Reversible Data Hiding in Encrypted Image using Chaotic Algorithm

Suyash Sharma, Jaipal Bisht

[1] M .Tech Student, [2]Associate Professor

Radharaman Institute of Technology & Science

Abstract - nowadays, the reversible data hiding research has become major issue. The reversible data hiding techniques are researched to improve the distortion in sensitive images. The embedding process of this technique is the some of the general data hiding scheme. However, the extraction process has an additional method in comparison with general data hiding scheme. After the embedded secret data is extracted, the cover image can be completely restored to its original state The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. Result show that our method can embedded the data and image in best quality and it can be calculate with the help of PSNR. In our proposed work we also find final PSNR(dB) which shows the value is equal to infinite that means our image is of good quality and distortion is less.

Keywords - PSNR, NPCR, UAIC, BER, CHAOTIC SEQUENCE, PSEUDORANDAM GENERATOR.

1. INTRODUCTION

As an effective and popular means for privacy protection and robustness of a image we use the technique called encryption. Encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing can not read the data before encryption or after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource [2].

The source is first compressed to its proposed method using a standard source code. Then, the compressed source is Encrypted using one of the many widely available encryption technologies. At the receiver, decryption is performed first, followed by decompression. The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy, and then to encrypt the compressed data to mask its meaning. At the receiver side, the decryption and decompression operations are orderly performed to recover the original data[3]. However, in some application scenarios, a sender needs to transmit some data to a receiver and hopes to keep the information confidential to a network operator in provides the channel resource for the transmission. That means the sender should encrypt the original data and the network provider may tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. At receiver side, a decoder integrating decompression and decryption functions will be used to reconstruct the original data.

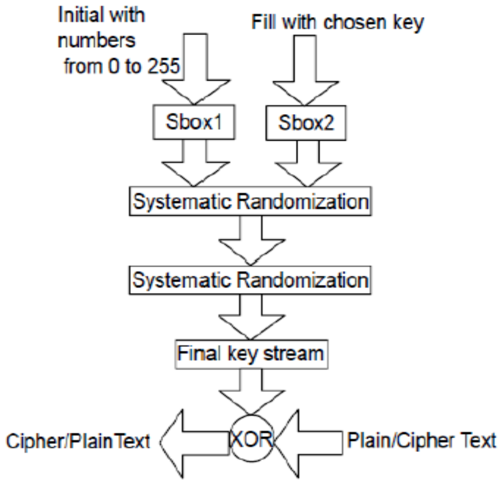
Some following Points are:

A. *Asymmetric Encryption*

Asymmetric or public key cryptography is potentially more Secure than symmetric methods of encryption. This type of Cryptography uses two keys, a "private" key and a "public key" to perform encryption and decryption. The use of two keys overcomes a major weakness in symmetric key cryptography, since a single key does not need to be securely managed among multiple users. In asymmetric cryptography, a public key is freely available to everyone and used to encrypt messages before sending them. A different, private key remains with the receiver of cipher text messages, who uses it to decrypt them. Algorithms that use public key encryption methods include RSA and Differ-Hellman. To encode a message and decode an encrypted message, one needs the proper encryption key or keys [1]. The encryption key is the table or formula that defines which character in the data translates to which encoded character. Here, encryption keys fall into two categories: public and private key encryption

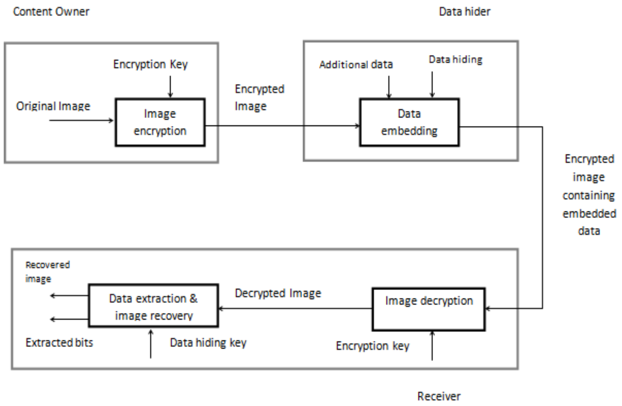
II. CHOTIC ALGORITHM

Chotic is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the ciphertext [7], [8].



