DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4861

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ANALYSIS OF APPLICATIONS USING VISUAL SECRET SHARING FOR SECURITY

R. Shanmuga Priya
Research Scholar, Dept. of Computer Science
Tamil University, Thanjavur, Tamilnadu, India

A, Senthilkumar
Asst. Professor, Dept. of Computer Science,
Tamil University, Thanjavur, Tamilnadu, India

Abstract: Visual secret sharing is a technique in the science of visual cryptography, which is the emerging field in recent techno world for exchanging images safely. Despite each technology has its own strength and weakness too. This paper aimed to discuss, what are all the security application using visual secret sharing (VSS) available for recent emerging trends and its characteristics. It is quite tough task and this mission may help the researchers to develop information sharing effectively. VSS originally proposed by Moni Naor and Adi Shamir in 1994 and it was still developing and updated by the researchers for the recent trends. In VSS process an image was split into number of slices and shared to receiver. N images decrypt the original image and single share reveals nothing information, mostly this technique used in biometric process. Efficiency of this technique is how it is implemented in real world applications. This journal elaborates the applications which was used VSS for sharing images safely.

Keywords: visual secret sharing, applications of VSS, VSS security applications

I. INTRODUCTION

Dozens of cryptographic methods has been proposed for information security. However, it needs complex computing power for both decryption and encryption. Web has become the ultimate resource for sending and receiving from simple documents to top secret documents. There is a need in a modern e-commerce environment to share documents, images and secret keys both personally and for business[14]. With the help of visual cryptography the secret documents can be shared and revealed by human visual system[13]. The notable characteristic of VC schemes is less encryption coding and the decoding done by human visual system. Visual cryptography is a moderate security system which doesn't needs any complex computation[13]. Comparing with traditional cryptographic system, the traditional system needs more complex algorithm and many security leaks. This technique majorly applied for bio-information and authentication system in internet. Subsequent sections show the elaborate study on visual cryptography applied in various domains. In 1994, Naor and Shami proposed a new scheme called image secret sharing which divides a image into number of shares and original image requires threshold shares to reconstruct[1]. Visual cryptography was applied in many real world applications. Major of them will be described here. The paper is organized as follows: Section 2 the discussion of the authentication system using VC schemes. Section 3 illustrates the applications of bio-metric privacy and section 4 illustrates medication application using VC schemes. Section 5 discuses the Linguistic and Genetic algorithm applied in VC schemes and section 6 concludes the financial documents security using VC.

II. AUTHENTICATION SYSTEM

Authentication is the essential process for any application like banking, payment system and other applications. Online payment system is one of the major tasks for every online shopping websites. How it to be in a secured way? This is major question arises for every business sites. Visual cryptography is the best solution for such kind of process. Authors Souvik Roy and P. Venkateswaran, proposed a online payment system for e-commerce application[2]. In this paper secured payment system using VC via debit or credit card. They proposed a new method which is the combination VC and Text Steganography. In this method minimized sharing information and safeguarding customer from malpractices by the merchants. The proposed method specially designed for online shopping and can be extended for physical banking also. Encoding and decoding process done by vedic numeric code for English letters in which fixed word order and periphrases for hiding data[2]. Chetana Hegde and Manu S et al., proposed secured authentication system for core banking system using VC and image processing[3]. In this paper authenticity of customer during online transaction by signature, when customer application is received the sign stored in database. Shares are created based on bank account threshold like 2X2 , 3X2 and 3X3 based on personal account, joint account etc., Before shares created the signature pre-processed into light-shaded and improved intensity. In every transaction shares are printed and given to the customer. Both debit or credit transaction user produces the given share, and then it will be stacked with banks share to reconstruct the original. Afterwards retrieved imaged tested for correlation to found fake shares. When the original image is successfully retrieved the customer authentication is also successful. Authors Jaya and Siddharth Malik et al., proposed a novel authentication system using VC scheme in which signature used as a input image[4]. In this paper color image is used and this will helpful in physical banking system or credit card application. Advantage of the proposed system is, if the IC of the person is lost, it won't be misused. There is two shares created of customer image and signature, one share is printed on IC and another one is stored in banks database, shared to central authority. CA never closes any share to any others for any reason. There is two-level check that ensures the strong security and the presence of third party CA will enhance further security and the intruder cannot hack the share and single share reveals nothing.

