DOI: 10.15439/2017R88
ACSIS, Vol. 10 ISSN 2300-5963

Lossless and Reversible Data Hiding in Encrypted Images With Public Key Cryptography

Monika Bartwal
M.Tech scholar, Department of
Computer Science & Engineering
Bipin Tripathi Kumaon
Institute of Technology
Dwarahat, Almora, Uttarakhand (India) 263653
Email: monikakandwal23@gmail.com

Dr. Rajendra Bharti
Assistant professor, Department of
Computer Science & Engineering
Bipin Tripathi Kumaon
Institute of Technology
Dwarahat, Almora, Uttarakhand (India) 263653
Email: rajendramail1980@gmail.com

Abstract—**The Lossless data hiding provides the embedding of data in a host image without any loss of data. This research explain a lossless data hiding and image cryptography method based on Choas - Block to image encryption the lossless means if the marked image is considered reliable, the embedding distortion can be totally removed from marked image afterward the embedded data has been extract. This procedure uses features of the pixel difference to embed more data than other randomly partition using Block based Sharpness Index Filtering and refine with single level wavelet decomposition shifting technique to prevent image distortion problems. In this work also manages reversible data hiding based on chaotic technique. In which initially image histogram processes to perceive the pixels which is chosen for hiding each bit of secret data, then by the logistic chaotic map compute an order of hiding each bit stream. Performances differentiate with other exist lossless data hiding plan providing show the superiority of the research. In this proposed research PSNR is found nearly 5.5*103 and existing 4.8*103 at 100 embedding rate which enhance for our existing technique that simulated in MATLAB 2014Ra.**

Index Terms—**chaotic S-block, reversible data hiding, Lossless data hiding, encryption, cryptography, SSI, BSSI.**

I. Introduction

In present always new devotion is funded to reversible data hiding in encoded images. meanwhile it protect the outstanding assets that the original cover can be losslessly improved afterward embedded data is deleted while defending the image content privacy. with the broad, universal use of the Internet, it is currently required to encrypt delicate data earlier transmission to defend those data. Reversible data-hiding methods can confirm that the receiver which can receive hidden messages and get well needed data without distortion. Reversible data-hiding has established wide attention since recoverable media are more valuable when protecting the security and privacy of sensitive information. For example, assume that the particular information of a persevering is personal information and the patient's X-ray image is used as cover media. It is very important to recover X-ray image without any loss of detail after recovering the patient's personal information. Presently, there are three useful domains used in reversible data-hiding systems (1) spatial domain, (2) distorted area and the (3) density compression field. In spatial domain pixels of the cover image convert directly to hide the data and in the distorted area the cover image is process through a transform process to reach frequency coefficients. Afterward frequency coefficient is enhanced to hide data. In the compression domain for changed to hide the data compression code is used.

A. Lossless Data Hiding and Reversible Data Hiding Scheme

Reversible data hiding (RDH) is a method which covers data and recovered original data afterward the embedded data is removed. It is an imperative method which broadly used in medical, military and law forensics imagery. where no distortion of the unique cover is acceptable. meanwhile first presented, RDH has involved substantial investigation attention.

B. Cryptography

Cryptography is a technique which is used to secure the data and safe data from several attacks. It gives encryption techniques for completely forms of data, documented and image data or software data for secured communication. The secret message is revised the data in a particular system. For the purpose of data privacy presently we have drawn together encryption and decryption. In cryptography there are three kinds of encryption are implemented.

C. Image encryption in Lossless data hiding

Generation of Encryption Image

There are three approaches for concept of the encrypted image

a) Image division
b) Self-reversible inserting
c) Image encryption

The first step is image division, the innovative uncompressed image is separated into two fragments A and B; and monitored through the LSBs. A is reversibly embedded into B, using self-reversible inserting and reversible data hiding technique. LSBs of A can be used to put up extra data. Afterward self-embedded data reorganized the encodes image using stream cipher. the values are 0 to 255 and signified by 8 bits.

