American Journal of Applied Sciences, 10 (1): 35-41, 2013
ISSN: 1546-9239

doi:10.3844/ajassp.2013.35.41 Published Online 10 (1) 2013 (http://www.thescipub.com/ajas.toc)

Performance Evaluation of Chaotic Encryption Technique

[1]Ancy Mariam Babu and [2]K. John Singh

[1]School of Information Technology and Engineering,
VIT University, Vellore, Tamil Nadu, India
[2]School of Information Technology and Engineering,
VIT University, Vellore, Tamil Nadu, India

Received 2012-11-05, Revised 2013-01-18; Accepted 2013-02-12

ABSTRACT

Drastic growth in multimedia communication resulted to numerous security issues in the transmission of data. Moreover, the network used for the digital communication does not provide much security for the data transfer. During this time, tens of millions people using the internet options for essential communication and is being a tool for commercial field increased, So that security is an enormously important issue to deal with. We need to be protected confidentiality of data and provide secure connections for it. Hence we necessitate recognizing the different aspects of security and their applications. Many of these applications ranging from secure commerce, protecting passwords or pin and payments to private communications. As we know that, Cryptography is now becoming an essential aspect of the secure communication. Cryptography is the science of writing secret code with confident algorithm and key. The basic components of cryptography are encryption and decryption algorithms, digital signature and hashed message authentication code. We know that encryption is the synonym of cryptography. Different kinds of encryption are used in this modern era. Chaotic encryption is the type of the encryption which has adopted the concept of chaos. In this study, we are studying the history of cryptography until chaotic cryptography and analyzing the performance of chaotic encryption technique. The evaluation is performed in terms of encryption speed, the CPU utilization with time and the battery power consumption. The experimental results are specified the efficiency of the algorithms.

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

1. INTRODUCTION

In the modern era, the communication amid the user is through internet. Though, we are concerned about security issues over a communication network and confidentiality of data. Hence cryptographic nature is needed for every communication. Cryptography is the major aspect of security. The term cryptography is coming from Greek word ‘κryptos and graphing’ meaning is hidden or secret. It is the study of security technologies and performs in the presence of third parties. More generally, cryptography is the science of privacy and is an ancient art. It is about constructing and analyzing the protocols that overcomes the authority of adversary and which are correlated with various aspects of information security such as data integrity, nonrepudiation and confidentiality and authentication (Singh and Manimegalai, 2012). In this cryptography, encryption and decryption are the two major processes in that. Encryption is the process of renovate plain text into cipher text. Here plain text is the original form of message while cipher text is the unrecognizable form of information. The typical reverse process of encryption is called as decryption (Buchmann, 2004).

Before the modern era, message confidentiality is solely depends on the cryptographic methods. The

Corresponding Author: K. John Singh, School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India

communication of messages from graspable form into an impenetrable one and acknowledgement back again from the other end without interpreting by pirates (Chen *et al*., 2011). To ensuring secrecy in communication encryption is worn up in the fields of conversation between the military leaders, diplomats and those of spies. Encryption and cryptography are nurturing to synonym in this era. Mainly, encryption and decryption used for privacy. Encryption algorithms are supported in achieving this privacy on each transmission over a network (Fridrich, 1998).

The earliest cryptography was the form of simple writing messages, as most of the people could not read this. It was solely concerned about the converting messages into the scribbled manner of figures to protect the message during the time of transmission of message from place to place. The need of cryptography arose because of the advance in our life mode (Wei *et al*., 2006). The most basic forms of cryptography were established in the crib of civilization including the region encompassed by Egypt, Greece and Rome. We have the history of cryptography at least 4000 years. The history of cryptography classified according to the era and mechanisms available. The classification is classical cryptography, Medivieal cryptography and modern cryptography. The classical cryptography is ranging from the early B.C 1600 to mechanical encryption. The medieval cryptography is mainly dealing with the cryptographic communication during the world war and the implementations of the classical cryptographic methods (Addison and Gray, 2006). The modern cryptography is mainly dealing with the symmetric key cryptography, public key cryptography and chaotic cryptography (Wong and Yuen, 2008). In this study, briefly describing the history of the chaotic cryptography and evaluate the performance of selected chaotic encryption techniques.

