Enhancing Data Security: Employing Finite State Machines in a Steganography Encryption Scheme

Mr. Manoj Kumar Vemula[1], I M V Krishna[2], B. Sowmya[3], Mrs. Mannepuli Srujana[4]

[1]Assistant Professor, Department Of Information Technology, Vallurupalli Nageswara Rao Vignana Jyothi Institute Of Engineering &Technology, Hyderabad,Telangana, India 500090
[2]Assistant Professor, P. V. P. Siddhartha Institute of Technology, Kanuru, Vijayawada 520007.
[3]Assistant professor, ECE department, J. B. Institute of Engineering and Technology, Hyderabad.
[4]Assistant Professor, Department of CSE, Malla Reddy Engineering College (Autonomous), Maisammaguda, Hyderabad, Telangana-500100

Email: [1]manojkumarv2251@gmail.com, [2] imvkrishna@gmail.com, [3] bsowmyak@gmail.com, [4]srujanamannepuli@gmail.com

Received 02/01/2024; **Accepted** 29/01/2024

Abstract:
Steganography is an intricate technique used for concealing confidential information within diverse types of media. Both Steganography and cryptography aim to protect data, with a key distinction lying in the processed output's appearance. Cryptography transforms the output into a scrambled format, rendering it challenging to decipher without the appropriate key. In contrast, Steganography ensures that the concealed data remains imperceptible, seamlessly blending into the cover medium without any observable changes. Within the domain of computer science, automata theory assumes a crucial role, exploring the study of abstract computing devices or machines. This field holds significance as it furnishes a theoretical framework for comprehending and modeling systems with finite states. Finite state systems are prevalent in computer science, and the theory of finite state systems emerges as a valuable design tool for crafting efficient and resilient systems. By applying concepts from automata theory, engineers and researchers can scrutinize, design, and implement intricate systems with finite states, thereby contributing to advancements in diverse computing applications.
In this paper, we present a pioneering technique for concealing data streams through the utilization of finite state machines. Furthermore, the paper systematically analyzes and evaluates the effectiveness of the proposed method

Keywords: Finite State Machines (Moore Machines), Encryption Key, Steganography, Recursive Matrix Algorithm.

1. INTRODUCTION

Steganography is the technique of concealing one piece of data within another, with the primary aim of discreetly hiding a confidential message within a cover medium to prevent detection by unauthorized parties [1-3]. In the contemporary landscape, modern Steganography takes advantage of opportunities to embed information into digital multimedia files. The crucial elements of Steganography encompass the secret message, cipher text, or any data type, the cover medium that conceals the information, and the stego function along with its inverse. Optionally, a stego key or password can be utilized for concealing and revealing the message. The stego function operates on the cover medium and the message, incorporating a stego key to produce a stego medium. Despite their functional disparities, Steganography and cryptography often collaborate, with the common practice of integrating Steganography alongside cryptography for enhanced security.

Automata theory assumes a significant role in the software domain, especially in verifying systems with a finite number of distinct states, such as communication protocols or those designed for the secure exchange of information. In the context of a Moore Machine, each state of the finite state machine corresponds to a fixed output [4-6].

Mathematically, a Moore machine is defined as a six-duple machine, encapsulating its fundamental components for precise modeling and analysis. so to mitigate the gape an efficient method is being proposed to enhance the security.

The present paper introduces an original methodology for concealing data streams, employing the principles of finite state machines. This inventive approach makes a noteworthy contribution to the field, providing a novel perspective on data hiding techniques.

Finite state machines, recognized for their adaptability in modeling and managing computational processes, form the foundational framework for the proposed method. The intricacies of the technique, encompassing its design and implementation, are thoroughly elucidated, offering a comprehensive understanding of its internal workings.

Furthermore, the effectiveness of this groundbreaking method undergoes a meticulous analysis. Through a series of thoughtfully designed experiments and evaluations, the paper aims to empirically validate the performance and resilience of the proposed technique.

The analytical process encompasses the assessment of various parameters, such as data hiding capacity, computational efficiency, and resistance against potential attacks. By rigorously scrutinizing the effectiveness of the method, the paper contributes not only to the theoretical underpinnings of data hiding but also provides practical insights with potential applications in real-world scenarios related to data security and confidentiality.

Overall, this paper serves as evidence of the ongoing evolution of techniques in information security, highlighting the potential of finite state machines in progress the field of data concealment. Moreover the detailed survey of stenography has been given by [7-11].

The remaining part of the paper is organized as follows in section 1 introduction and survey of the paper is being presented, the proposed approach and conclusion of the paper is being presented in section 2 and 3 respectively.

Proposed Approach

In a Moore machine, the system is defined by a nonempty finite set of states, denoted as Q. It also encompasses a nonempty finite set of inputs, represented as $\sum$, and a nonempty finite set of outputs designated as λ. The transition function, indicated as δ, is a crucial aspect of the machine's operation.

It takes two parameters, the current state and the input symbol, producing a single output state.

