Mobile Banking App Using Visual Cryptograpy And Steganography

[1]Sejal krishna Gajbhiye, [2]Pooja Gedam, [3]Lavanya Gannamani, [4]Mrunal Deshmukh

[1,2,3,4]Students of B.E.
Gajbhiye Gedam Gannamani Deshmukh Manapure
Student B.E. (CSE),
G.H.R.I.E.T, Nagpur

***Abstract*: Web application security has become an important concern for every user. This project implements a secure transaction platform that helps users to make secure bank transactions. In the communication between bank and merchant, every time merchant must be verified to prevent fraudulent transactions.**

In this project, the Steganography and visual Cryptography technique approach on image processing with the help of Mobile Phones is used to authenticate customer. The technique of embedding information of customer, subjecting it to an image, and generating shares of that particular image is used. Image shares are components of the original image so that any one share (on its own) does not reveal anything about the original image.

Only if you have all of the shares can you determine the secret image. One share is given to the merchant server and other share is kept with bank database. The customer has to provide the share during all the transaction. This share is stacked with the first share for the process of authentication. This project is an implementation of online fraud prevention using secure authentication process, visual cryptography and steganography.

I. INTRODUCTION

Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. The question is how to handle applications that require a high level of security, such as core banking and internet banking. In a core banking system, there is a chance of encountering forged signature for transaction. And in the 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 technique to secure the customer information and to prevent the possible forgery of signatures and password hacking.

The concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing 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 the method of encrypting a secret key into shares such that, stacking a sufficient number of shares reveals the secret key.

Naor and Shamir introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, termed as Visual Cryptography Scheme (VCS). Basically, Visual Cryptography Scheme is an encryption method that uses combinatorial techniques to encode secret written materials. The idea is to convert the written material into an image and encode this image into n shadow images. The decoding requires only selecting some subset of these n images, making transparencies of them, and stacking them on top of each other. The simplest Visual Cryptography Scheme is given by the following setup. A secret image consists of a collection of black and white pixels where each pixel is treated independently. To encode the secret image, we split the original image into n modified versions (referred as shares) such that each pixel in a share now subdivides into n black and white sub-pixels. To decode the image, a subset S of those n shares are picked and copied on separate transparencies. If S is a qualified subset, then stacking all these transparencies will allow visual recovery of the secret.

II. OBJECTIVE

User should enter a secret key. Before entering a secret key user should be select an Image. Encrypt the entered key. Encrypted secret key should be embedded with a selected image. Image should be divided into two share.One share should be downloadable and other should be stored into bank database. At the time of authentication, User should enter a share of image.Share entered through user should be merged with share in database.Key should be retrieved and treated as Transaction key.

III. RELATED WORK

A related work in area of banking security based on steganography and visual cryptography. Above both systems used to minimize information sharing between consumer and online merchant and enable fund transfer from customer account to merchant account and no misuse of data. In existing system there is no guarantee of getting authentication of data.

[1]It has presented a novel system for data and image encryption using AES algorithm for cryptography, image steganography and image stitching which can be used by banking, consultancies and detective agencies. As the image to be sent is broken down into parts and encrypted individually and sent over the network it becomes difficult of the intruder to get access of all the parts. Additionally since every part is camouflaged by a cover image, the encrypted image looks like just another regular image.

[2] While creating an account the bank, signature of the applicant is taken by scanning his/her signature from the application. Now the scanned image is taken as input and is pre-processed. This pre-processed image to encrypt into two share by using two out of two scheme. One share is stored in the bank database, another share is printed and given to the applicant. Applicant had to provide his share during every transaction. During transaction applicants share is scanned and overlapped with the banks share, if higher correlation coefficient is obtained, then authentication will be success.

[3] A payment system for online shopping is proposed by combining text based steganography and visual cryptography that provides customers data privacy and prevents misuse of data at merchant's side. The method is concern only with prevention of identity theft and customer data security. In comparison to other banking application which uses steganography and visual cryptography are basically applied for physical banking, the proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking.

[4] It have proposed an effective technique to provide greater security in the field of Internet banking system by restricting the unauthorized user. To verify the same by giving note or image will be broke into two parts and one will have buyer another will have seller, after meeting they need check it if it matches then item and money will be exchanged otherwise not. Based on this concept we did this application. Its useful to customers, website holders and banks. Image will divided, first half send to customer and second half of image will be kept in bank server. In future enhancement this can be extended to signatures. Here image are taken as inputs since they are uniquely Identified, but according to the user and bank convenience any kind of images can also be used like signature image of the applicant.

