ISSN 22773061

Secured Data Transmission Using Wavelet Based Steganography and Cryptography

M. IndrasenaReddy, V. Uday Kumar, K. Subba Reddy, P. Venkat Vijay Kumar

School of Computer Scince & Engineering, R.G.M. C.E.T, Nandyal-518 501
mir555mittapalli@gmail.com
School of Computer Scince & Engineering, R.G.M. C.E.T, Nandyal-518 501
vukuday@gmail.com
School of Computer Scince & Engineering, R.G.M. C.E.T, Nandyal-518 501
mrsubbareddy@yahoo.com
School of Computer Scince & Engineering, R.G.M. C.E.T, Nandyal-518 501
Venkat506@gmail.com

ABSTRACT

Steganography and cryptographic methods are used together with wavelets to increase the security of the data while transmitting through networks. Another technology, the digital watermarking is the process of embedding information into a digital (image) signal. Before embedding the plain text into the image, the plain text is encrypted by using Data Encryption Standard (DES) algorithm. 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. The receiver will perform the same operations in reverse order.

Indexing terms/Keywords

Cryptography, digital watermarking, steganography, wavelet.

Academic Discipline And Sub-Disciplines

Education

SUBJECT CLASSIFICATION

E.g., Mathematics Subject Classification; Library of Congress Classification

TYPE (METHOD/APPROACH)

Provide examples of relevant research types, methods, and approaches for this field: E.g., Historical Inquiry; Quasi-Experimental; Literary Analysis; Survey/Interview

ISSN 22773061

INTRODUCTION (**different of next section PAGESIZE, etc.)

In the present world of communication, one of the necessary requirements to prevent data thefts securing the information. Security has become a critical feature for thriving networks and in military alike. Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields: they are used to protect military messages, E-mails, credit card information, corporate data, personal files, etc.
Cryptography (from Greek crypto's, "hidden", and gráphein, "to write") is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge, the art of encryption. The art of protecting information (plain text) by transforming it (encrypting it) into an unreadable format is called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by
Cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. Cryptography encrypts the actual message that is being sent. This security mechanism uses mathematical schemes and algorithms to scramble data into unreadable text. It can only be decoded or decrypted by the party that possesses the associated key [1].
Steganography (from Greek Stegános, "Covered/hidden", and gráphein, "to write") is the art and science of communicating in a way which hides the existence of the communication [2]. Steganography hides the very existence of the message by embedding it inside a carrier file of some type. An eavesdropper can intercept a cryptographic message, but he may not even know that a stenographic message exists. Cryptography and Steganographyachieve the same goal via different means. Encryption encodes the data so that an unintended recipient cannot determine its intended meaning. Steganography, in contrast attempts to prevent an unintended recipient from suspecting that the data is there. [3]. Combining encryption with steganography allows for a better private communication. The goal of steganography is to avoid drawing suspicion to the transmission of the secret message. On the other hand, steganalysis is a way of detecting possible secret communication using against steganography. That is, steganalysis attempts to defeat steganography techniques. It relies on the fact that hiding information in digital media alters the carriers and introduces unusual signatures or some form of degradation that could be exploited. Thus, it is crucial that a steganography system to ascertain that the hidden messages are not detectable [4]–[6].
Steganography includes the hiding of media like text, image, audio, video files, etc. in other media of the same type or of different type. Later, the message hidden in the selected media is transmitted to the recipient. At the receiver end, the reverse process is implemented to recover the original message [7].
Many ideas and techniques have been proposed to secure data i.e., mainly concealing of text in images. The simplest method to do the same is Least Significant Bit replacement method in steganography. But it has its own limitations [8]. Steganalysis can be easily done on LSBreplacement technique [9]. This new proposed method overcomes this draw back [13 14 15 16].

Proposed Enhancement

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: DES 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 subband 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) our human eye cannot find the difference between the original image and the watermarked image. Once the cipher text is embedded into the LL subband, inverse wavelet transform is applied. Then this resultant image is sent to the receiver.

