Novel information security model using proposed e-cipher method with combining the features of cryptic-steganography

Prof. Venkateswaran Radhakrishnan, Dr. Sundaram Venkatachalam[2]

[1] Asst. Professor, GR Govindarajulu School of Applied Computer Technology and Research Scholar – Ph.D , Karpagam University, Coimbatore, Tamilnadu, India.

[2] Director , Department of CA , Karpagam College of Engineering Coimbatore, Tamilnadu, India.

Abstract

Cryptography is the art of hiding information in ways as to prevent detection of hidden messages. Secure data transmission method, which tries to alter the originality of the data files in to some encrypted form by using different methods and techniques. Encryption of data plays a vital role in the real time environment to keep the data out of reach of unauthorized people. After encryption, the files can be transferred securely by using multiple cytological methods.

In this Paper embed and de-embed processes of information hiding in various file format and carried out analysis in different approach and procedures are implemented in developing novel information security system in multimedia files like image and video, video file and other methods.

Varieties of techniques for embedding information in digital audio /video have been established. In this paper we will attend the general principles and different methodology adopted based on e -cipher model for hiding secret information using cryptographic technology, and an overview of functions and techniques, the goal of this paper is to know the different areas of information hiding and tools for providing secure data transmission with proposed e-cipher algorithms.

Keywords: Encryption; Decryption; data hiding; Mono Substitution; Poly Substitution; genetic keys.

1.Introduction

Information hiding technique is a new kind of secret communication technology. The majority of today's information hiding systems uses multimedia objects like image, audio and video files. Embedding secret messages in different file format is usually a more difficult process. Varieties of techniques for embedding information in digital image, audio /video have been established. In this proposed paper we will provide technique, which gives us more secure in information hiding system using cryptographic methods.

The importance of information and communications systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored on those systems. At the same time those systems and data are also increasingly vulnerable to a variety of threats, such as unauthorized access and use, misappropriation, alteration, and destruction. Proliferation of computers increased computing power, interconnectivity, decentralization, growth of networks and the number of users, as well as the convergence of information and communications technologies, while enhancing the utility of these systems, also increase system vulnerability.

Security of information and communications systems involves the protection of the availability, confidentiality and integrity of those systems and the data that is transmitted and stored on them. Availability is the property that data, information, and information and communications systems are accessible and useable on a timely basis in the required manner. Confidentiality is the property that data or information is not made available or disclosed to unauthorized persons, entities and processes. Integrity is the property that data or information has not been modified or altered in an unauthorized manner. The relative priority and significance of availability, confidentiality and integrity vary according to the information or communication systems and the ways in which those systems are used. The quality of security for information and communication systems and the data that

is stored and transmitted on them depends not only on the technical measures, including the use of both hardware and software tools, but also on good managerial, organizational and operational procedures.

Cryptography is an important component of secure information and communications systems and a variety of applications have been developed that incorporate cryptographic methods to provide data security. Cryptography is an effective tool for ensuring both the confidentiality and integrity of data.

2.Background study of this research work

1. Basic concepts of cryptography, cryptology, cryptosystem and fundementatal concepts of caeser cipher, features and break analysis and various related cipher like mono, homo and PolyGram and other substitution ciphers.

2. Detailed study about transposition, substitution, transformation and other related Encryption types symmetric and asymmetric algorithms and related key concepts.

3. Gathered information about different ciphers like block cipher and stream cipher methodology related issues, challenges and other features and draw backs of this system.

4. Various attacking methods especially for cipher text, concentrated on cryptanalysis and brute force attack.

5. Mathematical concepts of substitutions, permutation, modulus functions, factorization concept and related issues.

6. Study about Block size, Key size, Number of rounds, Sub key generation algorithm, Round functions, Fast software encryption or decryption Braking analysis

7. Differentiate various attacking methods for cipher text in the form Cipher text, Known plaintext, Chosen plaintext, Chosen cipher text, Chosen text and analysis of various essential ingredients of symmetric system, secret key, cipher text, encryption and decryption and algorithm development.

8. Various key concepts private keys, public keys, session keys, master keys and proposed genetic keys.
9. Study about symmetric and asymmetric algorithms like, DES, AES and other related concepts, it was analyzed in various ways performance, time taken analysis, processing power and other issues based on cryptography aspects.

10. Done base work based on the different analysis of various substitution ciphers, exiting algorithms, related issues of attacking cipher text, features and international journals published recently on the web and other related articles and books.

