DYNAMIC CRYPTOGRAPHIC AUTHENTICATION APPLIED REVERSIBLE DATA HIDING BY RESERVING ROOM BEFORE ENCRYPTION

Niranjana.K[1], Ramkumar.M[2], Kothaima.K[3]

[1]*PG Scholar (M.E)/CSE, Knowledge Institute of Technology, Salem, TamilNadu, India*
[2]*Assistant Professor/CSE, Knowledge Institute of Technology, Salem, TamilNadu, India*
[3]*UG Scholar (B.E)/CSE, Hindusthan Institute of Technology, Coimbatore, TamilNadu, India*

Abstract

In the emerging technologies, confidential information needs some authentication for access through internet. Cryptography plays an important role to transfer the data using different algorithm with privacy key to hide the original data through network. All data hiding method based on different schemes are used to image encryption and then data hiding in image using cryptographic keys otherwise using password. Reversible data hiding method provide security to transfer secret data by encrypted the carrier image and embedded the original data in image. In existing method, using RDH algorithm based on reserving area prior to encryption for security purpose. By the way of recovering the original data, there is possibility of hack the keys used for encryption and embedding process. In proposed method, provide authentication to recover the carrier image by allows only receiver to retrieve the original data across servers to prevent from hackers. It maintains confidential production that the original data can be extracted after data binding process with secret password authentication. To overcome the difficulties of existing process which may subject to increase the security, this project proposes a confidential method by reserving room after encryption with dynamically producing a password. This process can extract and embed the data without any error. In addition to that, the security of our data hiding is high when compare with other hiding approaches related to confidential.

Keywords: *Dynamic cryptographic authentication, Reversible data hiding, Image encryption, Histogram shift, confidential production.*

----------***----------

1. INTRODUCTION

Reversible data hiding (RDH) is a technique for transfer the secret information from owner to concern receiver by using carrier as image. This method provides privacy production to transfer the data through internet by which the original data can be encrypted image before and after hiding of data. Now a day, this is used in information and forensics, highly confidential government document, employee profile information and bank account details. Therefore, confidential and authentication plays important role to transmit the secret data through networks. The hiding technique encrypts the image using various encryption methods and using cryptographic keys then embed the secret data in image. The secret data may be in any format. Finally, the authorized user gets the image and applies the same technique as reverse to extract the image and secret data. In this technique, researchers are interested to increase the quality of carrier image, provide the security to hiding process and complete the whole process without any error. For example, hiding secret data from hackers, illegal users, terrorists and unauthorized persons in the stage of passing the secure information requires for the applications of share through interest, company document, highly protected military data and privacy information of individual person.

There are many approaches should be added to reversible data hiding techniques. Kyung-Su Kim *et al.* [5] constructed a sub–sampled image. Based on this process, the histogram modifies between the coefficients of sub-sampled images. It achieves the storage for hiding the data in the pixels and useful for embedding process. Shifting of histogram is one of the schemes used for limiting the storage in [8]. Pixels can be calculated to embedding of image. Modification can be done from peck to zero pixel values and achieving the quality of image after embeds the data.

In many aspects, Modification of histogram based data hiding scheme uses the value of peak point to hide the secret data. This method proposes by chia-chen Lin *et al.* [2] to minimum the distortion while hiding the data. Here, multilevel reversible data hiding framework generated to maintain the storage area for hiding and perform nine stages to explore the higher storage hiding such as cousin transform. In [3], the carrier

image divides into two blocks. Based on the thresholds, the categories may be differentiating to embed data only in any two categories. This process improves not only the quality of carrier image but also provides higher storage capacity payload. While measuring the ability of embedding process the values always more than 1 bit/pixel. According to optimal codes based data hiding [9], the embedded data in the area of smooth block and calculate the embedded space by difference of vertical and horizontal pixel values. Therefore, the extraction of data can be correctly recovered by using the smooth block to improve the hiding schemes.

In relevant aspects, Wien Hong *et al.* [10] using neighboring pixels to evaluate the smoothness of carrier image after embedding process. Based on these observations, the changes made in smoothness can be noticed to perform the extraction and data recovery process. Besides, the separation in data hiding [14] can be done for providing security for encryption and then encrypted image in lossless manner because of compression. Here, the image may be in gray scale after encryption. Focus on previous methods, Ju-Yuan Hsiao [1] established a block based reversible data embedding for RDH applied to gray scale image and instead of using normal block; smooth block can be used to hide the data.

