ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 4, April 2016

Image Encryption and Reversible Message Embedding with Efficient Compression using Subservient Data and Huffman Coding

Kasmeera K S, Shine P James

***Abstract*— While transmitting redundant data through an insecure and bandwidth limited channel, it is mandatory to encrypt and compress it. Generally encryption is followed by compression as the statistical properties of encrypted images are not suitable for applying conventional compression schemes. The problem is that many situations demand the reverse procedure. This paper proposes a scheme of compressing encrypted image with the help of a subservient data and Huffman coding and reversibly hiding a message in the encrypted data. For encrypting the original image, it is manipulated with a pseudorandom number sequence generated using a secret key. The subservient data is also created by the content owner. The encrypted data is then compressed using a quantization mechanism and Huffman coding. For quantizing the image the subservient data produced by the content owner is used. The quantized values are then coded using Huffman coding. At the reconstruction side the principal content of the data is reconstructed. This work proposes a novel reversible data hiding scheme for encrypted image. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be successfullyExperimental results show that the compression ratio distortion performance of this method is superior to the existing Techniques. The compression ratio of encrypted image is improved to the range 20 to 50.**

***Index Terms*— Compression ratio-distortion performance, Data Embedding, Image compression, Image Encryption.**

I. INTRODUCTION

Nowadays multimedia, computers and networks have a big influence in our lives. Especially the internet is becoming highly important for nearly everybody. Video messaging, distance learning, remote auctions, video conferencing, telemedicine, interactive television etc. have improved the impact of multimedia in our personal lives. At the same time, the security and protection of the data has become an important issue. Any unwanted persons can easily capture and read the data, if it is transmitted without applying encryption. Encryption is the conversion of the data into a secret code, so that only the intended user can access the data, and it is considered the most effective way to ensure the security of the data. To read an encrypted image, you must have access to the secret key that enables you to decrypt it. Thus encryption permits you to securely protect data that you don't wish anyone else to have ingress to. Government uses it to safeguard classified information and many individuals adopt it to protect personal information and to defend against things like identity theft. Businesses need encryption to conserve corporate secrets. Espionage exploits encryption to securely protect folder contents, which could contain emails, account details, tax information or any other sensitive information so that if the computer is stolen, the data is safe. Advancements in information technology have been highly advantageous to healthcare. Doctors are now able to send information at a much faster rate than in the days of paper charts, so that more effective patient care is possible. However, this advancement also creates risk because a hacker can potentially break into a system remotely and steal patient information. But implementing data encryption is an efficient safety measure that will protect confidential patient information. At the same time, compression also has a vital role. The ability of the internet to transfer data is fixed. In the case of data storage, the storage space may be limited. Thus, for good data throughput it is desirable to compress the data. If the channel bandwidth is limited, the compression of data becomes compulsory.

There are several schemes for performing the encryption and compression of image. Generally, compression is followed by encryption as the conventional compression schemes cannot be applied in the encrypted image. However there are situations where encryption followed by compression is preferred. Consider for example a data distribution scenario where the content owner and the network operator are two separate entities, and do not trust each other. If the content owner is interested to protect the privacy of the data through encryption, the network operator is forced to compress the encrypted data. Encrypted image is purely random in nature and does not contain any kind of redundancies. Thus compression of encrypted images is not up to that of natural images. Reversiblehiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message[20].

Manuscript received April , 2016.

***Kasmeera K.S**, Department of Electronics and Communication Engineering, College of Engineering Poonjar.*

***Shine P James**, Department of Electronics and Communication Engineering, College of Engineering Poonjar.*

This paper deals with a scheme of compressing encrypted images using subservient data and Huffman coding and reversibly hiding a message in the encrypted image. In encryption phase, the content owner performs the encryption of original uncompressed image, and subservient data is also created when the channel bandwidth is not enough. In compression phase, a quantization mechanism is used to compress the encrypted data in various DCT sub-bands. The quantized values are coded using Huffman coding. The quantization parameter is optimized by using an optimizing mechanism which employs the subservient data. At a receiver side an intended user with secret key can reconstruct the principal content. The encrypted message is kept without compression for perfect reconstruction. The experimental result shows the ratio-distortion performance of this work is significantly better than that of existing techniques.

II. RELATED WORKS

The field of encryption and compression encompasses diverse schemes, ranging from the order of the process to variety of techniques. Here the schemes in which encryption is followed by compression only is considered. We discuss them as follows.

