SECURE BANKING APPLICATION USING VISUAL CRYPTOGRAPHY AGAINST FAKE WEBSITE AUTHENTICITY THEFT

[1]Chandrasekhara & [2]Jagadisha

E-mail : chandrasekhara.ewit@gmail.com,jagadisha.n83@gmail.com

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. To solve this problem of authentication, we are proposing an algorithm based on image processing, i.e. visual cryptography. Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human visual system. But the encryption technique needs cryptographic computation to divide the image into a number of parts let n. In our paper we have proposed a new k-n secret sharing scheme for color image where encryption (Division) of the image is done using Random Number generator. 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. The customer has to present the share during all of his transactions. This share is stacked with the first share to get the original image. Then decoding method is used to take the hidden password on acceptance or rejection of the output and authenticate the customer.**

Keywords – **Visual Cryptography, secret sharing.**

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 password hacking. The concept of image processing, an 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 a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveal the secret image. Naor and Shamir introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, termed as Visual Cryptography Scheme (VCS). Any visual secret information (pictures, text, etc) is considered as image and encryption is performed using simple algorithm to generate n copies of shares depending on type of access structure schemes. The simplest access structure is the 2 out of 2 scheme

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.

Visual cryptography is a cryptographic technique which allows visual information (Image, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers. Image is a multimedia component sensed by human. The smallest element of a digital image is pixel. In a 32 bit digital image each pixel consists of 32 bits, which is divided into four parts, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency. If all bits of Alpha part are ‘0’, then the image is fully transparent. This is represented in the following figure.

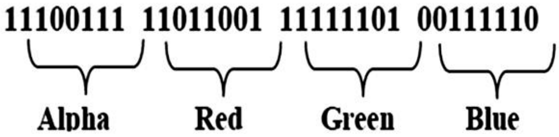


Fig.1: Structure of a 32 bit pixel

Human visual system acts as an OR function. If two transparent objects are stacked together, the final stack of objects will be transparent. But if any of them is non-transparent, then the final stack of objects will be nontransparent. Like OR, 0 OR 0 = 0, considering 0 as transparent and 1 OR 0=1, 0 OR 1 =1, 1 OR 1=1, considering 1 as non-transparent.

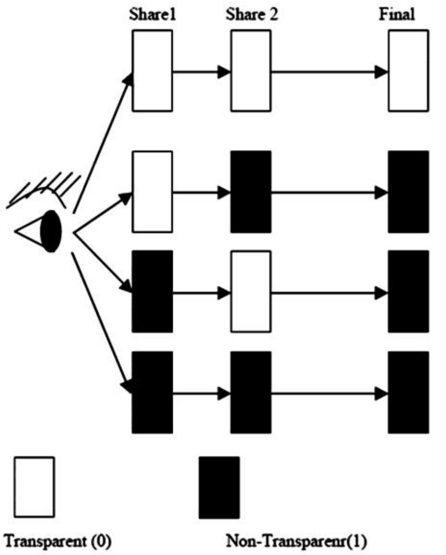


Fig. 2 : Human Visual system as OR Function

In k out of n visual cryptography scheme is a type of cryptographic technique where a digital image is divided into n number of shares by cryptographic computation. In the decryption process only k or more than k number of shares can reveal the original information [Here can form the original image]. Less than k number of shares can not reveal the original information.

II. LITERATURE SURVEY

With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want.

To deal with the security problems of secret images, various image secret sharing schemes have been developed. It is now common to transfer multimedia data via the Internet. With the coming era of electronic commerce, there is an urgent need to solve the problem of ensuring information safety in today's increasingly open network environment.

A. Black And White VC Schemes

Naor and Shamir's proposed encoding scheme to share a binary image into two shares Share1 and Share2. If pixel is white one of the above two rows of Fig. 2.1 is chosen to generate Share1 and Share2. Similarly if pixel is black one of the below two rows of Fig.2.1 is chosen to generate Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black. Secret image is shown only when both shares are superimposed. Stacking shares represents OR operation to human visual system. OR operation is lossy recovery. If XOR operation is applied instead of OR then we can get lossless restore of the original image. But, XOR operation requires computation. The physical stacking process can only simulate the OR operation.

