ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

De-identifying Fingerprint Image using Grey-Level Extended Visual Cryptography Scheme for Enhancing Privacy and Security

Dhara Kumari[1], Dr. Dinesh Kumar[2], Dr. Rajni Sharma[3]

M-Tech Scholar, Dept. of CSE, Shri Ram College of Engineering and Management, Palwal, India[1]

HOD, Dept. of CSE, Shri Ram College of Engineering and Management, Palwal, India [2]

Assistant Professor, Dept. of Computer Science, PT.J.L.N. Govt P.G College Faridabad, India[3]

ABSTRACT: This paper presents an application and technology, Fingerprint touch that provides a secure method of storing fingerprint images (Templates) in central database as paramount importance due to the potential threat of access by unauthorized and unknown person. This application can be done possible using visual cryptography techniques with pixel sharing using GEVCS (Gray-Level Extended Visual Cryptography Scheme) method based on the EX-OR operation for biometric privacy such as fingerprint images. In this procedure we can dithered a private fingerprint image into two host images(known as sheets)that are stored in two separate database servers such that the private image can be revealed only when both sheets are simultaneously available; at the same time but the individual sheet images do not reveal the identity of the private image. Using the encryption algorithm, we can store the images in the database. The stored images are encrypted and while verification that images are decrypted. Experimental results show that this application is feasible in the cases where the privacy of the data is more important than the accuracy of the system and the obtained computational time is satisfactory.

KEYWORDS: Visual Cryptography; Biometric Templates; Fingerprint Images; GEVCS; EX-OR operator; Security.

I. INTRODUCTION

Biometrics represent the perfect solution to the problem of digital authentication, by measuring unique physical characteristics compared to other, more traditional token-based approaches, because biometrics deals with automated method of identifying a person or verifying the identity of a person based on the physiological or behavioral characteristics such as face, fingerprints, iris[1].

In this paper, we produce the biometric data (like fingerprint), since fingerprint biometric is easily available and highly reliable compared too many other biometrics. A fingerprint is the reproduction of a fingertip epidermis, produced when a finger is pressed against a smooth surface. The most evident structural characteristic of a fingerprint is its pattern of interleaved ridges and valleys. Ridges and valleys often run parallel but they can bifurcate or terminate abruptly sometimes. A biometric authentication system operates by acquiring raw biometric data from subject (e.g., fingerprint image), extracting a feature set from the data (e.g., minutia points), and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity. The template of a person in the database is generated during enrollment and is often stored along with the original raw data. This has heightened the need to accord privacy to the subject by adequately protecting the contents of the database.

II. ANALYSIS OF PREVIOUS WORK

Literature Survey is most important part of the any research area for gathering a new type of information during the analysis that produce new technology, application and other beneficial information. A number of techniques have been developed to improve the privacy and security of fingerprint templates which are hardware based and software based solutions. At the very beginning keys were used to protect the privacy of fingerprint information [4].

Biometric cryptosystems is a new technique which combines biometrics and cryptography [5], and is popularly known as crypto-biometric systems. The system is also called helper data-based system. Biometric cryptosystems are classified into two classes based on how helper data is generated: key binding schemes and key generating schemes. In key binding schemes, the key or helper data is obtained by binding a chosen key to the biometric template. At authentication, keys are generated from the helper data by applying a key retrieval algorithm [6]. Fuzzy commitment scheme [7], fuzzy vault scheme [8], shielding functions [9] are various approaches to this technique. While in key generating schemes, the helper data is obtained only from the biometric template. Keys are generated from the helper data and a given biometric template [10].Various approaches to this technique are private template scheme [11] and quantization schemes [12]. The technique based on cryptosystem is so inconvenient that the original fingerprint can be reconstructed if the key and protected fingerprint is stolen.

- Teoh *et al.* [13] proposed a bio-hashing approach in which the fingerprint features are combined with a pseudo random number before storing into the database. The technique has significant advantages than solely biometric systems in the sense that it has zero equal error rates and it makes a clear separation between genuine and imposter users. Hence the technique allows the elimination of false accept rates without suffering from increased occurrence of false reject rates.
- Jain and Prabhakar [14] (2001) Most of the fingerprint identification system employs techniques based on minutiae points.
- Chikkerur et al. [15] (2006) Although the minutiae pattern of each finger is quite unique, noise and distortion during the acquisition of the fingerprint and errors in the minutiae extraction process results in a number of missing and spurious minutiae. Ridge feature-based method is used to remove this problem. It uses orientation of frequencies of ridges, ridge shape and texture information for fingerprint matching.
- Yusufi et al. [16] (2007) The correlation based technique uses two fingerprint images superimposed and correlate the corresponding pixels for different alignment.
- Latter on Agrawal et al. [17] (2008) proposed gradient based approach to capture textural information by dividing each minutiae neighborhood locations into several local regions of which histograms of oriented gradients are then computed to characterize textural information around each minutiae location.

