International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Review on Implementation of Cryptographic Method for Secure Audio Data Hiding in Digital Images

Pranjali Ihare[1], V. T. Gaikwad[2]

[1]Electronics and Telecommunication, SIPNA C.O.E.T/ SGBAU University, Maharashtra, India

[2]Associate Professor, Information Technology, SIPNA C.O.E.T/ SGBAU University, Maharashtra, India

Abstract: ***Information security is a major obstacle in different areas like military, network application, are illegally access the information. So, it is very important to hide the secret data efficiently. By means of cryptography we can hide information to be transmitted over network. The cryptography makes the secret message not understood unless the decryption key is available. In this project a symmetric key is introduced which provides secret arrangement of secret signal data bits in cover signal data bits. The encryption process is performed on secret audio signal. File is forwarded from one location to another location in the network. The algorithm used for file encryption provides more security. Cryptography along with the steganography provides perfect security.***

Keywords: Cover signal, *Cryptography*, Encryption, Secret audio signal, Symmetric key

1. Introduction

In today‟s internet world it‟s needed that the data transmission should be perfectly secured. In many cases secret signal data may get hacked by breaking the password assigns to the system. There are softwares developed by the hackers to attack on any weak secret key. Thus it is important to design an encryption technique for perfect data security. Cryptography is the process of encrypting and decrypting the data. Here data get encrypted which sender wants to send to the receiving party and decrypted on the other side. We are developing the encryption algorithm to provide secure transmission of an audio file. The various types of secret key encryption schemes are designed for implementation in software. As hackers have developed many types of software to attack on secret key, Password and ID can‟t provide the strong security. So, encryption technique along with the data hiding can provide the perfect security. Encryption is used to encrypt the secret audio signal to be transmitted. There are basically two types of cryptographic algorithms, symmetric-key and public-key. In symmetric-key cryptographic algorithm sender as well as receiver uses the secret key. Whereas, in public-key cryptographic algorithm different keys are used for encryption and decryption.

Data hiding is another technique which totally denies the existence of information in an image or video so there is no knowledge of existence of any message in an image or video. By means of data hiding we are hiding the encrypted audio file to be transmitted inside the digital image. So that it will provide more secured audio data transmission. Cryptographic technique in support to the data hiding in order to provide more security is used. The purpose of our project is to provide cryptographic method for perfectly secured transmission of an audio file hiding in digital images.

2. Literature Review

Sheetal A. Kulkarni and Shubhangi B. Patil [1] presented a robust encryption method presented a robust encryption method which provides an encryption technique along with the data hiding; data may be in the form of audio or video signal. The secret speech signal gets encrypted and embedding algorithm embeds the encrypted speech signal in the cover image with secret key. After performing embedding operation stego cover image is formed. Transmitter then transfers that stego cover image to the receiver. The cryptography concept is used for locking the secret message in the cover file. The cryptography makes the secret message not understood unless the decryption key is available. It is related with constructing and analyzing various methods that overcome the influence of third parties. Along with the encryption method authors have provided the data hiding technique, which provides more security. Embedding algorithm along with the encryption algorithm forms more robust system.

Rupesh Gupta and Dr. Tanu Preet Singh [2] presented a new method which consists of combination of three major security techniques such as cryptography, steganography and watermarking. Cryptography provides the data encryption and decryption technique. Encryption technique is used for encrypting the data where as decryption is used for decrypting the data. Steganography is an art of hiding information in a host signal. As many attacks made on the data communication, it is needed to hide the secret data efficiently. These three techniques not only provide hiding of the secret data but also provide better results for MSE. After noise attack too, it will provides PSNR and embedding capacity. As the invented technique is combination of three security techniques, it will provide strong security for hiding data in an image and watermarked video. Such efficient technique helps to make internet a safe environment for all the users.

