Secured Separable Reversible Data Hiding In Encrypted Image Using Blowfish Algorithm

Anjum Z. Shikalgar, Namrata S. Powar, Poonam D. Pawar, Prof. S. J. Koparde

***Abstract*— In this novel technique, data is embedded in encrypted image which is additional information in the form of either text or image for the applications such as military, medical images, deductive agencies and bank information sharing. This embedded data and original image can be separately recovered using two separate keys without any loss. There are two phases in this scheme. Firstly content owner encrypts the original image without compressing it using encryption key which is generated by blowfish algorithm then the one who wants to embed or hide the data may be service provider or data hider hides the data using data hiding key provided data can be text or image. At receiver side three cases are possible because of using separate keys i.e. receiver can only decrypt the image if he has only encryption key, only extract the data if he has data hiding key and both the things if he has both the keys. The proposed method uses blowfish algorithm for more security and safe data transmission over the network.**

***Index Terms*— Image Encryption, Data Embedding, Extraction, DWT, PSNR, Blowfish Algorithm.**

I. INTRODUCTION

In present scenario, the transmission of information in the form of digital images is increasing rapidly, so image security has got more attention for the applications such as video surveillance, military, confidential transmission and medical applications. It has become most necessary thing to find an efficient way of transmission of digital images over network since the cases like hacking, data manipulation, fraud and forgery are taking place so it is needed to convert the ordinary data into unintelligible data. Content owner cannot trust service provider, since his ability to manipulate the encrypted data when keeping the plain content is hidden is necessary. While transmission of secret data which is encrypted, there is possibility of compressing the encrypted data by channel provider without any knowledge about keys. Compression can be done in lossless manner by finding the syndromes of low density parity check codes[1], another method is for encrypted gray image using rate compatible punctured turbo codes and progressive decomposition is found[2]. Lossy compression method found in[3], in which gray image is efficiently compressed by removing the extra rough and fine information in[5], method of composite signal representation which involves packing together a number of signal samples and processing them as a unique sample is used to reduce the complexity of computation and the size of encrypted data. In system shown in fig.1, content owner having original image encrypts the image using encryption key, encrypted image is then given to the service provider i.e. data hider. Data hider will hide the additional data text or image using data hiding key. At receiver side, for non-separable technique encrypted image containing embedded data is used for original image decryption using same encryption key and then from decrypted image addition data is extracted using same data hiding key.

Manuscript received March 22, 2015.
Anjum Z. Shikalgar, Dept. of E&Tc, M.M.I.T., Lohgaon,Pune, India
Namrata S. Powar, Dept. of E&Tc, M.M.I.T., Lohgaon,Pune, India
Poonam D. Pawar, Dept. of E&Tc, M.M.I.T., Lohgaon,Pune, India
Prof. S. J. Koparde, Dept. of E&Tc, M.M.I.T., Lohgaon,Pune, India

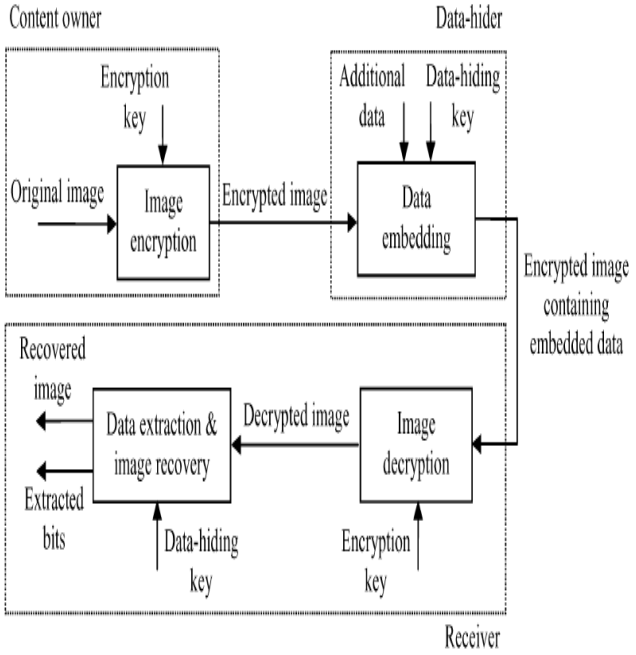


Fig.1. Block Dia. Of Non-separable reversible data hiding

II. PROPOSED SCHEME

The proposed scheme includes modules like image encryption, data embedding, data extraction and image-recovery. The original uncompressed digital image is encrypted using encryption key generated by Blowfish Algorithm at content owner then service provider will use encrypted image for data hiding.

He may compress the encrypted image for data hiding. Additional data can be text or image and embedding can be done using separate data hiding which is also generated using Blowfish Algorithm. At receiver side, three cases exist for separable reversible data and original image extraction. If receiver has encryption key then he can only recover the original image, if it has data hiding key then he can only extract the additional data .As shown in fig.2 below.

