ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 3, March 2017

A Hidden Encryption Scheme for Enhanced Security

B Siva Prasad Rao Naidu, T Sujatha

M.Tech Student, Dept. of CSE.,Vizag Institute of Technology, Dhakamarry, Vishakapatnam, India

Assistant Professor, Dept. of CSE.,Vizag Institute of Technology, Dhakamarry, Vishakapatnam, India

ABSTRACT: In the world of technology, the use of internet is rapidly increasing leading to the access of information by unauthorized users. To prevent this, the security aspect of system is designed. Security techniques such as encryption, firewalls and passwords are designed to prevent unauthorized gain to information to protect the integrity of computing resources and to limit the potential damage that can be caused by attackers and intruders. Establishing hidden communication is an important discussion that has gained increasing importance nowadays with the development of the Internet. In this paper we designed the one of the methods for establishing hidden communication through steganography.

KEYWORDS: Data files, Cryptography, Steganography, Encryption, Decryption

I. INTRODUCTION

The main objective of this paper is to provide more security on data file and text message in the secure communication channel by using steganography on data files. In this paper the data files and text messages to be hide behind another medium like images or audio wave files, video files and data files with the help of popular technique Least Significant Bit Insertion. After embedding the data files behind another medium then we can send, receiver can visualize only the stego file. After applying stego algorithm the user can see the original data or text message. So in this way we provide the more security on data file and text message.

II. RELATED WORK

As the usage of internet and technology have increased a lot challenging the security design. With the increasing usage of networks the intruders also have been increased. In this paper we have proposed a Hidden Message Generation Scheme which enhances the security of users data being used by the intruders. The explanation of this scheme is discussed in section 4.

III. EXISTING METHODOLOGY

Technology today is greatly based on communication. So the communication should be to say strictly must be secure. But that is not achieved with the usage of Cryptography. Let's extend that with a popular Technique called Steganography simply defined as the art of secret writing.

Cryptography vs. Steganography:

Cryptography is the art of scrambling messages so that even if a message is detected, then it is very difficult to decipher. The purpose of Steganography is to conceal the message such that the existence of the hidden message is 'camouflaged'. These techniques are not mutually exclusive.

Steganography and Cryptography are complementary techniques. Based on strength of algorithm, if an encrypted message is discovered, it will be subjected to cryptanalysis. Likewise, no matter how well concealed a message is, it is always possible that it will be discovered. Combination of Steganography with Cryptography we conceal the existence of an encrypted message. In doing this, we make it far less likely that an encrypted message will be found. Also, if a message conceived through Steganography is discovered, the discoverer is still faced with the formidable task of deciphering it.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 3, March 2017

