THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

High Capacity Data Embedding Technique for Separable Encrypted Data Embedding in Encrypted Image

Supriya S. Sonawane
M.E. Student, Department of Computer Engineering
KKWIEER, Nasik, University of Pune, Maharashtra, India
N. M. Shahane
Associate Professor, Department of Computer Engineering
KKWIEER, Nasik, University of Pune, Maharashtra, India

Abstract:
Traditionally, if receiver has encrypted image containing data and he wants to output as extracted data or decrypted image then receiver needs both an image encryption key and a data-hiding key. Here data extraction is not separable from image decryption. If receiver has the data hiding key but not the image encryption key then he cannot extract any data from the encrypted image containing data. This work introduces a new system of separable an encrypted data embedding in an encrypted image. At sender side, a content owner encrypts an original image. A confidential data is encrypted using hybrid cryptography. Then, using BPCS steganography, the encrypted confidential data can be effectively embedded in the encrypted cover image. An encrypted image containing embedded encrypted data is sent to receiver. With an encrypted image containing embedded encrypted data, receiver will get output using this key or combination of keys. Keys are image encryption key, data encryption key, and data-hiding key. Output may image, data or both depend on key/keys because of separable activity. A High capacity of confidential data embedding technique is achieved by using BPCS steganography.

Keywords: *BPCS, Data hiding, Hybrid cryptography, Image recovery, Steganography.*

1. Introduction

In the modern age, Internet is a very prevalent for electronic communication between two computers. Hackers are used many techniques to hack a system and steal data. There are also many types of data attacks. Data should be protected unauthorized users. Security threats are determining and finding solutions to tackle them for data security. Data hiding and Cryptography techniques are used for data protection. Cryptography is accomplished security by encoding data and data is interpreted in non-readable form so that unauthorized persons are unable to read it. In data hiding techniques, data is hidden that is kept secret inside other data. The hidden data is like invisible ink. A presence of data itself is hidden so that no one supposes the existence of the data other than authorized users. The secret data is hidden in a cover image for achieving data security.

This paper proposes a novel scheme of separable encrypted data embedding in encrypted images. A content owner first original image is encrypted by AES algorithm and image encryption key. Data is encrypted by hybrid cryptography (RSA+AES) using a data encryption key (RSA key and AES key). Then, an encrypted data is embedded in an encrypted image by data hider. An encrypted image containing embedded encrypted data is sent to the receiver. At receiver side there are many cases depending on available key/keys to get output that is original data and/or recovered image.

2. Related Work

There are several algorithms are developed in cryptography field. There are two types of cryptography a Symmetric Key Cryptography and Asymmetric Key Cryptography. Symmetric key cryptography uses same key for encryption and decryption for example AES algorithm [1]. Asymmetric key cryptography uses different keys for encryption and decryption for example RSA algorithm.

Numerous methods are developed in data hiding/extracting in encrypted domain. The digital watermarking field, a buyer seller watermarking protocol [2] ensures the seller does not obtain to identify the exact watermarked copy that the buyer receives. So that a seller cannot create copies of the original content containing the buyer's watermark. This watermark embedding protocol supports public key cryptography. Most work of reversible data hiding emphases on the data embedding. In Least Significant Bit (LSB) steganography approach, data is embedded in a cover media [3] where the 8th bit of every byte of the image is replaced with one bit of the secret data which we want to embed. The Least Significant Bit is altered from 1 to 0 or vice versa so there are only some changes in the appearance of the color of that pixel of image. Capacity of embedding data into the image using LSB is low because only one bit data can be embed for set of each 8-bits (1 byte). A hybrid approach of steganography is encrypted data is hidden into the image in 6th, 7th, and 8th bit locations of the darkest and brightest pixels [4]. In pixel-value differencing is developed in [5] where the largest difference value between the other three pixels close to the target pixel is estimated how many secret bits will be embedded into the pixel. Steganography using Bit-planes in this method [6], replaces 0 to 7 bits of image with message bits or 8 bit image data. Here first an image is converted into grayscale and then select the number of bit planes where the data is to be placed. Using BPCS (Bit Plane Complexity Segmentation) Steganography method a more data can be embedded into an image [7].

