# Image Encryption for Secure Internet Transfer using DWT with AES Algorithm

Dr. G. Vinoth Chakkravarthy[1], Lingeshwaran R[2], Nirmal Raaj S[3], Selvakumar C[4], Naveen Prasath M[5]

Associate Professor, Department of CSE, Velammal College of Engineering and Technology, Madurai, India[1]

UG Students, Department of CSE, Velammal College of Engineering and Technology, Madurai, India[2][3][4][5]

**ABSTRACT**: This Image Encryption algorithm makes use of keying a fused image(wavelet transform of the original image infused with the wavelet transform of dummy image), so how it's different from the normal image cryptography, here instead of keying a host image with a complex mathematical equation we are increasing its possibilities by a mixed wavelet algorithm,here we split different regions of the host image and the fusing image by using DWT[1] and intermixing those regions to achieve another image processed by DWT of the same format,which on inverse fusing among themselves , results in fusion image whose values are furthered enhanced with majority of dummy image after mixed DWT,these fused images will be masked by a means of a key, which is then transmitted.The **correlation** of this original image and the fused image with simple keying method are **less than 0.083** and which can withstand even Brute force-attack. So in order to decrypt this image,we need to know the key which is been used plus the dummy image which has been used for the fusion.Without knowing proper arrangement of this Image matrix followed, it would be impossible to fetch the data, the decrypting time taken is reportedly longer than the encryption.

**KEYWORDS**: Encryption, Image Compression, DWT, AES, Decryption, bands

## I. Introduction

In recent years, along with the rapid promotion and popularization of network technology and digital communication technology in the world, digital images, and digital video-based digital images have become an important medium for information storage and transmission in the computer network in the civil and military fields. However, network security issues have long been an important factor that plagued and restricted the development of network technology. Especially in the context of the information resources of the public and government departments, how to realize the data security protection in the computer network is the important content and direction of the research in the field of network security and information security. Among them, digital image and digital video have become the important content of data transmission in the network by virtue of its intuitiveness and convenience. Therefore, the security protection of digital images has received great attention from all parties. Especially in the background of the increasingly severe network security situation in recent years, information transmission and sharing based on digital images often face the problems of data theft, tampering, deletion, and attack, which have caused great losses to the owners or publishers of digital images.

## II. Related work

Secured image encoding is one of the novel methodologies that have been embraced in UVs for data transmission to the base station. The input image caught by the UVs is transformed utilizing Discrete Wavelet Transform (DWT) to get different sub bands, the sub bands are quantized and the quantized sub bands are encrypted. The encoding strategy, for example, Huffman encodes the encrypted data and compresses the data caught, and is transmitted to the base station. Figure 1 shows the block diagram of secured image coding [17]. DWT has been generally utilized as a part of numerous diverse fields of audio and video signal processing. DWT is constantly progressively utilized as compelling answers for the issue of image compression. Quantizer is the procedure of approximating the continuous set of values in the image data with a finite set of values. The outline of the quantizer has a critical effect on the measure of compression got and loss caused in a compression plan. AES is a block cipher with variable key length (128-bit, 192-bit, and 256-bit separately) and block size of 128-bit. AES require low memory to make it extremely appropriate for confined space situations, in which it additionally shows great execution. Huffman coding is a manifestation of encoding that makes the most productive set of prefix codes for a given content. The standard is to utilize a lower number of bits to encode the data that happens all the more as often as possible. The controller is a module required for improving provisions security prerequisites based on a variable framework asset.In this paper we investigate the execution of secure image coding utilizing software reference model.

## III. SYSTEM ARCHITECTURE

The below figures were explained the System Architecture (Figure. 3.1) and data flow diagram (Figure. 3.2) of the proposed system.