D. Data embedding

Afterward the encryption process, the data hider put up the encoded image, and insert a limited data into it. The data hider can´t change the original image and only can manage the access to the embedded data.

E. Data extraction and image decryption

The data mining and data extraction entirely differs from image decryption. Two different case are taking to show.

Case 1: Extracting data from encoded images: The database management merely becomes the privileges to have the data hiding key and manage data in encoded area. It can decrypt the LSB-planes and removes the extra data. The evidence of encrypted images can be efficient complete LSB replacement. The entire process is done by the encrypted image, where it avoids the escape of original data.

Case 2: Removing data from decrypted images: The inserting and removal of data can be complete through the encrypted area. But the image decrypted by operator and the data extracts from decrypted area.

F. Histogram shrinks and image encryption

The information hiding technique has been formed in two sets of data, a set of inserted data and shield broadcasting. In the data hiding techniques, shield media become distorted and it does not revert back the original data. The shield media created by stable distortion after the deduction of hidden data. Figure 1 show the data hiding technique to insert the data in host image and recover the image/data from receiver side.

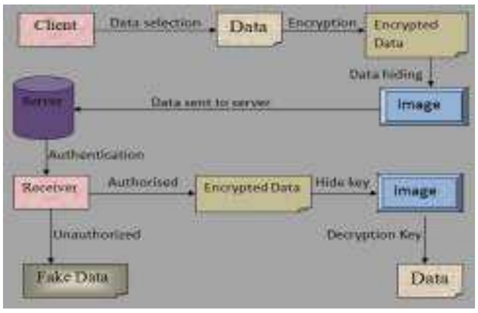


Figure (1) System architecture

In medical diagnosis, law application and military infrastructures reversing data hiding technique are uses at small level and it is significant to improve the innovative cover and it will private. It defends the encrypted data and actual technique for data communications.

G. Combined Data Hiding Scheme Embedding Process

This stage comprises all the actions that must be transmits obtainable to hide and defend the secret data secret the cover image. The sender usages certain algorithms to encode and compress the data and formerly inserts the bit stream into the image. The directing procedure involves of subsequent processes:

1. **Encryption** – In the initial stage of the inserting segment, the plan text will be encoded using different Encryption algorithms.

2. Compression – Compression technique is working efficiently to reduce the size of the message. Wavelet generates a table to exchange the repetitive following characters with binary code. This table, which is recognized as dictionary, will be shown to the recipient the end of the compression procedure to be used for extracting unique secret message.

II. USE OF CHAOTIC MODEL

In the recommended technique at the tip of the histogram diagram record gray surfaces for hiding the bits of the encrypted data. In the process of hiding data, initially numerous gray surfaces with 0 (zero) occurrences are originated. For an assumed image Fig. 2 (a) shows matrix and Fig. 2 (b) shows the histograms for assumed image in where several gray surface with zero occurrence are presented.

4	0	5	2	6
5	6	4	2	0
7	1	0	6	6
6	**5**	**6**	**4**	**7**
0	**0**	**2**	**5**	**6**

Figure (2) (a) image with gray surface for interval [0, 7],

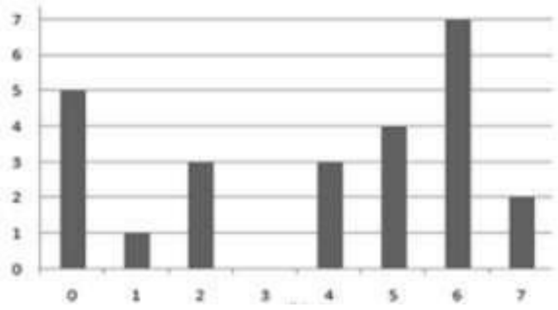


Figure (2) (b) image histogram in 2 (a)

In Fig. 2 (a) shows the gray surface has 6 extreme occurrences, and three has zero occurrences. Initially the value of each pixels of image has three different position can be expected. In plot shows the gray surface with zero frequency (set one pixels) and gray surfaces between them are the most frequent gray surface. And outside the interval of most frequent gray surfaces and devising zero incidence (assembly two pixels), whose gray surfaces equal to pixel which has maximum normal gray surface (collection three pixels). Afterward arranging pixels in process, for hiding the bit sequence subsequent stages are occupied.

