A Reformed Model on Data Hiding Using Hybrid Cryptography for Secure Communication

D. Muthu Lakshmi[1], P. Shiyamaladevi[2], S. Suganya[3] & Dr. A. Sundar Raj[4]

[1,3]*Assistant Professor, Department of ECE*
[2]*PG Scholar, Department of ECE*
[4]*Associate Professor, Department of ECE*

[1,2,3,4]*E.G.S. Pillay Engineering College, Nagapattinam, India.*

Abstract

Growth of the science and technology are in rapid rate. Technology turned our work easier, more efficient. Especially the communication sector reached its peak because of the development of science and technology. But at the same time, an improvement in technology has become a big trouble for privacy. When the technology get used in negative it will create a big assault a person's privacy. It is not only a matter of an individual's privacy. When this problem takes place in a highly confidential sectors like army, it will become the worst case. Transferring of important data in the organization will get affected by this issue. Since every individual data is valuable, it is necessary to ensure it's security. Hence this paper proposes a technique called cryptography. Cryptography is the method of sending data in encrypted form where only the sender and receiver can know the decryption method. And here a reformed model on hybrid cryptography is used, data or text will be hidden by using image, audio or video. So that, except the sender and receiver no one can know the actual data present inside the multimedia. This method will ensure the secrecy of data. Even if the person who is neither sender nor receiver got this message, there will be no chance for knowing for actual information.

Keywords: *Data hiding, cryptography, stenography, image, audio, stego key.*

1. Introduction

Now a days, data transfer has become easy and fast. High level of accuracy has been reached in data or information transmission due to it simple and fast mode of transmission. But still there is some difficulties in keeping the information secret during transferring. When the information reached an undesired receiver it will become a huge trouble. This will become worst case in transferring highly confidential data like information about an organization or government sector, confidential information in defence. No one would like to share their information with an undesired person. Hence security is the major need in all kind of data transfer. This security can be given in two kinds, one is the cryptography and other is the stenography [1]. Both of them is designed to ensure the secrecy of data transferred. Here we are using the technology of both cryptography and stenography for maintaining the secret of our information [2].

This kind of high security for the data is obtained by encrypting the text or information into any multimedia like image and audio shown in figure 1 [3]. Information to be transferred is covered up with audio or image [4]. The sender encrypt the information along with image or audio and a secret key called stego key is used as password. Then the message will get transmitted like a normal image or audio. After receiving the message, the receiver has to enter the stego key to view the actual information, otherwise it will remain as a normal image or audio. If a person steals this information, he cannot able to know the actual information. Just the covering image or audio will be visible to him [5].

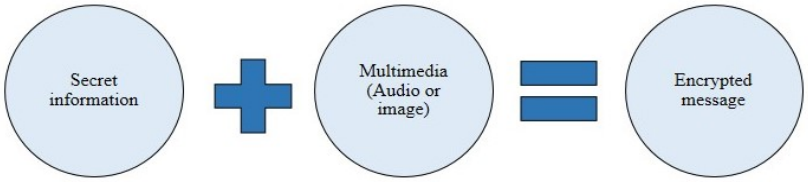

Figure 1. Basic concept of cryptography

In this method, the stego key has to be known to both the sender and receiver. The information opens only when the receiver input the correct stego key. By using this method, we can send confidential messages. After encryption of the hidden message, the system works similar to that of the normal data transmission so there will be no delay. Implementation of this method is also simple, in this paper we are using Matlab for developing this cryptography system [6]. Most important task in encrypting the message is there should be no loss during the compression of image or audio [7], [5].

2. Proposed method

This paper proposes a cryptography concept of embedding a text information into an audio or image file. The process of combining the text into image and audio is known as encoding. Here the secret text is encrypted into image or audio file and a stego key is assigned. In the receiver side, the stego key has to be entered correctly inorder to open the secret information [8]. Steps involved in combining the text and multimedia is shown in figure 2.

Figure 2. Steps involved in hiding information

This method uses Lease Significant Bit (LSB) coding for hiding the information into image or audio. Image used to cover the secret information is known as the cover image. In LSB the information get combined with the least significant bit of the image [9]. So that we can hide large number of information into the cover image. In the process of

hiding the information by image, we can use either 8-bit or 24-bit colour image. All the colours in the image is converted into Red, Green, Blue (RGB) format. Here there is no restriction in image size and format. Image formats like Bitmap (BMP), Graphic Interchange Format (GIF), and Joint Photographic Experts Group (JPEG) can be used. But some of the format may produce loss while compressing the image. Lossless compression can be achieved only by using GIF and 8-bit BMP type images, otherwise the compression process will become lossy compression. After compression, the information will embedded into the image. This process can be done by converting the information into digital format. Then overwriting of information to the least significant bit of pixel value takes place. This process of changing is very minute so that there will be no big changes in the image outlook. This is the major advantage of using LSB for data encoding [10].

If we consider this method for audio encryption, the high entropy noise of the audio is replaced with the high entropy of the secret information. Basic flow of process in encryption is similar to both image and audio encryption shown in figure 3. Nature of the audio signal is analog but in case of storing it in computer and for transmitting audio, it has to be in digital format. Thus we are encrypting the secret information into the audio by slightly changing its bits by replacing it with our information bit.

