IJCSE International Journal of Computer Sciences and Engineering Open Access
Research paper Volume-5, Issue-7 E-ISSN: 2347-2693

Enhanced Online Payment Security using Steganography, Quantum and Visual Cryptography

Anshu Arele[1], Vikas Sejwar[2]

[1*]Dept. of CSE and IT, Madhav Institute of Technology and Science, Gwalior, India
[2] Dept. of CSE and IT, Madhav Institute of Technology and Science, Gwalior, India

[*]*Corresponding Author: areleanshu@gmail.com, Tel.: +00-12345-54321*

Available online at: www.ijcseonline.org

Received: 26/May/2017, Revised: 12/Jun/2017, Accepted: 17/Jul/2017, Published: 30/Jul/2017

***Abstract*—** Visual Cryptography is Secret Sharing Scheme where it is an encryption methodology to hide the data under image in a fashion that it can only be decrypted by the combination of two shares. Quantum mechanics is the bsis of Quantum Cryptography Techniques. Use of Quantum key is the basis as Quantum mechanics concept has been utilized to have encrypted key in place between users and not used for data transmission. Steganography involves techniques of hiding information under other information so that extraction of data become difficult .In the existing work, it used these three techniques to improve the transaction security. But this is not enough to secure so to overcome this problem we apply image sequence and send OTP in the email id which makes them more secure to achieve more security.

Keyword- Payment System, Buisness, Internet, Keys, Visual Cryptography, Quantum Cryptography, Stagenography

I. INTRODUCTION

Electronic payment systems are becoming an essential part of electronic commerce and electronic business. The problem is that orthodox method of paying for goods and services is not compatible to work with internet. Trust, security and Reliability is still a concern for the users who are not used to to the online world, etc. [1]. This leads to the less acceptance of EPS systems resulting in less usage of EPS. To highlight the factors involved in user acceptance we had a survey with users of payment systems. Survey addressed the conventional (cash, offline credit cards) and electronic payment systems (debit and smart cards and credit cards on the Internet) [2].

Section II contains the introduction of Visual Cryptography , Section III contains the introduction of Quantum Cryptography, Section IV contains the introduction of Steganography, Section V contains the Literature Review, section V explain the results with flow chart, Section VI describes results and discussion, VII concludes research work with future directions).

II. VISUAL CRYPTOGRAPHY

Visual Cryptography is a encryption methodology where visual information will be encrypted in such a manner that it can't be decrypted without mechanical intervention. Visual Cryptography utilizes two transparent images. One image contains random or noisy pixels and the other image contains the secret data. Image containing information will be hidden under the other image containing meaningless or random image. It is nearly impossible to get the information from the encrypted image as information about both the images are required to hack the information. Implementation of Visual cryptography can be easily achieved by the use of one transparent sheet and print the two layer onto it. Beauty of Visual cryptography is that the computation required for decryption is not required as stacking process is used to restore the secret image. This feature reduces the computation involve in this method .This Method was introduced by Naor & Shamir 1994 [3]. It is a secret sharing scheme with good security for binary image. Through Human vision it can be decoded directly i.e. ensure that machine cannot decode the same. Different levels of visual cryptography has been defined.. In this document we will discussed the work done on the a. Binary images b. Gray Images c. Color Images. The research work are described in the subsequent topics [4].

III. QUANTUM CRYPTOGRAPHY

Quantum Cryptography is a latest method of information security. Quantum mechanics is the pillar for quantum cryptography. Quantum fundamental and properties like light, laser and free space transmission are the heart of

quantum cryptography Key distribution principle. Using Heisenberg uncertainty principle and Quantum Entanglement creation of symmetric key are possible which is used in the basic principle of quantum key distribution.

a) Heisenberg uncertainty principle

This Principle state that measuring the quantum state of any system is not possible without disturbing it. It conclude that polarization of photon and light particle can only be identify at the moment when it is measured. So if eavesdroppers are trying to locate/measure this they have to disturb it and will be caught. Also portioning of photon in two halves cannot be done as measuring the photon will affect the value. Anyone trying to detect the state of photons being send to the receiver, error can be detected.

b) Quantum entanglement

Another important principle is quantum entanglement. Entanglement of particle can be possible so that when particular property of one particle is measured, entangled particle will show the opposite state for same property instantaneously. Hence, state of entangled particle cannot be predicted prior to measurement. It conclude that in order to have communication between two channels it is must to have discussion on the state of particle.

