International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-2, Issue-3, March 2014

Metamorphic Cryptography: A Fusion of Cryptography and Steganography

Atul Haribhau Kachare, Mona Deshmukh

***Abstract*— In current information security, the interchange over the network stakes a most important threat of getting it hacked. The different approaches like Cryptography and Steganography are used for addressing such harms. But both of them have some gaps and when used discretely does not perform well. Hence, we use the amalgamation of both Cryptography and Steganography called as Metamorphic Cryptography. In state of the art system, image is used as a key component. But the core concern with image is that it intensifies the computational complexity because of its multi-dimensional nature. In the proposed algorithm dimensionality reduction is achieved using speech signal as a key component. The speech signal being vulnerable to noise, it is commonly parameterized before transmission over the channel. In this paper, Line Spectral frequencies are used as parameters of the speech signal. These parameters are further used to encode and hide text messages. The modest XOR process is used for encoding and decoding.**

***Index Terms*— Cryptography, steganography, metamorphic cryptography, linear prediction, line spectral frequencies.**

I. INTRODUCTION

In current age Information Security plays a vibrant role. Information or messages are exchanged over a network out of which enormous data is confidential or secluded which increases the demand for advanced information security. Security has become the important features in communication these days due to the existence of hackers who wait for a chance or opportunities to gain an access to confidential or secluded data. We can employ two diverse methodologies for the information security which are Cryptography and Steganography.

A. Cryptography

Cryptography is derived from` the Greek word "KRYPTOS" meaning "concealed" and "GRAPHEIN" meaning "to write". It is a study of means of altering information from its ordinary all-inclusive form to an incomprehensive format rendering it unreadable without the secret knowledge. Generally speaking, computer cryptographic tasks can be broken into two general categories: encryption and authentication [1]. Encryption refers to the scrambling of information so that the original message cannot be determined by unauthorized recipients.

Manuscript received March 20, 2014
Atul Haribhau Kachare, Student, Department of Information Technology, VESIT, Mumbai University, India, 9867718014.
Mona Deshmukh, Assistant Professor, Department of Master of Computer Applications, VESIT, Mumbai University, India, 9619079377.

An encryption algorithm is applied to the message, referred to as the plaintext, and a key to produce cipher text. A decryption algorithm converts the cipher text back into plaintext, but only if given the correct code.
Mainly there are three forms of cryptography:

- Classical cryptography
- Modern cryptography
- Rotor machine

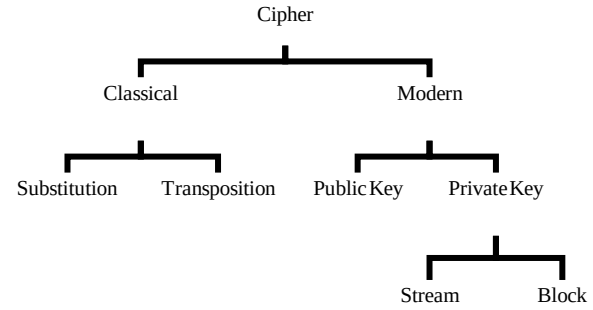

Figure 1Cryptography Techniques

Classical Cryptography is usually divided into two extensive categories [1]:

- Masking: The use of masking leads to substitution.
- Veiling: The use of veiling leads to transposition.

In Modern cryptography technique there are two type of cryptography [1] [2]

- Symmetric Cryptography Technique:
  A single key is used for both encryption and decryption which is already known to both Sender and Receiver.

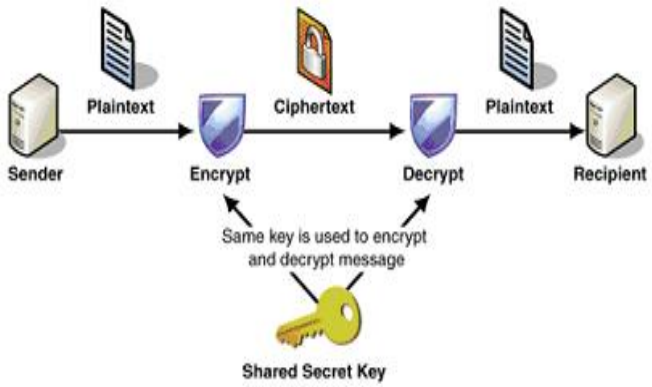

Figure 2 Symmetric Key Cryptography

- Asymmetric Cryptography Technique:

A pair of keys called public and private key is used for encryption and decryption.