[5] there are many techniques and methodologies applied for watermarking of images. In this paper, method to perform secure authentication using captcha image is discussed. The user has to generate image of the unique id and send to the server. Then watermarking techniques are used to check the re-captcha image and checks for authenticity.

IV. PROPOSED METHODOLOGY

In a core banking system, there is a chance of encountering forged signature for transaction. In the 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 technique to secure the customer information and to prevent the possible forgery of signatures and password hacking.

System Architecture:

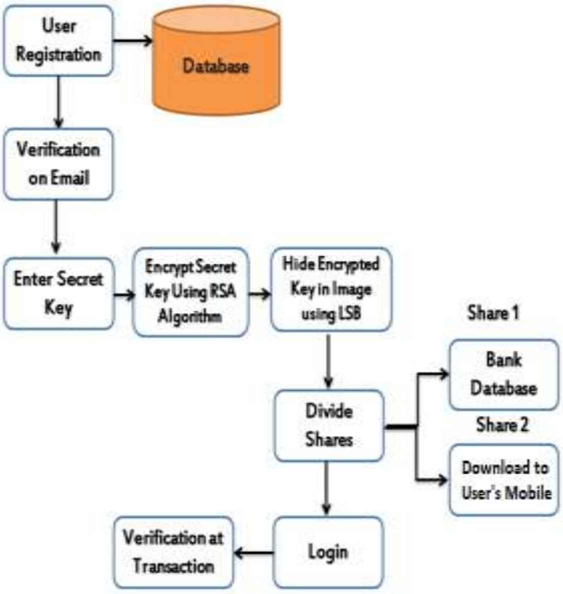

User Registration
Database
Verification on Email
Enter Secret Key
Encrypt Secret Key Using RSA Algorithm
Hide Encrypted Key in Image using LSB
Share 1
Bank Database
Share 2
Download to User's Mobile
Divide Shares
Login
Verification at Transaction

Figure 3.1: System Architecture

In a core banking system, there is a chance of encountering forged signature for transaction. In the 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 technique to secure the customer information and to prevent the possible forgery of signatures and password hacking. Our project proposes a technique of processing a secret key of a customer and then dividing it into shares. When two shares are created, one is stored in the Bank database and the other is kept by the customer. The customer has to present the share during all of his transactions. This share is stacked with the first share get the original secret key. The Correlation method is used to take the decision on acceptance or rejection of the output and authenticate the customer.

In all banking applications, the customer has to create an account in one branch initially. The flow of the algorithm is as follows. In the next stage, the pre-processed image is encrypted to get shares. The number of shares to be created is based on the scheme opted by the bank and the mode of operation of the account. The following schemes are developed:

2 out of 2 Schemes: This scheme can be adopted when the operational mode of the account is single. Here, two shares are created and both are necessary for decrypting the image. One of the shares is stored in the database of the bank and the other is kept with the customer.

2 out of 3 Schemes: It is useful for joint accounts. Here, three shares are created and any two are sufficient to reveal the image. Two shares are handed-over to two customers having joint account and the other is kept in bank database. Any one customer can transact with the bank by submitting his share.

3 out of 3 Schemes: This scheme is also useful for joint accounts. All three shares are required to get the output image in this case, and thus both the customers should be present for further transactions.

Key-Share Scheme: It uses the signatures of both the customers in joint account system. From two images, four shares are created in the similar manner of 2 out of 2 schemes. Then by combining two shares, each from two images, a key-share is created. Overlaying key share on each of the remaining shares will separately reveal two images. Thus, each customer can separately be authenticated and allowed to do transaction just by revealing his signature only.

In all the cases, the shares are printed and handed-over to customer, just like any credit/debit card. During further transaction, customer has to produce his share. This will be overlaid over the bank's share to decrypt the image. After decrypting the image, the post-processing is done on the decrypted image. Finally, the original image and the post processed image are compared to confirm the authenticity of the customer.

