ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

Image And Audio Based Secure Encryption And Decryption

Pawar Ashwini [1], Pawar Bhagyashree[2], Rajguru Ashwini[3], Prof.Y.R.Nagargoje [4] , Prof.M.A.Khan[5]

Student,CSE Department, Savitribai Phule Womens Engineering College,Aurangabad,India[1,2,3]

Assistant Professor, CSE Department, Savitribai Phule Womens Engineering College,Aurangabad,India[4,5]

Abstract: Steganography (a rough Greek translation of the term Steganography is secret writing) has been used in various forms for 2500 years. Briefly stated, steganography is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. In steganography, the message used to hide secret message is called host message or cover message. Once the contents of the host message or cover message are modified, the resultant message is known as stego message. In other words, stego message is combination of host message and secret message. Audio steganography requires a text or audio secret message to be embedded within a cover audio message.

Keywords: Steganography, Steganographic tools, RSA Algorithm, image and audio data hiding

I. INTRODUCTION

The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words “steganography means hiding one piece of data within another”. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements [3]

- The cover media(*C*) that will hold the hidden data
- The secret message (*M*), may be plain text, cipher text or any type of data
- The stego function (*Fe)* and its inverse (*Fe-1*)
- An optional stego-key (*K*) or password may be used to hide and unhide the message.

A. Image Steganography

Information security is essential for confidential data transfer. Steganography is one of the ways used for secure transmission of confidential information. Hiding information using steganography[7] in a photograph is less suspicious than communicating an encrypted file. The main purpose of steganography is to convey the information secretly by concealing the very existence of information in some other medium such as image, audio or video.

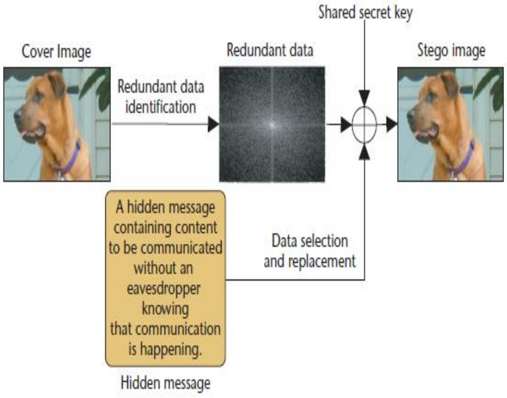
Shared secret key
Cover Image
Redundant data
Stego image
Redundant data identification
A hidden message containing content to be communicated without an eavesdropper knowing that communication is happening.
Data selection and replacement
Hidden message

Fig 1.1:Image Steganography

Cryptography: Cryptography scrambles messages so it can’t be understood. Modulo encryption is a popular data hiding technique in mobile devices.[4]

Steganography: It is an ancient art of hiding information. It hides information in digital images.

B.Audio Steganography

There are two concepts to consider before choosing an encoding technique for audio. They are the digitalformat of the audio and the transmission medium of the audio. There are three main digital audio formats typically in use. They are Sample Quantization, Temporal Sampling Rate and Perceptual Sampling. Sample Quantization which is a 16-bit linear sampling architecture used by popular audio formats such as (.WAV).Temporal Sampling Rate uses selectable frequencies (in the KHz) to sample the audio. The last audio format is Perceptual Sampling. This format changes the statistics of the audio drastically by encoding only the parts the listener perceives thus maintaining the sound but changing the signal. This format is used by the most popular digital audio on the Internet today in ISO MPEG (MP3). Transmission medium (path the audio takes from sender to receiver) must also be considered when encoding secret messages in audio.

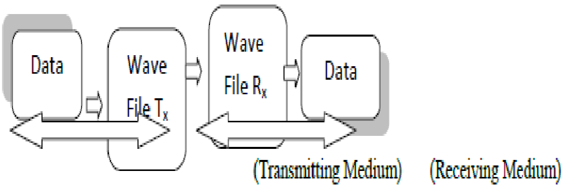

Fig 1.2:Audio Steganography

As shown above, the data is converted in stegano-object (in this case audio file) and is being transmitted and on the receiving terminal the stegano-object is processed and is converted back into the original data.

RSA Algorithm: Rivest , Shamir , Adlemen
Steps of algorithm:
Step 1: Let p and q be the 2 prime numbers.

Step 2: Subtract 1 from p and q and take product of them n= (p-1)*(q-1)

Step 3: The product is denoted by Ɵ(n) i.eƟ(n)=(p-1)*(q-1)

Step 4: Select the relative value of e such that it lies between 1<=e<=Ɵ(n)

Step 5:For decryption the formula can be used as (d*e)modƟ(n)=1

Step 6: public key(e,n) Private key(d,n)

II. LITERATERE SURVEY

In today's world, we often listen a popular term "Hacking". Hacking is nothing but an unauthorized access of data which can be collected at the time of data transmission. With respect to steganography this problem is often taken as Steganalysis[8]. Steganalysis is a process in which a steganalyzer cracks the cover object to get the hidden data. So, whatever be he technique will be developed in future, degree of security related with that has to be kept in mind.

