IMAGE ENCRYPTION TECHNIQUE INCORPORATING WAVELET TRANSFORM AND HASH INTEGRITY

Manish Mishra[1], Shraddha Pandit[2]

[1]*ICOT, M.Tech. Student, Department of Computer Science, Bhopal, MP, India*
[2]*Asst. Prof, Department of Computer Science and Engineering, ICOT, Bhopal, MP, India*

Abstract

This paper is basically designed for image encryption using wavelet Transform Techniques and its integrity incorporating hash value with SHA-256. Techniques which is involved in encryption is image confusion, image diffusion, wavelet Transform, Inverse wavelet Transform and finally hash value computation of original image. Techniques which are involved for Decryption is reverse of Encryption.

Keywords: *wavelet Transform, Hash value, Encryption, Decryption.*

----------***----------

1. INTRODUCTION

Encryption is a Technique which is used to encode the data of any object such as image, video, audio and Text. Decryption is a Technique which is used to decode the encoded information based on our specific requirement [3]. In this paper wavelet transform has been used to encode the information and reverse for decode the information. This paper has been also introduced the integrity with security and integrity is a higher level of security maintenance; here SHA-256 has been used to balance the integrity approach of cryptography.

1.1 Wavelet Transform

Wavelet Transform is used to have local parametric interval based on time series. It is observed by two different passes i.e. high pass and low pass. Low pass Technique is used to find the nearest co-efficient and it goes further as a recursive parameter, where as High pass is always constant. Discrete Wavelet Transform (DWT) is used to find local time interval [1].

Equation of wavelet Transform

$$\gamma(s,\tau)=\int f(t)\Psi^*_{s,\tau}(t)\,dt \quad \text{----------(i)}$$

$\gamma(s,\tau)$ is the coefficient of wavelet with scale 's' and time 'τ' , f(t) denotes time series, $_{s,\tau}(t)\,dt$ is complex conjugate of wavelet with scale 's' and time 'τ', Ψ^* is used for assuming real wavelet transform.

$$\Psi^*_{s,\tau}(t)=1/\sqrt{s}\;\Psi(t-\tau)/S \quad \text{---------- (ii)}$$

$\Psi^*_{s,\tau}(t)$ wavelet with scale 's' and time 'τ'.
$1/\sqrt{s}$ are normalization and $(t-\tau)$ means shift in time.
S means change in scale of wavelet.
Ψ means mother wavelet.

