# 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.

# Chapter 1

## INTRODUCTION

Data security is paramount concern for all the net users irrespective of the network. The present day hackers are a threat to the data and the threat hangs like a Damocles sword. The transmission of data through any channel of communication needs strong encryption techniques for the purpose of data security. The recent trends and development in information technology highlights the need for safe, secure and protected transmission of data. The conventional encryption methods failed to give the desired result of protecting the data. Simple way is to come up with unique id and passwords, and a combination of alphabets & numerical .AES has emerged as a frontrunner and efficient algorithm because of inherent inbuilt in advantage of better security with less implementation complexity. After extensive research in image coding, for image compression application, DWT works as a standard tool, for their data reduction capability. The complete image is compressed and transformed into a single data object by

wavelet compression system, rather than block by block as in a DCT-based compression system. When the entire image is achieved there will be a uniform distribution of compression error across that image. An image resolution enhancement in the wavelet domain is a subject of interest for further research and recently many new algorithms have been proposed. Of these the Discrete Wavelet Transforms (DWT) is the most-suited application. DWT decomposes an image into different sub-band images. Which can be named as low-low (LL), low-high (LH), high-low (HL), and high-high (HH).Here the sub-bands have the same size as the input image. Xuan et al.’s method is based on the integer wavelet transform to improve the embedding capacity .

### 1.2 Aim & Objective of the Project

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

# Chapter 2

## LITERATURE SURVEY

**TITLE:** “High capacity image steganographic model”

**AUTHOR:** Y. Lee, L. Chen,

**DESCRIPTION:** Steganography is an ancient art of conveying messages in a secret way that only the receiver knows the existence of a message. So a fundamental requirement for a steganographic method is imperceptibility; this means that the embedded messages should not be discernible to the human eye. There are two other requirements, one is to maximise the embedding capacity, and the other is security. The least-significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image. However, how to decide on the maximal embedding capacity for each pixel is still an open issue. An image steganographic model is proposed that is based on variable-size LSB insertion to maximise the embedding capacity while maintaining image fidelity. For each pixel of a grey-scale image, at least four bits can be used for message embedding. Three components are provided to achieve the goal. First, according to contrast and luminance characteristics, the capacity evaluation is provided to estimate the maximum embedding capacity of each pixel. Then the minimum-error replacement method is adapted to find a grey scale as close to the original one as possible. Finally, the improved grey-scale compensation, which takes advantage of the peculiarities of the human visual system, is used to eliminate the false contouring effect. Two methods, pixelwise and bitwise, are provided to deal with the security issue when using the proposed model. Experimental results show effectiveness and efficiency of the proposed model.

**TITLE:** “A Practical Approach for Secured Data Transmission using Wavelet based Steganography and Cryptography”

**AUTHOR:** M. IndraSena Reddy,

**YEAR: 2013**

**DESCRIPTION:** Steganography and cryptography methods are used together with wavelets to increase the security of the data while transmitting through networks. In the discrete wavelet transform, an image signal can be analyzed by passing it through an analysis filter bank. This analysis filter bank consists of a low pass and a high pass filter at each decomposition stage. Another technology, the digital watermarking is the process of embedding information into a digital (image) signal which may be used to verify its authenticity or the identity of its owners. The watermark to be embedded is ‘text’. Before embedding the plain text into the image, the plain text is encrypted by using Data Encryption Standard (DES) algorithm. The plain text can be any sentence in English, and the key can be anything in English with a length of 8-characters. The encrypted text is embedded into the LL subband of the wavelet decomposed image using Least Significant Bit (LSB) method. Then the inverse wavelet transform is applied and the resultant image is transmitted to the receiver. At the receiver’s end, the image is transformed using wavelet, from the LL subband the encrypted text is extracted by using the LSB method and the result is decrypted using DES.

**TITLE:** “Secured Data Transmission using Wavelet based Steganography and Cryptography”,

**AUTHOR:** M. IndraSena Reddy, K Subba Reddy and V Uday Kumar,

**YEAR: 2013**

**DESCRIPTION:** Steganography and cryptography methods are used together with wavelets to increase the security of data while transmitting through networks. 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. The digital watermarking plays an important role in embedding information into a digital image signal, for verification and identity of its owners. In this paper the embedded information is applied as text. Before embedding the text in image, text is encrypted using Advanced Encryption Standard (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 image transformed using wavelet and encrypted text is extracted by using LSB method. The paper also shows how the AES algorithm is used in decryption of result.

**CHAPTER 3**

**EXISTING SYSTEM AND PROPOSED SYSTEM**

**EXISTING SYSTEM**

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 SYSTEM DRAWBACKS**

* The conventional 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.**

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. The wavelet-based steganography has a new concept irrespective of application of wavelets. Here the information is stored in terms of wavelet coefficients of an image. But in the LSB technique there is a change in the bits of actual pixels.

**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.

**FLOW CHART:**

KEY

LL sub-band

EXTRACTED DATA

LL sub-band

TEXT

IMAGE

WAVELET TRANSFORM

INVERSE WAVELET TRANSFORM

SEND IMAGE

WAVELET TRANSFORM

ENCRYPT Text

DECRYPTED DATA

ENCRYPTION

**CHAPTER 4**

**HARDWARE AND SOFTWARE REQUIREMENTS**

**4.1 Hardware Requirements**

The necessary hardware regarding private PC that comprises configuration as specified as follows:-

1. Processor: Intel core i5.

2. Disk capability: 1GB for MATLAB only.

3. RAM: 2GB.

**4.2 SOFTWARE REQUIREMENTS**

* MATLAB 8.3 Version R2014a
* Windows 7(64-bit) operating system.

.

