IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Modern Techniques of Encrypted Image using Wavelet Transform

PB KAVYA[1], BULLARAO. D[2]

[1,2]Swetha Institute of Technology and science, Tirupati India

Abstract: In recent years, compression of encrypted image has attracted significantly towards research interest. This paper proposes an approach to compression of encrypted image based on wavelet and random permutation. Original image is first encrypted using random permutation then compressed using wavelet. The primary focus of this work is on the practical design of a pair of image encryption and compression schemes. The process of compressing the encrypted images is nearly same as compressing unencrypted image. The receiver does decryption and enhancement process. Decryption process is same as encryption process but for enhancement we have used median filter. Thus this paper focuses on achieving better security and improved transmission rate.

Keywords: Wavelet ,Image compression, random permutation, Image encryption.

I.INTRODUCTION

Image compression is playing a significant role in saving storage space efficiently. It also helps in accelerating transmission speed. Data compression methods are usually classified as either lossless or lossy methods. The traditional way of image transmission, image is first compressed for higher data transmission and then encrypted for secure information. Both the operation are performed by internet service provider it means secret information is visible to the service provider who may miss used it hence we also need to secure information from service provider. To secure information from service provider, the image must be encrypted by the user before transmitted and then encrypted image is compressed by the service provider for fast transmission. In this method, secret information is secure from both network intruder as well as service provider.

Some methods compression of encrypted image has been previously proposed. In [5] Ran, proposed a method in which encrypted gray scale image is compressed using the spatial correlation and quantization. The image is divided into 2x2 blocks and then it is encrypted by modulo 256 addition and block permutation. It is impossible perform a brute force search to recover the original image. In [16] Zhang presented a novel scheme for lossy compression of an encrypted image with flexible compression ratio. A pseudorandom permutation is used to encrypt an original image, and the encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. The compression ratio and the quality of reconstructed image vary with different values of compression parameters. In [13] Rosaline presented Reversible Data Hiding (RDH) Technique aims in recovering back the original content from the marked media. Securing the multimedia content can be achieved by performing encryption. Transmission time is further decreased by compressing such encrypted images. Encrypts the original image using Stream Cipher process. The encrypted image is then used as the media for hiding secret image. In [15] Zhou presented a novel scalable compression method for stream cipher encrypted images, where stream cipher is used in the standard format. The bit stream in the base layer is produced by coding a series of non overlapping patches of the uniformly down-sampled version of the encrypted image. The embedded image can then be compressed using wavelet compression.

Various wavelet based schemes for image compression has been implemented. Wavelet compression is a form of data compression well suited for image compression. The wavelet compression methods are better at representing transients, such as percussion sounds in audio, or high frequency components in two-dimensional images. Wavelets are a class of functions used to localize a given signal in both space and scaling domains. A wavelet transform can be used to decompose a signal into component wavelets. It can often compress or de-noise a signal without appreciable degradation.

II.METHODOLOGY

The figure.1 show block diagram of proposed technique of compression of encrypted image. The image shall be encrypted by random permutation using pixel and block permutation. The generated encrypted image is compressed by wavelet transform (DWT) which is a lossy image encryption scheme. At encryption stage encryption key k_{pe} and k_{be} is generated which is used for pixel permutation encryption and block permutation encryption respectively. Encryption key and image are input to encryption function that generates encrypted image (cipher image).The encrypted compressed image is transmitted to the receiver through communication channel. The random encryption keys which are used to generate cipher text will be transmitted to receiver by a secure channel.

The receiver has joint decompressor and decrypter. Encryption key k_{pe} and k_{be} are used to generate Decryption key k_{pd} and k_{bd} which is used to reconstruct original image. At reconstruction stage, received cipher image and decryption keys are taken as input to recover original image.