$$\Psi= 2\sin\theta(2t)-\sin\theta(t) \quad \text{----------(iii)}$$

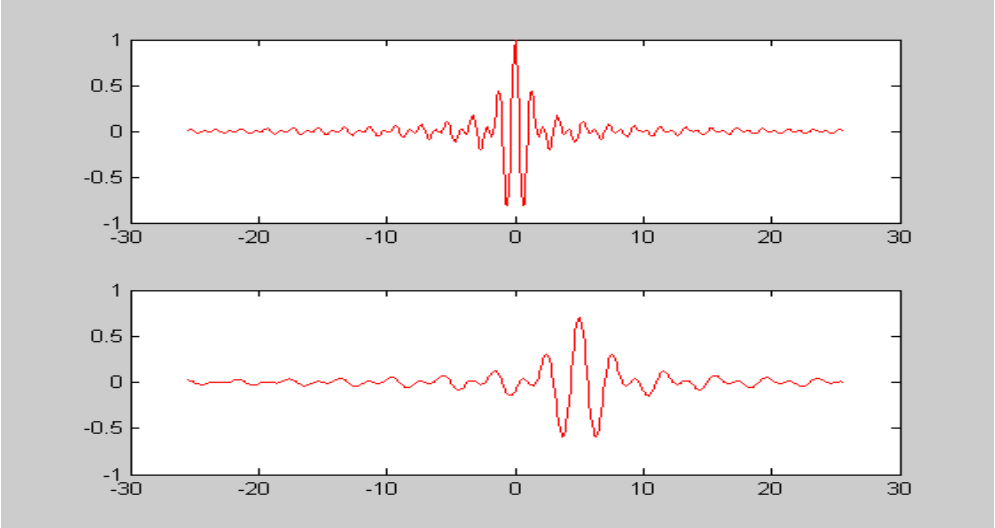


Fig 1 Mother wavelet to find nearest co-efficient

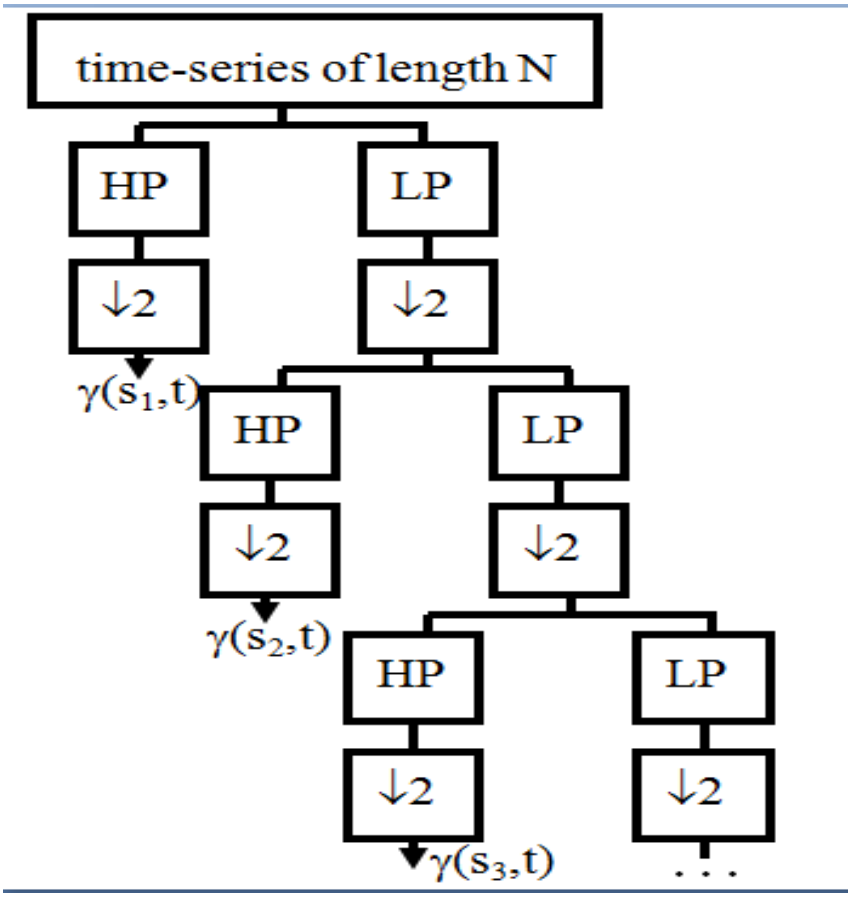


Fig 2 Discrete Wavelet Transform to find coefficient.

γ (s₁, τ) : N/2 Co-efficient. **γ (s₂, τ)** : N/4 Co-efficient.
γ (s₃, τ) : N/8 Co-efficient. Total: **N** Co-efficient**.**
Figure 2 effects have been shown in result.