Set one pixel

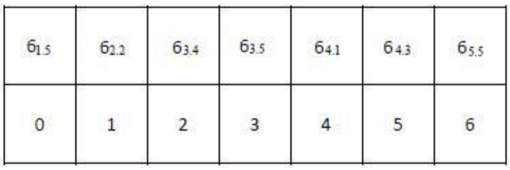
In this set pixel has zero frequency.

Set two pixels

In this set pixel collections are not change.

Set three pixels

On finding set one pixel initially zero is assigned the position of every pixel.



$6_{1,5}$	$6_{2,2}$	$6_{3,4}$	$6_{3,5}$	$6_{4,1}$	$6_{4,3}$	$6_{5,5}$
0	1	2	3	4	5	6

Figure (3): for most frequent pixel assigning number

For chaotic model we need a initial value to compute and construct to start the process through applying an eighty (80) bit key.

$$K= K_0, k1...K9 \text{ (ASCII)} \qquad (2)$$

And declared key transformed into binary (Equ. 3). This key, K i shows 8-bit block.

$$K=\left\{\begin{matrix} K_{01}, K_{02}, K_{03}, K_{04}, K_{05}, K_{06}, K_{07}, \\ K_{08}, ...K_{91}, K_{92}, K_{93}, \\ K_{94}, K_{95}, K_{96}, K_{97}, K_{98}\,(Binary) \end{matrix}\right\} \qquad (3)$$

Equ.3 shows j^{th} bit of the i^{th}block and Equ.4 shows the value of X_0 obtained in the interval [0, 1].

$$X_0=\left\{\begin{matrix} B_{01}\times 2^{79}+B_{02}\times 2^{78}+ \\ .... \\ B_{11}\times 2^{71}+B_{12}\times 2^{70}+ \\ .... \\ +B_{n7}\times 2^{1}+B_{r8}\times 2^{0} \end{matrix}\right\}/\,2^{80} \qquad (4)$$

Value of (X_1) in the interval [0, 1] is obtained after computing primary value of Logistic Map chaotic function.

$$Position = round(X_n \times (n-1)) \qquad (5)$$

In equation 5, n shows length of array. On computing first or initial gray surface to hiding encrypted data and remaining encrypted data is hidden on the basis of the behind of two rules

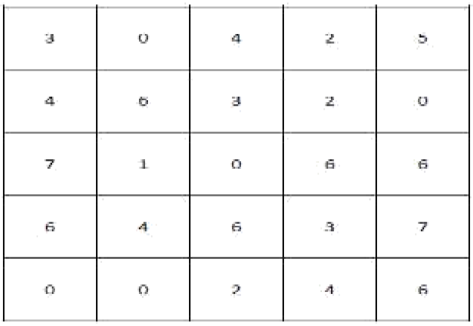
1) If significance of encrypted data is one through the chaos model the gray surface originates not change.
2) If cost of encrypted data is 0 (zero), by using chaos classic methods the gray surface originate. Where gray surface having zero frequency

For enhancing process hide 1 (one) encrypted data to the iteration of 10 (ten) shows in Fig 2.

First initial bit of encrypted data does not change which value is equal to 1 (one). And second bit of process is hidden as below.

$$X_2 = 3.99 \times 0.987525 \times (1 - 0.987525) = 0.0491543,$$
$$\text{Position} = \text{round}\,(0.0491543 \times (7-1)) = 0 \qquad (6)$$

For this module, value of the array of gray surface in first element is $6_{1,5}$.



3	0	4	2	5
4	6	3	2	0
7	1	0	6	6
6	4	6	3	7
0	0	2	4	6

Figure (4). Image after hiding encrypted bit series.