III. FUNCTIONING OF PROPOSED SYSTEM

In this paper, we proposed the visual cryptography techniques with pixel sharing using GEVCS (Gray-Level Extended Visual Cryptography Scheme) method based on the EX-OR operation to protect the privacy of biometric information (viz., raw images) by decomposing the original image into two images in such a way that the original image can be revealed only when both images are simultaneously available; further, the individual component images do not reveal any information about the original image. [1]. Figure 1 show block diagram of the proposed approach using Fingerprint Recognizer for system.

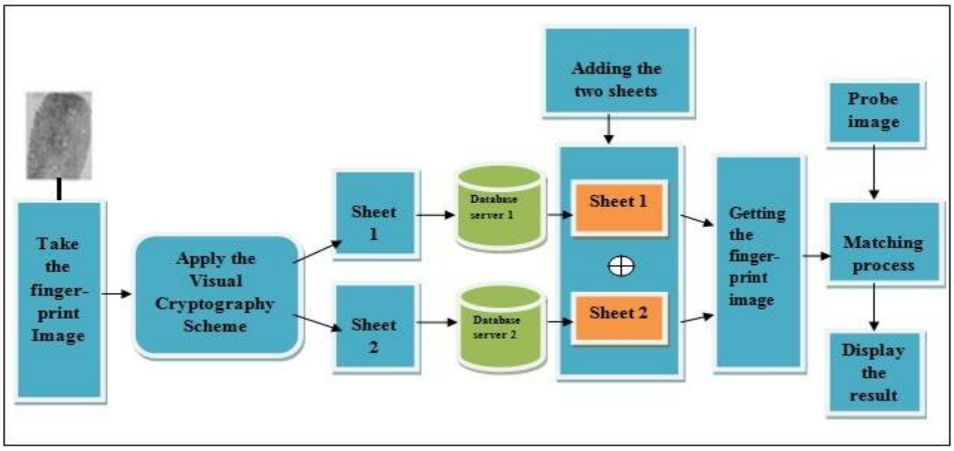

Fig. 1 Structure of Fingerprint Recognizer

DOI: 10.15680/IJIRCCE.2016. 0405020

In this figure there are two possibilities will be generated:

- Enrollment Process
- Authentication Process

During the enrollment process, System takes the input as an original fingerprint image & applies the Visual Cryptography on that image. After applying the in encryption phase it will create the two sheets of the original fingerprint image. Figure 2 shows block diagram of the Enrollment Process.

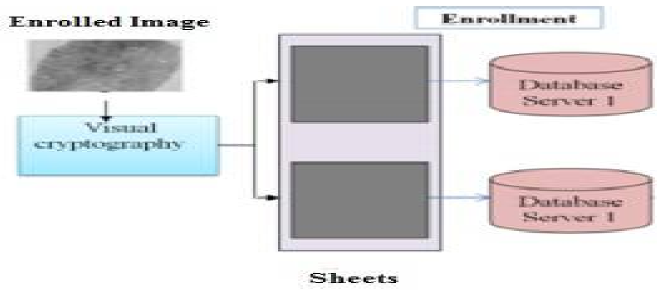

Fig. 2 Phase of Enrollment Process

During the Authentication process, two sheets are stored on the two different database servers separately. So, it will combine the two sheets getting from the two database servers & obtain the original image that will be matched with the registered image. Figure 3 shows block diagram of the Authentication Process.

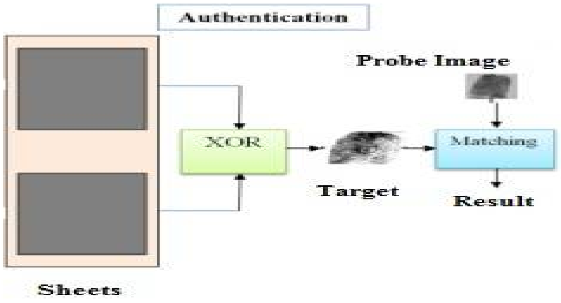

Fig. 3 Phase of Authentication Process

The basic working of the Fingerprint recognizer System is shown in the Fig 1. The fingerprint recognition can be grouped into three subcategories: fingerprint enrollment, verification and fingerprint identification. The authentication phase involves combining both the sheets simultaneously in order to recover the original fingerprint image by using the EX-OR operation. After getting the original fingerprint image it will be match with the registered image. Finally display the matching result. Once the matching score is computed, the reconstructed image is discarded. Further, cooperation between the two servers is essential in order to reconstruct the original biometric image. For fingerprints, as shown in Fig. 1, the biometric image is decomposed by the visual cryptography scheme and two noise-like images known as sheets are produced. Additionally, the proposed approach addresses the following template protection requirements as Diversity, Revocability, Security and Performance.