IV. STEGANOGRAPHY

Origin of Steganography word is from Greek which means Concealed writing. "steganos" is equivalent to "covered " and "graphical " to "writing". It support hiding the data with verity of transmission of secret data. It work in such a manner that information will be hidden in another file and user who is going to receive it can only know that the information exist in the wrapper message .It is very similar to the method used in the ancient time like hiding the information under writing table ,in stomach of rabbit or in the back of wax.. But today's most of the people transmit the data in the form of text, images, video, and audio over the medium. Wrapper like audio, video and images are used to hide the confidential information. Although it is ancient technique but in modern world it can be best describe by a story proposed by Simmons, where two prisoner communicate in a secret manner to execute their escape plan. The transport for passing the information was a warden who will through them in solitary imprisonment if he suspect any covert communication. He has all the authority to check on the communication exchanged between prisoners whether it is passive or active. Passive warden examine the communication and try to detect if the communication contain secret information. If he suspect that the communication is having some secret information he will take a note of it ,pass the information to the third party and let the information flows to the destination .An active warden will try to modify the information so that message will be distorted. [6]

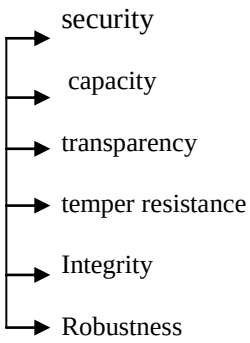

Fig.- Steganography Features

V. LITERATURE REVIEW

In [7] provided a protocol dependent on inherent secure nature of quantum cryptography (quantum no cloning theorem and quantum measurement rule). A secure multiparty quantum secret sharing scheme has been proposed to ensure that no one can eavesdrop or extractany share of the secret message via inherent security provided by quantum entanglement swapping and quantum teleportation. Entanglement swapping is a process that allows two non-interacting quantum systems to be entangled. Whereas, Quantum teleportation allows a party to send a qubit to another entangled party without sending the qubit over the channel. Moreover, in order to ensure security against possible active attacks, sender himself will generate and distribute EPR pairs to be used in the scheme. Result will be a secure multiparty QSS scheme which will be secure against internal and external eavesdropping, masquerading and brute-force attacks [7].

In [8] analysed possibilities of application of post-quantum code based signature schemes for message authentication purposes. An error-correcting code based digital signature algorithm is presented. There also shown results of computer simulation for this algorithm in case of Reed-Solomon codes and the estimated efficiency of its software implementation. We consider perspectives of error-correcting codes for message authentication and outline further research directions [8].

In [9] demonstrated implementation of BBM92 protocol using GUI including a system having quantum encryption with grid community technology along with detail high and level design of the system configured [9].

In [10] applied Hierarchical Visual Cryptography Scheme on gray image instead of binary image. So, generated shares are gray share, not binary shares that are generated by the binary image. Here we are using the new proposed gray share generation algorithm for generation of n number of shares.

Here original image is encrypted in to n number of levels so security of original image is increased. At decryption side all n shares must have to participate to reveal the original secret. Decrypted image has same size and better visual quality then original secret image [10].

Effective technique of share generation based on XOR-based visual cryptography for General Access Structures is introduced. Perfect restoration of the secret, no pixel expansion and no code book requirement are the advantages that the algorithm is expected to have. The generated shares are then covered in an image using steganography which provides additional security [11].

Novel technique about secure medical information transmission of patient inside medical cover image is presented by concealing data using decision tree concept. Decision tree shows a robust mechanism by providing decisions for secret information concealing location in medical carrier image using secret information mapping concept. RSA encryption algorithm is being used for patient's unique information enciphering. The outcome of the RSA is structured into various equally distributed blocks [12].

VI. PROPOSED WORK

PROPOSED ALGORITHM

Step:1 Initially user register
Step:2 Fill basic details in the form
Step:3 Perform encryption on user id and password on both server and client side
Step:4 Ask for image sequence
Step:5 Now user get registered
Step:6 For order placement user has to login
Step:7 Then user can choose and place an order
Step:8 For better security, image sequence asked
Step:9 If (Sequence is correct)

```
While (attempt<=3)
{
  Welcome to the Payment
Gateway
}
Session time out
Else
    Select image sequence
```

Step:10 Complete Transaction or choose COD Step:11 Order placed successfully with more security
Step:12 Stop