The drawbacks of this scheme are:

- It is for black and white images.
- Need more storage capacity as shares are four times the original image.
- It is time consuming as single pixel encoding at each run.

Many advanced schemes were introduced when a colored image is encrypted. A multi-pixel non-expanded scheme for color images introduced which can encode more than one pixel for each run resulting same size of shares as secret image. The scheme achieves high efficiency for encoding and this works well for general access structure for chromatic images without pixel expansion but it generates meaningless shares.

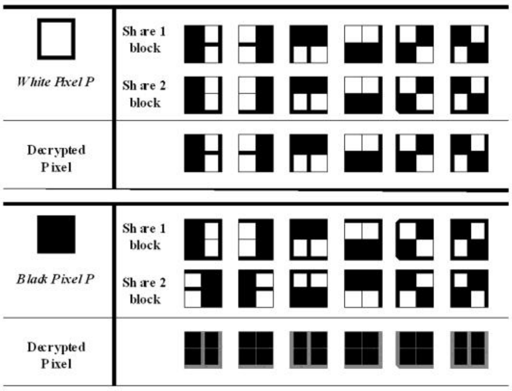


Fig. 3 : Construction of (2, 2) VC scheme.

The disadvantage of the above schemes is that only one set of confidential messages can be embedded, so to share large amounts of confidential messages several shares have to be generated.

In a construction of (2, 2) VC scheme a secret pixel is encoded into four subpixels in each of two shares. The decrypted pixel is obtained by superimposing the blocks in shares one and two.

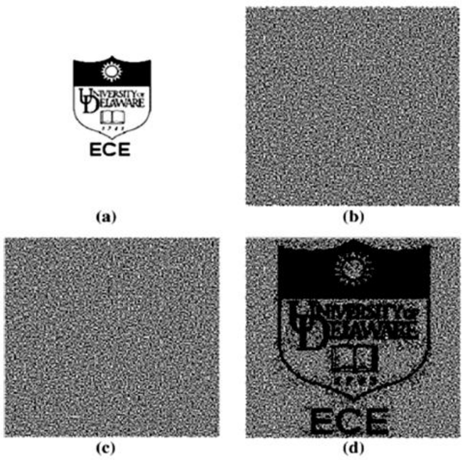


Fig. 4 : Example of 2-outof- 2 scheme.

In the above example the secret image is encoded into two shares showing random patterns. The decoded image shows the secret image with 50% contrast loss.

(a) Binary secret image.

(b) Encrypted share 1.

(c) Encrypted share 2.

(d) Decrypted secret message.

B. Color Visual Cryptography Schemes

Sharing a secret color image and also to generate the meaningful share to transmit secret color image Chang and Tsai anticipated color visual cryptography scheme. For a secret color image two significant color images are selected as cover images which are the same size as the secret color image. Then according to a predefined Color Index Table, the secret color image will be hidden into two camouflage images. One disadvantage of this scheme is that extra space is required to accumulate the Color Index Table.

In this scheme also number of sub-pixels is in proportional to the number of colors in the secret image as in Verheul and Van Tilborg Yang and Laih schemes. When more colors are there in the secret image the larger the size of shares will become.

To overcome this limitation Chin-Chen Chang et al developed a secret color image sharing scheme based on modified visual cryptography. This scheme provides a more efficient way to hide a gray image in different shares. In this scheme size of the shares is fixed; it does not vary when the number of colors appearing in the secret image differs. Scheme does not require any predefined Color Index Table. Though pixel expansion is a fixed in this scheme is not suitable for true color secret image. To share true-color image Lukac and Plataniotis introduced bit-level based scheme by operating directly on S-bit planes of a secret image. To illustrate basic principles of VC scheme, consider a simple (2, 2)-VC scheme in Fig. 3.