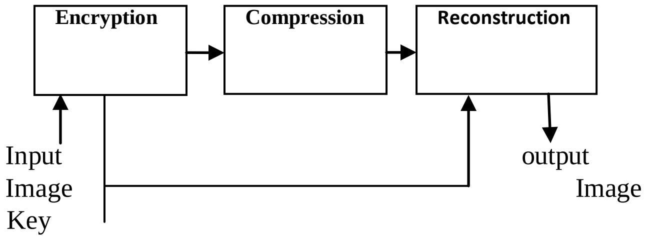


Figure.1 Block diagram of proposed compression of encrypted image method

A.Image Encryption

Image that has to be encrypted by random permutation has the dimension of (n x n), which is divided into αnumber of blocks in each row and column. Blocks are simply a two dimensional array of m x m. Encryption keys k_{pe} and k_{be} are generated. Encryption key $k_{pe}$is simple one dimension array which has length of m and
k_{be} is also a one dimension array has length ofα.

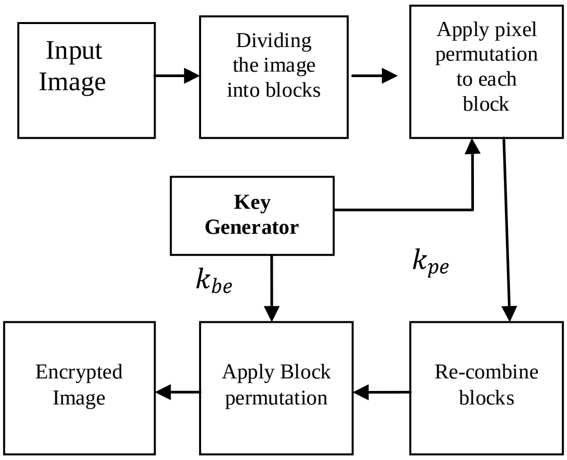


Figure 2. Random permutation encryption process

Figure 2 shows random permutation encryption process. Random pixel permutation is applied to each (m x m) size block using encryption keyk_{pe}. In pixel permutation, pixels of each row are first permuted after that pixel of each column is permuted. The random pixel permutation encryption process may be represented as follow

$$q = k_{pe}\,(p) \qquad 1$$

Where p represents pixel value of a block and q represents pixel value at different position. All blocks are combined after performing pixel permutation to each block. Combined n x n matrix and encryption key k_{be} is applied to Random block encryption function which generate random permuted encrypted image. The random block permutation encryption process may be represented as follow

$$u = k_{be}\,(s) \qquad 2$$

Where s represents a block has the dimension of m x m and u represents an encrypted block. The proposed encryption method is multilevel encryption scheme which makes a brute force attack redundant.

B.Image Compression

In the compression procedure, we compress the encrypted source using discrete wavelet transform (DWT). The encrypted cipher matrixis available at the compressor. Wavelet allows data analysis of images or signal. Wavelets are function which can be used for image compression, signal filtering, radar, human vision etc. Basic procedure for image compression using DWT involves reading image, converting image into discrete form, transforming by applying two dimensional DWT using haar, db, symlet, biothogonal and coiflet then selection the thresholding type and scalable hard hard thresholding is applied to the detail coefficient.

Wavelet algorithms process data at different scales or resolutions. The wavelet transform splits the image into high-frequency (H) and low-frequency (L) components at each scale. The H components at each scale are retained, and the L component are filtered again at the next scale The process continues, splitting the LL subsection of the image into four smaller subsections in the same way, until the LL sub-image is as many pixels wide as the number of taps for the wavelet [7]. we reduce the storage size of the image by removing low-frequency component which cannot be detect by human eye The mathematical representation of lowfrequency y_L and high- frequency y_H can be defined as:

$$y_L(n) = \sum_{i=0}^{t_L} L(i)X(2n-i) \qquad 3$$

$$y_H(n) = \sum_{i=0}^{t_H} H(i)X(2n-i) \qquad 4$$

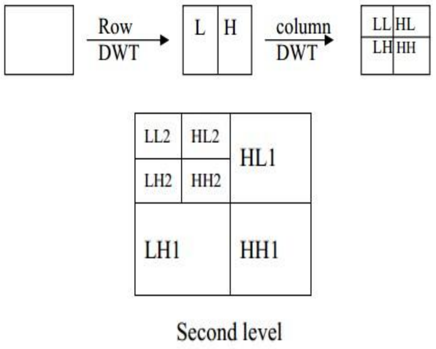


Figure 3 decomposition processes of level 1 and level 2

After decomposition hard thresholding is applied to the detail coefficient by selection the thresholding type. By applying hard threshold the coefficients below this threshold level are zeroed, and the output after a hard threshold is applied and defined by this equation:

$$\Theta_T^0(x)i=\{xi \text{ if } |xi| > T,\ \ 0\text{otherwise}.$$

A family of the mother wavelet is available; we are using basically five types of wavelets which are Haar wavelet, Biorthogonal wavelet, Daubechies wavelet, Symlet wavelet and coiflet wavelet. Haar wavelet is simplest and fastest type of wavelet transform for image compression. Symlets are improved in symmetry of Daubechies wavelets which is proposed by Daubechies. biorthogonal wavelet compression is lossy by but provide nearly lossless image compression.

C. Joint Decompression and Decryption

The original image can be reconstructed by performing decompression and decryption. The decryption process is same as encryption but here image is decrypted using decryption key which is generated with the help of encryption key. The encrypted image first pixel permutated after that block permutation is applied to get back original image. The size of decryption key is equal to encryption key so large number of decryption key makes various malicious attacks redundant.

The median filter is applied to the decrypted image for efficient image reconstruction. The median filter was one of the most admired nonlinear filter for removing noise. The window center value is replaced by the median value of center neighborhood. The median filter processed in a (a)rectangular area. The filter does find the noise in the center of rectangular area, the value of the pixel is replaced by the median value.

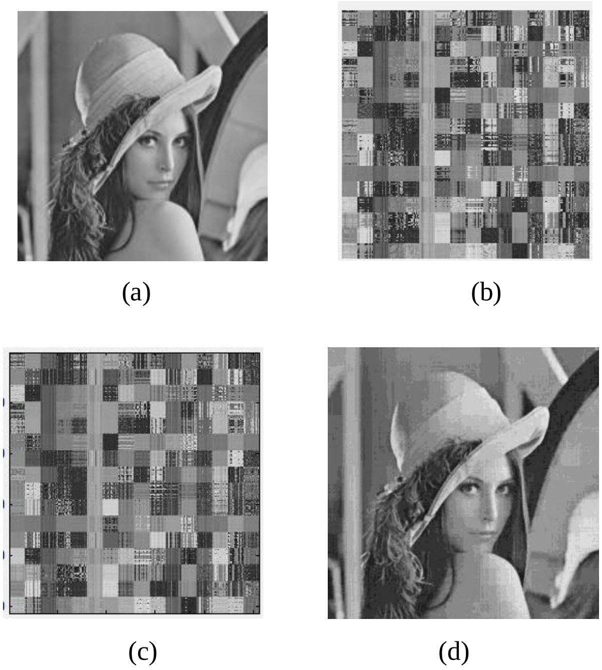
III.RESULT

We have performed simulation on six standard images lena, baboon, boat, goldhill, papers and barbara which have size of 512x512. Image is first encrypted by random permutation using 1-D key and then compressed by wavelet. The image is first divided into blocks of size (32, 32) and then pixel permutation is applied to each block using encryption key. During pixel permutation, row permutation is first applied then column permutation is applied using 1-D key of length 32. After pixel permutation, image is applied to block permutation process using encryption key of length 16. Number of available key using pixel permutation is equal to 2.6 x 10^{35} which is very large in number but image is also encrypted by block permutation have key space 2.09 x 10^{13} therefore total number of available key is equal to 5.50 x 10^{48}.The original and encrypted image using random permutation is shown in fig. 4.(a) fig. 4 (b) respectively. After encryption, image is compressed using wavelet transform of decomposition level 3. We also have compared five types of wavelets which are haar, db10, sym8 and bior3.3 and coif5. The original image is reconstructed by decryption of image using decryption key and after decryption median filter is applied for smoothen edge.

