International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015
ISSN 2091-2730

ADVANCED SECURITY ENHANCEMENT OF DATA BEFORE DISTRIBUTION

Fiji Joseph[1], Asst.Prof.S.Sivakumar[2]
Department of Electronics and Communication
Sri Shakthi Institute of Engineering and Technology, Coimbatore
fijirosejoseph@gmail.com[1], sshiva.ksv@gmail.com[2]

Abstract— Security is an important issue in the field of communication. During storing or transmission of data we have to take care of the confidentiality. The proposed work mainly deals with data hiding to enhance the security of data transmitted in a network. The Steganography which hides the existence of the message and the Cryptography which distort the message are combined. It is mainly employed for sending vital information in a secret way. Here we are discussing Adaptive Pixel Value Differencing technique as image Steganographic scheme whereas Advanced Encryption Standard is discussed as the Cryptographic scheme to encrypt the message. In APVD the image is divided into blocks and then data will be hidden. If we use simple pixel value differencing as embedding algorithm then there is a possibility that the resultant stego image may exceed the grey scale range of 0 to 255.This can affect the quality of stego image which in turn causes the observer to identify that a hidden communication is happening. The main objective of this proposed work is to enhance the quality of stego image and to increase the embedding capacity.

Keywords— Data hiding, Steganography, Cryptography, AES, Adaptive pixel value differencing, Stego Image, PVD

1. INTRODUCTION

Information security and privacy has become a growing concern since ancient times. Humans have continually sought new efficient secret ways to protect information. In the initial stage of communication numerous methods were used to protect the confidentiality of data. It includes usage of ink or chemicals, changing space or fonts etc. With the development of technology information hiding techniques came into existence to protect the secrecy of data. It involves techniques like Steganography, Encryption, and Watermarking. During data exchange, it is a basic request that only the intended recipient should be able to decipher the contents of the transmitted data.

The word Steganography is derived from the ancient Greek words '*steganos'* and '*graphia'*[3]. The word Steganos means covered, whereas graphia means writing. Steganography is the field that gives a meaningful way of secure data being transmitted through an open channel without the attention of eavesdroppers.The word Cryptography is derived from the Greek word kryptos which means hidden. The Cryptography scrambles the data. As a result only authorized people can access it. The specific requirement of Cryptography includes authentication, privacy and integrity non-repudiation.

The data hiding using the combination of Steganography and Cryptography includes mainly involve two processes. They are Embedding process and Extracting process. The embedding process uses a cover image to embed the secret text data. The result thus obtained after embedding is then subjected to encryption. The extracting process is used to recover the secret text data from the stego image. Here we require an extraction algorithm. The mathematical formulas are given below:

For embedding Process:

Cover Image +Secret text data+ Encryption algorithm=Stego Image

For Extracting Process:

Encrypted Stego Image+ Decryption algorithm+ Extraction Algorithm=Secret Text Data

Steganography can be used in a wide range of application areas such as, in defense organizations for safe circulation of secret data, in military and intelligence agencies and in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials [2]. In medical imaging, patient's details are embedded within image providing protection of information and reducing transmission time and cost. The Cryptography also has got a wide range of applications including mp3 protection in the networks, military applications etc.

2. EXISTING METHOD

Many Steganographic schemes and Cryptographic schemes are there. The classification of the Steganography depends on the cover object used. The cover object can be an image, audio, video etc. The common audio Steganographic schemes include Parity

coding, Phase encoding, Echo data hiding etc. If the cover object is an image the LSB insertion technique, PVD technique etc. is used. One of the most advanced Steganographic scheme is Adaptive Pixel value Differencing. It is an enhanced version of Pixel Value Differencing and so it overcomes the pitfalls of PVD technique. Various Cryptographic schemes are also there. It is generally classified as Public Key Cryptography and Private Key Cryptography.