2. PREVIOUS WORK

The proposed method in [10] can be allocated the space after the encryption phase by using vacating room after encryption. By using this framework, an owner of the content encrypts the image using different ciphers. After encryption process, the image is used by data hider process. The data hide by using keys with vacating the room without any loss of data and then send the image to the receiver or else the image stored in their own database. Suppose the stego image transferred to receiver that is third party authorized person through the internet need some authentication for security purpose. Because the hackers are waiting for hack the image in between them to use different techniques. If they trace the encryption and data hiding keys then easily retrieve the data and finally recover the image with any modification. To overcoming this problem in vacating the space while the hide the data in image [1] introduce the new framework that is reserve the rooms before encryption. This framework reserves the space with the help of LSB technique and process by owner of the content because of security purpose. Then data embed in image by using data hiding key in addition to that, use self-reversible embedding algorithm and transfer the data to the receiver. There are two problems can be identified as follows:

- Before encryption process, spaces to hiding data can be allocated. But there is no security can be providing for allocation process.
- By transfer the stego image from client to server. Then receiver retrieves the data by using encryption key and recovers the image by using data hiding key with any error. Here, authentication cannot be introduce while transaction.

In all methods of [10]-[13], generating gray-scale images by encrypts each bit with cipher keys to embed the data in that image. The encrypted image divided into number of blocks *b* x *b*; each block added with 1 bit. Then, the data hiding keys are random can be generated by using pseudo-random number generator.

Hong and chen *et al.* [10] error can be reduced compared to Zhang's method [13] by exploiting smoothness of every block with the help side match. By calculating the difference between two blocks used to recover and extract the blocks. Zhang's method in [14] divides the image after encryption into number of smaller groups *G* and in encryption process done by calculating random numbers.

$$B_{i,j,v} = b_{i,j,v} \oplus r_{i,j,v}$$

$r_{i,j,v}$ denotes the encryption key and $B_{i,j,v}$ denotes the order of encryption. In embedding process, use of parameter embeds in the image pixels with LSB technique.

3. PROPOSED METHOD

To proposes the novel method with security and the receiver's authentication purpose. Protocol can be applied in RDH to authenticate the receiver while retrieving the stego image because the receiver may be a hacker, owner of the content and third party authenticators. So need to verify the person who receives the image. Here, single password protocol (SPP) used in the transaction process by giving password to transfer the data. Then the password can be changed dynamically by using pseudo random number generators (PRNG). Suppose the intermediate unauthorized user hack only fake password that is generated by PSNR algorithm. Only the receiver gets the stego image which is transferred by the content owner.

3.1 Generation of Encrypted Image

Reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks into encrypted images would be more natural and much easier which leads us to the novel framework, "RRBE". The content owner first reserve enough space on original image and then converts the image into its encrypted version with the encryption key.

To construct the encrypted image, the first stage can be divided into three steps: image partition, self-reversible embedding followed by image encryption. Note that after image encryption, the data hider or a third party cannot access the content of original image without the encryption key, thus privacy of the content owner being protected.

3.2 Image Encryption

A number of secure stream cipher methods can be used here to ensure that anyone with the encryption key, such as a potential attacker or the data hider, cannot obtain any information about original content from the encrypted data. Although someone with the knowledge of encryption key can obtain a decrypted image and detect the presence of hidden data using LSB methods, if he does not know the data-hiding key, it is still impossible to extract the additional data and recover the original image.

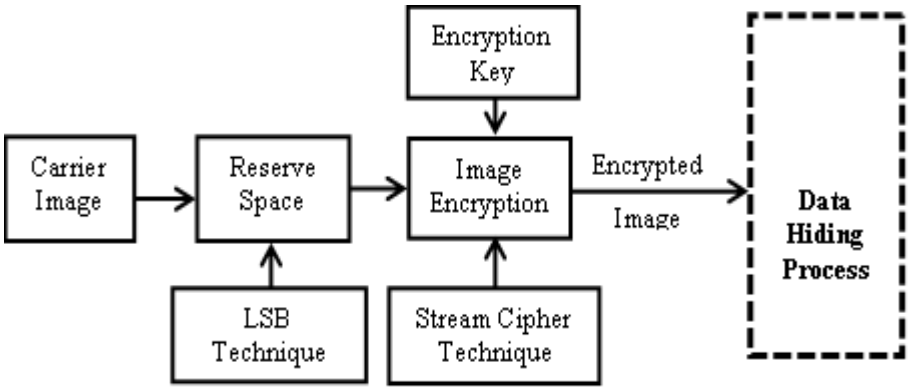

Fig -1: Sketch of content owner to allocate space for hiding data in image.