A. NON-SEPARABLE REVERSIBLE DATA HIDING

IN ENCRYPTED IMAGE PROPOSED ALGORITHM



A. Encryption of image

In this generation of encryption keys and generation of pseudo random sequence is obtained.

Encryption key Generation*:*

Here encryption key is 128 byte and it is generated through random function. The key is uniformly distributed to the function.

Pseudo Random Sequence Generation*:*

By using encryption key pseudo random sequence consists of random bits is generated. Here we use chaotic sequence to create pseudo random sequence with 128 bit key. The number of bytes generated should be equal to the number of pixels in the input image provided the pixels are represented as 8-bit values. If the pixels are represented as 16-bit values then the number bytes in pseudorandom sequence should be double the number of pixels

Proposed Algorithm:

Step1:

IV **Data Embedding**

A gray scale image X of size MxN is given as input with L bits per pixel and generate a pseudo random code of size same as X and it is based on chaotic transformation which is calculate on the size of image. Now encrypted the image X with pseudo random image R using the exclusive OR method.

The encrypted image E is being segmented in to number of non overlapping bocks size BXB and of that block is having one additional bit. For every block B divide the pixel into two sets B0 and B1 and the probability that pixel belongs to B0 and B1 in is ½.Suppose the bit that is to embedded is 0 than flip the 3 least significant bits of each encrypted pixel in B0.If the embedded bit is 1 than the bit is in B1.

Step2:

DATA-EXTRACTION AND IMAGE-RECOVERY

At the receiver end receiver first generate the pseudo random code by using chaotic sequence generator with the same key as used at the time of encryption. After that apply XOR operation between encrypted image and pseudo random code and yield the decrypted image y. With the help of data hiding key segment the decrypted image into non overlapping block of size BxB. As we have done it before divide the pixel of each block in two sets in the same way as done in data embedding time.

For each decrypted block receiver flip all the LSB of the pixel in to B0 and to form a new block ,flip all LSB of pixel in B1 and form another new block and we denote them as a H0 and H1 and compare that block with B0 and B1.With the help of function we can calculate the flauction and denote them as f0 and f1[4].It is denoted as

$$f = \sum_{u=2}^{B-1} \sum_{v=2}^{B-1} \left| P(u,v) - \frac{p(u-1,v) + p(u,v-1) + p(u+1,v) + p(u,v+1)}{4} \right|$$

If f0<f1 then H0 is original content of the block and let the extracted bit is 0 otherwise H1 is the original content of the block and extracted bit is 1.At the end concatenate the extracted bit to retrieve the addition message and collect the required block to form the original image.

Differential Attack:

Attack to the image is very important aspects to research in now a days. The data which we are going to hide is valuable and required to be safe and in images the attack to the image is known as differential attacks.

Differential attack is a plaintext chosen attack. Attackers often use differential analysis to crack the cipher text. They usually change one or several pixels of the image, by comparing the two cipher text to find encryption rules.

There are two evaluation indicators testing ability to resist differential attack which are NPCR and UACI. NPCR refers to changes in the number of pixels of the cipher text after a pixel gray image changed and UACI refers to change of gray of cipher text after one pixel change in gray. NPCR and UACI are shows as formula (10) and (11).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

$$UCAI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{\left| C_1(i,j) - C_2(i,j) \right|}{255} \right] \times 100\%$$

B. RESULTS

The test image Lena sized 512 ×512 is used as the original image in the experiment. After image encryption, the four encrypted bits of each pixel are converted into a gray value to generate an encrypted image.

