International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

A FINGERPRINT BIOMETRIC PRIVACY USING VISUAL CRYPTOGRAPHY

M.Suganya[1] and Dr.S. Suganya[2],

[1]*Research Scholar, Dept of Computer Science, Rathnavel SubramaniamCollege of Arts & Science, Sulur, India.*

[2]*Associate Professor, Dept of Computer Science, Rathnavel Subramaniam College of Arts & Science, Sulur, India.*

Abstract-*Biometric authentication systems are gaining wide-spread popularity in recent years due to the advances in sensor technologies as well as improvements in the matching algorithms. Preserving the privacy of digital biometric data stored in a central database has become of paramount importance. VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret image. This technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image. The stored images are encrypted and while verification that images are decrypted. This work implements visual cryptography for color images in a biometric application. The project modules have a strong authentication and robustness scheme.*

Keywords: Fingerprint Image, Biometric, Visual Cryptography, Enrollment, Authentication

1. Introduction

BIOMETRICS is the science where identity of an individual based on physical and behavioral traits such as face, fingerprints, iris, retina and voice. For automated personal identification biometric authentication is getting more attention. When biometric authentication is used, system operates by getting raw biometric data from a subject then extracts the feature set from a subject and compare that feature set with the template stored in database, the template of a person in the database is generated during enrollment and is often stored with original raw data.

To deal with the security problems of secret images, various image secret sharing schemes have been developed. Visual cryptography is introduced first by Noar and Shamir in 1994. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation.

In this work, the use of visual cryptography is explored to protect the privacy of biometric data (raw image). In this technique first the private image is decomposed into two images in such a way that the original image can be obtained only when both the original image is available further the individual image cannot create private image. Fig 1 shows block diagram of the proposed approach. During the enrollment process, the private biometric data is sent to trusted entity once the trusted party acquires it the biometric data is transferred into two images and original data is removed. The created components are then transmitted and stored in two different databases. During the identification process the trusted entity sends request to each server and corresponding sheets are sent. Sheets are overlaid to each other to create the original image.

The remaining work is organized as follows: section 2 discussed about the previous work, Section 3 describes the methodology used for fingerprint authentication, Section 4 shows the experimental result for the proposed methodology and Section 5 summarizes the conclusion of this work.

2. Literature Survey

Preserving the privacy of digital biometric data (e.g., face images) stored in a central database has become of paramount importance. Ross and Asem (2011) explores the possibility of using visual cryptography for imparting privacy to biometric data such as fingerprint images, iris codes, and face images.Biometrics Systems consists of the physical and behavioral features for e.g. face, fingerprints etc. So Rajanwar et al introduced a design to protect biometrics data from the various attacks. Here using the concept of visual cryptography, where cryptography is the concept of sending

and receiving encrypted messages and that can be decrypted by the authorized persons with the required keys only.Kang et al (2011) introduces the concept of visual information pixel (VIP) synchronization and error diffusion to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality.Hou et al (2011) proposed a brand new sharing scheme of progressive VC to produce pixel-unexpanded shares. In this research, the possibility for either black or white pixels of the secret image to appear as black pixels on the shares is the same, which approximates to 1/n. Therefore, no one can obtain any hidden information from a single share, hence ensures the security.

Conventional visual secret sharing schemes generate noise-like random pixels on shares to hide secret images. It suffers a management problem, because of which dealers cannot visually identify each share. Lee et al (2012) propose a general approach to solve the above- mentioned problems; the approach can be used for binary secret images in non-computer-aided decryption environments.A pixel-expansion-free threshold VCSs approach based on an optimization technique is proposed by Chiu et al (2011) in order to encrypt binary secret images. In addition to contrast, consider blackness as a performance metric in the evaluation of the display quality of recovered images. Furthermore, try to promote the contrast by slightly relaxing the density-balance constraint.Phishing is an attempt by an individual or a group to get personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. James introduced a new approach named as "A Novel Anti-phishing framework based on visual cryptography "to solve the problem of phishing. Here an image based authentication using Visual Cryptography is implemented.Biometric cryptosystems and cancelable biometrics represent emerging technologies of biometric template protection addressing these concerns and improving public confidence and acceptance of biometrics. A comprehensive survey of biometric cryptosystems and cancelable biometrics is presented by Rathgeb et al (2011).

