Nivedita, International Journal of Advanced Trends in Computer Applications (IJATCA)
Volume 3, Number 2, February - 2016, pp. 26-30
ISSN: 2395-3519

International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Designing an Efficient Image Encryption-Compression System using a New HAAR and Symlet Wavelet Transform

[1]Nivedita, [2]Sanjay Yadav
[1]SIEET Sunder Nagar, Mandi
[2]Assistant Professor
SIEET Sunder Nagar, Mandi
[1]nivedita867@gmail.com, [2]sanjay12062@yahoo.com, samjess.jess@gmail.com

Abstract: *Nowadays there is quick advancement in the media and network technologies. That is the reason the protection and security turns into the real issues subsequent to the mixed media is transmitted straightforwardly over the network. Alongside the protection and security, storage space is likewise a vital point that can't be missed. That is the reason to give the privacy and security to the media, encryption function as the root and also to reduce the storage space compression can be utilized. Decrease in size additionally reduces the time taken for transmission. In many practical situations, image encryption must be led preceding image compression. This has prompted the issue of how to plan a pair of image encryption and compression algorithms such that compressing the encrypted images can still be efficiently performed. In this work, we design and implement a productive image encryption-compression system where lossy compression is considered. The proposed image encryption plan is operated with random permutation technique which is shown to be able to give reasonably high level of security. It also implement a new image compression algorithm or solution using Haar and Symlet Wavelet Transform which can be used to efficiently compress the encrypted image. After that the compression approach applied to encrypted image is proved more efficient in terms of Compression Ratio (CR), Mean Square Error (MSE), and Peak Signal to Noise Ratio (PSNR).*

Keywords: *Image Encryption, Image Compression, New HAAR Wavelet Transform and Symlet Wavelet Transform*

I. INTRODUCTION

The security of multimedia becomes more important, since multimedia data are transmitted over open networks more frequently. Typically, reliable security is necessary to content protection of digital images and videos. Encryption schemes for multimedia data need to be specifically designed to protect multimedia content and fulfil the security requirements for a particular multimedia application. For example, real-time encryption of an image using classical ciphers requires heavy computation due to the large amounts of data involved, but many multimedia applications require security on a much lower level, this can be achieved using selective encryption that leaves some perceptual information after encryption.

Image Encryption

When more and more sensitive information is stored on computer and transmitted over the internet, we need to ensure information security and safety. Image is also an important part of our information. Therefore, it is very important to protect our image from unauthorized access. Basically, Image Encryption means that convert an image to unreadable format so that it can be transmitted over the network safely. Image Decryption means to convert the unreadable format of an image to original image.

Figure 1: Encryption of an image

Figure 2: Decryption of an image

Fig. 1 and 2 shows that the encryption and decryption of an image respectively. The output showed in Fig. 1 can be obtained by using various image encryption techniques.

Image Compression

Image compression addresses the issue of reducing the measure of information needed to represent a digital image. It is a methodology expected to yield a reduced representation of an image thereby reducing the image storage/transmission requirements. Compression is attained by the removal of one or more of the three fundamental data redundancies:

- Coding Redundancy
- Interpixel Redundancy
- Psychovisual Redundancy

Coding redundancy is available when less than optimal code words are utilized. Interpixel redundancy results from relationships between the pixels of an image. Psychovisual redundancy is because of data that is overlooked by the human visual framework (i.e. visually non essential information). Image compression procedures decrease the quantity of bits needed to represent an image by exploiting these redundancies. An inverse procedure called decompression (decoding) is connected to the compressed data to get the remade image. The goal of compression is to reduce the quantity of bits however much as could be expected, while keeping the resolution and the visual quality of the recreated image as near to the first image as possible. Image compression frameworks are made out of two distinct structural blocks that are an encoder and a decoder.

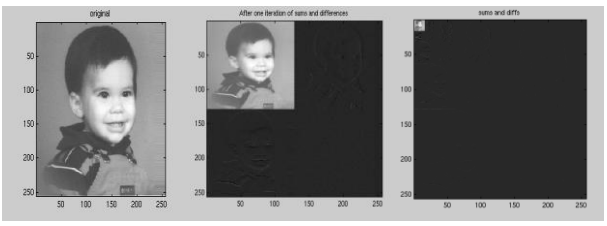

Fig. 3: Image Compression

Advantages of Image Compression

- It gives a potential cost savings connected with sending less data over exchanged phone system where cost of call is really usually based upon its duration.
- It not only reduces storage requirements as well as general execution time.
- It also decreases the probability of transmission mistakes subsequent to less bits are exchanged.
- It also gives a level of security against illicit monitoring.

