International Journal of Advanced Technology & Engineering Research (IJATER)
www.ijater.com

A FRAMEWORK FOR SECURE MESSAGE COMMUNICATION USING 3-TIER SECURITY SYSTEM

1Manoj Kumar Sharma, 2Vishal Shrivastav
1 Research Scholar, M.Tech Arya College Of Engineering and IT
2 Associate Professor, M.Tech, Arya College Of Engineering and IT
1manoj.sharma1010@gmail.com ,2vishal500371@yahoo.co.in

Abstract

The network security is becoming more important as the amount of data being exchanged on the Internet is increasing. Security requirements are necessary both at the final user level. There are a number of ways for securing data. Steganography play an important role for secure communication in network security. When we combine the property of steganography with cryptography, we can achieve more secure complex system. This paper work proposed a frame work for secure message communication, it uses multilevel security techniques for securing secret data as well as provision for user authentication and control eavesdropping. This paper also gives comparative study with current techniques.

1.INTRODUCTION

Network security measures are needed to protect data during their transmission. All business, government and academic organizations interconnect their data processing equipments with a collection of interconnected networks. Such a collection is often referred to as „internet" and the term „internet security" stems from the security of data flowing over such network [1].

1.1 APPLICATION

There are a number of applications driving interest in the aspect of information hiding:

- Military and intelligence agencies require unobtrusive communications. Even if the content is encrypted, the detection of a signal on a modern battlefield may lead rapidly to an attack on the signaler.
- Criminals also place great value on unobtrusive communications. Their preferred technologies include prepaid mobile phones, mobile phones that have been modified to change their identity frequently, and hacked corporate switchboards through which calls can be rerouted.
- Law enforcement and counter intelligence agencies are interested in understanding these technologies and their weaknesses, so as to detect and trace hidden messages.
- Recent attempts by some governments to limit online free speech and the civilian use of cryptography have spurred people concerned about liberties to develop techniques for anonymous communications on the net, including anonymous remailers and Web proxies.
- Schemes for digital elections and digital cash make use of anonymous communication techniques.
- Marketeers use email forgery techniques to send out huge numbers of unsolicited messages while avoiding responses from angry users. [4]

1.2 Limitations of the Existing Technology

1. Usually most of existing approaches for security are having utmost 2-tier security.
2. Steganography has been used and many Steganographic tools are existing but none of them fulfill the requirements of secure communication and also never Watermarking has been used with it for authentication. The few security challenges faced by modern steganographic tools are following:
    - Provision of authentication.
    - The amount of data to be hidden and sent.
    - Provision of secure channel.
    - The specification of the types of files to be used as cover file and message file.
3. Existing Encryption Algorithms are large, complex and time consuming.

1.3 Problem statement

Thus the main Problem Statement or objective of this paper work which can be summarized form the above discussion is to design a "Secure Message Communication System" which will provide 3-tier security.

1.4 Proposed Approach

This Paper aims to:

1. Design an algorithm for Encryption & Decryption which has better performance than existing algorithms.

2. Design tool for Steganography which gives less Noise and saves from attacks.

3. For ensuring 3-tier Security Authentication model may also be designed.

The proposed framework first establishes secure transmission system by sender entering his password or secret key and then either short text message or entire message file can be encrypted and then the result can be used to be stegnographed. The message file could be stego text file/ image file. At the receiver end same secret key or password is used to get the secret message received encrypted and steganographed.