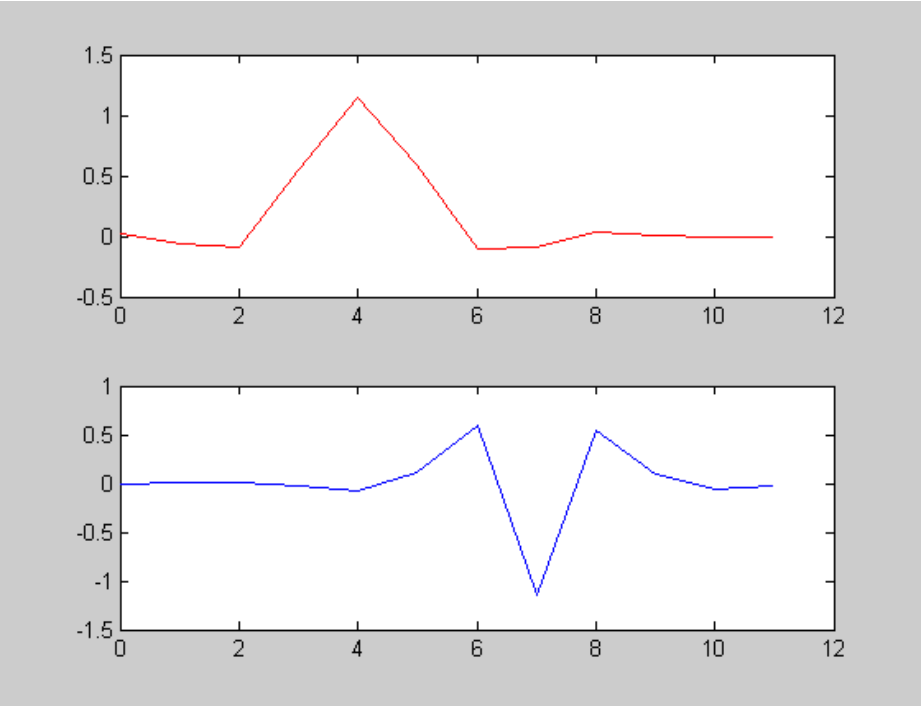


Fig 3 Time Series of Low and High Pass Co-efficient

1.2 Diffusion /Confusion Technique

In Image Cryptography confusion is a technique which is used for image pixel permutation in a secret order, without any changes in their values. The function of the diffusion is to modify the pixel values sequentially so that tiny changes in one pixel are spread out of many pixels, hopefully the whole image. To decorrelate the relationship between adjacent pixels, the confusion stage is performed ***n times*** where n is usually larger than 1. This is followed by the diffusion stage. The whole n-round confusion and single round diffusion repeat for ***m times,*** with m usually larger than 1, so as to achieve a satisfactory level of security. The parameter of permutation is calculated with equation (iv) in 2D.

$$\left.\begin{aligned} X_{k+1} &= (x_k + y_k + r_x + r_y) \text{ MOD } N \\ Y_{k+1} &= (y_k + r_y + K_c \sin(2\Pi x_{k+1}/N)) \text{ MOD } N \end{aligned}\right\} \quad \textbf{(iv)}$$

K_c is a positive integer.
r_x and r_y are a random value of permutation.
x_k and y_k are original value of image pixel.

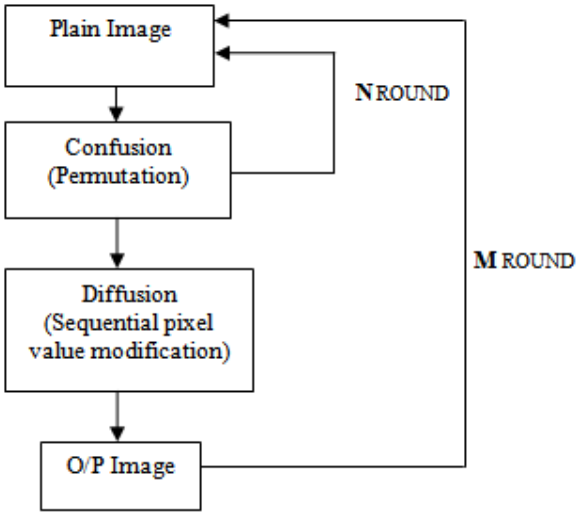


Fig 4 for confusion and diffusion process

1.3 Inverse Wavelet Transform

Inverse wavelet is used to reconstruct the data from the given co-efficient by performing single level or multilevel of inverse discrete wavelet transform.

$$f(t)=\int\int \gamma(s,\tau)\, \Psi_{s,\tau}(t)\, d\tau ds \quad \text{----------(v)}$$

$$\Psi_{s,\tau}(t)=1/\sqrt{s}\, \Psi(\tau-t)/S \quad \text{----------(vi)}$$

$f(t)$ denotes time series.
$\gamma(s,\tau)$denotes coefficient of wavelet.
$\Psi_{s,\tau}(t)d\tau ds$ denotes wavelet with scale s and time τ.