3. Data hiding and retrieval process in multimedia file.

The vast improvement of the Internet and the digital information revolution caused major changes in the overall environment in the world. Flexible and simple-to-use software and decreasing prices of digital devices have made it feasible for consumers from all over the world to create, edit and exchange multimedia data. Broadband Internet connections almost an errorless transmission of data helps people to distribute large multimedia files and makes identical digital copies of them. In modern communication system Data Hiding is most essential for Network Security issue. Sending sensitive messages and files over the Internet are transmitted in an unsecured form but everyone has got something to keep in secret. Multimedia based data hiding method is one of the most effective ways to protect your privacy.

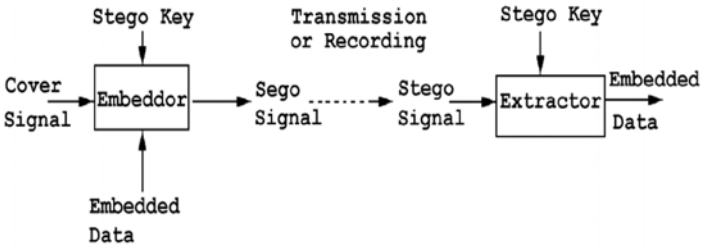

Fig1: Block Diagram of Data hiding and Retrieval

4. Objectives of this research work

· ***Authentication:*** This means that before sending and receiving data using the system, the receiver and sender identity should be verified.
· ***Secrecy or Confidentiality:*** Usually this function (feature) is how most people identify a secure system. It means that only the authenticated people are able to interpret the message (date) content and no one else.
· ***Integrity:*** Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver).

The basic form of integrity is packet check sum in IPv4 packets.

· ***Non-Repudiation:*** This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

· ***Service Reliability and Availability:*** Such systems should provide a way to grant their users the quality of service they expect.

5. Analysis of various model with proposed EC method.

The various analyses have taken to find strengthens and weakness of the many systems available using substitutions cipher method, based on the background study in different approached, finally we have got the poly alphabetic genetic keys substitutions cipher method. This method is used as a base method for security and then the output of this algorithm is passed to multimedia file (audio and video files) for high security in network.

Table 1. Shows analysis on various substitutions cipher Model

Mono Substitution Cipher
Methodology used: Shift Characters by fixed amount
Demerits: Easy to break algorithm based on frequency analysis poor security.
Example: Caeser Cipher & Vernam Cipher
Poly Substitutions Cipher
Methodology used: More than one replacement applied
Demerits: Message and keys are long, easy to break based on frequency analysis
Example: Vignere Cipher and Beaufort Cipher
Transposition Cipher
Methodology used: Permutes the symbols of the message according to a preset pattern.
Demerits: Insecure algorithms
Example: Row and Column Transposition Cipher Model
PolyGram Substitution Ciphers
Methodology used: Arbitrary Substitution for group of characters
Demerits: Reparative analysis to decipher the cipher text.
Example: Hill cipher, Flay air Cipher model
Proposed Substitution Model
Methodology used: ASCII with multiple key substitutions method
Merits: Genetic key used, fast, high security, embedded with multimedia files

The various analyses have taken to find strengthens and weakness of the many systems available using substitutions cipher method, based on the background study in different approached, finally we have got the poly alphabetic genetic keys substitutions cipher method. This method is used as a base method for security and then the output of this algorithm is passed to multimedia file (audio and video files) for high security in network.

Poly-alphabetic substitution ciphers the plaintext letters are enciphered differently depending upon their placement in the text. As the name poly alphabetic suggests this is achieved by using several two, three keys and random keys combinations instead of just one, as is the case in most of the simpler crypto systems.

Using two keys, we take 2 keys e1, e2 and let the ASCII values of e1 be 1 and e2 be 2 and take the text, add ASCII values of e1 to first character and ASCII values of e2 to second character. Alternatively add the value of e1 and e2 to consecutive characters.

5.1 Goal of my research

- •Efficient to use.
- •Must be available for all users.
- •Fast.
- •Provides high security.
- •Improved version than Existing one.

6. Proposed information security system model

In polyalphabetic substitution ciphers the plaintext letters are enciphered differently depending upon their placement in the text. As the name polyalphabetic suggests this is achieved by using several two, three keys and random keys combinations instead of just one, as is the case in most of the simpler crypto systems.

