International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-3, February 2013

Lossy Image Compression and Data Embedded In Compressed Encrypted Image

Suguna, Logesh Kumar, Lavanya

Abstract-This work is based on lossy image compression and data embedded in compressed encrypted image. In this, the original image is compressed by lossy compression method and encrypted using the encryption key. Data is hided into the compressed encrypted image using the data hiding key. If the receiver has encryption key then he can recover the image after decompression, if data hiding key he can extract the data, if both data hiding key and encryption key then he can extract the data and recover the original image after decryption and decompression.

Keywords- Lossy Compression, Encrypting an image, Data hiding, Recovery of image/ Extraction of data.

I. INTRODUCTION

Image security becomes increasingly important for many applications such as, confidential transmission, military and medical applications. Confidential data used for military purpose and medical purpose are transmitted over the internet. Nowadays, the transmission of images happens frequently and it is necessary to find an efficient way to transmit them over networks. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal the necessary information. Encryption and compression technologies are the important to the efficient solving of network bandwidth and security issues. Encrypting the data and compressing it, so that the compressor will not have the knowledge of the encryption key so that the secrecy is maintained [1]. The analysis of lossless image where the image data undergoes stream-cipher based encryption before compression is developed in [2]. Original image is encrypted by pseudorandom permutation and then compressed. Iterative reconstruction is used to retrieve the values of coefficients of original image. In this lossy compression is used [3]. The difference between embedded image and original image is almost imperceptible from human eyes, reversible data embedding could be thought as a convert communication channel. In this they calculate the neighboring pixel values and select some different values for the difference expansion [4]. A new reversible data embedding technique can embed large amount of data by using the algorithm. It slightly modifies the pixel gray values to embed data [5]. In [6] lossless embedding takes the host signal and the message data and provides watermarked signal in which the message data is embedded.

Manuscript published on 30 February 2013.
***** Correspondence Author (s)
Suguna, ECE Department ,Deemed University, Avinashilingam Institute for Home Science and Higher Education for women University In Coimbatore, India.
Logesh Kumar, ECE Department, Anna University, Assistant Professor in KCT Coimbatore, India.
Lavanya, ECE Department, Deemed University, Avinashilingam Institute for Home Science and Higher Education for women University In Coimbatore, India.

This technique allows complete recovery of original host signal and introduces only a small amount of distortion. The G-LSB is used. In [7] an embedded pixel value is generalized according to the difference between predicted pixel value and its original pixel value. It has great data capacity and quality of them is increased. The original image is encrypted using the encryption key and data is hided into the image using the data hiding key. A receiver first decrypt the image using the encryption key and then extracts the data and recover the image using the data hiding key in [8]. Fig.1 gives the separable reversible data hiding in an encrypted image. In this original image is encrypted using the encryption key and the data are hided into the encrypted image using the data hiding key. If the receiver has encryption key he can recover the image, if data hiding key he can extract the data, if both encryption and data hiding key he can recover the original image and extract the data without any error in [9].

This paper proposes a scheme on lossy image compression and data embedded in compressed encrypted image. The original image is compressed using the 2D Haar wavelet compression method and then the image is encrypted using the encryption key. Data is hidden into the compressed encrypted image using the data hiding key. At the receiver side, after decompression the image can be recovered using the encryption key. If he has data hiding key he can extract the data. If he has both encryption and data hiding key he can extract the data and recovery of original image takes place after decompression. Compression ratio will be higher and file size will be reduced.

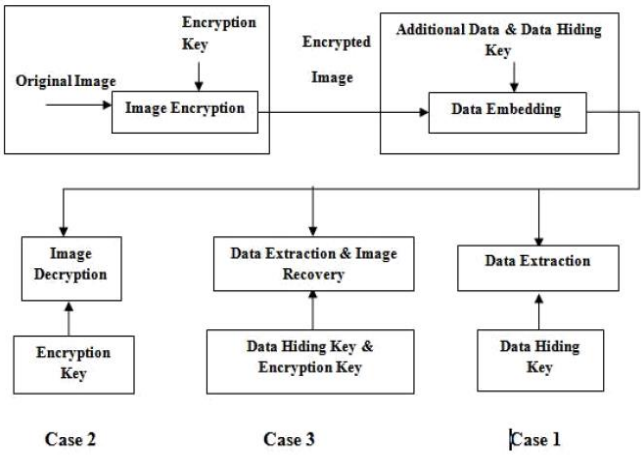


Fig .1 Separable reversible data hiding in an encrypted image

II. PROPOSED SCHEME

The proposed scheme consists of Haar wavelet compression, encrypting an image, Data hiding, Recovery of image and Extraction of data. The original uncompressed image is compressed using the Haar wavelet compression technique and the compressed image is encrypted using the encryption key.

The data is hidden by compressing the least significant bits of the compressed image using a data hiding key. At the receiver side data hidden into the compressed image can be extracted using the data hiding key as it affects only the LSB and by using the encryption key the recovery of image is done after decryption. By using both data hiding and encryption key, data can be extracted from the compressed LSB and the image is recovered. Fig.2 shows the sketch of lossy image compression and data embedded in compressed encrypted image.