The rest of the paper is organized as follows. In Section IV a basic introduction to visual cryptography and its extensions are presented. Sections V discuss the proposed approach for securing fingerprint images and future scope. Section VI concludes the paper.

IV. VISUAL CRYPTOGRAPHY

Visual cryptography is a cryptography technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption can be performed without using any mathematical calculations. In visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. Visual Cryptography [2] is the technique in which original fingerprint image will be encrypted into the n number of sheets. In the case of enrollment process when applying the Visual Cryptography on the fingerprint image it will create the two sheet images of the original image. One of the sheets will be store on the first database server & another sheet will be store on the second database server whereas, In decryption process certain numbers of sheet images are required to obtain the original fingerprint image. Suppose consider the one example, in that original fingerprint image is F, it will be divides into the n sheets, such that, F=Sh1+Sh2+Sh3+…..+Shk Where + is the Boolean operation, Shi ∈ 1, 2, 3,…,k is the sheet images, k<n and n is the number of sheet images. It is difficult to obtain the original image F using the individual Sheets.

A. Explanation of Two-out-of-Two Scheme (2 subpixels layer):

The encoding scheme is to share a binary image into two different shares Share 1 and Share 2. Each pixel is divided into a black and white subpixel placed next to each other. For the case of white pixel, one of the two combinations of subpixels will be chosen with a probability of 0.5 to represent the pixel in each of the shares. When these shares are placed one on top of the other, the pixel are visually ORed[1] and hence a white pixel looks gray (half black and half white) to the human eye. The pixels are chosen in a similar manner for the case of a black pixel. But when the subpixels are visually ORed, the two black subpixels placed next to each other appear as a single black pixel. This idea can be applied to images to develop a basic Two-out-of-Two scheme by using 2 subpixels. The 2 out of 2 visual secret sharing problems can be solved by the following collection of $n \times n$ matrices:

C0 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ }

C1 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ }

Pixel		Share 1	Share 2	Result
□	$P = {}^{1}/_{2}$	◧	◧	◧
	$P = {}^{1}/_{2}$	◨	◨	◨
■	$P = {}^{1}/_{2}$	◧	◨	■
	$P = {}^{1}/_{2}$	◨	◧	■

Fig. 4 Partitions for black and white pixels for 2-out-of-2 scheme (2 subpixels)

Fig. 5 Original Fingerprint Image

When applying Visual Cryptography on the fingerprint image shown in the figure 5, it will be generate the two transparency images from the original fingerprint image shown in figure 6 and 7. The value of the original pixel P can be obtained by combining the two shares. If the original pixel is a black, then we can get the two black subpixels; if the original pixel is a white, then we can obtain the one black subpixel and one white subpixel. Therefore, the size of the obtaining image will becomes the large the original image and there will be 50% loss in contrast, but reconstructed image will be visible. To securing the fingerprint images two sheets of the original image are stored on two different database servers separately. If anybody want to generate the original fingerprint image, both sheet images are required at the same time. No one can generate the original image using only the single sheet image. Fig.6 shows the transparency image 1 which will be stored on the database server first and Fig.7 shows the transparency image 2 which will be stored on the image database server second.

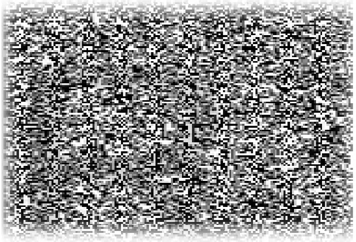

Fig. 6 Transparency image 1

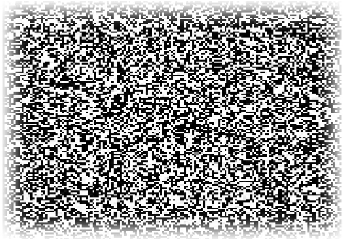

Fig. 7 Transparency image 2

[1]The term "ORed" as used in this paper refers to when two values are combined, they are bitwise ORed together.

B. GREY-LEVEL EXTENDED VISUAL CRYPTOGRAPHY SCHEME (GEVCS)

VCS allows one to encode a secret image into sheet images, each revealing no information about the original. Since these sheets appear as a random set of pixels, they may pique the curiosity of an interceptor by suggesting the existence of a secret image. Ateniese introduced such a framework known as the extended VCS. They proposed a theoretical framework to apply extended visual cryptography on grayscale images (GEVCS) and also introduced a method to enhance the contrast of the target images. The GEVCS operates by changing the dynamic range of the original and host images, transforming the gray-level images into meaningful binary images and then applying a Boolean operation on the halftoned pixels of the two hosts and the original image. However, some of these pixels (in the host and the original) have to be further modified. This is done by following way: Pixel Expansion and Encryption.