6.1 About proposed Model

The majority of today's steganographic systems uses multimedia objects like image, audio and video etc as cover media because people often transmit digital pictures over email and other internet communication. Depending upon the nature of cover object, steganography can be divided into 5 types: Text steganography, Image steganography, Audio steganography, video steganography, and Protocol steganography. We hereby propose new novel information security system, which gives us high security system with features of cryptography tools and methods. There are various methods described in this paper about e-cipher model

which is base Model for multiple data hiding system in the following methodology

- Text Cryptography, Image cryptography, Audio cryptography, Video cryptography, Unicode cryptography

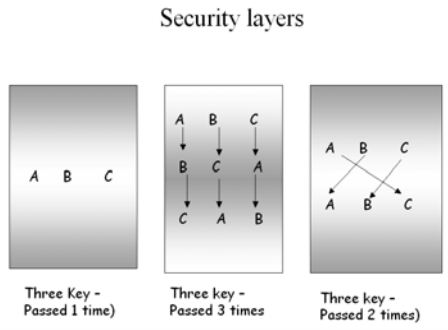

Fig. 2 Enhanced Security model using e-cipher model

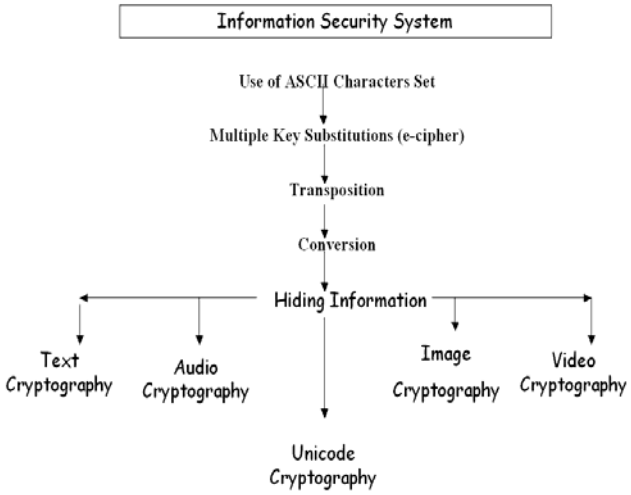

Fig. 3. Diagram shows difference security layers

6.2 Genetic keys

We can use Genetic keys (Three private keys) for text encryption by 2 keys and 3 keys and even more then 3 keys to make the decryption process more complicated.
•Using two keys, we take 2 keys e1, e2 and let the ASCII values of e1 be 1 and e2 be 2 and take the text, add ASCII values of e1 to first character and ASCII values of e2 to second character. Alternatively add the value of e1 and e2 to consecutive characters.

6.3 E-Cipher model

- Take the example text
- •Take three key e1, e2, e3 and assign a character e1 be 'a' and e2 be 'D' and e3 be 's'
- •Let ASCII value of e1 be 1 and e2 be 2 and e3 be 3 and take the text, add ASCII value of e1 to value of first character, and e2 to second character and e3 to third character, alternatively add the value of e1, e2, e3 to consecutive characters.
- •Three layers to be applied to each three consecutive letters and same to be continued thru the remaining text.
- •After adding ASCII value of all values of given text, the resultant text is an encrypted message. And it generate a combination of 3* (256 * 256 * 256) letters encrypted coded text with 128 bit manner.
- •Transposition takes place in each character after all the process are over that is moves or change one bit either LSB or MSB, the end result is increasing security
- •Finally takes the decimal values of each updated character in the given text and print in the encrypted format.

6. 4 Audio Steganography

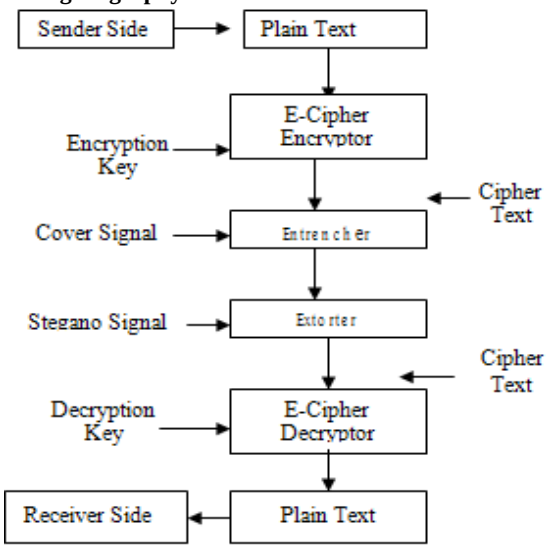

Fig 4. Audio steganography data flow model

In this work we propose a new model Information Security System – Information Hiding in Audio Signal - Embedding Text in Audio Signal that embeds the text with

encryption that gains the full advantages of cryptography. In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. For more security not only altering the bits of audio files, we embed high security e-Cipher cryptography algorithm in audio signal for data hiding.