Each pixel from a secret binary image is encoded into black and white sub-pixels in each share. If is a white (black) pixel, one of the six columns is selected randomly with equal probability, replacing. Regardless of the value of the pixel, it is replaced by a set of four sub-pixels, two of them black and two white. Thus, the sub-pixel set gives no clue as to the original value of. When two sub-pixels originating from two white are superimposed, the decrypted sub-pixels have two white and two black pixels.

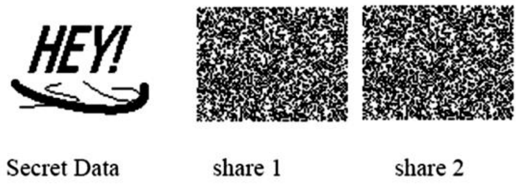
On the other hand, a decrypted sub-pixel having four black pixels indicates that the sub-pixel came from two black pixels. Fig.4 shows an example of a simple (2, 2)-VC scheme with a set of sub-pixels shown in Fig. 3. Fig. 4(a) shows a secret binary message, Fig. 4(b) and (c) depict encrypted shares for two participants. Superimposing these two shares leads to the output secret message as shown in Fig. 4(d). The decoded image is clearly identified, although some contrast loss is observed.

III. ADJUSTMENT TECHNIQUE

Visual cryptography, the most notable features of this approach is that it can be recovery secret image without any computation. It exploits human visual system to read the secret message from some overlapping shares, thus overcoming disadvantage of complex computation required in the cryptography. Naor and Shamir introduced a simple but perfectly secure way that allows secret sharing without any cryptography computation termed as a visual cryptographic scheme.

The problem of encrypting written material (printed text, hand written notes, pictures etc) in a perfectly secure way which can be directly by the human visual system. 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.

- Level 1 hiding using Visual Cryptography



- Super Imposing Share1 and Share2 to Form the Original Secret Data

The secret Information

The original motivation was to safeguard cryptographic keys from loss. One of the best known techniques to protect the data is cryptography. it is a art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the messages.

Visual Cryptography Scheme is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes.

- (2,2) Threshold VCS scheme- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.
- (2,n) Threshold VCS scheme-This scheme encrypts the secret image into n shares such that when any two(or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.
- (n,n) Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image be revealed.
- (k,n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for n, number of participants.