Implementation

DES (the Data Encryption Standard) is a symmetric block cipher developed by IBM. The algorithm uses a 56-bit key to encipher/decipher a 64-bit block of data. The key is always presented as a 64-bit block, every 8th bit of which is ignored. However, it is usual to set each 8th bit so that each group of 8 bits has an odd number of bits set to 1. The algorithm is best suited to implementation in hardware, probably to discourage implementations in software, which tend to be slow by comparison. However, modern computers are so fast that satisfactory software implementations are readily available.

DES is the most widely used symmetric algorithms in the world, despite claims that the key length is too short. Ever since DES was first announced, controversy has raged about whether 56 bits is long enough to guarantee security. The key length argument goes like this. Assuming that the only feasible attack on DES is to try each key in turn until the right one is found, then 1,000,000 machines each capable of testing 1,000,000 keys per second would find (on average) one key every 12 hours. Most reasonable people might find this rather comforting and a good measure of the strength of the algorithm. The general working of a DES algorithm will perform for 16 rounds are shown in Fig. 1. the working of single round is shown in Fig. 2.

ISSN 22773061

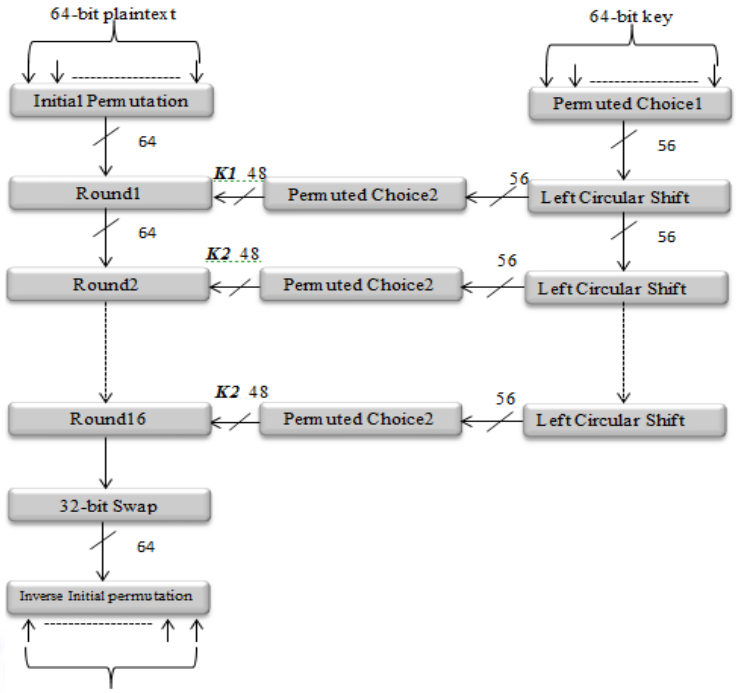

Fig: 1. General Description of DES Encryption Algorithm.

