**SECURED DATA TRANSMISSION USING WAVELET BASED STEGANOGRAPHY AND CRYPTOGRAPHY BY USING AES ALGORITHM**

**ABSTRACT**

The transmission of data through any channel of communication needs strong encryption techniques for the purpose of data security. The digital watermarking plays an important role in embedding information into a digital image signal, for verification and identity of its owners. In discrete wavelet transform, “analysis filter bank “can be used for analyzing image signal by passing through it.. This filter bank consists of a low pass and a high pass filter at each decomposition stage. In this paper, a method to combine steganography (Least Significant Method) and cryptography (AES) is considered, so as to provide a more secure way for data transmission through any unsecured or public networks. Before embedding the text in image, text is encrypted using Advanced EncryptionStandard (AES) algorithm. The text can be a sentence or a key with alphabetic words having the length of 8 characters. Using Least Significant Bit (LSB) method, the encrypted text is embedded into the “LL sub-band wavelet decomposed image”. The inverse wavelet transform is applied and the resultant image is transmitted to the receiver. Now at the receiver’s end, the imagetransformed using wavelet and encrypted text is extracted by using LSB method.

**OBJECTIVES**

* To enhance the security of the data transmission.
* ToDesign a method that is robust against hacking.
* To improve image quality and embedding capacity.

**EXISTINGSYSTEM**

To hide the secret information, the message is embedded in cover text by using some embedding algorithm.The image Steganography allows the two parties to communicate secretly by allowing copyright protection and using digital watermark. The revised LSB matching was proposed to improve by applying lowering the number as a modification.To improve the image quality, the optimal LSB substitution, the approximately optimal LSB substitutions based on genetic algorithm and the modulus LSB substitution proposed.

In cryptographic solutions DES and AES will provide the security but from cryptography point of view they differ one is symmetric and another one is asymmetric.

**EXISTING SYSTEMDRAWBACKS**

* Theconventional encryption methods failed to give the desired result of protecting the data.
* DES is breakable,as the key is 56-bit length .
* The existing Encryption Standard comparatively slower.

**PROPOSED SYSTEM**

In this paper, a new method is used to send the data in a more secured manner. The given text which is to be transmitted is encrypted with one of the symmetric key techniques: Advanced Encryption Standard (AES) is a symmetric encryption algorithm in which we can use only one key for both encryption and decryption that can be used by sender and receiver. In this process by using the key, the given text is encrypted. Then, that cipher text is embedded into the LL sub-band of the wavelet transformed image. The method to embed the data is the Least Significant Method. As weare modifying the LSB (±1 or no change to the given pixel value) since our human eye cannot find the difference between the original image and the watermarked image. Once the cipher text is embedded into the LL sub-band,inverse wavelet transform is applied. Then this resultant image is sent to the receiver.

At the receiver’s end, the receiver does the forward wavelet transform of the received image. Now, from the LL sub-band, the text is extracted. The extracted text which has encrypted form is decrypted using the one key.

**PROPOSED SYSTEM BLOCK DIAGRAM**

**INPUT IMAGE**

**DISCRETE WAVELET TRANSFORM (DWT)**

**DECOMPOSED IMAGE**

**HIGH FREQUENCY COEFFICIENTS**

**LOW FREQUENCY COEFFICIENTS**

**HL**

**HH**

**ENCRYPTION (AES)**

**TEXT**

**LL**

**KEY**

**INVERSE DISCRETE WAVELET TRANSFORM**

**SEND IMAGE**

**FIGURE 1: PROPOSED SYSTEM AT SENDER SIDE.**

**FORWARD WAVELET TRANSFORM**

**DECRYPTION (AES)**

**ORIGINAL TEXT**

**RECEVIED IMAGE**

**KEY**

**FIGURE 2: PROPOSED SYSTEMAT RECEVIER SIDE.**

**FLOW CHART:**

TEXT

IMAGE

KEY

WAVELET TRANSFORM

ENCRYPTION

ENCRYPT Text

SEND IMAGE

INVERSE WAVELET TRANSFORM

LL sub-band

WAVELET TRANSFORM

LL sub-band

DECRYPTED DATA

EXTRACTED DATA

**PROPOSED METHODOLOGIES**

**Algorithm-1: Least Significant Method**

Step-1: Read the value of the pixel.

Step-2: Convert it to its equivalent binary form.

Step-3: Modify the least significant bit accordingly.

**Algorithm-1: AES is a block cipher.**

It contains the byte substation, shift rows, mix columns and then add round key.

**PROPOSEDSYSTEM ADVANTAGES**

* Our proposed method shows better performance compared to existing.
* It is safe, secure and protected transmission of data .
* AES is faster.
* In AES we can use 128,192 or 259 bits long key ,so AES key is harder to break than DES,
* The encrypted text is embedded in the LL-sub-band of the wavelet transformed image.

**SOFTWARE REQUIREMENTS**

* MATLAB 7.14 Version R2012

**MATLAB**

The MATLAB high-performance language for technical computing integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

* Data Exploration ,Acquisition ,Analyzing &Visualization
* Engg drawing and Scientific graphics
* Analyzing of algorithmic designing and development
* Mathematical functions and Computational functions
* Simulating problems prototyping and modeling
* Application development programming using GUI building environment.

Using MATLAB, you can solve technical computing problems faster than with traditional programming languages, such as C, C++, and Fortran.

**Expected input and output**

**Input**

* Any input images ,medical images ,Text Files

**Output**

* Encrypted images, Decrypted Images