2. Related Work

Steganography is used not only to digital images but also to other media such as voice, text, binary files and communication channels. Steganography can be used for variety of reasons. Legitimate use includes watermarking images for copyright protection. Digital watermarks are similar to steganography in that they appear to be part of the original object and is not easily detectable by the normal eye. Unfortunately steganography can also be used for illegitimate purposes. For example, if someone was trying to steal data, they could conceal it in files and send it out in an innocent looking email or file transfer[1] [3]. A comprehensive legal infrastructure needs to be established to enable copyright and ownership protection of digital content by watermarking techniques and to avoid legal attacks that diminish protection by watermarking. Steganography, the art of hiding information: The author feels that various applications of Steganography must be scrutinized in order to understand the future progression of this technology. In his paper he attempts to reveal new and current angles of Steganography. His paper tests the Steganography community's theory that, in general, the stego process diminishes contrast within a digital photo and proves it true. He tries to appreciate and measure the complexity and completely different methods with which to "attack" suspected or confirmed stego messages. [5] Steganography (Lewandowski, Palmisano): This paper discusses the history of Steganography and how it has grown since its humble beginnings. This paper also discusses what types of Steganography are in use today. Also, where and how they are being used.. One of the biggest uses today is with copyrighted materials like DVDs. Seeing how complex Steganography is today, it is hard to imagine what the future could hold. But with the way technology is growing exponentially, the bounds for Steganography seem limitless. One day, hiding a message inside someone's brain without the person even knowing it, may become a reality.[6] Information hiding, a survey (Petitcolas, Anderson and Kuhn): in this work they gave an overview of information hiding in general and Steganography in particular. They reviewed range of applications and tried to place the various techniques in historical context in order to elucidate the relationships between them, as many recently proposed systems have failed to learn from historical experience.

Then they discussed number of attacks on information hiding systems, which between them demolish most of the current contenders in the copyright marking business and have described a tool, "StirMark", which breaks many of them by adding sub-perceptual distortion; and they described a custom attack on echo hiding. They concluded that it is impractical to demand that any one marking scheme satisfy all the requirements simultaneously; of `the marking problem'. Both historical precedent and recent innovation provide us with a wide range of tools, which if applied intelligently should be sufficient to solve most of the problems that one meets in practice [7].

Image Steganography and Steganalysis (Chandramouli, Kharrazi, and Memon): The past few years have seen an increasing interest in using images as cover media for Steganographic communication. There have been many public domain tools, available for image based Steganography. Given this fact, detection of covert communications that utilize images has become an important issue. In this paper the authors reviewed some fundamental notions related to Steganography using image media, including security. They also described in detail a number of Steganalysis techniques that are representative of the different approaches that have been taken. [8]

Image Authentication Techniques (Madhurendra Kumar): In these modern eras, visual surveillance system finds application in almost all fields, ranging from commercial to defense. The video data acquired by VS system are forming vital evidence for several legal situations. So for such situations, the importance of authenticating their content is very high. Cryptography and watermarking based authenticating techniques are quite safe and efficient for this purpose and they are likely to remain for quite for some while.[9]

Merits of this approach are:

1. Robustness to high quality lossy image compression.
2. Automatic discrimination between malicious and innocuous manipulations.
3. Controllable visual deterioration of the VS sequence by varying the watermark embedding power.
4. Watermark embedding and detection can be performed in real time for digital data.

Demerits of this approach are:

1. Frame independent watermark can be easily found by comparative analysis of all image sequence frames and then could be easily added again to fake frames.

2. The detector should know the frame number in order to perform authenticity check

2.1 Motivations

By analyzing the above literatures and related works following conclusions have been drawn:

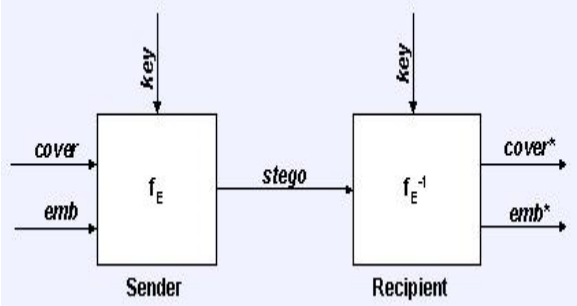

Fig.2.1. A Steganographic system

1. Steganography is a great art of covert communication but has to be used safely and proficiently.
2. For Secure Communication Steganography can also be supplemented with Cryptography.
3. Most of the existing Steganography models or tools have been designed very complex.
4. Secret key Steganography or in other words encrypted text Steganography is possible but as proposed till now has a greatest drawback of high complexity and large key length.
5. No authentication protocol has been given for the Steganographic tools. So Visible Watermarking with private key encryption can be used for authentication purpose.