II. HAAR WAVELET

The HAAR wavelet is a sure arrangement of capacities which is presently perceived as the first known wavelet. HAAR utilized these capacities to give an illustration of a countable ortho-ordinary framework for the space of square vital capacities on the genuine line. The investigation of wavelets and the expression "wavelet" did not come until much later. The HAAR wavelet is also the simplest wavelet. The HAAR wavelet has a technical disadvantage is that it is not continuous and not differentiable.

The HAAR wavelet's function $\psi(t)$ can be described as:

$$\psi(t) = \begin{cases} 1 & 0 \le t < 1/2, \\ -1 & 1/2 \le t < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Scaling function $\varphi(t)$ can be described as:

$$\phi(t) = \begin{cases} 1 & 0 \le t < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Wavelets are numerical capacities that were created by researchers working in a few separate fields with the end goal of sorting information by its recurrence. At that point the Translated information can be sorted at a determination which matches its scale. At distinctive levels, the Studying information takes into consideration the advancement of a more finish picture. By this, both little highlights and extensive highlights are discernable in light of the fact that they are concentrated on independently. After that, the wavelet change is not Fourier-based and subsequently wavelets improve employment of taking care of discontinuities in information. The HAAR wavelet works on information by computing the totals and contrasts of components which are neighbouring. The HAAR wavelet operates first on adjacent horizontal elements and after that on adjacent vertical elements. The HAAR transform is computed by using the following:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

III. SYMLET WAVELET

In *symN*, *N* is the order. Some authors use 2*N* instead of *N*. Symlets are only near symmetric and consequently some authors do not call them symlets. By typing waveinfo('sym') at the MATLAB command prompt, you can get a review of the principle properties of this family.

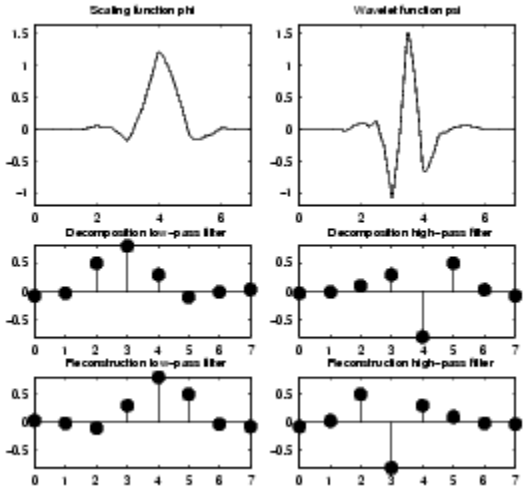

Figure 4: Symlets sym4

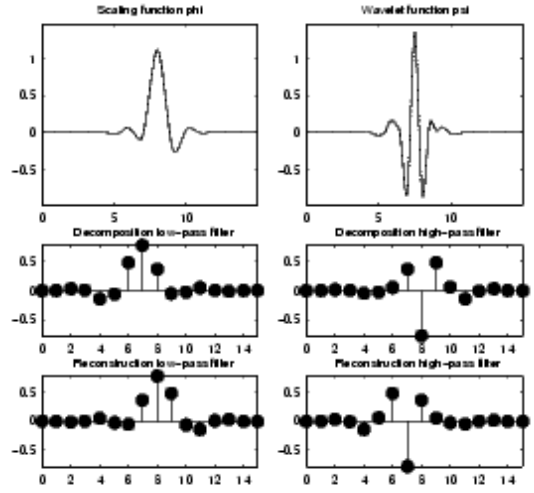

Figure 5: Symlets sym8

Daubechies proposes alterations of her wavelets that expand their symmetry can be expanded while holding awesome effortlessness.

The thought comprises of reusing the function m_0 introduced in the *dbN*, considering the $|m_0(\omega)|^2$ as a function *W* of $z = e^{i\omega}$.

Then we can factor *W* in several different ways in the form of $W(z) = U(z)\overline{U\left(\frac{1}{\bar{z}}\right)}$ because the roots of *W* with modulus not equivalent to 1 go in sets. In the event that one of the roots is z_1, then $\frac{1}{z_1}$ is also a root.

By selecting *U* such that the modulus of every one of its roots is entirely less than 1, we construct Daubechies wavelets dbN. The U channel is a "base stage channel." And by settling on another decision, we acquire more symmetrical channels; these are symlets. The symlets have different properties like those of the *dbN*s.

IV. EVALUATION PARAMETERS

There are some parameters given which are useful in our implementation.

- ***CR(Compression Ratio)***

The compression ratio i.e. the size of the compressed image compared to that of the uncompressed image. Still images are often lossily compressed at 10:1, but the quality loss is more noticeable, especially on closer inspection.

$$C_R = n1/n2$$

where n1 is the size of original image and n2 is the size of compressed image.