Punam V. Maitri, Dattatray S. Waghole and Vivek S. Deshpande [3] presented low latency algorithm for file encryption and decryption in order to provide network security. As it‟s needed to send the file from one location to another. Network security is major obstacle in different areas. Hackers access the information illegally in order to provide security against such tasks different algorithms is introduced. Such as AES, DES and triple DES. But, such algorithm takes more time for encryption and decryption. So that it makes algorithm bit complex. The algorithm is developed in such a way that it takes smallest amount of time for both encryption as well as decryption. We can apply such algorithm on any type of data to be transmitted such as image, audio, video files. Implementation of such algorithm takes less amount of time as well as provides perfect security.

Harshitha K M, Dr. P. A. Vijaya [4] presented an algorithgm for secure data hiding using encrypted secret message. Security carries vital importance in any communication. It provides the technique which consists of both cryptography as well as steganography in order to provide perfect security. Specific security system includes certain requirements such as confidentiality, authenticity, integrity, non-repudiation. It specifies the technique to secure data or message with authenticity and integrity. Before starting the actual embedding process, secret message has to be encrypted. Whole work has to be performed on MATLAB. First of all by using a simple encryption algorithm, a hidden message is encrypted. A secret key is used to encrypt the message and hence it will be almost impossible for the intruder to unhide the actual secret message from the embedded cover file without knowing secret key. Secret key is known to sender as well as receiver only. For embedding and extraction method N-bit LSB substitution technique is used. This technique could be most appropriate, in order to provide strong security by hiding secret message.

Chandra Prakash Shukla, Mr. Ramneet S Chadha [5] presented a technique which provides the way for secure transmission of the secret information by hiding it into the digital media called as „Steganography‟. Basically the word „Steganography‟ comes from the Greek word steganos which literally means “covered” and graphia which means “writing”, i.e. covered writing. Stego media consists of the secret data to be transmitted, whereas the media without such secret data is called as cover media. They introduced the technique of steganography in detail with introduction, concept and the main applications in this field. Steganography can be used for embedding the secret data into the digital image without compromising over its quality. With the help of such „Steganography‟ technique one file can be hidden into another file. The secret information can be hide in such a way that the observer can‟t recognize the existence of the secret data inside the digital image. The capacity is defined by the size of the hidden object as compared to the size of the cover object. Robustness is defined by the way the hidden-object withstand transformations applied to the stego-object. Steganography is such a technique by which we can hide the secret information as well as can retrieve it safely by maintaining its own quality. In this way this technique provides the strong security.

3. Proposed Work

Proposed system here with mainly consists of encryption algorithm as well as embedding algorithm. Encryption algorithm provides encryption technique to encrypt the secret audio file to be transmitted to the receiver. Embedding algorithm embeds the secret audio file into the cover image file with secret key in order to form stego cover image. Stego cover image get transmitted along the network towards the receiver. Receiver takes stego cover image as an input and gives it to the de-embedding algorithm. Receiver gets the secret audio file iff secret key get matched. In this way, encryption algorithm along with the data hiding technique provides perfect security to the audio file to be transmitted inside the digital cover image.

3.1 Transmitter Flow Diagram

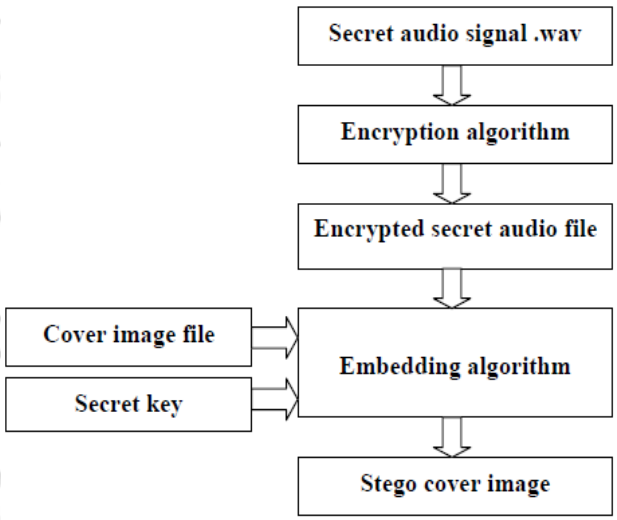

Figure 3.1: Transmitter Flow Diagram

Transmitter flow diagram mainly consists of the following blocks:

1) Secret audio file .wav

This block proceeds the secret audio signal to the next encryption algorithm block. Secret audio signal should be in .wav form.