These related works motivates to use image watermarking for authentication in the proposed Secure Message Communication System using 3-tier Security.

3. Proposed Approach of Secure Message Communication Using Three-Tier Security System

3.1 Proposed Technique

In the proposed framework for Secure Message Communication using Three- tier Security system, in this paper there are three levels of security, for the secret message (text) file are being designed. These methods or security levels either existed in previous work but were quite weak in terms of security or were not existing at all in similar way.

1. Authentication: This layer of security did not exist in the earlier models of Steganography and here a new method for authentication is proposed. In this approach private key Cryptography is used with visible watermark over the covert image so that the recipient of the message can be verified along with the secret message received.
2. Cryptography: In this layer of security another level of security is introduced, even though this layer of security has been existent in previously proposed algorithms too but the basic drawback with them was high complexity and huge key length. Instead of that in this proposed method Vigenere Cipher model has been modified with ECB model algorithm which is quite a simple yet strong algorithm.
3. Steganography: This is another layer of security, which will have two more layers inside which are Authentication & Cryptography to increase the security of the text message.

The proposed model works for a simple text file (Secret Message file) which is encrypted using proposed symmetric-key cryptographic algorithm first, and then embedded inside a simple bitmap or a PNG image (Cover file) file using LSB technique generating a Covert image file. Then the Covert image is encoded with a visible watermark which is created with the sender A's signature which is encrypted with A's private key using RSA Algorithm and then embedded into the covert image for authentication &finally, it can be used for communication.

3.1.1 Secure Message Generation and Transmission Process

Step-1: User A encrypts the secret text file by entering the password for encryption and perform Symmetric-key encryption using the proposed encryption algorithm.
Step-2: Hide the encrypted file from previous step in the cover file(image) using LSB steganography.
Step-3: Use private key of A for encrypting A's signature (here email id is used as signature) using RSA algorithm.
Step-4: The steganographic image file carrying text from step-2 is now watermarked by encrypted signature from step-3 for authentication
Step-5: The final steganographed and watermarked image carrying embedded text is then transmitted to the designated recipient using communication channel.

3.1.2 Secure Message Extraction and Receiving Process

Step-1: User B at the receiving end, receives the covert image with A's signature watermark through the communication channel.
Step-2: The watermark message is decrypted using A's public key for authentication of the received message.

Step-3: The steganalysis of the covert image (steganographic image file carrying the secret text) is done to get the encrypted secret message file separated from the cover file.
Step-4: The encrypted text file from step-3 is decrypted using the proposed symmetric key algorithm.
Step-5: After decryption the secret text file will be recovered and received by the designated receiver.
This proposed framework not only hides the message but also hides the pattern of message storage and at the same time demands authentication.

3.2 Algorithms for Secure Communication using Proposed Three- tier Security System

3.2.1 Model for Authentication

User A uses his specific signature, which is encrypted using RSA algorithm which uses the private key of user A. This encrypted message is converted to the respective ASCII code and which in turn finally embedded as a visible watermarking into the Steganographed image.The receiver B on the other hand detects the encrypted watermark from the watermarked steganographed image. This file yields two parts –one is encrypted steganographed image file and other one is encrypted watermarked message. Here now the ASCII code of the message is converted back to the respective character code by applying RSA algorithm on the message with the public key of the user A. This decryption leads to the production of the respective sender's signature which will be similar to the sender's email-id of course. Hence the authentication is done.

3.2.2 Algorithms for Cryptography

In this Model an Algorithm named Symmetric key cryptographic Algorithm is designed by Modifying the existing Vigenere Cipher Model & ECB Coding Model.

3.2.2.1 Vigenere Cipher Model of Encryption and Decryption

The Vigenère cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution.

Description

To encrypt, a table of alphabets can be used, termed a tabula recta, Vigenère square, or Vigenère table. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig 3.1 The Vigenère square or Vigenère table, also known as the *tabula recta*, it can be used for encryption and decryption [10].

