ISSN No. 0976-5697

Volume 5, No. 4, April 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Dual Stegnography Scheme for Secure Data Communication using Finite State Machine

S. Srilakshmi
Department of Mathematics,
J.N.T.U. (A) College of Engineering Anantapuramu, A.P. India
sirivaram.srilakshmi@gmail.com

Abstract: Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. It combines the Greek words *steganos* (στεγανός), meaning "covered or protected", and *graphei* (γραφή) meaning "writing". The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Automata theory is the study of abstract computing devices or machines. In computer science we find many examples of finite state system and the theory of finite state systems, as a useful design tool for these systems. In the present paper an innovative technique for encrypting and hiding the data is proposed based on finite state machines. The efficacy of the proposed method is analyzed, and the analysis shows an improved cryptographic protection in digital signals.

Keywords: Moore Machines, Key, Encryption, Cipher Text, Steganography

I. INTRODUCTION

Today in the e-age, the need to protect communications from prying eyes is greater than ever before. Cryptography, the science of encryption plays a central role in mobile phone communication, e-commerce, pay-T.V., sending private e-mails, transmitting financial information and touches on many aspects of daily lives. Today's technology can be traced back to earliest ciphers, and have grown as a result of evolution. The initial ciphers were cracked, so new, stronger ciphers emerged. Code breakers set to work on these and eventually found flaws, forcing cryptographers to invent better ciphers. The significance of key is an enduring principle of cryptography. With the advent of the computer age, the mechanical encryption techniques were replaced with computer ciphers. Again each cipher depended on choosing a key known only by the sender and the receiver which defined how a particular message would be. This meant that there was a problem of getting the key to the receivers so that the message could be deciphered. This had to be done in advance, which was an expensive slow and risky process.

The art and science of hiding information by embedding messages within other , seemingly harmless messages is call steganography and works by replacing bits of useless or unused data in regular computer files such as graphics , sound , text, html or even floppy disks with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. Steganography is used when encryption is not permitted, or more commonly steganography is used to supplement encryption. An encrypted file may still hide information using steganography so even if the encrypted file is deciphered, the hidden message is not seen.

Automata theory is a key to software for verifying systems of all types that have a finite number of distinct states, such as communication protocols or protocol for secure exchange of information. In Moore Machine every of finite state machine has a fixed output. [1][2][4]

Mathematically Moore machine is a six- tuple machine and is defined as

M= ($Q, \sum, \Delta, \delta, \lambda', q_0$)

Q : A nonempty finite set of state in Moore machine

$\sum$: A nonempty finite set of inputs.

Δ : A nonempty finite set of outputs.

δ : It is a transition function which takes two arguments one is input state and another is input symbol. The output of this function is a single state.

λ' : Is a mapping function which maps Q x $\sum$ to Δ, giving the output associated with each transition.

q_0 : is the initial state of Q

Moore machine can also be represented by transition table, as well as transition diagram.

Example

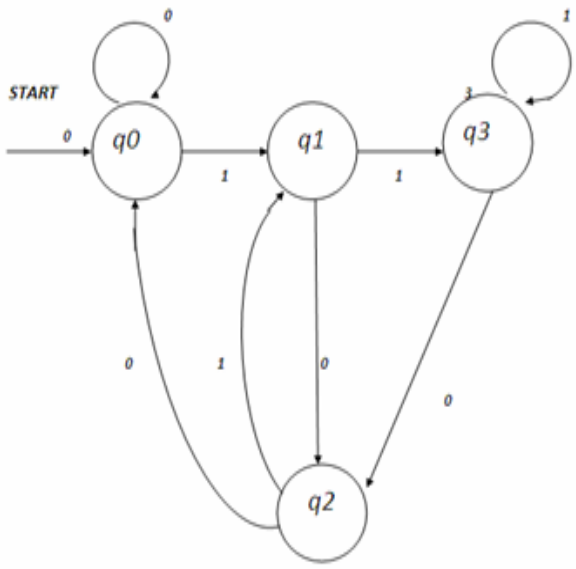

Figure 1 Moore machines which calculates residue mod 4.

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

II. RELATED WORKS

There are many papers proposed in finite state machine with most of the papers on cryptography. The author is mainly concerned with the security of the message. To achieve high robustness and capacity of our steganalysis various methodologies have been implemented and verified their approach.

In [5] Robert Krenn proposed good work on stegnography and stegnanalysis and in [6] Bert Dunbar proposed the inforamtion security reading room .

In [7] author proposed a stegnography schem using finite state machine using simple operations.

III. DEVELOPMENT OF SECRET KEY, MEDIA, ENCRYPTION SCHEME AND STEGNO FUNCTION

We know that, for a given finite state machine the secret key is given in only binary numbers, so the secret key is in binary numbers only. Media in this paper is considered as a square matrix of order 'n' encryption scheme may be any symmetric key cipher and stegano function is any ordinary mathematical function which defines the position of the data in the considered square matrix of order 'n'.

