SECURE TRANSACTION USING VISUAL CRYPTOGRAPHY

[1]Karishma Patel, [2]Prof. D.R.Kasat, [3]Dr. Sanjeev Jain, [4]Dr. V.M.Thakare
[1]Student SCET, [2]Associate Professor SCET, [3]Director MITS, [4]Professor Amravati University
Email:[1]patelkarishma4444@gmail.com,[2]dipali.kasat@scet.ac.in

Abstract— In today's world the major issue in banking sector is authenticity of customer to bank and vice-versa. Visual cryptography is one of the most prominent ways to provide authentication because it allows hiding the data and its secure transmission on open communication channel. In our proposed approach, we take one host image agreed upon by bank and customer and create its shares using 2-out-of-2 visual cryptography scheme. Out of the two shares created, one is server share that will be stored in bank database along with other details of the customer and the other is client share which is kept by the user. The user will present his/her client share during all the transactions with bank. To initiate the transaction with bank the customer will apply the watermark technique on its own share using our application DWT watermarks are generated by our application for providing the copyright protection and also deal with various RST attacks. At the receiver side, the bank will apply watermark detection process on received share and authenticate it. At last the bank stacks the server share with received client share and reveals the original image or message. After then server send acknowledgement message to client for acceptability of user and same process will done for authenticate the bank. So, that our scheme will provide two-way authentication. Our scheme will be robust against various geometrical attacks and also provide authenticity and data integrity.

Index Terms— Digital image watermarking, Discrete Wavelet Transform, Visual cryptography Scheme.

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 using visual cryptography. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and characteristics of the input image.

Visual cryptography having the ability to hide information such as personal details is very desirable. When the data is hidden within separate shares, it is completely unrecognizable. While the shares are separate, the data is completely incoherent. Each image holds different pieces of the data and when they are brought together, the secret can be recovered easily [1-2]. Each share depends on one another in order to obtain the decrypted information.

There should be no way that anyone could decipher the information contained within any of the shares. When the shares are brought together, deciphering is possible when the shares are placed over one another. At this point, the information becomes instantly available. No computational power is required at all in order to decrypt the information, thus making it suitable for the online transactions.

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. 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 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. If XOR operation is applied instead of OR then we can get lossless restore of the original image. But, XOR operation requires computation.

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. Less than k number of shares can not reveal the original information.

Visual cryptography cannot provide higher security when an enemy attacks on client/server share image in transaction processing. Hence, in our proposed approach we will be using digital watermarking algorithm with visual cryptography to further improve security from client to server and vice versa.

A digital watermark is intended to complement cryptographic processes. It is a visible or invisible identification code that is permanently embedded in the data and remains present within the data after any decryption process. A wide variety of image watermarking schemes has been proposed and each addresses many different application scenarios. Watermarking techniques are classified into spatial domain methods and transform domain methods. Spatial domain methods are less complex, but less robust against attacks [16]. Transform domain methods alter frequency transform of data elements to embed watermark data. In general, transform domain algorithms are more robust than spatial domain algorithms. In transform domain, watermark is distributed irregularly over the entire image when inverse transform is applied on image during watermarking process. This makes attacker difficult to read or modify the watermark. The watermarking scheme based on the transform domains can be further classified into the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) etc. In our scheme we provide a robust dwt-svd blind watermarking based on Zernike moments algorithm.

The paper is organized as follows: Section II presents the related work. In section III, we discuss the proposed secure transaction algorithm. Section IV concludes this paper.

II. Procedure for Paper Submission

A. *Visual Cryptography*

Naor and Shamir at Eurocrypt’94 first introduced visual Cryptography (VC). Visual cryptography is a new type of cryptographic scheme that focuses on solving this problem of secret sharing. Visual cryptography uses the idea of hiding secrets within images. These images are encoded into multiple shares and later decoded without any computation up to various levels [6]. This decoding is as simple as superimposing transparencies, which allows the secret to be recovered. The main parameters of Visual Cryptography include image contrast and the number of sub pixels of recovered image. The contrast of an image is a relative difference between the original and retrieved image. As increased in number of sub pixels while creating the shares, size of the share also increases.

Jonathan *et al* [2] proposed a sharing multiple secrets using visual cryptography which is hide multiple information. Jose J Tharayil *et al* [13] proposed visual cryptography using hybrid halftoning scheme which is relays on hybrid halftoning and inter-pixel exchanging. Yi-chong zeng *et al* [4] proposed a high capacity multi-scale image sharing scheme is used to hide multiple images to two meaningful sharing images.