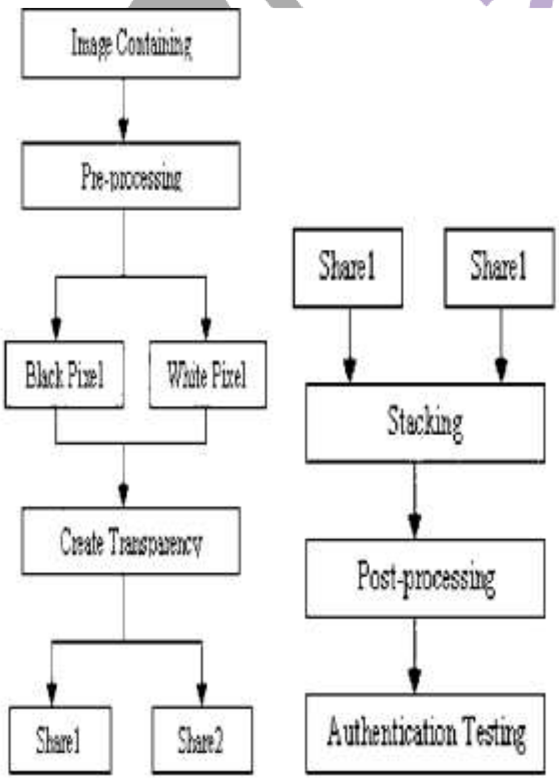


Figure 3.2: Share Creation and Authentication

In a core banking system, the customer needs to present his share for every transaction. This share is overlaid on bank's share to get the secret key and thus to authenticate the customer. Customer may be authenticated based on password and the output image obtained using the share produced by him.

Least Bit Significant Algorithm

Technique basics

Today, when converting an analog image to digital format, we usually choose between three different ways of representing colors:

- 24-bit color: every pixel can have one in 2^24 colors, and these are represented as different quantities of three basic colors: red (R), green (G), blue (B), given by 8 bits (256 values) each.
- 8-bit color: every pixel can have one in 256 (2^8) colors, chosen from a palette, or a table of colors.
- 8-bit gray-scale: every pixel can have one in 256 (2^8) shades of gray.

LSB insertion modifies the LSBs of each color
24-bit images, or the LSBs of the 8-bit value for 8-bit images.

Example: The letter 'A' has an ASCII code of 65(decimal), which is 1000001 in binary. It will need three consecutive pixels for a 24-bit image to store an 'A': Let's say that the pixels before the insertion are:

10000000.10100100.10110101,10110101.11110011 .10110111, 11100111.10110011.00110011

Then their values after the insertion of an 'A' will be:

1000000**1**.1010010**0**.1011010**0**,1011010**0**.1111001**0**.
1011011**0**, 1110011**0**.1011001**1**.00110011

(The values in **bold** are the ones that were modified by the transformation)

The same example for an 8-bit image would have needed 8 pixels:

10000000, 10100100, 10110101, 10110101, 11110011, 10110111, 11100111, 10110011

Then their values after the insertion of an 'A' would have been:

1000000**1**, 1010010**0**, 1011010**0**, 1011010**0**, 1111001**0**, 1011011**0**, 1110011**0**, 1011001**1**

Shamir's Scheme Algorithm

Shamir's Secret Sharing is an algorithm in cryptography. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Formally, our goal is to divide some data *D* (e.g., the safe combination) into *n* pieces *D*1,…,*Dn* in such a way that:

1. Knowledge of any *k* or more *Di* pieces makes *D* easily computable.
2. Knowledge of any *k*−1 or fewer *Di* pieces leaves *D* completely undetermined (in the sense that all its possible values are equally likely).

This scheme is called (*k, n*) threshold scheme. If *k*=*n* then all participants are required to reconstruct the secret.

The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes *k* points to define a polynomial of degree *k*−1.

Suppose we want to use (*k, n*) threshold scheme to share our secret *S*, without loss of generality assumed to be an element in a finite field *F*.

Choose at random *k*−1 coefficients *a*1,⋯,*ak*−1 in *F*, and let *a*0=*S*. Build the polynomial *f*(*x*)=*a*0+*a*1*x*+*a2×2*+*a*3*x*3+⋯+*ak*−1*xk*−1. Let us construct any *n* points out of it, for instance set *i*=1,⋯,*n* to retrieve (*i*, *f*(*i*)). Every participant is given a point (a pair of input to the polynomial and output). Given any subset of *k* of these pairs, we can find the coefficients of the polynomial using interpolation and the secret is the constant term *a*0.

