DESIGNING AN EFFICIENT IMAGE ENCRYPTION-THEN-COMPRESSION VIA RANDOM PERMUTATION

[1]V.Vineeth kumar, [2]Rishi Raj Dwivedi, [3]T.Punesh Reddy, [4]R.Sreekanth, [5]P.Ramesh
[1,2,3,4]Student, [2]Associate Professor
[1,2,3,4,5]Department of ECE,
[1,2,3,4,5]MLR Institute of Technology, Hyderabad, INDIA

Abstract— In the modern world, the privacy, security features and hidden information of the image is rapidly growing this lead towards the research interest. This paper proposes a new design of image encryption of an image using random permutation and then compression of an encrypted image using discrete wavelet transform. The main part of the work is the practical design of a pair of image encryption then compression. Compression process in this paper is similar to the normal compression of an image. The receiver side performs decompression and decryption. The decompression process by Inverse discrete wavelet transform and decryption process is the reverse of the encryption process. Thus image encryption then compression provides better security features and transmission rate.

Index Terms— Image encryption, Random permutation, Image compression, Wavelet transform.

I. INTRODUCTION

This is the era, where the transmission of images is at their peak level. Every day millions of images are being transmitted around the globe from one person to another person. These images contain information which is to be protected, so there is a need to make sure that security is provided to these images while being transmitted from the network intruder as well as the service provider. As number of images are increasing, we also need to maintain the transmission speed. For this compression should be done before the image is being transmitted. The traditional way of transmitting the image is, the image is compressed and then encrypted for information. Both of this processes are done by the service provider, so there is a chance of hacking the original data. Here the security of the information is lost, so the user needs to encrypt the image to secure the information. This is achieved by following the sequential process of encryption and then compressing the image. Here the encryption process is done by the user, so the service provider has no chance to access the information. By this, the image is secured from both, service provider and network intruder.

II. RELATED LITERATURE

In [1] sesha proposed permutation based image encryption technique, which performs random pixel permutation over the image without affecting the quality of the image by making use of 64 bit key shared between the sender and the receiver. Previously proposed an image encryption using combinational permutation technique. The idea behind their approach is to combine different permutation techniques randomly based upon bit, block and pixel, which produces good results when combined together instead carrying it separately for encryption process. In [2] Yang, proposed a method where encrypted gray scale image is compressed by spatial correlation and quantization. An image is divided into small blocks and it is encrypted via modulo 256 addition and block permutation. To recover the image it is impossible method a brute force search. In [3], a novel scheme for lossy compression of an encrypted image with compression ratio. Encryption using pseudo random permutation and compressed by removing the excessively rough information of coefficients of orthogonal transform. In [8] Zhou given a novel scalable compression method for encryption based on stream cipher is used in the standard format. The bit stream of the base layer is done by coding a series of non overlapping of uniformly down sampled of the encrypted image. The embedded image is compressed by wavelet.

III. PROPOSED METHODOLOGY

The figure.1 shows the block diagram of proposed methodology of efficient image encryption then compression. The image which is to be encrypted by an information or data is to be encrypted by random permutation using pixel permutation and block permutation and then block combining. Encrypted image is compressed by the discrete wavelet transform which is similar to lossy image compression. The compressed encrypted image is transmitted to the receiver side through a channel. The receiver side has both decompression and decryption which is used to recover the original image.

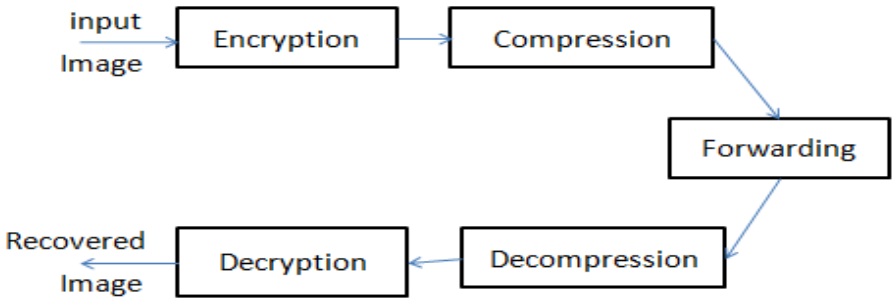

Fig1.Block diagram of proposed encryption then compression

III.I IMAGE ENCRYPTION

An image that is to be encrypted via random permutation has the dimension of (n x n), is resized to dimension of k x k so that every image can be easily divided into n number of blocks in each column and row. Blocks are simply a two dimensional m x m array.

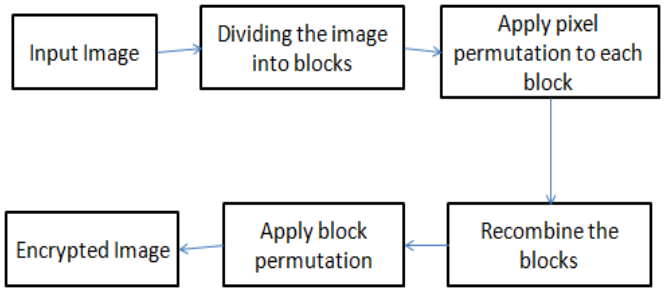

Fig2.Block diagram of encryption process

First the image is divided into number of blocks and then pixel permutation is applied to each individual block of m x m size. In pixel permutation, each pixel of the block is randomly permutated so that no pixel falls into its own place and if it falls it is represented as zero. After the pixel permutation is applied to every block then all the blocks are recombined. Apply block permutation to the recombined blocks to form random permuted encrypted image. The proposed approach is multi level encryption similar to brute force attack redundant.

