International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Survey on Wavelet Based Image Encryption and Decryption

Manju Lakshmi [1], Smita C Thomas [2], Sreelakshmi K [3]

[1, 2, 3] Mount Zion College of Engineering, Kadamannitta, Pathanamthitta, Kerala

Abstract: ***The process of transmitting image encryption using the image securely over the network so that an unauthorized user cannot able to decrypt the image .Different techniques for using image encryption. The most common method of image encryption is wavelet transform. Wavelet transform of the image generates the different components basically classified in the approximation and detail components. The approximation component has major information. A partial encryption technique is using only approximation component. The decryption techniques used a key for decryption. In this paper say that survey of different wavelet based image encryption and decryption techniques.***

Keywords: image encryption, decryption, MSE, DWT, CWT, PSNR

1. Introduction

The process of transmitting image encryption using the image securely over the network so that an unauthorized user cannot able to decrypt the image. The image encryption, video encryption, have applications in many fields such as the internet communication, transmission, medical imaging, Tele-medicine and military Communication, etc. The analysis of encryption is moving towards a future of endless possibilities [1]. The bulk capability, high redundancy and high correlation among the pixels these are properties of special image data. Encryption techniques are very useful method to protecting the secret information. Encryption is process of converting a plain message into a cipher text it cannot be read by any unauthorized user without decrypting the cipher text. The process decryption is the converting the encrypted text into its original plain text which process is reverse of encryption , so that it can be read.

A wave-like oscillation with an amplitude are called wavelet that is begin at zero, increases, and then decreases back to zero Wavelet also known as one complete cycle it, is not an oscillating wave like characteristic but it has the ability to allow simultaneous time and frequency . wavelets compare with sine waves, which are the basis of Fourier analysis. Sinusoids do not have limited duration they extend from minus to plus infinity. And where sinusoids are smooth and excepted, wavelets tend to be irregular and asymmetric. Wavelet is one of the most mathematical tools in image cryptography and analysis. This wavelet has the ability to combined with other mathematical tools. Wavelet is a mathematical tool popularly used in different image processing algorithms. Wavelet are two type discrete and continuous. Continuous wavelet transform (CWT) is used in the analysis of sinusoidal time varying signals [3]. It is difficult to implement and the information that has been picked up may overlap and results in redundancy. The CWT is defined as the sum over all time of the signal multiplied by scaled, shifted versions of the wavelet function If the scales and translations are based on the power of two, DWT is used in the analysis. The discrete wavelet transform (DWT) refers to wavelet transforms for which the wavelets are discretely sampled.

A transform which used a function both in space and scaling and has some desirable properties compared to the Fourier transform. The wavelet transform based image processing algorithms mainly consists of discrete wavelet transform. The discrete wavelet transform of the digital image followed by down sampling process generates four component of the image each of 1/4size of original image. The first part is termed as the approximation component which consists of most information of image and other three parts are horizontal. The wavelet transform based image processing algorithms consists of mainly three steps. The first step is to find the discrete wavelet transform of the digital image, the next to find out the wavelet decomposition coefficient the last step is to perform the required operation on the selected coefficient and find inverse wavelet transform. Wavelet transform based image encryption consists of mainly two types that is encryption can be either partial encryption using any one or some of the components of wavelet decomposition structure or it may be full encryption algorithm using all the components of the wavelet decomposition structure [1].

The Mean square error (MSE) denotes the error in the image. Image more difficult to understand when the MSE in the encrypted image hence it improve more security. The mean squared error (MSE) or mean squared deviation (MSD) of an estimator measures the average of the squares of the errors or deviations. MSE is a risk functions, because of corresponding to the expected value of the squared error loss or quadratic loss. The difference of randomness or the estimator doesn't account for a information that could produce a more accurate estimate. MSE is a measure of the quality of an estimator it is always non-negative, and values closer to zero are better. The MSE is the second moment(about the origin) of the error. And the MSE incorporates both the variance of the estimator and its bias. For an unbiased estimator and the MSE is the variance of the estimator. Like the variance and MSE has the same units of measurement as the square of the quantity being estimated. In an analogy to standard deviation, taking the square root of MSE yields the root-mean-square error or root mean square value(RMSE or RMSD), which has the same units as the quantity being estimated; for an unbiased estimator, the

RMSE is the square root of the variance, known as the standard deviation.

