International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 17
December 2017

An Enhanced Encryption Scheme for Securing Data Transmission

1st N Krishnavardhan [1], 2nd Swathi Amancha[2]
[1]Associate Professor,CSE,St Martin's Engineering College
[2]Assistant Professor, CSE, St Martin's Engineering College

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 invisible data transmission is an important discussion that has gained increasing importance now a day with the development of the Internet. In this paper we designed the one of the methods for establishing invisible data transmission through steganography.

Keywords

Datafiles,Cryptography, Steganography, Encryption, Decryption

1. 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 more security on data file and text message.

2. Existing system

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 popular Technique called STEGANOGRAPHY simply defined as the art of secret writing.

Cryptography vs. Steganography:

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

Steganography and Cryptography are complementary techniques in which 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. By combining Steganography with Cryptography we can 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 concealed through Steganography is discovered, the discoverer is still faced with the formidable task of deciphering it.

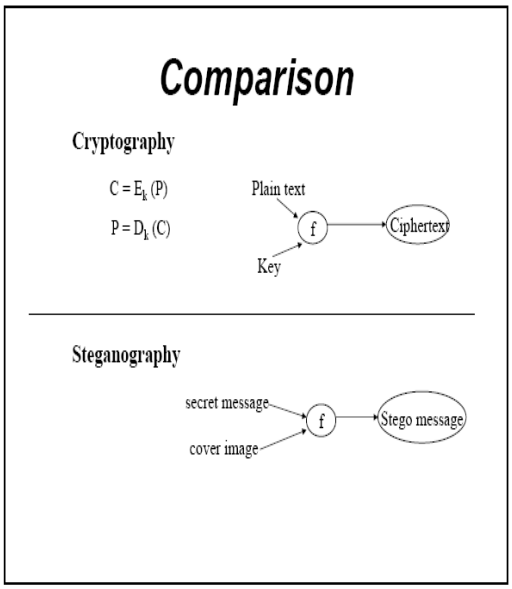

Figure 1: Demonstration of Cryptography vs. Steganography

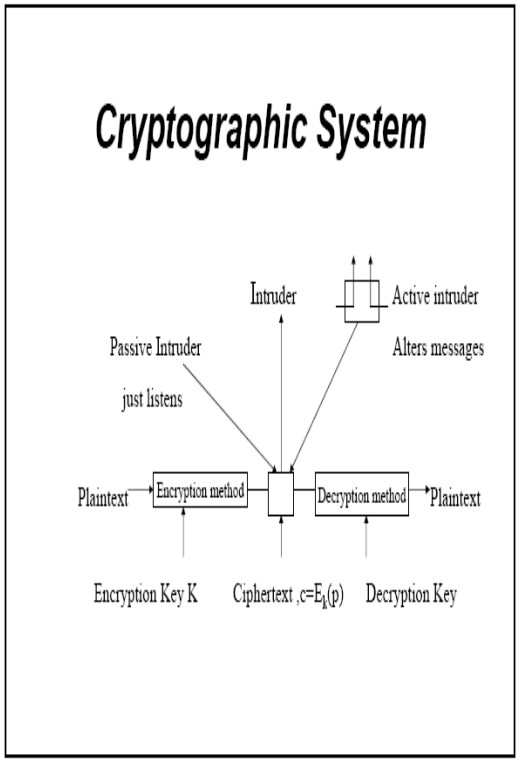

Figure 2: Demonstration of a Cryptographic System

Cryptography is the technique of using mathematical calculations to encrypt and decrypt data and enables the users to store sensitive information and transmit across insecure networks (like Internet) so that it cannot be read by anyone except the intended recipient.

3. Problem Definition

With the rapid development of multimedia data management technologies over the internet there is need to concern about the security and privacy of information. In multimedia document, dissemination and sharing of data is becoming a common practice. At present as the internet forms the open source for all users, security forms the critical issue. Hence the transfer of information over the internet forms the critical issue. At present situations we are using cryptography technique for providing security.