Figure 1 illustrates the basic scheme of encoding one pixel in a 2-out-of-2 Visual Cryptography scheme. A white pixel is divided into two identical blocks of sub-pixels. A black pixel is divided into two complementary blocks of sub-pixels [1][2][5][7]. While creating the shares, if the given pixel p in the original image is white, then the encoder randomly chooses one of the first two columns of Table 1.

If the given pixel p is black, then the encoder randomly chooses one of the last two columns of Table 1. Each block has half-white and half-black sub-pixels, independent of whether the corresponding pixel in the secret image is white or black. Here, all the pixels in the original image are encrypted similarly using independent random selection of columns. Thus, no information is reveal by looking at any group of pixels on a share.

Table 1. Two-out-of-two visual cryptography scheme

Pixel	White □		Black ■	
Probability	50%	50%	50%	50%
Share 1	■□	□■	■□	□■
Share 2	■□	□■	□■	■□
Stack both Share 1&2	■□	□■	■■	■■

To encode a secret employing a 2-out-of-2 VC Scheme, the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two sub-pixels. Not anyone who holds only one share will be able to reveal any information about the secret. To decode the image, each of these shares are stacked together. Stacking both these transparencies will reveal visual recovery of the secret.

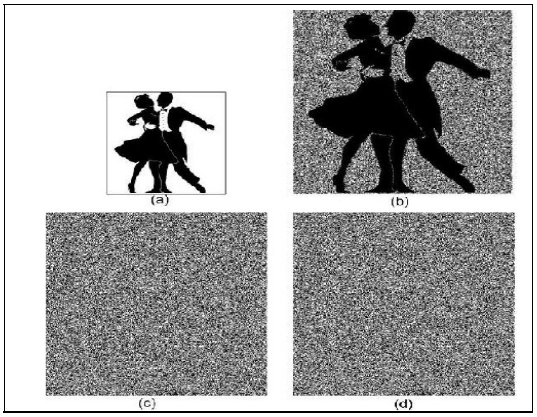


Figure.1 Example of (2, 2) visual cryptography scheme [9] (a) secret image; (b) reconstructed image; (c) first share; (d) second share

Figure 1 shows the results of example 2-out-of-2 VC Scheme. When the two shares are stacked together, as in Figure 2(b), the black pixels in the original image remain black and the white pixels become gray. Although some contrast loss occurs, the decoded image can be clearly identified. Since each pixel in the original image is replaced by two sub-pixels in each share, the width of the decoded image is double then the original image and also used for various level of decomposition [9].

B. Digital IMAGE WATERMARK

Digital watermarking on the other hand should be robust against attempts to remove the hidden data. A popular application of watermarking is to give proof of ownership [11]. It is obvious that for this application the watermark should be robust against any manipulation that may attempt to remove it. We can classify digital watermarking into two classes depending on the domain of watermark insertion, i.e. the spatial- and the frequency-domain watermarking [11][3].

Spatial domain watermarking is easy to implement and requires no original image for watermark detection. However, it often fails under signal processing attacks such as filtering and compression. Besides, the fidelity of the original image data can be severely degraded since the watermark is directly applied on the pixel values. Frequency domain watermarking generally provides more protection under most of the signal processing attacks [14][16].

Digital image watermarking embeds the watermark into host images in an imperceptible or perceptible way. Digital image watermarking can use in a number of applications with different requirements including copyright protection, content authentication and content description [11].

Figure.2 is a typical watermarking system, which includes watermark embedder and watermark detector. The inputs to the watermark embedder are the watermark, the cover media data and the embedding security key. The watermark can be a number sequence or a binary bit sequence. The key is used to enhance the security of the whole system. The output of the watermark embedder is the watermarked data.

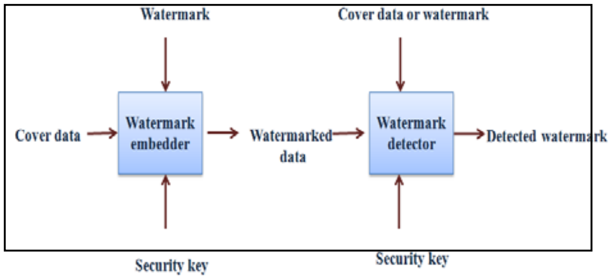


Figure.2 A typical watermarking system

The inputs to the watermark detector are the watermarked data, the security key and, depending on the method, the actual data and/or the actual watermark. A watermark detector includes two-step process. The first step is watermark extraction that applies one or more pre-processes to extract a vector referred to as extracted mark. Then, the second step is to determine whether the extracted mark contains the original watermark or not.

