RDH in Image with Asymmetric Key Cryptography

S.A.Vajiha Begum[1]
[1]M.Phil Scholar, Computer Science, Mother Teresa Women's University Kodaikanal,India
vajihabegum7391@gmail.com

Dr. M.Pushpa rani[2]
[2]Professor and Head,Department of Computer Science ,Mother Teresa Women's University Kodaikanal, India
drpushpa.mtwu@gmail.com

***Abstract*—** Reversible Data Hiding technique (RDH) is an approach to embed secret data into the encrypted original cover image. The confidentiality must be there when the secret media is transmitted to the receiver via network. This paper proposes a new framework for embedding the secret data into the image with the combination of RDH technique with asymmetric key cryptography to gain high security. It achieves perfect extraction of data and quality original image retrieval on decryption process. Thus this system will gain maximum efficiency and maintain high secrecy for both data and image than the existing RDH systems.

Keywords- *Reversible Data Hiding (RDH); secret data; asymmetric key; cover image; embedding; encryption*

*****

I. INTRODUCTION

Reversible data hiding (RDH) method helps to embed secret information into an original cover image in a reversible manner. On the receiving side, the hidden secret information can be extracted and the original image perfectly restored without error. This RDH technique is particularly useful in applications such as medical imaging, military and confidential transmission, where the original cover image must not be distorted after the embedded secret data are extracted [1][2]. This method emphasizes quality image reconstruction and data extraction than the existing watermarking systems.

Reversible data hiding method combines three processes such as encryption of original image, embedding secret data into the encrypted image and decryption of embedded image for the retrieval of original cover image and secret data extraction without any loss. For maintaining secrecy here we implement asymmetric key cryptography RSA algorithm with RDH method. RSA is one of the first workable public-key cryptosystems and is widely used for secure data transmission in network. In this cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described this algorithm in 1977. It is very hard to break the RSA encryption because of using two large prime factors as key [6]. Data hiding can also be used for various purposes such as for copyright, data integrity, authentication of image and fraud detection.

II. REVIEW OF LITERATURE

Jui Tian et al [3] have proposed a difference expansion technique which gives extra storage space by inquiring the redundancy in the image content. The secret data embedding capacity and the visual quality of decrypted images of the difference expansion method are among the best, along with a low computational complexity.

Wen-Chung Kuo et al [4] has proposed a method of adaptive reversible data hiding based on histogram technique and slope method which enhance the data hiding capacity and embedding point flexibly. This method ensures high embedding capacity and also maintains the high quality of stegno-image.

Vivek Jain et al [5] have proposed a technique to implement steganography and cryptography to hide the secret data inside the image. Here the original secret data will be encrypted by the stego key which is created and exchanged by using Diffie Hellman key exchange protocol. The LSB of selected pixel is taken for hiding the data. The receiver with shared stego-key only can extract the secret data embedded in the image. Thus it will guarantee more security to the embedded data.

III. EXISTING SYSTEM

A technique for Reversible Data Hiding in Encrypted JPEG Bitstream has been introduced by Zhenxing Qian et al [1] by preserving the bit stream structure. The secret data bits are encoded with ECC and embedded into the encrypted bit stream by altering the appended bits related to the AC coefficients of the DCT functions. He has chosen suitable functional bits for data hiding so that the encrypted bit stream carrying secret data can be perfectly decoded. The secret bits are encoded with error correction codes to achieve a faultless data extraction and image recovery. By using the encryption key and embedding keys, the receiver can extract the embedded secret data by inspecting the blocking objects of the adjacent blocks and perfectly restore the original image.

The receiver with encryption key only can recover approximately the original image without extracting the secret data. This method ensures high embedding capacity

and quality image recovery. All previous approaches were considering embedding capacity and image recovery while maintaining less confidentiality for both data and image. The sharing of private key between sender and receiver creates less privacy in the existing system. Thus the new framework has been proposed to gain maximum security than existing RDH systems with the use of RSA key generation algorithm.

