

Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol 2, No.3, 2012

www.iiste.org



Recursive Visual Secret Sharing Scheme using Fingerprint

Authentication

Mayura Kinikar Viraj Thakur Sandesh Sonawane

Department of Computer Engineering

MAE, Alandi, Pune-411006

University of PUNE, INDIA.

Email: thakur.viraj1@gmail.com

Abstract

Recursive Visual Secret Sharing scheme takes the idea from the basic scheme of Visual cryptography to stack two transparent shares to obtain the original image. The paper proposes a scheme of recursive creation of shares using the basic scheme and embedding secrets into the shares. This results levels of share creation i.e. n - secrets equals $n/2$ levels. The Recursive visual cryptography produces shares from level $n-1$ when encrypted. For the purpose of user identification Biometric fingerprint authentication using minutiae extraction is provided with pixel pattern match and RGBA intensity match. Thus the proposed scheme would make efficient utilization of data.

Keywords: Recursive Visual Cryptography, Embedding secrets, secret sharing, Minutiae pattern match, authentication, levels of shares.

1. Introduction

Internet is one of the most popular communication channels but is insecure. Since it is an open and insecure medium, malicious users can intercept data. The fast growth of online applications results in the data security problem. In order to achieve data security, users need secure communication methods for transmitting secret messages over the Internet. Encryption is well-known method for achieving data security. It transforms secret information into an encrypted form, which looks like a random message. Transformation procedure is called encryption process and the result is called cipher text. A computational device is required to perform decryption of the cipher text. Therefore, the cost or efficiency of the hardware, complex algorithms and mathematical computations increase to encrypt and decrypt the data. Therefore, the cost increases and efficiency reduces and mathematical computations increase to encrypt and decrypt the data.

2. Data Security

Security of data has been a major issue from many years. Using the age old technique of encryption and decryption has been easy to track for people around. Providing security to data using new technique is the need of the hour. This project uses the technique of Visual cryptography and providing biometric authentication.

Thus using the above technique Recursive Visual cryptography would be implemented.

2.1 Objectives

To provide security in any real time application. To store more than one secret at a time. Providing efficient algorithm for storage and retrieval of images from database. To provide much more security by adding biometric authentication. Providing an algorithm for fingerprint recognition through minutiae pattern extraction and matching.

3. Visual Cryptography

One of the best known techniques to protect data such as image is Visual cryptography. Naor and Shamir introduced the visual cryptography scheme as a simple and secure way to allow the secret sharing of images without any cryptographic computations. [1]VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. [1] The basic scheme is referred to as the 2-out-of-2 VCS which is denoted as VCS.[2] Given an original binary image, it is encrypted in images, such that where a Boolean operation is is an image which appears as white noise, and is the number of noisy images. It is difficult to decipher the secret image using individual's. The encryption is undertaken in such a way that one or more out of the generated images are necessary for reconstructing the original image. In the case of (2, 2) VCS, each pixel in the original image is encrypted into two sub pixels called shares. [1]

The paper proposes the scheme of share creation taken from $N \times N$ share creation, we hereby propose the scheme of 2×2 Share creation proposed in this paper. Fig.1 denotes the shares of a white pixel and a black pixel.[1],[2],[12] Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel can be determined. If is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel. Therefore, the reconstructed image will be twice the width of the original secret image. [6]

4. Related Work

The topic of recursively hiding secrets within a share has been extensively researched. The scheme proposed in this paper applies to images and attempts to increase the efficiency of traditional VC to make it possible to hide extra secret information that serves as a steganographic channel.[10] The scheme involves recursive hiding of smaller secrets within a larger secret. It is obvious from the previous work that many thoughts have been given to the idea of recursive information hiding within visual cryptography.[11] However, the idea of embedding these types of recursive shares within the share and providing biometric security at the last level so that no previous shares would be recovered, to our knowledge, has never been considered.

4.1 Our contribution

There are two main contributions that are discussed within this paper. The first deals with recursive creation of shares. This involves a recursive multiple resolution VC scheme which allows smaller secret to be hidden within one large share. [2]

The second contribution is providing biometric security to the last level of share, such that when the last share is authenticated the upper level of embedded secrets would be revealed. The Fingerprint recognition algorithm would be used to provide biometric security to last level of client share.[3] The well known algorithm The median metric algorithm would be implemented.

5. Proposed Modules:

5.1 Data storage and retrieval: For the purpose of authentication there would a server database which stores all the biometric images of the User, and the other information related to the user. The database would store all the shares created at the runtime.[5]

5.2 Recursive Visual Cryptography

This method put forth has a secret image. Each secret is identified, two shares are created of that secret, as in the above figure. Share 1 is stored at client side and share 2 is stored at server side. In the next level the secret image 2 is taken and this secret is embedded in the application side share. The share that is stored at the application side has a secret embedded in it. Now this secret and share is converted into 2 shares and one stored at the client side and one store the server side. This method is followed recursively, such that at each level a secret would be embedded in the corresponding share. Thus this is the method of recursive visual cryptography.