Non-separable reversible data hiding in encrypted image is presented in paper [8]. A content owner encrypts an original image using an encryption key where as a data-hider can hide additional data into the encrypted image using a data-hiding key. Data hider doesn't have the knowledge of the original content. An encrypted image containing embedded data is sent to receiver. A receiver might first decrypt it by using encryption key and then extract the embedded data and recover the original image according to the data-hiding key. Figure 1 shows Non-separable reversible data hiding in encrypted image. The activity of image decryption is not separable from the activity of data extraction. If someone has the data hiding key but not the encryption key then he is unable to extract any information from the encrypted image containing additional data so this is a non-separable reversible data hiding in encrypted image.

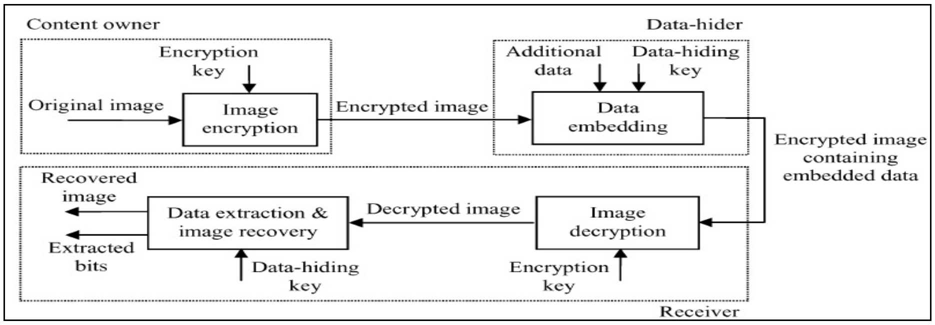

Figure 1: Non separable reversible data hiding Sketch[8].

An innovative scheme of separable reversible data hiding in encrypted image is presented by Zhang [9]. A content owner encrypts the image using an encryption key and a data hider embeds additional data into the encrypted image using a data hiding key and LSB insertion method. A data hider is compressed the LSB bits of the encrypted image to create a sparse space to accommodate some additional data by using a data-hiding key and an encrypted image containing embedded additional data is sent to receiver. Figure 2 shows the three cases at the receiver side. If the receiver has the data hiding key and encrypted image containing additional data then he can extract the additional data but he does not recover the image that is given in first case. If he has the encryption key and encrypted image containing additional data then he can decrypt the image which is similar to the original one but does not extract the embedded additional data is given in second case. In third case, if the receiver has both the keys that are encryption key and data-hiding key as well as encrypted image containing additional data, he can extract the additional data and recover the original image without any error by exploiting the spatial correlation in natural image. This method is applicable when the amount of additional data is not too large.

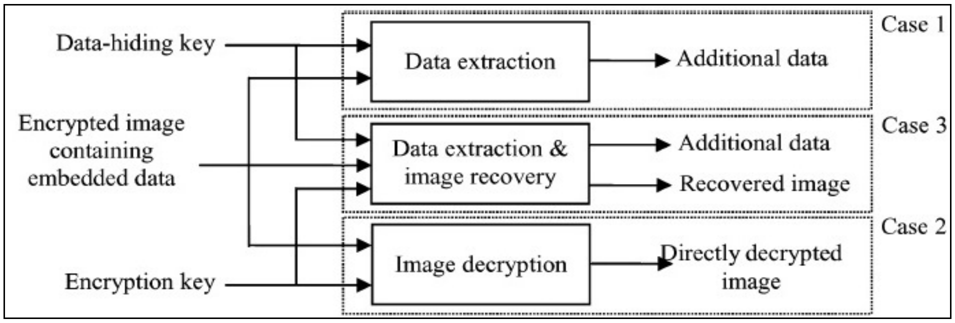

Figure 2: Three cases at receiver side of the separable reversible data hiding in encrypted image scheme[9]

3. Details of System Block Diagram

A novel system for separable encrypted data embedding in encrypted image is proposed. The activities of separation are extraction of payload and extraction of carrier image. The separation exists according to keys. There are number of separation cases to take out the data which was embedded and to obtain the cover image. Figure 3 shows block diagram of the separable an encrypted data is embedding in an encrypted image.