A. Kingston proposed a scheme [19] in 2007 which was motivated by a French project that was intended to securely store the digital data base of Louvre museum. Besides the use of a lossless compression algorithm, the Louvre Museum wants this whole database to be secured by both encryption techniques. Instead of encrypting the entire image only selective encryption is performed. The proposed technique takes advantage of a kind of Discrete Randon Transform(DRT) called the Mojette transform properties. Standard encryption techniques, such as AES, DES, 3DES, or IDEA can be applied to encrypt very small percentages of high resolution images. Golomb coding is employed for compression. This method enables perfect reconstruction of image. But as we increase the number of blocks that should be encrypted the time requirement increases exponentially. So it is impossible to completely encrypt the image using this method.

In 2008, another method was proposed by A. Anil Kumar [7], which applies encryption on the prediction errors instead of directly applying on the images and use distributed source coding for compressing the cipher texts. Prediction based coding is an efficient technique for achieving good lossless compression. Prediction error computation is least expensive, and can be implemented in an image acquisition system with minimal cost. Also, the compression achieved by predictive encoding is better than individual bit plane encoding. In predictive encoding, the current pixel will be estimated using the neighboring pixels. Then we will separate the bit planes of predictive encoded values. The simulation results show that by using the proposed technique comparable compression gains, with compression ratios varying from 1.5 to 2.5 can be achieved despite encryption.

In order to increase the compression gain the quality of the image should be sacrificed. In 2009, another work was proposed by A. Anil Kumar [12] in which considers the problem of lossy compression of encrypted image by compressive sensing technique. The encrypted image of size ($N \times N$) is multiplied a matrix of size ($M \times N$) where M is less than N. Hence the size of the product will be reduced which will result in the compression of data. Joint decoding/decryption is proposed with the modified basis pursuit decoding method to take care of encryption. Denoising of output image will improve the PSNR of the result. Through this method compression ratio could be improved up to 3.2.

Xinpeng Zhang [15] proposed a novel scheme for lossy compression of an encrypted image with flexible compression ratio. This method is based on iterative reconstruction. The data sender pseudo randomly permutes the pixels and the permutation way is determined by a secret key. For compression permuted pixels are divided into two sets as rigid pixels and elastic pixels. Rigid pixels will be kept as such. Orthogonal transform is performed for the elastic pixels. Transformed values are quantized. Compressed data includes data of rigid pixels, bits generated for quantized values and parameter values. After receiving the compressed data, with the aid of spatial correlation in natural image, a receiver can reconstruct the principal content of the original image by iteratively updating the values of coefficients. Compression ratio increased to 4 in this method.

A method for reversible data hiding on encrypted images was proposed by X.Zhang. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered.

The method of scalable coding [16] of encrypted images was proposed by X.Zhang. In the encryption phase, the original pixel values are masked by a modulo-256 addition with pseudorandom numbers that are derived from a secret key. For compression, the encrypted image will be down sampled by 2 and stored in a variable g. The remaining pixels are stored in a variable Q. The values in g are divided by Δ and quantizing each value. These values are surely transmitted. At the same time Q is permuted and divided into different sets. These are also divided by Δ. As more and more sets in Q are transmitted, the PSNR increases but CR decreases. Because of the hierarchical coding mechanism, the compression ratio varies between 2.7 to 4.5.

III. PROPOSED SCHEME

In this scheme, the content owner firstly encrypts the image and message using a secret key and the encrypted data is provided to the channel provider. In this method encrypted data has three parts ED, EI I and EI II ie., Encrypted data First Part of Encrypted Image and Second part of Encrypted Image. If the bandwidth of the channel is enough for transmission of the data, the channel provider transmits the encrypted data without Compression. Otherwise, the channel

provider sends a bandwidth insufficiency message to the content owner, and then the content owner generates the subservient data according to the image and provides it to the channel provider. Then, the channel provider who cannot access the original content may compress the coefficients in EI I by a quantization method with the subservient data and Huffman Coding. The Second part of Encrypted Image and Encrypted data are compressed lossless using Huffman Coding . At receiver side, an authorized user can reconstruct the principal content of original image and message by retrieving the coefficient values. Using this method the compression ratio distortion performance is improved. The sketch of this work is shown in Fig.1.

