International Journal of Research in Advent Technology, Vol.4, No.3, March 2016
E-ISSN: 2321-9637
Available online at www.ijrat.org

Security Enhanced Reversible Data Hiding using AES and Histogram Shifting

Nidhi Antony[1], Rinju Mariam Rolly[2]
M.Tech Student[1], Assistant Professor[2]
Department of Electronics & Communication Engineering[1, 2]
Rajagiri School of Engineering and Technology,Kerala
Email: nidhian92@gmail.com[1] ,rinju.mariam@gmail.com[2]

Abstract- Security enhanced communication has gained much importance nowadays. More importance is given to reversible data hiding (RDH) in encrypted images, because its lossless recovery nature of cover image after extraction of secret data**.** The cover image is retrieved in a separable manner from the marked image. In the content owner side cover image is encrypted by 2D logistic map-chaotic based permutation- substitution algorithm using a security key defined by user. It is used instead of 1D logistic map algorithm to protect 2D nature of images.2D logistic map has higher complexity chaotic behavior compared to 1D logistic map hence it enhances security. Instead of directly embedding data into encrypted image we encrypt the data using AES for providing double layer security. The data hider conceals AES encrypted data into the encrypted image by shifting its histogram, by utilizing another user defined data hiding key. Various security analyses are also carried out in this paper to ensure security. Among various RDH algorithms we use histogram shifting for data embedding since it offers high capacity. Hence, the proposed method is a reliable and secure technique for reversible data hiding.

Index Terms- AES, Data Hiding, Histogram Shifting, Logistic Map, Reversible Data Hiding, Security Analysis

1. INTRODUCTION

With the advancement in technology scope of secure communication has gained importance. Security of image and data plays vital role in the field of communication. Image and data can be copied in media or transferred within seconds to any part of the world. This technology can be used by terrorists or unauthorized users to hack the secret files and confidential information. Unexpected exposure of confidential data or images of military, government or any other organizations may lead to tremendous impacts. It may shatter the whole security system.

In data hiding lossless recovery of cover image is not ensured rather emphasis is on lossless recovery of secret data. Reversible data hiding is a technique by which the original cover image can be retrieved without any loss after the secret messages are extracted .It is widely used in the field of medical, military, law and government, where distortion of original cover is not allowed. Researchers have proposed various types of reversible data hiding techniques.

The main aim of this work is to enhance the security of reversible data hiding for secure communication. It provides the property of lossless recovery after secret data is extracted while protecting the cover image's confidentiality [3]**.** Cover image is retrieved separately from marked image. In the content owner side cover image is encrypted by using 2D logistic map-chaotic based permutation- substitution algorithm[1].It is used instead of 1D logistic map.2D logistic map has higher complex chaotic behavior than 1D logistic map hence it enhances security. Instead of directly embedding data into encrypted image we encrypt the data using AES for providing double layer security. The data hider hides AES encrypted data into the encrypted image by shifting its histogram, which uses another user defined data hiding key. Out of various RDH algorithms we use histogram shifting for data embedding since it offers high capacity [6]. Hence, the proposed method is a viable and secure technique for reversible data hiding.

2. PROPOSED METHOD

The flow of this work is shown in the Fig-1. In the content owner side cover image is encrypted by means of user-defined security key derived-2D logistic map-chaotic based transposition algorithm instead of 1D logistic map. It has more complex chaotic behaviors in comparison with 1D Logistic map. We utilize this more complicated logistic map to generate pseudo random sequences where we propose a key schedule algorithm to translate a binary encryption key to initial values and parameters used in the 2D logistic map [1]. We use an image encryption algorithm developed using these pseudo-random sequences under the framework of the permutation- substitution network, which is found to be very useful to maintain both confusion and diffusion properties in stream ciphers

and block ciphers. Instead of directly embedding data into encrypted image we encrypt the data using AES for providing double layer security. The data hider embeds AES encrypted data into the encrypted image by shifting its histogram, which makes use of another user defined data hiding key .Among various RDH algorithms proposed by researchers we use histogram shifting for data embedding since it offers high capacity and constant PSNR over other methods[6].