1.4 Hash Value Computation

A hash function is used to produce a fixed length output for arbitrary input message. The fixed length output or hash value is generated by decomposing the message into smaller equal size block, now these blocks are operated sequentially using compression function[5]. The last block processed also indicates the length of message, which enhances the properties of the hash. The majority of the hash functions like MD4, MD5, and SHA family are used in this form.

1.5 Proposed Methodology

The survey of the several research papers show that encryption is used for security but security does not have integrity alone so maintaining the integrity Hash function has been used in proposed algorithm. The proposed work will help in safely delivering and sharing of information and avoid the access of unauthorized users. The proposed method has been summarized in figure 5.

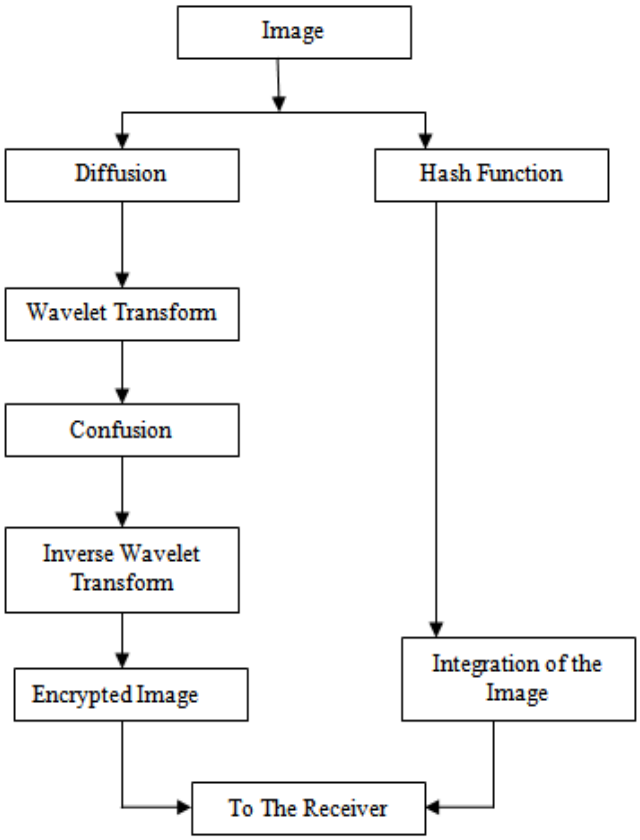


Fig 5 Flowchart of Proposed Method

2. ANALYSIS OF WAVELET TRANSFORM

2.1 Wavelet and DCT

Discrete Cosine Transform (DCT) Technique is used for compression of image and Decompression of image but in this technique mean square error (MSE) are high as well as pick signal to noise ratio (PSNR) is very low. DCT is not having local change in coefficient because of its PSNR effect as well as MSE [11]. Wavelet Transform is used to have compression and decompression but it is having very low MSE and high PSNR so that local effect of image can be easily maintained [4].

2.2 Wavelet and Fourier Transform

Wavelets are localized in both time and frequency whereas the standard Fourier transform is only localized in frequency. The wavelet transform take advantage of the intermediate cases of the Uncertainty Principle. Each wavelet measurement (the wavelet transform corresponding to a fixed parameter) tells you something about the temporal extent of the signal, as well as something about the frequency spectrum of the signal. That is to say, from the parameter *w* (which is the analogue of the frequency parameter *k* for the Fourier transform), we can derive a characteristic frequency *k*(*w*) and a characteristic time *t*(*w*), and say that our initial function includes a signal of "roughly frequency *k*(*w*)" that happened at "roughly time *t*(*w*)". The classical Fourier transform of a function allows you to make a measurement with 0 bandwidth: the evaluation *f*^(*k*) tells us precisely the size of the component of frequency *k*. But by doing so you lose all control on spatial duration: you do not know when in time the signal is sounded. This is the limiting case of the Uncertainty Principle: absolute precision on frequency and zero control on temporal spread [19]. (Whereas the original signal, when measured at a fixed time, gives you only absolute precision on the amplitude at that fixed time, but zero information about the frequency spectrum of the signal, and represents the other extreme of the Uncertainty Principle.)