III.II IMAGE COMPRESSION

The encrypted cipher image matrix is available at the compression process. The analysis of images or signal done by wavelet tool box. Wavelet functions are used for the image compression, signal filtering, human vision, radar etc. Basic implementation to do image compression using discrete wavelet transform is reading an image and converting into discrete form, by applying two dimensional discrete wavelet transform using haar. Then selection of the scalable and thresholding type is applied to the detail coefficient.

The wavelet transform splits the image into two parts, one is low frequency component and other is high frequency component at each scale. The high frequency components are kept as it is and the low frequency components are filtered again at each scale. This is followed till the lower of the lower frequency components splits into four smaller subsections in the same way, until the lower of the lower sub image is as many pixels wide as the number of taps of the wavelet[7]. The storage size of an image can reduced by removing the lower frequency component which can't be seen by human eye. The mathematical representation of low frequency L and high frequency H can be written as

$$L(n) = \sum_{n=0}^{t_L} \mathrm{L(i)X(2n - i)} \qquad (1)$$

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

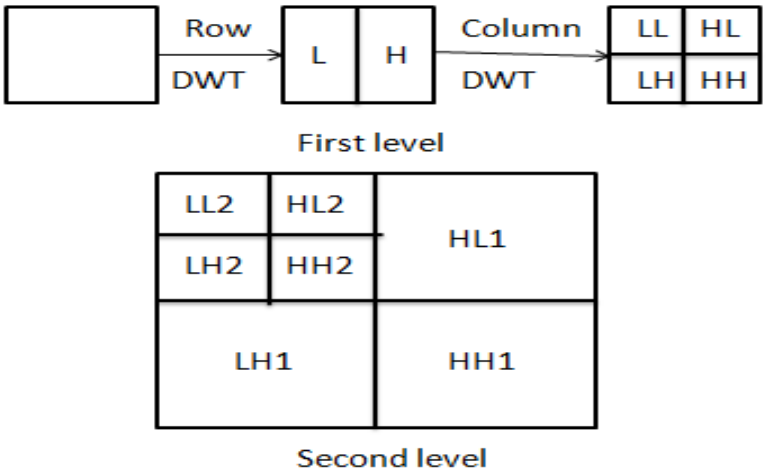

Fig3.level 1 and level 2 decomposition process

After decomposition process, hard thresholding is applied for the detail coefficient by selecting the type of thresholding. By applying this the coefficients less than threshold are zeroed and the output after a hard threshold is applied and given by the equation

$(\Theta^0)_T(\mathrm{x}) = \{\mathrm{xi\ if\ |xi|} > T$

0 otherwise (3)

A Wavelet family is available in which we are using Haar, Daubechies, Symlet and coiflet. Haar wavelet is simple and fast type of wavelet for image compression.

IV. RESULTS

We have performed the simulation of four standard images Lena, Barbara, Cameraman and a dog which have different image resolution. An image is encrypted via the random permutation and compressed by using discrete wavelet transform. The original and encrypted image using random permutation is shown in fig. 4.1 fig.4.2 respectively. We also have compared five types of wavelets which are haar, db4, sym4 and bior3.3 and coif4.

Table 1 MSE and PSNR values of different wavelets of Lena image

WAVELET	***MSE***	***PSNR***
Haar	3.089e-005	45.1019
Daubechies	0.0321	14.937
Symlets	0.0166	17.78
Coiflets	0.0447	13.49

From the above table, we can have better PSNR using haar wavelet compression for reconstructed image. Haar wavelet transform compressed image has PSNR equal to 45.1019 and MSE of 3.089e-005 which is greater than the other transform. Lesser the PSNR, the recovery of the image is also not possible.

(a) (b)

(c) (d)

Figure 4 .(a)Original image

(b) Encrypted image using random permutation
(c)Compressed image using haar
(d) Recovered image

Table 2 MSE and PSNR of various image using haar transform

WAVELET	***MSE***	***PSNR***
Lena	3.089e-005	45.1019
Barbara	8.8428e-005	40.5341
Cameraman	1.7342e-005	47.6091
Dog	2.9248e-005	45.3391

Proposed approach is also compared with the article [8] for Lena and. It is found that Lena image proposed scheme have better PSNR value, PSNR is nearly same. The above table results show that MSE and PSNR values of Lena, Barbara, cameraman and dog is shown using haar transform. The compression ratio of the images is around 37.5.

V. CONCLUSION

This proposed approach of encryption then compression is a quite tough task when compared with the traditional compression then encryption process. It has been proved that encryption process via random permutation is fast and gives high security. Wavelet family have been used for image compression and proven that haar transform has better MSE and PSNR. Thus Efficient image encryption-then-compression via random permutation provide high security and better compression ratio.

VI. ACKNOWLEDGMENT

I would like to thanks our Associate Professor. P. Ramesh for his guidance and for helping us to carry out our project successfully.

REFERENCES

[1] Sesha Pallavi Indrakanti and Avadhani P.S, "Permutation based image encryption technique", International Journal of Computer Applications, Vol. 28, No.8, 2011.

[2] 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.

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

[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] G. A. Sathish kumar and K. Bhoopathy Bagan, "A novel image encryption algorithm using pixel shuffling and base-64 encoding based chaotic block cipher", WSEAS Transactions on computers, Vol. 10, No. 6, pp. 169-178, 2011.

[6] 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.

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