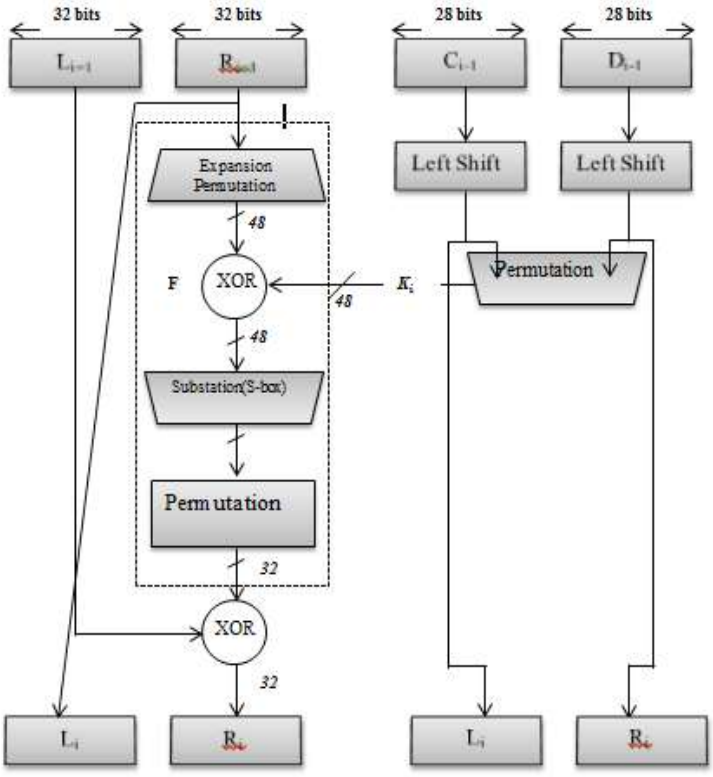

Fig: 2. Single rounds in DES

Conversion from Plain text to Ciphertext

DES is a **block cipher**--meaning it operates on plaintext blocks of a given size (64-bits) and returns ciphertext blocks of the same size. Thus DES results in a **permutation** among the 2^64 (read this as: "2 to the 64th power") possible arrangements of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block **L** and a right half **R**. (This division is only used in certain operations.)

Example: Let **M** be the plain text message **M** = 0123456789ABCDEF, where **M** is in hexadecimal (base 16) format. Rewriting **M** in binary format, we get the 64-bit block of text:

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

L = 0000 0001 0010 0011 0100 0101 0110 0111

R = 1000 1001 1010 1011 1100 1101 1110 1111

The first bit of **M** is "0". The last bit is "1". We read from left to right.

DES operates on the 64-bit blocks using key sizes of 56- bits. The keys are actually stored as being 64 bits long, but every 8th bit in the key is not used (i.e. Bits numbered 8, 16, 24, 32, 40, 48, 56, and 64). However, we will nevertheless number the bits from 1 to 64, going left to right, in the following calculations. But, as you will see, the eight bits just mentioned get eliminated when we create subkeys.

This is the encrypted form of **M** = 0123456789ABCDEF: namely, **C** = 85E813540F0AB405.

Decryption is simply the inverse of encryption, following the same steps as above, but reversing the order in which the sub keys are applied.

Wavelet Based Digital Watermarking with DES Encrypted Text

A 'wavelet' is a kind of mathematical function used to divide a given function or continuous-time signal into different frequency components and study each component with a resolution that matches its scale. The wavelet transform is a multi-resolution technique, which can be implemented as a pyramid or tree structure and is similar to sub-band decomposition[10,11].

There are various wavelet transforms like Haar, Daubechies, Coiflet, Symlet and etc. They differ with each other in the formation and reconstruction. The wavelet transform divides the original image into four subbands and they are denoted by LL (low-low), LH (low-high), HL (high-low) and HH (high-high) frequency subbands. The HH subimage represents diagonal details (high frequencies in both directions – the corners), HL gives horizontal high frequencies (vertical edges), LH gives vertical high frequencies (horizontal edges), and the image LL corresponds to the lowest frequencies which is shown in Fig. 3.

Fig:3 (a). Original Image and (b) Level-1 Wavelet Transformed Image.

At the subsequent scale of analysis, the image LL undergoes the decomposition using the same filters, having always the lowest frequency component located in the upper left corner of the image. Each stage of the analysis produces next 4 subimages whose size is reduced twice when compared to the previous scale. I.e. for level 'n' we get a total of '4+ (n-1) *3' subbands. The size of the wavelet representation is the same as the size of the original.