III. PROPOSED SYSTEM

The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. In a computer-based audio steganography system, secret messages are embedded in digital sound.

The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files. In future we can also implement video steganography.Proposed Image and Audio Steganography system is a method of data hiding [5] is the process of hiding information behind the wave file that is carrier file. The message is first encrypted and then embedded in the carrier. The system has following four layers

- Encryption
- Encoding
- Decoding
- Decryption

Encoding : The process of hiding the message in the image and audio file.
Decoding : Decoding is a process of retrieving the message from the Image and audio file.

IV. ADVANTAGES

- Provision for encryption of message before encoding it into the audio file to enhance the security.
- Provision of encryption key and complex encryption algorithm.
- The encryption key is modified by the algorithm to get a new key which is used for encrypting the message. So even if the key is known for an intruder, he cannot break the code.
- Time to encode and decode is very less.

V. APPLICATION

Stegnography can be used any time you want to hide data.There are many reasons to hide data but they all boil down to the desired to prevent unauthorized persons from becoming aware of the existence of a message. With these new techniques,a hidden message is indistinguishable from white noise.Even if the message is suspected,there is no proof of its existence.In the business world steganography can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used for corporate espionage by sending out trade secrete without anyone at the company being any the wiser.[9]. Terroist can also used steganography to keep there commmunication secret and to coordinate attacks.

VI. CONCLUSION

This paper we have introduced a robust[6] method of imperceptible audio data hiding. This system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format.

Thus we conclude that audio data hiding techniques can be used for a number of purposes other than covert communication , information tracing and finger printing. As the sky is not limit so is not for the development. Man is now pushing away its own boundaries to make every thought possible. So similarly these operations described above can be further modified as it is in the world of Information Technology.

ACKNOWLEDGMENT

We would like to thank our guide Prof.Y.R.Nagargoje, for their guidance and feedback during the course of the project. We would also like to thank our department for giving us the resources and the freedom to pursue this project.

REFERENCES

[1] Kesslet, Gary C. An Overview of Steganography for the Computer Forensics Examiner, Burlington, 2004.

[2] Lin, Eugene and Edward Delp: A Review of Data Hiding In Digital Images, West Lafayette, 1999

[3] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn,―Information Hiding—A Survey,‖ Proc. IEEE, vol. 87, no.7,1999, pp. 1062–1078.

[4] William Stalings "Cryptography and NetworkSecurity",prentice Hall of India Private Limited,NewDelhi 110001.

[5] W. Bender, D. Gruhl, N. Morimoto and A.Lu, "Techniques for data hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-336, 1996.

[6] Chen and G.W. Womell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding",IEEE Transactions on Information Theory, Vol. 47, No. 4,pp. 1423-1443, May 2001.

[7] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin and M. Z. I. Shamsuddin, "Information Hiding using Steganography", 4th National Conference on elecommuni cation Technology Proceedings, Shah Alam, Malaysi.

[8] Introduction to steganography, Brigitte Si Athabasca University, COMP607 Project, July, 2004

[9] The WEPIN Store,"Steganography(Hidden Writting)",1995

[10] Ross J. Anderson, Fabien A.P. Petitcolas, On The Limits of Steganography, IEEE Journal, May 1998.

BIOGRAPHIES

Miss.Ashwini M. Pawar is currently pursuing B.E.degree in Computer Engineering from Savitribai Phule Womens Engineering (BAMU) .Intrested area are ASP.NET,C#.Net.

Miss. Bhagyashree B. Pawar is currently pursuing B.E. Degree in Computer Engineering from Savitribai Phule Womens Engineering (BAMU) ASP.NET, C#.Net

Miss. Ashwini V. Rajguru is currently pursuing B.E.degree in Computer Engineering from Savitribai Phule Womens Engineering (BAMU). Intrested areas are ASP.NET, C#.Net.

Y.R.Nagargoje received his BE degree in Computer Science And Engineering from Mumbai University(MH). He is currently working as Assistant Professor in Savitribai Phule Women's Engineering College.Aurangabad(MH)

M.A.Khan received his BE degree in Information Technology from Dr.BabasahebAmbedkar Marathwada University. Aurangabad (MH). He is currently working as Assistant Professor in Savitribai Phule Women's Engineering College. Aurangabad (MH)

Miss. Bhagyashree B. Pawar is currently pursuing B.E.degree in Computer Engineering from Savitribai Phule Womens Engineering