Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 03 (2026)

Recital Assessment of Chaotic Encipherment Method

B. Shalini

Assistant Professor, Department of Computer Science and Business System,

Dhaanish Chennai College of Engineering, Chennai, Tamil Nadu, India

Abstract

The rapid expansion of multimedia communication led to a number of data transfer security problems. Furthermore, there is little data transmission security offered by the network utilized for digital communication. Tens of millions of individuals used the internet during this time for necessary communication and as a tool for business. Therefore, security is a crucial topic to address. Data confidentiality must be safeguarded, and secure connections must be made. As a result, we must acknowledge the various facets of security and their uses. Numerous of these applications cover anything from private chats to secure commerce, password or pin protection, and payment processing. As is well known, cryptography is becoming a crucial component of safe communication. The science of creating secret code using a reliable algorithm and key is known as cryptography. Digital signatures, hashed message authentication codes, and encryption and decryption algorithms are the fundamental elements of cryptography. We are aware that cryptography and encryption are synonymous. In this day and age, various forms of encryption are employed. The kind of encryption that has embraced the idea of chaos is called chaotic encryption. This paper examines the development of cryptography up till chaotic cryptography and evaluates the effectiveness of the chaotic encryption method. The evaluation is carried out in terms of battery power consumption, CPU utilization over time, and encryption speed. The efficiency of the algorithms is described in the experimental findings.

Keywords: Chaotic Encryption, Chaotic Video Encryption Scheme, Non-Linear Chaotic Algorithm, Escrowed Encryption Scheme, Scalable Encryption Algorithm

1. Introduction

Nowadays, people communicate with one other over the internet. However, we are worried about data confidentiality and communication network security. Therefore, every communication must be of a cryptographic character. The main component of security is cryptography. The Greek words "κryptos and graphing," which indicate hidden or secret, are the source of the word "cryptography." It is the study of security technologies and operates when other people are around. In a broader sense, cryptography is an age-old art and the science of privacy. It involves creating and evaluating protocols that subvert adversary authority and are connected to different facets of information security, including data integrity, nonrepudiation, secrecy, and authentication. The two main procedures in this cryptography are encryption and decryption. The process of transforming plain text into cipher text is called encryption. In this case, cipher text is an unidentifiable type of information, whereas plain text is the original form of the communication. Decryption is the standard term for the encryption's reverse procedure.

Prior to the contemporary era, cryptographic techniques were the only means of ensuring message confidentiality. the transfer of messages from a comprehensible format to an impenetrable one and the return of acknowledgement from the other end without pirate interpretation. Encryption is used to protect confidentiality in communications between military leaders, diplomats, and spies. In this day and age, encryption and cryptography are becoming synonymous. Encryption and decryption are mostly used for privacy. To provide this privacy on every communication across a network, encryption methods are supported.

Since most individuals could not read simple written communications, this was the first type of cryptography. Its

only concern was transforming communications into scrawled figures in order to safeguard them while they were being transmitted from one location to another. Because of the advancements in our way of life, cryptography became necessary. The earliest types of cryptography were developed at the cradle of civilization, which included the area that included Egypt, Greece, and Rome. Cryptography has been around for at least 4,000 years. The history of cryptography is categorized by the time period and available mechanisms. Classical, Medivieal, and Modern cryptography are the three categories. Classical cryptography spans from mechanical encryption to early B.C. 1600. The use of classical cryptographic techniques and encrypted communication during the World War are the primary topics of medieval cryptography. Symmetric key cryptography, public key cryptography, and chaotic cryptography are the three basic types of modern cryptography. This article assesses the effectiveness of particular chaotic encryption methods and provides a brief history of chaotic cryptography.