In this technique zero frequency of the gray surface is from 6 to 5 and the number of the element $6_{1,5}$ changes. If we consider rules which considered three groups of pixels, final matrix transform as shown in Fig. 4.

III. SYSTEM MODEL (CHAOTIC MODEL)

Chaotic pixels behavior look like noise, but totally definite. In the initial values and mapping function same value exactly produced again. Following are the three advantages of these pixels.

A. Sensitivity to the Primary Conditions

We can produces a huge changes in the resulting standards of the process through a minor change in initial value. The subsequent pixel will be very different from the early one.

B. Random Behavior

Chaotic simulations are the procedures which are used in producing arbitrary numbers in algorithms and allow the original of the related random statistics.

C. Definite Procedure

Chaotic models is entirely positive but seem to be arbitrary, A set of values can be prepared if the plotting purpose and the original values are recognized and instruction to be used in the imitation of those same initial values.

The Logistic Map is well-known pixels which has chaotic behavior shown in Equ.7

$$Xn+1= rx_n (1-x_n) \qquad (7)$$

Where X_n is a value in the interval (0, 1). In this pixel the r separated into three different intervals and shows three chaotic performances

1. For the value of r [0, 3] pixel behaves slightly chaotically for main ten values and develops constant afterwards the tenth iterations shown in Fig.5 (a).
2. For the value of r [3, 3.57] pixel behave slightly chaotically for initial twenty values and after twentieth values, be different among two unchangeable values shown in Fig. 5 (b).
3. For the value of r [3.57, 4] pixel usually is chaotic showing Fig. 5 (c). From above statement, object is a totally chaotic model and the chaotic pixel Logistic Map with initial values $X_0 = 0.3$ & r [3.57,4] is used.

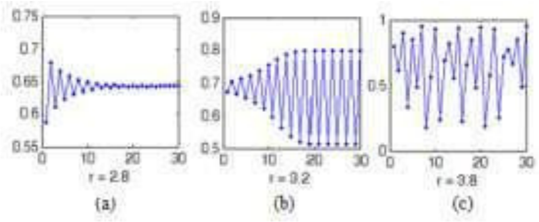


Figure (5) Logistic Map pixel for X_0= 0.3. (a) r [0, 3] , (b) r [3,3.57], (c) r [3.57,4]

IV. METHOD

In an image by using the redundancy used a key of reversible data embedding for finding an embedding area. To enlarge the other space the current techniques decrease the redundancy by the execution of pixel value calculation and make use of image histogram. The modern techniques show unlimited embedding volume without severely demeaning the visual excellence of embedded consequence. The focus of this part of the present paper is on the proposed algorithm which is used to encrypt and decrypt color images in different sizes as will be described in detail. It includes four major parts as follows:

Part One: this part is suitable for the diffusion of the image pixels. It is done by applying the forward Exclusive X-or and Backward Exclusive as follows:

1.Decompose the Red (R), Green (G), Blue (B) components of the image and store them in three arrays with size N*M, where N and M are rows and columns of the image.

2. Apply the following eq.(8) for forward Exclusive Xor on each of the image components respectively. C1(1)=P(1) where P(1) is the first pixel of the plain image which is used as seed.

$$C1(i)=C1(i-1)\oplus P(i) \qquad (8)$$

Where i =2…N*M where P(i), C1(i) are the present pixels in the plain and cipher images respectively and C1(i-1) is the previous cipher pixel . While the backward Exclusive X-or is applied on the resulted image as follows using eq.(9)

$$C2\ (i-1)= C2(i) \oplus C1(i-1) \qquad (9)$$

Where K=N*M, i =K…2, C2 (K)=C1(K) as seed.

In Result Fig.1 illustrates the plain image as input image.

Part Two: this part is suitable for disturbing the relationships between the neighboring pixels by altering their position but not making any change to the pixel value so the histogram of the image is stable. Scrambling of image pixels is done in the following steps.

