FUZZY VAULT: A TEMPLATE PROTECTION TECHNIQUE FOR MULTIMODAL BIOMETRICS

Raseena Arayakandiyil[1], Kiran Kumar K[2], Rithika Pradip[3]

[1]Assistant Professor CSE SNGCET
[2,3]CSE SNGCET

Abstract:

Template preservation is one of the major issues in biometric authentication systems. Stored templates during enrollment are subjected to different types of intrusion attacks. The stored templates can be revoked or reissued by intruders using spoofing techniques. To overcome these issues multimodal biometrics are used to authenticate a user rather using single biometric template. A multimodal biometric system uses two or more biometrics to authenticate a user. Unique and effective biometrics obtained from a single individual are fused together to obtain a single template. Feature transformation or biometric cryptosystems can be used to protect the templates from compromises. So, this work proposes a fuzzy vault technique to preserve the multimodal biometric templates from any sort of compromises or attacks. False acceptance rate(FAR) and Genuine acceptance rate (GAR) can be used to evaluate the system.

Keywords: *Multimodal Biometric Systems , Template, FAR, GAR, And Fuzzy Vault.*

----------***----------

1. INTRODUCTION

Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements ,for authentication purposes.

Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point of sale (POS) applications. In addition to security, the driving force behind biometric verification has been convenience. To prevent identity theft, biometric data is usually encrypted when it's gathered.

To convert the biometric input, a software application is used to identify specific points of data as match points. The match points in the database are processed using an algorithm that translates that information into a numeric value. The database value is compared with the biometric input the end user has entered into the scanner and authentication is either approved or denied.

2. LITERATURE SURVEY

Cancellable biometrics consists of applying transformation functions to the original biometric template[1].The transformed templates are always processed and stored.

Fuzzy vault is a cryptographic primitive to protect the biometric templates. Minutiae based fuzzy vaults implementation is done to prevent the record multiplicity attack[2].

Watermarking based two stage authentication framework is built to address the authentication problem[3]. Face features are embedded into finger print images of the same individual as data credibility token and secondary authentication source.

Biometrics are combined and used for authentication purposes such as fingerprint[4][13], voice[6],hand vein[7] and palm print[15]. Fuzzy logic[12] has been also discussed for the template protection.

Biometric cryptosystems generates a secure key[10]. Error correcting code and the generated key is applied on biometric template to get the helper data. Face images are analysed in this technique and the results shows a decrease in error rate and increase in accuracy.

3. MULTIMODAL BIOMETRICS

In biometry, there are two types of biometric features. They are behavioral biometrics and physiological biometrics. Behavioral biometrics is used for verification purposes. Verification is determining if a person is who they say they are. This method looks at patterns of how certain activities are performed by an individual. Physiological biometrics is the other type used for identification or verification purposes. Identification refers to determining who a person is. This method is commonly used in criminal investigations.

Multimodal biometric systems involves multiple sensors to obtain different biometrics. Biometrics such as face, fingerprint, iris, etc. are obtained using the corresponding

sensors. The sensors will provide a digital image as output. All these images are preprocessed initially. Features are extracted from these preprocessed images. The obtained features are then fused together to form a single template. There are three main fusion techniques available such as feature level fusion, decision level fusion and score level fusion. The fused template is then projected using fuzzy vault technique to create the vault. The vault is then stored in the database.

Methodology

There are two major phases in any biometric system. The first phase is the enrollment phase or training phase. The another phase is called as verification phase or testing phase.

The first time an individual uses a biometric system is called enrollment. During the enrollment as shown in Fig:3.1 , biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment.

In verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.

These phases includes steps such as sensor module, feature extraction, template protector, matcher and decision maker.