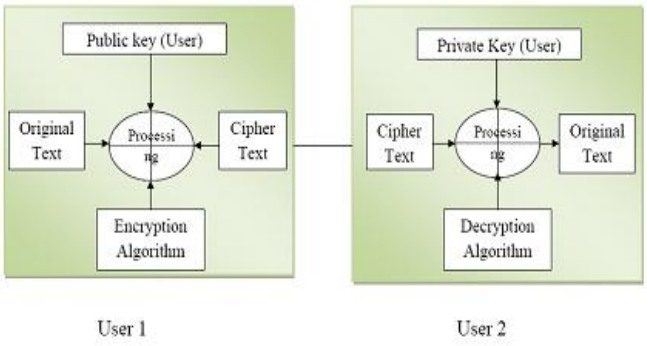

Figure 3 Asymmetric Key Cryptography

There are fundamentally two approaches of producing cipher text. They are:

- Stream cipher:
  Each bit of data is sequentially encrypted using one bit of the key.
- Block cipher:
  Here data is encrypted in chunks of specific size.

B. Steganography

Steganography is derived from the Greek word "STEGANOS" meaning "enclosed/secret" and "GRAPHEIN" meaning "to write/draw". It is the study of means of masking the information in order to prevent hackers from sensing the existence of secret information [1]. The process of wrapping message without leaving remarkable traces is known as Steganography.

The majority of today's steganography systems uses multimedia objects like image, audio, video etc. as cover media because people often transmit digital pictures, images or audios over email and other Internet communication [3]. In modern tactic, depending on the nature of cover object, steganography can be separated into five natures:

- Text Steganography
- Image Steganography
  - Least significant bit insertion
  - Masking and filtering
  - Redundant pattern encoding
  - Encrypt and Scatter
  - Algorithms and Transformations
- Audio Steganography
- Video Steganography
- Protocol Steganography

Cryptography and Steganography both undertake the same goal using completely different means. Encryption encodes the data so that an unintended beneficiary cannot determine its intended meaning. Whereas, Steganography in contrast attempts to prevent an unintended addressee from suspecting that the data is present.

The proposed method is a blending of both the techniques to provide a very high degree of security for the information. The metamorphic cryptography can be termed as a paradox among the Cryptography and Steganography.

The objective of this paper is to describe the proposed model for integrating together cryptography and steganography through audio signal processing. In particular, we present a system able to perform steganography and cryptography at the same time. We will show such system is an effective steganography and is also an unbreakable proposed cryptographic one. Rest of the paper is organized are as follows: Section – 2 is presents literature survey and problem definition, Section – 3 is presents proposed work, Section – 4 is presents outcome, Section – 5 is presents conclusion, and final Section is presents acknowledgment and references.

II. LITERATURE SURVEY

There are many numbers of encryption algorithms available from simple additive cipher to the complicated Symmetric and Asymmetric key ciphers. Using this various ciphering or encryption techniques we can increase the security of our data. But the question is whether these encryption techniques are good enough to protect our data. If large numbers of cryptographic techniques are there then more number of cryptanalysis techniques are also available.

The main goal of the cryptanalyst is to obtain the maximum information about the plaintext. So using various kinds of possible attacks the cryptanalyst can broke down the cipher code. By using the knowledge of ciphertext, known plaintext, chosen plaintext, chosen ciphertext, cryptanalyst can easily get access to the encryption key.

In paper [4] various attacks possible on both symmetric as well as asymmetric cryptographic techniques are listed such as Boomerang attack, Brute force attack, Davie's attack, Differential cryptanalysis, Integral cryptanalysis, linear cryptanalysis, Man-in-the-middle.

Thus we can say using only cryptography cannot provide the required security.

