International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Survey Paper on Utilizing Visual Cryptography for Secure Bank Transaction

Vaishali.D.Shinde[1], Avinash Nagul[2], Pooja More[3], Sharayu Sawant[4], Jyoti Sawant[5]

[1]Assistant Professor, Computer Engineering. JSPM's Rajarshi Shahu, College of Engineering, Pune, India

[2, 3, 4, 5]Computer Engineering, JSPM's Rajrshi 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 i.e. only the authorized users can take part in the transaction. Regarding this purpose 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 along with Aes algorithm is used. Visual Cryptography is an efficient encryption scheme in which information hide inside the images and decrypted only by human visual system. In this paper we propose a secure XOR operation based visual cryptography along with Aes algorithm and image processing technique to secure banking transaction.***

Keywords: Steganography, Security, Visual Cryptography, Performance

1. Introduction

Most 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 Banking system there is a chance of encountering forged signature for transaction and net banking system the password of customer may be hacked and misused. Thus security is still a challenge in these applications. Here we propose a Aes 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 technique on the other hand this technique hide the existence of the message itself, which makes it difficult for an observer to figure out where the message is.In AES Algorithmdata stored in an array and number of transformation is stored. The first step of the cipher is to put the data into an array; after which the cipher transformations are repeated over a number of encryption rounds with key. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys using AES Algorithem.

2. 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.AlQershi,"Image Steganography Techniques: An

Overview", [6] An agent to sendsecret information using steganographic techniques, he or must select a suitablesteganographic algorithm and suitable cover imageas well.The required applicationis the only thing to decide the most appropriate steganographic method among allthe 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 forembedding secret image pixels and permutation-only ciphers are insecure, in all ofthe existing (k, n)-SIS schemes, one may recover some partial secret pixels from(k1) shadows. Thus, the threshold properties of those schemes are compromised. Inthis paper, we address this weakness, and propose a (k, n)-SIS scheme basedon encrypted pixels.

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

Dana Yang, Inshil Doh, Kijoon Chae, "Enhanced Password Processing SchemeBased on Visual Cryptography and OCR", [9] Numerous individuals utilize theequivalent or short length of passwords in different frameworks and are carelesssecret phrase administration. Importantly digital mishaps are happened regularly.We proposed a particular technique unique in relation to customary secret keyplan. It depends on encoded pictures by VC with a SEED number and OCR andmore 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. Inthis paper we analyze the vigor of TBS and give a powerful location calculation forTBS. 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.

3. Proposed Methodology

A) Software Requirements
Database Requirements- Database MySql
Software Requirement – Java Tool Eclips
Programming Languages –Java /J2EE
Software Version –JDK 1.7 or above
Database Tools –MySql Query Browser
Front End –JSP

B) Hardware Requirements
Processor - Pentium IV/Intel I3 core
Speed -1.1GHz
RAM-512 MB
Hard Disk-5GB

3.1 System Architecture

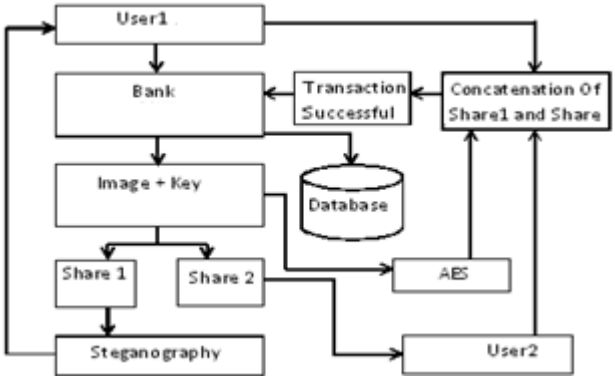


Figure 1: System Architecture

3.2 System Working

3.3 Algorithm

AES Algorithm
STEP1:
Sub Bytes for byte- by- byte substitution during the forward process. The corresponding substitution step used during decryption is called Inv SubByte.

This step consists of using a 16 16 lookup table to find a replacement byte for a given byte in the input state array.

The entries in the lookup table are created by using the notions of multiplicative inverses in and bit scrambling to destroy the bit-level correlations inside each byte.

STEP 2:
Called Shift Rows for shifting the rows of the state array during the forward process. The corresponding Mix Columns Shift Rows Substitute Bytes In- verse Mix Columns Add Round Key Inverse Shift Rows Inverse Substitute Bytes Round Key Round Key Encryption Round Decryption Round .

One round of encryption is shown at left and one round of decryption at right. 16 Computer and Network Security by during decryption is denoted InvShiftRows for Inverse ShiftRow .

