 39, (2006), pp. 1155-1167.

[15] Balkrishan and Amar Partap Singh, "Hiding Encrypted Data using Randomly Chosen Moderate Bit Insertion in Digital Image Steganography", Journal of Computer Science and Engineering, vol. 1, issue 2, (June 2010), pp. 21-27.

[16] Jindal B, Singh AP (2013) Camouflaging in Digital Image for Secure Communication. J. IE(I)-Springer: Electrical, Electronics & Telecommunication and Computer Engineering, vol. 94, no. 2, pp 85-92, June 2013.

[17] Gonzalez R C and Woods R E. Digital Image Processing. Pearson Education, (2003).