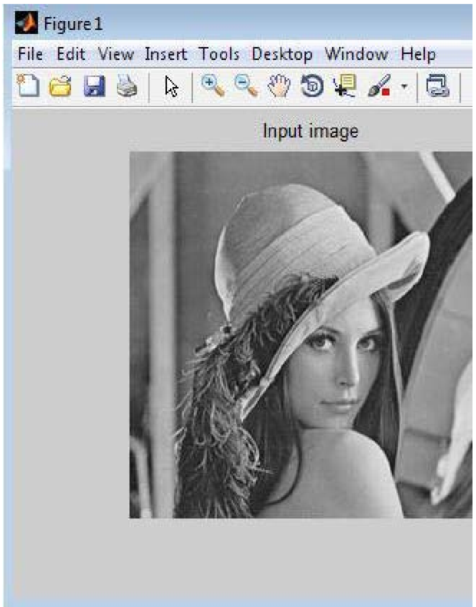


Fig:-input image

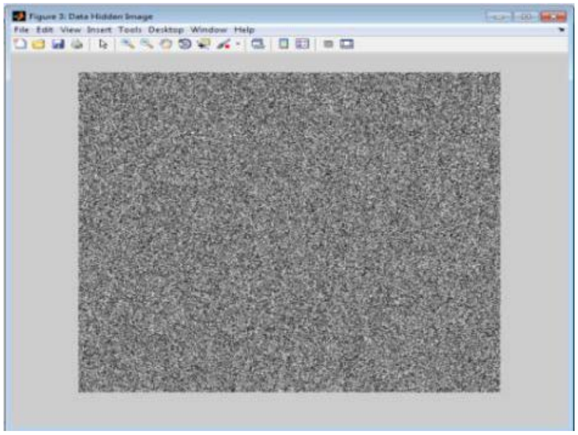


Figure 3: Data Hidden Image
File Edit View Insert Tools Desktop Window Help

Fig:-encrypted image

Let the encrypted image is having M=2 and N=1 and L= 128 .The above encrypted image is having the encrypted image containing the embedded data , we could extract the

additional data using the data-hiding key. Then, embedded the values of the parameters M, N and L into the LSB of image. When we put the value of M and N and random value from 0 to 1 and give block size 8 to 64 we obtain the encrypted image and data hiding image one by one and by giving the same values at the receiver end we received the stegeo image and the original image both.

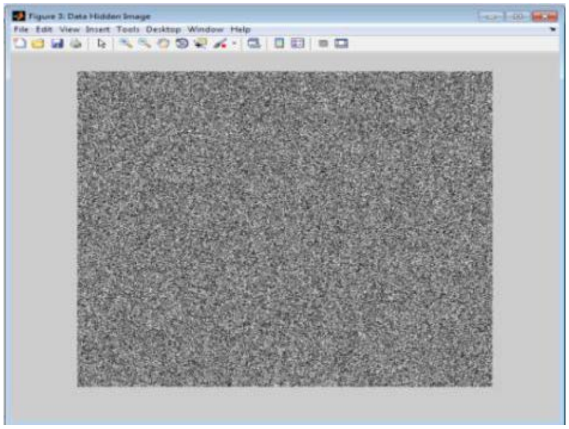


Figure 3: Data Hidden Image
File Edit View Insert Tools Desktop Window Help

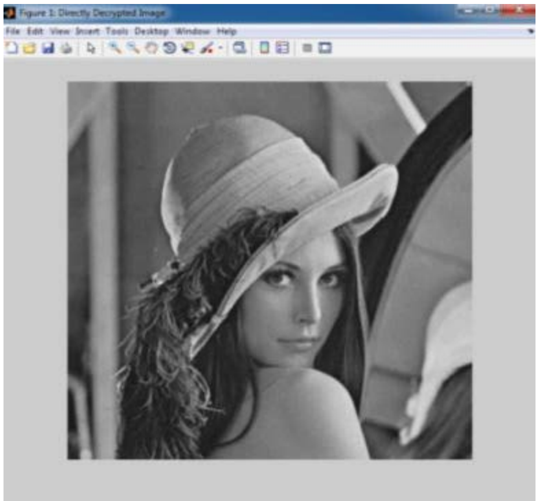


Figure 1: Directly Decrypted Image
File Edit View Insert Tools Desktop Window Help

Fig: Recovered image

We find the PSNR of recovered image is near about 52 which shows that our proposed algorithm is best image which we obtain is of best quality .

Table No1: Experimental value of the image Lena and here we calculate the value of NPCR, UAIC, PSNR, TIME, here the time is calculated to encrypt the image.

IMAGE	NPCR	UAIC	PSNR(db)	TIME(sec)
8X8	98.0023	5.678	42.569	.098176
16X16	98.0034	5.871	47.9275	.098458
32X32	99.0507	6.129	49.3469	.098563
64X64	99.1008	6.235	51.575	.091065

PSNR is defined as the ratio between maxim power of the signal and power of noise .The signal in this case is the original data, and the noise is the error introduced by compression.

Table No:-2 Comparison between Existing PSNR obtained from RC4 algorithm and Derived PSNR obtained by using chaotic sequence for the image LENA of size 512x512.

