Secured E-Commerce Transactions Through Choatic Map

Bremnavas Ismail Mohideen
Department of Computer Engineering and Networks
Jazan University, Jazan
Kingdom of Saudi Arabia
jmcnavas@gmail.com

Anand Mahendran
School of Computer Science and Engineering
VIT University, Vellore, India
manand@vit.ac.in

***Abstract*—Internet has become widespread, and is used for all transactions to support client and server services. E-commerce is also one of theservices to sell thegoods using the Internet. E-Transaction has becomes more important, security for E- transaction is a important work because of the insecure communication channel. In this paper, we have proposed a new algorithm for a secure e-transaction using chaos.**

Keywords—E-commerce, chaos; logistic map; electronic transaction; client and server.

I.INTRODUCTION

In the last three decades, there are significant developments in computer and communications technology. Internet has became the important marketplace in many applications.In the current scenario, e-commerce or e-marketing is a good methodology in modern business for buying and selling the goods over the Intenet.For the purpose e-marketing, it is motivating and encouraging the client and server technology. This technology is help to interactivities between businesses, the connection between government agencies and individuals of all sizes. People are adopting the Internet technology for their professional and personal usages such as execute their money transfer, shopping, electronic payments and many other activities over the Internet[12,13]. The problem of information security and privacy is increased due to more usage and dependence on the Internet. In particularly the e-commerce transaction is how to attain and provide a high level of security for the customer and merchant transactions [14].This has motivated the researchers to solve such problems to protect Internet users from hackers or intruders.

E-commerce is a good methodology for buying and selling the goods over the Intenet. It is a new approach of providingbusiness transaction over the traditional business transaction systemsuch as payroll, order processing, reservations and employee records [15]. Electronic payment procedure is a key component in e-commerce, along with selection, ordering and delivery process.Various payment methodsare widely used, currently focussed on our day to day commercial dealings[15]. Each of its payment methods hasown advantages and disadvantages.For example the basic payment methods is cheques. The advantage of this model is used a lot for business to large amounts of business payment transations but the same time the main disadvantage of this process is vulnerability of cheques to fraud. Every payment method needs a security for money transaction on the Internet for their users which is considered to be an important process of the e-commerce. The major security issues are related to the use of e-commerce systems, which turns around the question of how one can pay securely over networks which are inherently insecure.

For e-commerce security purpose, transaction of money through the Internet make sure thatthe different alogithms are used in alltransaction process, for example the fingerprint biometric modality algorithm has focussed the importantance of it's couple of characteristics such as the unique identity and permananence that's able to stay unchanged over the lifetime [3]. E-commerce transaction(s) security is most important one among factors in confirming the achievement of e-commerce. Therefore, it is necessary to have enough security features to protect the data on computers, distribution systems, and individual secret key.

II.THE BASIC E-COMMERCE SECURITY ISSUES

In this section, we discuss about the key technology to report the issues of security that can happen in e-commerce. The generally addressed security issues addresses in e-commerce transactions are:

- *Authorization:*It can prevent a person user account.
- *Authentication:*It can verify the user authorization. This process enforces that the user is the only person permitted to login to his account.
- *Confidentiality:* The protectionof user data against the unauthrized disclosure.
- *Non repudiation:* To the ability to ensure that a party to a communication cannot deny the authenticity of their signature on a document.
- *Availability:*Assures that user works promptly and data services is not denied to unauthorized users.

Secrity Requirements and Performance Parameters of E-commernce

The security system requirement of an e-commerce can initially addresses into three important areas:

978-1-5090-4559-4/17/$31.00©2017IEEE

- Information and communication protection
- Identification and verification of communication partners
- The various system components security [11].

A set of performance parameters are needed to define on which,the evaluation and comparsionof the different schemes of image security.