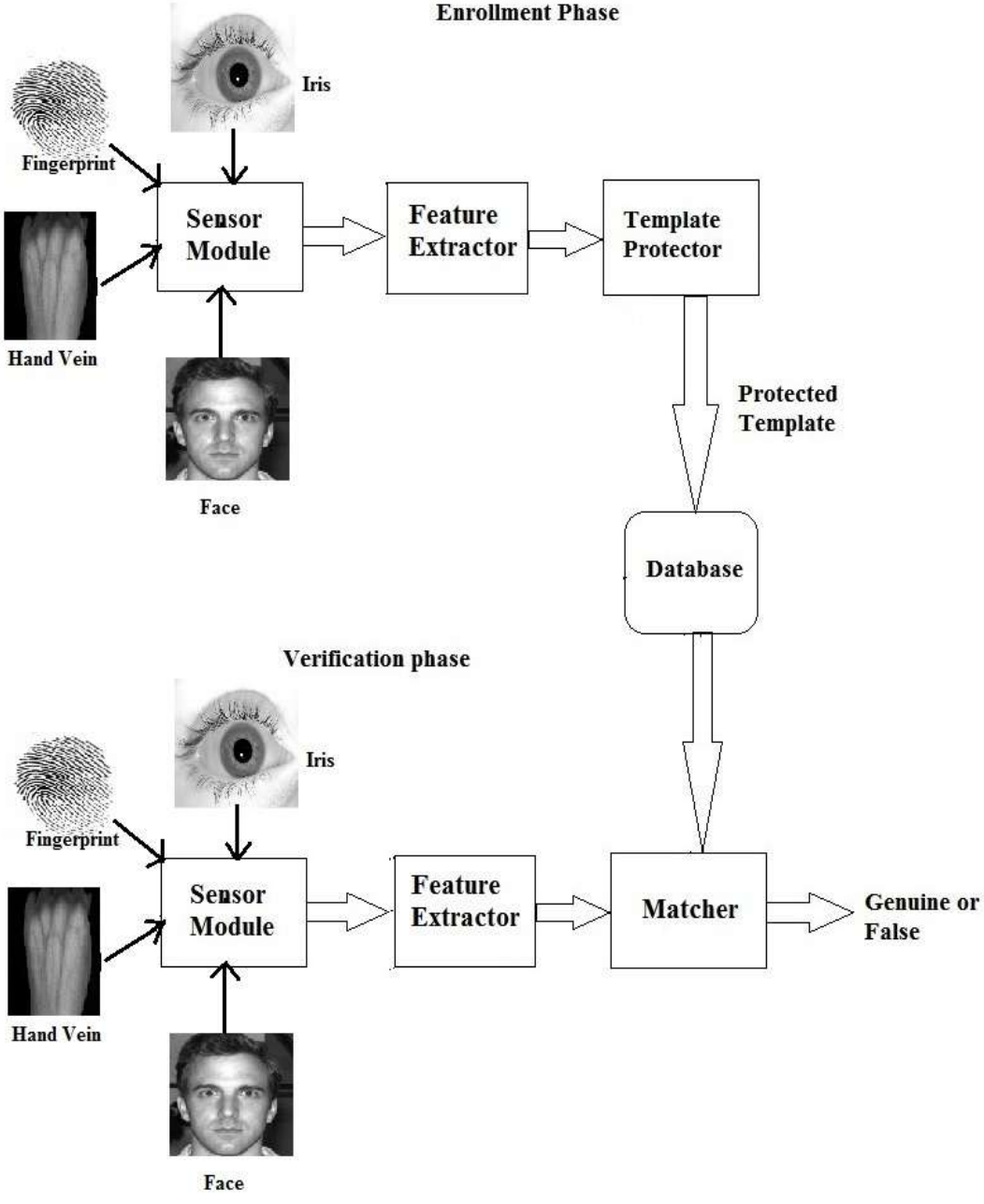

Fig: 3.1 Multimodal biometric authentication system

4. PROPOSED TECHNIQUE

4.1 Preprocessing

The biometrics are first preprocessed to obtain a clear image. The image is first subject to Region of Interest(ROI). A certain region covering from the biometrics are first cropped and taken. The Cropped image is binarized to obtain a black and white image. The binarized image is subjected to thinning process to get the thinned image of it.

4.2 Feature Extraction

Minutiae points has to be extracted from the thinned image of the biometric. Bifurcation and Ridge endings can be obtained from both the fingerprint and hand vein images. Bifurcation is a single ridge that divides into two ridges. Ridge Endings are abrupt end of a ridge. Pupil detection can be obtained from iris. These obtained features are considered to be the feature vectors to be used in the further process.

