PEER- REVIEWED INTERNATIONAL JOURNAL

Aarhat Multidisciplinary International Education Research Journal (AMIERJ)

ISSN 2278-5655

Bi-Monthly

VOL - II | ISSUES - V | [2013]

Chief-Editor:

Ubale Amol Baban

[**Editorial/Head Office**: 108, Gokuldham Society, Dr.Ambedkar chowk, Near TV Towar,Badlapur, MS

DATA HIDING IN ENCRYPTED IMAGE USING AES AND TWELVE SQUARE SUBSTITUTION CIPHER ALGORITHMS

Sheela Bankar

M.E (Second Year)

Mrunalieeni Patole

Asst.Profesoor

RMD Singhad School of Engineering, Varje

Pune

Abstract –

Now a day a serious business and other types of transaction are being conducted over the Internet. Some secret information is send from one place to other via Internet .We required some kind of security for our data so that intruder cannot capture the data and miss use. Using this proposed method we hide the data and send to receiver using encrypted image .Using this method we provide more security to our data instead of just hiding the data, first encrypt it and then hide. One more advantage of this method is if we compress the image because of limited channel resources by channel provider it will not affect our hide data .With encrypted image also we can transfer the important image . So two way use this method to send the data and to send the image both in secure manner. In the first phase, a sender encrypts the original uncompressed image using an encryption key. Then, a data-hider encrypts the data and may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error .The limitation of this method is that additional data is not too large. Still with these limitations in recent years, signal processing in the encrypted domain has attracted considerable research interest.

Key words-*Data Encryption, Image Encryption, Separable Reversible Data Hiding.*

I INTRODUCTION

For privacy protection of the data, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource. While an encrypted image can be compressed with a lossless manner [3,4]. To encrypt the image AES algorithm can be used because AES based on 128-bit blocks, with 128-bit a key which removes the weakness in DES. This algorithm gives the lot of flexibility and security to the implementers. It also stands up well against cryptanalysis attack. Also this algorithm works well with modern processors.[17].

In [5] Author presented the lossy compression method .There are different methods for data hiding in encrypted domain. In a buyer–seller watermarking protocol [6], the seller of digital multimedia product encrypts the original data using a public key, and then permutes and embeds an encrypted fingerprint provided by the buyer in the encrypted domain. After decryption with a private key, the buyer can obtain a watermarked product. This protocol ensures that the seller cannot know the buyer's watermarked version while the buyer cannot know the original version. In [7] author presents the Okamoto-Uchiyama encryption method for fingerprinting which will improves the enciphering rate. In data-hiding and encryption schemes, a part of cover data is used to carry the additional message and the rest of the data are encrypted, so that both the copyright and the privacy can be protected. For example [8-9], In [10], the content owner encrypts the signs of host DCT coefficients and each content-user uses a different key to decrypt only a subset of the coefficients, so that a series of versions containing different fingerprints are generated for the users. The reversible data hiding in encrypted image is investigated in [11].Figure.1 shows the sketch of scheme which is represented in [11]. In this 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. Most of the

work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain [12-16].