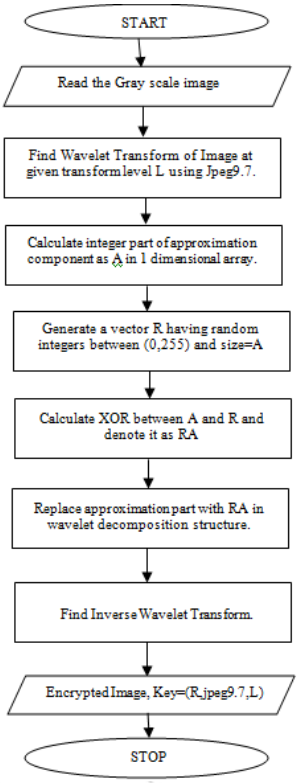
The PSNR (Peak Signal to Noise Ratio) denotes the ratio between peak signal to MSE. More the PSNR value in decrypted image means more efficiently it is decrypted. Less PSNR value in encrypted image denote more efficient image encryption. Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of loss compression codes(e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codes, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content. PSNR is most easily defined via the mean square error(*MSE*).

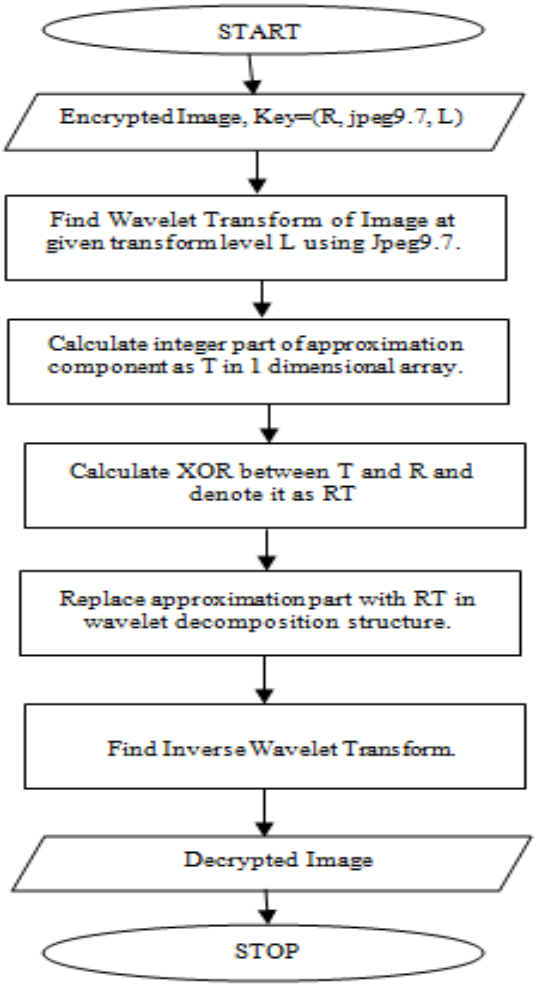
2. Literature Survey

In this paper [1] the process involve here is joint technique of the wavelet transform as used in and XOR operation as in for partial image encryption. The algorithm is used for the encryption and decryption it have written wavelet transform and inverse wavelet transform means wavelet transform followed by down-sampling and inverse wavelet transform followed by up-sampling respectively.

For algorithm to take a grey scale image. A random array R having values between 1 and 255 is generated which is equal in dimension as the approximation component of that wavelet transform. The wavelet coefficient for convolution and finding the wavelet transform of the image. The R, the wavelet applied and level of the wavelet transform should be passed as the decryption at the receiver end.