Concurrently, the mapping function λ' plays a key role in linking each transition within the machine. Specifically λ' maps the Cartesian product of the set of states (Q) and the set of inputs (∑) expressed as Q x ∑, to the set of outputs (λ).

This mapping provides the output associated with each transition. In totality, these components collectively define the foundational elements of a Moore machine, contributing to a thorough comprehension of its structure and operational dynamics. q_0 : is the initial state of *Q*.

A Moore machine can be effectively portrayed through practical visualizations like a transition table and a transition diagram, in addition to its mathematical definition and components. These graphical representations provide intuitive ways to understand the machine's behavior and transitions.

The transition table serves as a tabular representation of the machine's transitions, featuring rows for different states, columns for input symbols, and entries indicating the resulting output states. Each cell in the table holds crucial information about the machine's responses to various inputs in specific states, offering a systematic and organized overview of its functionality.

Conversely, a transition diagram, also referred to as a state diagram, visually depicts the Moore machine's states, transitions, and associated outputs. Utilizing circles to denote states and arrows to represent transitions between states, this graphical representation enhances clarity.

The labels on the arrows indicate the input symbols initiating the transitions, and additional details, such as output symbols, can be included for further understanding. Transition diagrams provide an intuitive visual narrative, facilitating the comprehension of the dynamics and behavior of the Moore machine.

Both the transition table and transition diagram act as complementary tools, providing distinct perspectives on the Moore machine and aiding in a comprehensive understanding of its operation, transitions, and output behaviors.

These visual representations are valuable in both educational settings and practical applications, supporting engineers, researchers, and students in the analysis and design of systems modeled using Moore machines

a. Example:

Let us consider the state diagram as represented in figure 1

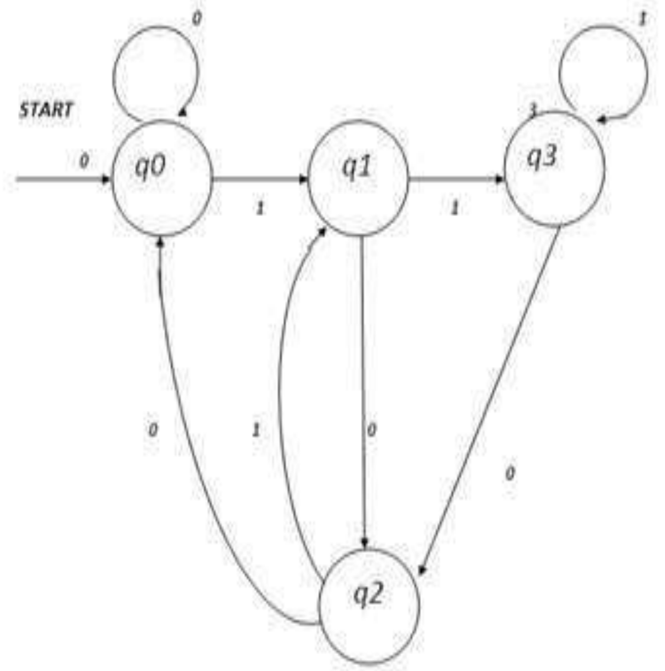

Figure 1: Moore machines which calculates residue

b. Creating A Secret Key, Media, and Stegno Function

In the realm of a finite state machine, it is crucial to acknowledge that the secret key is uniquely expressed in binary numbers. This implies that, specifically for a given finite state machine, the secret key is inherently binary, providing a standardized format for cryptographic operations within the system.

Within the context of this study, the term "media" denotes a square matrix of order 'n'. In the context of concealing and retrieving data, this matrix structure offers a systematic and well-organized framework for the manipulation of information.

The square matrix with an order of 'n' serves as a clearly defined medium for the application of various cryptographic techniques, the stegno function, integral to the processes of data concealment and extraction explored in this study, is characterized as a conventional mathematical function.

This function assumes a pivotal role in pinpointing the precise location of data within the aforementioned square matrix of order 'n'. By employing mathematical operations, the stegno function delineates the strategic placement of information, ensuring a secure and efficient process of data hiding and extraction within the designated media.

In summary, this comprehensive approach emphasizes the fundamental aspects of binary representation for secret keys, the structural significance of the media as a square matrix, and the critical role played by the stegno function in orchestrating the concealment and retrieval of data.

c. ALGORITHM

1 Step 1: Let P denote the plain text.

2 Establish a Moore machine through a public channel. Transmit the secret key confidentially to the receiver in binary form and provide the stegno function for determining the data position within the designated matrix.

3 Define the cipher text at the $(i+1)^{th}$ state
The cipher text at the $(i+1)^{th}$ state is calculated as the product of the cipher text at the i^{th} state and the output of the $(i+1)^{th}$ state.

4. Transmit the cipher text to the receiver.
Upon reception of the finite state machine, the secret key in binary digits, and the stegno function, the process of locating and decrypting the message to plain text becomes straightforward.

d. Enhancing the Effectiveness of the Proposed Algorithm through Thorough Mathematical Analysis.