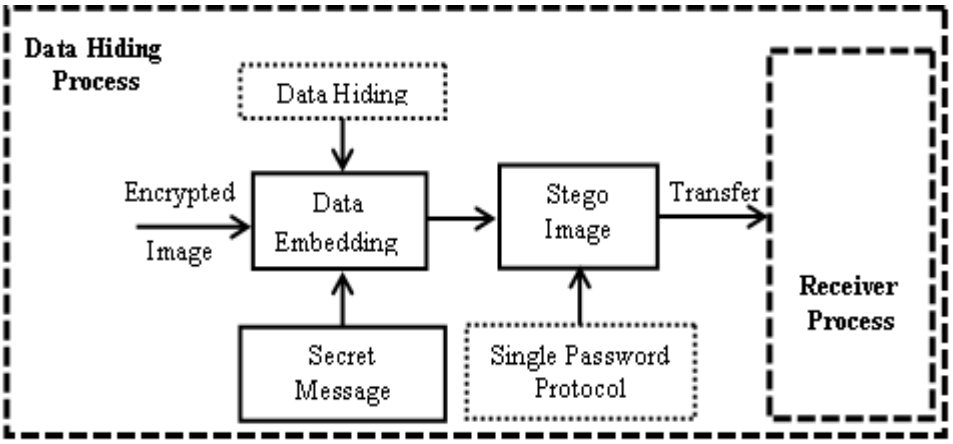

Fig -2: Data hiding using password generated by single password protocol.

3.3 Data Hiding Using Single Password Protocol

Based on manipulating, the least-significant-bit planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity, but unfortunately LSB insertion is vulnerable to slight image manipulation such as cropping and compression. Protocol applied in RDH based reserving room before encryption allows a client to securely use a single password across multiple servers, and prevents phishing attacks. The protocol [7] achieves client authentication without the client revealing his password to the server at any point. Therefore, a compromised server cannot steal a client's password and replay it to another server.

3.3.1 Algorithm:

Step 1: Initially, Using the data hiding key *dk* to hide the secret data in the carrier image.
Step 2: Hiding key combines with a Diffie Hellman algorithm to encrypt the key and generate shift key *hk*.
Step 3: The key *hk* transfer to the password process for security purpose.
Step 4: After the data hiding process, transfer the image by using a single password protocol.
Step 5: Password can be encrypted by using secure hashing algorithm (impossible to decrypt the password in the receiver side) and then transfer the encrypted password to the database.
Step 6: Authenticate the receiver by using a password and then receive the encrypted image.

Step 7: Decrypt the image by using Encryption and data hiding keys.
Step 8: Finally, extract the secret data which embed in the image.

3.4 Dynamic Authentication Process

Password can be given in the data hiding process to improve the security level because if the hacker knows the encryption and hiding key then hacker can retrieve the original data with extraction of image. By using the dynamic password authentication, the receiver only allow to extract the image. Others are unable to retrieve because here password can be change dynamically. So that password can be used in both processes of data extraction and data hiding. In Receiver part, initially authenticate the user by login using single password protocol. This password should be given in the data hiding process and then encrypt the password by using Secure Hashing Algorithm (SHA).Then encrypted password allow to save in database. So that, impossible to decrypt the password by unauthorized users because of using SHA. The Sender only allows hiding the data in image and receiver only extract the data from the image by using the corresponding password which is used by the sender for that image.