Image	Embedded ratio derived by rc4 algorithm	Previous PSNR derived from rc4 algorithm (db)	PSNR derived by using chaotic sequence(db)
(8x8)	0.004975	54.1733	56.6042
(8x8)	0.00995	47.1882	47.6033
(4x4)	0.0149925	40.9275	42.8627
(4x4)	0.0199	34.9458	41.6102
(4x4)	0.024876	30.8380	36.6498

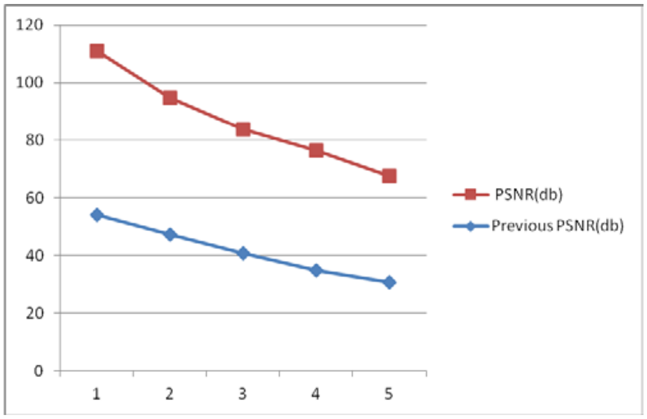


Fig: comparision graph between PSNR and previous PSNR

Bellow table gives the results for image lena having dimension 512x512

Table no.3 : In our system the distortion of image is obtained as very Low and the results shows that the PSNR is obtained is equal to infinite at receiver side which shows that our proposed algorithm is good and we obtained a good quality image.

Image	Embedded ratio derived by rc4 algorithm	PSNR derived from chaotic algorithm (db)
(8x8)	0.004975	Infinite
(8x8)	0.00995	Infinite
(4x4)	0.0149925	Infinite
(4x4)	0.0199	Infinite
(4x4)	0.024876	Infinite

C. *RESULTS AND DISCUSSIONS*

By using the encryption key Pseudo random sequence consists of random bits is generated. Here we are using the chaotic sequence algorithm to create the pseudo-random sequence using the 256-bit.By using the parameter additional data is inserted to encrypted image. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one when we are using only the encryption key.

When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image. When we are comparing with the other algorithms, the proposed system demonstrated successful accuracy in recovering the original image. In the future, distortion in image due to natural factors can be studied and speed of image transmission can be studied further

REFERENCES

[1] X. Zhang, “Lossy compression and iterative reconstruction for encrypted image,” IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[2] W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” IEEE Trans. Image Process., vol. 19 no. 4, pp. 1097–1102, Apr. 2010.

[3] K. Hwang and D. Li, “Trusted cloud computing with secure resources and data coloring,” IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[4] W. Hong, T. Chen, and H .Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process. Let, vol. 19, no. 4, pp. 199–202, Apr. 2012

[5] Y. C. Lin, “Reversible data hiding for progressive image transmission,” Signal Processing: Image Communication, vol. 26, no. 10, pp. 628–645, Nov. 2011.

[6] C. Candan. A Transcoding Robust Data Hiding Method for Image Communication Applications. IEEE International Conference on Image Processing, 2005, vo!.3: 660-663.

[7] M. Ashourian, P. Moallem, Y. S. Ho. A Robust Method for Data Hiding in Color Images. Lecture Notes in Computer Science, 2005, vo!.3768: 258-269.

[8] A. Parisis, P. Carre, M. C. Fernandez, N. Laurent. Color Image Watermarking with Adaptive Strength of Insertion. IEEE International Conference on Acoutstics, Speech, and Signal Processing, 2004, vol.3: 85-88.

[9] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, X. Lin. Robust Lossless Image Data Hiding. IEEE International Conference on Multimedia and Expo., 2004: 2199-2202.

[10] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Reversible watermarking algorithm using sorting and prediction,” IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009]

[11] Miscelaneous Gray Level Images [Online]. Available: http://decsai. ugr.es/cvg/dbimagenes/g512.php

Suyash Sharma has received his Bachelor of Engineering degree in Electronics & communication Engineering from REC Engineering College, Bhopal in the year 2011. At present he is pursuing M.Tech. with the specialization of Digital Communication in Radharaman Institute of Science & Technology College.