Now if consider the steganography technique, from paper [5] we can conclude that if we use Text Steganography then also there are some disadvantages are possible such as some text steganography methods do not allow Optical Character Recognition , also they hide very small part of data, etc. Even in case of Image Steganography there are some loopholes are present. In some methods we have the overhead of hiding extra bits [6], in some method hidden capacity is low [7], in some methods computational complexities is higher as compare data hidden [8], in some method matching pattern has to be stored [9], in some methods hidden capacity degrades the visual quality [10] and some methods do not support the color images for steganography [11]. In case of audio steganography maximum time only .wav format is used as media and transferring only .wav files over network may attract the attention of malicious intruder. Hence we can conclude that even Steganography technique do not provide the stronger security.

In paper [12] focus is given on the combination of Cryptography and Steganography method and a new technique – Metamorphic Cryptography has suggested. In the system specified in paper [12] image steganography is for the metamorphic cryptography. The message is transformed into a cipher image using a key, concealed into another image using steganography resulting into some intermediate text which is finally converted into final cipher image. To find the original message whole process is reversed.

III. PROPOSED WORK

A. Motivation

As we know due to some measures like Secrecy, Robustness and Complexity, existing system lacks to provide the ample security to the data. So to elude it, in this proposed idea we use Audio media for the audio steganography along with the cryptography.

B. Proposed System

In proposed scheme, input is taken from the user in string format. We may use some simple ciphering algorithm over to provide optionally added security advantage. The resultant string is then converted into set of ASCII codes. On the other hand, an audio or speech is taken as input and encoded using one of the feature extraction algorithms to compute the feature vectors which are used for encryption purpose. Then the simple logical xor-ed operation is performed on the ASCII value and encrypted audio feature vectors. The modified feature vectors resulting from the xor-ed operation are resynthesized to produce the cipher audio signal. The cipher audio is then covered by a cover audio using steganography and is converted into an intermediate text. This intermediate text is once again encrypted using the encryption algorithm as proposed above to obtain final cipher audio or speech. This speech is transmitted to the receiver. The received speech signal is decrypted it to obtain the intermediate text and analyzed with the cover audio signal to reconstruct the cipher audio. This cipher audio is further deciphered to obtain the encrypted message. Finally the decryption algorithm is used to recover the original text message.

C. Algorithm for Proposed System

Algorithm for Sender:

- Input the message to ENCRYPTION ALGORITHM.
- Obtain the cipher audio.
- Input the cipher audio to STEGANOGRAPHY ALGORITHM.
- Obtain the intermediate text.
- Load the intermediate text to ENCRYPTION ALGORITHM again.
- Obtain the final audio to be transmitted.

Algorithm for Encryption:

- Input the message to be encrypted.
- Input the sample speech signal.
- Perform the segmentation and framing [13] to create different frames of the size of message blocks.
- For every frame calculate the LPC [14] parameters using auto-correlation and toiplitz matrix.
- Using the Conversion equation the LPC parameters are again converted into LSF [15] parameter.
- Perform the Xor-ed operation on the LSF parameter and the ASCII values of the message.
- The resultant matrix of Xor-ed operation is again converted into Speech signal using LPC Synthesis.

Algorithm for Steganography:

- Input the cover speech signal.
- Input the cipher speech signal.
- Calculate the LPC and finally the LSF parameters for both the signals.
- Perform the Xor-ed operation on the LSF parameters of both the signals.
- Convert the resultant ASCII value matrix into corresponding text format which is known as intermediate text.

Algorithm for Receiver:

- Input the final cipher speech to DECRYPTION ALGORITHM.
- Obtain the intermediate text.
- Input the intermediate text to RETRIVAL CIPHER_SPEECH_ALGORITHM.
- Obtain the cipher speech.
- Input the cipher speech to the DECRYPTION ALGORITHM.
- Obtain the original plain text message.

Algorithm for Decryption:

- Input the final cipher speech.
- Input the sample speech used by sender.
- Perform segmentation and framing on both the signals to get frames.
- For every frame calculate the LPC parameters.
- Using conversion equation LPC parameters are converted into LSF parameters for both signals.
- The LSF parameters of both signals are Xor-ed to get the resultant matrix of ASCII values.
- This ASCII values are converted into the Intermediate text.

Algorithm for Retrieving Cipher Speech:

- Input the cover speech.
- Input the intermediate text.
- Perform segmentation and framing on the cover speech signal.
- Calculate the corresponding LPC and then LSF parameters.
- Perform XOR operation on LSF parameters and the ASCII values of intermediate text.
- Obtain the cipher speech.