1. Decompose each component into 16 16 sizes blocks

2. Initialize the secret parameters of 3D logistic map to generate secrets keys separately for R, G, and B components and each block in the component as follows:

3. Where x for Red, y for Green, and z for Blue. x0=0.976, y0=0.677 , z0=0.973 λ=3.8414991 , β=0.024, α=0.017.

4. Convert the secret keys to decimal number using the following eq.(10) as

$$Xi = floor\ (Xi,\ * 10^4) \qquad (10)$$

5. Exclusive X-or between the digits of the number.

6. Rotate each of the components (R, G, and B) left or right on the basis of the first bit of the number in step 5. Hence, Rotate is right if the first bit is 1 otherwise Rotate is left.

7. Rotate each block (16x16) of components right or left based on the first bit of the number in step 5; hence rotate right when the first bit is 1 otherwise Rotate left. In the decryption part the rotation process is done in reverse order hence rotat4MJe left when the first bit is 1, otherwise rotate right.

Part Three: it is suited to the diffusion of the relation between the plain and cipher mages by changing the pixel values. This part has the steps as indicated below:

1. Initialization of the three secret parameters to generate individual secret keys for R, G, and B of the scrambled image as follows: Where x for R, y for G, z for B and x0=0.234; y0=- 0.398; z0=-0.88

2. Convert them to values between 0…255 using the following eq.(13)

$$Xi, = \text{floor}\ (Xi, * 10_{10}\, mod\ 256) \qquad (11)$$

Algorithm (1): For Data encryption and embedding

1. Take input image or Selection of cover image.
2. Convert RGB Program into gray
3. RGB image has been converted to Gray scale
4. Program is Converting Image to type Double
5. Gray Image Has been Converted to type Double
6. Decompose the image by wavelet transform first and second level of Decomposition
7. Detail coefficient extracted to embedded data & approximation coefficient used for Image encryption.
8. use Block based SSI asymmetric key algorithm for secret data encryption
9. Data covered using S-block.
10. for Image encryption using chaos encryption.
11. lapsed time is calculated for checking efficiency through Performance Analysis like PSNR,

Process for Image and text decryption:-

Image and data can be recovered in two ways:

Case (1): First of all image is decrypted – Text is extracted - Text is decrypted - Original image is recovered.

Case (2): First of all Text is extracted- Text is decrypted - Image is decrypted - Original image is recovered

Algorithm (2): For image and data extraction

1: First encrypted image is extracted from encrypted image and then it decrypted

2: Then encrypted data is extracted from the decrypted image

3: And finally the encrypted data is decrypted using the related key.

V. RESULTS

Data Used

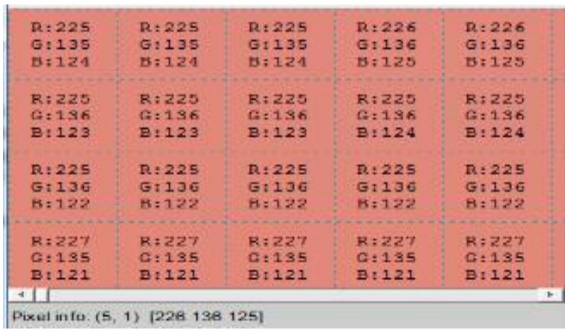
In this paper digital color image of JPEG format and other formats like bmp, png are used as cover image. The data files used for embedding are of txt, docx, pdf format. The size of image depends on the data size.

Process of work implementation

1. Select the key for Image Encryption using Chos-S Block based Technique

Figure (6): Input image

The input color image (.jpg, .tiff, .bmp,) is selected. Image is used in the form of carrier where the secret text can be inserted. Proposed technique has used different format and different types of images. After selection of images it proceeds to further process.