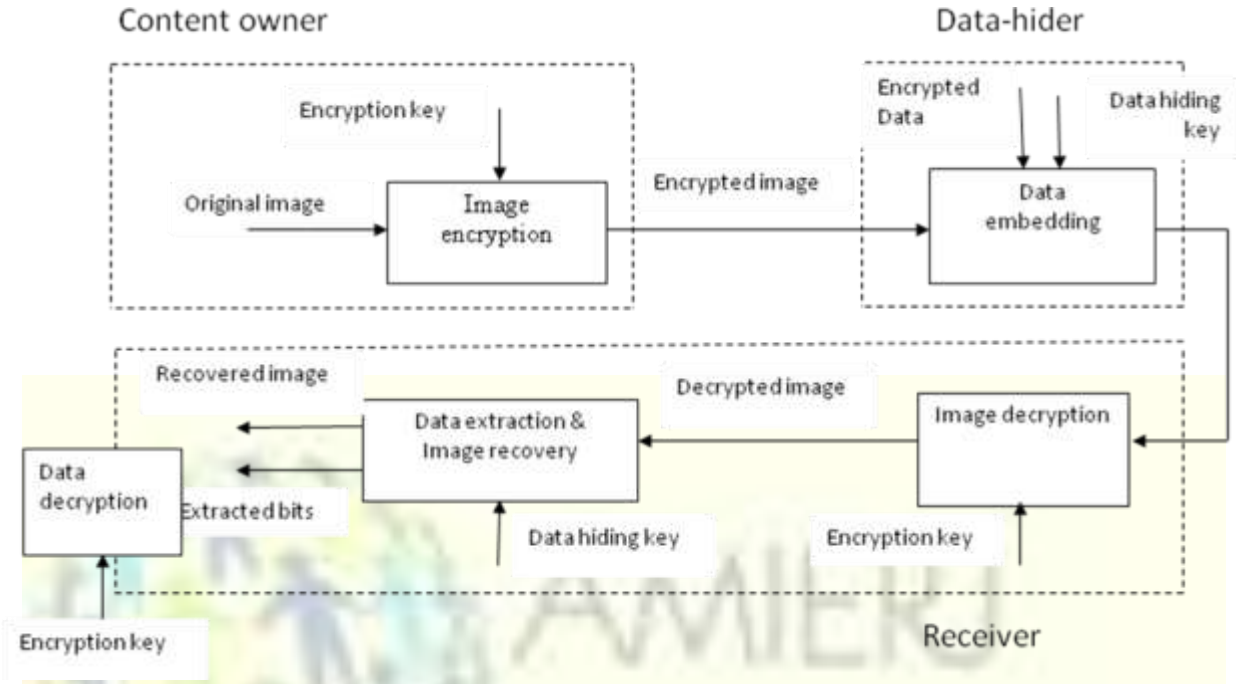

Figure.1.Sketch of non-separable reversible data hiding in encrypted image

II. PROPOSED SCHEME

The proposed scheme is made up of image encryption, data encryption, data embedding and data extraction/image-recovery phases [1]. The sender encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key and using encryption key get the original data. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be recovered. Figure. 2 show the three cases at the receiver side which shows the proposed separable scheme.

A. Image Encryption and Data Encryption.

B. **Assume the original image of size *N1×N2* is in uncompressed format and each pixel with gray value falling into [0, 255] which is represented by 8 bits. Denote the bits of a pixel as $b_{i,j,0}$,$b_{i,j,1}$,.....,$b_{i,j,7}$ where $1 \le i \le N1$ and $1 \le j \le N2$, the gray value as $P_{i,j}$, and the number of pixels as *N(N= N1×N2)* [1]. That implies**

$$b_{i,j,u} = \lfloor p_{i,j}/2^u \rfloor mod\ 2 \quad u=0,1,\ldots,7 \qquad (1)$$

And

$$p_{i,j} = \sum_{u=0}^{7} b_{i,j,u} \cdot 2^u \qquad (2)$$

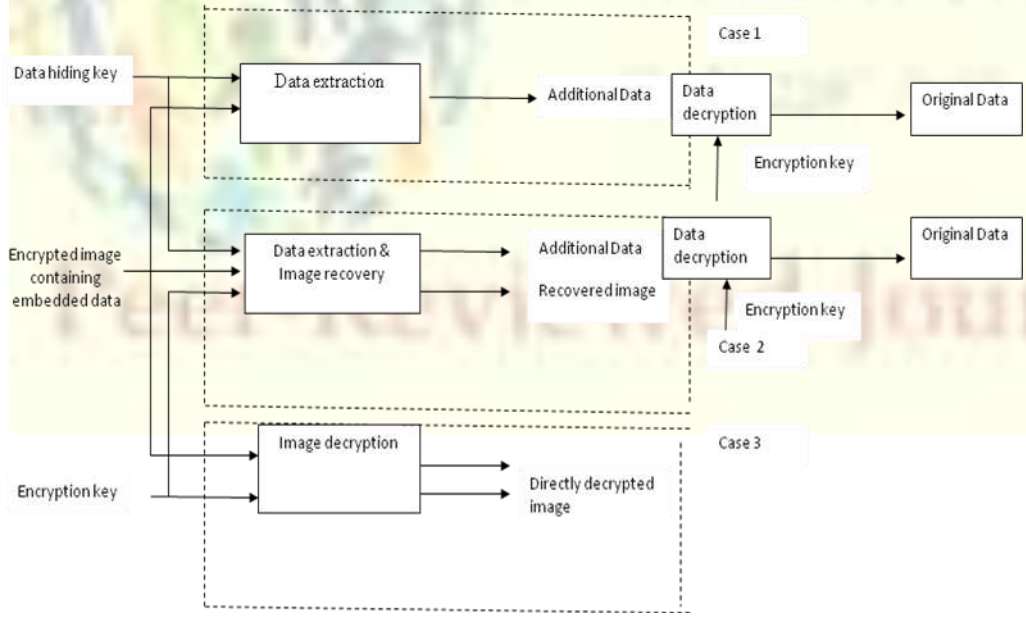

Figure. 2 Three cases at receiver side of the proposed separable scheme.

In image encryption phase in this paper we are using standard AES algorithm to encrypt the original image [17]. Before the data is embedded in encrypted image give more security to

data using encryption. To encrypt the data twelve square substitution cipher algorithm can be used which include alphabets as well as numerals and special characters. In this algorithm first create the six 5 by 5 matrices arrange in square which contain only the alphabets (usually omitting "Q" to reduce the alphabet to fit into the square) and another six 6 by 7 matrices arranged in squares for digits and special characters and remaining six square contain. The twelve-square cipher encrypts alphabets, digits and special characters and thus is less susceptible to frequency analysis attacks [2].

C. Data Embedding

In this phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters. The detailed procedure which is presented in [11, 1] as follows.