Simoens et al (2012) analyze the vulnerabilities of biometric authentication protocols with respect to user and data privacy. Our goal is to emphasize that when going beyond the usual honest-but-curious assumption much more complex attacks can affect the privacy of data and users.The design of single-use biometric security systems is analyzed by Lai et al (2011) from an information theoretic perspective. A fundamental trade-off between privacy, measured by the normalized equivocation rate of the biometric measurements, and security, measured by the rate of the key generated from the biometric measurements, is identified.Fuzzy commitment is an efficient template protection algorithm that can improve security and safeguard privacy of biometrics. Zhou et al (2011) gives a comprehensive analysis on security and privacy of fuzzy commitment regarding empirical evaluation.Bringer et al (2013) presents a tutorial overview of the application of techniques of secure two-party computation (also known as secure function evaluation) to biometric identification. These techniques enable to compute biometric identification algorithms while maintaining the privacy of the biometric data.

Wang et al (2012) introduced a theoretical framework for the analysis of privacy and security trade-offs in secure biometric authentication systems. Our analysis highlights the revocability and reusability properties of key-based systems and exposes a subtle design trade-off between reducing information leakage from compromised systems and preventing successful attacks on systems whose data have not been compromised.Data security and privacy are crucial issues to be addressed for assuring a successful deployment of biometrics-based recognition systems in real life applications. A template protection scheme exploiting the properties of universal background models, eigen-user spaces, and the fuzzy commitment cryptographic protocol is presented by Argones et al (2012).Yuan and Shucheng (20103) propose a novel privacy-preserving biometric identification scheme which achieves efficiency by exploiting the power of cloud computing. In proposed scheme, the biometric database is encrypted and outsourced to the cloud servers.Biometric encryption (BE) is highlighted as a prominent example of Privacy by Design, where privacy is embedded as core functionality in the biometric system. BE binds a digital key to (or extracts the key from) the biometrics. Earlier technical challenges to this new technology, as well as recent advances, are presented by Cavoukian et al (2012).

3. Research Methodology

This section gives the brief explanation of visual cryptography and methodology used for fingerprint biometric privacy.

3.1 Visual Cryptography

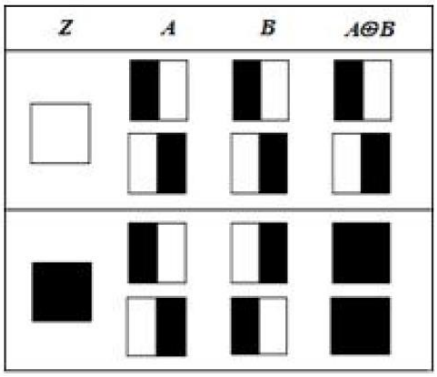
Cryptography is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. This scheme is referred to as the k-out-of-n VCS which is denoted

as (k,n)VCS. Given an original binary image, it is encrypted in n images, such that

$$T = S_{h1} \oplus S_{h2} \oplus S_{h3} \oplus \dots\dots\dots\dots S_{hn} \quad (1)$$

WhereÅ is a Boolean operation, Shi, hi Î 1,2,....k is an image which appears as white noise, kd"n, and n is the number of noisy images. It is difficult to decipher the secret image T using individuals Shi's. The encryption is undertaken in such a way that k or more out of the n generated images are necessary for reconstructing the original image T. In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. For biometric privacy, here 2-out-of-2 scheme is using.

TABLE -1: ENCODING A BINARY PIXEL P INTO 2 SHARES A AND B



In this scheme for sharing a single pixel p, in a binary image Z into two shares A and B is illustrated in Table I. If p is white, one of the first two rows of Table 1 is chosen randomly to encode A and B. If p is black, one of the last two rows in Table 1 is chosen randomly to encode A and B. Thus, neither A nor B exposes any clue about the binary color of p. When these two shares are superimposed together, two black sub-pixels appear if p is black, while one black sub-pixel and one white sub-pixel appear if p is white as indicated in the rightmost column in Table 1. Based upon the contrast between two kinds of reconstructed pixels can tell whether p is black or white.

3.2 Proposed Approach

Protecting template in the database securely is one of the challenges in any biometric system. Here visual cryptography is applied to biometric authentication system. In this system, there are two modules: Enrollment module and Authentication module.

Enrolment module:

During the enrollment process, administrator collects the template and performs image scrambling. Image scrambling is used to make images visually unrecognizable such that unauthorized users have difficulty decoding the scrambled image to access the original image. Image scrambling is done by applying the above permutation algorithm. Using the key value some permuted sequence will be generated and apply the sequence to the image. The original image can be decomposed into blocks; each one containing a specific number of pixels. The blocks are transformed into new locations by the above permuted sequence, which produces the scrambled image. The scrambled image is then sent to a trusted third-party entity. Once the trusted entity receives it, the scrambled image is decomposed into two noisy images (i.e., sheets) and the original data is discarded. The decomposed components are then transmitted and stored in two different database servers such that the identity of the private data is not revealed to either server.