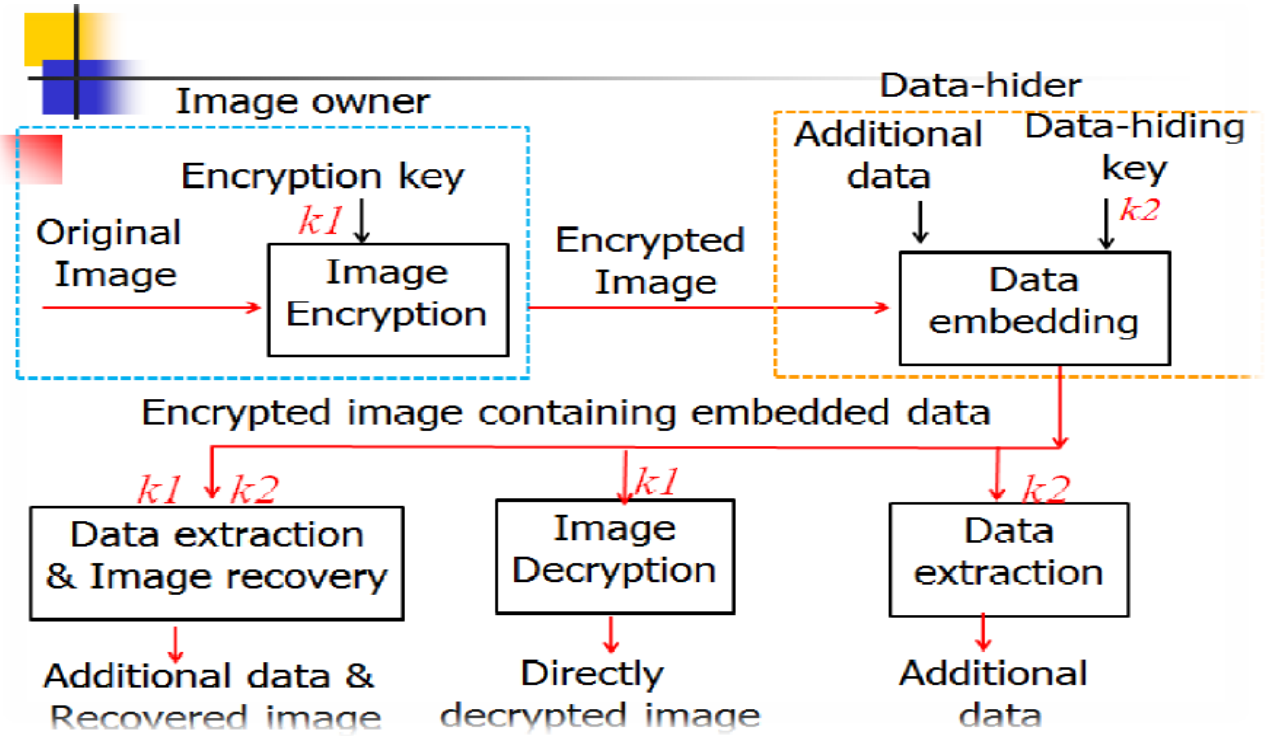


Fig.2: Architecture dia. For Separable Reversible Data hiding In Encrypted Image

A. Image Incryption

Consider the original image with a size of M1 X M2 in uncompressed color format. Now we have to convert image into gray level and each pixel with gray value falling into [0,255] is represented by 8 bits. Indicate bits of pixel as p1,p2,p3,…….pn. The gray values are denoted by Pi,j and given by (1)

$$P_{i,j} = \sum_{u=0}^{7} b_{i,j,u} \cdot 2^{u} \quad (1)$$

While converting into gray scale we have to follow the RGB rule i.e. c.G > c.R and c.G > c.B where G represents green, R represents red and B represents blue. Data image as plaintext and the encryption key are two inputs of encryption process. In this case, original image data bit stream is divided into the blocks length of blowfish algorithm. Image header is excluded to encrypt and the start of the bitmap pixel or array begins right after the header of the file. The byte elements of the array are stored in a row order from left to right with each row representing one scan line. Divide image Im into 32 halves Im1 and Im2.

Im1=Im1 Pi

Im2=F(Im1)Im2

Swap Im1 and Im2

Im2=Im2 P17

Im1=Im1 P18

Recombine Im1 and Im2

output X

The bits of pixels of encrypted image can be calculated using following formula (2)

$$B_{i,j,u} = b_{i,j,u} \oplus r_{i,j,u} \quad (2)$$

Where $r_{i,j,u}$ are the pseudo random bits calculated using Blowfish Algorithm from encryption key.