- ***MSE (Mean Square Error)***

MSE is essentially a signal fidelity measure. The goal of a signal fidelity measure is to compare two signals by providing a quantitative score that describes the degree of similarity/fidelity or, conversely, the level of error/distortion between them. Usually, it is assumed that one of the signals is a pristine original, while the other is distorted or contaminated by errors. The MSE between the signals is given by the following formula:

$$MSE = \frac{1}{M * N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[f(x,y) \quad - F(x,y)]$$

where MxN is the size of image, f(x,y) is the original image and F(x,y) is the reconstructed image.

- ***PSNR (Peak Signal to Noise Ratio)***

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g. for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. Although a higher PSNR generally

indicates that the reconstruction is of higher quality, in some cases it may not.
The PSNR values can be obtained using following formula-

$$PSNR = 10 \log_{10}(255/(\sqrt{MSE}))^2$$

MSE and PSNR are most commonly used to measure the quality of reconstruction of lossy compression codecs. The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality.

V. PROPOSED WORK

There are some steps of proposed work:-
Step 1: Develop an opening GUI for this implementation. After that code is developed for the loading the image file in the MATLAB database.

Step 2: Develop a code for encryption algorithm with suitable key. Finally HAAR and SYMLET wavelet transform with encryption algorithm are applied on the input image.

Step 3: Develop a code for Image Compression Using HAAR and SYMLET Wavelet Transform.

Step 4: Analysis of result obtained is done on the basis of various parameters like Compression Ratio, MSE and PSNR.

VI. RESULTS AND DISCUSSION

The objective of the research was to compress an encrypted image in efficient way. Encryption technique focus on making changes to the original image in a manner that makes it invisible. Compression is used to reduce the size of image. The objective was to provide privacy as well as least possible storage space. The same has been achieved with transformation based compression using encryption but with a new algorithm of Haar and Symlet wavelet transform. Encrypting the image with random permutation method, results in distortion of image, which is visible to human eye. The research has resulted in a good CR (Compression Ratio), MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio).