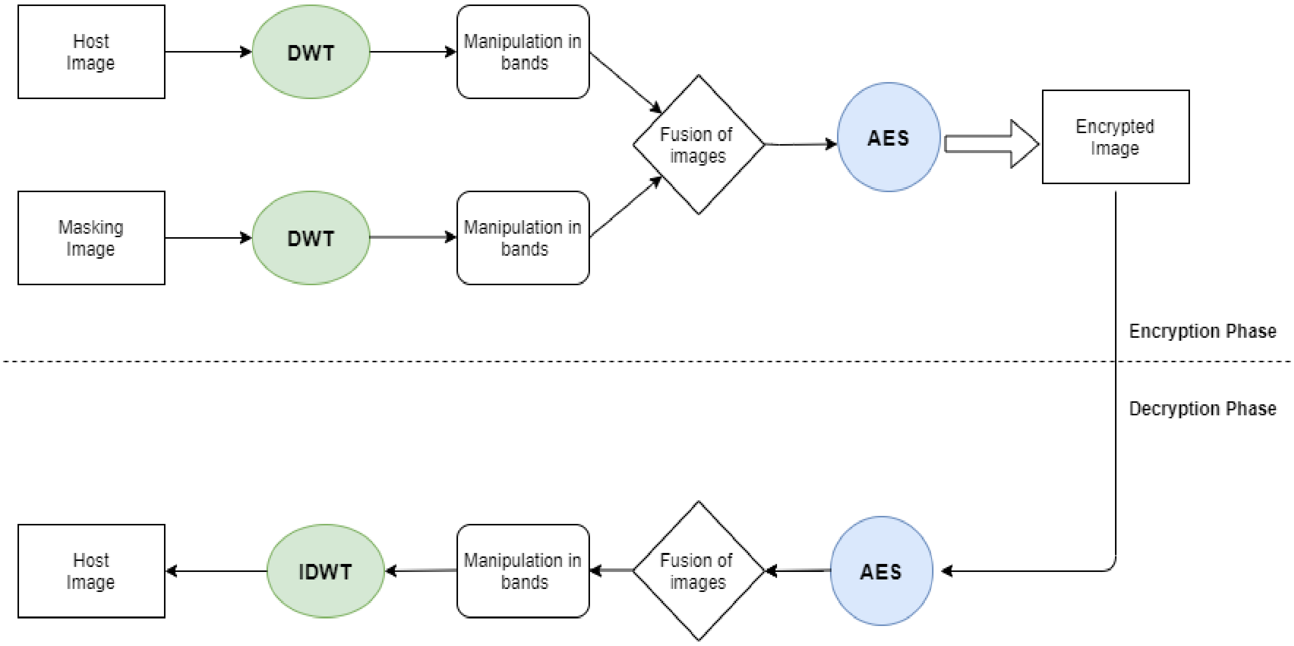

Figure. 3.1 System Architecture

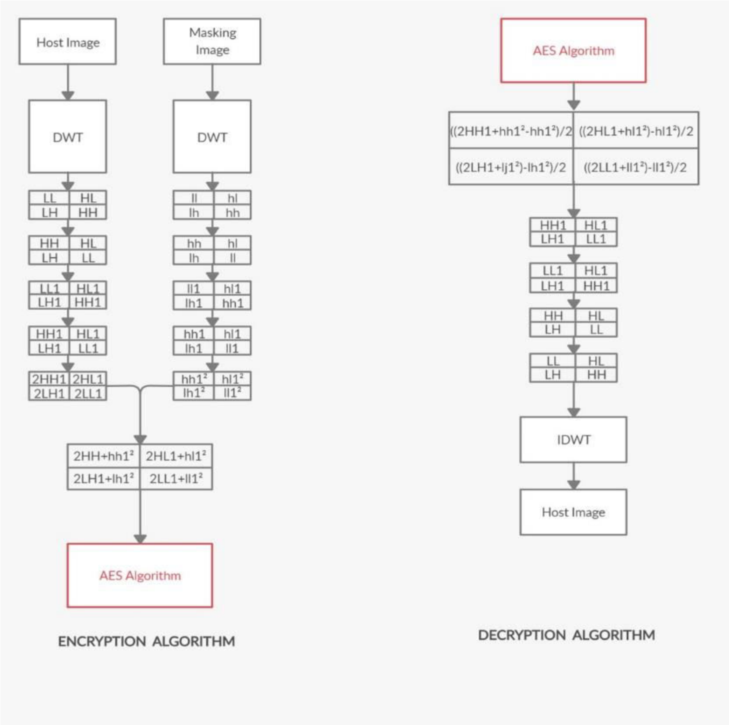

Figure. 3.2 Data Flow Diagram

## IV. METHODOLOGY

To improve the security of transferring an image through internet, we using the DWT compression and AES Encryption to transfer the image. In another end, decrypt the file using the AES algorithm.

### *a.Discrete Wavelet Transform (DWT)*

An image is represented as a two-dimensional array of coefficients, each coefficient representing the brightness level in that point. When looking from a higher perspective, we can't differentiate between coefficients as more important ones, and lesser important ones. But thinking more intuitively, we can. Most natural images have smooth colour variations, with the fine details being represented as sharp edges in between the smooth variations. Technically, the smooth variations in colour can be termed as low frequency variations and the sharp variations as high frequency variations.
The low frequency components (smooth variations) constitute the base of an image, and the high frequency components (the edges which give the detail) add upon them to refine the image, thereby giving a detailed image. Hence, the smooth variations are demanding more importance than the details. Separating the smooth variations and details of the image can be done in many ways. One such way is the decomposition of the image using a Discrete Wavelet Transform (DWT).

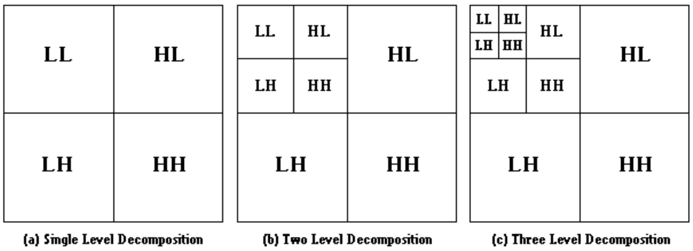
LL
HL
LH
HH
(a) Single Level Decomposition
LL
HL
LH
HH
HL
LH
HH
(b) Two Level Decomposition
LL
HL
LH
HH
HL
LH
HH
HL
LH
HH
(c) Three Level Decomposition

Figure 4.1 Pyramidal Decomposition of an Image

### *b. Advanced Encryption Standard (AES) Encryption*

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

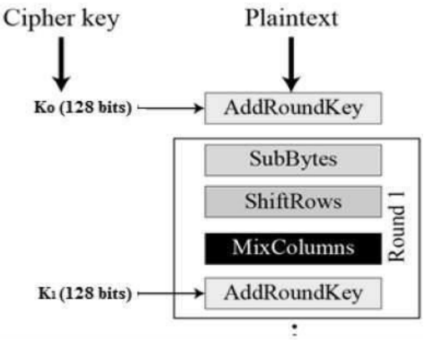

Fig. 4.2 AES Encryption

*c. Advanced Encryption Standard (AES) Decryption*

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order.