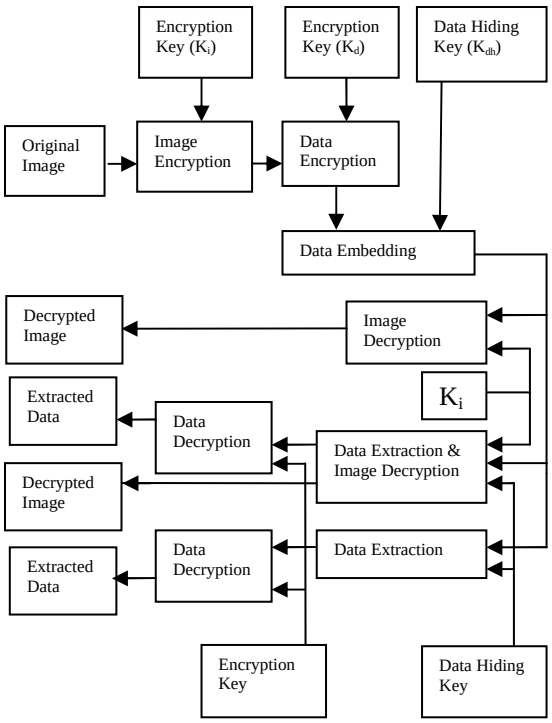

Fig. 1. Block Diagram

2.1. Image Encryption Using 2D Logistic Map

It is composed of three stages 2D Logistic Permutation, 2D Logistic Diffusion and 2D Logistic Transposition where each stage itself is considered as image cipher and they together constitute the permutation-substitution network. Encryption key E is a 256-bit string. It has five parts m_0, n_0, a, Z, and $X_1 \ldots X_8$, where (m_0, n_0) and a are the initial value and the parameter in the 2D logistic map. For coefficients X_0; X_1; …; X_7, each of which is composed of 6-bit string $\{c_0; c_1; c_5\}$, we translate these 6-bit strings to integers and obtain the required coefficients. X and Z are the parameters of the linear congruential generator [1].

In 2D permutation stage it performs both row permutation and column permutation. The pixels in the plaintext image P are then well shuffled and the permutated image is made unrecognizable. In 2D diffusion a slight change is made in plaintext image which leads to significant changes in cipher text and thus attains the diffusion properties. The plaintext image P becomes completely unintelligible after two-rounds of diffusion. The 2D transposition changes pixels values with respect to the reference image I, which is dependent on the logistic sequence generated from the previous stage.

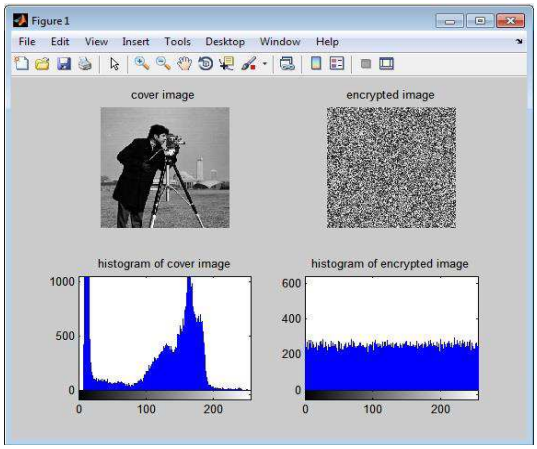

Fig. 2. Image Encryption

2.2 Data Encryption using AES

Instead of directly embedding data into encrypted image we encrypt the data using AES for providing double layer security [4].

- Rijndael algorithm is the basis of AES
- Process data blocks of 128 bits
- Cipher keys with lengths of 128, 192, and 256 bits.

AES Transformations:

- Sub Bytes
- Shift Rows
- Mix Columns
- AddRoundKey

2.3 Histogram Shifting:

Previous HS algorithms utilized the zero point of the histogram of a cover image and then slightly alter the pixel grayscale values to create space for secret data to be embedded. It has low execution time and low computational complexity**.** It offers less capacity [5].

Step l.The zero point and the maximum point of histogram is found. The zero point refers to the grayscale value in which there are no pixels in the given image. The maximum point corresponds to the grayscale value in which there is the maximum number of pixels in the given image.

Step 2. The whole image in scanned in a sequential order, such as row-by-row, from top to bottom. The range of grayscale value of pixels between 175 (including 175) and 254(including 254) is incremented by "1", i.e., perturbing the range of the histogram, [175 254] to the right-hand side by 1 unit and leaving the grayscale value 175 empty.

Step 3.Hide the secret data into the grayscale value of 174 and 175.