B. Data Embedding

Data embedding is based on cascading discrete wavelet transform (DWT) with singular value decomposition (SVD). DWT decompose the image into four frequency bands i.e. LL, HL, HH, LH. LL represents low frequency. HL and LH represents middle frequencies. HH represents high frequency. Again LL band represents approximate details. HL band gives horizontal details. LH gives vertical details. HH represents diagonal details. HH band is used to embed the particular data either text or image because it contributes fine details and insignificantly to the image energy hence data embedding will not affect the perceptual fidelity of cover image. The proposed scheme is based on the idea of replacing singular values of HH band with singular values of data. It observed that singular values lies between 84 and 173. If data to be embedded is selected such that its singular values lie within the given range then the energy of the singular values of embedded data will be approximately equal to the energy of the singular values of HH band. Hence replacement of the singular values of HH band will not affect the cover image. Data embedding is done using singular values and orthogonal

matrices. Uw and Vw obtained using SVD of data to be embedded.

$$W_E = U_w \times S_H \times v_w^T$$

C. Image recovery

For original image recovery receiver will need encryption key and encrypted image containing data.The same Process is applied as encryption except that the sub keys Pi must be supplied in reverse order. The nature of the Feistel network ensures that every half is swapped for the next round. The bits of pixels of decrypted image can be recovered using following formula (3)

$$b'_{i,j,u} = B'_{i,j,u} \oplus r_{i,j,u} \quad (3)$$

$B'_{i,j,u}$ are the bits of pixels of input image at receiver and $r_{i,j,u}$ are pseudo random bits calculated using Blowfish Algorithm from encryption key. The gray values of decrypted image can be calculated using formula given below (4)

$$P'_{i,j} = \sum_{u=0}^{7} b'_{i,j,u} \cdot 2^u \quad (4)$$

u denotes number of bits used to represent pixel of image i.e. from 0 to 7.