3. PROBLEM DEFINITION

Steganography enable us to hide messages in the cover of something else. The embedding phase determines how the data can be embedded. This algorithm can be more or less advanced, ranging from simple least-significant bit (LSB) embedding in the spatial domain to bit scattering in the frequency domain. The actual hiding process starts with embedding bits of the message into the cover image. Most methods in use today are invisible to an observer's senses. But as the number of bits embedded increases the quality of stego image decreases. These expose the fact that hidden communication is happening. So, there are two important issues that must be considered during the embedding process. They are:

(i) the decision of the number of bits that each pixel uses to embed message, and
(ii) quality of the stego image

Due to the above two reasons we can state that the Steganography simply cannot provide a secure data hiding. So we go for the combination of Steganography and Cryptography.

4. PROPOSED METHOD

The proposed method is a combination of two information hiding techniques. That is Steganography and Cryptography. The Adaptive Pixel Value Differencing which is an enhanced version of Pixel Value Differencing is used as the Steganographic scheme whereas Advanced Encryption Standard is used as the Cryptographic Scheme. Since encrypted messages are more difficult to differentiate effective private communication can be done easily. The Implementation involves mainly embedding and extracting process.

The block diagram of the proposed method is as shown below.

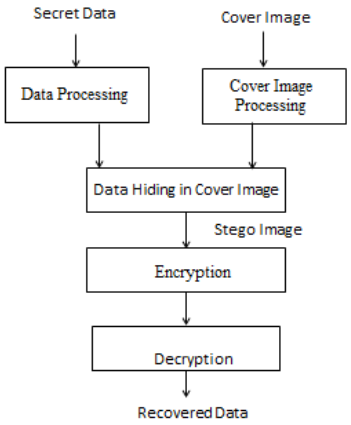

Fig 1: Block Diagram

The important operations involve secret data processing, cover image processing, data hiding, encryption and decryption. The information that the sender want to keep confidential is known as secret data. In such cases to keep it confidential some sort of security actions should be provided. The data can be in the form of a letter, word or character etc. The data processing involves processing of this secret data. It involves calculating the number of bits in the input data and converting it into binary. This binary data is used for embedding purpose.

The cover image is one in which the secret data is hidden. The cover image should be a grey scale image. So the pixel size should be 256×256.If the pixel size is high we have to first bring it to this range. If the input image is a color image we have to first convert it into the grey scale range to use it as cover image.

The data hiding is the process of hiding the data into the cover image and is done by APVD algorithm. The resultant image obtained after hiding the data is the stego image. This image is encrypted using AES. The AES scrambles the image. If unauthorized

people try to access it, they will get only stego image. As the quality of stego image is higher in APVD the existence of the data cannot be easily identified which in turn makes recovery difficult.

5. RESULTS & ANALYSIS

To implement the process an input image is taken. If the image that we are taking is color then we have to convert it into grey scale. We have to take care of the size of the input image. Generally if the image exceeds the grey scale range the quality of stego image get affected and there is a chance of improper visualization. So in order to avoid such situations the range of the input image is limited. The input image is as shown below. The actual size is 160×160.We have to first convert this image into 256 × 256. For performing this operation we have an image resize function in MATLAB.

Fig 2: Original Image

In order to convert the input image into the greyscale range we have rgb2grey function in the MATLAB. After the execution of this command our image will be converted into grey scale range. This image is again splitted into blocks for embedding purpose. The resultant image is the cover image in which we are embedding the data. If we take a grey scale image as cover image the processing operations will be rather simple.

Fig 3:rgb2grey converted image

The image that is used for embedding purpose is known as cover image or cover object. Here we are obtaining the secret data from the user. After receiving the data which is to be kept secret we have to first find out the number of bits in it. This data is converted into their corresponding binary values. Data which is in binary format is embedded into the cover image along with the hamming codes. The hamming codes enable us to reduce the error that occurs during embedding process. The resultant image obtained after embedding is known as stego image.

Fig 4: Stego Image

After data embedding process encryption is done with AES algorithm. This enables as to scramble the stego image. The main characteristics of AES algorithm is its flexibility, simplicity and the reasonable cost. If intruders try to decrypt the resulting image, they will only get the stego image. To get the secret data they again have to make effort so that they can obtain it from the stego image.