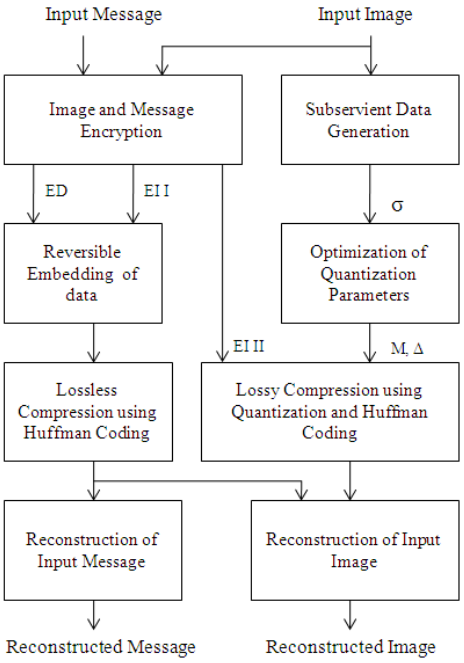

Fig 1. Block Diagram of Proposed System

A. Encryption of Image

A pseudo random number sequence in the range of 0 to 255 and in the same size of original image is used for encrypting the original image. The pseudorandom numbers are generated using a secret key, which is known to the content owner and the authorized user alone. Modulo 256 addition is performed between the input image and PN sequence. The encrypted data has two parts. Let, the input image be represented as *p*, with a size of m×n. Pseudorandom number sequence, *k* of same size is generated using the secret key. It is desirable that the value of the PN sequence vary in between 0 to 255. The first part of Encrypted data [18] is calculated as in (1),

$$c = \mathrm{mod}[(p+k), 256] \tag{1}$$

Clearly for reconstruction we should have the information about the quotient of this Modulo 256 addition. Since the value of image and PN sequence varies in between zero and 255, the quotient of Modulo 256 addition will be a binary sequence. It is calculated as,

$$s = floor[(p+k)/256] \tag{2}$$

It is advisable to encrypt this data as well. Thus, it is XORed with pseudorandom binary sequence. *s* has the same size of original image, and the values are binary in nature. Any biplane of the previously generated pseudorandom number sequence can be used for the encryption of *s*. In fig 1 *c* and *s* are represented as EI I and EI II respectively.

B. Encryption of Data

A key is used for the Encryption of data which will be known for content owner and the authorized user alone. The input message is first converted to ASCII format. The input message is encrypted using the bitwise XOR operation between the input data and secret key as shown in (3).

$$em = msg \otimes key \tag{3}$$

em, *msg* and *key* denoted the encrypted message input message and key respectively

C. Subservient Data Generation

Subservient Data is generated for efficient compression and reconstruction of encrypted data. For generating subservient data, the input image is first down sampled by a factor of 8. More specifically, we are dividing the image into blocks of 8×8, and from each block the last pixel is selected. Down sampled image is then interpolated using bilinear interpolation. The input image and interpolated image are divided into blocks of 8×8 and block wise 2D discrete cosine transform is calculated. With viewing the coefficients as 64 sub-bands, calculate the square roots of the average interpolation distortion [18] as shown below.

$$\sigma^{(u,v)} = \sqrt{\frac{\sum_{i=0}^{m/8-1}\sum_{j=0}^{n/8-1}[P(8i+u,8j+v)-G(8i+u,8j+v)]^2}{mn/64}} \tag{4}$$

Thus the subservient data σ can be generated where P and G are the block wise 2D DCTs of original image and interpolated image respectively. The values of u and v vary from 1 to 8.

D. Reversible Embedding of Data

With the encrypted data, although a data-hider does not know the original image content, he can embed additional message into the image by modifying a small proportion of encrypted data. Firstly, The encrypted message is converted in to binary sequence. Then the data-hider segments the encrypted image into a number of non-overlapping blocks. In each block are enlarged to carry more bits in regular pattern or pseudo randomly using a secret key where the encrypted message is placed.

E. Lossy Compression Using Quantization

After encrypting the image, if the channel resource is sufficiently abundant any compression is needless. In this case the channel provider may transmit the encrypted image

directly. Thus an authorized can decrypt the received data to reconstruct the original image without any distortion. If the channel resource is limited, the channel provider should obtain the subservient data from the content owner, and then perform a data-compression using a quantization and entropy coding before transmission. The compression procedure is as follows.