IV. OUTCOMES

The proposed system stated above was applied to a message in Figure IV-1. The cover audio used for the process is shown in Figure IV-2. The encrypted results were obtained as shown in Figure IV-3 and Figure IV-4.

The audio in was decrypted using the decryption technique to obtain the decrypted outputs as shown in Figure IV-5, Figure IV-6 and Figure IV-7.

Metamorphic Cryptography: A Fusion of Cryptography and Steganography

Figure 4 Message to be Encrypted

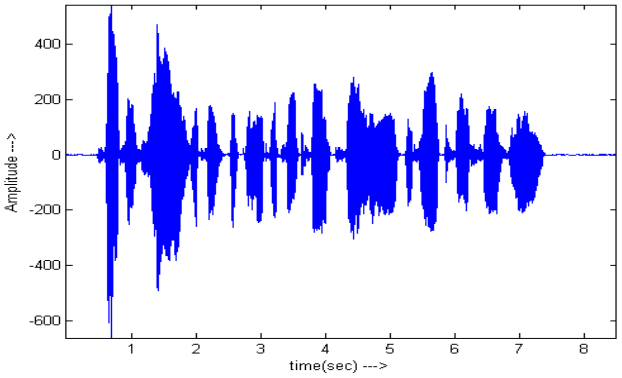

Figure 5 Intermediate Audio Signal

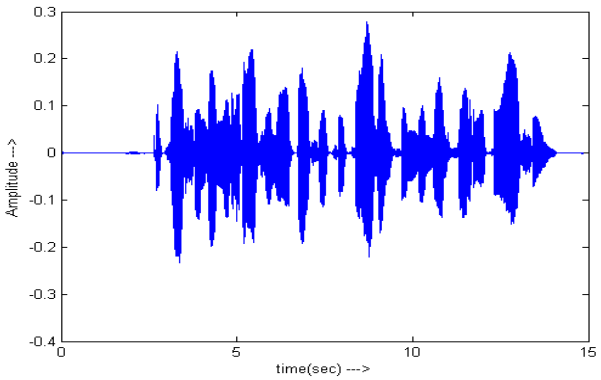

Figure 6 Cover Audio Signal

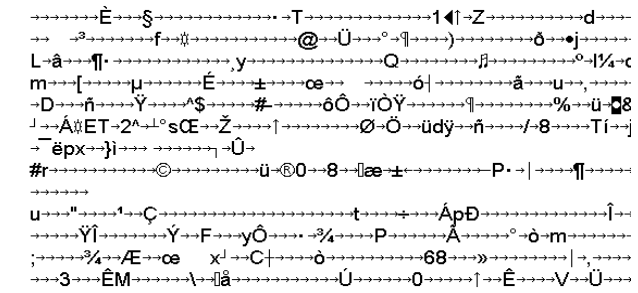

Figure 7 Intermediate Text

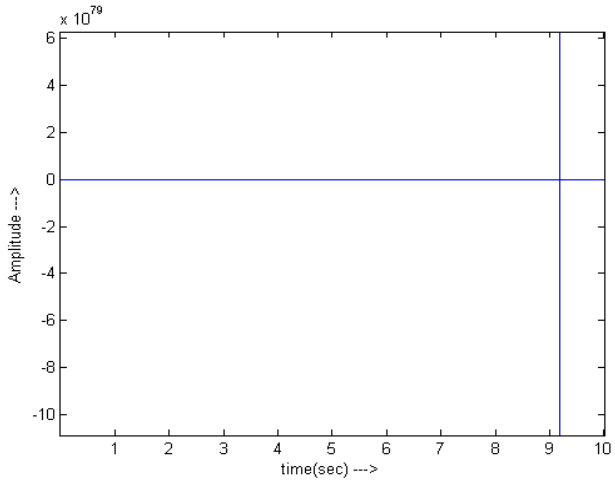

Figure 8 Final Cipher Audio

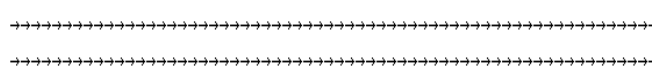

Figure 9 Intermediate Text after Decryption

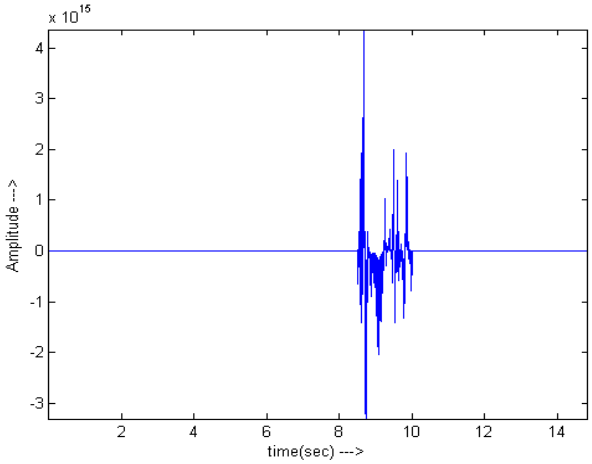

Figure 10 Intermediate Audio Signal after Decryption

Metamorphic Cryptography: A Fusion of Cryptography and Steganography

Figure 11 Decrypted Original Message

V. Conclusion

The paper proposed a novel algorithm using one dimensional speech signal as key component in metamorphic cryptography. The use of cryptography and steganography together provides added advantage of good information security whereas, the line spectral parameters representing speech signal provides good stability and correlation over the channel. The proposed system implementation is under process using MATLAB as a tool for digital signal processing.

The system implementation still needs few more inspection about the number system algorithm should work on and types of speech signals that can be used.

Acknowledgment

The authors would like to thank Prof. Smita Jangale, Department of Information Technology, VESIT and Prof. S. M. Toraskar, pursuing PhD, IITB for sharing his valuable inputs and suggestions regarding this study. Authors would also like to thank Prof. M. Vijaylakshmi, Head Department of Information Technology, VESIT for giving permission to work on this project and making available the laboratory resources.

We are thankful to our parents to whom we are greatly indebted for their support and encouragement.

