**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 image transformed using wavelet and encrypted text is extracted by using LSB method.

**OBJECTIVES**

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

**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.

**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.

**DISADVANTAGE**

* 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. 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: AES with the given key. In this process by using the key, the given text is encrypted. Then this resultant text is decrypted with the same key. (Here, the key is of length 56-bit.) 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. This method is described in Algorithm-1. Note that, as we are 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.

2.1. **Algorithm-1: Least Significant Method**

Begin

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.

End.

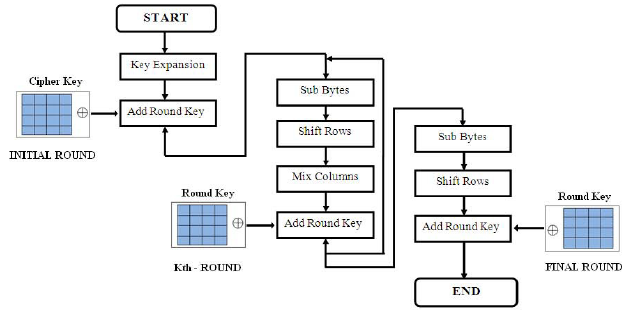
**Algorithm-2: AES is a block cipher.**

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

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.

**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.



**Figure 2: AES algorithm**

**CONVERSION FROM PLAIN TEXT TO CIPHER TEXT**

AES is a block cipher. It operates on plain text with a block of bits and returns cipher text with the same size. In this algorithm we have performed 10/12/14 rounds. It contains the byte substation, shift rows, mix columns and then add round key. The sub-stution of each byte uses one table with a 16x16 bytes and it contained a permutation of all specified values. Each byte of state is replaced by the byte indexed with row and column. In shift rows is used circular byte. Shift in each, the 1st row is unchanged and the 2nd row is 1 byte circular shift to the left and the 3rd row is 2 bytes circular shift to the left likewise it may process and decrypt inverts using circular shift to right. In the mix columns, each column is processed and separated and each byte is replaced by a value dependent on all bytes in the column. And add round key is a XOR state with 128-bits of key processed by column and inverse for decryption. AES decryption is not identical to encryption since the steps done in reverse order but is defined as equivalent inverse cipher with steps as for encryption by using inverse of each step with a different key.

**SYSTEM ARCHITECTURE**

**TRANSMITTER**

**INPUT IMAGE**

**DISCRETE WAVELET TRANSFORM (DWT)**

**DECOMPOSED IMAGE**

**HIGH FREQUENCY COEFFICIENTS**

**LOW FREQUENCY COEFFICIENTS**

**HH**

**LL**

**TEXT**

**ENCRYPTION (AES)**

**INVERSE DISCRETE WAVELET TRANSFORM**

**SEND IMAGE**

**KEY**

**HL**

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

**RECEIVER**

**FORWARD WAVELET TRANSFORM**

**DECRYPTION (AES)**

**ORIGINAL TEXT**

**RECEVIED IMAGE**

**KEY**

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

**FLOW CHART:**

KEY

ENCRYPTION

LL sub-band

LL sub-band

TEXT

IMAGE

WAVELET TRANSFORM

INVERSE WAVELET TRANSFORM

SEND IMAGE

WAVELET TRANSFORM

ENCRYPT Text

DECRYPTED DATA

EXTRACTED DATA

**FIGURE 2: FLOW OF PROPOSED SYSTEMAT**

**TECHNIQUES**

**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.

**STEGANOGRAPHY**

Steganography is a technique used to hide information in some covered media. In Steganography the existence of information will not be noticed by viewers as it is embedded inside some medium. This medium is referred to as covered object or data. The main function of Steganography is to convey the information secretly by concealing in media such as image, audio and video and also implementing watermarking. To hide the secret information, the message is embedded in cover text by using some embedding algorithm, so that the “stego text “or “cipher text” is formed. The text is subsequently delivered to the receiver through transmission channel. The same stego text is processed by the extraction algorithm using “secret key “or the “stego key”.

**Least significant bit incorporation**

Least significant bit incorporation is a general approach for embedding information in a cover image. In the proposed research the LSB technique is used in the concept of 24 bit image or 8-bit image. The 24-bit image is embedded with three bits of information one in each pixel. One in each Least Significant bit position of the three 8-bit values, either increases or decreases, while the value of changing the Least Significant Bit does not change the appearance of the image. So the stigma image remains same as the cover image. Least Significant Bit (LSB)-substitution make replaces the least significant bit with a secret bit stream. While LSB matching is either added or subtracted randomly from the pixel value of the cover data, the embedding bit does not match. In the 8-bit ,one bit of information could be hidden. Now any one can hide a message in three pixels of an image.

The original three pixels are

(11101010 11101000 11001011)

(0110011011001010 11101000)

(11001001 00100101 11101001)

A stenographic system can hide the letter “A” which has a position 65 into ASCII character set and has a binary representation “1000001”by altering the channel bits of pixels.