For example, suppose that the plaintext to be encrypted is[10]:

ATTACKATDAWN

The person sending the message chooses a keyword and repeats it until it matches the length of the plaintext, for example, the keyword "LEMON":

LEMONLEMONLE

The first letter of the plaintext, A, is enciphered using the alphabet in row L, which is the first letter of the key. This is done by looking at the letter in row L and column A of the Vigenère square, namely L. Similarly, for the second letter of the plaintext, the second letter of the key is used; the letter at row E and column T is X. The rest of the plaintext is enciphered in a similar fashion:

Plaintext: ATTACKATDAWN

Key: LEMONLEMONLE

Cipher text: LXFOPVEFRNHR

Decryption is performed by finding the position of the ciphertext letter in a row of the table, and then taking the label of the column in which it appears as the plaintext. For example, in row L, the ciphertext L appears in column A, which taken as the first plaintext letter. The second letter is decrypted by looking up X in row E of the table; it appears in column T, which is taken as the plaintext letter.

Vigenère can also be viewed algebraically. If the letters A–Z are taken to be the numbers 0–25, and addition is performed modulo 26, then Vigenère encryption can be written,

$$C_I = (P_I + K_I) \bmod 26$$
(Equation No. 3.1)

and decryption,

$$P_I = (C_I - K_I) \bmod 26$$
(Equation No. 3.2)

3.3.2.2 Proposed Modified Vigenere Cipher

In this work a modified Vigenere Cipher Model and ECB encoding model are combined, where instead of using a static key pattern (used in Original Vigenere Cipher model) a dynamic key pattern is used; which is done by shifting the key matrix n number of times for m rounds.In the proposed model the encryption work is performed by:

$C_I = (P_I + K_I) \bmod 256$
(Equation No. 3.3)
And decryption is performed
$P_I = (C_I - K_I) \bmod 256$
(Equation No. 3.4)

In this new model the plain text is modified into the cipher text by adding some value from the tabula recta (the key matrix) in each round and then the obtained value is added 32 X 32(1024) times with different key values. After every round of 1024 modification key pattern is changed by matrix shifting and again the same process is repeated.

3.3.3 Proposed Steganography Model

Least Significant Bit (LSB) substitution is well known and widely used method. Take for example a True-Color BMP image file format. A color of pixel is coded in 3 byte array of indices to RGB palette. If only LSB bit in each color element is changed, then the picture will seem still the same, but is not. It carries hidden information. A picture with size 120x100 pixels can hold approximately up to 4500B of hidden data, if this method is used [11].

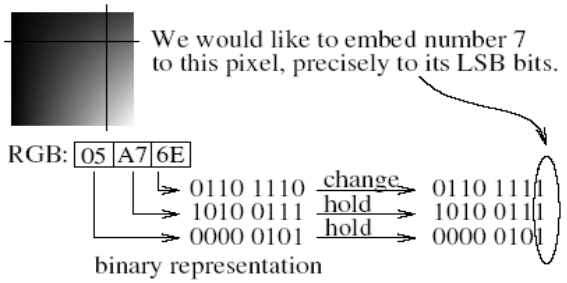

Fig 3.2 Image Encoding [11]

To secure out the algorithm at least a bit, some conventional pseudo-random number generator can be used. Supplied password will serve as initial seed. Generated numbers will specify which pixel to use for encoding next 3 bits of embedded data. The adversary, even with the complete knowledge of stegosystem, cannot extract the hidden message without the password. This system is secure in a sense of Keckhoffs' assumption, that everything is known except the password.

These changes have usually projection to specific statistical properties of common multimedia data. For few formats these properties have been already discovered, for many not yet. The main problem is that these tests are still quite fragile. They tend to fail, if only a small amount of hidden information is embedded or algorithm is modified. Moreover, recent research of Niles Provos [12] has shown how to balance statistical properties after the embedding process.

Next to multimedia format even the binary executables files without breaking their functionality can also be modified. Hydan programme by Rican El-Khalil [13] exploits redundancy in Intel x86 instruction set. Instruction addl $20, %eax can be altered to subl $-20, %eax and vice versa. Then let the add means logical 1, sub means logical 0 and a solid base for stegosystem has born. Possibilities how to add hidden information to existing data are almost endless. Even in a very secure operating system, programs can still communicate by measuring CPU load or memory usage, and so on.