R:225 G:135 B:124	R:225 G:135 B:124	R:225 G:135 B:124	R:226 G:136 B:125	R:226 G:136 B:125
R:225 G:136 B:123	R:225 G:136 B:123	R:225 G:136 B:123	R:225 G:136 B:124	R:225 G:136 B:124
R:225 G:136 B:122	R:225 G:136 B:122	R:225 G:136 B:122	R:225 G:136 B:122	R:225 G:136 B:122
R:227 G:135 B:121	R:227 G:135 B:121	R:227 G:135 B:121	R:227 G:135 B:121	R:227 G:135 B:121

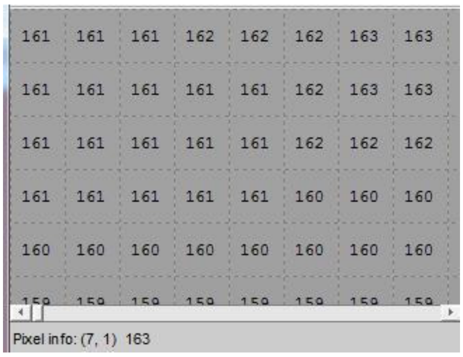
Pixel info: (5, 1) [228 138 125]

Figure (7): Matrix generation of input image

The Pixel Area tool opens a separate window containing a great close-up view of a small region of pixels in target image

.

Figure (8): RGB Image transformed into Gray Scale



161	161	161	162	162	162	163	163
161	161	161	161	161	162	163	163
161	161	161	161	161	162	162	162
161	161	161	161	161	160	160	160
160	160	160	160	160	160	160	160
159	159	159	159	159	159	159	159

Pixel info: (7, 1) 163

Figure 9: Matrix generation of gray image

Gray Image has been converted to type double

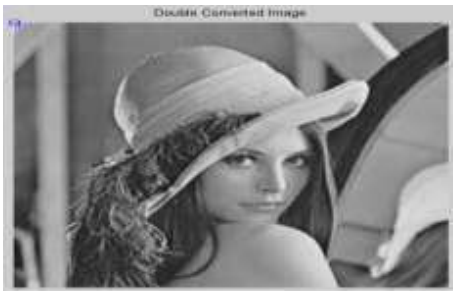
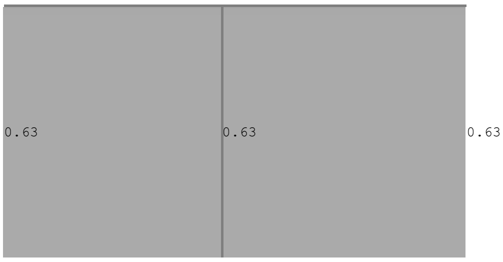


Figure (10): Double converted image



0.63	0.63	0.63

Figure (11): pixel region of Double converted image (Pixel region ((1,1) (0.63))

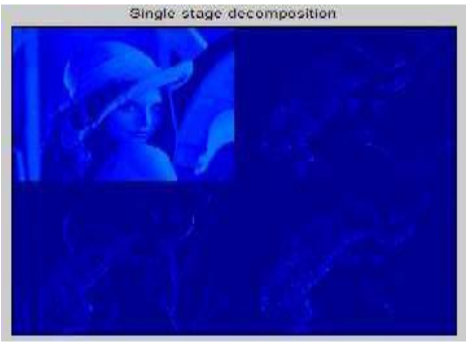


Figure (12): Image after 1st level of Decomposition

Figure (7), shows the fused image which we have browsed in figure 6 and 8 as first and second image respectively. In storage of image and image transfer image compression is more advantageous. Discrete Wavelet Transform image compression procedure is used for compressing the image in this research.

The effectiveness of altered wavelets with numerous decomposition stages are examined built on the standards of Peak signal to Noise Ratio (PSNR), Compression ratio (CR).