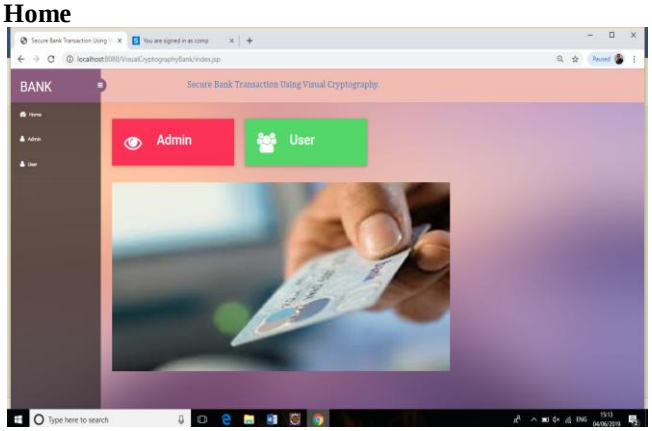
STEP 3:
Mix Columns for mixing up of the bytes in each column separately during the forward process. The corresponding transformation during decryption is denoted InvMixColumns and stands for inverse mix column transformation. The goal is to further to secure image with the 128-bit input block. The shift-rows step along with the mix-column step causes each bit of the cipher text to depend on every bit of the plaintext after 10 rounds of processing. In DES, one bit of plaintext affected roughly 31 bits of cipher text. But now we want each bit of the plaintext to affect every bit position of the cipher text block of 128bits.

STEP 4:

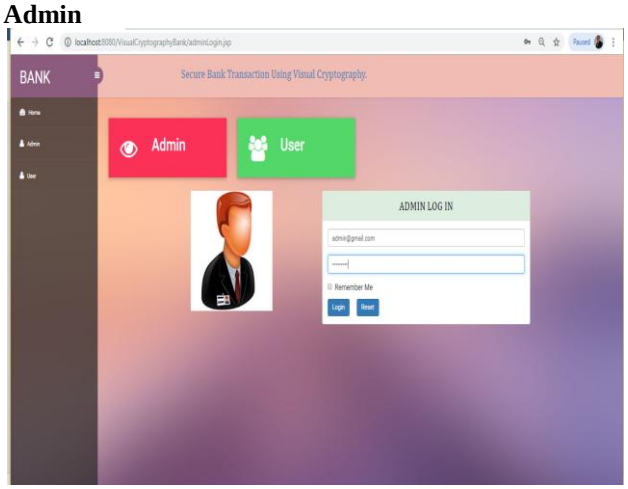
Add Round Key for adding the round key to the out\put of the previous step during the forward process. The corresponding step during decryption.