4.3 Template Protector: Fuzzy Vault

The template is subjected to cryptographic technique called Fuzzy vault. In the fuzzy vault scheme, To encode a secret K in the fused template, the unordered set of extracted features, X from the template are projected on the polynomial ,P. Additionally some chaff point are added to the template and a vault , V is obtained and stored in the database.

uring testing, the query template will again have unordered set of features ,X`. If adequate number of X` can overlap on X , then polynomial P can be recreated back and Secret K can be decoded. If there is no adequate match between X and X`, then authentication will fail resulting the false user.

In the enrollment stage, the extracted features are projected into a polynomial. The polynomial can be of any degree. For more security, we can choose a high degree polynomial which becomes complex for an intruder to interpret. Some additional chaff points are added along with the polynomial to confuse the attackers. The template is then stored in the database.

In the verification phase, similar preprocessing is done and features are extracted. If features get match with the stored template, the polynomial can be reconstructed and the user is verified. It is not necessary that all the features exactly gets matched. Adequate number of matching is enough to verify an user because there might be position differences in placing the hand during sensor module. Thus , this technique has been named as fuzzy vault. Figure 4.1 shows the steps involved in the fuzzy vault technique.

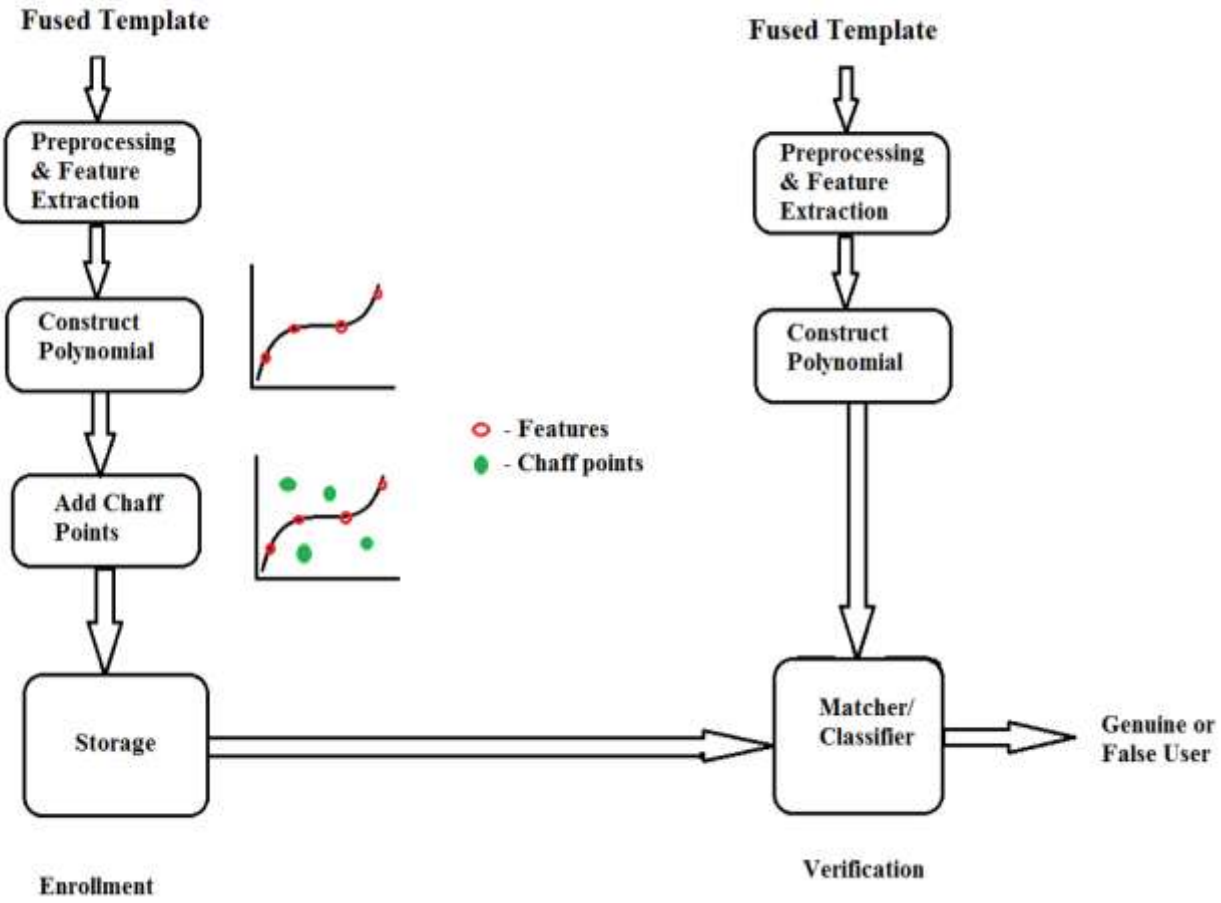

Fig:4.1 Fuzzy Vault technique

5. CONCLUSION

False acceptance rate(FAR) and genuine acceptance rate (GAR) can be used to evaluate the system performance. FAR is defined as a percentage of impostors accepted by the biometric system. In identification biometric system the users are not making claims about their identity. Hence it is necessary that this percentage is as small as possible so that the person not enrolled in the system must not be accepted by the system. Thus False Acceptance must be minimized in comparison to false rejections. GAR is defined as a percentage of genuine users accepted by the system. GAR should be high as maximum. This proposed methodology will provide a high level of security to the stored template because when an biometric vault is lost one's own individuality is lost and it cannot be regained. Thus, fuzzy vault technique protects the template from such compromises.

REFERENCES

[1]. Anne M.P. Canuto , Fernando Pintro, Joao C. Xavier-Junior(2013)," Investigating fusion approaches in multi-biometric cancellable recognition", Elsevier:Journal on Expert Systems with Applications, 40,pp. 1971–1980.