Figure (13): Image after 2nd level of Decomposition

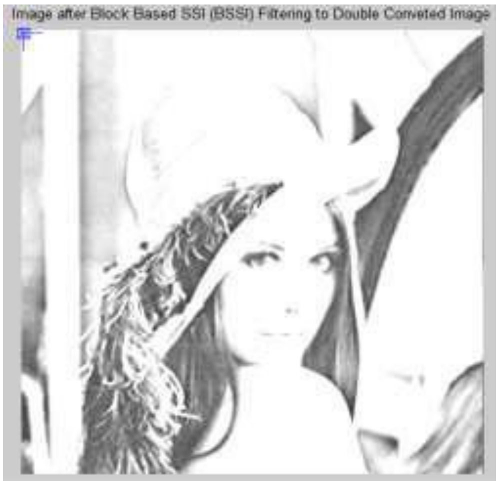
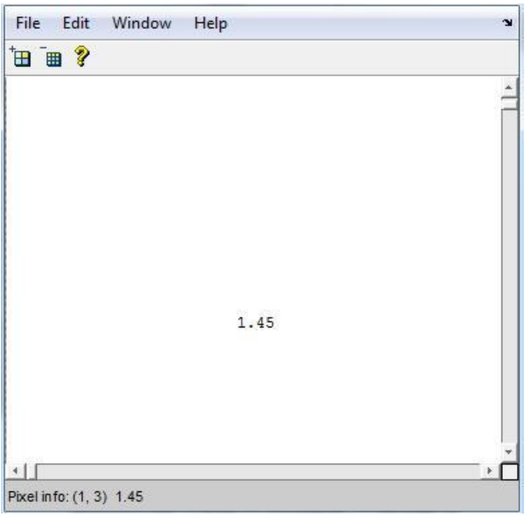


Image after Block Based SSI (BSSI) Filtering to Double Conveted Image

Figure (14): Image after block based (SSI) filtering to double converted image



```
1.45
```

Pixel info: (1, 3) 1.45

Figure 15: Pixel information of Image after block based (SSI) filtering to double converted image

Enter the key for Decryption: 2

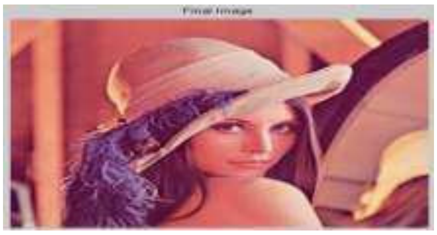


Figure (16): Final image after encryption

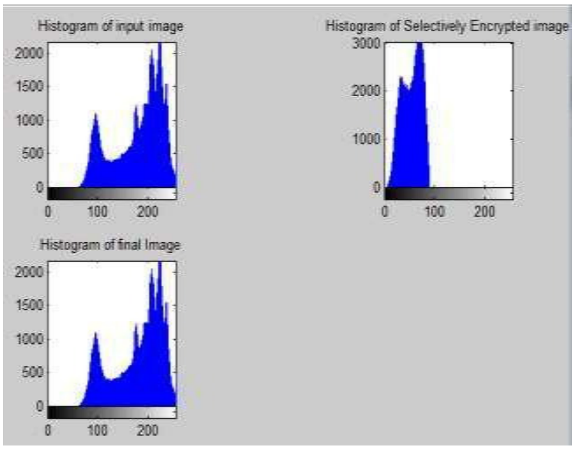


Figure (17): Histogram of the final image

Histogram operation can be used efficiently for image improvement. The histogram of a digital image in the interval [0, L_k-1] with gray surfaces has a discrete function $h(r_k) = n_k$, where r represent is the k^{th} gray close and n represents the number of pixels in image taking gray surfaces or level r_k. To control a histogram dividing each values to the total number of pixels in the image is a common preparation represent by *n*. and standardized histogram is supposed by $p(rk)=\frac{n_k}{n}fork=0,1$ and p (r_k) gives an approximation of occurrence of gray level is r_k.