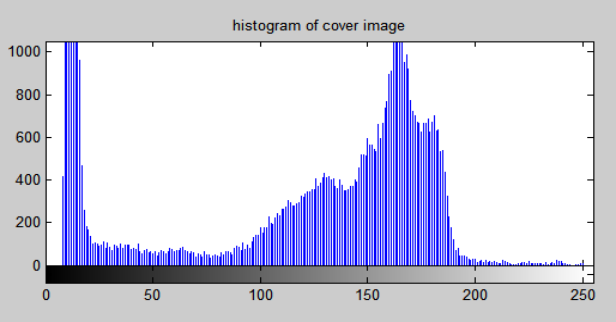

Fig. 3. Histogram with minimum and maximum points

This method does not have much space for hiding data. So when the size of secret data to be embedded is more the modified approach is used. The modified approach has more embedding capacity. The modified approach is as follows:

Step 1. Find out one maximum point which is location of 174 and two minimum points which are location of 247 and 23.

Step 2.The location information is stored in location map in order to recover original images. The location information of the pixels consists of maximum point, left minimum point, and right minimum point.

Step 3. Embedding space is generated by shifting the pixels that are located in histogram between left minimum point and left side of the maximum point (pixel value of 174) one pixel left.

Step 4. Hide the secret data into the grayscale value of 172 and 173 or 175 and 176.

2. 4 Data Extraction & Image Recovery

When the receiver has,

• **Data Hiding Key alone**: When receiver has only data hiding key alone and encrypted cover containing hidden secret message, then extraction of hidden information alone is possible. Decryption of encrypted cover or any small fragment or region of encrypted cover will not be possible.

• **Encryption Key alone**: When receiver has encryption key alone and encrypted cover containing hidden secret message, then only the decryption of the cover alone is possible. The extraction of hidden secret message or any fragment of hidden secret message is not possible.

• **Both Data hiding and Encryption Keys**: When the receiver has both keys, then both the cover image and hidden data can be retrieved. Hence the condition of separability also satisfied.

3. SECURITY ANALYSIS

The security analysis is carried out to ensure the security of proposed method. An efficient RDH method should resist all kind of known attacks and its encryption quality should be high.Inorder to enhance security the key size must be large, even a small change in key should make large difference in output so that its resistance to attack will be strong. Several security analysis is explained here.

3.1 Key Space Analysis

The key used for encryption of the proposed image encryption algorithm consists of five parts, i.e. m_0, n_0, a, Z and X. First four parts represents fraction part for double precision float number of 52-bit length and the last part X stores eight initial coefficients for round keys generation, each of which contains six bits [1]. Encryption key size of the proposed method is of 52 x 4 + 8 x 6 = 256-bit length. As cipher key size increases it has a strong resistance to brute-force attacks.

3.2 Histogram Analysis

The histogram analysis of cipher text image is one of the simplest methods to ensure the image encryption quality. Uniformly-distributed histogram for a cipher text image implies that encryption method is efficient. Since it encrypts a plaintext image to random-like its resistance to attacks is strong.

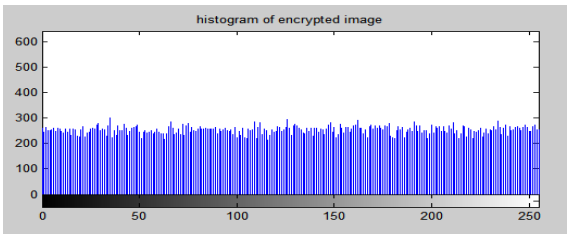

Fig. 4. Histogram of encrypted image

3.3 Key Sensitivity Analysis

This analysis shows that even a slight change in the key will result in some large changes in the cipher text. This makes the cryptosystem resistant to statistical or differential attacks. A security enhanced cipher should be sensitive to the encryption key. Key sensitivity has two aspects:

Encryption: Consider two encryption keys K1 and K2 which differs by only 1 bit. With respect to the same plaintext image how different are two cipher text image C1 and C2 using K1 and K2.

Decryption: Consider two encryption keys K1 and K2 which differs by only 1 bit. With respect to the same plaintext image how different are two decrypted image D1 and D2 using K1 and K2.

