ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

SURVEY REPORT

Available Online at www.ijarcs.info

A Survey on E-Payment using Quantum and Visual Cryptography

Anshu Arele
Department of CSE/IT
MITS , Gwalior
Gwalior (M.P.), India

Prof. Vikas Sejwar
Department of CSE/IT
MITS, Gwalior
Gwalior (M.P.), India

Abstract: In recent years, E-shopping obtained a huge growth because of its advantages. Advantages of E-shopping are comparison of prices, save time, save energy, save fuel, 24*7 availability ,high availability of merchandise, no need to waiting in lines, etc. If there are advantages there will be disadvantages like personally you can't check the item, diminished instant satisfaction. Also it creates some security threats such as debit, credit card fraud, phishing etc. Cryptography includes a procedure called encryption and it does not mean that using it we are hiding the information behind the image. Modern cryptographic technique include Quantum cryptography which uses quantum physics phenomena (particularly quantum coincidence and quantum retribution) to accomplish cryptographic errands or to disrupt encoded system.. Visual Cryptography generates shares to hide the customer details and image stenography protect the data with using OTP for secure the transmission. In this report, we have studies about E- Commerce that uses different-different cryptography algorithms e.g. XOR, NTRU etc.. Also discussed about how it secure the e-payment system.

Keywords: E-Payment system, Quantum, Visual cryptography, Stenography

I. INTRODUCTION

E-payment system is an alternative solution provided to user to have cashless transaction in returns to the services/purchase done. Simply we can say that e-payment is a device by which user can make Online Payments for his purchase of valuable items or services without physical transfer of cash and cheques, irrespective of time and location. It is the basis of on-line payments and on-line payment system development is a higher form of electronic payments. It makes electronic transaction available 24*7 using internet network to support e-commerce [1]. E-payment uses cryptographically signed promises/digital cash as trust. Using this validation of the authenticity and intention of payee-payment done. E-payment uses digital cash in place of physical currency and authenticate it using signature on digital cash. Digital cash as signed message does not contain any personal information about payee (anonymous transaction). In all terms it's secure and easiest way to have cashless transaction. [2].

II. TYPES OF E-PAYMENT SYSTEM

E-payment system ca be classified into six broad categories.

A. Credit cards

A Credit Based Payment card/ is a piece of plastic which have information that permit you to do purchase now pay for it later. Credit based cards/credit card of visa maser or any such service provider permit you to purchase or use services by the financial value from the credit provided by financial organization in the form of lending/Borrowing service, but merchandise from merchant who facilitates you to use credit card, now a days merchants has the swapping machine to make us buy things and pay using credit cards.

B. Debit Card

Debit card is based on pre-payment system and also famous by other name called ATM Card. Transaction via Debit card required account number in the same bank which issued it. Bank will provide you with a card with unique number and a secret pin Associated to it.whenever we will make any payment we will use that security pin to make transaction at the shop. When we swipe our card on machine at the shop it will use bank transaction system either Visa Service or Master Service to check the authentication and validity of card and its pin. In successful scenario where card information has been validated, transaction will be successful otherwise it's declined. Apart from authentication these transaction system will also check the banking details about balance and eligibility of account for this kind of service. The moment you will use the card and make payment it will be synched with your bank account i.e. credit/Debit transaction will be synched to your account in real time.

C. Smart card

Smart cards were firstly used in Europe known as stored value card. A smart card is almost of equal in size similar all other cards for example credit card, ATM Card. Smart card is based on microprocessor chip which in embedded in the card and hold personal information about the owner of the card along with financial constraint imposed by the bank which issue it. This chip is dynamic and get recharged periodically. This only keep the details about the cash and financial value.

The amount or the credit in card is make safer by having encryption and also by the security pin or password. To do payment by such smart card we are required to use a machine issued by bank and work on software controlled by bank and secured by keys issued by bank. Smart Cards can be recharged (credit) and terminated when required.

D. Digital Wallet (Electronic wallet)

They are very often used for making quick payment via internet e.g. many internet using devices like Personal Computers, Smartphones, Tablets etc. They offer a secure, convenient and portable tool for online shopping. They keep financial and personal details of the person such as cards, passwords, PINs and much more.

To support the E-payment processing several companies are using E-Wallet services. E Wallet permits one to keep an eye

on his billing and shipping details to ease the use of merchant site. E wallets can also keep e cheques, e cash and your card details for multiple cards.