1.1. History of Chaotic Cryptography

The time line is starting in early 1950, Shannon clearly mentions that the chaos can be used in cryptography, because of its basic stretch and fold mechanism. The time period until 1980's, the necessity of cryptography becomes more important and chaos theory becomes more popular among the cryptographers. The implementation of chaos by Shannon has developed the chaos theory at 1980s. In 1990, the first chaos based ciphers were proposed and more over the synchronization of chaos entered the scene. Approximately 30 more publications were obtained about chaos. In 1996, the chaotic encryption was developed by (Baptista, 1998). The year of 2000, chaos started to recognize widely and obtained an application for secure communication. It is the greatest achievement in chaotic cryptography (Alvarez and Li, 2006). Here we are more concentrating the evaluating the chaotic encryption technique. The chaotic encryption technique which is similar to other encryption techniques. But it is performed the activation through chaos only. Let us discuss as detail.

2. MATERIALS AND METHODS

To grant more perspective about the performance evaluation of the selected chaotic encryption algorithm. Section 2 will discuss briefly about the chaotic encryption (Kocarev *et al*., 1998). The comparative study of the selected algorithms. The comparison is obtained by the encryption speed, the data size and the battery power consumption.

2.1. Chaotic Encryption

The chaotic systems are defined on a complex or real number space called as boundary continuous space. Chaos theory generally aims that to recognize the asymptotic activities of the iterative progression (Wei *et al*., 2006). The properties essential for chaotic systems designed for cryptography is sensible to an initial condition with topology transitivity (Hermassi *et al*., 2010).

The chaotic encryption method is proposed by (Baptista, 1998). It seems to be a much better encryption algorithm than traditional algorithms were used. We first identify the mapping scheme for a trajectory to encrypt the message. Subsequently decide the initial state and parameters for the key. We assume the initial condition as the current route (trajectory). Iterate the chaotic equation until the path reaches the target site and then store the amount of iterations as a code for each message symbol. Encrypt the next message by iterating the recent trajectory. Produce the next cipher according it and so on.

The **Fig. 1** represents the graphical map of the chaotic encryption. It indicated that the presence of the chaotic sign generator during the encryption technique. It helps to generate the chaotic signal sequence stream for encrypting as a key. Set the initial state and parameters to decrypting the message. Apply the similar mapping format for every decryption. Iterate the chaotic equation by the cipher have number of iterations. Find out the site that the trajectory belonged to. Then store the figure of the site as message symbol. Decrypts next message by iterating the current route and produce the next symbol and so on.

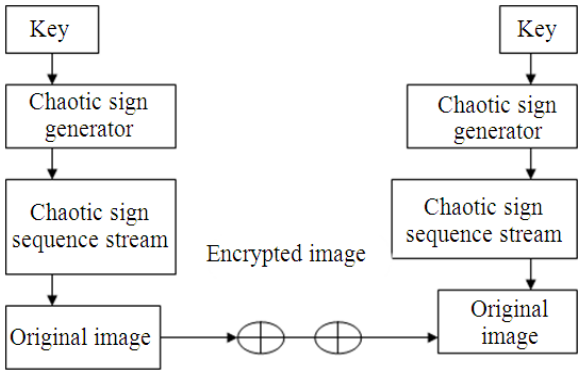

Fig. 1. Chaotic encryption scheme

The broad chaos encryption method is the simplest technique to encrypt video data or message by chaotic equation. This method can facilitate to discover some essential information and establish the crucial stage of security. The advantage of chaotic encryption is (1). High level security (2). The encryption is achieved by iteration (3). Simplest (4). No short cuts are available. Whereas the requirement of large cipher storage and slow in speed are considered the major disadvantages. The properties of chaos are slightly producing some changes in the entire cryptography. Sensitive on initial stage and topology transitivity are the properties in it. In an initial condition, chaotic is always sensitive. Hence it will produce a slight difference in trajectory. It gives the totally different trajectory sectional value. Identical trajectory only can produce the same values. The topology transitivity defines that the state points reside in a bounded space state and approaches infinitely secure to any point of the state space.

In this project, we are focused on the performance evaluation of the chaotic encryption technique. Through security analysis, power consumption, encryption speed and size of data can be found out the performance of each algorithm. Let us discuss selected chaotic encryption algorithm.

2.2. Chaotic Video Encryption Scheme (CVEA)

CVES is an independent of any video encryption algorithm. It can be merely realized both hardware and software. It can provide higher security for real time video encryption. CVES is universal hasty encryption scheme and it can simply expand into further real time applications. This chaotic encryption was proposed by (Li *et al*., 2002). They proposed that the plain video is encrypted by using a cluster to form plain-cluster. The plain cluster is fixed size of video stream data. The cluster is a combination of video data frames.