1.1. History of Chaotic Cryptography

The timeline begins in early 1950, when Shannon makes it obvious that the basic stretch and fold process of chaos makes it useful for cryptography. Up until the 1980s, chaos theory gained popularity among cryptographers and the importance of cryptography increased. The chaos theory was established in the 1980s by Shannon's use of chaos. The first cyphers based on chaos were proposed in 1990, and chaos synchronization also made an appearance. We found roughly thirty more publications about chaos. Baptista created the chaotic encryption in 1996 and 1998. In 2000, chaos began to gain widespread recognition and a secure communication application. It is chaotic cryptography's finest accomplishment. Here, we are focusing more on assessing the chaotic encryption method. The chaotic encryption method is comparable to other encryption methods. However, the activation is only carried out through turmoil. Let us talk about it in more depth.

2. RESOURCES AND TECHNIQUES

To provide further insight into the chosen chaotic encryption algorithm's performance assessment. A brief discussion of chaotic encryption will be covered in Section 2 (Kocarev et al., 1998). the analysis of the chosen algorithms in comparison. The data size, battery power usage, and encryption speed are used to make the comparison.

2.1. Chaotic Encryption

The boundary continuous space, a complex or real number space, is used to define chaotic systems. The general goal of chaos theory is to identify the repeated progression's asymptotic activities (Wei et al., 2006). According to Hermassi et al. (2010), the fundamental characteristics of chaotic systems intended for cryptography are sensitive to an initial condition with topology transitivity. (Baptista, 1998) suggests the chaotic encryption technique. Compared to more conventional encryption techniques, this one appears to be far superior. To encrypt the message, we must determine the mapping scheme for a trajectory. Next, determine the key's starting state and parameters. We take the present path (trajectory) as the initial condition. Store the number of iterations as a code for each message symbol after iterating the chaotic equation till the path arrives at the destination. Iterate the recent trajectory to encrypt the subsequent message. Create the subsequent cipher in accordance with it, and so forth.

The chaotic encryption's graphical map is shown in Fig. 1. It revealed that the encryption method used a chaotic sign generator. It aids in creating the stream of chaotic signals that are used as a key for encryption. To decode the message, set the initial state and parameters. For each decryption, use the same mapping format. Use the cipher to repeat the chaotic equation a certain amount of times. Determine which site the trajectory belonged to. Next, save the site's figure as a message symbol. decrypts the subsequent message by repeating the current path, generating the subsequent symbol, and so forth.

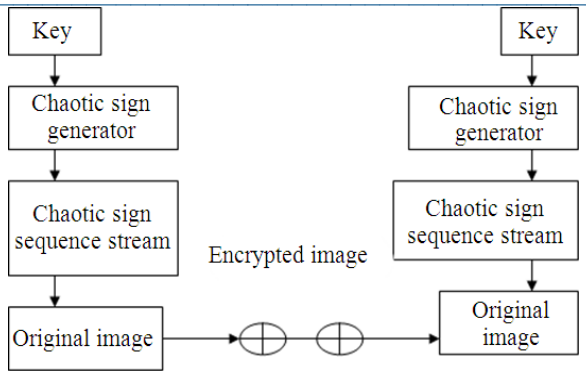

Fig. 1. Chaotic encryption scheme

The most straightforward way for encrypting video data or messages using a chaotic equation is the broad chaos encryption method. This approach can make it easier to find certain important information and determine the critical security stage. Chaotic encryption has the benefit of (1). high degree of security (2). Iteration is used to accomplish the encryption (3). easiest (4). There are no shortcuts. On the other hand, slow speed and the need for a lot of cipher storage are seen to be the main drawbacks. The characteristics of chaos are slightly altering cryptography as a whole. Its features include topological transitivity and sensitivity in the initial stage. Chaos is always sensitive in an initial state. As a result, the trajectory will change slightly. It provides a completely different trajectory sectional value. The same values can only be produced by an identical trajectory. According to the topology transitivity, every point in the state space is indefinitely secure and the state points are located in a bounded space state.

In this work we mainly focus on the recital assessment of the chaotic encipherment method. Security analysis can be used to determine each algorithm's performance in terms of power consumption, encryption speed, and data size.