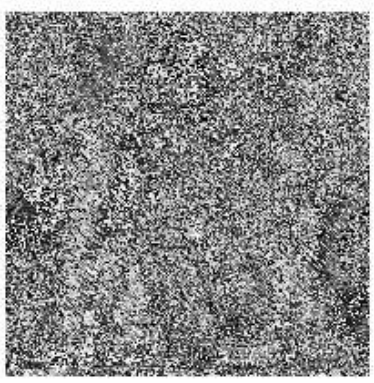

Fig 5: Encrypted Stego Image

Even though the encryption reveals the existence of secret communication, it is difficult to obtain the data as we are employing a combination of Steganography and cryptography.

6. CONCLUSION

A combination of Steganographic scheme using Adaptive Pixel Value Differencing and Cryptographic scheme using AES is implemented using MATLAB The main disadvantage of pixel value differencing is that if the image exceeds grey scale range then it will result in the improper visualization of the stego image. This problem is also avoided here. The quality of stego image is also ensured. In other Steganographic schemes, as the number of bits that are to be embedded increases, the error also increases abruptly. In this approach the error does not increase that much as the number of bits increases. Since the stego image is encrypted the intruder cannot easily obtain the data. The method presented here is applicable to all the image formats and is the one of the great success of this work.

ACKNOWLEDGEMENT

First of all we sincerely thank the almighty who is most beneficent and merciful for giving us knowledge and courage to complete the project work successfully. We also express our gratitude to all the teaching and non-teaching staff of the college especially to our

department for their encouragement and help done during our work. Finally, we appreciate the patience and solid support of our parents and enthusiastic friends for their encouragement and moral support for this effort.

REFERENCES:

[1] J. K. Mandal and Debashis Das, "Steganography Using Adaptive Pixel Value Differencing(APVD) of Gray Images Through Exclusion of Overflow/Underflow", The second International Conference on Computer Science, engineering and applications (CCSEA-2012) ,May 2012.

[2] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18, DOI: 10.14429/dsj.62.1436, 2012, DESIDOC.

[3] H.B.Kekre, Archana Athawale, Swarnalata Rao and Uttara Athawale, "Information Hiding in Audio Signals", International Journal of Computer Applications (0975 – 8887)Volume 7– No.9, October 2010.

[4] Sumedha Sirsikar and Jagruti Salunkhe,"Steganographic Techniques of Data Hiding using Digital Images", International Conference on Electronic Systems, Signal Processing and Computing Technologies,2014.

[5] Khalil Challita and Hikmat Farhat "Combining Steganography and Cryptography: New Directions" International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208 and the Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085).

[6] Julia Juremi, Ramlan Mahmod, Salasiah Sulaiman and Jazrin Ramli "Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key" International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 183-188 The Society of Digital Information and Wireless Communications (SDIWC) 2012 (ISSN: 2305-0012).

[7] Ms. Hemlata Sharma,Ms. MithleshArya and Mr. Dinesh Goyal ,"Secure Image Hiding Algorithm using Cryptography and Steganography", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 5 (Jul. - Aug. 2013), PP 01-06

[8] Ajit Singh and Swati Malik, "Securing Data by Using Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 5, May 2013.

[9] Abdulkarim Amer Shtewi,Bahaa Eldin M. Hasan and Abd El Fatah .A. Hegazy, "An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems", IJCSNS International Journal of Computer Science and Network S 226 ecurity, VOL.10 No.2, February 2010.

[10] Minal Moharir and Dr A V Suresh, "A Novel Approach Using Advanced Encryption Standard to Implement Hard Disk Security", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012.

[11] Khalil Challita and Hikmat Farhat, "Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208, The Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085).

[12] Mihir H Rajyaguru, "CRYSTOGRAPHY-Combination of Cryptography and Steganography With Rapidly Changing Keys", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 10, October 2012