- *Visual Degradation* **:**This parameter is to measures and compare the perceptual alteration of the image data with respect to the original plain image
- *Tunability:*This parameter is dynamically defined thedisimilar application requirements of encryption parameters.
- *Speed:* The security algorithms are so fast to enough meet the basic requirements of any real time applicationrequirementssuch as Data encryption standard (DES), Rivast Cipher (RC5) and Advanced Encrryption Standard (AES).
- *Encryption Ratio:* It measures that how many amount of data to be encrytpted and minimised to reduce computational complexity.
- *Compression Friendliness:* The security algorithm is consideredto be compression friendly. Some of the algorithm like choas impact date compressibility[16].

III.E-COMMERCE AND ITS TYPES

In this section, we discuss about the different types of e-commerce in mode of communications.

B2B (Business to Business) : B2B process is intermediate process between the businesses. All electronic goods or services communicated between companies.

B2C (Business to Consumer): B2C process is no intermedicate steps between the business to consumer. Through website, the consumer and business can directly connect to make a order for the goods to the organaization at the same time. The organization reply an authentication email and dispatches the goods to the consumers. The example of this B2C process, virtual stores and malls which seel all kinds of consumer goods through the Internet.

C2C (Consumer to Consumer): C2C process is an interaction between the consumers on both sides. Selling the property, product and any other movable things, the consumer posts their advertisement on internet. Any consumer wants to buy the product after seeing this advertisement will directly contact the consumer. These C2C transactions process is to provide the online platform where the transactions are carried out through a third party direction.

*B2G (Business to Government):*Through government website, various organizations will be connected to the government website to trade and exchange the business information. The concept of this process can use central web sites to exchange information such as government forms, e-procurement services and update corporate information.

G2B (Government to Business): The auction and tender applications of business will be received and filled through the government website through online. For example, the rules, requirements and permission needed to start a new business and other specifications for business.

IV.LITERATURE REVIEW

Suhad et al., discussed about the fast development of the electronic document interchage, storing and communication of knowledge safety measures[1]. Ravi et al., focussed about the fingerprint documentaion biometric method, it is common methodof biometric, because of the easiness in obtaining and through gathereing of the adequate sources of informaion. This paper also discuss about the matching and recognition of the fingerprint techniques and their presentation examination. [2].

Jaya Lakshmi et al. presented anew way for bio-crypt key based on finger print and the finger print biometric modality and its applications [3]. Thambiraja et al., discussed in specific about the private key block ciphers which is used for the complete document and connection of encryption. This paper also focuson various encryption techniques by means of a comparitive study betweenexisting and recent techniques [4]. Ishaan Agarwal et al., discussedabout the password based image encryption methodand it's progress . This method is secured from brute force attacks [5]. Muthu kannan et al., implemented various security aspects of wireless networks. The biometric technique also to discuss about the security problems of the wireless commincation and provide solutions for above. The above workmainly focus on two biometric features, two factor biometric keys generation and to more secure provision for accessing of wireless networks [6]. Chun-I Fan et al., discussed about the biometric data used as a key to encrypt, and the idea conservesthe privacy of biometric templates [7]. In May 2012, Eun-Jun Yoon et al.,discussed a flexible and robust biometric remoteuser authentication scheme [8]. Arian Rahimi et al., focussed about an iris authentication efficiency for e-commerce transactions by using the chaos theorybased cryptography. [9].

V. PROPOSED WORK

Over the past few decades, in the field of non-linear dynamics system chaos has engaged in many researchers attention, such as fluid dynamics, weather forecasting, electronic systems, climate, laser, cryptography and steganography [17,18]. For security point of view, chaos manipulating different chaotic 1D and 2D maps, such as logistic map, cat map, henon map and tent maps. There are few resemblances and differences between chaotic maps and cryptography algorithms. Both or more generally maps are defined on finite sets have some similar properties such as initial conditions and parameters. The initial condition parameters in chaotic maps are meaningful on real numbers, which is be used in the cryptographic algorithms as encryption and decryption keys [19].