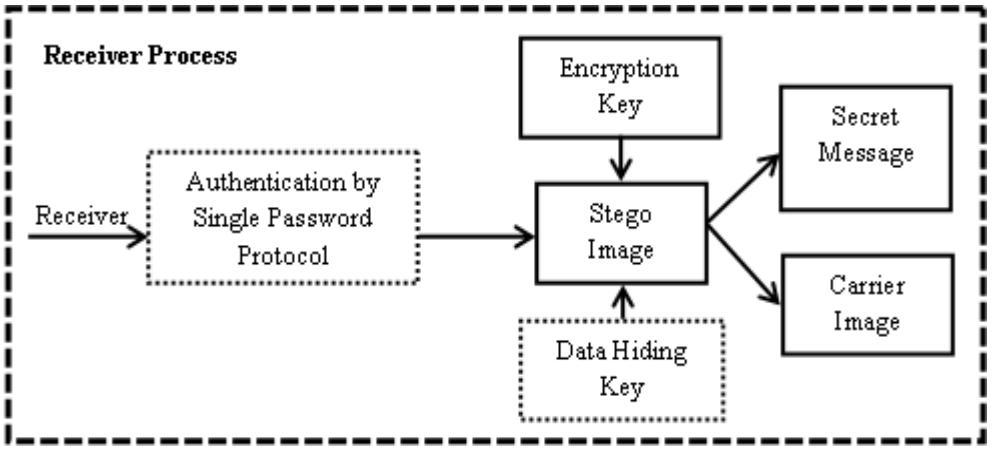

Fig -3: Receiver Authentication Process

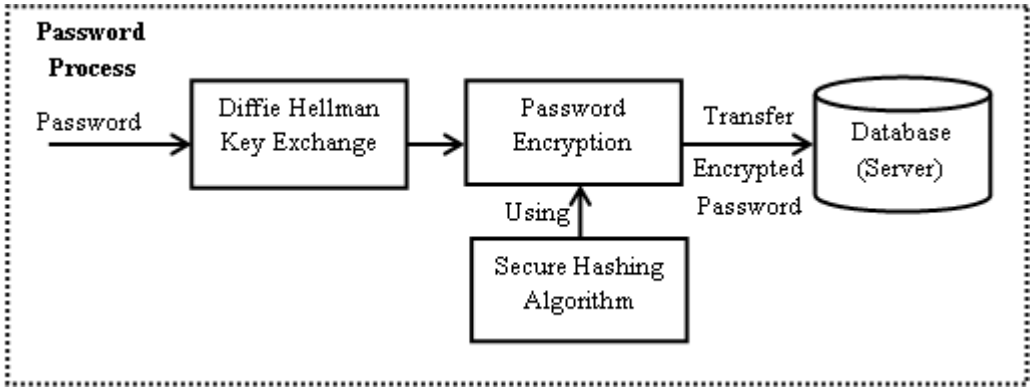

Fig -4: Single Password Protocol Process

3.5 Data Extraction and Image Recovery

In this module, it will consider the three cases that a receiver has only the data-hiding key, only the encryption key, and both the data-hiding and encryption keys, respectively. Note that because of the pseudo-random pixel selection and permutation, any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data. Furthermore, although the receiver having the data-hiding key can successfully extract the embedded data, he cannot get any information about the original image content. Then, the receiver will extract the embedded bits and recover the original content from the encrypted image as shown in fig.3. Finally, concatenate the extracted bits to retrieve the additional message and collect the recovered blocks to form the original image.

4. EXPERIMENTAL RESULT

While hiding the data in the image, using a histogram to find the changes of encrypted image pixels compared to the original image. After recovering the carrier image in receiver side, that image cannot be same as the original image. Peak signal-to-ratio (PSNR) algorithm is used to find the quality of image which is recovered from the receiver side. In the proposed method, the PSNR value is 11.2508 dB.

5. CONCLUSIONS

Reversible data hiding based on reserving room before encryption is a novel method for hiding the data in image using encryption and data hiding keys to secure transfer of original data from owner to receiver. To improve the security level, using a password in the phase of data hiding and data extraction processes. Based on the single password protocol, the password can be changed dynamically. Other user's hacks the keys used for encryption and extraction, then they can easily retrieve the original data hide in the image. To overcome this problem, the protocol used in this project allows only receiver can extract the image and get the original data. So authentication can be applied due to changing of rooms at runtime and improve confidence while receiving the original data. In this project, the data owner can encrypt the image before that reserve the room for data hiding process. After encryption, password can be used for hiding the data in the encrypted image. Here, authentication requires for retrieving the data and extract the image. Using the single password protocol for confidential and authentication purpose. Furthermore, improve the real reversibility for using any image as a carrier image to enhance the environment reality purpose.