Embedding rate	Base [1]	Chaoas-Sblock (Proposed)
0	0	0
50	0.01	0.05
100	0	0.23
150	0.01	0.056
200	0	0.74
250	0	0.89
300	--	1

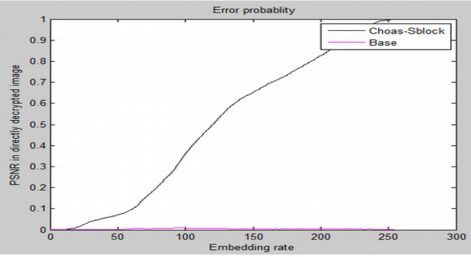


Figure (18): PSNR in density decrypted image for existing [1] and proposed technique over embedding rate and error probability

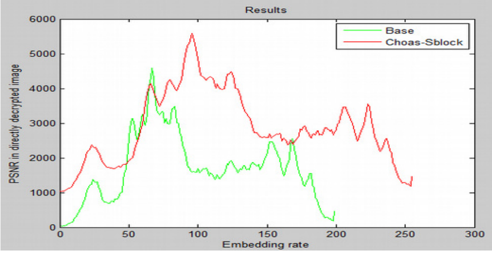


Figure (19): PSNR value over embedding rate

In above plot PSNR of the proposed technique is nearly 5.5x10^3 and existing 4.8x10^3 at hundred embedding rate which develop for existing technique. Total Elapsed time is 6.795790 seconds in execution program.

VI. Conclusion

Comparison of results make between conventional algorithms and the proposed algorithm. Proposed algorithm produces individually advanced embedded quality of images provided with a same embedding capacity. In proposed research a Symmetric image encryption algorithm based upon SSI S-Block and chaotic sequence is proposed. The unique BSSI s-block performs the change on the chaotic encoded image initially and then pixel matrix is completed by shuffling columns and rows of cipher. After simulation of the algorithm it shows that faster execution time. The proposed technique is studied in terms of key space analysis, statistical analysis, brute-force attack. in future the technique can be verified on various attacks. And this proposed work also explore the use of dynamic S- box for improved computing security.

References

[1] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng “Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography” 1051-8215 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.

[2] Shamim Ahmed Laskar and Kattamanchi Hemachandran “High Capacity data hiding using LSB Steganography and Encryption” Department of Computer Science International Journal of Database Management Systems (IJDMS) Vol. 4, No. 6, December 2012.

[3] Ashwak Mahmood Alabaichi “Color Image Encryption using 3D Chaotic Map with AES key Dependent S-Box” IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.10, October 2016

[4] M. Ushanandhini and D. Chitra “Optimal Prediction Scheme Using Reversible Information Hiding” International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 23 Issue 4 –August 2016.

[5] Patil K. U. 1 & Nandwalkar B. R. “GA Based Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption” IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834, p-ISSN: 2278-8735

[6] X. L. Li, B. Yang, and T. Y. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, December. 2011.

[7] Lokesh Kumar, Novel Security Scheme for Image Steganography using Cryptography Technique, Volume 2, Issue 4, April 2012.

[8] Z. Ni, Y. Shi, N. Ansari, and S. Wei, —Reversible data hiding, IEEETrans. CircuitsSyst. VideoTechnol.,vol.16,no.3,pp.354–362,Mar. 2006.

[9] Anchal Jain, Navin Rajpal, “A Two Layer Chaotic Neural Network based Image Encryption Technique”, IEEE National conference on computing and Communication systems, ISBN 978-1-4673-1952-2, 2012.

[10] Grasha Jacob, A. Murugan, "An Encryption Scheme with DNA Technology and JPEG Zigzag Coding for Secure Transmission of Images”, arXiv: 1305.1270v1, 2013.

[11] Grasha Jacob, Murugan A, “A Hybrid Encryption Scheme using DNA Technology”, IJCSCS Vol 3, Feb 2013.

[12] Zhang Yunpeng, Zhu Yu, Wang Zhong, Richard O.Sinnott, “Index-Based Symmetric DNA Encryption Algorithm”, IEEE (4th CISP), DOI 10.1109/CISP.2011.6100690.

[13] C. E. Shannon, “Communication theory of secrecy systems, Bell System” Technical Journal 28–4 (1949) 656–715.

[14] Xingyuan Wang · Qian Wang “A novel image encryption algorithm based on dynamic S-boxes constructed by chaos”, Nonlinear Dyn (2014) 75:567-576.