The properties of chaotic systems are more sensitive in the initial conditions, unpredictable behaviour in the long term, thus representing the confusion and diffusion in cryptographic encryption algorithms. Chaotic iterations process leads to spreading of the initial region over the entire phase space, for example the range of logistic map in the chaos region value is 0.0 to 4.0.We design the algorithm by utilizing chaotic maps characteristics such as deterministic nature unpredictability, random behavior and sensitivity to initial value. Chaos has certain potential properties in creating new way(s) of securing important information to be transmitted or stored. Here, we consider one dimensional chaotic logistic map. It is a simple model which yields chaos. In this paper, we focus secure e-commerce transaction on choatic logistic map [10].

Here, we consider the logistic map, is a one dimensional chaotic map, written as

$x_{n+1} = a\, x_n\, (1-x_n)$ ($x_n=x_0,x_1,x_2\ldots$), where $0<=a<=4$

This is a discrete-time map which receives a real number between 0 and 1, and returns a real numbers in [0,1]."n" denotes a discrete time step, "x_n" denotes the data at "n".

As the user perception the initial key value "a" is assigned when the logistic difference equation is evaluated to generate a sequence of random number. For example, if the key value is 0.3, this value acts as an encryption key for the encryption process that is to be carried out. The image pixel in the one dimensional array format is being encrypted with the random numbers generated by the logistic map in the chaotic region i.e., a value 0 to 4. Now the image is encrypted in the chaotic region and it is ready to send across the transmission channels.

VI. RESULTS

In electronic money transaction needs to provide the security for our payment data such as our password which may be identified by biometric like fingerprint identification, iris, voice, etc., in this paper, we focus on chaotic logistic algorithm for security and stenography to encrypt the biometric input image for the secure transaction purpose.

Sender side algorithm

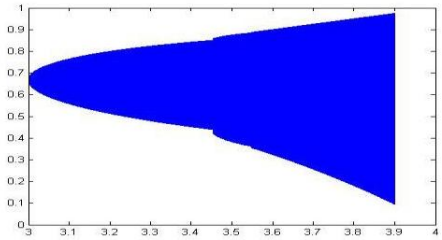
Input: User biometric image, I
Output: Encrypted signal, ES

1:Load an user biometric image and store an image in the one-dimensional array named as I.
2:Generate the chaotic signal S using logistic equation
$X_{n+1} = aX_n\ (1- X_n)$
3:The image I is embedded within the chaotic signal S using the following steps
3.1.Fix the covered boundary region based on the size of an image I
3.2.The signal is assumed to be generated from the starting position of the boundary region
3.3.Set a key value K dynamically within the boundary region for representing the initial position.
3.4. The image value I is embedded with chaotic signal S from K.
4:The encrypted signal (ES) is transferred along with the key value K. (The key value is embedded in a standardized position of the signal ES).

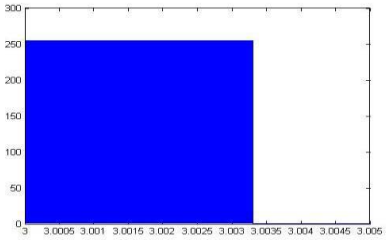
B. Receiver side algorithm

Input: Encrypted signal, ES
Output: User biometric image, I
1:Receive the encrypted signal, ES from the open communication channel.
2: Retrieve the key value K from encrypted signal ES.
3:Generate the chaotic signal S using logistic equation
$X_{n+1}= aX_n\ (1- X_n)$
4:Subtract the received encrypted signal, ES with the raw logistic signal, S using the key value K, to obtain a one-dimensional array for biometric image, I
5:Construct the resultant biometric image, I from the one-dimensional array.