IV. RDH IN JPEG IMAGE WITH ASYMMETRIC KEY CRYPTOGRAPHY

The proposed method combines the Reversible Data Hiding technique with the use of asymmetric key cryptography in images. This approach will give maximum security than the existing techniques in the area of reversible data hiding. The proposed system has four phases which are shown in figure1, are as follows:

- Asymmetric key generation phase
- Image encryption phase
- Data embedding and hiding phase
- Data extraction/Image recovery phase

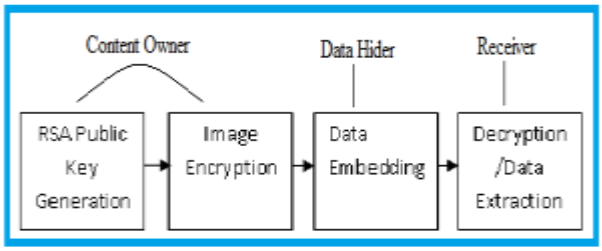

Figure 1: Four phases of proposed system

The three parties used in the four phases of this system are content owner, data hider and receiver. The works of these three parties are as follows:

a) ***Content Owner*****:** public key and private key is generated using the RSA public key algorithm. Then the original image bitstream is parsed and encrypted using Public key to cover the principal content of the original image. The same structure is managed for encrypted bitstream as the original bitstream, so that it can be decoded correctly to give an accurate image.

b) ***Data hider:*** Embed the secret data into the encrypted bitstream by using the embedding key for security. Suitable positions for data hiding are chosen and secret bits are embedded with error correction codes (ECC).

c) ***Receiver:*** Extract the secret data and recover the original image bitstream. With both the private key and embedding key, the secret data bits are extracted and the original image is perfectly restored. If the receiver only has the public key, an image can be obtained approximately.

ASYMMETRIC KEY GENERATION

Asymmetric key cryptography helps high secure transmission of private secret information over insecure channels. Here we consider RSA public key cryptography system for secure transmission of data. Before encryption of cover image the public and private key is generated with the help of RSA –public key cryptography. Here the public key is used for encryption of the cover image while for the decryption of the image private key is used.

RSA Key Generation Algorithm

B. Choose two large prime numbers p and q.

C. Calculate n = p * q and ϕ (n) = (p-1)*(q-1).

D. Choose an integer e, such that e is co- prime to ϕ (n).

E. Compute the secret d such that (d *e) mod ϕ (n) =1.

F. Now, the public key is (e, n) and private key is (d, n).

G. The sender can encrypt the message P as C = Pe mod n.

H. The receiver can regenerate the message P as P = Cd mod n

As the calculation of the secret d from public key (e, n) is quite difficult, this algorithm resists the general attacks. Hence, it is measured to be a secured algorithm.

IMAGE ENCRYPTION:

In Image Encryption phase the original image is encrypted using the RSA public key. In this phase we have to perform two operations such as bitstream parsing and then bitstream encryption. The process of image encryption phase is shown in figure 2.

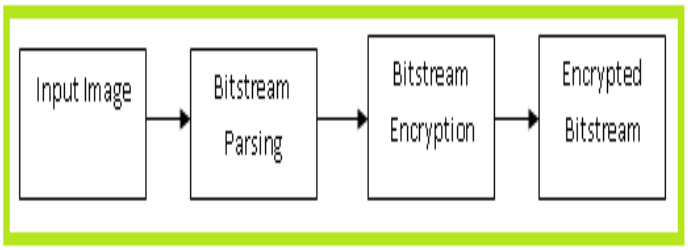

Figure 2: Shows the process of image encryption phase.

First the original JPEG bitstream is parsed and the information is stored in a structure. The information contains quantization and Huffman coding tables are stored in the JPEG file header, which are need for both entropy encoding and decoding. After bitstream parsing of JPEG image we can start encoding the parsed bitstream. The parsed bitstream can be decomposed to a set of quantized DCT coefficients in non-overlapped 8X8 blocks, and then coded into a bitstream with entropy encoding [7]. The DC coefficients and the AC coefficients are handled separately during entropy encoding.

The DC coefficients are coded with the Huffman codes. For AC coefficients, since there are many zeros, the coefficients are efficiently encoded with the run length coding (RLC). Then the quantization tables stored in the JPEG file header is encrypted by extracting the binary bits corresponding to it and replaced with pseudo-randomly generated bits. Thus the above process generates the encrypted bitstream. The file structure and the Huffman codes should be kept unchanged for the purpose of decoding.

DATA EMBEDDING AND HIDING:

Data Hider chooses the suitable positions for data hiding by using blocking artifact function, which will be used during data extraction and image recovery and the feasible embedding capacity are calculated. By using Error Correction Codes (ECC) the plain data bits are encoded before data embedding. All the AC coefficient blocks with zero value is avoided for data embedding. The usable blocks are selected for data embedding. The data hider can embed one secret bit into the AC coefficient of the selected usable blocks. Thus the data embedding process is completed and the encrypted image containing secret data generated and sent to the receiver.

