ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 7, July 2017

LOSSLESS AND REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES USING CHOAS BASED SBLOCK EMBEDING TECHNIQUE

Punisha Rajput[1]
Email I'd- punisha6335@gmail.com
AmitAsthana [2]
Computer Science engineering
Subharti Institute of Technology and Engineering (Meerut, India)

ABSTRACT

Recently more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content'sconfidentiality.In this reserch, design of chaos-based 4 x 4-bit substitution box (S-box) is presented. The chaotic 4x4-bit S-box provides good cryptographic properties and has software efficiency. The proposed chaotic 4x4-bit S-box is used for design of chaotic S-boxes chaining layer, which offers a highly secure level. The result of implementation shows that the proposed chaotic 4x4-bit S-box and LSB is suitable for the lightweight block cipher due to low resource utilization. The proposed method can achieve real reversibility that is data extraction and image recoveries are free of any error which simulated using MATLAB 2014Ra Version.

Keywords: Image Encryption, Image encryption key, Data Hiding Key , Image Decryption , Lossless, Reversible etc.

I.INTRODUCTION

1.1. Reversible data hiding technique

The term "reversible data hiding" means getting the exact retrieval of the data after performing the process like encryption-decryption and data hiding. A content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image, and then a data hider embeds additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted version. The detailed procedure of reversible data hiding techniques is as follows
It mainly consists of three basic steps

1.2. Image Encryption

Encryption is a process which changes image into a stream of coded data which makes it difficult to understand by unauthorized user. A number of secure stream cipher methods can be used here to ensure that anyone without the encryption key, such as a potential attacker or the data hider, cannot obtain any information about original content from the encrypted data.

1.3. Data embeddingfor block size

After Image encryption data embedding step will be executed. In this step, although a data-hider does not know the original image content, he can embed additional message into the image by modifying a small proportion of encrypted data

1.4. Data extraction & image recovery

At receiver site when encrypted image with embedded data is received, we have to decrypt original data and image. With calculation of encrypted key and data hiding key, a user can extract an image and then added data from that image.
A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types:
a) Lossless compression based methods,
b) Difference expansion (DE) methods,
c) Histogram modification (HM) methods.
In reversible data hiding scheme, the data extraction is not separable from the content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is revealed before data extraction, and, if someone has the data-hiding key but not the encryption key, he cannot extract any information from the encrypted image containing additional data.

1.5. Lossless Data Hiding Scheme

- A lossless data hiding scheme for public-key-encrypted images is proposed. There are three parties in the scheme: an image provider, a data-hider, and a receiver.

- With a cryptosystem possessing probabilistic property, the image provider encrypts each pixel of the original plaintext image using the public key of the receiver, and a data-hider who does not know the original image can modify the ciphertext pixel-values to embed some additional data into the encrypted image by multi-layer wet paper coding under a condition that the decrypted values of new and original cipher-text pixel values must be same.
- When having the encrypted image containing the additional data, a receiver knowing the data hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image.

- The embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption since the decrypted image would be same as the original plaintext image due to the probabilistic property.

II.RELATED WORK

Yih-Chuan Lin and A Tzung-Shian Li [1] proposes to use the quad-tree segmentation for increasing the hiding capacity of the reversible image data hiding scheme that embeds secret data through shifting the histogram of image pixels. In this paper a hierarchical segmentation is done on the input host image and converts it into several variable-sized blocks of pixels. These partitioned blocks are organized as a tree structure for the ease of representation. The secret message and the partition tree information are then embedded in these image blocks. With the proposed segmentation scheme, the algorithm can easily find a suitable non-overlapped partition of the image to significantly increase embedding capacity**.**

Jaya V. L and Munaga R. Gopikakumari [2] shows that the quality of an image after extracting from the hiding data is one of the important aspect which is usually assessed using image quality metrics. In this paper, a new FR metric, Image Enhancement Metric (IEM) is proposed which has been observed that the only metric that can be used for general and medical images for assessing improvement in contrast and sharpness is IEM. Standard Deviation also increases with increase in contrast and sharpness. So IEM together with SD may be considered useful for assessing quality of the enhanced image with respect to contrast and sharpness variations.

