Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 62 – 69

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm

M. Indra Sena Reddy [a,*], Dr. A.P. Siva Kumar [b],

[a] *R.G.M.College of Engineering & Technology, Nandyal-518501, A.P. India*
[b] *J.N.T.U A, College of Engineering, J.N.T.University, Anantapuram-515002, A.P, India.*

Abstract

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.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: Steganography, cryptography, watermarking, discrete-wavelet, Encryption, Decryption

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

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +91 810 644 8352.
*E-mail address:*mir555mittapalli@gmail.com

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.177

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 [13] 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].

1.1. Present Associated Work

Now days, data hiding techniques are needed to conceal a number of applications. For such as digital images, audio, and video. Today it includes distinguishing and imperceptible marks that contain a hidden copyright notice or serial number to help and prevent from unauthorized copying [2, 3,4]. 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 [14,16].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. Using this method the sender and the receiver may be able to confirm one another and also maintain the secrecy of the given message. Nowadays, steganography is basically considered a sub-discipline of digital data communication security domain [57]. Steganography is a technique used to hide information in some covered media. The term “Steganography” is derived by combining two Greek words i.e “steganos “ and “ Graphy” , where “Steganos” means „covered‟ or „secret‟ and “Graphy “ means „writing‟ or „covered data‟. 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”. The image Steganography following the concept of “what you see is what you get” ,allows the two parties to communicate secretly by allowing copyright protection and using digital watermark. 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. The revised LSB matching was proposed to improve by applying lowering the number as a modification [8]. To improve the image quality, the optimal LSB