The compression will be performed in 64 sub-bands of discrete cosine transform with different optimized quantization parameters. The channel provider performs 2 dimensional DCT in the encrypted image with a block-by-block manner with a block size of 8×8. Each block is of size 8×8 and considered as 64 different sub-bands. It is converted into row vector. Such vectors corresponding to every block are concatenated downwards to obtain a matrix of size *(mn/64×64)*. Next step is orthogonal transform of the matrix. Orthogonal transform will help to obtain better visual quality as it is uniformly scattering the reconstruction error. In orthogonal transform the matrix of size *(mn/64×64)* is multiplied with an orthogonal matrix of size *(mn/64× mn/64)*. Then quantization of the orthogonally transformed matrix is performed as follows

$$Q^{(u,v)}(t) = \mathrm{mod}\{round\left[\frac{D^{(u,v)}}{\Delta^{(u,v)}}\right], M\},$$
$$where, 1 \le u, v \le 8, 1 \le t \le mn/64 \quad (5)$$

D represents the orthogonally transformed matrix. The quantization parameters, M and Δ are optimized using the procedure explained in section 3.5. The quantized values are encoded using Huffman coding.

Sub image of the encrypted image is calculated simply by down sampling the encrypted image by a factor of 8. Thus the sub-image, the encrypted binary data, Huffman coded data and the quantization parameter values are transmitted to the receiver.

F. Lossless Compression Using Huffman Coding

Lossy compression method cannot be used for encrypted message compression. So the second part of encrypted image and the message embedded on it is compressed using Huffman coding. For that x number of consecutive binary numbers is converted in to decimal values. These decimal values are then converted in to Huffman coded sequence.

G. Reconsruction of Image

With the compressed data and secret key the receiver should perform the following operations to reconstruct the principal image content.

1. Decompose the compressed data.
2. Decode the Huffman coded data to obtain quantized values i.e., Q.
3. Decrypt the sub-image to retrieve the original sub image and bilinear interpolation of this sub-image is performed. Interpolated image is denoted as *g*. Then decrypt binary encrypted data as well.
4. Find an estimate of encrypted image using (6)

$$\tilde{c} = g + \bar{k} \quad (6)$$

where $\bar{k}$ is equal to *k* if corresponding binary data is zero, else 256 is subtracted from k to obtain $\bar{k}$.

5. The estimate of the encrypted image is transformed using block wise 2D discrete cosine transform. The coefficients in each block are converted into vectors. Such vectors of every block are concatenated to obtain a matrix of size *(mn/64×64)*. This vector is orthogonally transformed to obtain $\tilde{D}$
6. $\tilde{D}$ is approximated to closest value [18] of original value using (6)

$$\hat{D}^{(u,v)}(t) = round\left[\frac{\tilde{D}^{(u,v)}(t) - Q^{(u,v)}(t).\Delta^{(u,v)}}{\Delta^{(u,v)} M}\right]\Delta^{(u,v)}.M + Q^{(u,v)}\Delta^{(u,v)} \quad (7)$$

7. Inverse orthogonal transform of $\hat{D}$ is calculated to obtain $\hat{C}$.
8. Inverse 2D DCT is also performed on $\hat{C}$ in block by block manner to obtain $\hat{c}$
9. Finally, the reconstructed image is obtained [18] as

$$\hat{p} = \hat{c} - \bar{k} \quad (8)$$

H. Reconstruction of Data

For reconstructing the message the embedded bits are retrieved from the particular positions of the message embedded encrypted image. Then it is converted from binary to ASCII. It is then unencrypted using (9)

$$decry\_msg = em \otimes key \quad (9)$$

Where *decry_msg*, *em* and *key* represent the decrypted message encrypted message and key respectively. The decrypted ASCII values are then converted to message.