2) Encryption algorithm

Secret audio file in the .wav form is provided as an input to the encryption algorithm block. Encryption algorithm block applies an encryption algorithm on to the secret audio file which is in the .wav form. Encryption algorithm consists of Discrete Wavelet Transform. Discret Wavelet Transform is applied on secret audio file in the .wav form in order to divide it into low frequency and high frequency components. Later on random noise get added into the low frequency components of the signal. After performing Inverse Descrete Wavelet Transform, it provides encrypted secret audio file which is ready to hide inside the cover image. Limitation is only that the size of cover image should be much greater than secret audio file.

3) Encrypted Secret Audio File

In this way after performing encryption algorithm on secret audio file in the .wav form, we will get encrypted secret

audio file. Now, this encrypted secret audio file is provided as an input to the next embedding algorithm block.

4) Embedding Algorithm

Cover image file and secret key both together are provided as an input to the embedding algorithm. Cover image file is the digital image which is used as a cover to hide the secret audio signal to be transmitted. Size of secret key is 8 bits (binary form).Embedding algorithm embeds the secret key along with the encrypted secret audio file inside the cover image.

5) Stego Cover Image

Cover image along with the secret audio file as well as secret key forms the stego cover image. Now, in this way the stego cover image is now ready for the transmission over the channel.

3.2 Receiver Flow Diagram

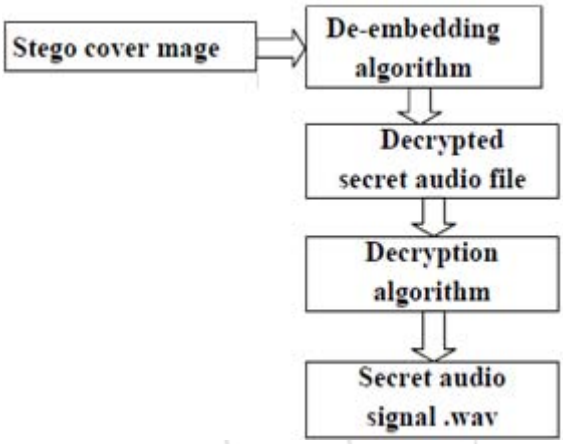

Figure 3.2: Receiver Flow Diagram

Receiver flow digram mainly consists of the following blocks:

1. Stego cover image:

Stego cover image which is the digital image hiding the encrypted secret audio file along with the secret key is provided as an input to the De-embedding algorithm.

2. De-embedding algorithm:

De-embedding algorithm performs the de-embedding steps on to the input stego cover image. After performing the de-embedding algorithm onto the stego cover image it provides the cover image along with the decrypted secret audio file and the secret key.

3. Decrypted secret audio file:

After performing De-embedding algorithm onto the stego cover image. Encrypted secret audio file is then provided as an input to the decryption algorithm.

4. Decryption algorithm:

Decryption algorithm block takes the encrypted secret audio file and performs the de-embedding algorithm steps in order to have decrypted secret audio signal in the .wav form, which is the original required secret audio signal in the .wav form.

First of all a secret audio signal in the .wav form is provided to encryption algorithm. Encryption algorithm is used to encrypt secret audio signal in .wav form. The encrypted secret audio file is then given as an input to the embedding algorithm. Cover image as well as secret key are provided to the embedding algorithm. Embedding algorithm embeds encrypted secret audio file into the cover image to form a stego cover image with secret key. In this way the operation of hiding encrypted audio file into the digital image takes place at the transmitter side in order to provide perfect security.Stego cover image transmitted by transmitter is provided as an input to the de-embedding algorithm. After applying de-embedding algorithm onto the stego cover image we will have cover image with secret key. Receiver will have a secret audio file if the secret key gets matched. Inside the cover image there is a decrypted secret audio file. The decrypted secret audio file is given as an input to the decryption algorithm. After applying decryption algorithm onto the decrypted secret audio file we will get desired secret audio signal as an output to the receiver side. In this way secret audio file reaches to the receiver side with highest security.