The encryption procedure of CVES is described as follows. First we have to initiate Control Chaotic Scheme (CCS) with 2^n iterations. Then iterate this component 2^n times to obtain the pseudo random initial conditions x_{e0}. Iteration undergoes to produce corresponding pseudo control parameters and prime number for encryption again. These parameters are used for obtaining the encrypted text (Li *et al*., 2002). The encryption procedure is: one plain-cluster is encrypted by stream sub cipher and followed by block sub cipher. Decryption is the inversion of the encryption process. The encrypted plain-cluster is firstly decrypted by block sub-cipher and pre decrypted plain cluster is encrypted by stream sub cipher.

The most important parameters for CVES are L and n. L declares the key space is 2^{2L}. If the key space ought to be large enough to provide high security. N declares the relationship with the realization complexity of CVES. It should not be large. Usually the ‘n’ will be ‘8’.

2.2.1. Speed

We can estimate the encryption speed by evaluating the speed of both stream sub cipher and block sub cipher. Generally the hardware system is always faster than software. Hence the hardware realization and software realization are used to find out the fastness of the medium.

2.2.2. Security

There are three essential features for ensuring the security performance. (a) Statistical cryptanalysis more complex (b) for different cluster, the pseudo random codes are entirely different in every s-box cluster. It will make it as same one time pad effect. (c) The combinational product of block cipher and stream cipher makes known plaintext and chosen plain text attack unfeasible.

2.3. Scalable Encryption Algorithm (SEA)

SEA is a low cast encryption routine targeted for limited instrumentation sets. This is a parametric nature in text, key size and the processor. It allows the combination of the encryption and decryption. Moreover the simplicity of the SEA algorithm makes the implementation as straight forward (Mace *et al*., 2008). SEA operates several word sizes, text and key. It is based on the Feistel Theory with random rounds of variable number. Generally it defined with the respect to the parameters associated with it. The parameters are: n, deals with the size of the plain text as well as the size of

the key. b, the processor or word size. n_b = n/2b, is the number words per Feistel branches. n_r is the no of block cipher rounds. The parameter n should be the multiple of 6b. The SEA is usually based on the limited no of basic operations. The basic operations are bitwise XOR, substitutions-box, bit rotation r and addition mod 2^b. The method action will be first the cipher iterates by nr number of rounds. The obtainable pseudo code will encrypt the plain text with suitable key K.

As we know that, the SEA is a simple algorithm for encryption. It can easily implement in any type of processor. The flexibility of SEA makes it less sensitive to the processor than the standard algorithm. The proposed pseudo assembly code of an encryption or decryption intended with "on the fly" key scheduling (Mace *et al*., 2008).

2.3.1. Speed

The speed of the encryption can be achieved by the efficient performance of no of cycles required for the encryption. The code size and variable no of rounds are made it complexity of cryptanalysis. The combination of register of SEA and RAM words, the implementation is lower than the block cipher.

2.3.2. Security

The properties of the components will give the greatest security for the structure. The maximum number nonlinear order and recursive definitions raise the complexity to decrypt. The classical extensions of linear and differential cryptanalysis are non-linear estimations of outer rounds, multiple linear cryptanalysis, rectangle and attacks. Though these extensions frequently involve only a tiny improvement compared to the basic attacks. Related key attacks, square attacks and side attacks are possible attacks can possible in this algorithm.

2.4. Nonlinear Chaotic Algorithm (NCA)

The NCA is a chaotic encryption algorithm which uses the power function and the tangent function instead of linear function. The structural parameter of this is obtained by experimental study. For an image transmission, it is designed as one time one password. It was proposed by (Alvarez and Li, 2006). They proposed that it has greater security and large key space while maintaining the efficiency for experiments. NCA contains two parts of the analysis. (1) Logistic map analysis and (2) NCA map design. On a logistic map, the cryptosystem is based on the one dimensional discrete chaotic map. It can simply call it as logistic map. They are very weak on security. In NCA map design, to avoiding the attacks on the plain text it will limit the key space and time. It is done by changing key accordingly. A sequence of chaotic is used for encrypting the video. The NCA map to encrypt the video data with different keys for different data. The original chaotic consists of decimal functions. These chaotic sequences contain integers. Then the image can be encrypted using the XOR operation with the integers (Alvarez and Li, 2006).