I. Optimization of Compression Parameters

For optimization of Δ the subservient data is required. The following steps are performed to optimize Δ. The difference between D and $\tilde{D}$ is calculated as,

$$\varepsilon^{(u,v)}(t) = \tilde{D}^{(u,v)}(t) - D^{(u,v)}(t), 1 \le u, v \le 8, 1 \le t \le mn/64 \quad (10)$$

Denoting,

$$D_Q^{(u,v)} = round\left[\frac{D^{(u,v)}}{\Delta^{(u,v)}}\right]\Delta^{(u,v)} \quad (11)$$

And

$$\delta^{(u,v)}(t) = D_Q^{(u,v)}(t) - D^{(u,v)}(t) \tag{12}$$

Using these values the function f is calculated as in (13). f is the measure of expectation of error in each sub-band. It is calculated for various values of Δ. And the value Δ which provides the minimum f for each sub band will be selected [18].

$$f = \sum_{-\alpha}^{\alpha} \sum_{-\Delta/2}^{\Delta/2} \frac{\exp(-\varepsilon^2 / 2\sigma^2)}{\sqrt{2\pi}} \left(round\left[\frac{\varepsilon - \delta}{\Delta.M} \right] \Delta.M + \delta \right)^2 \tag{13}$$

From (5), it is clear that as the value of M decreases, the range of values of Q will decrease and hence the compression ratio will increase with a trade off in the quality of the image. For optimizing M a negative value of λ is selected and a condition is set such that as the value of λ becomes more and more negative the compression ratio increases. The condition is given below

$$\frac{\sigma^{(u,v)2}[f(m_{k-1}) - f(m_k)]}{\log_2(m_{k-1}) - \log_2(m_k)} \le \lambda$$
$$\frac{\sigma^{(u,v)2}[f(m_k) - f(m_{k+1})]}{\log_2(m_k) - \log_2(m_{k+1})} > \lambda \tag{14}$$

where m_k is the trail values which should be preferably in the range of 1 to 64. The value of m_k satisfying (12) is selected as M for each sub band. Likewise the optimized compression parameters is calculated as $M^{(u,v)}$ and $\Delta^{(u,v)}$ where u and v varies from 1 to 8.

IV. Experimental Results

The test image Lena sized 512 ×512 was used as the original in the experiment. Image used for the experiments and it's encrypted versions are shown below.

Fig. 2. (a) Lena.gif of size 512×512 (b) Encrypted image (EI 1)

The second part of encrypted image embedded with the secret message is shown in fig 3.

Fig. 3. Second part of encrypted image embedded with the secret message

When producing an encrypted version, we also generated the subservient data. For generation of subservient data, the original image is down sampled and then bilinearly interpolated. These images are obtained as shown in Fig.4.

Table 1. Subservient Data generated for Lena.gif

77.7625	42.40857	35.46888	19.95584	12.65996	8.746655	6.632905	4.751187
35.80099	23.63785	23.85513	14.56859	10.88474	7.40233	5.250137	3.901758
18.8984	18.06758	16.61955	12.51748	9.193477	6.582822	4.495953	3.808209
10.61505	11.05452	9.734604	9.025581	7.468964	5.598245	4.076743	3.312393
5.995669	6.835529	6.789681	5.855751	5.323113	4.089382	3.151376	2.609989
4.064488	4.532727	4.357729	4.230052	3.825474	3.200274	2.72246	2.251332
3.000554	2.858269	3.03227	2.742975	2.704609	2.535005	2.220658	2.037143
2.226691	2.295044	2.209036	2.282222	2.133696	1.999293	1.842401	1.683565

Fig. 4. (a) Downsampled image (b) Interpolated image

The subservient data generated for Lena image in gif format is shown in Table 1.

The value of λ is given as -20 and -50 and the optimized values of M are shown in Table 2 and Table 3 respectively.

Table 2. Optimized values of Δ for λ =-20

255.5054	254.4514	253.3492	182.4534	115.7482	1.249522	0.947558	0.678741
255.7214	216.1175	218.1041	131.1173	99.51761	1.057476	0.75002	0.557394
172.7854	165.1893	151.9501	114.4456	1.313354	0.940403	0.642279	0.54403
97.05187	101.0699	87.61143	1.289369	1.066995	0.799749	0.582392	0.946398
0.856524	0.976504	0.969954	0.836536	0.760445	0.584197	0.900393	0.745711
0.580641	0.647532	0.622533	0.604293	0.546496	0.914364	0.777846	0.964857
0.857301	0.816648	0.866363	0.783707	0.772745	0.724287	0.951711	0.873061
0.954296	0.98359	0.94673	0.978095	0.914441	0.85684	0.789601	0.962037

Table 3 Optimized values of M for λ =-20

63	63	63	55	34	23	9	1
63	62	63	40	19	11	9	1
54	53	55	23	21	15	17	8
19	29	22	17	10	7	1	1
10	18	12	7	4	2	1	4
1	1	8	1	7	1	1	1
1	1	1	6	1	4	1	1
1	1	1	4	1	1	1	1

Thus we obtained the compressed values and the compression ratio is found to be 42.54 and 42.91 for λ values of -20 and -40 respectively which is very high compared to the existing works of encrypted image compression. The space saved due to this compression is above 96% with Huffman coding. The reconstructed image was of good subjective quality and with a PSNR above 36dB. The reconstructed image is as shown in Fig.5.