[2]. Benjamin Tams, Preda Mihailescu and Axel Munk(2015),"Security considerations in minutiae-based fuzzy vaults", IEEE Transactions on Information Forensics and Security.

[3]. Bin Ma ,Yunhong Wang, Chunlei Li ,Zhaoxiang Zhang , Di Huang(2014)," Secure multimodal biometric authentication with wavelet quantization based fingerprint Watermarking", Springer – Multimedia Tools Application.

[4]. Cai Li, Jiankun Hu, Josef Pieprzyk, Willy Susilo," A new bio-cryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion", IEEE transactions on Information Forensics and Security.

[5]. Enrique Argones,Emanuele Maiorana, Jose Luis Alba, Patrizio Campisi(2012) ," Biometric template protection using universal background models: an application to online signature", IEEE Transactions on Information Forensics and Security , Vol 7,No 1.

[6]. Hua-Hong Zhu, Qian-Hua Hei, Yan-Xiong Li(2012)," A two -step hybrid approach for voiceprint-biometric Authentication on mobile phones", International Conference on Machine Learning and Cybernetics, Xian, pp.15-17.

[7]. Maleika Heenaye, Mamode Khan(2012)," A multimodal hand vein biometric based on score level fusion",Elsevier: International Symposium on Robotics and Intelligent Sensors.

[8]. Padma Polash Paul, Marina Gavrilova(2014)," Multimodal biometrics using cancelable feature fusion" IEEE:International Conference on Cyberworlds.

[9]. Salman H.Khan , M.AliAkbar , FarrukhShahzad , MudassarFarooq , ZeashanKhan(2015) ," Secure biometric template generation for multi-factor authentication", Elsevier – Journal on Pattern Recognition, 48,pp.458–472.

[10]. Sanaa Ghouzali, Wadood Abdul(2013)," Private chaotic biometric template protection algorithm", IEEE Second International Conference on Image Information Processing (ICIIP-2013).

[11]. Takeda.T, K. Kuramoto, S. Kobashi, Y. Hata(2011)," Fuzzy-logic is precise-its application to biometric system", Elsevier:Journal on Scientia Iranica D 18 (3), pp.655–662.

[12]. Wencheng Yang, Jiankun Hu, and Song Wang(2014) , " A Delaunay quadrangle-based fingerprint authentication system with template protection Using topology code for local registration and security enhancement", IEEE transactions on Information Forensics and Security, Vol. 9, No. 7.

[13].].Karthik Nandakumar and Anil K. Jain(2008), "Multibiometric Template Security Using Fuzzy Vault", BTAS.

[14]. V Evelyn Brindha and AM Natarajan(2012), " Multi-Modal Biometric Template Security: Fingerprint and Palmprint Based Fuzzy Vault", Journal of Biometrics & Biostatistics, Vol.3, pp.3-6.