A. S. Al-Fahoum and M. Yaser [3]describes a novel and fully reversible data embedding algorithm for digital images is proposed. And the proposed algorithms are used to enhance their payload capacity. In this paper contrast stretching is used to produce space for hide the information without affecting the quality of image. For extremely important images, such as those used in medical, legal or military environment, the technique is very useful.

Dr. Vijay Dhir and Sanjeev Kumar [4]presents a review on the different image contrast enhancement techniques. Image enhancement is a processing on an image in order to make it more appropriate for certain applications. Image Enhancement techniques increase the contrast of image which is result produce better picture. There are many image contrast enhancement techniques like Linear Starching, Histogram Equalization, Adaptive Histogram Equalization, Convolution Mask Enhancement and Enhancement by Point Processing. This paper focuses on the comparative study of contrast enhancement techniques with special reference to local and global enhancement techniques.

AshwindS , Ganesh K , Gokul R [5] a Novel method is proposed by reserving room before encryption with a traditional RDH algorithm. It maintains the excellent property that the original image can be lossless recovered after embedded data is extracted while protecting the image content's privacy. An algorithm on Reversible Data Hiding on images and data, not only enhances the data transmission but also data security.

NutanPalshikar and Prof. Sanjay Jadhav [6] proposed scheme introduces a lossless recovery with visible digital watermarking technology. In this paper the hiding and recovering the information without loss is achieved by histogram shifting and also resolving the destruction of original images in visible digital watermark, and solving small amount of information hidden problems.

Sruthi and Manoj Ray D [7], this paper presents is a review on RDH reversible data hiding technique.

This paper shows that there are difference methods like expansion, interpolation technique, prediction and sorting, histogram modification for data hiding which is now used in encrypted images to improve security. Different RDH algorithms have their own merits and no single approach is optimal and applicable to all cases. This paper is a comprehensive exploration of all the major reversible data hiding approaches and also presents a new method RDH by reserving room before encryption.

Wei Liu et al. [8] in this proposal, resolution progressive compression scheme is used which compresses an encrypted image progressively in resolution, such that the decoder can observe a low resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. The encoder starts by sending a down sampled version of the cipher text. At the decoder, the corresponding low-resolution image is decoded and decrypted, from which a higher-resolution image is obtained by intra-frame prediction. The predicted image, together with the secret encryption key, is used as the side information (SI) to decode the next resolution level. This process is iterated until the whole image is decoded. So this multi-resolution approach makes it possible to have access to part of the spatial source data to generate more reliable spatial and temporal side information. But there is need to increase the efficiency of overall data compression to avoid the loss of any kind of data.

W. Puech et al. [9] proposed an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step for protection of multimedia based on Encryption and watermarking algorithms rely on the Kirchhoff's principle, all the details of the algorithm are known, and only the key to encrypt and decrypt the data should be secret.

Christophe Guyeux et al. [10] developed a new framework for information hiding security, called chaossecurity. In this work, the links among the two notions of security is deepened and the usability of chaos-security is clarified, by presenting a novel data hiding schemethat is twice stego and chaos-secure. The aim of this approach is to prove that this algorithm is stego-secureand chaos-secure, to study its qualitative andquantitative properties of unpredictability, and then to compare it with Natural Watermarking. Some of the probabilistic models are used to classify the security of data hiding algorithms (Runge-Kutta algorithm) in the Watermark Only Attack (WOA) framework. Hence method possesses the qualitative property of topological mixing, which is useful to withstand attacks but cannot be applied in KOA and KMA (Known Message Attack) setup due to its lack of expansively schemes which are expansive.