3. ANALYSIS OF HASH VALUE

There is several well-known hash functions used in cryptography. These include the message-digest hash functions MD2, MD4, and MD5, used for hashing digital signatures into a shorter value called a message-digest, and the Secure Hash Algorithm (SHA), a standard algorithm, that makes a larger (60-bit) message digest and is similar to MD4. A hash function that works well for database storage and retrieval, however, might not work as for cryptographic or error-checking purposes but it can work for integrity. A hash function hash is a transformation that takes an input sequence of bits m (the message) and returns a fixed-size string, which is called the hash value(also the message digest, the digital fingerprint). The basic requirement for a cryptographic hash function is that the hash value does not reveal any information about the message itself, and moreover that it is hard to find other messages that produce the same hash value. If only a single bit of the message is changed, it is expected that the new hash value is dramatically different from the original one. A hash function is required to have the following features: Preimage resistant. A hash function hash is said to be preimage resistant if it is hard to invert, where “hard to invert” means that given a hash value h, it is computationally infeasible to find some input x such that hash (x)=h Second preimage resistant. If, given a message x , it is computationally infeasible to find a message y different from x such that hash(x)=hash(y), then hash is said to be second preimage resistant Collision-resistant. A hash function hash is said to be collision-resistant if it is computationally infeasible to find two distinct messages x and y such that hash(x)=hash(y).

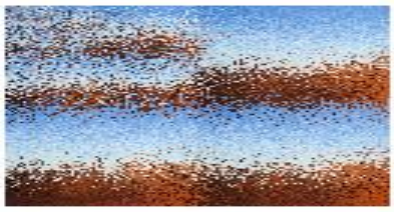
Result

Encryption Technique

Confusion

Inverse wavelet

Encryption



Decryption Technique

Encrypt

Inverse Wavelet

Confusion

Hash value of Image
ec738cddec9221b7c5f82dee555099e6d103111873275b750e bce0efe9410c1e

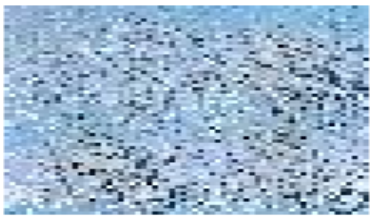
Encryption Technique

Hash value
ec738cddec9221b7c5f82dee555099e6d103111873275b750e bce0efe9410c1e

Decryption Technique

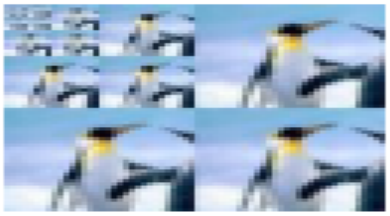
Confusion

Encrypt



Inverse wavelet

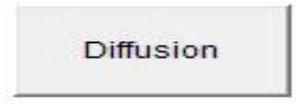
Inverse Wavelet



Encryption

Confusion

Hash value
a46897b8e26cbfe09448d4ee612423db820f8c118bbfc9166d
29629a2bda4ed8



Hash value
a46897b8e26cbfe09448d4ee612423db820f8c118bbfc9166d29629a2bda4ed8

4. CONCLUSION AND FEATURE ENHANCEMENT

This paper is used with cryptography technique using wavelet transform. In this paper Hash value is matched for making integrity of original image. The image encryption techniques have been implemented using DWT (discrete wavelet transforms). This paper shows that the method have been achieved to maintain the privacy of the image as well as integrity of the image in unreliable channel, so increase in demand of internet and the information which is being shared on it requires the method which can maintain privacy and integrity of the image during the transmission from unauthorized and illegal access. Therefore this paper presents a new method for the encryption of image. The proposed method is efficient and will deliver the image safely to the receiver. This Technique (Wavelet) can also be used for Compression of image and other source of file.