The presented algorithm relies on standard multiplication techniques, incorporating a secret key, a designated matrix for operations, and a chosen finite state machine. The preservation of confidentiality is achieved through a stegno function.

The number of computation rounds is determined by the complexity of the secret key, ensuring a robust level of security. The modified form of the data introduces a challenging barrier for identification or deletion, contributing to the algorithm's resilience against unauthorized access or tampering.

e. Limitations of the Algorithm

The dataset must be finite to reduce the vulnerability to potential attacks, and a substantially large matrix order is essential for heightened security.

The number of computation rounds is intricately tied to the specific secret key and the chosen finite state machine. Accurately predicting the number of rounds and matrix characteristics without the proper secret key presents a significant challenge.

f. Time calculation

Let's denote 'ta' as the time required to perform a single multiplication operation using the given matrix of order 'n'. Subsequently, for a 'k'-bit secret key, the overall time can be expressed as 'ta * k', where 'k' is the sum of the outputs from the finite state machine.

This formulation encapsulates the computational complexity associated with the multiplication operation and the influence of the secret key size on the total time required for the process.

g. **Security**

The manipulation of electronic media to conceal objects within it can lead to alterations in the inherent properties of the media, resulting in quality degradation or the emergence of unusual characteristics. Stenographic attacks involve the processes of detecting, extracting, and potentially destroying the hidden object within the stego media.

Following this, steganalysis is applied to scrutinize and analyze the concealed information.

The task of extracting the original information from the manipulated media proves challenging due to the inclusion of a secret key, a matrix of order 'n', a stegno function, and a selected finite state machine.

The intricacy introduced by these components makes brute force attacks on the key particularly demanding, primarily because of the increased key size. This comprehensive combination of factors contributes to the security of the steganographic technique, rendering it resistant to unauthorized extraction attempts. Table 1 represents the security analysis.

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	Steganographic only Attack	Difficult	Due to the chosen finite state machine.
4	Known message only Attack	Difficult	Due to the chosen finite state machine.

h. **Applications**

Let p = [1 4]

Considering the stegno function, which specifies that the position of the data corresponds to the value of the data, and the matrix ‘θ’ is characterized as

$\theta = \begin{matrix} a & b \\ c & d \end{matrix}$

Let the secret key be 21(10101).

Then, the resulting cipher text is denoted by $\begin{matrix} 4 & 4b \\ 4c & 32 \end{matrix}$

Table 2 represents the example of the desired algorithm

Table 2: Example with respect to above data

S.No	input	previous state	Present state	out put	Cipher text
1	1	Q_0	Q_1	1	1 b c 4
2	0	Q_1	Q_2	2	2 2b 2c 8
3	1	Q_2	Q_1	1	3 2b 2c 8
4	0	Q_1	Q_2	2	4 4b

					4c 32
5	1	Q_2	Q_1	1	4 4b 4c 32

2. CONCLUSIONS

The proposed algorithm is built upon the integration of a finite state machine, a secret key, a stegno function, and a matrix of higher order. This architectural design ensures multi-layered secrecy, placing emphasis on the confidentiality of the secret key, the selected finite state machine, and the high-order matrix.

Such a strategic approach significantly elevates the overall security of the algorithm. Through the utilization of a matrix of higher order, intricately woven with the secret key and finite state machine, the algorithm generates a robust cipher text that poses substantial challenges for decryption.

The complexity introduced in extracting the original information from the resulting cipher text remains a formidable task, even when the algorithm is known.

The dynamic interplay of these elements not only reinforces the security of the algorithm but also contributes to its resilience against potential attacks. This renders the algorithm a dependable and effective method for safeguarding information across diverse applications.

3. REFERENCES

[1] . A.Menezed, P.Van Oorschot and S.Vanstone Hand book of Applied Cryptography e-Book. John E.Hopcroft, Rajeev Motwain, Jeffrey D.Ulman.

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

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

[4] . B.Krishna Gandhi ,.A.Chandra Sekhar, S.Srilakshmi “Cryptographic scheme for digital signals using finite state machine” international journal of computer applications (September 2011)

[5] . Adesh K.Pandey. Reprint 2009, “An introduction to automata theory and formal languages ‘S.K.Kararia & sons. New Delhi.

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

[7] . Mulla, Nilofar, Godse, Deepali, Aysha sayyed, Ishwari shelke, sonakshe shande,priti shinde, Bagyashri pawar (2023)“Review on Steganography and Cryptography” Ecosystem Services , vol 25(1), pp 281-288.

[8] . Krishna Chaitanya Nunna, Ramakalavathi Marapareddy, “Secure data transfer through internet using cryptography and image steganography”, 2020.

[9] . Sachin Dhawan, Rashmi Gupta, “Analysis of various data security techniques of steganography: A survey”, 2021.

[10] .Marc Chaumont, “Deep learning in steganography and steganalysis”, 2020.

[11] .Pratap Chandra Mandal, Imon Mukherjee, Goutam Paul, BN Chatterji, “Digital image steganography: A literature survey”, 2022.