E. Electronic Cheque

Electronic checks or digital checks have all the information which an ordinary checks consist. Use of digital technology make it easy to place digital signature in electronic checks and a certificate associated with it on order to have authentication with bank account. Number of websites are accepting Electronic Checks. It is easiest process to have electronic payment which work similar to paper checks and offer great security along with other features. It is commonly used for the payment processing of orders place online as a regular paper checks do. Sense of insecurity has been also taken care by placing digital signature and authentication measure while doing digital transactions.

F. Electronic cash

It remove third parties and financial organization as a mediator for having transaction between customers. It is directly transfer to respective stake holders i.e. Merchants vending machine. Its credit assigned to Smart card which is having embedded microprocessor chip. The chip will store cash value and user can avail it through secure payment gateway. Reconciliation of e-cash will be done easily without any problem as it basic feature of e-cash to have it or receive it from different banks. Typically transaction through e-cash happens from the customer to merchant's site. Transaction will not require any remote authorization or personal identification number at the time of transactions. [3].

III. SECURITY CRITERIA

A. Authority

Secure e-Payment require to validate the authenticity of parties involve in transaction.It is must have feature to make transaction safe from intruders and avoid unathorized transfer.

B. Privacy

The Objective of having this is to secure data that is sent over the internet.It is essential to have proper measures to safeguard the confidential data from unknown authority and hackers.

C. Integrity

Integrity is the assurance that the information is trustworthy.

D. Not be faked

In order to avoid security problems related to faked monies and signs.

E. Non-repudiation

Design of electronic payment system should be done in such a manner that parties involved cannot be able to ignore/deny their participation in the transaction. Therefore, records of details, such as the time of the transaction, the transactional information etc. must be kept in a secure database.

F. Anonymity

A condition in which an individual's identity is unknown [4].

IV. VISUAL CRYPTOGRAPHY

It is a technique of data encryption behind an image. It can be decrypted by person by decrypting the combined share. Share is nothing but a random pixel image which gives no information to an attacker about the data. Shares are generated by implementing visual cryptography algorithm. Leading techniques is Moni Naor and Adi Shamir, which was developed in 1940. Visual Cryptography creates two shares of same image, one will contains random pixel and other one consist of confidential information [5].

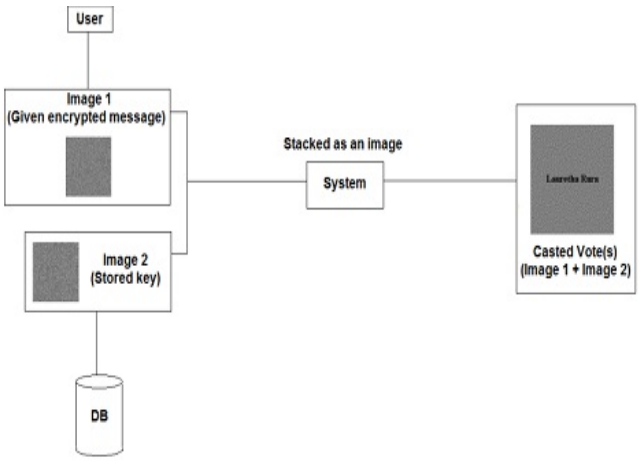

Fig. 1 DFD of how visual cryptography applied in the system

Visual Cryptography (VC) is a cryptographic technique based on visual secret sharing used for the encryption of image. Implementing k `out of n (k, n) visual secret sharing scheme, a redundant image is encrypted in share which can be send over any channel. It is only possible to get the original image by combining the k shares or more. [6].

A. Applications for visual cryptography

- Print and scan applications
- Human machine identification using visual cryptography.
- Visual cryptography authentication for data matrix code.
- Captcha
- Fingerprint based authentication
- Signature based authentication
- Sheltered iris attestation
- Offline QR code authorization
  A QR (Quick response) code is matrix barcode which is readable by specific readers dedicated to QR code .There are six important features of a QR code:
- High capacity encoding of data
- Chinese/Japanese (Kanji and Kana) capability
- Dirt and damage resistance
- Readable from any direction in 360 degree.
- A structure append feature