Authentication module:

During the authentication process, the trusted entity sends a request to each server and the corresponding sheets are transmitted to it. Sheets are overlaid (i.e., superimposed) in order to reconstruct the scrambled image. An inverse permutation sequence is obtained by using the same key, and applies this sequence to the scrambled image in-order to reconstruct the original image.

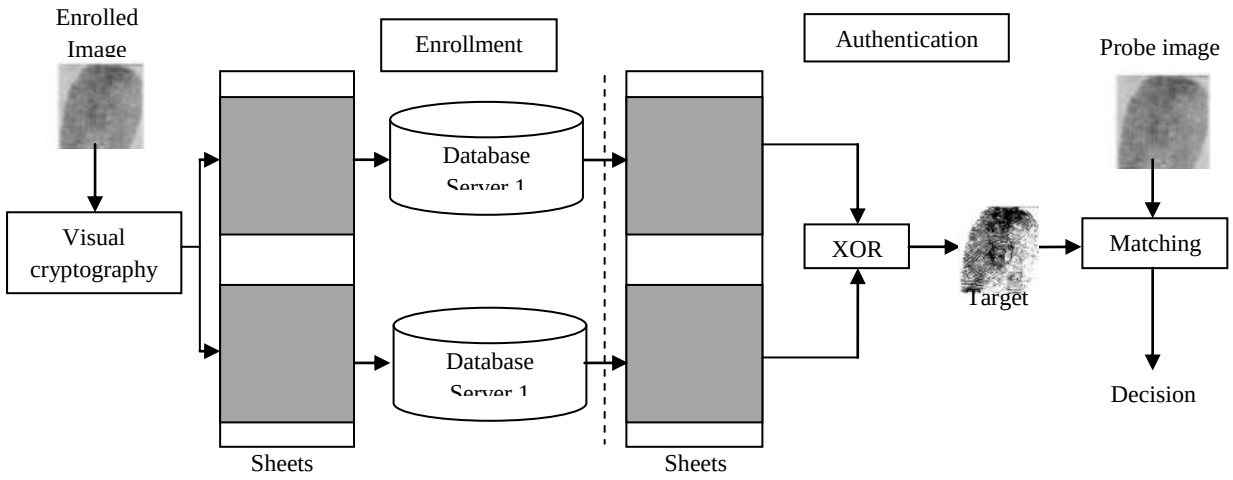


Fig -1: Proposed approach for de-identifying and storing a fingerprint image

By using the proposed method, as shown in Fig. 1, the biometric template is scrambled and decomposed by the visual cryptography scheme and two noise-like images known as sheets are produced.

4. Experimental Results

In the case of fingerprints, the performance of the proposed technique was tested on the NIST-4 fingerprint database2 containing inked fingerprints exhibiting large variations in quality. The database consists of the grayscale images of 2000 fingers with two impressions per finger. One of these impressions was used as a probe image and the other was added to the gallery. Since the proposed technique was devised for binary fingerprint images, a threshold value was used to generate the binary image for each probe. Each binary image was then decomposed into two sheets using VCS. The sheets were superimposed to get the target image. The reconstructed as well as the original grayscale fingerprint probes were matched against the impressions in the gallery. These experiments suggest the possibility of decomposing and storing fingerprint images.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 given on the user ID Card. Table 2 shows the result of using the reconstructed fingerprints as probes; the performance is reported as a function of the different threshold values used to binarize the original probe images. It is observed that a threshold of 190 results in an EER of 7.65%.