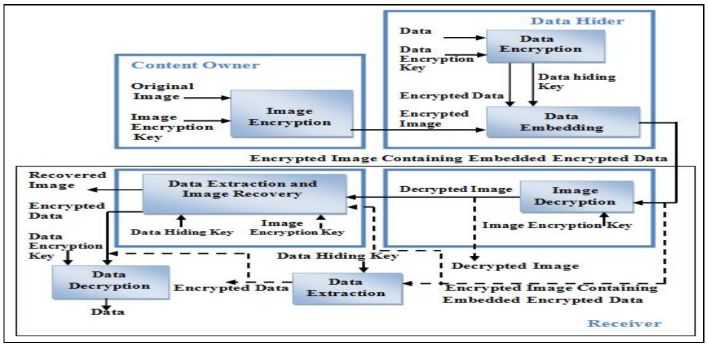

Figure 3: Block diagram of separable encrypted data embedding in encrypted image system

In this proposed method, at sender side, a content owner first an original image is encrypted using an image encryption key. Then a data that we want to embed is encrypted using a data encryption key.Then the data-hider hides encrypted data into the encrypted image using a data-hiding key without knowledge of data content. An encrypted image containing embedded encrypted data is sent. Receiver using encrypted image containing encrypted data and keys there are different cases. In case (a), if he has only the image encryption key then he is able to decrypt the received image and he will get decrypted image that is same as the original one but he cannot extract the embedded data which is in encrypted form. If the receiver has only the data hiding key then he is able to extract the embedded data but which is in encrypted form also he does not know the image content. In case (b), if the receiver has the data hiding key and data encryption key then he can extract the embedded encrypted data and encrypted data is decrypted by using data encryption key, so that get the data which is similar to original data successfully but he is unable to know the image. In the next case(c), if the receiver has both the data hiding key and the image encryption key then he is able to recover the original image without any error and extract the encrypted data which was embedded but this data is in encrypted form. Case (d), if the receiver has image encryption key, data encryption key and, data hiding key then he is able to recover the original image and extract the encrypted data then the encrypted data is decrypted by using data encryption key so he will get the data which is similar to original data successfully. Following Figure 4 shows number of cases according to available key/keys at receiver side to get output.

The proposed scheme is made up of number of phases which are explained below. Original image is encrypted using symmetric cryptography algorithm and data which we want to embed is encrypted by using hybrid cryptography. Encrypted data is embedded within an encrypted image using improved BPCS steganography.

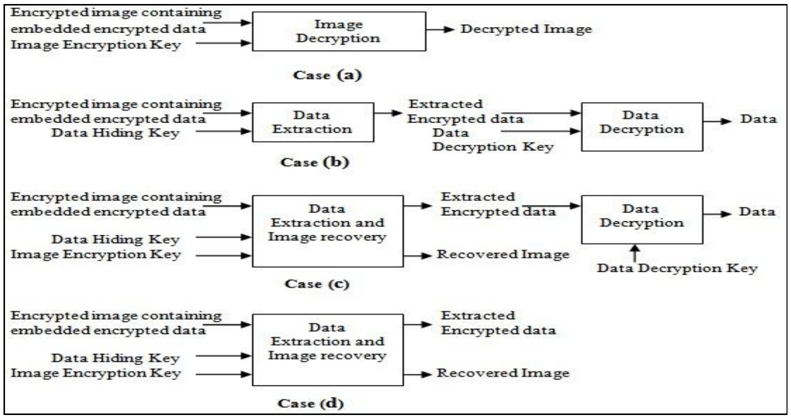

Figure 4: Four cases at receiver side of the separable scheme

3.1. Image Encryption

Original image is encrypted using AES algorithm. Content owner encrypts the original image using an AES image encryption key to obtain an encrypted image. AES used 128 bits plain text, 128 bits key as well as by using 10 rounds and gives 128 bits cipher text. AES is used same key for both encryption and decryption of data/image. The encrypted image using AES image encryption key in sent to data embedding block.