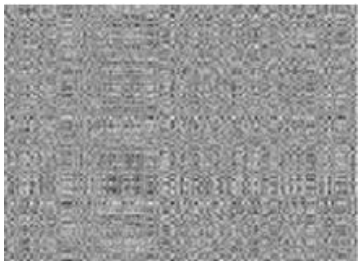
a) Original fingerprint image



b) Generated signal based on the logistic equations

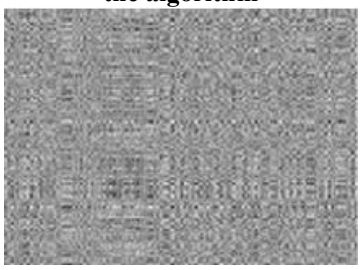


c) Embedded image and signal with the cover region (steganography)

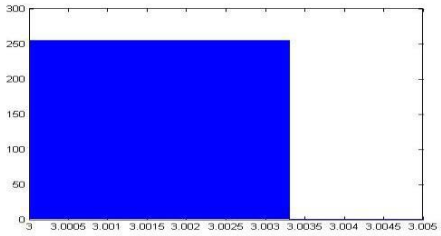


d) Encrypted fingerprint image

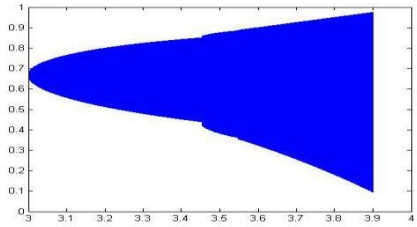
Figure1. The Finger print image encrypted after using the algorithm



a) Encrypted fingerprint image



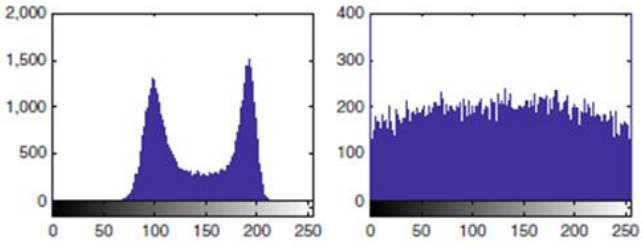
b) Received the key K from encrypted signal



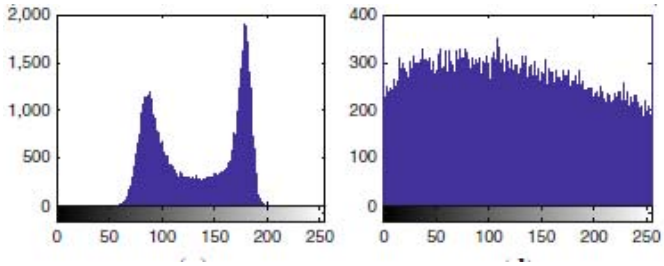
c) Generate and subtract the logistic signal

d) Decrypted fingerprint image

Figure2. The finger print image decrypted after using algorithm

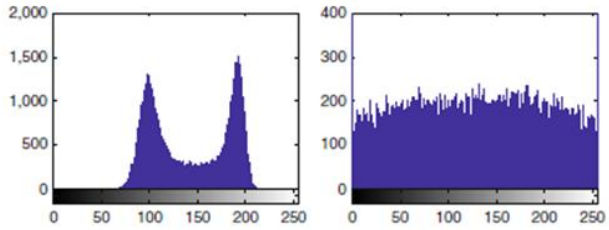


a) Histogram of original finger print image

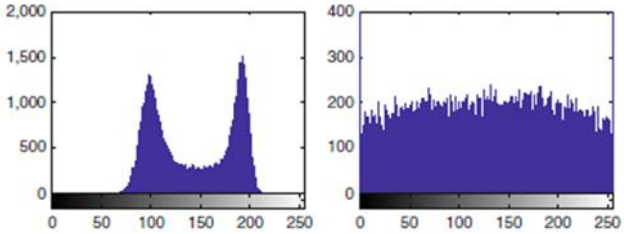


b) Histogram of encrypted finger print image

Figure3. The histogram comparsion of orignial and after encryption the image.



a)Histogram of original finger print image



b) Histogram of finger print image after decryption

Figure4. The histogram comparison of image before and after encryption and decryption

VII CONCLUSION

In e-commerce transactions security is becomes a vital important. In this paper, we havediscussed the secure e-commerce transction by using biometric image identification through choatic logistic map.By using chaos algorithm is to encrypt the biometric image data are embedded to perform stenography. By this process has reduced the time with the adoption of multithreading for encryption and decryption.