The decryption process is more similar to the encryption process. But it needed to an encryption key for decrypting. As per the experimental analysis, the encrypted images are stumbling, unknowable and jagged. The same key is used for decryption. The decrypted images are always clear and correct without any distortion. A wrong key can make completely different decryption. Hence we can conclude that the key which is used for both processes is very sensitive. The analysis of data shows that encryption covered all the characters of plain text statically. It will show balanced performance in the ratio of 0-1. It resulted to high security and Zero correlation.

2.4.1. Speed

The speed of the encryption can be achieved by analyzing the sensitivity of the key and chaotic sequence.

2.4.2. Security

The algorithm belongs to one time one password. The NCA algorithm satisfies the uniform distribution property. The NCA algorithm has the characteristics of the Zero Correlation, Ideal Non-linearity. Hence the encryption by NCA can oppose a gray code attack, statical attack strongly. It has the ability to resist the brute force also. The chosen or known plain text attack inefficient in this algorithm.

2.5. Escrowed Encryption Standard (EES)

The Escrowed Encryption Standard (EES) was approved by U.S department of commerce in 1994. It is a standard for encrypted communication. It is always known as the term of implementation is as clipper chip. The considerable feature of EES is a key escrowed method enabling for detecting the eavesdropping. Both SKIPJACK and LEAF creation methods are used for the encryption or decryption in the EES. It is the type symmetric key encryption method.

For the data encryption, 80 bit key is used to encrypt the plaintext with the one of the following mode are; FIPS81, CBC, ECB.

3. RESULTS

For the experimental analysis, the performance data is collected in a laptop with IV CPU 2.4GHz. The laptop encrypts the various file sizes ranging from 320k to 7.873 megabytes. For the text data, it is about 135 megabytes. For audio data, it ranges from 30kbytes to 7822 bytes and from 4000kbytes to 5994 bytes of video data. The performance parameters are: (1) encryption time (2) CPU utilization with time and (3) battery power consumption.

3.1. Encryption Time

The encryption time is the time which the encryption algorithm takes to produce the cipher text. It helps to calculate the throughput of the encryption. It indicates to find out the speed of the encryption. The throughput is calculated as total plaintext encrypted in bytes divided by the total time taken for encryption.

3.2. CPU Utilization

CPU utilization means the CPU processing time. It is the time which the CPU is committed to the particular process calculation. It indicates the load on the CPU. If the encryption time is higher, the load on the CPU is also high.

3.3. Power Consumption

The CPU cycle is a metric. It reflectin in the CPU power consumption during encryption process carried out. The measurement of CPU cycle helps to find out the power consumption in each of the process. Each cycle is consuming a small amount of energy for encryption. As we know that, there is no significance for encoding scheme in encryption. So no need to find out any comparative study based upon the encoding.

3.4. The Effect of Changing Packet Size for

Encryption Algorithm on Power Consumption Encryption time is used to calculate the throughput of an encryption technique. The throughput of the encryption technique is calculated by dividing the total plain text in Megabytes encrypted on the total encryption time for each algorithm in. it indicates the speed of encryption technique. The power consumption of this algorithm decrease as the throughput value increased accordingly.

The analysis of resulted shown in **Fig. 2 and Table 1** as follows. Here, we consider different packet size of data with different encryption time in each algorithm. Hence calculated the throughtput of the each encryption algorithm.

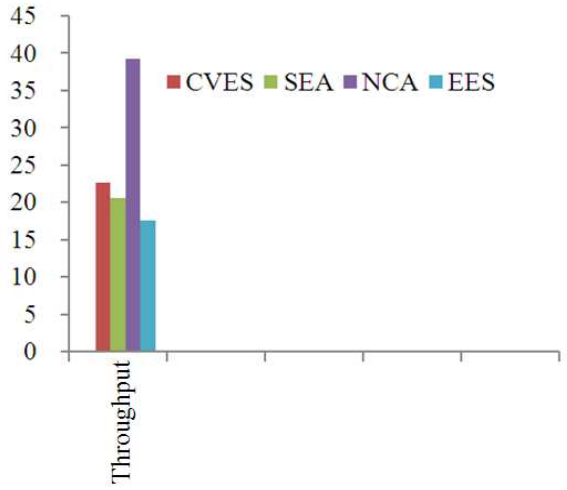

Fig. 2. Throughput of each encryption algorithm

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

From the **Fig. 2 and Table 1**, the results are shown the superiority of NCA algorithm over other algorithms in terms of processing time. Another point can be notice here, CVEA requires less time than all algorithm except NCA. Third point is, EES has low performance in terms of poer consumption and throughput. It requires more time to encrypt because of its special escrowed key method and the presence of both LEAF and SKIPJACK creation method.