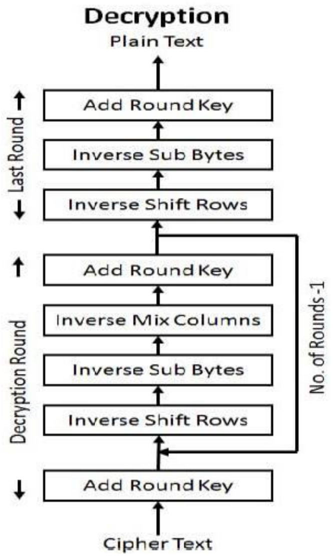

Fig. 4.3 AES Decryption

## V. IMPLEMENTATION DETAILS

The system allows the user to login and upload an image with limited size and in-different types in the image format. Once the image has been uploaded, the image was redirected to the compressor. The decomposer which decomposed the image as bands were processed by the DWT Algorithm.

Once the DWT algorithm, decomposesthe image. It returns the points and moved towards the Encryptor.

Figure. 5.1 Representation of Decomposition Image

The Encryptor takes the input from DWT bands and encrypt using the AES Algorithm with the help of Private Key. The Private Key which is used to encrypt the DWT bands. The System finally generates the encrypted file for the user.

In the Decryptor end, the user uploads the encrypted file using the system. The file has been decrypted by the same private key which is used to encrypt the same. It returns the bands which is decomposed by IDWT.

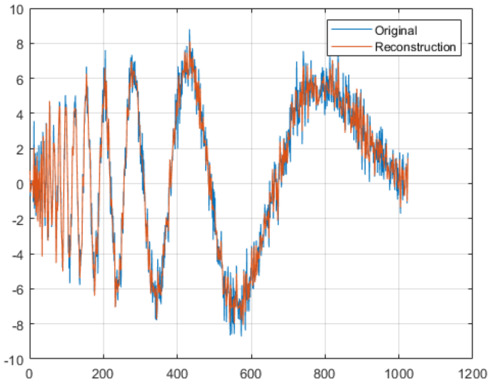

Figure 5.2 Graphical Representation of Decrypted File

## VI. RESULTS

Time complexity played a vital role in image encryption and compared to text Encryption process. The DCT Decomposition and AES Encryption security wise results are better performance and more secured encrypted file which is very difficult to crack when we use AES over DWT.

## VII. FUTURE WORK

In the future compress and encrypt more than one images at a time and also it’s tries to improve no one should crack the encrypted file.

## VIII. CONCLUSIONS

In the paper results and discussions prove that the image has been transferred through internet using Discrete Wavelet Transform (DWT) and AES Encryption and Decryption (AES). AES gives the better assurance and performance of the process.

## REFERENCES

1. Ravi S P, Dhanalakshmi L, "DWT and Modified AES based Secure Image Steganography on ARM A8 Processor," 2015 International Journal of Engineering Research & Technology (IJERT).
2. Jie Cui and others, ‘An Improved AES S-Box and Its Performance Analysis’, International Journal of Innovative Computing, Information and Control, 7 (2011), 2291–2302.
3. Neha Gupta and NidhiSharma,“Dwt and Lsb Based Audio Steganography” International Conference on Reliability, Optimization and Information Technology -ICROIT 2014, Feb 2014.
4. JaspalKaurSaini and Harsh K Verma, “A Hybrid Approach for Image Security by Combining Encryption and Steganography” IEEE Second International Conference on Image Information Processing (ICIIP-2013)
5. Manoj .B,Manjula N Harihar (2012, June). “Image Encryption and Decryption using AES”, International Journal of Engineering and Advance Technology (IJEAT) volume-1, issue-5, pp.290-294.
6. Kundankumar R. Saraf,Sunita P. Ugale, “Implementation of text encryption and decryption in Advance Encryption Standard”, ASM’S International E-journal of ongoing Research in Management and IT.
7. VedkiranSaini, ParvinderBangar, Harjeet Singh Chauhan, (2014, April).”Study and Literature Survey of Advanced Encryption Algorithm for Wireless Application”, International Journal of Emerging Science and Engineering ( IJESE) volume-2, issue-6, pp.33-37.
8. Sourabh Singh, Anurag Jain, (2013, May). “An Enhanced Text to Image Encryption Technique using RGB Substitution and AES”, International Journal of Engineering Trends and Technology (IJETT) volume-4,issue-5,pp.2108-2112.