Fig. 5 Reconstructed image (a) PSNR=37.78 Compression ratio without using Huffman coding is 5 and with Huffman coding 42.54 for λ =-20 (b) PSNR=26.72 Compression ratio without using Huffman coding is 6 and with Huffman coding 28.91 for λ =-50

Even without using Huffman coding this method could improve the compression ratio than the previous methods. The tradeoff between compression ratio and PSNR without using Huffman coding is shown in Fig below

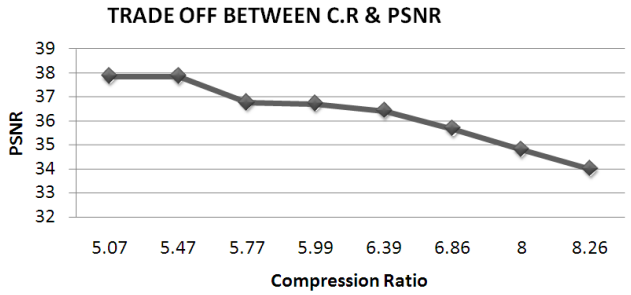

Fig 6. Tradeoff between Compression ratio and PSNR without using Huffman coding

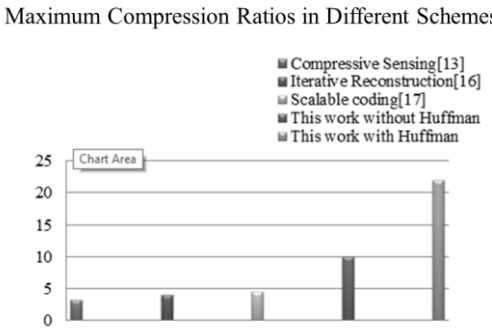

Fig. 8. Comparison chart

The graph shown in Fig.7 compares this method with other techniques which perform the compression of encrypted image. The maximum compression ratios obtained in different methods are displayed. The maximum compression ratio obtained through distributive source coding is 2.5. It is improved to 3.2 using compressive sensing method. Using iterative reconstruction and scalable coding compression ratio obtained is 4 and 4.5 respectively. Using this work a maximum compression ratio of 10 and 45 can be obtained with and without Huffman coding. The same input image is used for comparison.

The embedded message tested was 'Lena image in gray level representation' was encrypted ' .%*k" &*,.k"% k,9*2'.= .'k9.;9.8.%?* "$%' using a secret key 075 and then reconstructed with 100% accuracy.

V. Conclusion

This work proposes a scheme of embedding an encrypted message to encrypted image and compressing encrypted data with subservient data and Huffman coding. While the content owner produces the encrypted data and the subservient data, the channel provider quantizes the encrypted data using the optimal parameters derived from the subservient data, and then performs coding of the quantized values using Huffman coding. Then transmits an encrypted sub-image with embedded message, the Huffman coded data, the quantization parameters and the encrypted binary data. At receiver side, the principal image content and the embedded message can be reconstructed using the compressed encrypted data and the secret key. Compared with existing methods, the compression performance is improved. The encrypted message was compressed without loss. So it is reconstructed with 100% accuracy.

Acknowledgment

I would like to express my deepest gratitude to my guide Mr. Shine P James, Assistant Professor at College of Engineering, Poonjar, for his guidance and support. I would also like to thank my colleagues for devoting their time in discussing ideas with me and giving their invaluable feedback. Special thanks to X. Zhang the author of the IEEE paper "Reversible Data Hiding in Encrypted Image" for

providing me the thread of this work.

REFERENCES

[1] 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.

[2] StrunkJr Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," *EURASIP J. Inf. Security*, pp. 1–20, 2007.

[3] N. S. Kulkarni, B. Raman, and I. Gupta, "Multimedia encryption: A brief overview," *Recent Adv. Multimedia Signal Process. Commun.*, vol. SCI 231, pp. 417–449, 2009.