4. Expiremental Results

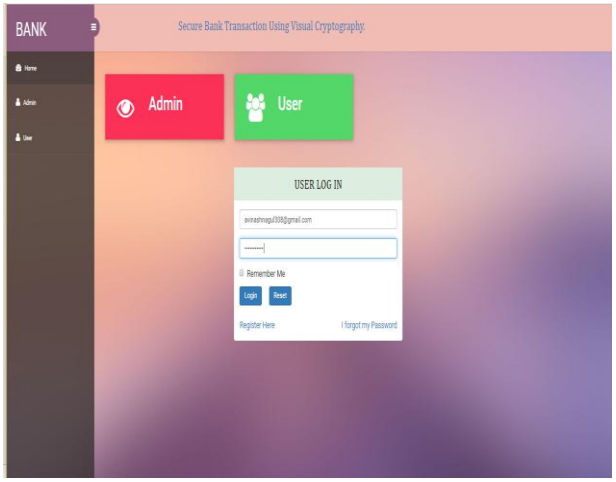
Home



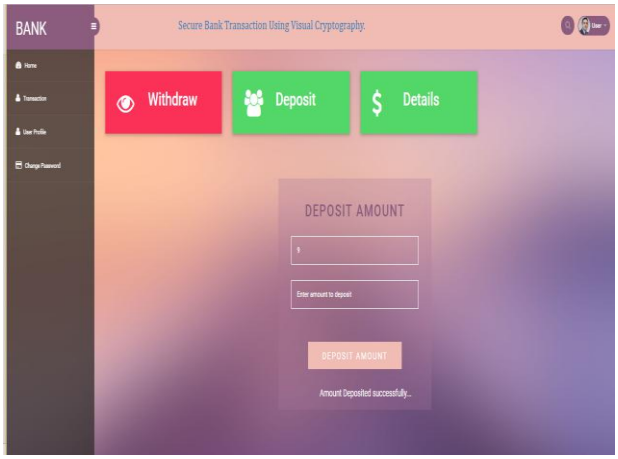
Admin



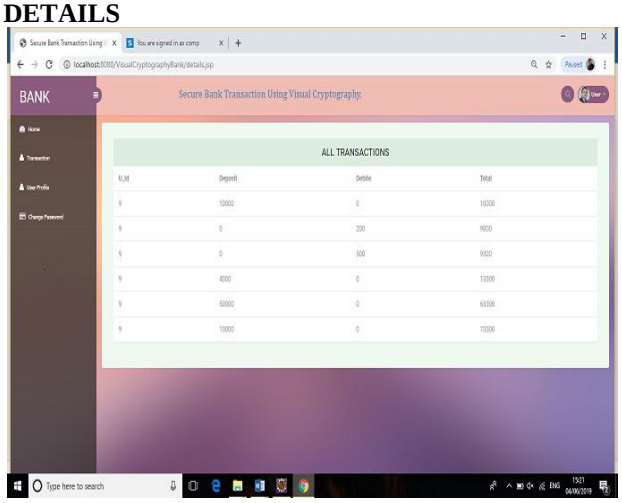
USER



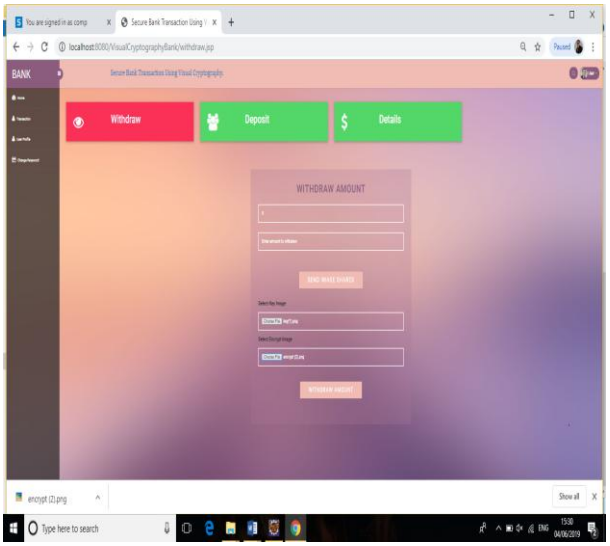
DEPOSITE



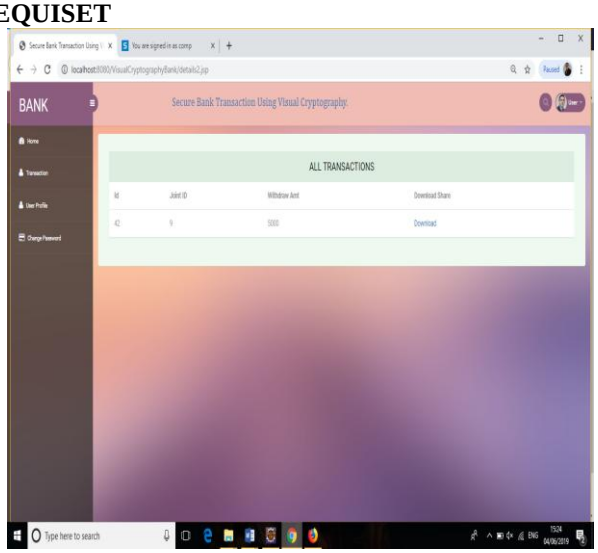
DETAILS



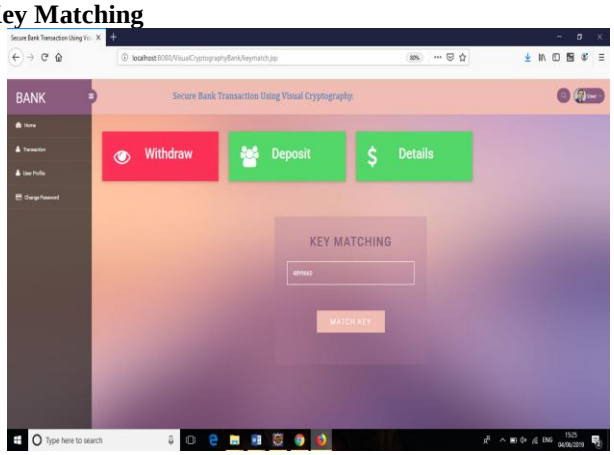
WITHDROW



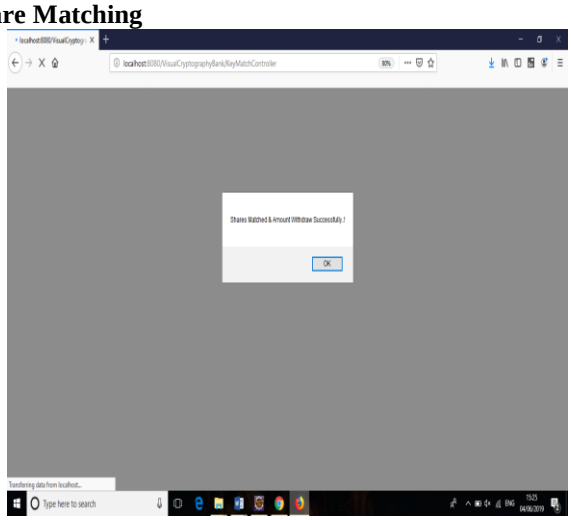
REQUISET



Key Matching



Share Matching



5. 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

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,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 Chin ya"Medical image encryption based on a composition of Logistic Maps." Proceedings of International Conference on Information and Automation (lClA), 2012, pp. 210-214.
[8] J. Chen, T. S. Chen, M. W. Cheng, Visal cryptography Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on Multimedia Software Engineering, pp. 88-93, 2003.
[9] Chen, "Fully incrementing visual cryptography with Aes from a succinct non-monotonic structure,"May 2017.
[10] Jaishri Chourasia, "Identification and authentication using visual cryptography based finger print watermarking over natural image", Springer, December 2013, pp.343-348.