3.2. *Data Encryption*

Hybrid cryptography is new research area in recent years. Hybrid cryptography is combination of symmetric and asymmetric cryptography. Data which want to embed is encrypted by using hybrid cryptography which is combination of RSA and AES algorithm. Data is encrypted using AES data encryption key to get an encrypted data and that AES image encryption key is encrypted using receiver’s RSA public key and RSA algorithm. RSA algorithm is the asymmetric key cryptography so RSA is used different keys for encryption and decryption of message. The private and public keys in RSA are based on very large prime numbers. This algorithm is simple. AES is symmetric key cryptography.

The speed of AES is faster than RSA when encrypting when data/image size is large. RSA is only suitable for encrypting a small amount of data. In RSA algorithm can distribute encryption key openly and keep the decryption keys secret but AES algorithm requires distributing a secret key before communication is more difficult. Also AES need to generate and keep a different key for different communication objects so RSA is better than AES. To give the advantages of the two algorithms by comparing AES algorithm and RSA algorithms form a new algorithm AES and RSA hybrid encryption algorithm. Hybrid encryption algorithm is produced more secure image/data. The entire hybrid encryption process is as: (assuming that the sender and receiver know RSA public key).

The encrypted data using AES data encryption key and encrypted AES key using Receiver's RSA public key are put together is sent to next block that is data embedding block. Here AES image encryption key and AES data encryption key are different.

3.3. Image Decryption

If receiver wants output decrypted image like Figure 4 Case (a) then he has to AES image encryption key. Same AES algorithm which was used by content owner for image encryption and AES image encryption key, receiver decrypts the image and obtains decrypted image same as original image.

3.4. Data Decryption

If receiver has extracted encrypted data and data encryption key then he will get data. Receiver first using its own private key and RSA decryption algorithm decrypts AES symmetric key which was encrypted by receiver's public key. So now receiver gets AES symmetric key. Using AES key and same AES symmetric key algorithm which was used by sender, receiver encrypts cipher text and gets data which is similar to original data successfully.

Using this hybrid approach, the symmetric key of AES is no need to transfer secretly before communication using RSA symmetric key is encrypted. Need to keep only one RSA decryption key secret. Data is encrypted using AES is faster only time consumed to encrypt AES symmetric key using RSA. Under the data transmission will be more secure using dual protection of AES algorithm and RSA algorithm.

3.5. Data embedding

To embed encrypted data in encrypted image BPCS technique is used [7]. The Aim is to embed encrypted data as much as possible into a cover image and balance the quality of stego image and capacity of embedding data. Inputs to this block are encrypted image and encrypted data. Output of this block is encrypted image containing embedded encrypted data.

An image is consisting of bit-planes. Every Bit-plan is divided into small square binary pixel blocks which are shown in Figure 5. Encrypted data which is secret information is embedding in a binary pixel block if a binary pixel block has a complex black-and-white pattern which is noisy region. A pixel consists of RGB component of values from 0 to 255.

- The container image is divided into 8R, 8G, 8B different Bit Planes. There are total 24 plans.Bit-plane blocks are formed by dividing each bit-plane into small blocks of the same size as 8 × 8 bits.
- Determine the complexity α of each binary pixel block. The complexity is determined as the amount of all the adjacent that get different values and that value is either 0 or 1.

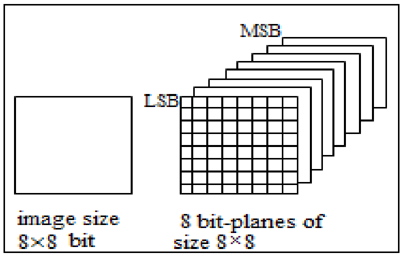

Figure 5: Block of 8×8 bit image and its 8 planes

- 3. This method uses of the more complex regions of an image to embed encrypted data. Assign the complexity threshold of the bit-plane block is max *minAlpha* that is customize parameter.