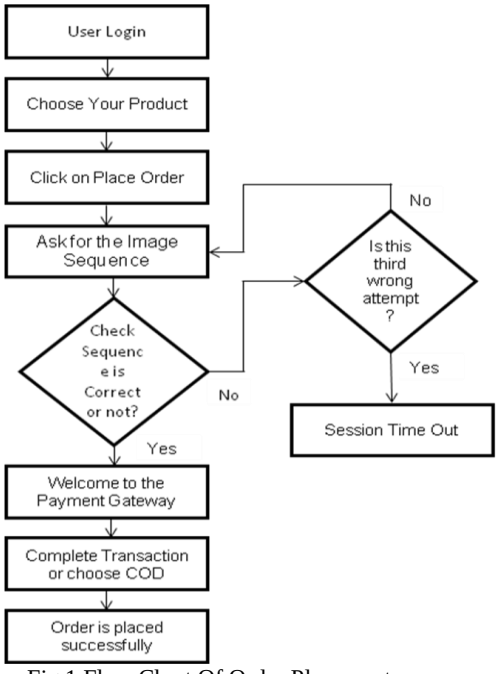

Fig.1 Flow Chart Of Order Placement

VII. RESULTS AND DISCUSSION

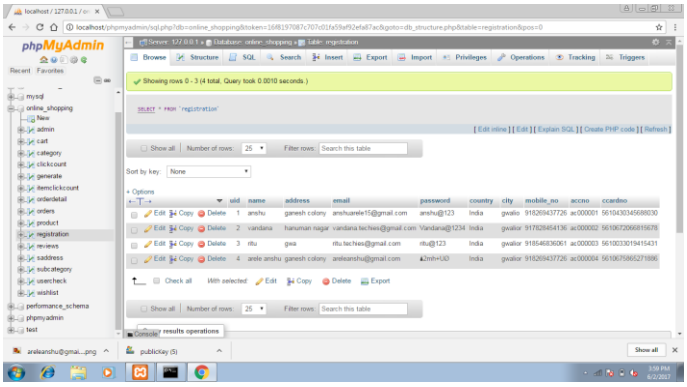

Fig.1 Encrypted Password

Fig.2 password in the form of image sequence

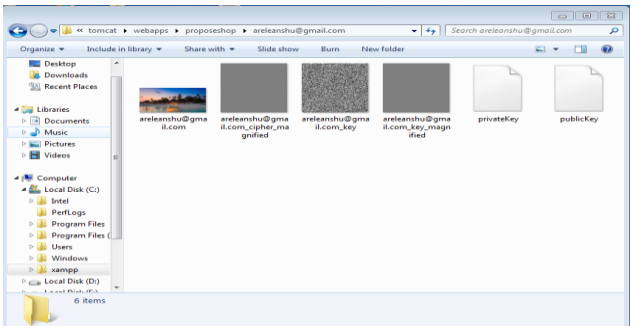

Fig.3 generated pattern in encrypted form

In Fig.3 First image is generated from stagenography ,by which we generate password in image sequence form.
Second ,third, and fourth image is generated from visual cryptography technique where shipping address ,credit card no. and other different information of customers are saved in encrypted form.

Fifth and sixth image means public key and private key is generated with the help of quantam cryptography by which we can encrypt and decrypt our OTP generation that can enhance the security of online payment system.

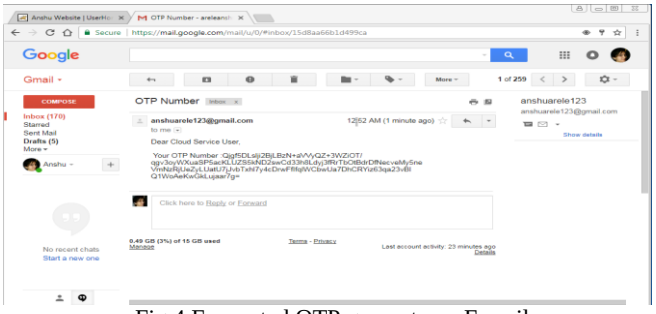

Fig.4 Encrypted OTP generate on E-mail

We will generate an OTP which can secure authenticated identity of authorized person and can make sure that any product is ordered or cancelled by valid customers.OTP is in encrypted form and is converted into decrypted form for increase the security of payment of any product.

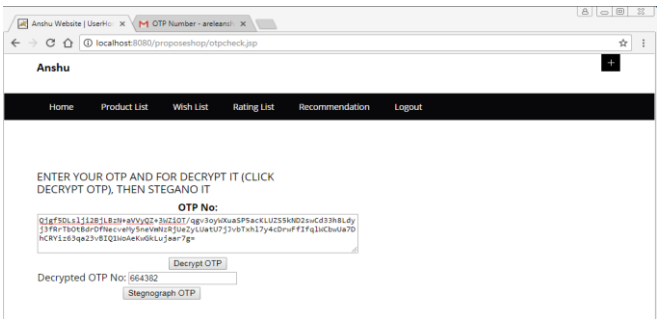

Fig.5 Encrypted OTP is convert into decrypt form

It should include important findings discussed briefly. Wherever necessary, elaborate on the tables and figures without repeating their contents. Interpret the findings in view of the results obtained in this and in past studies on this topic. State the conclusions in a few sentences at the end of the paper. However, valid colored photographs can also be published.