A. 2D Haar Wavelet Compression:

To calculate Haar transform of array of n samples,

1. Find the average of each pair of samples. (n/2 averages)
2. Find the difference between each average and samples it was calculated from. (n/2 differences)
3. Fill the first half of the array with averages.
4. Fill the second half of the array with differences.
5. Repeat the process again to get 2D Haar wavelet transform.

The compression of image was done using the 2 dimensional Haar wavelet transform. By this the compression ratio is higher.

Advantages of Haar wavelet transform:

1. Best performance in terms of computation time.
2. Computation speed is high.
3. Simplicity.
4. HWT is efficient compression method.

B. Encrypting an Image:

Let us assume the compressed image size as N1xN2 with the gray values of [0,255]. Each pixel is 8 bits denoted as $b_{i,j,0}$, $b_{i,j,1}$…..,$b_{i,j,7}$ where $1 \le i \le N1$ and $1 \le j \le N2$, $p_{i,j}$ is the gray value, N is number of pixels (N1xN2). Bits of a pixel is

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

Gray values of a pixel is found by

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

The encryption of image is done by Xor operation. The bits of pixel are Xored with the secret key i.e encryption key using a standard stream cipher.

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

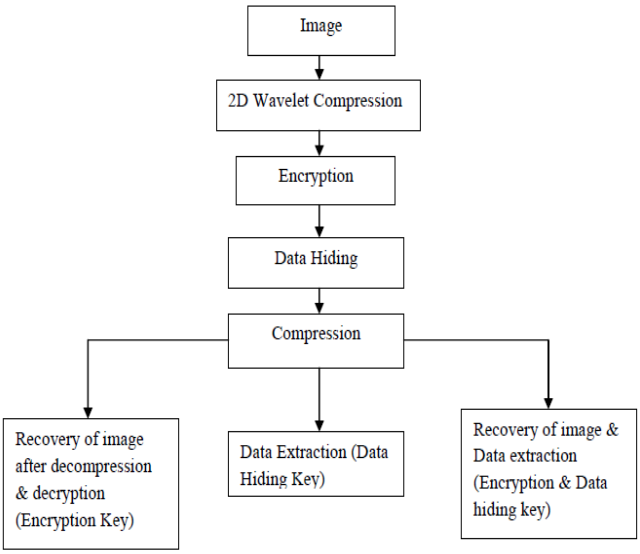


Fig 2. Lossy image compression and data embedded in compressed encrypted image

C. Data Hiding:

Here some of the parameters are considered. By pseudo randomly selecting the encrypted pixels as Np which carry the parameter for data hiding. For example if Np=16 then (N-Np) pixels are separated into groups by L pixels. For each pixel group collect the M least significant bits of L pixels and denote them as B(k,1), B(k,2)……B(k, M. L) where k is within [1,(N-Np)/L], M is small positive integer which is less than 5. Then the G matrix is calculated by Identity matrix and Q derived from the data hiding key.

$$\mathbf{G} = [\mathbf{I}_{M \cdot L - S} \mathbf{Q}].$$

Where I is (M. L – S) x (M. L – S) and Q is (M. L-S) x S. Here S is small positive integer. The parameter values of L, M and S are embedded into the Np encrypted pixels. Suppose if Np = 16 and L, M, S are 15, 2, 2. Based on this the number of data to be embedded can be calculated.

For each group calculate

Where the arithmetic is modulo-2 and [B(k,1) , B(k,2)…..B(k, M.L) is compressed as B'(k, M.L-S). by this the data can be hided into the bits of the pixels. It affects only the LSB and the MSB are kept unchanged.

D. Recovery of image & Data extraction:

With the compressed encrypted image which contains the embedded data, receiver using the data hiding key data can be extracted by obtaining the values of parameter M, L and S from the LSB of Np encrypted pixels. (N-Np) are the pixels which are grouped by parameter L. By using (N-Np)/L the groups are known and the S bits embedded can be extracted from the LSB of each group pixel. As the parameter values are embedded into the Np encrypted pixels the hackers only by using data hiding key alone cannot extract the embedded data. Receiver having the data hiding key alone cannot get any information about the original content of the image.

If the receiver has encryption key but not the data hiding key, he cannot obtain the values of parameter and cannot extract the data. If the receiver has encryption key then the bits of the pixel is derived using,

$$b'_{i,j,u} = B'_{i,j,u} \oplus r_{i,j,u}$$

The gray values will be derived using

$$p'_{i,j} = \sum_{u=0}^{7} b'_{i,j,u} \cdot 2^u.$$

Since MSB is not affected while data embedding process only the LSB is affected. The average energy of distortion is calculated using

$$A_E = \frac{(2^S - 1)}{2^S} \cdot 2^{-2M} \cdot \sum_{\alpha=0}^{2^M-1} \sum_{\beta=0}^{2^M-1} (\alpha - \beta)^2.$$