III. PROPOSED IMPLEMENTATION

S-BLOCK (LOW DETECTION STEGANOGRAPHY) USING MODIFIED STEGANOGRAPHIC ALGORITHM

Algorithm S-BLOCK: Modified S-Steganographic Algorithm (MSblock)

Input: Cover Image I

Input Parameters: Rows and Columns to be cropped(**u, v**),Block size(**m× n**),Quantization Matrix (Q)

Output: Stego Image Is

Begin

1. Partition the cover image Ì into Î u, vand Ì u, v and $I^{\delta}_{U,\ V}$ by cropping *u* topmost rows and *v* leftmost columns.

2. Perform m×n non-overlapping block partitioning on $\hat{I}_{U,\ V}$.

Let us denote this set of blocks by$P_{I\,u,\ v}^{(m\times n)}$

3. Choose a set of blocks from $P_{\hat{I}\,u,\ v}^{(m\times n)}$ (using a key shared by both ends) and perform the embedding in each of the selected blocks using any standard DCT based steganographic scheme. The quantization matrix *Q* which is a shared secret is used for obtaining the quantized coefficients.

4. Apply dequantization and Inverse Discrete Cosine Transform (IDCT) to the set of blocks used for embedding in Step 3.

5. Join $I^{\delta}_{U,\ V}$ with the resulting image obtained at Step 4. This combined image is the outputs Stego image I_S which is compressed using JPEG compression and communicated as the stego image.

End

The algorithm that can be used to generate n-bit x nbit S-boxes basically operate by converting the outputs of chaotic systems into integers between 0 and 2n . The algorithm's operation is given below: Algorithm

Step 1: System trajectories are obtained by solving the fractional chaotic Lorenz system with selected initial conditions and chaotic parameter values employing.

Step 2: Select four parameters, base-ten value denoted by these digits is converted into integers between 0 and 2^n by taking the modulus of this number at mod (2^n).

Step 3: S-Box is generated using the codes corresponding to outputs with the code corresponding to the smallest output being the first cell of the S-Box.

Step 4: The obtained number is added to the table if it is not already present; otherwise the process reverts back to Step 1 to generate a new integer value.

Step 5: The process goes on until all cell values are filled.

Step 6: After the S-Box is generated; we have apply affine transformation to each element of our chaotic S-boxes elements $x^T = [x_0, x_1, x_2, \ldots, x_7]^T$, i.e.;

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Step 7: We have applied S-box transformation on the obtained S-boxes in Step 6 for image encryption.
The proposed S-box is tested by statistical methods to determine the strength and resistance against cryptanalysis. The primary objective of the S-box is to induce nonlinearity in plaintext.

IV. Result and discussion

The Standard executed image of size 256×256 is used as plain image. The corresponding encrypted image analysis is provided in the following experimental graph. The proposed scheme is also tested with other standard images.

It is known that the generated cipher has to pass the statistical analysis and is of crucial importance for a cryptosystem. To evaluate the security, the following statistical tests are performed. The result proves that the cipher image is robust against any attacks and bears no statistical similarity to the plain image.

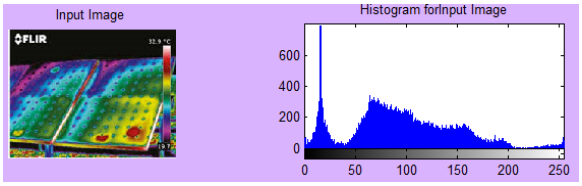
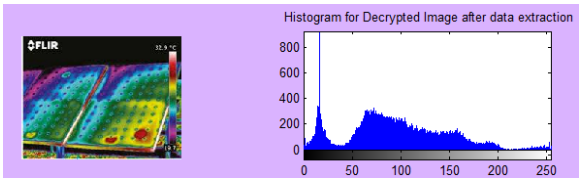