5.2.1 Visual cryptography Algorithm:

Input: A $W \times H$ secret image $P, p(i,j)$ of P

Output: 2 shares $S_m, m=1$ to n ;

Process:

1. Generate sharing matrices C_0 and C_1 .
2. For each pixel $p(i,j), 1 < i < W$ and $1 < j < H$;

3. For l as the expanded pixel l to n ;

4. For $m=1$ to n

4.1: If $\text{pixel} p(i,j)=0$ (White), the pixel value

$S_m(i,j)=C_0(l,m)$

4.2: If $\text{pixel} p(i,j)=1$ (Black), the pixel value

$S_m(i,j)=C_1(l,m)$

5.2.2 Recursive storing of secrets Algorithm

1. For each $S_m, S_{m+1}=\text{next secret}, m=1$ to n .

2. $E_m = \text{Embedded secret in share } C_m, m = \text{Odd share}$;

3. Expand E_m using the 2×2 secret sharing scheme

4. Go to step 1 of RVC for each new secret
5. Store S_m , m =Even share stored at client side,
 S_m =Odd share stored at application side

Our policy is to provide biometric authentication at the client end such that when biometric authentication is provided by the client the secret would be stacked on the application side here and the secret would be revealed .

5.3 Biometric Authentication

There are various techniques provided for authentication in general scheme. Biometric authentication is the scheme provided by recognizing the human visual identity recognition. This paper would be implementing the Fingerprint Recognition with minutiae pattern match system. An efficient method for personal identification based on the pattern of human Fingerprint is proposed.[7] It is composed of image acquisition, image pre-processing to make a flat fingerprint then the minutiae patterns are extracted. Here there are various parameter match proposed ,firstly the RGBA pattern match would be done and then for resolution match the fingerprint ratio would be matched against the original registered.[8] Thus the authentication would be carried out. The results show that proposed method is quite effective.

5.3.1 Methodology:

In Fingerprint recognition image acquisition is an important step. Since Fingerprint is small in size and dark in colour, it is difficult to acquire good image. The colour image is captured .The image is then changed from RGB to gray level for further processing.[9]First of all to separate the fingerprint(minutiae pattern) from the image the boundaries of the finger and extract the minutiae a rough estimate of its center (C_x, C_y) is performed using the following

Formula

$$C_x = \arg \min(x)(I(\Sigma(x,y)))$$

$$C_y = \arg \min(y)(I(\Sigma(x,y)))$$

Where $I(x, y)$ is the fingerprint image intensity at point (x, y) . To find the exact pixel of the fingerprint, a part of image is binarized. [8]Then using the median matrix method the image pixel intensity would be calculated and median would be calculated and stored in the array. The algorithm used here is the median matrix method; here the edges of the biometric images would be detected by using edge detection algorithm.The RGBA intensity, resolution match by contracting the image to 32 x32 pixel resolution size would be provided for biometric authentication.

Thus the above ten parameters along with the median matrix method would be provided for authentication of users.

5.4 Decryption

After the biometric authentication is done the customer will give his part of the share. The two shares from

the

Application side and the client side would be superimposed and if they match the secret would be revealed.

[1] This would be done for each level and the embedded secrets at each level will also be revealed.

6. Advantages

The advantages of such type of Recursive Visual cryptographic scheme are: Original image security is provided. Secure Authentication is provided. Chance of fake share creation is not possible. More than one image be kept as secret. Recursive cryptography is first of the concepts to be implemented for security. Efficient and fast retrieval of images from database by storing the image id rather than the entire image. This scheme can be used in any company whose data is its asset.

7. Experiments And Results

Two shares are generated Share1 and Share2 as output of visual cryptography algorithm. One share along with username is kept by system and other is kept on card. For authentication user provides share which is on the card. The share extracted from this card is superimposed with corresponding share that is stored in the database, generates the original image.[7] From this fingerprint template image feature template is generated. Now this feature template is matched with fingerprint feature of newly provided fingerprint by the user.[8] As main intent of this paper is providing security to the Fingerprint template in the database, image processing algorithm for fingerprint feature extraction are derived from.[12] The working of proposed system is shown in shown above. For enrollment the image is taken from CASIA and NIST database.[7][8] After performing segmentation, normalization and feature extraction feature template is generated. Fingerprint template image (generated from feature template) and another binary image which is chosen by system Administrator is given as input to the visual cryptography algorithm. For each of the image the secret images from the shares are revealed.[12]

8. Conclusion

We have proposed a scheme to build a secure intense project in which security would a major issue, thus making security with the intense algorithm of Recursive visual cryptography, and adding biometric authentication to it. Various approaches adopted by researchers to secure the raw biometric data and template in database are discussed here. In this paper a method is proposed to store fingerprint template securely in the database using visual cryptography. Experimental results indicate that by applying recursive visual cryptography techniques on fingerprint template for more security, matching performance of fingerprint recognition is unaffected with extra layer of authentication.