2.2 Chaotic Video Encryption Scheme (CVEA)

All video encryption algorithms are independent of CVES. It can simply be implemented in both software and hardware. For real-time video encryption, it can offer increased security. CVES is a universal hashing encryption algorithm that can easily be extended to more real-time applications. Li et al. (2002) proposed this chaotic encryption. They suggested employing a cluster to create a plain-cluster in order to encrypt the plain video. The video stream data in the plain cluster has a set size. A collection of video data frames makes up the cluster.

The following is a description of the CVES process. The Control Chaotic Scheme (CCS) must first be started with two iterations. The pseudo-random initial conditions xe0 are then obtained by iterating this component 2n times. Iteration is used to generate the prime number and matching pseudo control parameters for encryption once again. The encrypted text is obtained using these parameters (Li et al., 2002). The encryption process is as follows: a stream sub cipher encrypts one plain cluster, which is then followed by a block sub cipher. The encryption procedure is reversed during decryption. The block sub-cipher first decrypts the encrypted plain cluster, and the stream sub-cipher then encrypts the pre-decrypted plain cluster.

L and n are the two most crucial CVES parameters. L states that 22L is the crucial space. If great security is required, the key space should be sufficiently large. N states how the realization complexity of CVES is related. It should not be big. The "n" is often "8."

2.2.1 Speed

By comparing the speeds of the stream and block sub ciphers, we may calculate the encryption speed. Hardware systems are typically faster than software. Therefore, the fastness of the medium is determined using both hardware and software realization.

2.2.2 Security

To guarantee the security performance, there are three key components. (a) Statistical cryptanalysis is more complicated; (b) Each S-box cluster has a completely separate pseudo-random code. It will produce the same one-time pad effect. (c) Known plaintext and chosen plaintext attacks are rendered impossible by the combinational product of block cipher and stream cipher.

2.3 Scalable Encryption Algorithm (SEA)

SEA is a low cast encryption method designed for small groupings of instruments. The text, key size, and processor are all parametric. It permits the encryption and decryption to be combined. Moreover the simplicity of the SEA method makes the implementation as easy forward (Mace et al., 2008). SEA uses a variety of text, key, and word sizes. It uses random rounds of a variable number and is based on the Feistel Theory. In general, it is defined in relation to the parameters that are connected to it. The parameters are: b, the processor or word size; n, the plain text and key sizes. The amount of words per Feistel branch is $n_b = n/2b$. The number of block cipher rounds is denoted by n_r. The multiple of 6b should be the parameter n. Typically, the SEA is built on a small number of fundamental processes. Bitwise XOR, substitutions-box, bit rotation r, and addition mod 2^b are the fundamental operations. The cipher will initially be iterated by the number of rounds in the method action. The plain text will be encrypted using the appropriate key K by the accessible pseudo code.

The SEA is a straightforward encryption scheme, as is well known. Any kind of processor can readily implement it. Compared to the traditional approach, SEA is less processor-sensitive due to its flexibility. The suggested pseudo assembly code for encryption or decryption with "on the fly" key scheduling (Mace et al., 2008).

2.3.1 Speed

The effective execution of the number of cycles needed for the encryption can increase its speed. The complexity of cryptanalysis is determined by the code size and the variable number of rounds. The implementation is less complex than the block cipher when the register of SEA and RAM words are combined.

2.3.2 Security

The components' characteristics will provide the structure with the highest level of security. Recursive definitions and the maximum number of nonlinear orders increase the decryption complexity. Non-linear estimations of outer rounds, multiple linear cryptanalysis, rectangles, and attacks are the traditional extensions of linear and differential cryptanalysis. Even so, these extensions usually only represent a slight improvement over the fundamental attacks. This method is susceptible to side attacks, square attacks, and related key attacks.