**4.2.1 Overview of MATLAB**

MATLAB is built up by means of math works intended for fourth-generation programming language. A variety of process approved within MATLAB contains control concerning the matrix, purpose as well as plotting of data, execution regarding algorithms, design of user interface, as well as integrating by means of programs formed within other languages like C, C++, and java. Despite mathematical calculation, MATLAB can be meant for representational calculation as well. MATLAB can be meant for embedded methods and by the guide regarding extra package known as simulink. Specifically MATLAB permit intended for matrix estimation as well as thus can be intended for image processing. MATLAB is simple towards gaining knowledge of a variety of device boxes used for it; an illustration is image processing toolbox.

MATLAB interfaces programming surroundings, calculation as well as mental picture. This contains integrated correcting, data compositions as well as object-oriented correcting devices. These integrated tasks create MATLAB appropriate used for education as well as do research. To resolve scientific trouble MATLAB includes other benefits than usual programming language like c plus java. MATLAB arrived into promotion in 1984 in addition to now it is employed globally. Additional graphical instructions are offered within MATLAB that builds the visual effects obtainable right away. A variety of device box contains signal processing, simulation, control theory as well as some former that are employed extensively in science and technology. The lone disadvantage regarding MATLAB is expenditure worry.

**4.2.3 Features of Matlab**

* Interactive background meant for aim investigation as well as resolving the difficulty.
* MATLAB is a sophisticated language intended for creating, calculating as well as building up a purpose.
* It contains numerical tasks such as figures, calculus, sorting out, developments, mathematical integration, as well as working out equations.
* Graphics integrated intended for visualization.
* Intended for generating traditional plot integrated equipments is accessible.
* Troubles as well as way outs are given in well-known numerical symbol.

**CHAPTER 5**

**IMPLEMENTATION**

**CRYPTOGRAPY**

Cryptography is a technique for storing and transmitting data in a specified form. It is closely related to scrambling plaintext i.e. ordinary text into cipher text (i.e. a process called encryption), then back again for getting plain text named as decryption. Cryptography can also be categorized as symmetric key cryptography and asymmetric key cryptography.

The symmetric key cryptography is also defined as private-key cryptography, where the secret key may be held by the person concerned or a copy of the private key cryptography may share the massage by sender and receiver.

Asymmetric key cryptography also called public key system is a two-key system, in which one key encrypts the information and the other one decrypts it. The encrypted message has a private key which is never shared while only the sender knows it. If the system encrypted the message with the proposed receiver’s public key and then again with the sender’s secret key or private key, then the receiving system may decrypt the message by first manipulating its secret key and then by the sender’s public key.

**AES DATA**

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 AES we can use 128,192 or 259 bits long with each of them contains 2128,2192 and 2256 combinations. The secrecy maintained by the key is secured andauthentication is maintained the key itself. In this both the keys must be kept secret. But without knowing private key or at least other information impossible to decode the cipher text. With the help of public key and algorithm it must be insufficient to find the private key. 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. AES key is harder to break than DES, and both need more dealing out to distribute keys between sender and receiver.

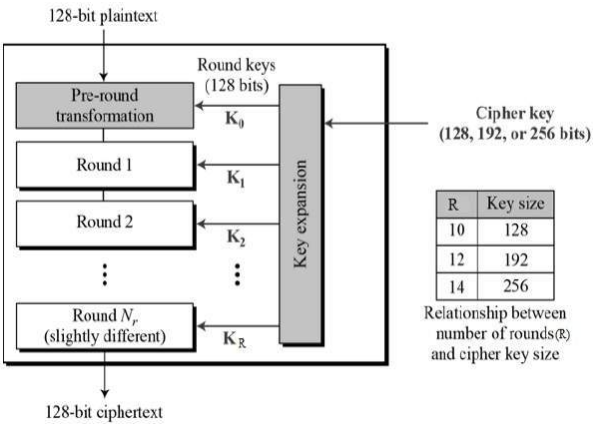
The features of AES are as follows −

* Symmetric key symmetric block cipher
* 128-bit data, 128/192/256-bit keys
* Stronger and faster than Triple-DES
* Provide full specification and design details
* Software implementable in C and Java

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).

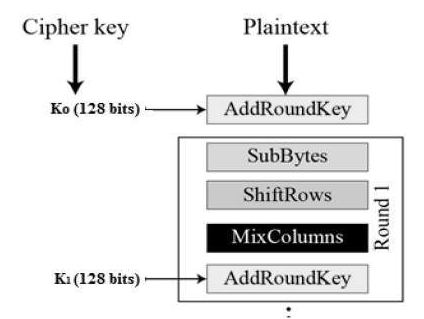
Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

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.



## Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −

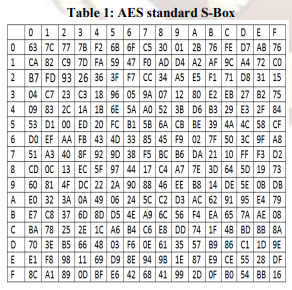


### Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

**S-box Generation**

The S-box has the task of minimizing the susceptibility of the algorithm to methods of linear and differential cryptanalysis and to algebraic attacks. In addition to the requirement of complexity, the S-box function must be invertible; it must have no fixed points S(a)= a or complementary fixed points S(a)= a ; and it must also execute rapidly and be easy to implement. S-box contains a permutation of all possible 256 8- bit values. Each individual byte of state is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the Sbox to select a unique 8-bit output value. Table 1 represents S-box. During encryption each value of the state is replaced with the corresponding Sbox value



### Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that ‘fall off’ are re-inserted on the right side of row. Shift is carried out as follows −

* First row is not shifted.
* Second row is shifted one (byte) position to the left.
* Third row is shifted two positions to the left.
* Fourth row is shifted three positions to the left.
* The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

### MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

### Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.