The proposed technique of cryptography is the symmetric-key cryptography, in which sender as well as receiver uses the same key for encryption as well as decryption. For encrypting the secret audio file to be hide inside the digital image a secret key is used. Further the same secret audio file can be encrypted with the same cover image but, with different secret key. So, by doing this for the same secret audio file every time a new secret key is generated. Secret audio file encrypting procedure can be performed multiple times by using this technique. All possible words from all characters ASCII code between 0 to 255 in random order are there in the proposed key block. The secret key entered by the user can find out the pattern of the key blocks. To encrypt the secret audio file proposed system consists of 256 * 2 = 512 bits key size. On the receiver side to decrypt the secret audio file one should know the exact secret key which finds out position of the secret blocks. One has to apply 2^{512} trial run in order to find the position of the secret data and it's somewhat annoying for the hackers. As secret key generation is on the basis of 256 * 2 =512 bit key, the proposed method is perfectly secured.

In this way the encrypted secret audio file is ready in order to hide inside the cover image. At the receiver side in order to obtain the original secret audio file, one has to apply the reverse encryption algorithm. The secret audio file's bits can be decrypted by one, who will enter the correct secret key.

Proposed algorithm for secret key hiding in cover image at transmitter end:

1) Acquire the secret key from the secret audio .wave file.
2) After acquiring the secret key, check the secret key is in binary form.
3) Rotate the number of pixels in particular fashion.

Proposed algorithm for encryption of secret audio file:

1) Enter the secret audio file.
2) Implement Discrete Wavelet Transform on secret message and divide it into low frequency and high frequency components.
3) Add high frequency babble noise bits at low frequency components of the signal.
4) The random number is generated by using random number generator.

5) Each bit value is subtracted from random number generated.
6) Implement amplitude ascending order, the minimum value of the signal bits becomes the first value.
7) Apply Inverse Discrete Wavelet Transform and rearrange the signal again.
8) Check the size of original secret audio file and encrypted signal, it should be same. In this way the encrypted secret audio file is ready to hide inside the cover image.
9) In order to obtain the original secret audio file, the reverse encryption algorithm is applied. The one who entered the correct secret key can decrypt the secret audio file.

References

[1] Sheetal A. Kulkarni, Shubhangi B. Patil, "A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security", IEEE, P.P. 2015InternationalConference on Pervasive Computing (ICPC).
[2] Rupesh Gupta, Dr. Tanu Preet Singh, "New Proposed Practice for Secure Image Combing Cryptography Steganography and Watermarking based on Various Parameters", IEEE, p.p. 2014.
[3] Punam V. Maitri, Dattatray S. Waghole, Vivek S. Deshpande, "Low Latency for File Encryption and Decryption Using BRA Algorithm in Network Security", IEEE, P.P. 2015 International Conference on Pervasive Computing (IPCP).
[4] Harshitha K M, Dr. P. A. Vijaya, "A Separable Reversible Data Hiding in Encrypted Image with Improved Performance", IEEE, P.P.(ICMiCR-2013) International Conference on Microelectronics, Communication and Renewable Energy .
[5] Chandra Prakash Shukla, Mr. Ramneet S Chadha, "A Survey of Steganography Technique, Attacks and Applications", IEEE, P.P. Volume 4, Issue 2, February 2014International Journal of Advanced Research in Computer Science and Software Engineering.
[6] N. Umate, Shubhang Dhengre, "IMPLIMENTATION OF ADVANCED ENCRYPTION ALGORITHM", IORD, vol-1, Issue-5, ISSN 2348-0831, pp. 33-39, July-August 2014.
[7] M. Madhurya, B. A. Krishna, T. subhashini, "Implementation of Enhanced Security Algorithms in Mobile Ad hoc Networks", IJCNIS, Vol-2, pp.30-37, January 2014.
[8] Krishna Kumar Pandey, Vikas Rangari, Sitesh Kumar Sinha, "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security", International Journal of Computer Applications, Vol. 74, No. 29, PP. 29-33, July 2013.