α = (total length of black-and-white border in the image) / (The max. possible black–white changes in the image) (1)

Where α is image complexity parameter and complexity value range is $0 \leq \alpha \leq 1$

Determine an image complexity α over the whole image which gives the global complexity of a binary image. α can be used for a local image complexity of 8 × 8 pixel size area. If complexity of the bit-plane block is greater than *minAlpha* then it is used to embed encrypted data. Noisy plan has more complexity value than threshold.

- 4. Encrypted data is hidden into bit-plane blocks. If bit plane block's complexity is greater than *minAlpha* then the bit-plane block can replace encrypted data block. It wants to conjugate processing with the white checkerboard pattern block if the block complexity less than equal to *minAlpha* then take the new block replaces the original one.
- 5. Record the all conjugate processing blocks. This record information is also embedded into the encrypted image. The embedding of extra information of conjugate processing blocks cannot effect on the embedded secret data also it must be appropriately select.

The flowchart of BPCS steganography is explained which is shown in Figure 6.

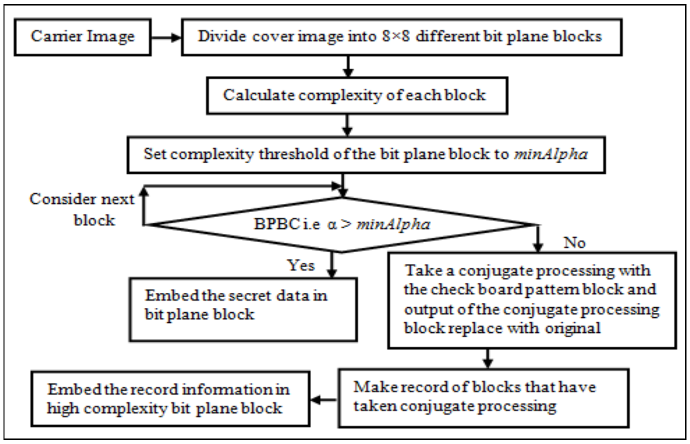
Carrier Image
Divide cover image into 8×8 different bit plane blocks
Calculate complexity of each block
Set complexity threshold of the bit plane block to minAlpha
Consider next block
BPBC i.e α > minAlpha
Yes
No
Embed the secret data in bit plane block
Take a conjugate processing with the check board pattern block and output of the conjugate processing block replace with original
Embed the record information in high complexity bit plane block
Make record of blocks that have taken conjugate processing

Figure 6: Modified BPCS Steganography Flowchart.

3.6. Data extraction/ Image Recovery

The encrypted data extraction is an easy process. Firstly, take all the bit plain block of the original data whose complexity is greater than *minAlpha* and then take the extra-embedded data to verify the blocks that have taken conjugate processing which declared in step (5) of data embedding phase. To get the recovery of encrypted data, these blocks have to take XOR operation with white chessboard block. If receiver has image encryption key and data encryption key to this block then get the output that are encrypted data and recovered image.

4. Result and Discussion

Receiver will get the results according to available key/keys. Result of the existing system is shown in Figure 7. Figure 7(a) is shown an original Lena image. Figure 7(b) shows encrypted Lena image. After that data which wants to embed is also encrypted and an encrypted data embedded in encrypted image is shown Figure 7(c). Figure 7(d) shows output at receiver side as a recovered image. At receiver side gets output as decrypted image, recovered image, and data.

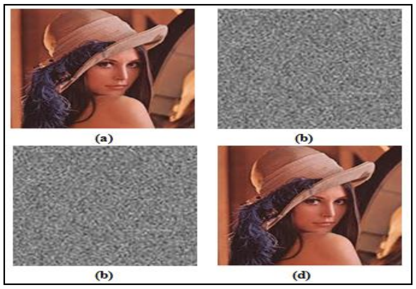

Figure 7: (a) Original Lena image, (b) Encrypted Lena image,
(c) Encrypted image containing embedded data, and (d) Recovered image

Recovered image is better than decrypted image because that decrypted image at receiver side contains some noise. The proposed system will give us better results. Up to 50% data can be embedded into image. In proposed system large data can be embedded using BPCS also image quality is better. Hybrid cryptography is stronger for encryption and decryption of data.