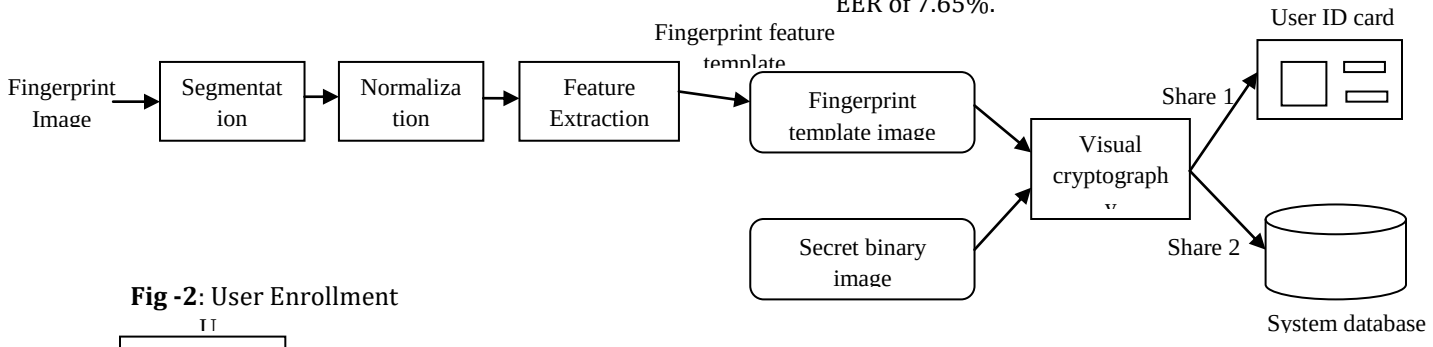


Fig -2: User Enrollment

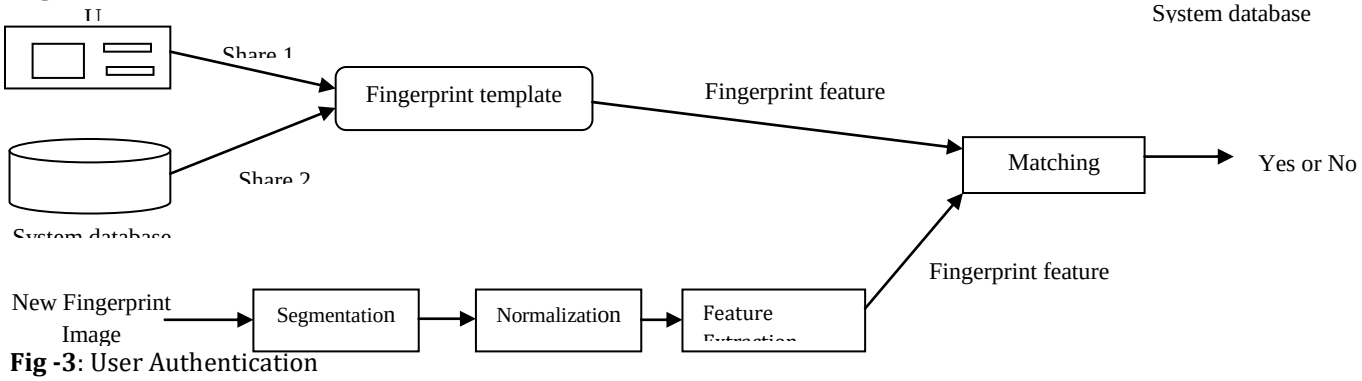


Fig -3: User Authentication

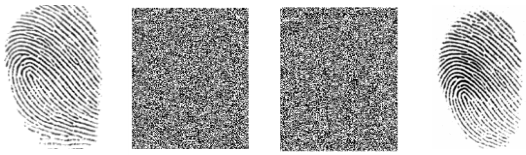
TABLE -2:
EQUAL ERROR RATE (%) AT DIFFERENT THRESHOLD VALUES

Threshold	Equal Error Rate
140	29.5
170	15.9
190	7.65

For authentication user provides share which is on the ID card. The share extracted from this card is superimposed with corresponding share that is stored in the database, generates the Fingerprint template image as shown in figure 5. From this fingerprint template image feature template is generated. Now this feature template is matched with fingerprint feature of newly provided fingerprint image using hamming distance.

(a) (b) (c)

Fig -4: (a) Fingerprint Image (b) Fingerprint segmentation (c)Extracted feature template



(a) (b) (c) (d)

Fig -5: (a) Fingerprint template image (b) Share1 (c) Share2 (d) Result of superimposing of share1 and share 2

In this experiment, the possibility of exposing the identity of the secret image by using the sheet images in the matching process is investigated. For this experiment, the sheet images for three different fingerprint samples of the same subject were first computed. Next, the reconstructed images and the corresponding sheets were independently used in the matching process (i.e., sheet image 1 of all the private images were matched against each other; sheet image 2 of all the private images were matched against each other; reconstructed images of all the private images were matched against each other).The public datasets used in this experiments were datasets A. This experiment resulted in three EERs: the first was a result of using the reconstructed target images for matching, while the second and the third EERs were a result of using the first sheet and second sheet, respectively, for matching. The results in Table 3 confirm the difficulty of exposing the identity of the secret face image by using the sheets alone.