4. DISCUSION

4.1. The Effect Changing File Types for

Encryption on Power Consuption The video data type analysis reults are shown in **Fig. 3** at encryption. The **Fig. 3** shows that the time consumed in each algorithm during the encryption. From the analysis, EES is using the most time to encrypt the data.

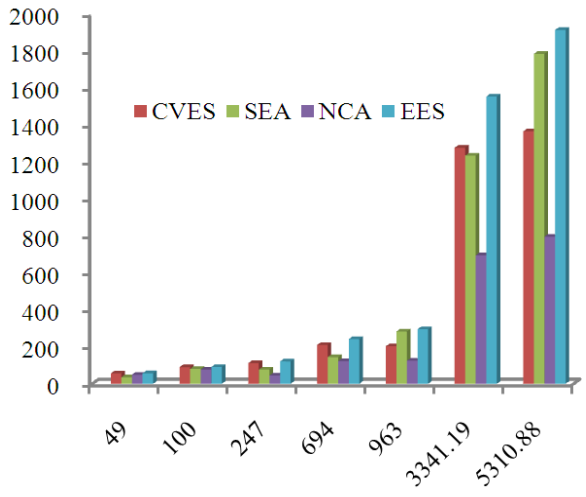

Fig. 3. Power and time consumption for encryption schemes

Table 2. Levels of security

Algorithm	Security
CVES	High
SEA	Medium
NCA	High
EES	Medium

NCA needs the less time for consumption. If the NCA compares with the CVES, the difference is not much more. They are approximately equal. Hence resulted that the CPU load is more in EES compare to other. The analytical mechanism in NCA provides the less CPU load.

4.2. Analysis on Level of Security on Each Algorithm

Table 2 represents the level security provided in each selected algorithm. It represent as follows.

From the **Table 2**, CVES and NCA have the greatest security while compared to the other algorithm. The iterative control over the chaotic scheme will give the highest security in CVES. While in NCA having two types of analyzing before encrypting. It will give the strong base for the secure nature. In the case of the EES. Compared to these both algorithms, SEA and EES have less security. But in the escrowed nature of keying in the EES provide better security while transmitting

5. CONCLUSION

Rapid advancements in multimedia communication, video encryption plays more and more vital role. The video transmission required privacy while transmitting. Here we are analyzing the security analysis and performance efficiency of chaos based encryption. Chaos based encryption provides a fast and realistic solution for secure video transmission. While comparing with traditional cryptographic algorithm, it shows that chaotic has the greatest security and efficiency to resist the attack. The security analysis shown that high to medium level of secure nature provided by this.

In this study, several selected algorithms are used to evaluate the performance. The selected algorithms are NCA, CVES, EES and SEA. From experimental analysis, several points are concluded. (1) In the terms encryption speed and time, we concluded that CVES and NCA are best among. (2) In terms of time consumption, NCA is the best amid and EES needs more time to encrypt between all other algorithm. (3) The NCA and CVES providing better security while comparing the other two. There is no significancal difference when different encoding used foe encrypting.

6. REFERENCES

Addison, S.R. and J.E. Gray, 2006. Chaos and encryption: Problems and potential. Proceedings of the IEEE 38th Southeastern Symposium on System Theory, Mar. 5-7, IEEE Xplore Press, Cookeville, TN., pp: 444-448. DOI: 10.1109/SSST.2006.1619122

Alvarez, G. and S. Li, 2006. Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos, 16: 2129-2151.

Baptista, M.S., 1998. Cryptography with chaos. Phys. Lett. A, 240: 50-54. DOI: 10.1016/S0375-9601(98)00086-3

Buchmann, J., 2004. Introduction to Cryptography. 2nd Edn., Springer, New York, ISBN-10: 0387207562, pp: 335.

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

Fridrich, J., 1998. Symmetric ciphers based on twodimensional chaotic maps. Int. J. Bifurcat. Chaos, 8: 1259-1284. DOI: 10.1142/S021812749800098X

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

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

Li, S., X. Zheng, X. Mou and Y. Cai, 2002. Chaotic encryption scheme for real-time digital video. Proc. SPIE, 4666: 149-160.

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

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

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

Wong, K.W. and C.H. Yuen, 2008. Performing compression and encryption simultaneously using chaotic map. City University of Hong Kong.