9. References

- [1] Visual Cryptography Moni Naor and Adi Shamir EUROCRYPT -1994
- [2] Resolution Variant Visual Cryptography for Street View of Google Maps Jonathan ,WeirWeiQi YanQueen's University Belfast Belfast, BT7 1NN.
- [3] Visual Cryptography for Biometric Policy, Arun Ross & Asem Othem IEEE-Information Forensics 2011.

- [4] User friendly random grid based Visual Secret Sharing-Tzung Chen & Kai Hsiang Tsao, National Chiayi University, Taiwan, ROC.
- [5] Fast and Efficient Visual cryptography for Medical Images-S.Manimurugan.K.Porukumaran, Anna University Coimbatore, India
- [6] Progressive Visual Cryptography with Unexpanded shares-Young Chang Hou & Zen-Yu Quan, IEEE – Information Security and Forensics.
- [7] N. Agrawal and M. Savvides, “Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching,” in Proc. Computer Vision and Pattern Recognition Workshop, 2009.
- [8] A. Jain, P. Flynn, and A. Ross, Handbook of Biometrics. New York: Springer, 2007.
- [9] R.Ito, H. Kuwakado, and H. Tanaka, “Image Size Invariant Visual Cryptography,” IEICE Transactions of Fundamentals of Electronics, Communications and Computer Sciences.
- [10] J. Weir and W.-Q. Yan, “Dot-size variant visual cryptography,” in IWDW '09: Proceedings of the 8th International Workshop on Digital Watermarking..
- [10] M. Gnanaguruparan and S. Kak, “Recursive hiding of secrets in visual cryptography,” Cryptologia.
- [11] D. Chaum, Secret-ballot receipts: True voter-verification elections, IEEE Security and Privacy.











Pixel	Probability	Shares		Superposition of the two shares	
		#1	#2		
□	$p = 0.5$				White Pixels
	$p = 0.5$				
■	$p = 0.5$				Black Pixels
	$p = 0.5$				

Figure 1. Pixel expansion scheme

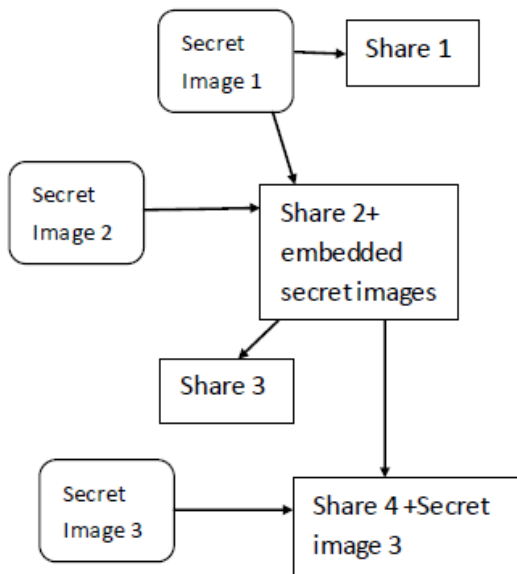


Figure 2. Recursive Creation of shares

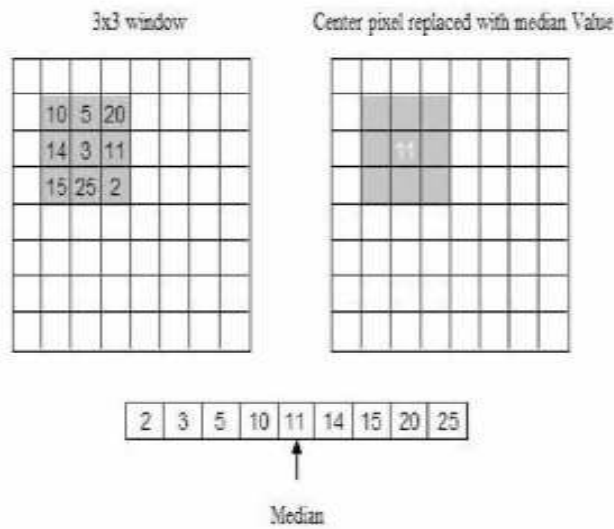


Figure 3. Median matrix method

This academic article was published by The International Institute for Science, Technology and Education (IISTE). The IISTE is a pioneer in the Open Access Publishing service based in the U.S. and Europe. The aim of the institute is Accelerating Global Knowledge Sharing.

More information about the publisher can be found in the IISTE's homepage:

<http://www.iiste.org>

The IISTE is currently hosting more than 30 peer-reviewed academic journals and collaborating with academic institutions around the world. **Prospective authors of IISTE journals can find the submission instruction on the following page:**

<http://www.iiste.org/Journals/>

The IISTE editorial team promises to review and publish all the qualified submissions in a fast manner. All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Printed version of the journals is also available upon request of readers and authors.

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digital Library, NewJour, Google Scholar