TABLE -3: EQUAL ERROR RATE (%) FOR THE EXPERIMENT SHOWS THE INDIVIDUAL SHIFT IMAGES TO REVEAL THE SECRET IMAGES

	ERR (%)
Reconstructed vs Reconstructed	2.1
Sheet 1 vs Sheet 1	39.2
Sheet 2 vs Sheet 2	34.6

5. Conclusion

In the proposed system visual cryptography techniques is applied to protect fingerprint template in the database as well as providing extra layer of authentication to the existing fingerprint based authentication system. This work explored the security of visual cryptography by scrambling the image using random permutation. Here, the templates are scrambled and decomposed into two noises like images using VCS, and since the spatial arrangement of the pixels in these images varies from block to block, it is impossible to recover the scrambled image without accessing both the shares and an XOR operator is used to superimpose the two noisy images to get the scrambled image. Experimental results indicate that by applying visual cryptography techniques on fingerprint template for more security, matching performance of fingerprint recognition is unaffected with extra layer of authentication

REFERENCES

[1] Argones Rua, Enrique, Emanuele Maiorana, Jose Luis Alba Castro, and Patrizio Campisi. "Biometric template protection using universal background models: An application to online signature." Information Forensics and Security, IEEE Transactions on 7, no. 1 (2012): 269-282.

[2] Bringer, Julien, Hervé Chabanne, and Alain Patey. "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends." Signal Processing Magazine, IEEE 30, no. 2 (2013): 42-52.

[3] Cavoukian, Ann, Michelle Chibba, and Alex Stoianov. "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to

Deployment." Review of Policy Research 29, no. 1 (2012): 37-61.

[4] Chiu, Pei-Ling, and Kai-Hui Lee. "A simulated annealing algorithm for general threshold visual cryptography schemes." Information Forensics and Security, IEEE Transactions on 6, no. 3 (2011): 992-1001.

[5] Hou, Young-Chang, and Zen-Yu Quan. "Progressive visual cryptography with unexpanded shares." Circuits and Systems for Video Technology, IEEE Transactions on 21, no. 11 (2011): 1760-1764.

[6] James, Divya, and Mintu Philip. "A novel anti phishing framework based on visual cryptography." In Power, Signals, Controls and Computation (EPSCICON), 2012 International Conference on, pp. 1-5. IEEE, 2012.

[7] Kang, InKoo, Gonzalo R. Arce, and Heung-Kyu Lee. "Color extended visual cryptography using error diffusion." Image Processing, IEEE Transactions on20, no. 1 (2011): 132-145.

[8] Lai, Lifeng, Siu-Wai Ho, and H. Vincent Poor. "Privacy–Security Trade-Offs in Biometric Security Systems—Part I: Single Use Case." Information Forensics and Security, IEEE Transactions on 6, no. 1 (2011): 122-139.

[9] Lee, Kai-Hui, and Pei-Ling Chiu. "An extended visual cryptography algorithm for general access structures." Information Forensics and Security, IEEE Transactions on 7, no. 1 (2012): 219-229.

[10] Rajanwar, Shubhangi, Shirish Kumbar, and Akshay Jadhav. "Visual Cryptography for Biometric Privacy."

[11] Rathgeb, Christian, and Andreas Uhl. "A survey on biometric cryptosystems and cancelable biometrics." EURASIP Journal on Information Security 2011, no. 1 (2011): 1-25.

[12] Ross, Arun, and Asem Othman. "Visual cryptography for biometric privacy."IEEE transactions on information forensics and security 6, no. 1 (2011): 70-81.

[13] Simoens, Koen, Julien Bringer, Hervé Chabanne, and Stefaan Seys. "A framework for analyzing template security and privacy in biometric authentication systems." Information Forensics and Security, IEEE Transactions on 7, no. 2 (2012): 833-841.

[14] Wang, Ye, Shantanu Rane, Stark C. Draper, and Prakash Ishwar. "A theoretical analysis of authentication, privacy, and reusability across secure biometric systems." Information Forensics and Security, IEEE Transactions on 7, no. 6 (2012): 1825-1840.

[15] Yuan, Jiawei, and Shucheng Yu. "Efficient privacy-preserving biometric identification in cloud computing." In INFOCOM, 2013 Proceedings IEEE, pp. 2652-2660. IEEE, 2013.

[16] Zhou, Xuebing, Arjan Kuijper, Raymond Veldhuis, and Christoph Busch. "Quantifying privacy and security of biometric fuzzy commitment." In Biometrics (IJCB), 2011 International Joint Conference on, pp. 1-8. IEEE, 2011.