Figure 1: (a). Original Image (b). Histogram of the Original Image

Figure 2:Cipher Image

Figure 3: Histogram of the Cipher Image



4: Reversible output of input image

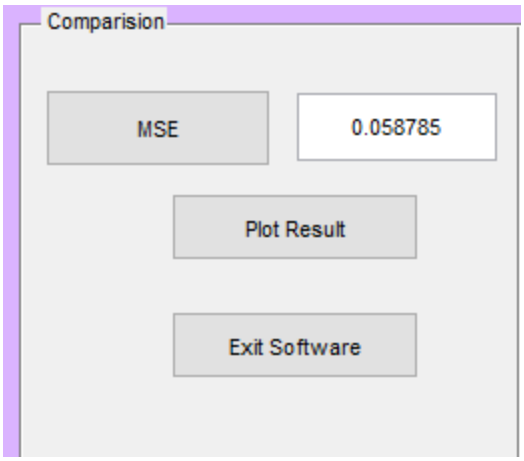


Figure 5: MSE value of experimental image

V.CONCLUSION

This work proposes a lossless, a reversible, and a combined data concealing plans for figure content foot age disorganized by open key cryptography with probabilistic and homomorphism properties within the reversible set up, a preprocessing of bar graph healer is created before encoding, and a 1/2 cipher text element qualities are altered for data inserting. On beneficiary facet, the additional data may be separated from the plaintext area, and, in spite of the very fact that a small twisting is bestowed in unscrambled image; the primary plaintext image may be recuperated with no mistake attributable to the two's similarity plots, the data implanting operations of the lossless and therefore the reversible plans may be all the whereas performed during a disorganized image during this means, the collector could take away a bit of put in data within the disorganized area, and concentrate another piece of inserted data and recoup the primary plaintext image within the plaintext space.

REFERANCES

[1] Yih-Chuan Lin and A Tzung-Shian Li, "Reversible Image Data Hiding Using Quad-tree Segmentation and Histogram shifting", Journal Of Multimedia, Vol. 6, No. 4,pp.349-358 August 2011.

[2] Jaya V. L and Munaga R. Gopikakumari, "IEM: A New Image Enhancement Metric for Contrast and Sharpness Measurements", International Journal of Computer Applications, Vol.79 No.9, pp.233-243. October 2013.

[3] A. S. Al-Fahoum and M. Yaser, "Reversible Data Hiding Using Contrast Enhancement Approach", International Journal of Image Processing (IJIP), Vol.7Issue 3 ,pp.348-356 October 2013.

[4] Dr. Vijay Dhir and Sanjeev Kumar, "Review of Various Image Contrast Enhancement Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4 Issue 8 pp.110-113 August 2014.

[5] Ashwind S , Ganesh K , Gokul R and Ranjeeth Kumar C, "Secure Data Transmission Using Reversible Data Hiding", International Journal of Computer Science and Information Technologies, Vol. 5 Issue 2 pp. 861-1863 , 2014.

[6] NutanPalshikar and Prof. Sanjay Jadhav, "Lossless Data Hiding using Histogram Modification and Hash Encryption Scheme", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 1pp.485-493 January 2014.

[7] Sruthi and Manoj Ray D, "A Review: Reversible Data Hiding Techniques", IOSR Journal of Computer Engineering, pp.16-21, 2014

[8]Wei Liu, WenjunZeng,Lina Dong, and QiumingYao"Efficient Compression of Encrypted GrayscaleImages", Image Processing, IEEE Transactions Vol: 19, April 2010, pp. 1097 –1102.

[9] W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for Encrypted Images", SPIE, IS&T'08: SPIEElectronic Imaging,Security, Forensics, SteganographyandWatermarking of Multimedia Contents, San Jose, CA, USA.

[10] Christophe Guyeux, Nicolas Friot, and Jacques M. Bahi, "Chaotic iterations versus Spread-spectrum: chaos and stego security", January 25-2011, IIHMSP,pp. 208-211.