2.4 Nonlinear Chaotic Algorithm (NCA)

The NCA is a chaotic encryption technique that substitutes the tangent and power functions for linear functions. Experimental research is used to determine this structural parameter. It is intended to be a one-time password for image transmission. Alvarez and Li (2006) made the proposal. They suggested that it maintains experiment efficiency while offering more security and a large key space. There are two components to the analysis in NCA. (1) NCA map design and (2) logistic map analysis. The one-dimensional discrete chaotic map serves as the foundation for the cryptosystem on a logistic map. It might be referred to as a logistic map. Their security is really inadequate. NCA map design will restrict key space and time in order to prevent assaults on the plain text. This is accomplished simply adjusting the key appropriately. The video is encrypted using a chaotic sequence. Using distinct keys for each type of data, the NCA map encrypts the video data. Decimal functions make up the original chaos. There are integers in these chaotic sequences. The XOR method with the integers can then be used to encrypt the image (Alvarez and Li, 2006). The encryption and decryption processes are more comparable. However, in order to decrypt, it required an encryption key. The experimental study shows that the encrypted visuals are jagged, clumsy, and unknowable. The decryption process uses the same key. The decrypted pictures are consistently accurate, clear, and free of distortion. A different decryption can result from using the incorrect key. We can therefore draw the conclusion that the key employed in both procedures is extremely delicate. Data analysis reveals that encryption statically covered every character in plain text. It will display balanced performance in the 0–1 ratio. High security and zero correlation were the outcomes.

2.4.1 Speed

By examining the sensitivity of the key and chaotic sequence, the encryption speed can be increased.

2.4.2 Security

The algorithm is a one-time-only password. The uniform distribution property is satisfied by the NCA algorithm. Zero correlation and ideal non-linearity are features of the NCA algorithm. As a result, NCA encryption can effectively thwart both statistical and gray code attacks. It is also capable of withstanding brute force. In this approach, the selected or known plain text assault is ineffective.

2.5 Escrowed Encryption Standard (EES)

The US Department of Commerce authorized the Escrowed Encryption Standard (EES) in 1994. It is a standard for communication that is encrypted. The phrase "clipper chip" is always used to describe its implementation. The key escrowed approach that makes it possible to identify eavesdropping is a significant element of EES. The EES uses both the SKIPJACK and LEAF generation methods for encryption and decryption. It is a symmetric key encryption technique. The plaintext is encrypted using an 80-bit key in one of the following modes: FIPS81, CBC, or ECB.

3. RESULTS AND DISCUSSION

A laptop with an IV CPU running at 2.4GHz is used to gather performance data for the experimental analysis. The laptop encrypts files of all sizes, from 320k to 7.873 megabytes. It is roughly 135 MB for the text data. It spans from 4000kbytes to 5994 bytes for video data and from 30kbytes to 7822 bytes for audio data. The three performance metrics are (1) encryption time, (2) CPU utilization over time, and (3) battery power consumption.

3.1. Encryption Time

The amount of time the encryption algorithm takes to generate the cipher text is known as the encryption time. Calculating the encryption's throughput is helpful. It suggests determining the encryption's speed. The throughput is computed by dividing the total amount of plaintext encrypted in bytes by the total encryption time.

3.2. CPU Utilization

CPU processing time is referred to as CPU utilization. It is the amount of time the CPU spends on a specific process calculation. It shows the CPU load. A longer encryption time corresponds to a higher CPU demand.

3.3. Power Consumption

One metric is the CPU cycle. It is reflected in the amount of CPU power used during the encryption process. The CPU cycle measurement aids in determining the power usage of each process. A tiny amount of energy is used for encryption in each cycle. As far as we are aware, the encoding strategy in encryption is meaningless. Therefore, there is no need to research any comparative analysis based on encoding.

3.4. The Outcome of Changing Packet Size

Power Consumption of the Encryption Algorithm an encryption technique's throughput is determined by its encryption time. The total plain text in megabytes encrypted divided by the total encryption time for each algorithm yields the encryption technique's throughput. It shows how quickly the encryption method is working. As the throughput value climbed, the algorithm's power usage decreased.