There are many methods to embed the watermark. The transform algorithm includes chiefly DWT, DFT, and DCT. [19][20]. Wavelet transform is superior to time frequency transform for its inner predominance. DWT provide higher image imperceptibility and the much more robust to image manipulation. In order to provide robustness in watermark data we will use DWT based watermarking.

Dong Zheng *et al* [12] discuss a various domain based RST invariant image watermarking algorithm and various rectification based watermarking algorithm. In domain based algorithm they explained Fouier Mellion transform based watermarking algorithm (FMT), Log-polar mapping based watermarking algorithms (LMP), log-polar mapping based watermarking algorithms (ILMP) based watermarking algorithms. And in rectification based watermarking algorithm they explained template based watermarking algorithm and RST invariant feature based watermarking algorithm.

Sangita Zope *et al* [16] proposed robust copyright protection of raster images using wavelet based digital watermarking for protect copyright of raster images using wavelet transform. 2-D DWT is applied on each channel (R, G, and B) of raster image and watermark is embedded in low and high frequency bands at third level wavelet decomposition using haar wavelet.

Ye Xueyi, Deng Meng *et al* [3] According to the Zernike moments’ rotation invariance and scale invariance, a robust DWT-SVD watermarking algorithm is presented based on Zernike moment (ZM). The proposed not just has good resistance to rotation, scaling attacks, and as well, kinds of common signal processing, and can achieve blind extraction.

C. Discrete wavelet transform (DWT)

The transform of a signal is just another form of representing the signal. It does not change the information content present in the signal [8].

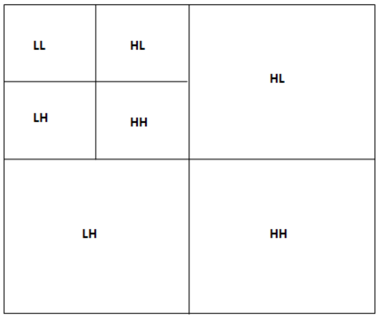


Figure.3 Decomposition model of DWT at level 2

The Wavelet Transform provides a time-frequency representation of the signal. The basic idea of applying DWT on the image processing is that by using discrete wavelet transform, the original image can be decomposed into lower frequency sub-band and higher frequency sub-bands. The sub-band LL1 represents the coarse-scale DWT coefficients while the coefficient sets LH1, HL1 and HH1 represent the fine-scale of DWT coefficients. To obtain the next coarser scale of wavelet coefficients, the sub-band LL1 is further processed until some final scale N is reached [19].

III. The Proposed Algorithm for Secure Transaction

After studying various visual cryptography schemes and watermarking schemes, we propose new technique for secure bank transaction. In this scheme we provide authenticity and data integrity of the shares using watermark technique. In our scheme we take one image as original image or host image and create shares using 2-out-of-2 visual cryptography scheme. When two shares will be created, server share is stored in bank database and client share is kept by user. The user will present with client share during all the transactions with bank. After that we apply the watermark technique on that client share image for providing the authentication and data integrity and send it on the open communication channel.

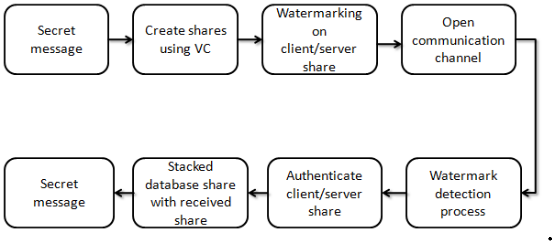

Secret message
Create shares using VC
Watermarking on client/server share
Open communication channel
Watermark detection process
Authenticate client/server share
Stacked database share with received share
Secret message

Figure.4 System Overview of Proposed Scheme

At the receiver side we apply watermark detection process on received client share and authenticate the client share. Then stack the server share with received client after extracting the watermark and reveal the original image. After then server send acknowledgement message to client for acceptability of user and the same process will done for authenticate the bank is called as two-way authentication. That means the server (bank) send their image share to client with embedding watermark (bank logo watermark). The user received bank's share and stacked database share and received share and authenticate the bank (server).Our scheme will be robust against various geometrical attacks and also provide authenticity and data integrity.

The beauty of our system lies in the fact that, if any attacker makes a copy of any image share to forge it later, the watermark will be distorted so for such forged image share our system will not allow the generation of host image from the stack of 2 image shares. Thus, the attacker will not get the original image.