TABLE I. List of Bpp (bit per pixel) and PSNR of different wavelet for LENA image

	bpp	PSNR	bpp	PSNR
HAAR	1.0634	32.75	2.08	35.59
DB10	1.01	31.84	2.05	34.65
SYM8	0.99	31.89	2.005	34.67
BIOR3.3	1.0037	31.56	2.09	34.33
COIF5	1.010	31.62	2.09	34.73

It is clear from test result; the haar wavelet compression has better PSNR of reconstructed image. Haar wavelet compressed image has PSNR equal to 32.75 at nearly 1bpp and 35.59 at nearly 2bpp which is higher than other wavelet analysis.



(a) (b)

(c) (d)

Figure 4. (a) Original image.
(b) Encrypted image using combination of pixel and block permutated image. (c) haar wavelet compressed image (d) Reconstructed image (2bpp and PSNR = 33.61db)

TABLE II: shows compression ratio and bpp of six test image using haar wavelet

	bpp	PSNR	bpp	PSNR
Lena	1.0634	32.75	2.08	35.59
baboon	1.0572	29.55	2.036	30.14
Boat	1.0387	31.54	2.001	33.60
goldhill	1.0247	31.67	2.0053	33.61
papers	1.0081	31.81	2.0658	35.06
barbara	1.0043	30.29	2.0072	31.62

Proposed scheme is also compared with the article [15] for lena and baboon image. It is found that for LANA image proposed scheme have better PSNR value at lower bpp (0.46 bpp, 30.92db) and nearly 2 bpp, PSNR is nearly same. Proposed scheme is also compared for baboon test image, it can be seen that Proposed scheme have high PSNR value as compare with [15]. The comparison graph for LENA and BABOON image is shown in figure 6.6 and 6.7 respectively

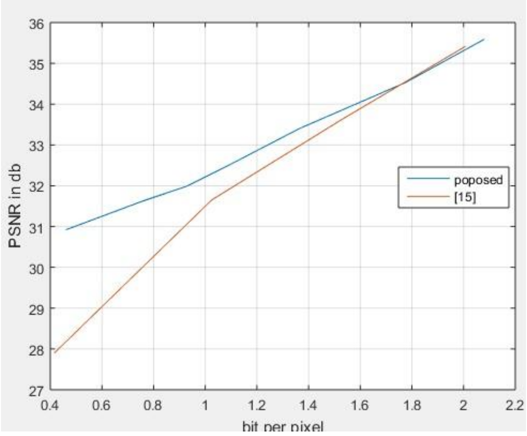


Figure 5 Comparison of proposed method with [15] of lena image

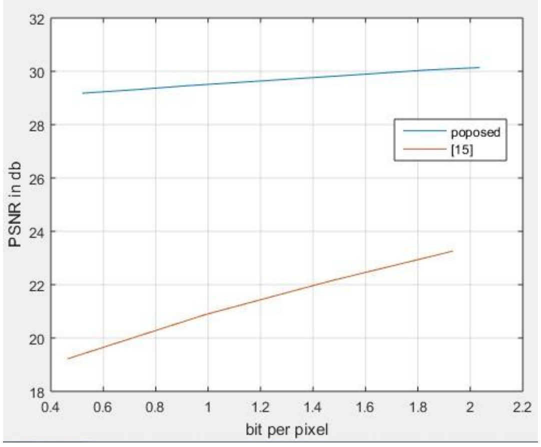


Figure 6. Comparison of proposed method with [15] of baboon image

IV.CONCLUSION

This proposed work mainly focus on compression of an encrypted image, Compression of encrypted image is quite complex as compare with traditional image compression scheme. In the proposed work Combination of pixel and block permutation technique have been used for image encryption and encrypted image is compressed using wavelet analysis. It has been seen that available number of key for encryption is very large which make encryption algorithm very strong. It has been proven that random permutation based encryption technique is fast and provide high degree of security. Five types of wavelets (haar, debuncies, Biorthogonal, Symlet, coifelet) are used for image compression. It can be seen that haar wavelet has higher compression ratio with better reconstructed image and PSNR of reconstructed image is better than [15] at lower bpp. Compression of encrypted image is very useful where high level of security is needed.

