International Journal of Research in Science advanced Technology and management studies (IJRSTMS)

ISSN: 2459-425X • Website: www.ijrstms.com

Survey Paper On Utilizing Visual Cryptography For Secure Bank Transaction

Prof.S.M. Prasad
Computer Engineering. Jspm's Rajarshi Shahu
College of Engineering Pune ,India

ABSTRACT

Security has become the most important aspect in today's banking transaction system because banks are committed to provide secure core banking services to their customers. To achieve this goal authenticity of the users is required only the authorized users can take part in the transaction.For that purpose banks uses Biometric based authentication systems but due to unavoidable malicious activities database of the banking system is no longer secure. Smart hackers can fetch biometric details of customers from the bank's database and later can use it for fake transactions. To avoid all this catastrophic things Visual cryptographic technique along with AES algorithem is used. Visual Cryptography is a cryptographic technique which allows information to be in encrypted form in such way that decrypted infromation as a visual image. In this paper we propose a secure XOR operation based visual cryptography along with AES algorithem and image processing technique to secure banking transaction.

Keywords— Steganography, Security, Visual Cryptography, Performance**.**

I. INTRODUCTION

Most of applications are just as secure as their fundamental framework. Since the outline and innovation of middleware has enhanced relentlessly, their discovery is a difficult issue. Therefore, it is almost difficult no doubt regardless of whether a PC that is associated with the web can be viewed as dependable and secure or not. The inquiry is the means by which to deal with applications that require an abnormal state of security, for example, center saving money and web managing an account.In the Net banking system,It is the chance of password of customer may be hacked and misused. Thus security is still a challenge in these applications.Hence Here we are propose a technique to secure the customer information and to prevent the possible forgery of signatures and password hacking. Picture handling is a procedure of preparing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. Visual Cryptography (VC) is a technique of encoding a secret image into shares with the end goal that stacking an adequate number of shares uncovers the secret image. Steganography techniques is a data hidden within data. is is an encryption technique that can be used along with the cryptography as an extra secure transcation in which to protect the data. this technique can be applied to images,a video file or an audio file.In the AES encryption Algorithm cipher is substitution of data using a substitution table the second transformation shifts data rows, the third mixes columns. The last

transformation is a simple XOR operation performed on each column using a different part of the encryption key longer keys need more rounds to complete.

II. LITERATURE SURVEY

Aaditya Jain, Sourabh Soni, [1] have represented Banks uses Biometrics based authentication systems but due to unavoidable malicious activities database of the banking system is no longer secure. Smart hackers can fetch biometric details of customers from the bank's database and later can use it for fake transactions. To avoid all this catastrophic things Visual cryptographic technique is used. Visual Cryptography is an efficient encryption scheme in which information hide inside the images and decrypted only by human visual system.

Velumurugan Andi and Logashanmugam Edeswaran [2] Transmitting the image in defined manner using the visual cryptography , steganography technique as well as AES encryption. Share one is embedded with Least Significant Bit (LSB) on cover sheet. AES is used for encryption of embedded image using the cipher key. Cipher key is generated using DCT (Discrete Cipher Transform)

Jitendra Saturwar, D.N. Chaudhari, [3] An image watermarking model based on progressive visual cryptography is propose dto decide optimal number of shares. A study on implementation of meaningful shares in combination with visual cryptography scheme for secret images is carried out for implementation of algorithm.

Velumurugan Andi and Logashanmugam Edeswaran [4] Transmitting the image in defined manner using the visual cryptography , steganography technique as well as AES encryption. Share one is embedded with Least Significant Bit (LSB) on cover sheet. AES is used for encryption of embedded image using the cipher key. Cipher key is generated using DCT (Discrete Cipher Transform).

Abul Hasnat, Dibyendu Barman, Satyendra Nath Mandal, [5] Number of parts is generated from one image. The parts are sent to the receiver and receiver reconstructs the original image by stacking all the share images. Generation of parts is different for different types of binary, gray and color images. K out of K visual cryptography scheme by Naor and Shamir is a well known visual cryptography algorithm.