Fig.(a). Original Input Image

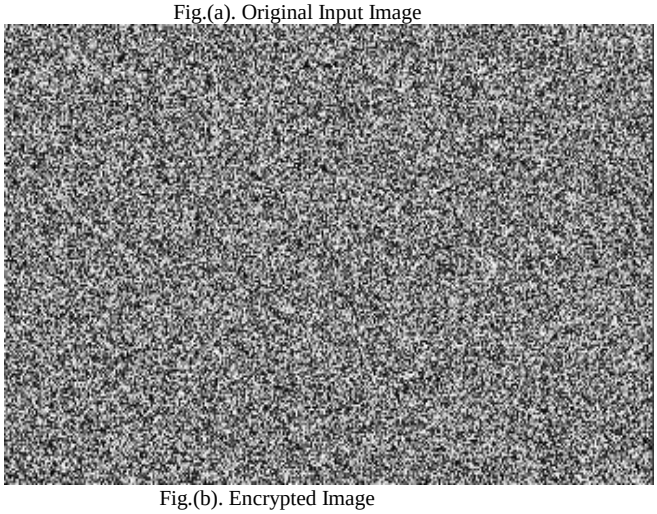


Fig.(b). Encrypted Image

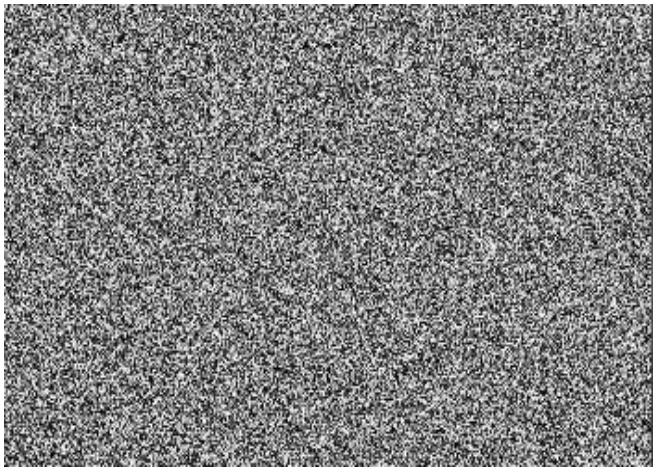


Fig.(c). Encrypted Image containing Data

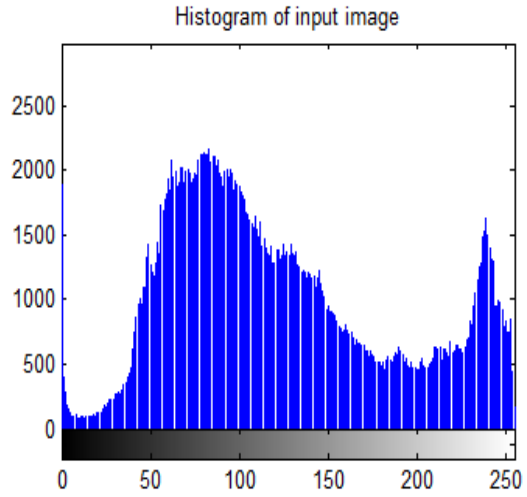
Fig.(d). Decrypted Image

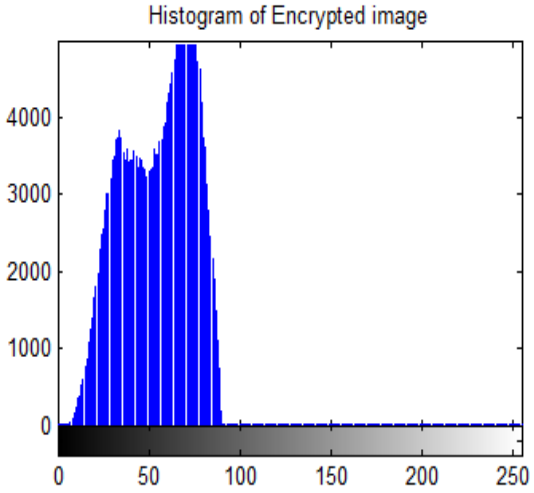
D. Data Extraction

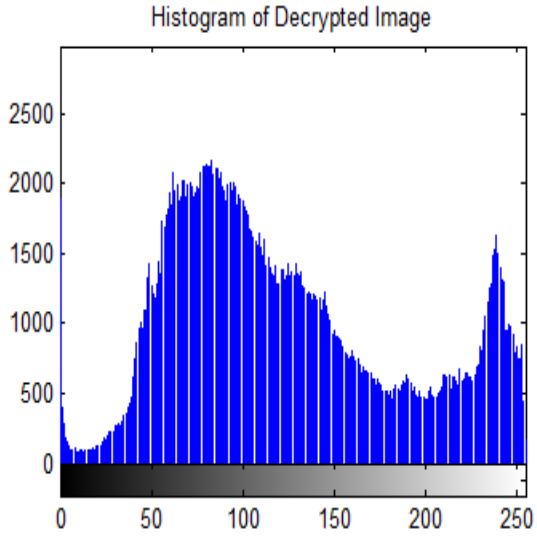
At receiver side for data extraction it will need data hiding key and encrypted image. While extracting data again using DWT, decompose the encrypted containing data in four sub bands i.e. LL, HL, LH and HH with the help of haar wavelet and applying inverse DWT to HH band get back the singular value of hided.

III. Experimental Results

The input original image will be resized to 512 X 512 as shown in Fig. (a) in the experiment. Fig.(b) shows the encrypted image in which the eight encrypted bits of each pixel are converted into gray value to generate an encrypted image. Fig.(c) shows hiding of data in HH band of encrypted image. By using both the data hiding and the encryption keys, the embedded data could be successfully extracted and the original image could be perfectly recovered from the encrypted image containing embedded data. For checking the accuracy of decrypted image we have plot the histogram indicating similarities between original image and decrypted image as shown below.







We have also tested other four images for their PSNR values and the result is as discussed further.

TABLE I. PSNR VALUES OF TEST IMAGES

IMAGES	IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5
PSNR(DB)	40.6136	39.7130	40.6790	39.3388	40.5136
CORRELATION COEFFICIENTS	0.9994	0.9995	0.9996	0.9994	0.9991

IV. CONCLUSION

In this paper, a novel technique for separable reversible data hiding in encrypted image is proposed and it consists of image 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, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data may text or image, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large.

V. FUTURE SCOPE

The lossless compression method is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data. However, the lossy compression method compatible with encrypted images generated by pixel permutation is not suitable here since the encryption performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation. The implemented a Novel Reversible method can be enhanced in future by using the following provisions

• And MLSB technique can also be applied after embedding when there is lot of change in the pixel to retain nearest to the original value.
• Can be applied in networking and the keys are sent and received securely.

ACKNOWLEDGMENT

We express our great pleasure in submitting this project paper titled ‘Secured Separable Reversible Data Hiding In Encrypted Image Using Blowfish Algorithm’. We express our deep sense of gratitude towards Prof. S.J. Koparde, due to her valuable guidance.

We are also thankful to Prof. J. M. Bakliwal (Head of E&TC Department) for his involvement and interest in the project.

REFERENCES

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

[2] 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.

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

[4] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discreteFourier transform in the encrypted domain," *IEEE Trans. Inform. Forensics Security*, vol. 4, no. 1, pp. 86–97, Feb. 2009.

[5] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," *IEEE Trans.Inform. Forensics Security*, vol. 5, no. 1, pp. 180–187, Feb. 2010.

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

[7] 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.

[8] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in *Proc. 11th ACM Workshop Multimedia and Security*, 2009, pp. 9–18.

[9] 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.

[10] 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," *Signal Processing: Image Commun.*, vol. 26, no. 1, pp. 1–12, 2011.

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

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

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

[14] 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.