V. SECURING PRIVATE FINGERPRINT TEMPLATES

The uses of basic visual cryptography for securing fingerprint templates however, no experimental results were reported to demonstrate its efficacy [3]. Moreover, basic VCS leads to the degradation in the quality of the decoded images, which makes it unsuitable for matching process, as shown in fig 4, where the white background of the original image becomes gray in the decrypted (target) image [2].The overlaying or superimposing operation in visual cryptography is computationally modeled as the binary OR operation which causes the contrast level of the target image to be lowered. Loss in contrast in target images could be addressed by simply substituting the OR operator with the XOR operator. Furthermore, the target image can be down-sampled by reconstructing just one pixel from every block. Thus, the reconstructed image will be visually appealing while requiring less storage space.

VI. Conclusion and Future Work

Biometric is the art of identifying the individuality of person on the basis of physical and behavioral traits such as iris, face, fingerprint and voice. General Biometric Systems works on the basis of registration, enrollment and authentication phases. The objective behind designing this system is to privacy and protecting the Biometric data using the Visual Cryptography Techniques In this the templates are divided into two images using VCS, so it is impossible to recover the original image without accessing both the shares. The XOR operator is used to superimpose the two images and fully recover the original template. The designed algorithm works the better in the performance and gives the better results than the existing pixel expansion technique. The implemented system gives better image quality so that fingerprint matching process becomes simple and efficient. Future work can be achieved by using 2-out-of-2 VCS with 4-subpixel layout using the Extended Gray-level Visual Cryptography Scheme (EGVCS) that is based on the XOR and XNOR operation in which we combine two biometric information (face and fingerprint templates) for privacy and protecting the all type of information during the transmission of data over the Internet. It also works on the central database for biometric information (like face, fingerprints, and iris).

REFERENCES

1. Jain, P. Flynn, and A. Ross, Handbook of Biometrics. New York: Springer, 2007.
2. Moni Naor, Adi Shamir, Visual Cryptography, Department of Math and Computer Science, Rehovot, 1994.
3. Y. Rao, Y. Sukonkina, C. Bhagwati, and U. Singh, "Fingerprintbased authentication application using visual cryptography methods (improved id card)," in Proc. IEEE Region 10 Conf., Nov. 2008, pp.1–5.
4. S. Li and A. C. Kot, "A novel system for fingerprint privacy protection," in Proc. 7th Int. Conf. Inform. Assurance and Security (IAS),Dec. 5–8, 2011, pp. 262– 266.
5. A. Ross and A. Othman, "Visual cryptography for biometric privacy," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81, Mar. 2011.
6. AK Jain, K Nandakumar, A Nagar, Biometric template security. EURASIP J Adv Signal Process, 1–17 (2008).
7. A Juels, M Wattenberg, A fuzzy commitment scheme. 6th ACM Conf on Computer and Communications Security, 28–36 (1999).
8. A Juels, M Sudan, A fuzzy vault scheme. Proc 2002 IEEE Int Symp on Information Theory, 408 (2002).
9. J-P Linnartz, P Tuyls, New shielding functions to enhance privacy and prevent misuse of biometric templates. Proc 4th Int Conf Audio- And Video-Based Biometric Person Authentication, 393–402 (2003).
10. AK Jain, K Nandakumar, A Nagar, Biometric template security. EURASIP J Adv Signal Process, 1–17 (2008).
11. G Davida, Y Frankel, B Matt, On enabling secure applications through off-line biometric identification. Proc of IEEE, Symp on Security and Privacy, 148–157 (1998).
12. H Feng, CC Wah, Private key generation from on-line handwritten signatures. Inf Manag Comput Secur 10(18), 159–164 (2002).
13. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, 2004.
14. JAIN A. K. AND PRABHKAR S. 2001. Fingerprint Matching Using Minutiae and Texture Features. Proceeding of International Conference on Image Processing (ICIP), pp. 282-285.
15. CHIKKERUR S., PANKANTI S., JEA A., AND BOLLE R. 2006. Fingerprint Representation using Localized Texture Features. The 18th International Conference on Pattern Recognition.
16. YOUSIFF A. A. A., CHOWDHURY M. U., RAY S., AND NAFAA H. Y., 2007. Fingerprint Recognition System using Hybrid Matching Techniques. 6th IEEE/ACIS International Conference on Computer and Information Science, pp. 234- 240.
17. AGGARWAL G., RATHA N. K., TSAI-YANG J., AND BOLLE R. M. 2008. Gradient based textural characterization of fingerprints. In proceedings of IEEE International conference on Biometrics: Theory, Applications and Systems.