REFERENCES

[1] Abirami, J., Narashiman, K., SivaSankari, S., & Ramya, S. (2013, April). Performance analysis of image compression using wavelet thresholding. In *Information & Communication Technologies (ICT), 2013 IEEE Conference on* (pp. 194-198). IEEE.

[2] Rengarajaswamy, C., & Rosaline, S. I. (2013, April). SPIRT compression on encrypted images. In *Information & Communication Technologies (ICT), 2013 IEEE Conference on* (pp. 336-341). IEEE.

[3] Chuanmu, L., & Lianxi, H. (2007, April). A new image encryption scheme based on hyperchaotic sequences. In *Anti-counterfeiting, Security, Identification, 2007 IEEE International Workshop on* (pp. 237-240). IEEE.

[4] Dixit, A., Dhruve, P., & Bhagwan, D. (2012). Image encryption using permutation and rotational XOR technique. *Natarajan Meghanathan, et al.(Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT*, *6*, 01-09.

[5] Hu, R., Li, X., & Yang, B. (2014, May). A new lossy compression scheme for encrypted gray-scale images. In *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on* (pp. 7387-7390). IEEE.

[6] Indrakanti, S. P., & Avadhani, P. S. (2011). Permutation based image encryption technique. *International Journal of Computer Applications (0975–8887) Volume*.

[7] Karras, D. A., Karkanis, S. A., & Mertzios, B. G. (1998, August). Image compression using the wavelet transform on textural regions of interest. In *Euromicro Conference, 1998. Proceedings. 24th* (Vol. 2, pp. 633-639). IEEE.

[8] El Khamy, S. E., Hamdy, N., & Shatila, H. (2003), December). Adaptive fractal image compression using wavelet sub-tree coefficients. In *Circuits and Systems, 2003 IEEE 46th Midwest Symposium on* (Vol. 2, pp. 536-539). IEEE.

[9] Kumar, A. A., & Makur, A. (2009, January). Lossy compression of encrypted image by compressive sensing technique. In *TENCON 2009-2009 IEEE Region 10 Conference*.

[10] Liu, W., Zeng, W., Dong, L., & Yao, Q. (2010). Efficient compression of encrypted grayscale images. *Image Processing, IEEE Transactions on*, *19*(4), 1097-1102.

[11] Mitra, A., Rao, Y. S., & Prasanna, S. R. M. (2006). A new image encryption approach using combinational permutation techniques. *International Journal of Computer Science*, *1*(2), 127-131.

[12] Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. *Image and Vision Computing*, *24*(9), 926934.

[13] Rosaline, S. I., & Rengarajaswamy, C. (2013), February). Reversible data hiding technique for stream ciphered and wavelet compressed image. In *Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on* (pp. 374-377). IEEE.

[14] Zhou, J., Liu, X., Au, O. C., & Tang, Y. Y. (2014). Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation. *Information Forensics and Security, IEEE Transactions on*, *9*(1), 39-50.

[15] Zhou, J., Au, O. C., Zhai, G., Tang, Y. Y., & Liu, X. (2014). Scalable
Compression of Stream Cipher Encrypted Images Through ContextAdaptive Sampling. *Information Forensics and Security, IEEE Transactions on*, *9*(11), 1857-1868.

[16] Zhang, X. (2011). Lossy compression and iterative reconstruction for encrypted image. *Information Forensics and Security, IEEE Transactions on*, *6*(1), 53-58.

[17] Zhang, X., Ren, Y., Shen, L., Qian, Z., & Feng, G. (2014).
Compressing encrypted images with auxiliary information. *Multimedia, IEEE Transactions on*, *16*(5), 1327-1336.