The results of the analysis are displayed as follows in Table 1 and Fig. 2. Here, we take into account various data packet sizes with varying encryption times for each approach. Thus, the throughput of each encryption technique was determined.

The NCA method outperforms other algorithms in terms of processing time, as demonstrated by Table 1 and Fig. 2. Another thing to note is that, with the exception of NCA, CVEA takes less time than all algorithms. The third point is that EES performs poorly in terms of throughput and power consumption. Because

of its unique escrowed key technique and the existence of both LEAF and SKIPJACK creation methods, it takes longer to encrypt.

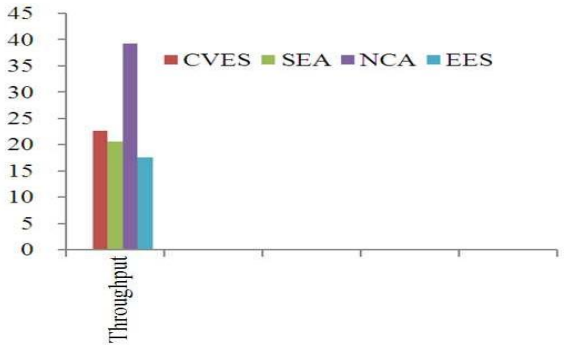

Fig. 2. Throughput of each encryption algorithm

Table 1. Comparison of different execution time (milliseconds) of various encryption schemes with different packet size

Input size	CVES	SEA	NCA	EES
49	56.0	35.0	49.00	57.00
100	90.0	81.0	77.00	91.00
247	112.0	77.0	45.00	121.00
694	210.0	144.0	123.00	242.00
963	203.0	283.0	125.00	295.00
3341.19	1277.0	1234.0	695.00	1554.00
5310.88	1366.0	1785.0	796.00	1914.00
Average time	473.4	519.8	272.08	610.05
Throughput	22.6	20.6	39.23	17.53

The NCA method outperforms other algorithms in terms of processing time, as demonstrated by Fig. 2 and Table 1. Another thing to note is that, with the exception of NCA, CVEA takes less time than all algorithms. The third point is that EES performs poorly in terms of throughput and power consumption. Because of its unique escrowed key technique and the existence of both LEAF and SKIPJACK creation methods, it takes longer to encrypt.

3.5 The Outcome of Changing File Types

Power Consumption Encryption Fig. 3 displays the results of the video data type analysis at encryption. The time spent on each algorithm during encryption is displayed in Fig. 3. According to the analysis, EES takes the longest to encrypt data.

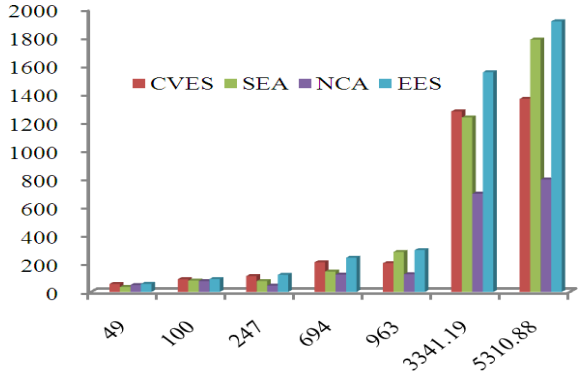

Fig. 3. Power and time consumption for encryption schemes

Table 2. Levels of security

Algorithm	Security
CVES	High
SEA	Medium
NCA	High
EES	Medium

NCA requires less time to be consumed. When comparing the NCA and CVES, there is not much of a difference. They are roughly equal. As a result, EES has a higher CPU load than other systems. Less CPU burden is provided by NCA's analytical mechanism.

3.6 Exploration on Level of Security on Each Algorithm

The degree of security offered by each chosen algorithm is shown in Table 2. It is represented as follows.