REFERENCES

[1] D. Sinha and A. Tewfik. "Low Bit Rate Transparent Audio Compression using Adapted Wavelets", IEEE Trans. ASSP, Vol. 41, No. 12, December 1993

[2] P. Srinivasan and L. H. Jamieson. "High Quality Audio Compression Using an Adaptive Wavelet Packet Decomposition and Psychoacoustic Modeling", IEEE Transactions on Signal Processing, Vol. 46, No. 4, April 1998.

[3] Burrus, C.S., Gopinath, R.A., Guo, H., 1998.Introduction to Wavelets and Wavelet Transforms New Jersey: Prentice-Hall.

[4] PrabhakarTelagarapu, V.Jagan Naveen, A.Lakshmi..Prasanthi,G.Vijaya Santhi, "Image Compression using DCT and Wavelet Transform" in International Journal of Signal Processing, Image Processing and Pattern Recognition(IJSIP). Vol 4. 3 September,2011

[5] Khalifa O. O., Review of Wavelet theory and its application to Image Data Compression, International Islamic University Malaysia Engineering Journal, Vol.4, No.1, p25-43, 2003.

[6] Khars, M., & Brandenburg, K., 1998.Applications of Digital Signal Processing to Audio and Acoustics. Massachusetts: Kluwer Academic Publishers.

[7] Philip P. Dang and Paul M. Chau, "Image Encryption for Secure Internet Multimedia Application", IEEE Transaction on Consumer Electronics , Vol 46, No. 3 pp. 395-403 AUGUST 2000.

[8] S. Singh, and G. Agarwal, "Use of image to secure text message with the help of LSB replacement," International Journal of Applied Engineering Research, Dindigul, Vol. 1, No. 1, 2010, pp. 200–205.

[9] C. Chan, and L. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, Vol. 37, 2004, pp. 469–474.

[10] K. Kumar, K. Raja, R. Chhotaray, and S. Pattanaik, "Bit Length Replacement Steganography Based on DCT Coefficients," International Journal of

Engineering Science and Technology, Vol. 2, No. 8, 2010, pp. 356–570.

[11] C. Lin, and P. Shiu, "High Capacity Data Hiding Scheme for DCT-based Images," Journal of Information Hiding and Multimedia Signal Processing, Vol. 1, No. 3, 2010, pp. 220–240.

[12] A. Al-Ataby, and F. Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform," The International Arab Journal of Information Technology, Vol. 7, No. 4, 2010, pp. 358–364.

[13] P. Chen, and H. Lin, "A DWT Based Approach for Image Steganography," International Journal of Applied Science and Engineering, Vol. 4, No. 3, 2006, pp. 275–290.

[14] L. Ganesan, and S. Jinna, "Reversible Image Data Hiding Using Lifting Wavelet Transform and Histogram Shifting," International Journal of Computer Science and Information Security, Vol. 7, No. 3, 2010, pp. 283–290.

[15] S. Singh, and T. Siddiqui, "A security Enhanced Robust Steganography Algorithm for Data Hiding," International Journal of Computer Science Issues, Vol. 9, No. 1, 2012, pp. 131- 139.

[16] C. Kung, S. Chao, Y. Tu, and Y. Yan, "A Robust Watermarking and Image Authentication Scheme used for Digital Contant Application," Journal of Multimedia, Vol. 4, No. 3, 2009, pp. 112-119.

[17] G. Xuan, Y. Shi, C. Yang, Y. Zheng, D. Zou, and P. Chai, "Lossless Data Hiding Using Integer Wavelet Transform and Threshold Embedding Technique," Multimedia and Expo, ICME, IEEE International Conference, 2005, pp. 1520–1523.

[18] C. Chang, P. Pai, C. Yeh, and Y. Chan. "A high payload frequency-based reversible image hiding method," Information Science, Elsevier 180, 2010, pp. 2286–2298.

[19] J. Shapiro, "Embedded Image Coding Using Zerotrees of Wavelet Coefficients," IEEE Transaction On Signal Processing, Vol. 4, No. 12, 1993, pp. 3445–3462.

[20] M. Abu Zaher, "Modified Least Significant Bit (MLSB)," Computer and Information Science, Vol. 4, No. 1, 2011, pp. 60–67.