Cryptography constitutes of encryption and decryption processes. Encryption is the process of converting normal text to cipher text. Now, this cipher text (not understandable form of data) is sent to destination. At the destination, decryption process is to be done. Decryption is the process of converting cipher text to normal text. We think that here security is provided. But in between source and destination, unauthorized user identifies that there is transfer of some data which is not understandable. So though he cannot understand he can modify data. So with this, at destination, we can find modified data. Hence the problem is occurring here.

4. Proposed System

The majority of the messages hidden today are inside digital images, audio files or video files. That means there are 256 different variations of each color in every pixel that makes a picture. So to representation of the white color, the code would look like 11111111 11111111 11111111. Now, the human eye cannot distinguish the difference between too many colors and so the color 11111110 11111110 11111110 would look exactly the same as white.

Because of this, the last digit in every bit in every pixel could be changed. This is based on the Least Significant Bit Insertion technique. Hence our methodology is named as Hidden Message Encryption Scheme.

Here, Steganography involves hiding of text message inside an audio file (.wav0, inside a text message (.txt), inside an image file (.jpg). The sender can send the embedded messages, images, audio/video without knowing the actual message hidden in them by the third party. That hidden message can be only viewed by the destination party if and only if the destination party is aware of the Key.

BLOCK DIAGRAM:

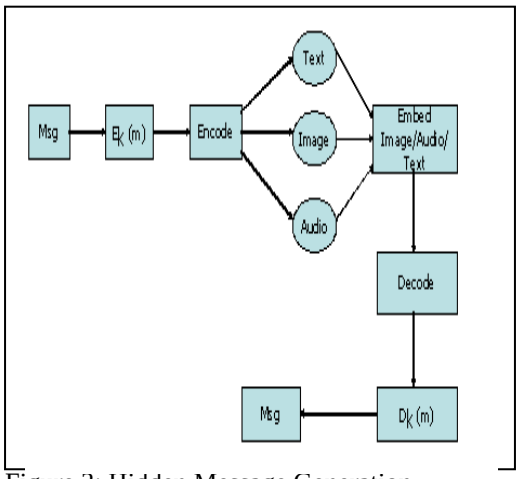

Figure 3: Hidden Message Generation

From figure 3 we can see the stegnographic 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 cover image.

5. 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.

6. 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.

7. References

[1]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

[2]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

[3]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).

[4]S. Low and N. Maxemchuk, "Performance comparison of two text marking methods," IEEE J. Sel. Areas Commun. 16_4_, 561–572 (1998).

[5]K. Matsui, J. Ohnishi, and Y. Nakamura, "Embedding a signature to pictures under wavelet transform," IEICE Trans. J79-D-II(6), 1017– 1024(1996).

[6]Information Hiding Techniques for Steganography and Digital Watermaking- Stephan Katzenbeisser; Fabien Petitolas

[7]Investigator's Guide to Steganography- Gregory Kipper

[8]Hiding in Plain Sight: Steganography and the Art of Covert Communication (paperback) – Eric Cole

[9]Steganography and the Attacks –Emmanuel Sodipo

[10]Stallings, W. Cryptography and Network Security

[11]Schnier, B. Applied cryptography

[12]Johnson, N. Steganography & Cryptography

8. Author's Biography

Mr.N.Krishnavardhan,post graduated in computer science(M.Tech)from jntuh in 2010 and graduated in computer science and engineering(B.Tech) from jayaprakash Narayanganj college of engineering in 2004.having 6 years of experience as asst.professor and 6 years of experience as assoc.professor.he is presently working as assoc.prof in cse department in St.Martin's engineering college,hyderabad.Area of interest in computer networks,network security and big data

. Ms Swathi Amancha, Post Graduated in Computer Science and Engineering (M. Tech) from JNTUH in 2012 and graduated in Computer Science and Engineering (B.Tech) from JNTUH in 2009.Having 8 years of experience as Asst Professor. She is presently working as Asst Professor in Computer Science and Engineering department in St. Martin's Engineering College, Hyderabad. Area of interest in Computer Networks, Network Security, Big Data, Information Security, Image processing.