[4] G. Jakimoski and K. P. Subbalakshmi, "Security of compressing encrypted sources," in *Proc. 41st Asilomar Conf. Signals, Systems and* Computers (ACSSC 2007), 2007, pp. 901–903.

[5] D. Schonberg, S.C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in *Proc. 43rd Annu. Allerton Conf.*, Allerton, IL, USA, 2005.

[6] R. Lazzeretti and M. Barni, "Lossless compression of encrypted greylevel and color images," in *Proc. 16th Eur. Signal Processing Conf. (EUSIPCO 2008)*, Lausanne, Switzerland, Aug. 2008.

[7] A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," inProc. IEEE 10th Workshop Multimedia Signal Processing, 2008, pp. 760–764.

[8] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Signal Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[9] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, "Toward compression of encrypted images and video sequences," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 749–762, 2008.

[10] D. Klinc, C. Hazayy, A. Jagmohan, H. Krawczyk, and T. Rabinz, "On compression of data encrypted with block ciphers," in *Proc. IEEE Data Compression Conf. (DCC '09)*, 2009, pp. 213–222.

[11] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[12] E. J. Candes and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar.2008.

[13] A. Kumar and A. Makur, "Lossy compression of encrypted image by compressing sensing technique," in *Proc. TENCON 2009 IEEE Region 10 Conf.*, 2009, pp. 1–6.

[14] X. Zhang, Y. Ren, G. Feng, and Z. Qian, "Compressing encrypted image using compressive sensing," in *Proc. 7th Int. Conf. Intelligent* Information Hiding andMultimedia Signal Processing (IIHMSP 2011), 2011, pp. 222–225.

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

[16] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 3108–3114, Jun. 2012.

[17] S.-W. Ho, L. Lai, and A. Grant, "On the separation of encryption and compression in secure distributed source coding," in *Proc. IEEE Information Theory Workshop*, 2011, pp. 653–657.

[18] Xinpeng Zhan, Yanli Ren, Liquan Shen, Zhenxing Qian, and Guorui Feng "Compressing Encrypted Images With Auxiliary Information " in IEEE Transactions On Multimedia, Vol. 16, No. 5, August 2014

[19] A. Kingston et al. "Lossless Image Compression And Selective Encryption Using A Discrete Radon Transform" IEEE-1-4244-14377/07,ICIP, pp.IV 465-468, 2007

[20] X.Zhang. "Reversible Data Hiding in Encrypted Image" IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 4, APRIL 2011

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

[22] Z. Ni,Y.-Q. Shi,N. Ansari, andW. Su, "Reversible data hiding," *IEEETrans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, 2006.

[23] 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.

[24] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible imagewatermarking using interpolation technique," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 1, pp. 187–193, 2010.

[25] 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.

[26] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, "Reversible data-embeddingscheme using differences between original and predicted pixel values," *Inform. Secur.*, vol. 2, no. 2, pp. 35–46, 2008.

[27] 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, 2007.

[28] 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 Process.: Image Commun.*, DOI 10.1016/j.image.2010.11.001, to be published.

[29] D.Kundur andK.Karthik, "Video fingerprinting and encryption principles for digital rights management," *Proc. IEEE*, vol. 92, pp. 918–932, 2004.

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

Kasmeera K S is pursuing M.Tech (Signal Processing) in College of Engineering Poonjar. She completed her B.Tech from ASIET, Kalady. Her areas of interests are Data Compression, Data Encryption and Image Processing. She has attended International Conference Global Colloquium on Recent Advancements and Effectual Researches in Engineering Science and Technology and presented a paper entitled "Efficient Compression of Secures Images using Subservient Data and Huffman Coding"

Mr.Shine P James is working as Assistant Professor in Department of ECE at College of Engineering ,Poonjar from 2001 and continuing as Principal in charge of the college from 2013 onwards. He worked as Engineer in All India Radio and Doordarshan from 1993 to 2001. He completed his B.Tech (ECE) from NSS College of Engineering, Palakkad in 1991 and M.Tech in Signal Processing from NIT Calicut in 2013. His areas of specialization are Audio Signal Processing and Image Processing. He has published his works in International Journals IJECS, IJARECE, IJCA and IJERGS and attended International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013) and presented a paper entitled "Secure Selective Encryption of Compressed Audio".