IV. ALGORITHM

An image is taken as input. The number of shares the image would be divided (n) and number of hares 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
```

Decryption Algorithm In the case of visual cryptography, decryption is done by human visual system. It is already discussed that human visual system acts as an OR function. In the case of decryption.

V. EXPERIMENTAL RESULTS

Encryption Process:

Source Image: Lena.png

Source image is

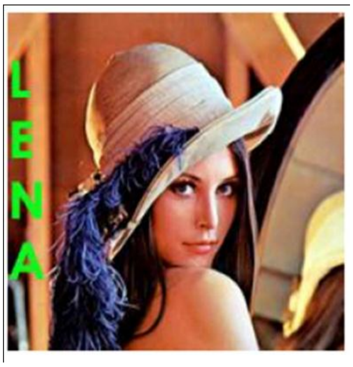


Fig. 3 : Source Image

Number of Shares: 6

Numbers of shares to be taken: 5

The experimental result after encryption by the encryption algorithm is given below.

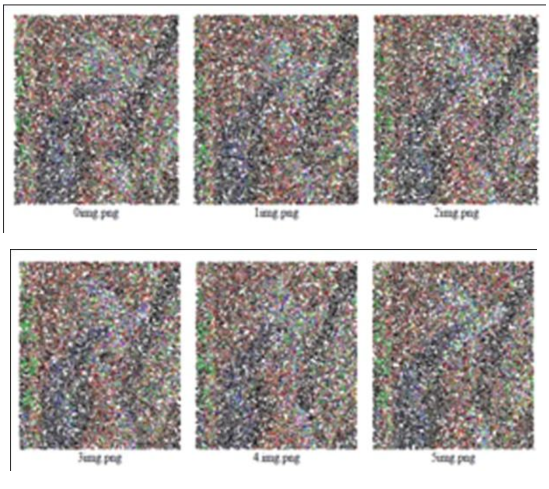


Fig.4 : Encrypted Shares

Decryption Process:

Number of shares: 5

Height and Width of each share: 200, 200

Shares inputted

0img.png, 1img.png, 3img.png, 4img.png, 5img.png

Final image reconstructed:

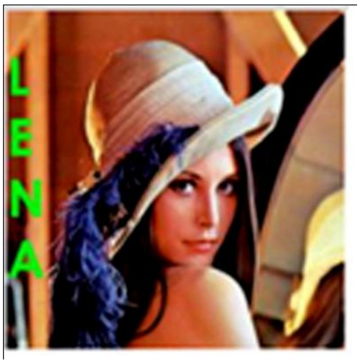


Fig. 5 : Reconstructed Image

If three shares let 0img.png, 2img.png, 5img.png are taken, the decrypted image become

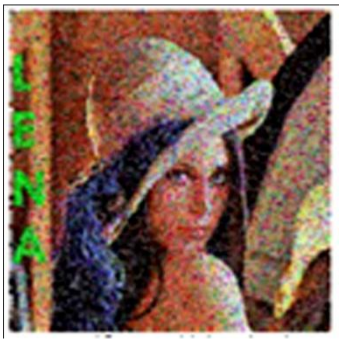


Fig. 6 : Reconstructed Image with less than k number of shares

The image is a distorted image and conveys partial information about all pixels. If some text is hidden within the image by invisible digital watermarking, then original image is required to get that watermarked text.

VI. CONCLUSION

This system is developed as a Web Application in Java Technology. It is implemented on TomCat Web server and tested with sample data and the experimental result shows this system fulfill 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.

VII. FUTURE SCOPE

Since it is a web based application, when more number of user are access the web server the response time will be increased, to avoid this delay we can enhance this system to cloud environment, where based on the number of user access, cloud configuration will change and minimize the response time.

Also we can add some more security features like Digital Signature in high level transaction process. Visual cryptography technique is used to make the data secure. Here the original data is divided into a number of shares which are sent through different communication channels from sender to receiver. Therefore the intruder has less chance to get the whole information. But still it is not so secured. This can be made more secure by introducing a symmetric key for both encryption and decryption process.

Using the key, the image is first encrypted then divided into a number of shares. If the intruder gets k number of shares s/he cannot be able to decrypt it if the key is not known to his/her. For key, a combination of character or number can be used. The change of higher bits make the image more blur, so the key can be applied on the higher bits of each pixels.

VIII. REFERENCES

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

[2] M. Kutter and S. Winkler, “A vision-based masking model for spread- spectrum image watermarking,” IEEE Trans. Image Processing, vol. II, pp. 16-25, Jan. 2002.

[3] C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognition, pp. 469—474, Mar. 2004.

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

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

[6] M. Naor and A. Shamir, “Visual cryptography,” Advances in Cryptology-Eurocrypt’94, pp. 1–12, 1995.

[7] Li Bai , A Reliable (k,n) Image Secret Sharing Scheme by, IEEE,2006.

[8] John F Koegel Buford, Multimedia Systems, Addison Wesley, 2000

[9] S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, and K. Chen, “Sharing multiple secrets in visual cryptography”, Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.

[10] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, “Multi-Secrets Visual Secret Sharing”, Proceedings of APCC2008, IEICE, 2008.

[11] Provos, N. (2001). Scanning USENET for Steganography. from http://niels.xtdnet.nl /stego /usenet. php.

[12] Schildt, H. The Complete Reference Java 2, Fifth Ed. TMH, Pp 799-839.

❖❑❖