6.4.1 Audio steganography base algorithm

Step 1: Load the audio file (AF) of size 12 K. Step 2: Input key for encryption

Step 3: Convert the audio files in the form of bytes and this byte values are represented in to bit patterns.

Step 4: Using the key, the original message is encrypted using E-Cipher algorithm.

Step 5: Bisect the audio file bit patterns horizontally.
•Step 6: Split the Encrypted message bit patterns vertically

Step 7: Insert the LSB bit of the vertically spitted encrypted text file (TF) into the LSB bit of the horizontally spitted audio file.

Step 8: Repeat Step 7 for the remaining bits of encrypted text file.
Step 9: If size (AF) ≥ size (TF) then
Embedding can be done as explained above
Else
The next higher order bit prior to previous bit position can be used
Until it is exhausted.

6.5 Image Steganography

In Image Steganography, There are a variety of methods using which information can be hidden in images. Least Significant Bit Replacement Technique: In image steganography almost all data hiding techniques try to alter insignificant information in the cover image. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. For instance, a simple scheme proposed, is to place the embedding data at the least significant bit (LSB) of each pixel in the cover image. The altered image is called steno-image. Altering LSB doesn't change the quality of image to human perception but this scheme is sensitive a variety of image processing attacks like compression, cropping etc. We will be emphasizing more on this technique using e-cipher with LSB processing model gives us high and enhanced security for data transmission over networks.

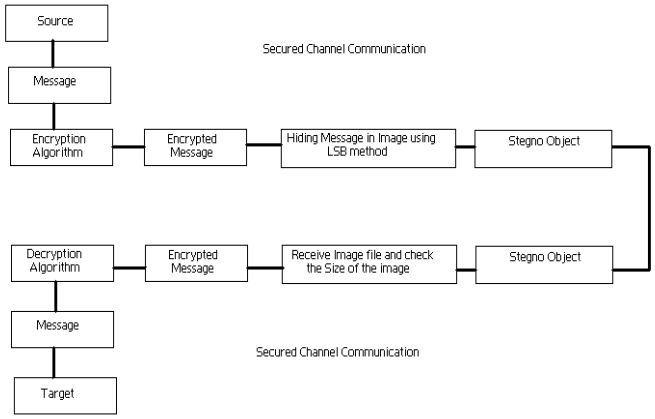

Fig 5. System Flow Diagram –Cryptic-steganography

6.5.1 Image Steganography base algorithm

1. Input encrypted file using EC algorithm.
2. Reading the text file and converting each char. To 8 bits in array (Conversion)
3. Reading the bmp file and adding each byte with the mask bits. (Watermarking)
4. Then adding to it 1 or not depending on the array. (Transposition)
5. Saving the result back to the bmp file.

7. Applications of the proposed work.

Audio/Video data hiding can be used anytime you want to hide data. There are many reasons to hide data but most important is to prevent unauthorized persons from becoming aware of the existence of a message. In the business world Audio data hiding can be used to hide a secret chemical formula or plans for a new invention. Audio data hiding can also be used in corporate world.

Audio/Video data hiding can also be used in the non-commercial sector to hide information that someone wants to keep private. Terrorists can also use Audio data hiding to keep their communications secret and to coordinate attacks. In the project which aims to embed animation parameters into audio and video contents. Data hiding in video and audio is of interest for the protection of copyrighted digital media, and to the government for information systems security and for covert communications.

It can also be used in forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds, and in the music business for the monitoring of the songs over broadcast radio.

This work is more suitable for automatic control of robotic systems used in military and defence applications that can listen to a radio signal and then act accordingly as per the instructions received. By embedding the secret password in the audio signal the robot can be activated only if the predefined password matches with the incoming password that reaches the robot through audio signal. It can then start functioning as per the instructions received in the form of audio signal. More such sort of applications can be explored but confined to audio medium usage.