V. QUANTAM CRYPTOGRAPHY

It's a cryptographic technique based on quantum mechanics. It is the methodology where quantum mechanics fundamental are applied to implement the feature of quantum key distribution. Encrypted key distribution is not used for data transmission between users. Quantum states known as qubits is the basis for having encryption. Because of the concept of

relativity and uncertainty it is nearly impossible to measure and clone qubits. To implement this technique two channels, quantum channel required to transfer the key and classic channel for verification of key received. IDQ (quantum random number generator) adhere to the security by providing highly safe network and encrypted data during the transmission of data. IDQ has the capability of encrypting high data traffic which can up to 100 gb across various network e.g. local area, storage area. It can be later used as data back and recovery in case of any disaster happen and also for fully meshed global WAN networks for international operations. Quantum cryptography, or quantum key distribution (QKD), provides unconditionally secure communication. Security implemented uses concept of physics and has been tested successfully. If quantum security protocol has been followed properly it is nearly impossible to read the message from cipher. [7].

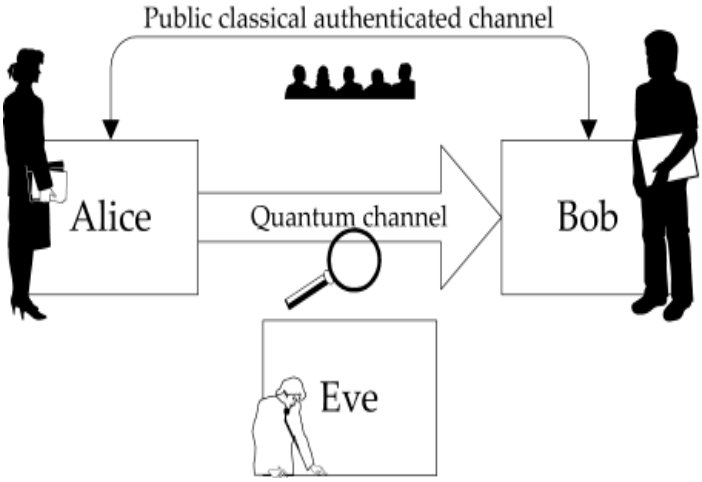

Fig. 2 Quantum cryptography

Quantum cryptography (QC) could be assumed as the very first commercial application built using quantum physics (qubits). Apart from quantum mechanics, the 20th century is known for two other major scientific revolutions: information theory and relativity. Encryption and decryption of data over the public network is handled by mutual authentication using key. Data is encrypted using the algorithm 'Key ‘and decryption of data can be only done by user having the access of same key. This method on encryption and decryption is called as Symmetric Key cryptography. There are several standard symmetric key algorithms defined.

A. Quantum Cryptography Applications:

- Key Agreement,
- Data Encryption,
- Digital Signature [8].

Quantum Cryptography is a method of sending secured information over various network system. These information are required in various organization including banking, secret services, military, business, scholastic instruction and research in various fields both in private and open System to work properly. Currently, Mathematical fundamental are applied for decoding and encoding data between parties. Hence, to utilize security assault with superior system hacker has to get the key and get the information in given period. Quantum cryptography works in such manner that utilization of polarization ensures that the information sent is not decoded by any interfering entity.

Quantum cryptography characterize the leverage of quantum mechanical properties (particularly quantum correspondence and quantum retribution) to accomplish cryptographic errands or to disrupt encoded systems. Understood specimens of quantum cryptography are the usage of quantum correspondence to securely interchange a key (QK dissemination) and the conjectural use of quantum machines that would permit the tearing of distinctive standard open key encryption and imprint arranges. The point of convergence of quantum cryptography exists in a way that it permits the realization of distinctive cryptographic assignments that are wound up being impossible using conventional (i.e. non-quantum) correspondence (see underneath for tests). Case in point, quantum mechanics promises that assessing quantum data disrupts that data. This can be utilize to perceive listening stealthily in quantum key movement [9].

VI. STEGNOGRAPHY

It is the method in which secret information is hide behind the other data so that it cannot be detected from human's casual eye contact. To achieve this two file will be required to embedding hidden message in another data.one will be the file which will hold hidden message known as cover media and the other one contain the data that is to be hidden. Steganography broadly classified in to text steganography, image steganography, video and audio steganography on the basis of cover media. Image steganography avail image as cover media and message can be hidden in bit stream. Combination of two known as stego-image [10].