III. BIO METRIC APPLICATION

VC plays vial role in biometric applications like biometric authentication, identification of consumers. Physiological characteristics are used to identify a person by the forms biometrics[5]. Biometrics takes major part in online transaction. Fingerprints, iris code and face images etc., are the examples of biometrics. Digital biometrics dumped in a central database and will be compared in transaction. Authors Rajeswari Mukeshi and V.J.Subashini[5], proposed fingerprint based authentication using VC technique. In this paper they proposed threshold authentication technique, in which fingerprint of the customer is divided into n shares. A dummy share is compressed associated with customer ID card and rest n-1 shares are stored in the database. When the transaction process the dummy share retrieved from the customer and will be minutiae. The minutiae will be compared with n-1 shares minutiae. If the result found then the customer will be authenticated. False rate will be less than 0.2% by this method. Another interesting paper by the authors Sowmya Suryadevara and Rohaila Naaz et al., tongue as a biometric for identification of a person[6]. Tongue has unique pattern that potentially useful in application. With the help of VC they proposed tongue as authentication system for banking application. High resolution digital camera is used to capture customers tongue and stored along with CIN code in banks database. When the customer wants to made transaction like in ATM, tongue will be captured by the digital camera and gets CIN code[6]. Captured information processed with banks database with VC techniques. Authors Arun Ross, Senior Member, IEEE, and Asem Othman [7], proposed biometric privacy using visual cryptography. In this paper face images are the biometric concern. The idea is hiding a face image into two host face images and IMM database used for experiments. Original image will be reconstructed from the successful matching shares. Two shares will be created and original image will be reconstructed by decomposing two shares simultaneously.

IV. MEDICATION APPLICATION

Medical documents need considerable concern in modern exchanging information. Nowadays medical documents like X-Rays, scan documents and other patient details are exchanging worldwide for treatment and other things. This particular area needs more security to protect patient's privacy. VC plays major role in this domain and this area shows how to handle such challenging task like storing and transmitting patient medical images. There are much more issues while sharing patient's medical details. This section not covers all of them and very few of them are illustrated. Authors Rajendra Basavegowda and Sheshadri Seenappa [8], proposed electronic medical security using VC sharing schemes. They proposed a VC scheme for black and white images such as CT scan, X-Ray, MRI-Scan and ultrasound. Two out of two shares are generated with black and white pixel and single share reveals nothing information[8]. If two shares overlaid then the secret information will be retrieved. And this technique will be useful in secret sharing of electronic medical information. Keeping patient's confidentiality will be safe by this approach. Each share has the key and communicated separate channel, if any hacker or intruder tries to get the detail, they get single share only. Authorized hospital personnel have the key and will get the original image. Authors Mustafa Ulutas, Güzin Ulutas and Vasif V. Nabiyev [9], proposed security of electronic patients record and medical images using Shamir's secret sharing method[1]. In this paper they proposed (k,n) secret sharing scheme for medical images for in secured network communication, although it is crucial in medical security[9]. The criteria of this method is hidden clinical images will reduce the storage and bandwidth requirements considerably. Shares look like a natural image and it doesn't attacker any intruder or hacker. It doesn't allow any single person to reveal secret information political person or higher official in defense. And the authenticated recipients could receive the unmodified shares. There is two phases in retrieving phase namely verification and reconstruction. Verification phase checks the shares weather it is real or damaged and reconstruction phase has the Lagrange's interpolation method to reveal the original image, while the sharing phase has the built-in authentication.

V. LINGUISTIC AND GENETIC APPLICATION

Linguistic is another and emerging major field. With help VC schemes all domains getting new look. Authors Marek R. Ogiela and Urszula Ogiela, proposed mathematical linguistic methods using secret sharing threshold algorithms[10]. In this paper context free grammar used and input information converted into bit sequence. A general pattern of grammar illustrated and bit or block positions are generated for shared information. Then the bit sequence will parsed using grammar analyzer that is already defined. Sequence of grammar rules generated by the parser that allows shared secret in the form of bit representation and the number of shares represented by selecting threshold level. Shares distributed particular participants and this may called linguistic secret splitting, although the security of this approach is mathematical methods used for splitting information. Complexity level of the entire process remains multinomial and this method is also applicable for DNA cryptographic[10]. Genetic algorithm and VC is another emerging area for secure data transmission over internet and other networks. Authors Mrs.G.Prema and S.Natarajan [11], proposed Genetic algorithm along VC scheme in wireless network application. In this paper LSB based steganography with Genetic algorithm along and Visual cryptography. Hiding information in input image using LSB technique and pixel modified by genetic algorithm, then the shares are generated. With the power of LSB low computation and high capacity this will be strong one[11]. The proposed work has two algorithms. One is stegenography and another one visual cryptography. When the first process is completed the output is steago image then the second process splits the steago image into secret shares. The performance of this approach is measured by means of Mean Squared Error (MSE)[11].