References

[1] William Stallings, Cryptography and Network Security: Principles & Practices, Second edition.
[2] Luis Von Ahn, Nicholas J. Hopper, "Public-Key Steganography".
[3] Danah Boyd and Alice Marwick,"Social Steganography: Privacy in Networked Publics", ICA 2011.
[4] Mr. Vinod Saroha, Suman Mor, Jyoti Malik,"A Review of Various Techniques of Cryptanalysis", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, ISSN: 2277128X, IJARCSSE October 2012.
[5] Swati Gupta, Deepti Gupta, "Text-Steganography: Review Study & Comparative Analysis", International Journal of Coomputer Science and Information Technologies, Vol. 2(5), ISSN: 0975-9646, 2011.
[6] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.

[7] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, (2009).
[8] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.
[9] M. A. Al-Husainy, "Image Steganography by Mapping Pixels to Letters", Journal of Computer Science, vol.5, no. 1, (2009), pp. 33-38.
[10] A. M. Hamid and M. L. M. Kiah, "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis", International Journal of Engineering and Technology (IJET): 0975-4042, (2009).
[11] S. Ohyama, M. Niimi, K. Yamawaki and H. Noda, "Lossless data hiding using bit depth embedding for JPEG2000 compressed bit-stream", Journal of Communication and Computer, vol. 6, no. 2, (2009) February.
[12] Thomas Leontin Philjon and Venkateshvara Rao," Metamorphic Cryptography – A Paradox between Cryptography and Steganography Using Dynamic Encryption", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.
[13] Yizhong Song, Xin Peng," Spectra Analysis of Sampling and Reconstructing Continuous Signal Using Hamming Window Function", Fourth international Conference on Natural Computation, 2008.
[14] J. Murakami, Y. Tadakoro, "A New Toiplitz Approximation method for Linear Prediction Matrices", ISBN 0-7803-0946-4, IEEE, 1993.
[15] Peter Kabal, Ravi Prakash Ramchandran, "The Computation of Line Spectral Frequencies Using Chebyshev Polynomials", IEEE Transactions on Acoustics, Speech and Signal Processing, Vol. ASSP – 34, No. 6, December 1986.