Some of the useful properties of Shamir's (*k, n*) threshold scheme are:

1. **Secure**: Information theoretic security.
2. **Minimal**: The size of each piece does not exceed the size of the original data.

3. **Extensible**: When *k* is kept fixed, *Di* pieces can be dynamically added or deleted without affecting the other pieces.
4. **Dynamic**: Security can be easily enhanced without changing the secret, but by changing the polynomial occasionally (keeping the same free term) and constructing new shares to the participants.
5. **Flexible**: In organizations where hierarchy is important, we can supply each participant different number of pieces according to his importance inside the organization. For instance, the president can unlock the safe alone, whereas 3 secretaries are required together to unlock it.

V. RESULT

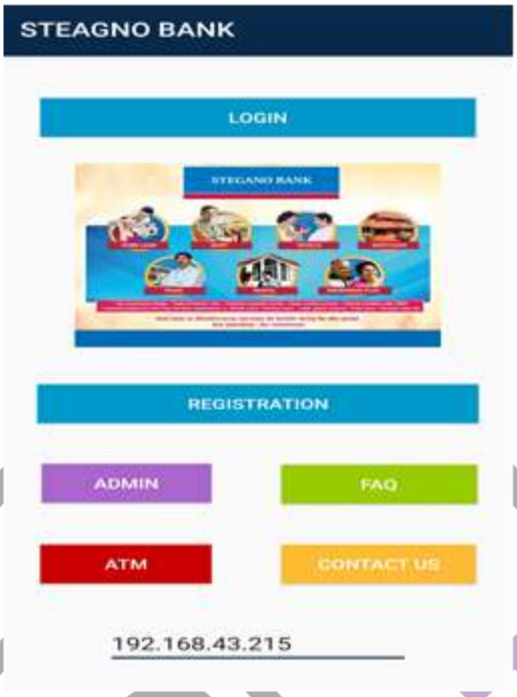
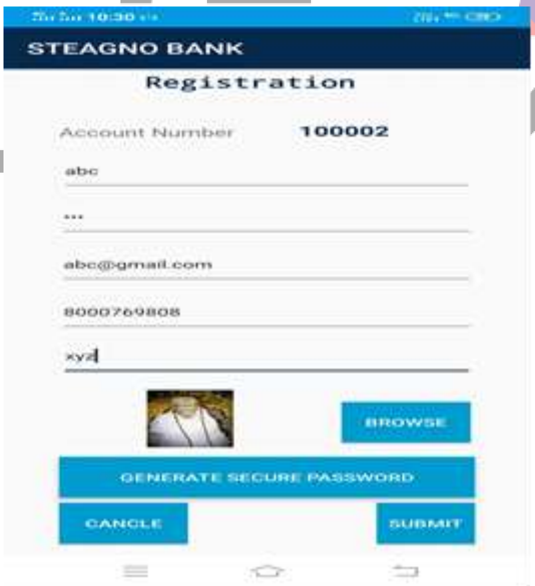