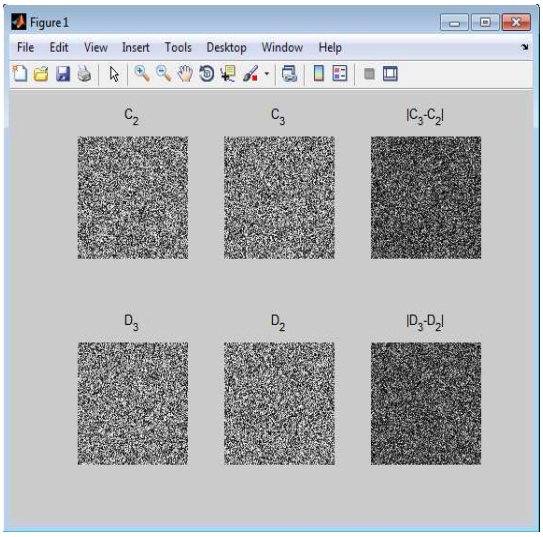

Fig. 5. Key Sensitivity Analysis

3.4 Information Entropy Analysis:

The entropy for a encrypted image with 256 gray levels, should ideally be $H(X) = 8$. If the entropy is less than 8, then it threatens the system security due to the existence of certain degree of predictability. The proposed algorithm is has its entropy much closer to 8. This means that leakage of information in the encryption process is negligible and the cryptosystem is resistant to entropy attack [1].

3.5 PSNR

Peak Signal to Noise Ratio is the ratio between the maximum possible power of a signal and the power of the noise that affects the fidelity of its representation [3].

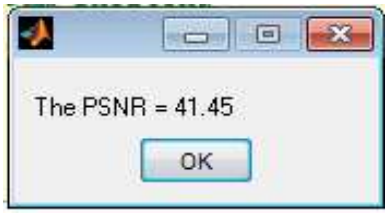

Fig. 6. PSNR

3.6 NPCR

NPCR (number of changing pixel rate) concentrates on the absolute number of pixels which changes values in differential attacks [1].

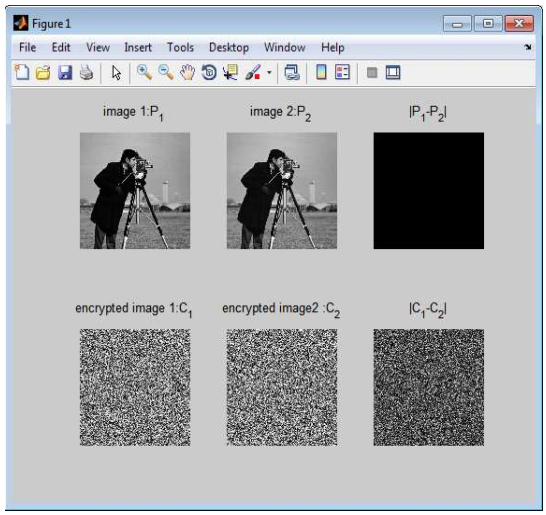

Fig. 7. NPCR

4. CONCLUSION

This work proposes a novel algorithm for enhanced image security with reversible data hiding in a separable manner. The algorithm has mainly four like image encryption, data hiding, data extraction and image recovery phases. The proposed image encryption method adopts a 2D logistic map permutation-substitution network structure with good confusion and diffusion properties instead of 1D approach [1]. This increases the image encryption quality. Instead of directly embedding data into cipher text image this method encrypts the data by means of AES algorithm for ensuring double layer security. The cipher text image obtained from the proposed image cipher has strong resistance to all known attacks. Simulation results of using several security analysis methods like the conventional histogram analysis, key space analysis, the key sensitivity analysis, the information entropy test, shows the effectiveness, resistance and robustness of the proposed algorithm[1].

ACKNOWLEDGEMENT

First of all, I would like to take this opportunity to thank God Almighty for his blessings and for helping me to complete the work successfully. I would like to express my gratitude towards Dr.Deepti Das Krishna, for her constant encouragement and support. I am also grateful to my guide Ms. Rinju Mariam Rolly for her kind guidance.

REFERENCES

[1]Y.Wu, G.Yang, H.Jin and J.P. Noonan, "Image Encryption using the Two-dimensional Logistic Chaotic Map", Journal of Electronic Imaging, January 2012

[2]K.Ma, W.Zhang, X.Zhao, N.Yu, and F.Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" IEEE transactions on information forensics and security, vol. 8, no. 3, march 2013

[3]A.K.Mohan, S.M.R and K.Anusudha, "Improved Reversible Data Hiding Using Histogram Shifting Method", Signal Processing, Informatics, Communication and Energy Systems (SPICES), IEEE Conference, 2015.

[4]J.Daemen and V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, September 3, 1999

[5]J.Gupta, P.Gupta, S.C.Gupta, "Reversible Data Hiding Technique Using Histogram Shifting", 2nd International Conference on Computing for Sustainable Global Development (INDIA Com), 2015

[6]M.Nosrati, R.Karimi and M.Hariri, "Reversible Data Hiding: Principles, Techniques, and Recent Studies", World Applied Programming, Vol (2), Issue (5), May 2012. 349-353 ISSN: 2222-2510