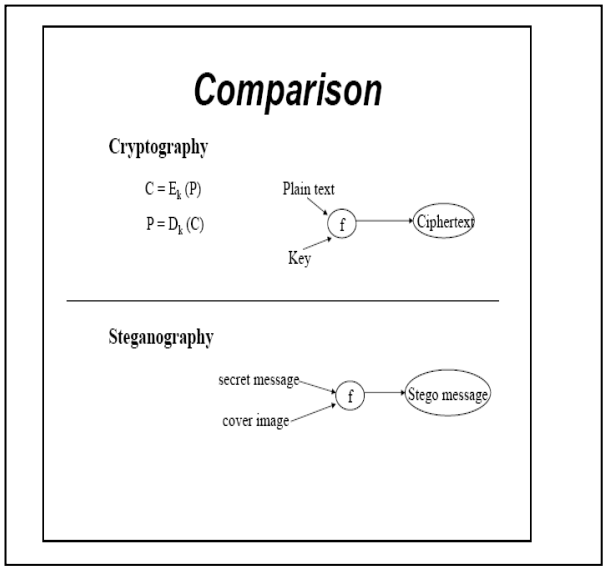

Figure 1: Demonstration of Cryptography vs. Steganography

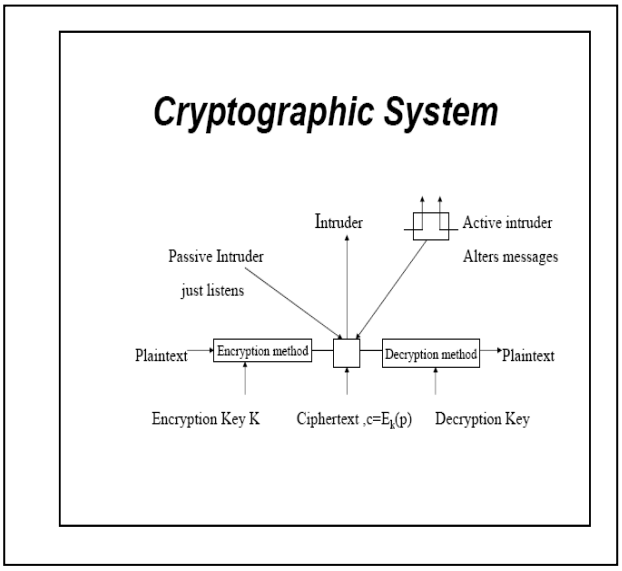

Figure 2: Demonstration of a Cryptographic System

In the above figure 1 we can see the processing of a plain text message with a key in a function f to generate cipher text. This process is depicted in terms of the equation C = Ek (P) ---------- (1)

From the equation 1 we can say that cipher text message C is generated by Encryption E of Plain text message P by using a key k.

Similarly we can see the equation P = Dk (C) ----------\----------(2)

From the equation 1 we can say that plain text message P is generated by Decryption D of Cipher text message by using the key k.

The decryption process can be done either by using the same key used for encryption or if sender used a public key for encryption then receiver uses the sender's private key.

This is the depiction of encryption and decryption process in Cryptography.

From figure 1 we can also see the processing of a 'stego' message. The secret message and cover image are processed through function f to generate a stego message. This is the depiction of message processing in Steganography.

In the above figure 2 we can see the demonstration of a Cryptographic system. Here we can see the demonstration of plain text message and cipher text message by using encryption method and decryption method , in the communication channel used for data transmission there is a possibility of intruders (active intruders and passive intruders) attacking the messages transmitted through the channel. The plain text message p is encrypted with encryption key k for generation of cipher text message c. This can be seen in equation 1and figure 1, 2. This process is called Encryption Method. Similarly cipher text c is decrypted with decryption key k for generation of plain text p. This can be seen in equation 2 and figure 2. This process is called Decryption Method. Encryption method is applied always at the sender's side whereas Decryption Method is always applied on the receiver's side.

The cipher text message is transmitted through the communication channel from sender to receiver. During the message transmission in communication channel there is a chance of intruders attacking the channel. If there is a passive attack the intruder (passive intruder) just observes the passing of message then there will be not be much harm to the message but the intruder is observing the flow of messages in communication channel. In this case the transmitted message will be sent to the receiver without any change to the contents of message. If there is an Active attack the intruder (active intruder) will alter or modify the message then it is potentially harmful to the original message as the original message contents are being modified or completely replaced. In this case the transmitted message will be sent to the receiver after the alteration or modification of contents of message. This is the phenomena in a Cryptographic system (ref:figure 2).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 3, March 2017

Hence there is a need for introducing a secure scheme for transmission of messages. This Scheme can be used to secure the message by avoiding the intruders to attack the message. Thus we have come up with a hidden message scheme[section 3].

IV. PROPOSED ALGORITHM

BLOCK DIAGRAM:

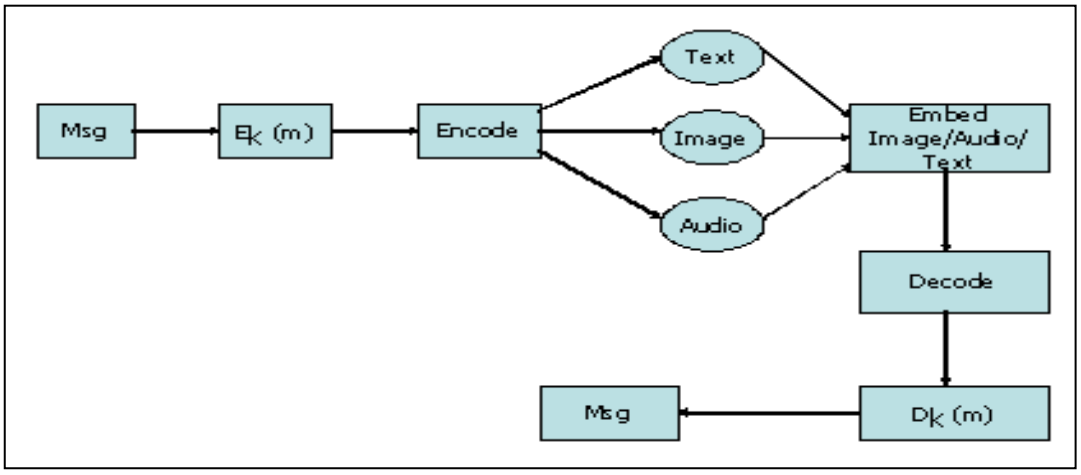

Figure 3: Hidden Message Generation

From figure 3 we can see the steganographic technique that embeds data or information within the spatial domain of the images, audio files by modifying the Least Significant Bit values of the pixels. Here we can see the processing of message through Ek(m) for encoding then the message can be embedded with either text, image or audio files. The message is added to any of the text or audio or video files but it is hidden in the original message to the file it is added to. The same message is transmitted through the communication channel and decoded using Dk(m) at the receiving end. During the message transmission even if the message is attacked by the intruder there is no chance of retrieving the original message as the original message is hidden and the hidden message is confidential to the sender and receiver by using the specified key, the message appears as an audio, video or image file to the intruders. Hence the intruder cannot modify the message as he/she cannot understand the original message contents.

Least Significant Bit Insertion :

We can use the lower bits of the color channels to hide data, then the maximum color change in a pixel could be 64-color values, but this causes a little change that is undetectable for the human vision system. The method is known as Least Significant Bit Insertion.

By usage of this method its possible to embed a significant amount of data with no visible degradation of the coverimage.

V.CONCLUSION

In this paper we have come up with a proposed methodology a technique named Hidden Message Encryption Scheme where all the original messages are embedded into the multimedia files (audio, video, and image) to provide enhanced security. The functionality of our scheme can satisfy the network users from all walks of life. If an intruder want to gain the data its impossible to extract data from the audio or video or image file as the original data is hidden.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 3, March 2017

VI. FUTURE WORK

The scope of the paper is laid in the usage for hide the data file or text message behind any other medium called images, audio files, video files again in data. Further the paper may be extended to hide images in to any other medium, video files will be hide another medium called data files, images, audio files and video files.

REFERENCES

1. R.China Appala Naidu and P.S.Avadhani, " A Comparison of Data Mining Techniques for Intrusion Detection", Proceedings of the 2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)-2012, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India,23rd August 2012, ISBN No. 978-1-4673-2047-4, pp. 42-45, 2012
2. A two phase copyright protection scheme for digital images using visual cryptography and sampling methods Venkateswara Rao Bolla; Swathi Amancha; T Venu Gopal 2016 International Conference on Electrical, Electronics, and Optimization Techniques(ICEEOT)-2016,DMI College of Engineering,Palanchur,Chennai,3rd March 2016,ISBN No. 978-1-4673-9939-5,pp 2041-2046
3. Modern approach of detecting packet loss and recovery in the networks Swathi Amancha; R. China Appala Naidu; Venkateswara Rao Bolla; K. Meghana 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) -2016,DMI College of Engineering,Palanchur,Chennai,3rd March 2016,ISBN No. 978-1-4673-9939-5,pp 1722 – 1727
4. I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process.6(12), 1673–1687 (1997).
5. S. Low and N. Maxemchuk, "Performance comparison of two text marking methods," IEEE J. Sel. Areas Commun. 16_4_, 561–572 (1998).
6. K. Matsui, J. Ohnishi, and Y. Nakamura, "Embedding a signature to pictures under wavelet transform," IEICE Trans. J79-D-II(6), 1017–1024(1996).
7. Information Hiding Techniques for Steganography and Digital Watermaking- Stephan Katzenbeisser; Fabien Petitolas
8. Investigator's Guide to Steganography- Gregory Kipper
9. Hiding in Plain Sight: Steganography and the Art of Covert Communication (paperback) – Eric Cole
10. Steganography and the Attacks –Emmanuel Sodipo
11. Stallings, W. Cryptography and Network Security
12. Schnier, B. Applied cryptography
13. Johnson, N. Steganography & Cryptography
14. Naughton. Java Complete Reference