Secured Online Transaction Using Visual Cryptography

Abhijit Pote[1], Ritesh Kumar[2], Rushikesh Bhasme[3] ,Prof. Ganesh Padole[4]
[1,2,3]Project Student, [4]Professor
Department of Computer Technology
Rajiv Gandhi college of Engineering And Research Nagpur

***Abstract*— Core banking is a set of services provided by a group of networked bank branches. Bank customers may access their funds and perform other simple transactions from any of the member branch offices. The major issue in core banking is the authenticity of the customer. Due to unavoidable hacking of the databases on the internet, it is always quite difficult to trust the information on the internet. To solve this problem of authentication, we are proposing an algorithm based on image processing and visual cryptography. This paper proposes a technique of processing the secret key of a customer and then dividing it into shares. Total number of shares to be created is depending on the scheme chosen by the bank. When two shares are created, one is stored in the Bank database and the other is kept by the customer or send to image server. The customer has to present the share during all of his transactions. This share is stacked with the first share to get the original Transaction key. The Correlation method is used to take the decision on acceptance or rejection of the output and authenticate the customer.**

***Index Terms*—Image processing; Visual Cryptography**

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.

PROPOSED SYSTEM

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.

METHODOLOGY

Visual Cryptography:

One of the novel approaches for encrypting the image is Visual Cryptography where is encrypted without using any encryption key but the image is divided into random shares in such a way the individual share does not convey any information about the secret image. For regeneration of the image all the shares are required.

Visual cryptography (VC) is a type of secret sharing scheme introduced by Naor [2]. In a *k*-out-of-*n* scheme of VC, a secret binary image is cryptographically encoded into *n* shares of random binary patterns. The *n* shares are Xeroxed onto *n* transparencies, respectively, and distributed amongst *n* participants, one for each participant.

No participant knows the share given to another participant. Any *k* or more participants can visually reveal the secret image by superimposing any *k* transparencies together. The secret cannot be decoded by any $k-1$ or fewer participants, even if infinite computational power is available to them. To illustrate a basic principle of VC, consider a simple (2, 2)-VCS in Fig: 4.5. Each pixel *p* from a secret binary image is encoded into *m* black and white subpixels in each share. If *p* is a white (black) pixel, one of the six columns is selected randomly with equal probability, replacing *p*. Regardless of the value of the pixel *p*, it is replaced by a set of four subpixels, two of them black and two white. Thus the subpixel set gives no clue as to the original

value of *p*. When two subpixels originating from two white *p* are superimposed, the decrypted subpixels have two white and two black pixels, on the other hand a decrypted subpixel having four black pixels indicates that the subpixel come from two black *p* pixels.

The concepts of VC have been extended such that the secret image is allowed to be a grayscale image rather than a binary image. Although the secret image is greyscale, shares are still constructed by random binary patterns.

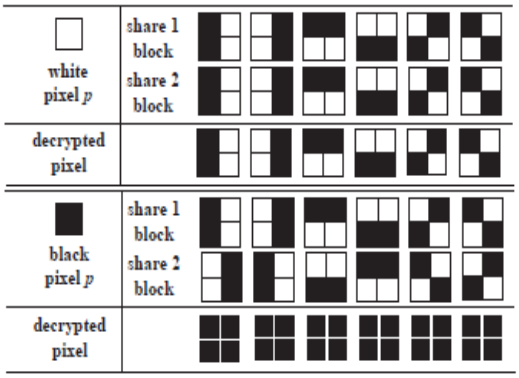

Fig1: Conventional visual cryptography

Basic principles of color:

The additive and subtractive models are commonly used to describe the constitutions of colors. In the additive system, the primaries are red, green and blue (RGB), with desired colors being obtained by mixing different RGB components. By controlling the intensity of red (green or blue) component, we can modulate the amount of red (green or blue) in the compound light. The more the mixed colored-lights, the more is the brightness of the light. When mixing all red, green and blue components with equal intensity, white color will result. The computer monitor is a good example of the additive model.
In the subtractive model, color is represented by applying the combinations of colored-lights reflected from the surface of an object (because most objects do not radiate by themselves). Take an apple under the natural light for example. The surface of the apple absorbs green and blue part of the natural light and reflects the red light to human eyes, so it becomes a red apple. By mixing cyan (C) with magenta (M) and yellow (Y) pigments, we can produce a wide range of colors. The more the pigment we add, the lower is the intensity of the light, and thus the darker is the light. This is why it is called the subtractive model. C, M and Y are the three primitive colors of pigment, which cannot be composed from other colors. The color printer is a typical application of the subtractive model

In the additive model, any color mixed with white color is still white color. It thus seems more reasonable to use red, green, blue, and black colors to fill the blocks. On the other hand, in the subtractive model, the combination of any two of R, G, and B colors results in black color. R, G or B combined with white color will not change and can only result in the same color. Consequently, it is more appropriate to fill the blocks with cyan, magenta, yellow and white colors. In computer systems, Application Interfaces (APIs) provided by most image processing software as well as the Windows operating system are based on the RGB model. This is mainly because they use monitors as the primary output media. Monitors themselves generate color images by sending out RGB light into human's retina. In true color systems, R, G, Bare each represented by 8 bits, and therefore Each single color of R, G, B can represent 0–255 variations of scale, resulting in 16.77 million possible colors. When using (R, G, B) to describe a color pixel, (0; 0; 0) represents full black and (255; 255; 255) represents full white.

In visual cryptography, we use sharing images as the decryption tool; that is, the Enal outputs are transparencies. Because the subtractive model is more suitable for printing colors on transparencies, we will use the CMY model to represent colors in what follows. Because (R, G, B) and (C, M, Y) are complementary colors, in the true color model, (R, G, B) and (C, M, Y) possess the following relationships: C = 255−R, M = 255−G, Y = 255−B: Thus, in the (C, M, Y) representation, (0; 0; 0) represents full white and (255; 255; 255) represents full black.

Comparison of various visual cryptography schemes:

Many research papers have been published using this approach, starting from a binary image moving to greyscale image and finally employing it to color images. Though with each subsequent research paper the quality of the recovered image improved. Detail of various visual cryptography schemes is below. One of the promising approaches for color images is proposed by Jaya, Siddharth Malik, Anjali Sardana in [3], the proposed technique involves splitting an image into multiple shares.

Authors Year	Pixel Expansion	Number of Secret Images	Image Format	Type of Share generated
Naor and Shamir[6] 1995	1	4	Binary	Random
Wu and Chang [23] 2005	2	4	Binary	Random
Chin-Chen et al [24] 2005	1	4	Binary	Meaningful
Tzung-Her Chen et al [25] 2008	n(n>=2)	4	Binary, Gray, Color	Random
F. Liu et al [26] 2008	1	9	Color	Random

Comparison of various visual cryptography schemes

Algorithm

An image is taken as input. The number of shares the image would be divided (n) and number of shares to reconstruct the image (k) is also taken as input from user. The encryption, i.e. division of the image into n number of shares such that k

numbers of shares are sufficient to reconstruct the image; is done by the following algorithm.

Step 1: Read Input Colour Image I, Read Number of Share N
Step 2: Let W = Width of the Image Let H = Height of the Image
Step 3: Create a Numeric Matrix R of Size [W,H]
Step 4: Fill the matrix with Random Number For s = 1 to W For q = 1 to H R[s,q] = Generate Random number between 1 to N Next q Next s
Step 5: Let c = 1
Step 6: Create a new Share Image SI
Step 7: For s = 1 to w For q = 1 to H V = R[s,q] If V = C then SI[s,q] = I[s,q] Next q Next s
Step 8: Write all the content of SI in new Share
Step 9: if c < N then c = c+1, Go To Step 6
Step 10: Stop

Increasing Intensity of the Image through Pre-processing

Step 1: Select an initial estimate for the threshold T.
Step 2: Segment the image using T. This will produce two groups of pixels: G1 consisting of all pixels with grey level values > T and G2 consisting of pixels with values <= T.
Step 3: Compute the average grey level values μ1 and μ2for the pixels in regions G1 and G2.
Step 4: Compute a new threshold value:
T = 1/2 (μ1 + μ2)
Step 5: Repeat steps 2 to 4 until the difference in Tin successive iterations is smaller than a predefined parameter T0.