IV. ALGORITHM

A. Matrix formation:

Step 1

Let P be the plain text.

Step 2

Define Moor machine through public channel. Send secret key to the receiver in binary form and also steganofunction, encryption scheme for the position and encryption of the data in the given matrix.

Step 3

Define cipher text at $q(i+1)^{th}$ state.

Cipher text at $q(i+1)^{th}$ state is equal to the cipher text at $q(i)^{th}$ state * the out put of the q(i+1) th state .

Step 5

Send the cipher text to the receiver.

On receiving the finite state machine, the secret key in the binary digits and the steganofunction; it is very easy to locate the message and decrypting the text to plain text.

V. PERFORMANCE OF THE PRPOSED ALGORITHM

A. Mathematical work:

Algorithm proposed is based on ordinary multiplication using secret key, matrix selected for the operation and chosen finite state machine. The secrecy is maintained in steganofunction and in encryption scheme. Number of rounds depends on the secret key. It is very difficult to identify or delete the data in modified form.

B. Limitations of the algorithm:

The number of data selected must be finite otherwise the possibility of attacks are high, and also the matrix order must be very large

C. Rounds:

Number of rounds depends on secret key used and the chosen finite state machine. It is very difficult to guess the number of rounds and the matrix without an apt secret key.

D. Time calculation :

Let'ta' be the time taken to calculate one multiplication operation with the given matrix of order 'n'. Then the for a'k' bit secret key it is 'ta k (sum of the output of the finite state machine)' and for encrypting the message it depends on the encryption algorithm proposed.

E. Security:

The properties of electronic media are being changed after hiding any object into that. This can result in the form of degradation of quality or unusual characteristics of the media. Stenographic attacks consist of detecting, extracting and destroying hidden object of the stegano media. Steganography attack is followed by steganalysis.

It is very difficult to extract the original information, due secret key, matrix of order n and the stegano function ,encryption scheme and the finite state machine. Brute force attack on key is also difficult due to the increase in key size.

Table 1 Security analysis

S.No	Name of the attack	Possibility of the attack	Remarks
1	Known carrier attack	Very difficult	Due to the secret key and finite state machine.
2	Known steganographic	Difficult	Due to the chosen finite state machine.
3	Steganographiconly attack	Difficult	Due to the chosen finite state machine.
4	Known message only attack	Difficult	Due to the chosen finite state machine.

VI. APPLICATION

The p Let P=[1 4]

Stegno function = hide the information any specified position for example (1,1) and (2,2) or any predefined function.

Enctyption function for example add a secret value 10 to the message

Matrix θ = $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

Let secret key be 21(10101)

Then stegno text will be $\begin{bmatrix} 74 & 4b \\ 4c & 86 \end{bmatrix}$

As follows

Table 2 Application

S.No	input	previous state	Present state	out put	cipher text
1	1	q0	q1	1	$\begin{bmatrix} 11 & b \\ c & 14 \end{bmatrix}$
2	0	q1	q2	2	$\begin{bmatrix} 32 & 2b \\ 2c & 38 \end{bmatrix}$
3	1	q2	q1	1	$\begin{bmatrix} 32 & 2b \\ 2c & 38 \end{bmatrix}$
4	0	q1	q2	2	$\begin{bmatrix} 74 & 4b \\ 4c & 86 \end{bmatrix}$
5	1	q2	q1	1	$\begin{bmatrix} 74 & 4b \\ 4c & 86 \end{bmatrix}$

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

VII. CONCLUSIONS

Algorithm proposed, is based on finite state machine and the secret key, steganofunction encryption scheme and matrix chosen of higher order. Secrecy is maintained at four levels, the secret key, the chosen finite state machine, encryption scheme and the matrix of higher order. The obtained cipher text in the matrix becomes quite difficult to break or to extract the original information even if the algorithm is known.

VIII.REFERENCES

[1]. B.Krishna Gandhi ,.A.ChandraSekhar, S.Srilakshmi "Cryptographic scheme for digital signals using finite state machine" international journal of computer applications (September 2011)

[2]. AdeshK.Pandey. Reprint 2009, "An introduction to automata theory and formal languages 'S.K.Kararia& sons. New Delhi.

[3]. A.Menezed, P.VanOorschot and S.Vanstone Hand book of Applied Cryptography e-Book.

[4]. John E.Hopcroft, Rajeev Motwain, Jeffrey D.Ulman. "Introduction to automata theory, language, and computation" Vanstone3rd imp.

[5]. Stegnography and steganalysis – Robert krenn,internet publication, march 2004. http://www.krenn.nl/univ/cry/steg/article.pdf

[6]. Stegnographic Techniques and their use in an open-systems environment –Bert Dunbar, the information security reading room, SANS institute 2002http://www.sans.org/reading-room/whitepapers/covert/677.php

[7]. Proceedings of International Congerence on Smart Systems ICSS2013 Paper entitled "Stegnography encryption scheme using finite state machines" by Dr.S.Srilakshmi page no 632-634

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014