Image quality index used to check quality of image [10]. The image quality is measured by peak-signal to-noise ratio (PSNR). PSNR is used to compare reconstruction results of image requires a measure of image quality. Here signal means original image and noise is called as error in reconstruction.

$$PSNR = 10 \times \log_{10}(\max_I^2 / MSE) db \qquad (2)$$

Where, $\max_I$ = 255 for grayscale images. The mean squared error (MSE) is difference between original to reconstructed image pixels and is defined as:

$$MSE = (1/MN) \times \sum_M^{i=1} \sum_N^{j=1} (|C_I(i, j) - S_I(i, j)|) \qquad (3)$$

Where, M - the number of horizontal pixels, N - number of vertical pixels, C - cover image, and S - a stego image. For the better image PSNR should be greater and MSE should be lower. To check the image quality, Image Quality Assessment is used [11].

5. Conclusion and Future Scope

Strong techniques which are BPCS steganography and hybrid cryptography are used in this novel paper. To secure a data used hybrid cryptography by using RSA and AES algorithm. To secure image used AES algorithm in this paper. To hide a data BPCS steganography is used and degradation in image quality due to data embedding is not noticeable to normal human eye. Sender can make a decision of data embedding capacity also quality of the image because of threshold is customized parameter. BPCS steganography has a high data embedding capacity.

A new system of high capacity of data embedding technique for separable encrypted data embedding in encrypted image is developed in this paper. An image and data are encrypted using an image encryption key and a data encryption key respectively. Without knowledge of the original content, a data-hider hides the encrypted data in the encrypted image with a data-hiding key and sent to receiver. Receiver gets output using key or combination of keys. If he has only image encryption key then he is able to decrypt the received image and get decrypted image that is same as the original one. If the receiver has the data hiding key and data encryption key then he gets only original data successfully. If the receiver has both data hiding key also image encryption key then he gets output as recovered image. If receiver has data encryption key, image encryption key, and data-hiding key then he gets recovered image and data successfully. In future, high capacity data embedding technique separable encrypted data embedding in encrypted image system can improve by embedding encrypted data in video.

6. References

1. Adam Berent, “Advanced Encryption Standard by Example” ,V.1.7
2. N.Memon and P. W. Wong. (Apr. 2001). A buyer-seller watermarking protocol. IEEE Trans. Image Process, vol. 10, no. 4, pp. 643–649.
3. M. S. Sutaone, M.V. Khandare.(Jan 2008). Image Based Steganography Using LSB Insertion Technique. Wireless, Mobile and Multimedia Networks, IET International Conference, pp-146 – 151.
4. Gandharba Swain, Saroj Kumar Lenka. (Dec 2010). A Hybrid Approach to Steganography Embedding at Darkest and Brightest Pixels.Proceedings of the International Conference on Communication and Computational Intelligence – 2010, pp.529-534.
5. Han-ling Zhange, Guang-zhi GENG, Cai-qiongXiong. (2009). Image Steganography using Pixel-Value Differencing. Second International Symposium on Electronic Commerce and Security, pp- 109 – 112.
6. B.Ramesh Kumar, K.Suresh, S.K.Basheer, M. Raja Krishna Kumar. (2012). Enhanced Approach to Steganography Using Bit planes”, IJCSIT, Vol. 3 issue 6.
7. S. Bansod, V. Mane, L. Ragha. (Oct 19-20 , 2012). Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity. International Conference on Communication, Information & Computing Technology (ICCICT) Mumbai, India.
8. X. Zhang. (Apr 2011). Reversible data hiding in encrypted image. IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258.
9. Xinpeng Zhang. (Apr 2012). Separable Reversible Data Hiding in Encrypted Image. IEEE Trans. on Inform. Forensics and Security, vol. 7, no. 2.
10. Z. Wang and A. C. Bovik. (Jan 2002). A universal image quality index. IEEE Signal Process. Lett., vol. 9, no. 1, pp. 81–84.
11. Nisha,S. Kumar. (Jul 2013) Image Quality Assessment Techniques. IJARCSSE,Vol. 3, Issue 7