Algorithm 1: Visual cryptography scheme.

Step 1: Read Input Binary Secret Image.
Step 2: Divide White Pixel into 4 sub-pixels using step 4.
Step 3: Divide Black Pixel into 4 sub-pixels using step 4.
Step 4: Random permuting the share generation.
Step 5: stop.

Algorithm 2: Geometrical invariant watermarking scheme.

2.1 Embedding Process:

Step 1: Let X represent the watermark embedding area, and use haar orthogonal wavelet filters to X; then obtain the band LL which has maximum energy. Divide LL into blocks Ai of size 4×4 where Yi^r is a vector, and λ_i is the non-zero SV of each block, and r is the rank of each block.

Step 2: Apply the basic logistic map to encrypt the watermark.

$x_{n+1} = \mu x_n(1 - x_n)$, 0< $x_n < 1, n = 0,1,2 \ldots\ldots$ [1]

Step 3: Calculate the value of Yi^r, Norms

$Yi^r = \sqrt{\sum_{j=1}^{r} \lambda_j * \lambda_j}$ [2]

N^{i} = Norms (Yi^r)/delta. [3]

Step 4: Embed bit using following method.
If b=1 then {if N is odd then N' = N +1 else N' = N} Else {if N is even then N' = N else N' = N +1}.

Step 5: Calculate the modified value and the modified vector as follows:
Norms (Yi') = N' ×Delta + (Delta/ 2) ,
Yi'= Yi× Norm(Yi')/ Norm(Yi))

Step 6: Apply inverse dwt to generate watermarked image.

2.2 Detection process:

Step 1: Use the saved Zernike moments to estimate and correct the geometric attacks; obtain the corrected watermarked image, and perform 1-level DWT decomposition to its watermark embedding area. Obtain the sub-band LL' which has maximum energy.

Step 2: Segment the sub-band LL" into blocks ' Ai of size 4×4, $Yi^{r}Yi^{r}$ = [λ_1, $\lambda_2, \lambda_3 \ldots\ldots, \lambda_r$]

where $\mathrm{YI}^{\prime\prime}$ is a vector, and λ_i is the non-zero SV of each block and r is the rank of each block.

Step 3: Calculate the value of $\mathrm{YI}^{\prime\prime}$, Norms using equation 1 and 2.

Step 4: Extract bit and extract watermark.

Step 5: Stacked extracted image with database share image with XORed operation.

IV. RESULT ANALYSIS

In the experiments, the gray level image Lena is selected as the vector image. The binary image is used as the watermark. To test the performance of the proposed, the PSNR is used to evaluate the invisibility of the proposed by comparing the difference between the original image and the watermarked.

The Table 2 and Table 3 and 4 demonstrate that the watermark can be better extracted by using Zernike moments to correct the rotation angle and scale factor. The simulation result has shown that the proposed work has good resistance to rotation and scale attacks.

Table 2 Rotation attacks

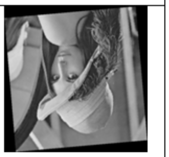
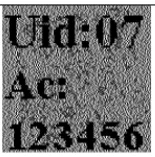
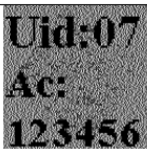
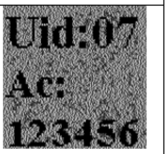
Rotation angle	10°	55°	185°
Rotated image			
Stacked image	 Uid:07 Ac: 123456	 Uid:07 Ac: 123456	 Uid:07 Ac: 123456
PSNR	59.1989	60.9671	58.5774
MSE	0.0782	0.0520	0.0902

Table 3 Scaling Attacks

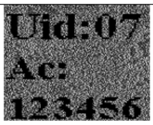
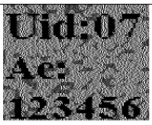
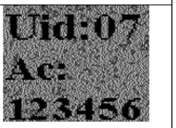
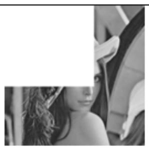
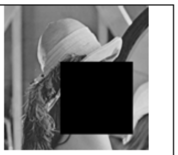
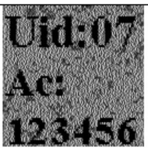
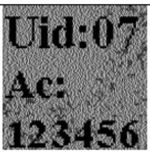
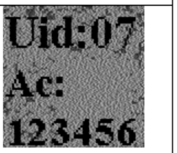
Size	0.7	2	1.2
Stacked image	 Uid:07 Ac: 123456	 Uid:07 Ae: 123456	 Uid:07 Ac: 123456
PSNR	57.9589	57.7356	57.8647
MSE	0.1040	0.1095	0.1063