Nagham Hamid, Abid Yahya, R. Badlishah Ahmad,Osamah M.Al Qershi,"Image Steganography Techniques: An Overview", [6] An agent to send secret information using steganographic techniques, he or must select a suitable steganographic algorithm and suitable cover image as well.The required application is the only thing to decide the most appropriate steganographic method among all the present image steganographic techniques.

Zhili Zhou, Ching-Nung Yang, "Secret Image Sharing based on Encrypted Pixels", [7] Because all coefficients of (k1)-degree polynomial are used for embedding secret image pixels and permutation-only ciphers are insecure, in all of the existing (k, n)-SIS schemes, one may recover some partial secret pixels from (k1) shadows. Thus, the threshold properties of those

schemes are compromised. In this paper, we address this weakness, and propose a (k, n)-SIS scheme based on encrypted pixels.

Praveen K, Sethumadhavan M, On the extension of XOR step construction for optimal contrast grey level visual cryptography", [8] The proposed XOR step construction of VCS for grey level images is vulnerable to collusive cheating attacks, but APE and Relative contrast of our scheme is better when compared to other grey level VCS. We have also designed a cheating immune step construction for VCS applicable to grey level images by modifying Liu et al. scheme, which mitigate collusive attacks by disclosing some number of pixels in the secret image to public.

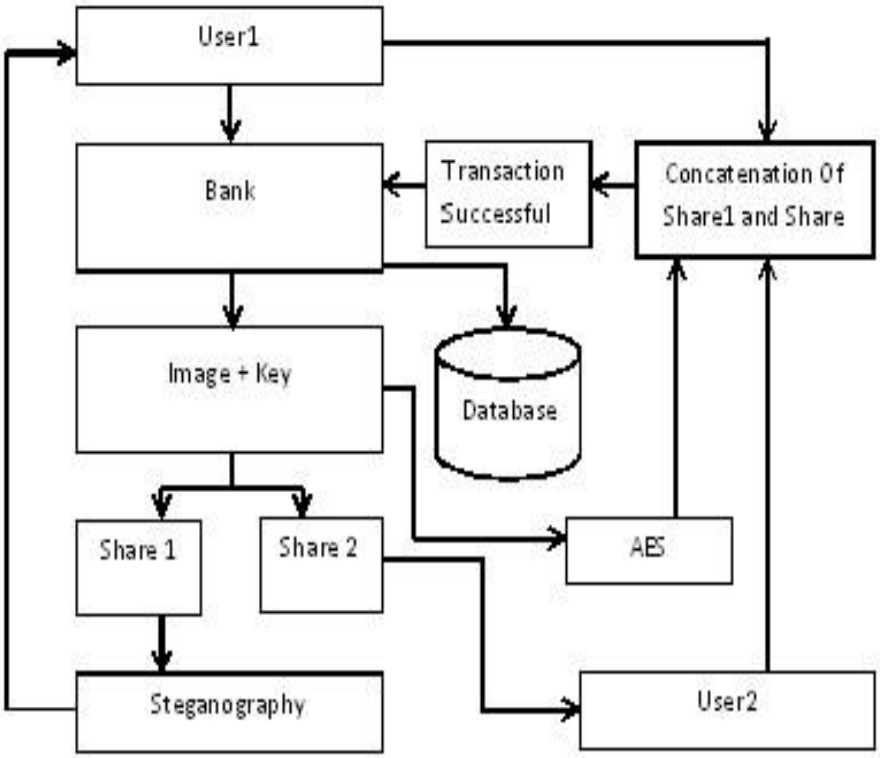
Dana Yang, Inshil Doh, Kijoon Chae, "Enhanced Password Processing Scheme Based on Visual Cryptography and OCR", [9] Numerous individuals utilize the equivalent or short length of passwords in different frameworks and are careless secret phrase administration. Importantly digital mishaps are happened regularly. We proposed a particular technique unique in relation to customary secret key plan. It depends on encoded pictures by VC with a SEED number and OCR and more solid assurance from digital assaults.