Modules Description

There are six main modules in the project. Those are:

- Homepage
- User Registration
- Email Verification
- Select Image and Generate Secret Key
- Admin Login

Homepage:-

This is the Homepage of any banking website in which we have to login. In Home page various options are provide like login, new user, forget password, e-mail verification. If we already have an account in the bank, then using our login id and password we can login. During login if the customer forget his password then by the forget password option customer reset his password. And after getting the new password customer will login to the bank site and perform his transactions. By using the new user option you create your account in the bank site. If you are new user to the bank then you have to go through the registration process. In registration process you have to fill registration form in which you have to enter your name, surname, contact number this basic information and valid Email id and also set your password from this password the customer perform their transactions. After the registration process the email id verification performs. In customer mail account a verification code will receive and this code is receive into the email verification box if the customer enter a valid code then his registration done successfully. And now the customer is ready to perform his transaction.

User Registration:-

If you are new user to the bank then you have to go through the registration process. In registration process you have to fill registration form in which you have to enter your basic information like your name, surname, contact number, and valid Email id and also your password from this password the customer perform their transactions. After the registration process the email id verification performs. In customer mail account a verification code will receive and this code is enter into the email verification box if the customer enter a valid code then his registration done successfully. And now the customer is ready to perform his transaction.

Email Verification:-

A verification code will send to customer email id. This valid code is enter in the email verification box if the code is correct the registration done successfully. After successful registration you get your login id and password on your Email account. Using that Id and password we can login into the bank website. This login id and password are the permanent for your all the transactions process.

Select Image and Generate Secret Key

After successfully registration user have to select a image as per his choice whatever he want. Then user should upload the image then after he have to enter a secret key. this secret key is hide behind the image which user was select. Encrypted Secret Key Should be Embedded with a selected image. This Image should be divided into two shares. One share should be downloadable and this downloadable image send to image server and other should be stored into Bank Database.

Admin Login

After successfully selecting image and generating secret key then back to login open the admin login page. It is the user login in which after login we get the banking account details. But at the time of transaction we have to enter our share. This share is merge with bank database share . our secret Key should be retrieved and treated as Transaction key.
After this process user should enter email id and password this id and password user could be use in the registration process then login this id and password. After successfully admin login verify the account details .account verification process we can choose the share image browse and upload this site then verify your bank details. Then after open the account details page then user should perform the transaction process.

CONCLUSION

This system is developed as a Web Application in .Net Technology. It is implemented on IIS Web server and tested with sample data and the experimental result shows this system fulfil the aim and objective of the project. This system uses Colour Image Visual Cryptography for password

protection and it is not able to break this protection with present technology. This system will be a boon for the Core Banking Application and the bank customers are feel free from the password hacking problems. Once this system is deployed in web Server, all the computer in the network can able to access this application through browser without any software installation in their computer.

REFERENCES

[1] Kede Ma. Weiming Zhang, Xianfeng Zhao, Nenghai Yu,Fenghua Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", IEEE Trans on Information Forensics and security, Vol. 8, No. 3, march 2013

[2] M. Naor and A. Shamir, ―Visual cryptography, Advances in Cryptology-Eurocrypt'94, pp. 1–12, 1995.

[3] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies.

[4] F. Liu1, C.K. Wu1, X.J. Lin, Colour visual cryptography schemes, IET Information Security, July 2008

[5] M. Shirali-Shahreza, ―Steganography in MMS, in Multitopic Conference, 2007. INMIC 2007. IEEE International, 2007, pp. 1-4