DATA EXTRACTION/IMAGE RECOVERY:

On receiving side the receiver receives the encrypted image containing secret data. The receiver with both embedding key and private key can extract the secret data and the original JPEG bitstream by analyzing the blocking artifacts of the neighboring blocks AC coefficient. Low Density Parity Check (LDPC) codes algorithm can be used to ensure correct extraction of the secret data. Although someone with the knowledge of data embedding key can detect the presence of hidden data, since he does not know the private key, it is still impossible to recover the original image.

RESULTS AND DISCUSSIONS:

The result of the two phases of the proposed method RDH in images with the asymmetric key cryptography is shown below. The generations RSA public and private key are shown in Figure 3. The original image before encryption and encrypted JPEG bitstream is shown in the figure 4.

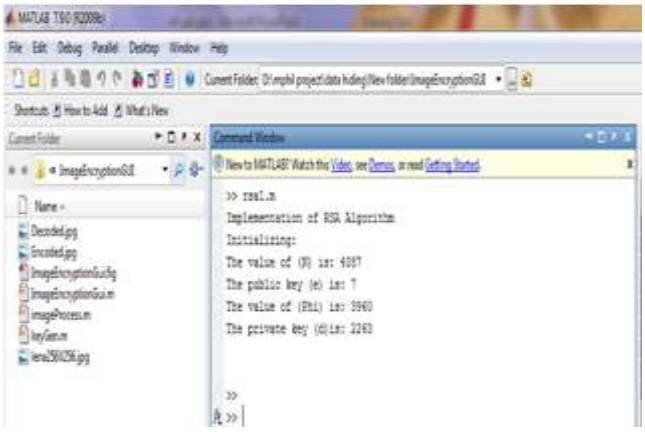

Figure 3: Generation of RSA public key and private key

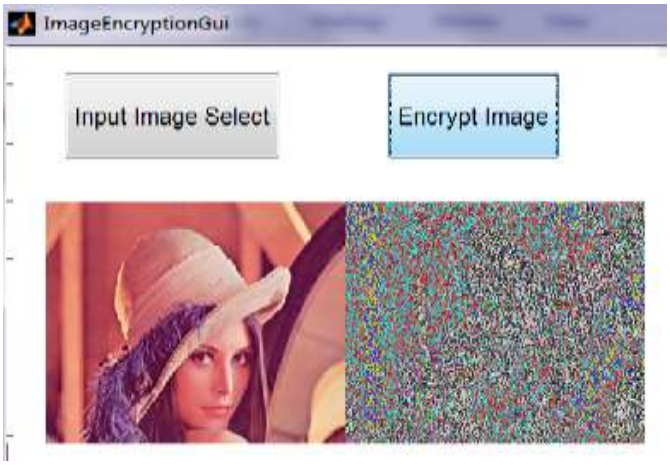

figure 4: Shows the original image and encrypted JPEG bitstream.

V. CONCLUSION

Reversible data hiding in image is paying lots of consideration because of maintaining confidential communication in network. This paper proposed a new method for RDH in JPEG image with combination of asymmetric key cryptography. This system consists of RSA key generation, image encryption, data embedding and data extraction/image recovery phases. The proposed system will give effective data extraction, robustness and high security in the network than the other existing RDH systems.

REFERENCES

[1] Zhenxing Qian, Xinpeng Zhang, Shuozhong Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream", IEEE Transactions on Multimedia, Copyright (c) 2013

[2] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in *Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents*, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

[3] J. Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Trans. on Circuits and Systems for Video Technology, 13(8), pp. 890−896, 2003.

[4] en Chung Kuo, Po Yu Lai, Lih Chyau Wuu, "Adaptive Reversible Data Hiding Based on Histogram", 10th International Conference on Intelligent Systems Design and Application, © IEEE 2010 (2002).

[5] Vivek Jain, Lokesh Kumar, Madhur Mohan Sharma, Mohd Sadiq, Kshitiz Rastogi," Public-Key Steganography Based On Modified Lsb Method", Journal of Global Research in Computer Science, Volume 3, No. 4, April 2012.

[6] www.en.m.wikepedia.org/wiki/RSA_(cryptosystem)

[7] Int. Telecommunication Union, CCITT Recommendation T.81, Information Technology-Digital Compression and Coding of Continuous-tone Still Images-Requirements and Guidelines 1992.