In the decryption process same random array R, name of wavelet and transform level is supplied as the key. This is used to decrypt the encrypted image. Firstly the encrypted image is wavelet transformed using same wavelet at the given level. Then its approximation component's integer part is XOR ed with R which generate approximation component of original image. Then it is inverse wavelet transformed.[1]





In this paper [2] using Fractional Wavelet Transform (FWT) and random phase masks (RPMs) for the coding of digital images. The digital image to encrypt is transformed with the

FWT, after the coefficients resulting from the FWT (Approximation, Details: Horizontal, vertical and diagonal) are multiplied each one by different RPMs (statistically independent) and these latest results is applied an Inverse Wavelet Transform (IWT), obtaining the encrypted digital image. The decryption technique is the same encryption technique in reverse sense. This technique provides immediate security compared to conventional techniques. The mathematical support for the use of the FWT in the computational algorithm for the encryption is also developed. A new scheme of digital images encryption using FWT has been proposed. For this encryption system was increased the level of security against brute force cracking by the large size of key space. The use FWT on digital images encryption increases a great deal the security parameters of the encrypted image, due to the sensitivity to any changes made on the fractional orders used (numeric key) and, in addition to this, the huge number of possibilities of using a wavelet family and several different RPMs, greatly increase the difficulty for anyone attempting to decrypt the image without being authorized. [2].

In this paper a method for an RGB image encryption supported by lifting scheme based lossless compression. Firstly we have compressed the input color image using a 2-D integer wavelet transform. Then we have applied lossless predictive coding to achieve additional compression. The compressed image is encrypted by using Secure Advanced Hill Cipher (SAHC) involving a pair of involutory matrices, a function called Mix() and an operation called XOR. Decryption followed by reconstruction shows that there is no difference between the output image and the input image. In this paper we have implemented an RGB image encryption supported by lifting scheme based lossless compression using MATLAB. In this analysis, we have considered lifting wavelet based on Haar transform. The input image and its corresponding transform coded image, encoded image, encrypted image, decrypted image, decoded image and reconstructed image. It is interesting to note that the reconstructed image is exactly identical to the original input image [3].

In this paper, we propose a novel method of gradient Haar wavelet transform for image encryption. This method use linearity properties of the scaling function of the gradient Haar wavelet and deterministic behaviors of rational order chaotic maps in order to generate encrypted images with high security factor. The security of the encrypted images is evaluated by the key space analysis, the correlation coefficient analysis, and differential attack. The method could be used in other fields such as image and signal processing. The simplest possible wavelets are Haar wavelet. They most widely used in the various sciences. Gradient Haar transform or gradient Haar wavelet transform is modified the Haar wavelet transforms which was proposed in 1909 by Alfred Haar. Based on the multi resolution analysis, Haar transforms have the scaling function and the Haar wavelet with various shifts and stretches [4].

3. Conclusion

Wavelet is one of the best mathematical tools using in image cryptography and analysis. Because it has the specific structure. The wavelet has the ability which is combined with other mathematical tools. In this paper proposed different methods of wavelet transform using in image encryption and decryption techniques. we conclude that each techniques of image encryption and decryption using very secure and different wavelet transform using.

4. Acknowledgement

We would like to thank, first and foremost, Almighty God, without his support this work would not have been possible. We would also like to thank all the faculty members of Mount zion college of engineering, for their immense support.

References

[1] Piyush Kumar Singh ",An Image Encryption Algorithm based on XOR Operation with Approximation Component in Wavelet Transform", DST-Centre for Interdisciplinary Dept. of Computer Science and Engineering.
[2] Juan M Vilardy1, J. Useche, C. O. Torres and L. Mattos, "Image encryption using the fractional wavelet transform", Laboratorio de Óptica e Informática, Universidad Popular del Cesar, IOP Publishing(2011).
[3] Ch. Samson," An RGB Image Encryption Supported by Wavelet- based Lossless Compression", Dept. of Information Technology, SNIST (IJACSA) publishing.
[4] Sodeif Ahadpour, Yaser Sadra, Meisam Sadeghi," Image Encryption Based On Gradient Haar Wavelet and Rational Order Chaotic Maps ", 1Faculty of Sciences, University of Mohaghegh Ardabili, Ardabil, Iran.

Author Profile

Manju Lakshmi obtained the Degree of Bachelor of Technology in Computer Science and Engineering from Mahatma Gandhi University, in 2015. She is now pursuing her master degree in Computer Science with specialization in Computer Science and Engineering at Mount Zion college of Engineering under Kerala Technological University.

Smita C Thomas obtained B.Tech in Computer Science and Engineering, and M.Tech in Computer Science. She is currently working as Assistant Professor in Mount Zion College of Engineering.