Steganography is derived from Greek language which mean “Covered Writing”. The first implementation of steganography has been observed in Greece. They practices the message writing on wooden tablet and apply wax in to it to hide written data. It edges over cryptography as in steganography data can be hidden in the image. The Image will be sent via internet. It had advantage over cryptography as now the middle person does not come to know about the hidden data in the image. Data decryption from image can only be done by authorized person as he have the authorized key which is required to decode the data and also well versed with the method of decoding it. With the invention of Steganography security and reliability of transmission of data has been improved as now no other person could alter the sent data. [11]. This technique is implemented to have data security.

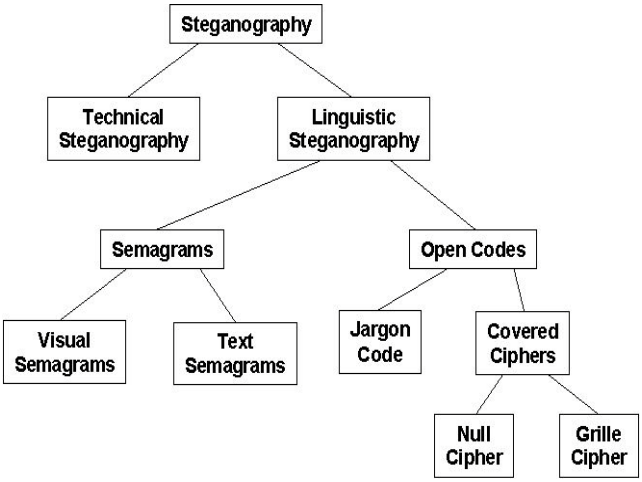

Fig 3 Types of Steganography

Steganography does not changes the structure of the secret message, it just hide the data inside a cover-object (carrier object). After the implementation of Steganography cover object and stego-object (carrying hidden information object) are similar. It implies that steganography (hiding information) and cryptography (protecting information) are totally different methodology. It's difficult to extract the hidden information without knowing technique and algorithms used in steganography. Detecting technique and alogoritham of steganography known as Steganalysis [12].

A. Application fields of steganography

The main application fields of steganography are [13]:

- Copyright Protection
- Feature Tagging
- Secret Communication
- Use by terrorists
- Digital Watermarking

B. Techniques for steganography

The various techniques for steganography is available. Some of them are as follows:

- LSB
- Distortion Technique
- Masking and Filtering
- Transform Domain Technique

C. Types of Steganography

1. Text steganography
2. Image steganography
3. Audio steganography
4. Video Steganography
5. Network or Protocol Steganography [14]

VII. RELATED WORK

s. no.	Author	Technique	Result	Problems
1	K.S.Seethalakshmi et. al [15]	visual cryptography and neural networks	High security and image quality. Secure transmission of image over the internet is achieved using visual cryptography.	Provide additional security using private or public keys during encryption
2	A.NANDHINIPREETHA et. al [16]	Visual cryptographic	Improve accuracy of the secured biometric system with finger vein and signature.	different fusion technique can be applied to enhance the performance of the model and also the number of shares can be expanded to enhance the verification level
3	Joyce Wenting Su et. al [17]	PCNP-WID3	Could identify the patterns of customer e-Payment adoption, and predict the potential customer adoption behavior.	the potential combination of PCNP and the other classification methods in various cases
4	D. Sam Sundar et. al [18]	cryptographic	An original method in which voting data is not stored in the voting machines but are transmitted in real time to an assigned secure location which has maximum security.	Quantum cryptography, building a successful encryption method using multivariate cryptography and in identifying loopholes in physical implementations of QKD systems.
5	Sreejitha Sasikumar et. al [19]	DNA	Cryptography, quantum cryptography and DNA based cryptograp	security is very fundamental and significant issues of data transmission

			hy. Information about technologies used in DNA is also provided here, such as PCR amplification	
6	K Suresh Babu et. al [20]	DWT	Steganography model Authentication of Secret Information in Image Steganography that can be used to verify the integrity of the secret message from the stego image.	Better performance viz., BER and PSNR than the earlier technique.

VIII. CONCLUSION

Many E-commerce systems for construction material procurement were developed to improve business process, to cut administration cost, and to provide more comprehensive information. Cryptography involves a process called encryption and is not concerned with hiding the secret data in the cover image. Here, we have studies and analysis of different cryptographic approaches for introduce an E-payment system that provides an unrivaled security using visual and quantum cryptography.