Fig 1: Home Page



Account Number 100002

abc

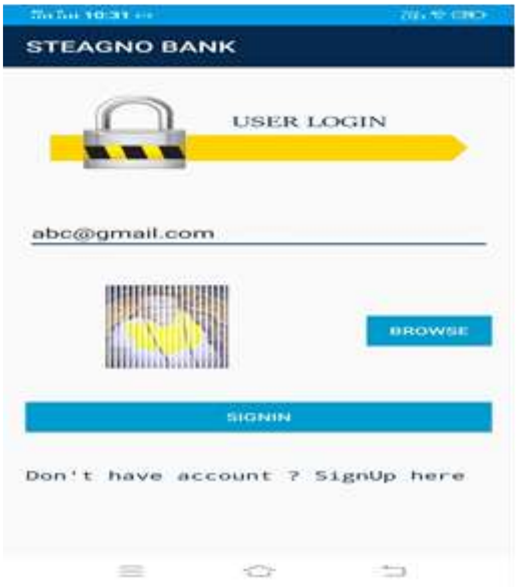
***

abc@gmail.com

8000769808

xyz

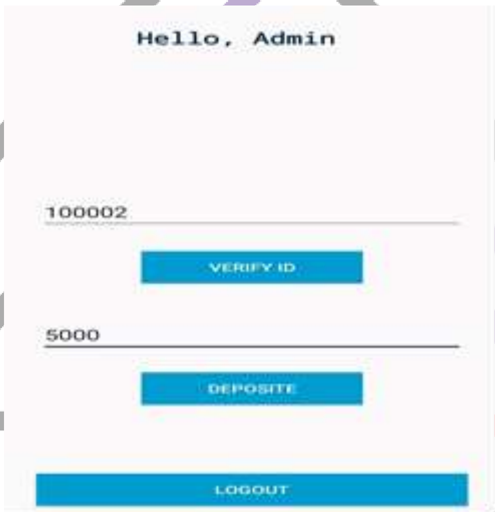
Fig 2: Registration Module



abc@gmail.com

Don't have account ? SignUp here

Fig 3: User Login Page



Hello, Admin

100002

5000

4: Admin Login Page

VI. CONCLUSION

After making a comparison study between the science of cryptography and stenography, the authors cannot guarantee that steganography can be used as an alternate to cryptography as each aspect has its peculiarities. Cryptography refers to the act of secret writing through the enciphering and deciphering of encoded message, while steganography refers to the ways of concealing a secret message into a cover message in a manner that its existence is completely hidden. Using only one of these techniques will render the system vulnerable to the third party. Therefore, the combination of steganography and cryptography give more security and robustness

VII. FUTURE SCOPE

In future work, this application could be extended by implementing dynamic LSB steganography techniques.

In addition, developing machine learning features to the system and determining a way to select optimum points to hide images will further improve the system.

Currently, when shares are merged, there is no authentication testing mechanism; authentication testing would improve the quality of share overlapping, which can be achieved through correlation algorithms. Adding correlation algorithms in future will help verify the authenticity of stacked shares, and will improve the results.

REFERENCES

[1] S. Roy, P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", Proceedings of the IEEE Conference on Electrical, Electronics and Computer Science, pp. 88-93, 2014.

[2] M. Suresh, B. Domathoti, N. Putta, "Online Secure E-Pay Fraud Detection in E-Commerce System Using Visual Cryptographic Methods", International Journal of Innovative Research in Computer and Communication Engineering ,vol. 3, no. 8, pp. 7519-7525, August 2015.

[3] Rahna E, V. Govindan, "A Novel Te chnique For Secure, Lossless Steganography With Unlimited Payload And Without Exchange Of Stegoimage", International Journal of Advances in Engineering & Technology, vol. 6, no. 3, pp. 1263-1270, July 2013.

[4] C. Chan, L. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, pp. 469– 474, August 2004.

[5] N. Shrivastava1, T. Verma, "A Survey on Various Techniques for Generating Image Steganography with Improved Efficiency", International Journal of Advanced Research in Computer Engineering & Technology , vol. 4, no. 3, pp. 1005-1009, March 2015.

[6] M. Kutter, S. Winkler, "A Vision-Based Masking Model for Spread-Spectrum Image Watermarking", Proceedings of the International Conference on Computing, Electronics and Electrical Technologies, pp. 313-336, 2004.

[7] X. Li, B. Yang, D. Cheng, T. Zeng, "A Generalization of LSB Matching", IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69-72, February 2009.

[8] P. Vaman, C. Manjunath, Sandeep , "Integration of Steganography and Visual Cryptography for Authenticity", International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 6, pp. 80-84, June 2013.

[9] C. Hegde , Manu S , P. Shenoy , Venugopal K R , L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications", Proceedings of the 16th International Conference on Advanced Computing and Communications, pp. 65-72, 2013.

[10] Suklabaidya, G. Sahoo, "Visual Cryptographic Applications", International Journal on Computer Science and Engineering, vol. 5, no. 06, pp 455-464, June 2013.

[11] Jaya, S. Malik, A. Aggarwal, A. Sardana, "Novel Authentication System Using Visual Cryptography", Proceedings of the 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, 2011.

[12] Vinodhini, L. Ambarasi, "Visual Cryptography for Authentication Using CAPTCHA", International Journal of Computer and Internet Security, vol. 2, no. 1,pp 67-76,2010.

[13] J. Chen, X. Xie, F. Jing, "The security of shopping online", Proceedings of the 2011 International Conference on Electronic and Mechanical Engineering and Information Technology, pp. 4693-4696, 2011.

[14] C. Hu and W. Tzeng, "Cheating Prevention in Visual Cryptography", IEEE Transaction on Image Processing, vol. 16, no. 1, pp. 36-45, 2007.