Peng Meng,Liusheng Hang Yang1, Zhili Chen'r', Kijoon Chae,"ATTACKSON TRANSLATION BASED STEGANOGRAPHY", [10] Interpretation Based Steganography is a sort of popular content steganography. In this paper we analyze the vigor of TBS and give a powerful location calculation for TBS. Our calculation can not just recognize regular dialect content and stego- content which was produced by TBS, yet in addition can recognize machine Deciphered content and stego-content.

III. SYSTEM ARCHITECTURE

We design a new concept called Secure Transaction in the Bank for Optimal Performance and Security that collectively approaches the security and performance issues. The proposed scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker. Banking system provides the facility of having joint account and operates jointly or individually. In case of individual operation it does not mean to have joint account but it provides flexibility to the members of joint account to operate individually. In some cases socially it is not secure. Suppose A and B have joint account and at later time A gets adverse to B and wish to withdraw all the money from the account. In this case B is cheated by A. In the proposed method it is ensure that transaction is only possible when both the users are available. It also ensure that nobody can misuse the information stored in the database because Shares are random noise like images and nobody can get any clue from a single share even he apply enormous amount of computing power and time. In the proposed method gray images of both the user are taken as input and processed for further use. Proposed system uses visual crptography for image encryption with AES algorithm for encrypt with cipher key. Cipher key generated using DCT technique. Encrypt image using least significant bit.

ISSN: 2459-425X • Website: www.ijrstms.com



Dig .Architecture Digram

In this method original image is secured by decomposing it into n shares. Mainly focuses on issues related to the identity theft and customers data security in the joint account transaction. For secure Banking Transaction in joint account operation this paper proposed a method that is based on (2, 2)-VCSXOR. Experimental results show that reconstructed secret image is same in size and quality of the original secret image. AES Algorithm is used for encryption using cipher key which is generated using descrete cipher transform. Comparison to other banking application which uses steganography and visual cryptography are basically applied for physical banking, but the method can be applied for E-Commerce and mostly it will focus on payment during online as well as physical banking.

V.CONCLUSION

The visual cryptography along with aes algorithem is a secret sharing scheme.In this method original imaged is secured with key and decomposing into n scheme.This paper proposed for better security provided to identity theft and customers data in the joint account transaction. For secure banking transcation in joint account operation this paper proposed better way to secure banking transaction using (2,2)-VCSxor method and Aes Algorithem

VI .REFERENCES

[1] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi, "Image Steganography Techniques: An Overview," International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012.

[2] Aaditya Jain, Sourabh Soni, "Visual Cryptography and Image Processing Based Approach for Secure Transactions in Banking Sector," 2017 2nd International Conference on Telecommunication and Networks (TEL-NET) 2017.

[3] Jitendra Saturwar, D.N. Chaudhari, "Secure Visual Secret Sharing Scheme for Color Images Using Visual Cryptography and Digital Watermarking," IEEE Transactions on Cloud Computing,Vol. 1, No. 1, 2013.

[4] Velumurugan Andi and Logashanmugam Edeswaran, "An efficient steganography algorithm using visual cryptography and AES encryption" , IIOABJ, 2016

[5] Yuqiao Cheng, Zhengxin Fu, Bin Yu, "Improved Visual Secret Sharing Scheme for QR Code Applications," IEEE Transactions, 2018.

[6] H. Wang and S. Wang, ―Cyber warfare Steganography vs. Steganalysis,‖ Commun. ACM, vol. 47, no. 10, pp. 76-82, 2004.

[7] Dai, Yin, and Xin Wang. "Medical image encryption based on a composition of Logistic Maps and Chebyshev Maps." Proceedings of International Conference on Information and Automation (lClA), 2012, pp. 210-214.

[8] J. Chen, T. S. Chen, M. W. Cheng, "A New Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on Multimedia Software Engineering, pp. 8893, 2003.

[9] Y.-C. Chen, "Fully incrementing visual cryptography from a succinct non-monotonic structure," *IEEE Trans. Inf. Forensics Security*, vol. 12,no. 5, pp. 1082–1091, May 2017.

[10] Jaishri Chourasia, "Identification and authentication using visual cryptography based finger print watermarking over natural image", Springer, December 2013, pp.343-348.