IX. REFERENCES

[1] . Mamta, Prof. Hariom Tyagi, Dr. Abhishek Shukla, The Study of Electronic Payment Systems", ISSN: 2277 128X/ Volume 6, Issue 7, July 2016

[2] . Paul J.M. Havinga, Gerard J.M. Smit, Arne Helme, "SURVEY OF ELECTRONIC PAYMENT METHODS AND SYSTEMS", http://doc.utwente.nl/18925/1/survey_havinga.pdf.

[3] . Karamjeet Kaur, Dr. Ashutosh Pathak, "E-Payment System on E-Commerce in India", ISSN : 2248-9622, Vol. 5, Issue 2, (Part -1) February 2015, pp.79-87

[4] . Shiva Zokaee,Seyed Babak Ebrahimi, Mostafa Ghazizadeh, "Electronic Payment Systems Evaluation: A Case Study in Iran", Vol. 4, No. 3, pp. 120-127, Mar 2012 (ISSN 2220-3796)

[5] . Nikita Chaudhari , Priya Parate, "Secure Online Payment System using Visual Cryptography", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 2, February 2016

[6] . Souvik Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science

[7] . Yi Zhao, **"**Quantum cryptography in real-life applications: assumptions and security", ACM Digital Library, University of Toronto , Ont., Canada, Canada ©2009 ISBN: 978-0-494-60903-3

[8] . Vijayalakshmi, C., Palaniammal, S. and ,Ramya, K., "Applications of Quantum Cryptography" , International Journal of Current Research Vol. 5, Issue, 01, pp.054-055, January, 2013

[9] . KostavChaudhuri, Tanya Singh, "Securing Networks using Quantum Cryptography", 978-1-4673-7231-2/15/$31.00 ©2015 IEEE

[10] . Shemin P A , Prof. Vipinkumar K S , "E – PAYMENT SYSTEM USING VISUAL AND QUANTUM CRYPTOGRAPHY" , International Conference on Emerging Trends in Engineering, Science and Technology(ICETEST - 2015), Procedia Technology 24 (2016) 1623 – 1628

[11] . Ashadeep Kaur, Rakesh Kumar, Kamaljeet Kainth, "Review Paper on Image Steganography" , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2016 ISSN: 2277 128X

[12] . Dr. Rajkumar L Biradar , Ambika Umashetty, "A Survey Paper on Steganography Techniques", International Journal of Innovative Research in Computer and Communication Engineering (A High Impact Factor, Monthly, Peer Reviewed Journal) Vol. 4, Issue 1, January 2016

[13] . R.Poornima, "AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY", (IJCSES) Vol.4, No.1,February 2013, pp 23-31

[14] . M.J.Thenmozhi , Dr.T.Menakadevi, "A New Secure Image Steganography Using Lsb And Spiht Based Compression Method", National Conference on Information, Communication, VLSI and Embedded systems (ICVE 2K16) (16 - 17 March 2016) International Journal of Engineering Research & Science (IJOER) ISSN: [2395-6992] [Vol-2, Issue-3 March- 2016

[15] . K.S.Seethalakshmi, Usha B A and Sangeetha K N, "Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography", 2016 International Conference on Computational Systems and Information Systems for Sustainable Solutions, 978-1-5090-1022-6/16/$31.00 ©2016 IEEE

[16] . A.NANDHINIPREETHA , N.RADHA, "Multimodal Biometric Template Authentication of Finger Vein and Signature Using Visual Cryptography", 2016 International Conference on Computer Communication and Informatics (ICCCI -2016), Jan. 07 – 09, 2016, Coimbatore, INDIA

[17] . Joyce Wenting Su , Kevin Kam Fung Yuen, "Towards A Hybrid Approach of Primitive Cognitive Network Process and Weighted Iterative Dichotomiser 3 for Customer E-payment Adoption Analysis",978-1-4799-4419-4 /14/$31.00 ©2014 IEEE

[18] . D. Sam Sundar , Nitin Narayan , "A novel voting scheme using quantum cryptography", 2014 IEEE Conference on Open Systems (ICOS), October 26-28, 2014, Subang, Malaysia

[19] . Sreejitha Sasikumar, P Karthigaikumar, "VLSI IMPLEMENTATION OF DNA CRYPTOGRAPHY USING QUANTUM KEY EXCHANGE", 2014 IEEE

[20] . K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, "Authentication of secret information in image steganography", IEEE Region 10 Conference, TENCON-2008, (2008) November, pp. 1-6.