According to a data-hiding key, the data-hider selects *NP* encrypted pixels that will be used to carry the parameters for data hiding. Here, *NP* is a small positive integer, for example, *NP* =20. The other *(N-NP)* encrypted pixels are pseudo-randomly permuted and divided into a number of groups, each of which contains *L* pixels. For each pixel-group, collect the *M* least significant bits of the pixels, and denote them as *B(k,1),B(k,2),….,B(k,M . L)* Where k is a group index within [1, *(N-NP)/L*] and *M* is a positive integer less than 5. The data-hider also generates a matrix G sized *(M.L-S)* × *M.L* which is composed of two parts

$$G = [I_{M.L-S} Q] \qquad (3)$$

While the left part is an *(M.L-S)* × *(M.L-S)* identity matrix, the right part Q sized*(M.L-S)*×*S* is a pseudo-random binary matrix derived from the data-hiding key. Here, *S* is a small positive integer. Then, embed the values of the parameters *M, L* and *S* into the LSB of *NP* selected encrypted pixels. For the example of *Np=20* , the data-hider may represent the values of *M,L* and *S* as 2, 14 and 4 bits, respectively, and replace the LSB of selected encrypted pixels with the 20 bits.

In the following, a total of *(N-NP).S/L* bits made up of *NP* original LSB of selected encrypted pixels and *(N-NP).S/L –NP* additional bits will be embedded into the pixel groups. For each group, calculate

$$\begin{bmatrix} B(k',1) \\ B(k',2) \\ \cdot \\ \cdot \\ \cdot \\ B(k',ML) \end{bmatrix} = G. \begin{bmatrix} B(k,1) \\ B(k,2) \\ \cdot \\ \cdot \\ \cdot \\ B(k,ML) \end{bmatrix} \quad (4)$$

B(k,1),B(k,2),….,B(k,M . L) are compressed as *(M.L-S)* bits, and a sparse space is therefore available for data accommodation. Let *[B'(k,M . L-S+1) , B'(k,M . L-S+2), B'(k,M . L-S+2)…. B '(k,M . L)* of each group be the original LSB and additional data to be embedded. Then, replace the *[B(k,1),B(k,2),….,B(k,M . L)]* with the new *[B'(k,1), B'(k,2),….,B'(k,M . L)]* and put them into their original positions. the (8-*M*) most significant bits (MSB) of encrypted pixels are kept unchanged. Since *S* bits are embedded into each pixel-group, the total *(N-NP).S/L* bits can be accommodated in all groups.

C .Data Extraction And Image Recovery

According to the Figure.2 at a receiver side there are three different cases. In first case with an encrypted image containing embedded data, if the receiver has only the data-hiding key get the embedded parameters and get the extracted bits but in encrypted version. To get the original data he should know the data encryption key [2]. Any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data. Using the data hiding key the receiver successfully extract the embedded data, but cannot get any information about the original image content. In the second case the receiver has the encryption key but does not know the data-hiding key. Clearly, cannot obtain the values of parameters and cannot extract the embedded data. But, the original image content can be roughly recovered by decrypting the image. And finally in the third case if the receiver has all the keys that is image encryption, data encryption, data hiding key he will get the original data as well as original image.

III Conclusion And Future Work

In this paper we discussed separable reversible data hiding in encrypted image, which consists of image encryption, data encryption data embedding and data-extraction/image-recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, data hider can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional encrypted data. The receiver may extract the additional data using only the data-hiding key. When the receiver has both of the keys, can extract the additional data and recover the original content without any error. In this paper we consider lossless compression of image. According to the proposed method which is used in this paper when we change the parameters in embedded phase expected result of PSNR in decrypted image can change. In the future, a image encryption and data hiding compatible with lossy compression deserves further investigation.

References

Xinpeng Zhang "Separable Reversible Data Hiding in Encrypted Image" *IEEE Transactions on Information Forensics And Security*, Vol. 7, No. 2, April 2012

Gandharba Swain, Saroj Kumar Lenka "Steganography Using the Twelve Square Substitution Cipher and an Index Variable" 978-1- 4244-8679-3/11/$26.00 ©

M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.* vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

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.

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

N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, Apr. 2001.

M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2129–2139, Dec. 2005.

S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and Watermarking in video compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.

M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," *Sign Processing: Image Commun.*, vol. 26, no. 1, pp. 1–12, 2011.

D. Kundur and K. Karthik, "Video fingerprinting and encryption Principle for digital rights management," *Proceedings IEEE*, vol. 92, no. 6, pp. 918–932, Jun. 2004.

X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

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

Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354– 362, Mar. 2006.

M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized- LSB data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253–266, Feb. 2005.

W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, "A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification," *Signal Process.*, vol. 90, pp. 2911–2922, 2010.

C.-C. Chang, C.-C. Lin, and Y.-H. Chen, "Reversible data- embedding scheme using differences between original and predicted pixel values," *IET Inform. Security*, vol. 2, no. 2, pp. 35–46, 2008. 2011 IEEE

Kahate A, 2012, CRYPTOGRAPHY *AND NETWORK SECURITY, Tata McGraw Hill Education Private Limited,541pp.*