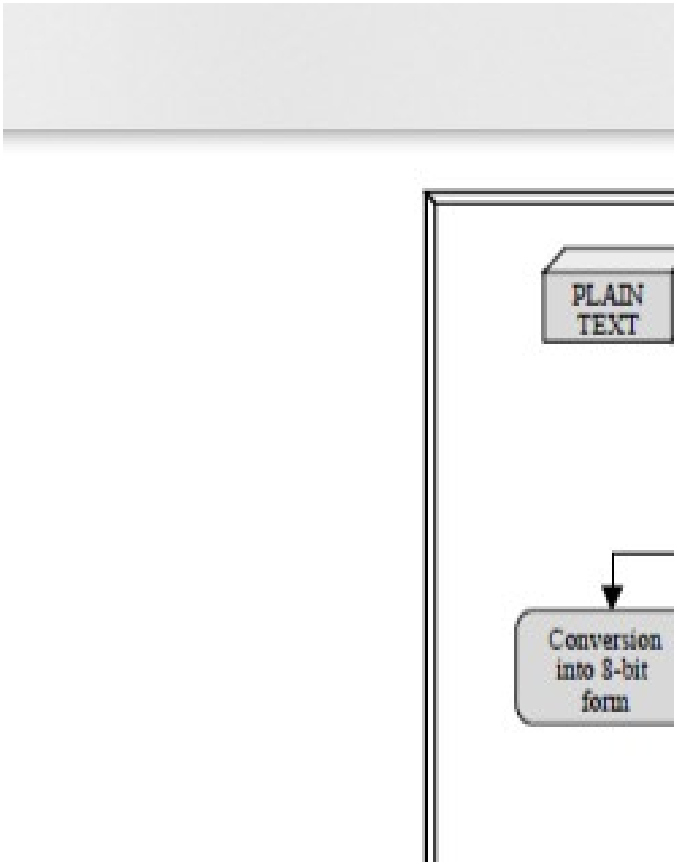

Figure 3. Data flow for encrypting information into multimedia

3. Result

Implementation of our data hiding method starts with encrypting the information into image or audio and assigning stego key to it. Figure 4 shows the home screen for our data

hiding process. From that, user can select their required mode of encryption. Input has to be given for both the cover image or audio and the secret information shown in figure 5 and figure 6.

Figure 4. Home screen for data hiding process

Figure 5. Browsing cover image and secret information

Figure 6. Browsing cover audio and secret information

Before browsing the image/audio and secret information, the system will ask for whether the user wants to embed the secret information or to extract it. After selecting the required option and input the secret information will get hided successfully shown in figure 7.

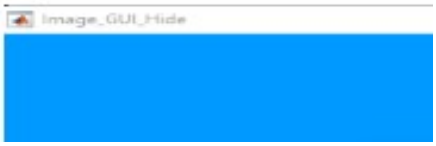

Figure 7. Data hided successfully

In the receiver end for retrieval process, the user will be asked for the image to be retrieved and the stego key as password shown in figure 8. After giving the correct stego key, the user will able to see the original information which is embedded in the multimedia. Final output is shown in figure 9. Receiver can see the hidden information only if the stego is entered correctly otherwise he can only see the image or audio file.

Figure 8. Browsing image for decryption of secret information

Figure 9. Final output for getting secret information

4. Conclusion

In the growing demand for security in data transmission, this paper suggest an efficient approach for using cryptography and stenography for the current scenario gropu of

societies. Here the information is hidden secretly inside the multimedia like image and audio. The main advantage of this method is the message is not visible if it goes in hand of an undesired user because stego key is necessary for showing the hidden information. And the process involved in implementing this method is very simple. It will be no occurrence of delay so that it is suitable for the real-time application. Hence this method can serve the need for data security in all confidential data transmission.

REFERENCES

[1] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, vol. 1, **(2010)**, pp. 1-4.

[2] DellaBaby, JithaThomas, Gisny Augustine, Elsa George, Neenu RosiaMichael, "A Novel DWT Based Image Securing Method Using Steganography", Procedia Computer Science, vol. 46, **(2015)**, pp. 612-618.

[3] Bingwen Feng, Wei Lu, and Wei Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, **(2015)**, pp. 243-255.

[4] Harshita Kapadia, Harawane Sneha Haribau, Harsha Patil, "Audio Steganography and Security Using Cryptography", International Journal of Computer Science and Network, vol. 4, no. 2, **(2015)**, pp. 285-288.

[5] Rajani Devi. T, "Importance of Cryptography in Network Security", Proceedings of the IEEE International Conference on Communication Systems and Network Technologies, Gwalior, India, **(2013)** April 6-8.

[6] Chintan Dhanani, Krunal Panchal, "Steganography using web documents as a carrier: A Survey", International Journal of Engineering Development And Research, vol. 10, pp. 172-179.

[7] Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application, vol. 2, **(2011)**, pp. 102-108.

[8] William Stallings, Editor, "Cryptography and Network security: Principles andpractice", Pearson, **(2011).**

[9] TanmayBhowmik, PramathaNathBasu, "On Embedding of Text in Audio A Case of Steganography", Proceedings of the 2010 International Conference on Recent Trends in Information, Telecommunication and Computing, Kochi, Kerala, India, **(2010)** March 12-13.

[10] K. Gopalan, "Audio steganography using bit modification", Proceedings of the IEEE Int.Conf. Acoustics, Speech, and Signal Processing, Hong Kong, China, **(2003)** April 6-10.