4. CONCLUSIONS AND FUTURE SCOPE

4.1 Conclusion

Information security has been implemented in many different ways for secure communication over a period of time in which there are two basic types; encoding (Cryptography) and embedding (Steganography & Watermarking). The goal of information hiding is to secure the message while being transmitted or being stored so that the integrity and authenticity of the message is retained.

This paper gives idea about a Symmetric Key Algorithm for creating a Symmetric Key Steganographic model by designing a new Symmetric Key Cryptography Algorithm. This algorithm can use ECB encoding techniques for a Caesar Cipher like model called Vigenere Cipher.

Symmetric key Steganography has been in use for last few years but the basic drawback of it was the transaction of keys every time a message is communicated across the users, this makes the system quite insecure and thus the level of security though it is 2-tier is not that reliable. In this work a 3-tier security system has been proposed which is used for Steganography and at the same time uses the symmetric key

algorithm for the encryption of the message before the message is being embedded into the cover file (image) using LSB technique. For this a static key is provided in the tool which is known to the authenticated users only.

This paper also highlights another drawback of the existing Steganographic algorithms that none of them verifies the sender and the receiver or more precisely known as Authentication of the message and the cover file. In this paper algorithms have been defined for Encryption, Steganography & Watermarking is used for Authentication.

The proposed approach has been designed, executed and tested in the form of a software tool. The proposed 3-tier security system seems more secure and is more reliable.

4.2 Future Scope

In proposed Symmetric Key Cryptographic Algorithm, the complexity of the same can further be extended by using CBC encoding technique and increasing the number of rounds and improving the complexity of the key.

In the proposed model for Steganography in future the above defined password authentication system can be made more user friendly and dynamic, using database or key chain tokens. The dynamic password generator algorithms can be implemented in the same tool. This will ascertain the integrity of the message and the cover file and also allow the proper and safe use of Steganographic tools.

The proposed model can further be extended for different types of the cover files as this designed tool only works on BMP & PNG image files. It also leaves a scope for different types of techniques of Steganography to be implemented.

5 REFERENCES

1. C. Kurak and J. McHugh, "A Cautionary Note On Image Downgrading," Proc Eighth Ann. Computer Security Applications Conf., pp.153-159, 1992.

2. William Stalli, Cryptography and Network Security Principles and Practices,4th edition,Prentice Hall, 2005.

3. Abbas Cheddad, Joan Condell, Kevin Curran, paul Mc Kevitt, "Digital image steganography:Survey and analysis of current methods", Signal Processing 90(3) pp.727-752, 2010.

4. F. A. P. Petitcolas, R. J. Anderson & M. G. Kuhn, "Information Hiding – A Survey", IEEE Journal of special issue on protection of multimedia content, 87(7), pp. 1062-1078, July 1999.

5.Alain C. Brainos II on "A Study of Steganography and the Art of Hiding Information", East Carolina University. Page No. 104-115

6.Dean Lewandowski, Mike Palmisano on "Steganography"

7.Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn on "Information Hiding A Survey" special issue on protection of multimedia content, 87(7): Page No.1062-1078, July 1999.

8.Rajarathnam Chandramouli, Mehdi Kharrazi, and Nasir Memon on "Image Steganography and Steganalysis: Concepts and Practice" Springer-Verlag Berlin Heidelberg 2004 Page No. 204-211.

9.Madhurendra Kumar on "Image Authentication Techniques", August 2008 Page No. 10-13

10.http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

11. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, on "Steganography and Digital Watermarking", University of Birmingham GNU Free Documentation License, Version 1.2 Page No. 1-23

12.Niels Provos. Defending against statistical steganalysis. 2001.

13.Rakan El-Khalil and Angelos D. Keromytis. Hydan: Hiding information in program binaries.Technical report, Department of Computer Science, Columbia University, 2004.