VI. CONCLUSION AND FUTURE SCOPE

E-shopping generally recognized as Electronic Commerce refers to the buying and selling of information, products and services via computer networks. Cryptography is the technique which improves the security of the data. We performed buying of products by creating website of Adidas in which we register with certain details and image sequence. Then select products and execute transaction which provides security to protect the transaction details. Image sequence is always asked when we used different system for registration and transaction. This improves the overall performance of the procedure of cryptography.

REFRENCES

[1] Wayner, P. "*Digital cash: Commerce on the net*", 2nd ed. London: AP Professional, 1997.

[2] Dennis Abrazhevich "*A Survey of User Attitudes towards Electronic Payment Systems*"2012.

[3] P. Sharma, D. Mishra, V.K. Sarthi, P. Bhatpahri, R. Shrivastava, "*Visual Encryption Using Bit Shift Technique*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.3, pp.57-61, 2017.

[4] Vinod. L. B and Nithyanada. C. R, "*Visual Cryptographic Authentication for Online Payment System*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.8, pp.109-114, 2015.

[5] Ajay L "*Survey of Most Prominent Quantum Key Distribution Protocols*" International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 05, 2016.

[6] SO. OKOLIE, BT. ADETOBA, "*Comparative Analysis of Performance Characteristics of well-known Symmetric Key Encryption Algorithms*", International Journal of Scientific Research in Network Security and Communication, Vol.4, Issue.3, pp.1-6, 2016.

[7] Gaurav Jain and Vikas sejwar,"*Improving the Security by using Various Cryptographic Techniques in cloud computing"*, ICICCS-International Conference On Intelligent Computing and Control Systems ICICCS 2017,

[8] Rajesh Shah and Yashwant Singh Chouhan, "*Encoding of Hindi Text Using Steganography Technique*", International Journal of Scientific Research in Computer Science and Engineering, Vol.2, Issue.1, pp.22-28, 2014.

[9] Noor Ul Ain "*A Novel approach for secure multi-party secret sharing scheme via quantum cryptography*" 2017 International Conference on Communication, Computing and Digital Systems (C-CODE), 2017.

[10] Yuriy Gorbenko, Igor Svatovskiy, Oleksiy Shevtsov "*Post-Quantum Message Authentication Cryptography Based on Error-Correcting Codes*" Third International Scientific-Practical

Conference Problems of Infocommunications. Science and Technology PIC S&T-16, Kharkiv,pp. 51-54, 2016.

[11] Kaur, R. Singh, S. Gagneja , "*Network Security and Methods of Encoding and Decoding*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.2, pp.11-15, 2014.

[12] Trupti Patel, Rohit Srivastava "*Hierarchical Visual Cryptography for Grayscale Image*" 2016 Online International Conference on Green Engineering and Technologies (IC-GET), 978-1-5090-4556-3/16/$31.00 ©2016 IEEE.

[13] Vandana Purushothaman, Sreela Sreedhar "*An Improved Secret Sharing Using Xor-Based Visual Cryptography*" 2016 Online International Conference on Green Engineering and Technologies (IC-GET), 978-1-5090-4556-3/16/$31.00 ©2016 IEEE.

[14] Mamta Jain, Rishabh Charan Choudhary Anil Kumar "*Secure Medical Image Steganography with RSA Cryptography using Decision Tree*" 2016 .

[15] Sudipta Sahana and Abhipsa Kundu, "*A Novel Approach on Adaptive Block Steganography Based Crypting Technique for Secure Message Passing*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.12, pp.42-46, 2014.

[16] Nour Elhouda Tabet, Media Anugerah Ayu "*Analysing the Security of NFC Based Payment Systems*" 2016 International Conference on Informatics and Computing (ICIC), 2016.

[17] Deepali Kayande, Elsa Rebello, Shweta Sharma and Monica Tandel "*Overview of a Payment Solution for NFC- Enabled Mobile Phones"* InICT in Business Industry and Government (ICTBIG), International Conference on Nov 18 (pp. 1-4), 2016.

.

Authors Profile

Miss.Anshu Arele pursed Bachelor of Engineering from Rustamji Institute Of Technology And Science (RJIT) Tekanpur (Gwalior (M.P)), in 2013 . She is currently pursuing Master Of Technology in Department of CSE/IT (cyber security branch), Madhav Institute Of Technology And Science Gwalior (M.P). She is a member of IET,IJARCS and IJCSE.

Mr.Vikas Sejwar pursed Bachelor of Engineering from Madhav Institute Of Technology And Science in 2006 and Master of Technology from School Of Information And Technology RGPV Bhopal in 2008. He is currently working as Assistant Professor in Department of CSE/IT,Madhav Institute Of Technology And Science Gwalior (M.P) since 2009. He has published more than 18 research papers in reputed international journals and conferences and it's also available online. His main research work focuses on Computer network, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, Image processing. He has 8 years of teaching experience and 6 years of Research Experience.