(11101011 11101000 11001010)

(01100110 11001010 11101000)

(11001000 00100100 11101001)

In this case, only four bits are changed to insert the character “A” successfully. So changes that are made to the LSBs are very small invisible to the human eye. That’s why the message is effectively hidden.

**ADVANTAGE**

* 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.

**MODULES OF PROPOSED SYSTEM**

**Selecting an Image file**

First, select any image file, behind which the user wants to hide data. The image which is selected should have fixed height and width. Now save the image file as in jpeg extension and the image appears as an original image file.

**Image Steganography**

**For Sender Side**

In this, The sender will select the original image in jpeg extension format. Now the sender read the file using „imread􁪃 function. And convert the image file from rgb to gray using a function „rgb2gray􁪃. After this read the text and convert that text into a binary format. Then the key is read and the text is converts into encrypted format .When the wavelet transformation function i.e. sumdiff() is used .The image can divide into the sub bands as LL, LH, HL , HH. The binary cipher has to be put into LL Sub band by using embeddingfunc(). We can apply the inverse wavelet transformation function and convert the image into its original size. And the image is sent to the receiver.

**Creating Stego Image file**

For creating stegno Image file, combine stego text file and stego image file using digital watermarking. This forms the stego image text file at transmitter side in which hidden text is present.

**For Receiver Side**

When the receiver reads the text file using „fread􁪃 it gets converted into an image. For this receiver apply the wavelet transformation function i.e., sumdiff( ) and divide the image into four sub bands as LL, LH, HL, HH. Now choose the required LL sub band from the image. Using extractionfun2 ( ) to extract the code from image and convert it into hexadecimal format and then store it into a variable „extra1􁪃.Now decrypt the encrypted code by using

des1keydecrfunc ( ).

**Image Recovery**

The image file is read by the function „imgread􁪃 and the text file is opened using fopen function and is stored into a variable „fid􁪃. Using the function fread it is stored into a variable „a􁪃. Now convert the text file into the image file using matrix representation. Here to perform some addition and subtractions on the matrix it is placed into the proper sub band i.e., LL, LH, HL, HH. The image can be recovered by the text using „extractionfun( ).

**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.

**CONCLUSION**

The cryptographic algorithm alone is not a very secure way to be used for the data transmission. So a new method which combines cryptography and steganography is provided to give much better option for data transmission. In this project 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. To further increase the security of the data, the encrypted text is not embedded in the image itself. Instead, it is embedded in the LL-sub-band of the wavelet transformed image

**REFERNCES**

[1]. Zeng XT, Li Z, Ping LD Reversible data hiding scheme using reference pixel and multi-layer embedding. Int J Electron Commun (2012)66:532–539.

[2]. Chan CK, Cheng LM Hiding data in images by simple LSB substitution. Pattern Recogn (2004)37:469–474.

[3]. Johnson NF & Jajodia S Exploring steganography: seeing the unseen. Comput Pract (1998)26–34.

[4]. Swanson M, Kobayashi M, Tewfik A Multimedia data embedding and watermarking technologies. (1998)Proc IEEE 86(6):1064–1087.

[5]. S. Kartalopoulos, “Security of Information and Communication Networks”, Wiley-IEEE Press, (2009).

[6]. N. F. Johnson and S. Katzenbeisser, Information Hiding, ch. A survey of steganographic techniques. Artech House, Norwood, MA, (2000).

[7]. Y. Lee, L. Chen, “High capacity image steganographic model”, IEEE Proceedings on Vision, Image and Signal Processing (2000)147, 288 -294.

[8]. Mielikainen J LSB matching revisited. IEEE Signal Processing Letters(2006) 13:285287.

[9]. Chang CC, Lin MH, Hu YC A fast and secure image hiding scheme based on LSB substitution. Int J Pattern Recog(2002) 16(4):399–416

[10]. Wang RZ, Lin CF, Lin JC (2001) Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recogn (2001)34(3):671–683

[11]. Thien CC, Lin JC A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recogn(2003) 36:2876–2881

[12]. Jung KH & Yoo KY Data hiding using edge detector for scalable images. Multimedia Tools and Appl doi:(2013)10.1007/s11042-012-1293-84.

[13]. Xuan G, Zhu J, Chen J, Shi YQ, Ni Z, Su W Distortionless data hiding based on integer wavelet transform. IEE Electronics Letters(2002)38:1646–1648.

[14]. M. IndraSena Reddy, “A Practical Approach for Secured Data Transmission using Wavelet based Steganography and Cryptography”, International Journal of Computer Applications (2013)(0975 – 8887)Volume 67– No.10.

[15]. VVS Kumar M. IndraSenaReddy , “Image Compression Techniques by using wavelet transform”, Journal of information engineering and applications,(2012) Vol.2, No.5,35-39.

[16]. M. IndraSena Reddy, K Subba Reddy and V Uday Kumar, “Secured Data Transmission using Wavelet based Steganography and Cryptography”, International Journal of Computers and Technology(2013) Volume 6(2)–311-316.