The value of PSNR in directly decrypted image is

$$\mathrm{PSNR} = 10 \cdot \log_{10}(A_E).$$

If the receiver has both data hiding and encryption key, he first extracts the embedded data and then the image is recovered. The data is extracted by obtaining the values of parameters L,M,S and it has affected only the LSB and the data are retrieved from those LSB.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The image is recovered by finding out the original gray values of the other (N-Np) pixels. Consider the pixel group, there must be one of the vectors meeting is calculated by,

$$\mathbf{v} = [B'(k,1)B'(k,2)\cdots B'(k,ML-S)00\cdots 0]^T + \mathbf{a}\cdot\mathbf{H}$$

Where a is arbitrary binary vector sized 1xS and H is SxML matrix made up of the transpose of Q

$$\mathbf{H} = [\mathbf{Q}^T\ \mathbf{I}_S].$$

The total difference between decrypted and estimated gray values in the group

$$D = \sum_{(i,j)\in G_k} |t_{i,j} - \hat{p}_{i,j}|$$

Estimated gray value is generated from the neighbors in the directly decrypted image by using

$$\hat{p}_{i,j} = \frac{\lfloor p'_{i-1,j}/2^M \rfloor + \lfloor p'_{i+1,j}/2^M \rfloor + \lfloor p'_{i,j-1}/2^M \rfloor + \lfloor p'_{i,j+1}/2^M \rfloor}{4} \cdot 2^M + 2^{M-1}$$

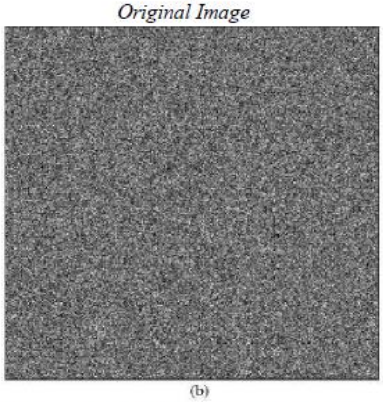
Thus we have 2^S different D corresponding to the 2^S decrypted pixel group G_k. The low D value will give the original pixel value of the image. S must be less than 10 to reduce the computation complexity.

III. RESULTS

The image of Lena sized 512x512 is used as an original image. The image is compressed and encrypted using the encryption key and data is embedded into the compressed encrypted image. The coding is done using VHDL and Matlab. The image is directly decrypted by using the encryption key and the PSNR is 34.07. Table 1 explains the comparison of PSNR, compression ratio.

(a)

Original Image



(b)

Compressed and Encrypted Image where the Data is embedded

(c)

Directly Decrypted Image with the PSNR 34.07

Table 1. Comparison of PSNR , Compression Ratio of existing and proposed method

Method	Parameter	Compression Ratio	PSNR of directly decrypted image	PSNR of recovered image
Proposed	M=2, L=15, S=2	0.02	34.0731	62.5
Existing	M=2, L=15, S=2	0.05	19.569	39.09

(d)

Data extracted using data hiding key in Modelsim

IV. CONCLUSION

In this paper the proposed method is compressing the image and then the image is encrypted using the encryption key. The data is hided into the compressed encrypted image using the data hiding key. If the receiver has encryption key then the image can be directly decrypted after decompression of an image, if data hiding key then receiver can extract the data from the compressed encrypted image, if both data hiding and encryption key the data can be extracted and the image is recovered after the decompression and decryption of an image. 2D Haar wavelet compression is used here so the compression ratio will be higher and file size will be reduced while transmitting.

REFERENCES

1. M.Johnson, P.Ishwar, V. M. Prabhakaran, D. Schonberg, and K.Ramchandran, "On compressing encrypted data" .
2. IEEE Trans. Signal Process. vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
3. 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.
4. [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.
5. J. Tian, "Reversible data embedding using a difference expansion ,"IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.
6. 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.
7. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber,
8. "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol. 14, no.2, pp. 253–266, Feb. 2005.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

9. 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.
10. X. Zhang, “Reversible data hiding in encrypted
11. image,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
12. X. Zhang, “Separable Reversible Data Hiding in Encrypted Image, ”IEEE transactions of information forensics and security” ,vol 7,No.2, Apr 2012

Suguna received the BE degree in Electrical & Electronics Engineering from Hindusthan College of Engineering, Coimbatore, affiliated to Anna University, Chennai. She presented a paper in National level Conference. Presented and participated ISTE workshop on “Introduction to Research Methodologies” conducted by IIT, Bombay through ICT (MHRD). She is currently pursuing her ME VLSI Design in Avinashilingam Institute for Home Science & Higher Education for Women University, Coimbatore- India

Logeshkumar Shanmugasundharam had received his M-tech degree in Nanotechnology specialisation from PSG College of Technology after his Bachelors in Electronics and Communication, His research interest includes cryptography, Nano electronics and Energy systems.Currently he is working as Asst. Professor at Kumaraguru College of Technology.

Lavanya received the BE degree in Electronics and Communication from Francis Xavier Engineering College, Tirunelveli affiliated to Anna University, Chennai. She presented a paper in National level Conference. Presented and participated ISTE workshop on “Introduction to Research Methodologies” conducted by IIT, Bombay through ICT (MHRD). She is currently pursuing her ME VLSI Design in Avinashilingam Institute for Home Science & Higher Education for Women University, Coimbatore- India

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)