The Haar wavelet is the first known wavelet and was proposed in 1909 by Alfred Haar. Haar used these functions to give an example of a counting orthonormal system for the space of square-integrable functions on the real line. The Haar wavelet scaling function coefficients are h {k} = {0.5, 0.5} and wavelet function coefficients are g {k} = {0.5, -0.5}[12]. The Daubechies wavelets [10] are a family of orthogonal wavelets defining a discrete wavelet transform and characterized by a maximal number of vanishing moments for some given support. With each wavelet type of this class, there is a scaling function which generates an orthogonal multiresolution analysis.

Methodology

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 subband 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) our human eye cannot find the difference between the original image and the watermarked image. Once the cipher text is embedded into the LL subband, inverse wavelet transform is applied. Then this resultant image is sent to the receiver.

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.

ISSN 22773061

End

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

The encryption and decryption process using these one key is shown in Fig: 4. The entire process of the method is shown in the form a flow chart in Fig: 4

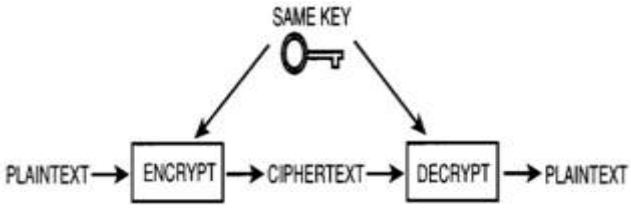

Fig: 4 Data Encryption and Decryption in DES.

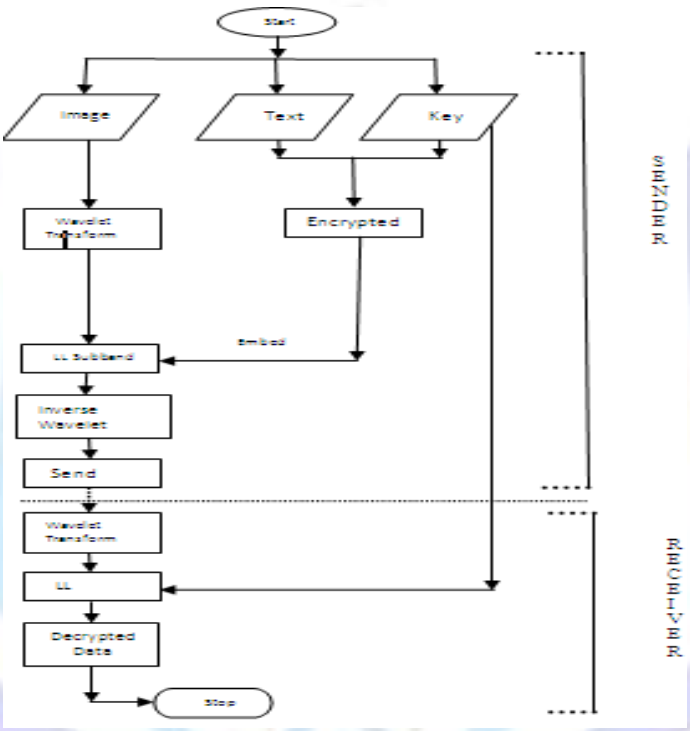

Fig. 5. The flow chart of the proposed method.

The Fig: 5. Shows about the process of encrypting the data into the image by using wavelet transform at the sender side and decrypting the data at receiver side of an image by using inverse wavelet transform.

The flow chart of the proposed method is shown in the Fig. 5.

Results and Discussion

By taking an example the text '**udayuday**' is taken as input. For this text, the corresponding hexa representation is '**7564617975646179'**. Key- '**asdfghjk'** which is of length 8 characters are taken to alter the message 'Gandhiji'. The result after the encryption using Key is '**E2DDF6ABE534CFF2**'. Now this result is decrypted using Key which results '**7564617975646179**'. Now this data is the one which is going to be embedded into the image. At the other end, the given image is transformed using Haar forward wavelet transform to get the LL, LH, HL and HH subbands. The data which are the result of the above method is embedded into the LL subband. After that, the image is transformed back to the original form using Haar inverse wavelet transform.