REFERENCES

[1]. Suhad Latef, "Color image encryption using random password seed and linear feed back shift register", Journal of Al-nahrain university, Vol.14 (1), March, 2011, pp.186-192.

[2]. Ravi Subban, " A study of biometric approach using fingerprint recognition", Lecture notes on software engineering, Vol. 1, No. 2, may 2013.

[3]. Jaya Lakshmi, "Design of secured key generation algorithm using fingerprint based biometric modality", IOSR Journal of Engineering, Vol. 2 issue 2, Feb.2012.

[4]. Taambiraja, "A survey on various most common encryption techniques", International journal of advanced research in comptuer science and software engineering, Volume 2, issue 7, July 2012.

[5]. Ishaan Agarwal, "Password-oriented image encryption with

multiple dependent factors", IOSR Journal of Computer Engineering (IOSR-JCE), volume 16, issue 5, ver. VI (Sep-Oct. 2014).

[6]. P.Muthu Kannan, "Secured Enctyption algorithm for two factor biometric keys", International journal of latest research and technology Vol.1, issue 2: page no. 102-105, July – August (2012).

[7]. Chun-I Fan and Yi-Hui Lin; Provably Secure Remote Truly Three-Factor Authentication Scheme With Privacy Protection on Biometrics, IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, December 2009.

[8]. Eun-Jun Yoon and Kee-Young Yoo; A robust and flexible biometrics remote user Authentication scheme, International Journal of Innovative Computing, Information and Control Volume 8, Number 5(A), May 2012.

[9]. Arian Rahimi, Sharhriar Mohammadi and Rozita Rahimi; An Efficient Iris Authentication Using Chaos Theory-based Cryptography for E-commerce Transactions.The Institute of Electrical and Electronics Engineers, 2009.

[10]. I.Bremnavas et.al, "Medical image security using LSB and Chaotic Logistic Map", Proceeding of Int. Conf. on Advances in Recent Technologies in Communication and Computing, 2011.

[11]. Jolly Shah et.al, "Performance study on image encryption schemes", International Jounral of Computer Science Issues, Vol. 8, Issues 4, No1, July 2011.

[12]. Turban, E., D.K.D. Viehland, and J. Lee, (2006). Electronic Commerce A Managerial Perspective2009. 3rd ed., Pearson Prentice Hall.

[13]. Schneier, B. (1996). Applied Cryptography. 2nd ed., Wiley, USA.

[14]. Stallings, W. (2003). Cryptography and Network Security: Principles and Practice. 2nd ed., PrenticeHall, USA.

[15]. EktaChauhanet.al, "A Hybrid Technique to Secure E-commerce Transaction with the help of AES encryption and stenography in image", International Journal of Hybrid Information Technology, Vol.8, No.8, pp. 271-278, 2015.

[16]. Alireza Jolfaei and Abdolrasoul Mirghadri,"An image Encryption approach using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology, Vol. 19, No. 2, September 2010,pp. 117-123.

[17]. Richardson, D. S. 1998: Obtaining economic value from the EPS ECMWF Newsletter 80, Summer 1998.

[18]. Buizza, R. 2001: Weather risk management with the ECMWF ensemble prediction system. ECMWF Newsletter 92, Autumn 2001

[19]. M. S. Baptista, "Cryptography with Chaos", *Physics Letters A*, vol. 240, pp. 50–54, 1998.