Table 4 Cropping attack

attacked image			
Stacked image	 Uid:07 Ac: 123456	 Uid:07 Ac: 123456	 Uid:07 Ac: 123456
PSNR	57.9799	59.9882	59.1898
MSE	0.1035	0.0652	0.0784

V. CONCLUSION

In today's world internet banking is very common so there is a constant need of making these transactions more secure. Our proposed scheme thus offers two way authentications to the internet banking transaction. Our scheme will be robust against various geometrical attacks and also give good result against JPEG attacks, Noise attacks.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology - Eurocrypt '94, vol. 950, pp. 1 – 12, 1994.

[2] Jonathan Weir and WeiQi Yan, "Sharing Multiple Secrets Using Visual Cryptography",IEEE Transactions on Image Processing, 2009, pp.509-512.

[3] Ye Xueyi, Deng Meng, Wang Yunlu and Zhang Jing, "A robust dwt-svd blind watermarking algorithm based on zernike moments", IEEE Transactions on Image Processing, 2014, pp.1-6.

[4] Yi-chong zeng and Chi- Hung tsai, "High capacity Multi-scale sharing scheme", IEEE Transactions on image processing, ICIP 2013, pp.4536-4539.

[5] Z. zhou, G. R.Arce, and G. Di crescenzo, "Halftone visual cryptography", ICIP, Sept.2003, pp.521-524.

[6] Rohith s and Mr. Vinay G, " A Novel two stage Binary image security system using (2,2) visual cryptography.", IJCER, May-June 2012, pp.642-646.

[7] Chandrasekhara and Jagadisha, “Secure banking application using visual cryptography against fake website authenticity theft”, International Journal of Advanced Computer Engineering and Communication Technology, 2013, pp.1-5.

[8] Hailiang Shi, Nan Wang, Zihui Wen, Yue Wang, Huiping Zhao and Yanmin Yang, “An RST Invariant Image Watermarking Scheme using DWT-SVD”, IEEE , 2012, pp. 214-217.

[9] N. Askari, H.M. Heys, and C.R. Moloney, “An extended visual cryptography scheme without pixel expansion for halftone images”, NSERC, 2013, pp.1-6.

[10] Anushree Suklabaidya and G. Sahoo, “Visual Cryptographic Applications”, International Journal on Computer Science and Engineering, 6 Jun 2013, pp.455-464.

[11] Dong Zheng, Yan Liu, Jiying Zhao, and Abdulmotaleb El saddik, “A Survey of RST Invariant Image Watermarking Algorithms”, ACM Computing surveys, June 2007, pp.1-91.

[12] Dong Zheng, Yan Liu, and Jiying Zhao, “A Survey of RST Invariant Image Watermarking Algorithms”, IEEE, May 2006, pp.2086-2089.

[13] Jose J. harayil, E, S Karthik kumar and Neena susan Alex, “Visual cryptography using Hybrid Halftoning”, ELSEVIER, Sep.2012, pp.2117-2123.

[14] Meryem Benyoussef, SamiraMabtoul, Mohamed El Marraki, and Driss Aboutajdine, “Robust Image Watermarking Scheme using Visual Cryptography in Dual-Tree Complex Wavelet Domain”, JATIT, February 2014, pp.372-379.

[15] Jaishri Chourasia, “Identification and authentication using visual cryptography based fingerprint watermarking over natural image”, Springer, December 2013, pp.343-348.

[16] Sangita Zope, “Robust copyright protection of raster images using wavelet based digital watermarking”, IEEE, 2014, pp.3129-3132.

[17] Dr.M.A.Dorairangaswamy and B.Padhmavathi, “An Effective Blind Watermarking Scheme For Protecting Rightful Ownership of Digital Images”, IEEE, 2009, pp.1-6.

[18] Munesh Chandra, Shikha Pandey and Rama Chaudhary, “Digital Watermarking Technique for Protecting Digital Images”, IEEE, 2010, pp-226-233.

[19] Saeed K. Amirgholipour and Ahmad R. Naghsh-Nilchi, “Robust Digital Image Watermarking Based on Joint DWT-DCT”, International Journal of Digital Content Technology and its Applications, 2009, pp. 1-13.

[20] Akshya Kumar Gupta ang Mehul S. Raval, “A robust and secure watermarking scheme based on singular values replacement”, Indian Academy of Sciences, 2012, pp. 425-440.