8. References

[1] Dr D Mukhopadhyay, A Mukherjee, S Ghosh, S Biswas, P Chakarborty: An Approach for Message Hiding using Substitution Techniques and Audio Hiding in Steganography, IEEE 2005

[2] Pradeep Kumar Singh,R.S. Agarwal, "Enhancement of LSP based steganography for hiding data., IJCSE , 02, No. 05, 2010, Page No.1652-1658

[3] Maram Balajee, Unicode and color integration tool for encryption and decryption , IJCSE, Vol. 3 No. 3 Mar 2011

[4] Nalani N, G. Raghavendra Rao,' Cryptanalysis of Simplified Data Encryption Standard via Optimization, Heuristics;IJCSNS, Vol.6 No.1B, January 2006

[5] William Stallings," Cryptography and Network Security: Principles and Practice", 2/3e Prentice hall, 2010.

[6] V. Lokeswara reddy, Dr.A. Subramaniyam, Dr. P. Cheena reddy. Implementation of LSP Steganograpy and its evaluation of various file formats , Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05, Pages: 868-872 (2011)

[7] Sujith Ravi, Kevin Knight,'Attacking Letter Substitution Ciphers with Integer Programming',Oct 2009,33,4; Proquest Science Journals Pg.321.

[8] K.Geetha, P.V. Vanthia muthu," International journal of Computer Science and Engineering" vol 2 No.4 PG No: 1308-1312, Year 2010

[9] Darrell Whitley,'A Genetic Algorithm Tutorial', Computer Science Department, Colorado State University, Fort Collins, CO 80523.

7. Conclusions and future enhancement

This work proposes a new model for data transmission at higher degree of secrecy by using Image steganography, audio steganography, video steganography and proposed e- cipher methods and other technologies are presented here. This proposed study provides an efficient method for hiding the data from the eavesdropper. LSB data hiding technique is the simplest method for inserting data into audio signals.

And audio steganography model is able to ensure secrecy with less complexity at the cost of same memory space as that of encrypted text and the user is able to enjoy the benefits of cryptography and steganography combined together without any additional overhead. This work is more suitable for automatic control of robotic systems used in military and defense applications that can listen to a radio signal and then act accordingly as per the instructions received. By embedding the secret password in the audio signal the robot can be activated only if the predefined password matches with the incoming password that reaches the robot through audio signal.

It can then start functioning as per the instructions received in the form of audio signal. Some methods usage image steganography, which provide new way to hide the information in a secured way. Based on the perspective analysis, still we have to analyze more methods and add few updating in future and make the whole system which definitely provides a platform for the research engineers to help them for more innovation in this area and helps us to transfer our data more secure on the net.

10. BIOGRAPHY

Prof. R. Venkateswaran received his professional degree MCA and MBA (IS) from Bharathiar University, Tamilnadu, India, He received his M.Phil in computer science from Bharathidasan University, Tamilnadu, India, and He is currently a Ph.D Scholar in the Karpagam Academy of Higher Education, Karapagam University, Tamilnadu, India, in the field of Cryptography and Network Security. Presently he is working as an Asst. Professor of Computer Applications, GR Govindarajulu School of Applied Computer Technology, Coimbatore, Tamilnadu. He has 12 years of teaching experience and 3 years of research experience. He has participated in many national level conferences and workshops, published papers in five international conferences proceedings and published four papers in international refereed journals.

He is a member of CSI, IAENG, IACSIT, CSTA and many online forums. He has completed his course in Oracle 9i at Oracle University. His research interests are in cryptography and network security, information security, software engineering and database management systems.

Prof. Dr. V. Sundaram received his professional degree M.Sc. in Applied Mathematics from the University of Madras in the year 1967 and he received his Professional Doctoral Degree Ph. D in Mathematics from the University of Madras in 1989. He had 45 years of teaching as well as Research experience at PSG College of Technology and Polytechnic, Kumuraguru College of Technology and also worked in Ibra College of Technology, Sultanate of Oman. He is currently working as Director, Department of Computer Applications in Karpagam College of Engineering, Tamilnadu, India; He is a research Guide for Anna University as well as Karpagam University in the field of Computer Science and applications.

He has delivered guest lectures in the areas of computer applications and he had organized one international conference and six national level conference / symposium in the academics. He has attended and organized many faculty development programmes. He published several papers in International Journals and Conferences and also published 13 books in the area of engineering mathematics and he is the life member of ISTE and ISIAM. His research interests are in Cryptography and network security, Applied Mathematics, Discrete Mathematics, Network etc.