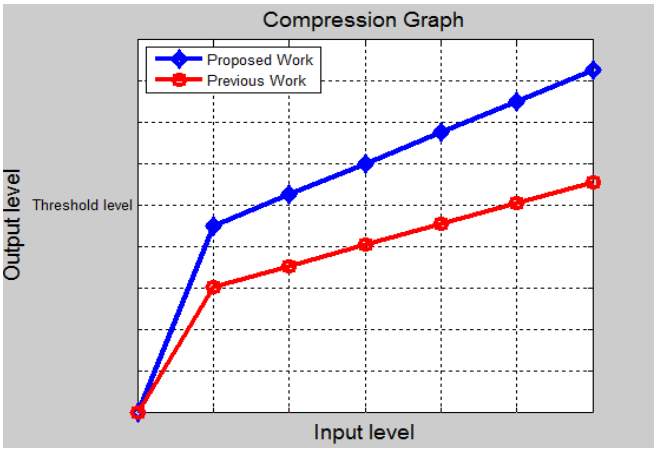

Figure 6: Compression ratio between previous and proposed work

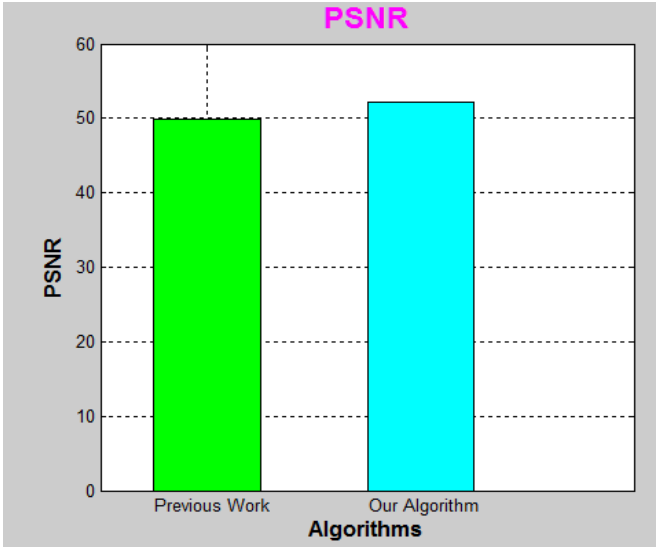

Figure 7: PSNR values of previous work and proposed work

Table 1: Comparison of PSNR between Previous and Proposed work

Comparison of PSNR between Previous and our algorithm

	Previous Work	Proposed Work
PSNR	49.9100	52.2565

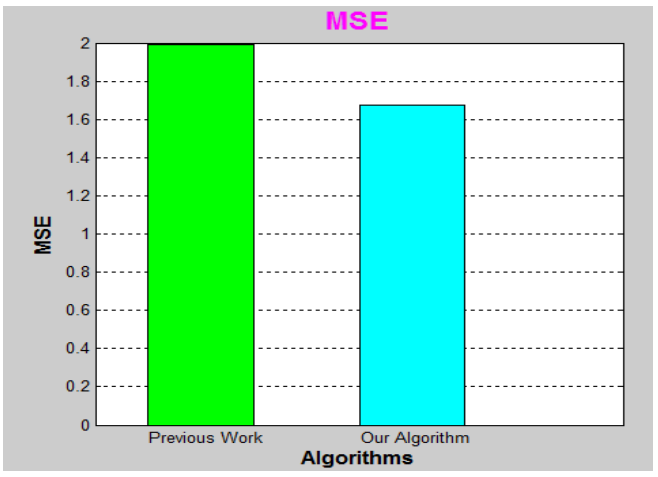

Figure 8: MSE values of previous work and proposed work

Table 2: Comparison of MSE between Previous work and proposed work

Comparison of MSE between Previous and our algorithm

	Previous Work	Proposed Work
MSE	1.9890	1.6763

CONCLUSION AND FUTURE SCOPE

In this research work, we have designed an efficient image Encryption-Compression system. Within the proposed framework, the image encryption has been achieved via random permutation. Highly efficient compression of encrypted image has been realized by a new image compression algorithm of Haar and Symlet wavelet transform. Experimental results have shown that reasonably high level of security has been retained. More notably, the coding efficiency of our proposed compression method on encrypted images is very close to that of state-of-art lossy image codecs, which receive original, unencrypted images as input. The PSNR values for resultant images are better than the previous one. Better PSNR indicates that the reconstruction of image is of higher quality. In future the same technique can be extended by applying different transforms to cover image and thus robustness of algorithm can be verified.

ACKNOWLEDGEMENT

Thanks to my Guide and family member who always support, help and guide me during my dissertation. Special thanks to my father who always support my innovative ideas.

REFERENCES

[1] Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation", IEEE Trans. Inf. Forensics Security, vol. 9, issue 1, January 2014.

[2] R. Mehala and K. Kuppusamy, "A New Image Compression Algorithm using Haar Wavelet Transformation", International Journal of Computer Applications(0975-8887), International Conference on Computing and Information Technology, 2013.

[3] X. Zhang, G. Sun, L. Shen, and C. Qin, "Compression of encrypted images with multilayer decomposition", Multimed. Tools Appl., vol. 78, issue 3, Feb. 2013.

[4] J. Zhou, X. Wu, and L. Zhang, "l_2 restoration of l_∞-decoded images via soft-decision estimation", IEEE Trans. Imag. Process. vol. 21, issue 12, Dec. 2012.

[5] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers", IEEE Trans. Inf. Theory, vol. 58, issue 11, Nov. 2012.

[6] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing", IEEE Trans. Inf. Forensics Security, vol. 7, issue 3, June 2012.

[7] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images", IEEE Trans. Imag. Process, vol. 21, issue 6, June 2012.

[8] Nidhi Sethi, Ram Krishna, R. P. Arora, "Image Compression using HAAR Wavelet Transform", IISTE Comp. Engg. & Intelligent Systems, ISSN 2222-1719, 2011

[9] X. Zhang, Y. L. Ren, G. R. Feng, and Z. X. Qian, "Compressing encrypted image using compressive sensing", in Proc. IEEE 7th IIH-MSP, Oct. 2011.

[10] M. Barni, P. Failla, R. Lazzeretti, A. R. Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural networks", IEEE Trans. Inf. Forensics Security, vol. 6, issue 2, June 2011.

[11] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image", IEEE Trans. Inf. Forensics Security, vol. 6, issue 1, Mar. 2011.

[12] W. Liu, W. J. Zeng, L. Dong, and Q. M. Yao, "Efficient compression of encrypted grayscale images", IEEE Trans. Imag. Process, vol. 19, issue 4, Apr. 2010.

[13] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals", IEEE Trans. Inf. Forensics Security, vol. 5, issue 1, Mar. 2010.

[14] V. Ashok, T. Balakumaran, C. Gowrishankar, Dr. ILA.Vennila, Dr.A.Nirmal kumar, "The Fast Haar Wavelet Transform for Signal & Image Processing", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, issue 1, 2010.

[15] Q. M. Yao, W. J. Zeng, and W. Liu, "Multi-resolution based hybrid spatiotemporal compression of encrypted videos," IEEE in Proc. ICASSP, Apr. 2009, pp. 725–728.

[16] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain", IEEE Trans. Inf. Forensics Security, vol. 4, issue 1, Mar. 2009.