After receiving the image from the sender, the image is once again transformed using Haar forward wavelet to extract the hidden data and that data is decrypted using the steps given in Fig 6. Finally, the original message is received as 'Gandhiji'. The following screen shots for this entire process are shown in Fig:6

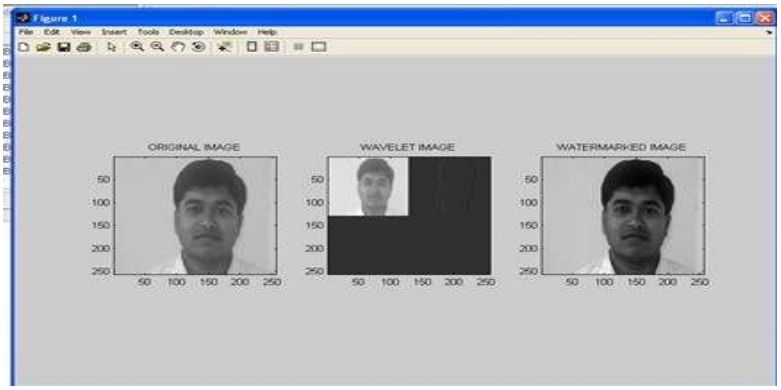

Fig.6: setgo image for Wavelet image and Watermarked image.

Conclusions

The cryptographic algorithm alone is not a much secure way to be used for the data transmission. So a new method which combines cryptography and steganography is provided which gives much better option for data transmission. In this project a method to combine steganography (Least Significant Method) and cryptography (DES) 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-subband of the wavelet transformed image.

References

[1]William Stallings, Cryptography and Network Security, Principles and Practice, Third editionPearsonEducation, Singapore, 2003.

[2] Clair, Bryan. “Steganography: How to Send a Secret Message.” 8 Nov. 2001

[3] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science, Springer, 1998. Pp. 32-47.

[4] C. C. Lin, and W. H. Tsai, "Secret Image Sharing with Steganography and Authentication," Journal of Systems and Software, 73 (3): 405-414, December 2004

[5] KafaRabah. Steganography - The Art of Hiding Data. Information Technology Journal 3 (3) - 2004.

[6] T. Morkel, J. H. P. Eloff, M. S. Olivier, ”An Overview of Image Steganography”, Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, SA.

[7] Krenn, R., “Steganography and Steganalysis”, http://www.Krenn.nl/univ/cry/steg/article.pdf

[8] R.J. Anderson and F. A. P. Petitcolas (2001) On the limits of the Stegnography, IEEE Journal Selected Areas in Communications, 16 (4), pp. 474-481.

[9] S. Dumitrescu, W.X.Wu and N. Memon (2002) On steganalysis of random LSB embedding incontinuous-tone images, Proc. International Conference on Image Processing, Rochester, NY, pp. 641-644.

[10] Rafael C. Gonzalez and Richard E. Woods, “Digital Image Processing,” 2nd Ed., Pearson Education Pvt. Ltd, Indian Branch, 2003.

[11] Duane Hanselman and Bruce Littlefield, “Mastering MATLAB 7”, Pearson Education, India.

[12] Daubechies Ingrid, “Ten Lectures on Wavelets,” Society for Industrial and Applied Mathematics, 1992

[13] J. Fridrich, M. Long, “Steganalysis of LSB encoding in color images,”Multimedia and Expo, vol. 3 pp. 1279-1282, July 2000..

[14] R. Chandramouli, M. Kharrazi, N. Memon, “Image Steganography and Steganalysis: Concepts and Practice “International Workshop on Digital Watermarking, Seoul, October 2004.

[15] Hide & Seek: An Introduction to Stegnography: http:\\niels.xtdnet.nl/papers/practical.pdf.

[16] Y. Lee and L. Chen (2000) High capacity image steganographic model, IEE Proceedings on Vision, Image and Signal Processing, 147 (3), pp. 288-294.