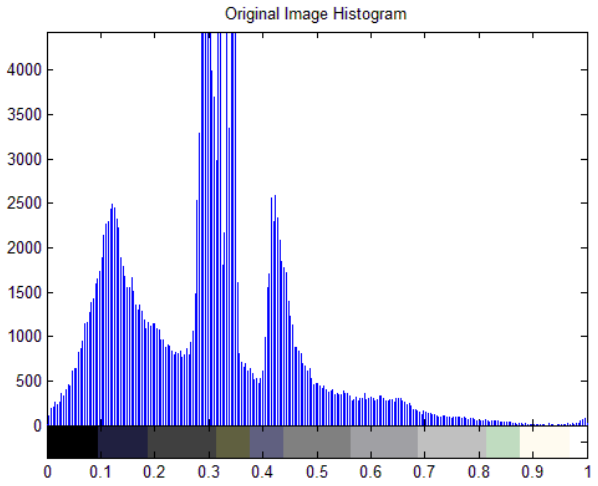

Fig -5: Histogram of original Image

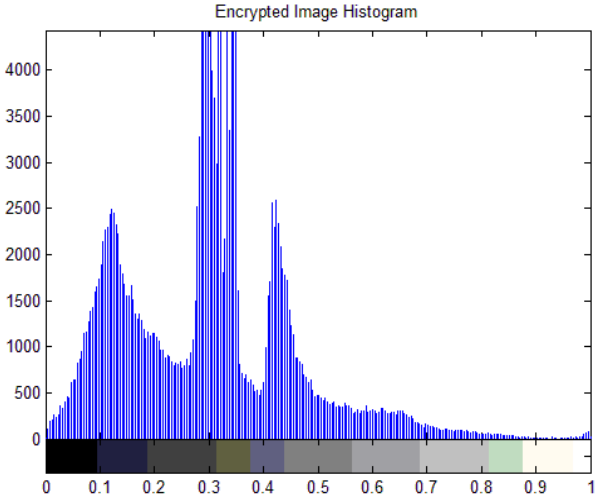

Fig -6: Histogram of Encrypted Image

REFERENCES

[1]. K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[2]. Chia-Chen Lin, Wei-Liang Tai, Chin-Chen Chang, "Multilevel reversible data hiding based on histogram modification of difference images," Elsevier on Pattern Recognition 41 (2008) 3582 – 3591.

[3]. Ju- Yuan Hsiao, Ke- Fan Chan, J. Morris Chang, "Block-based reversible data embedding," Elsevier on Signal Processing 89 (2009) 556–569.

[4]. J.Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[5]. Kyung-Su Kim, Min-Jeong Lee, Hae-Yeoun Lee, Heung-Kyu Lee, "Reversible data hiding exploiting spatial correlation between sub-sampled images,"Elsevier on Pattern Recognition 42 (2009) 3083 – 3096.

[6]. Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Z.Xiong, "Reversible Image Watermarking Using Interpolation Technique," IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, March 2010.

[7]. Mohamed G. Gouda, Alex X. Liu, Lok M. Leung, Mohamed A. Alam, "SPP: An anti-phishing single password protocol," Elsevier on Computer Networks Volume 51, Issue 13, 12 September 2007, Pages 3715–3726.

[8]. Piyu Tsai , Yu-Chen Hu, Hsiu-Lien Yeh , "Reversible image hiding scheme using predictive coding and histogram shifting," Elsevier on Signal Processing 89 (2009) 1129–1143.

[9]. Weiming Zhang, Biao Chen, and Nenghai Yu, "Improving Various Reversible Data Hiding Schemes Via Optimal Codes for Binary Covers," IEEE Transactions on Image Processing, vol. 21, no. 6, June 2012.
[10]. W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett, vol. 19, no. 4, pp. 199–202, Apr. 2012.
[11] Xinpeng Zhang, "Reversible Data Hiding with Optimal Value Transfer," IEEE Transactions on Multimedia, vol. 15, no. 2, February 2013.
[12] 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, Dec. 2011.
[13]. X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
[14]. X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[15]. Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.