VI. FINANCIAL DOCUMENTS

Another major security application in visual cryptography is sharing of financial documents. Where moderate security eases the sharing is threshold and original[12]. Thus the techniques are not adequate of financial documents sharing over the internet. Authors L. W. Hawkes and A. Yasinsac, C. Cline [12], proposed an application for sharing financial documents using VC schemes. VCRYPT, a window application solves the hectic problem and produce a crisp, clear and original document. The scheme that was proposed reduces the storage and transmission time. VCRYPT overcomes the limitation that was existing in the past VC schemes, particularly pixel expansion to overcome this a post-receipt threshold filtering command was added. The GUI is very user friendly with multiple document interfaces for separate actions like encoding and decoding. Since the natural file format Bitmap was used in the application. There two Boolean

matrices used for encode the source image into n shares. One is for black pixel and another one is for white pixel. The decoding process is done by two processes. One is overlay the shares and another one is filtering process for result image. Bitwise AND process is used for overlay of shares and by looking sub-pixel for filtering to represent the original[12]. Greying effect won't allow VC schemes are not an alternate for Cryptography. The system was tested with 640X480 pixels and 1280X960 pixels which show the adequate result.

VII. CONCLUSION

This study is an overview of the Visual cryptography application along with security concern in major domains, particularly enhancing security in real time application like e-commerce and biometrics. This publication is very helpful those users who want to develop a modern security system in any application with the help VC schemes. This mission is not only shows the applications of VC, it also reveals the simplicity and power. It distinguishes the secrete of VC and how it to be used in various domains. Authentication system and threshold level shows the level of authentication. There is tons of application which uses VC schemes for security and other concern and this paper not cover all of it like Electronic balloting system and others. This will be concluded Steganography and VC is an emerging field which gives moderate security.

VIII.REFERENCE

[1] 1. M. Naor and A. Shamir, .Visual Cryptography,. Advances in Cryptography -EUROCRYPT'94, Lecture Notes in Computer Science 950, 1995, pp. 1-12.

[2] 2. Souvik Roy1 and P. Venkateswaran2, Online Payment System using Steganography and Visual Cryptography, 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science 978-1-4799-2526-1/14/$31.00 ©2014 IEEE

[3] 3. Chetana Hegde and Manu S et al., Secure Authentication using Image Processing and Visual Cryptography for Banking Applications, Defence Institute of Advanced Technology, Deemed University, Pune, India

[4] 4. Jaya and Siddharth et al., Novel Authentication System Using Visual Cryptography, 2011 World Congress on Information and Communication Technologies

[5] 5. Rajeswari Mukeshi and V.J.Subashini2, Fingerprint Based Authentication System Using Threshold Visual Cryptographic Technique, IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[6] 6. Sowmya Suryadevara and Rohaila Naaz et al., Visual Cryptography Improvises the Security of Tongue as a Biometric in Banking System, International Conference on Computer & Communication Technology (ICCCT)-2011

[7] 7 Arun Ross, Senior Member, IEEE, and Asem Othman, Student Member, IEEE, Visual Cryptography for Biometric Privacy, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 1, MARCH 2011

[8] 8. Rajendra Basavegowda and Sheshadri Seenappa, Electronic Medical Report Security Using Visual Secret Sharing Scheme, 2013 UKSim 15th International Conference on Computer Modelling and Simulation

[9] 9. Mustafa Ulutas, Güzin Ulutas∗, Vasif V. Nabiyev, Medical image security and EPR hiding using Shamir's secret sharing scheme, The Journal of Systems and Software 84 (2011) 341–353

[10] 10 Marek R. Ogiela and Urszula Ogiela, The use of mathematical linguistic methods in creating secret sharing threshold algorithms, Computers and Mathematics with Applications 60 (2010) 267_271

[11] 11 Mrs.G.Prema and S.Natarajan, Steganography using Genetic Algorithm along with Visual Cryptography for Wireless Network Application.

[12] 12. L. W. Hawkes, A. Yasinsac, C. Cline, An Application of Visual Cryptography To Financial Documents, Security and Assurance in Information Technology Laboratory, Computer Science Department, Florida State University

[13] Shruti M. Rakhunde and Manisha Gedam, Survey on Visual Cryptography: Techniques, Advantages and applications, IOSR Journal of Computer Engineering (IOSR-JCE), PP 06-12

[14] Jen-Bang Fenga, Hsien-Chu Wub,∗, Chwei-Shyong Tsaic, Ya-Fen Changb, Yen-Ping Chud, Visual secret sharing for multiple secrets, Elsevier