When compared to the other algorithms, CVES and NCA have the highest security, according to Table 2. The maximum level of security in CVES will be provided by the iterative control over the chaotic scheme. There are two different kinds of analysis in NCA before encryption. It will provide the secure nature with a solid foundation. Regarding the EES. SEA and EES are less secure than these two methods. However, the escrowed nature of keying in the EES offers improved transmission security.

CONCLUSION

With the quick development of multimedia communication, video encryption is becoming increasingly important. Privacy was necessary for the video transmission. Here, we are examining the performance effectiveness and security analysis of chaos-based encryption. For secure video transmission, chaos-based encryption offers a practical and quick option. It demonstrates that chaotic cryptography has the highest security and effectiveness to fend off attacks when compared to conventional cryptographic algorithms. According to the security analysis, this offers a high to medium level of security.

The performance is assessed in this study using a number of well-chosen algorithms. NCA, CVES, EES, and SEA are the chosen algorithms. Several conclusions are drawn from the experimental investigation. (1) We found that CVES and NCA are the best in terms of encryption speed and time. (2) Out of all the algorithms, NCA takes the least amount of time to encrypt, while EES takes longer. (3) When compared to the other two, the NCA and CVES offer superior security. When alternative encodings are used for encryption, there is no discernible difference.

REFERENCES

1. Baptista, M.S., 1998. Cryptography with chaos. Phys. Lett. A, 240: 50-54. DOI: 10.1016/S0375-9601(98)00086-3
2. Fridrich, J., 1998. Symmetric ciphers based on two dimensional chaotic maps. Int. J. Bifurcat. Chaos,8:1259-1284. DOI: 10.1142/S021812749800098X
3. Kocarev, L., G. Jakimoski, T. Stojanovski and U. Parlitz, 1998. From chaotic maps to encryption schemes. Proceedings of the IEEE International Symposium on Circuits and Systems, IEEE Xplore Press, Monterey, CA., pp: 514-517. DOI: 10.1109/ISCAS.1998.698968
4. Li, S., X. Zheng, X. Mou and Y. Cai, 2002. Chaotic encryption scheme for real-time digital video. Proc. SPIE, 4666: 149-160.
5. Buchmann, J., 2004. Introduction to Cryptography. 2nd Edn., Springer, New York, ISBN-10: 0387207562, pp: 335.
6. Wei, J., X. Liao, K.W. Wong and T. Xiang, 2006. A new chaotic cryptosystem. Chaos Solitons Fractals, 30: 1143-1152. DOI: 10.1016/j.chaos.2005.09.005

7. Addison, S.R. and J.E. Gray, 2006. Chaos and encryption: Problems and potential. Proceedings of the IEEE 38th South eastern Symposium on System Theory, Mar. 5-7, IEEE Xplore Press, Cookeville, TN., pp: 444-448. DOI: 10.1109/SSST.2006.1619122
8. Alvarez, G. and S. Li, 2006. Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos, 16: 2129-2151.
9. Wong, K.W. and C.H. Yuen, 2008. Performing compression and encryption simultaneously using chaotic map. City University of Hong Kong.
10. Mace, F., F.X. Standaert and J.J. Quisquarter, 2008. FPGA implementation(s) of a scalable encryption algorithm. IEEE Trans. Very Large Scale Integrat. Syst., 16: 212-216. DOI: 10.1109/TVLSI.2007.904139
11. Hermassi, H., R. Rhouma and S. Belghith, 2010. Joint compression and encryption using chaotically mutated Huffman trees. Commun. Nonlinear Sci. Nume. Simulat., 15: 2987-2999. DOI: 10.1016/j.cnsns.2009.11.022
12. Chen, J., J. Zhou and K.W. Wong, 2011. A modified chaos-based joint compression and encryption scheme. IEEE Trans. Circ. Syst.-II: Express Briefs, 58: 110-114. DOI: 10.1109/TCSII.2011.2106316
13. Singh, J.K. and R. Manimegalai, 2012. A survey on joint compression and encryption techniques for video data. J. Comput. Sci., 8: 731-736. DOI: 10.3844/jcssp.2012.731.736