Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 5,May-2018

PRIVACY PRESERVATION OF MULTI-BIOMETRIC TEMPLATE

Dr. M.Ezhilarasan[1]
Pondicherry Engineering College,
mrezhil@gmail.com

N.Azhagumathi[2]
Pondicherry Engineering College,
azhagumathi1997@gmail.com

R.Sashanghi[3]
Pondicherry Engineering College,
sashanghi@gmail.com

C. Arun Kumar[4]
Pondicherry Engineering College,
arunkumar14IT106@pec.edu

N. Sivadharshan[5]
Pondicherry Engineering College,
sivadarshan14IT212@gmail.com

ABSTRACT

In biometrics, the focus has been moved to multibiometrics from single biometrics due to the demand in increasing operational and security. Multi biometrics are mandatory because of the security demands in the emerging technologies. These biometric data are very sensitive in nature and it can be misused if it is not more secure. In order to overcome these security issues, in our paper we propose a hybrid encryption method for the multi biometric template protection. And we use homomorphic encryption in which only encrypted data is handled to do operations and provides more privacy and protection to the biometric template.

I. INTRODUCTION

Biometrics refers to the metrics of human characteristics and now this is widely used for authentication purpose. These characteristics cannot be forgotten or cannot be lost and so these are more secure way of authentication. But due to the wide spread of cloud computing, there are more privacy concerns about these sensitive biometric data. So we need to protect those biometric data which are saved as a template. But due to those templates protection scheme there should not be any degradation in the performance of the biometric authentication system.

If two or more biometric traits like fingerprint iris face are considered, it is called multi biometrics. This provide more security than single biometric traits since it consider more than one trait, it increases the accuracy of authentication system. So this multi biometric fusion system itself considered as a more secure system. Here fusion means combining the feature vector of the considered biometric traits and thus less vulnerability to spoofing.

We use homomorphic encryption for protecting multi biometric template ensuring the privacy of the sensitive data and developing privacy preserving data services approaches [6], [7]. Homomorphic encryption is converting the sensitive data into cipher text and only this cipher text is handled throughout the process. So even if there is leakage of data, only cipher text is leaked and there is no chance of misusing the sensitive data.

II. RELATED WORK

In [1] the author has discussed about the time efficient, secure and privacy preserving comparison scheme based on homomorphic encryption through combination of fixed- length and sub sampled variable length descriptors.

In [2] author has discussed about multimodal biometrics feature with fusion level encryption. Here he considered two modality where he fused the vectors of fingerprint and iris and provider security by encrypting the template.

In [3] this paper author has given a solution for cryptographic key generation, encryption and for template protection. And also he provided a fingerprint-based multi-biometric cryptosystem

(MBC) using decision level fusion. This method has been done to prove that multi biometrics provides more security than single biometrics.

In [4] this paper the author has discussed about the data security and privacy in real life application of biometric system. He also the proposed approach in investigation with application to online signature recognition.

In [5] this paper the author has shifted the focus from single and multi-biometrics and thus it increased the operational and security demand. It also listed the security section survey and fusion section survey.

III. PROJECT PROPOSAL

To enhance multibiometric template with more privacy preservation technique we implementPallier-ElGamal cryptosystem to protect the biometric template. Therefore, it provides security to the template. These cryptosystemsare probabilistic asymmetric algorithm for publickeycryptography. Homomorphic encryption is a formof encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operation performed on the plain text.

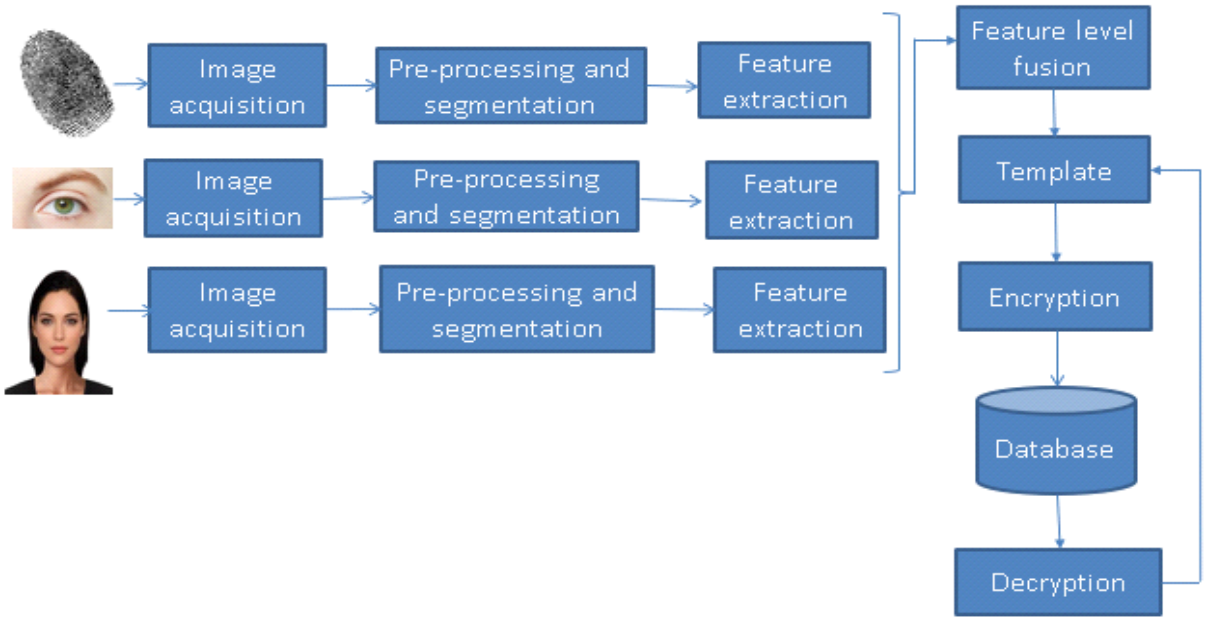

Figure 1: Overall Architecture Diagram

A. FINGERPRINT TEMPLATE FORMATION

IMAGE ACQUISITION:

Image acquisition is the process of acquiring the fingerprint from the sensor. The acquisition of a fingerprint images was accomplished by using either off scan or live scan. Live-scan scanners become presently more frequent, because of its simplicity in usage.

PRE-PROCESSING

The principal aim of enhancement is to improve the clarity of ridge in the recoverable area in the image and to assign the unrecoverable ridges as a noisy area. Recoverable region is considered when ridges and valleys are corrupted by a small amount of dirt, ceases, or other kind of noise. Unrecoverable region are the regions which are impossible to recover them from a very corrupted and noisy image.

The main steps in this stage are enhancement fingerprint image, binarization and thinning. For fingerprint image enhancement, we applied the following step

- Identify ridge segment
- Determine ridge orientations
- Determine ridge frequency
- Apply filters
- Histogram Equalization
- FFT Enhancement

SEGMENTATION:

The primary purpose of segmentation is to avoid extraction of feature in the background that is in reality considered as a noisy area. Segmentation indicates the separation of fingerprint area or foreground from the image background.

FEATURE EXTRACTION:

Features are the pattern or detail of the fingerprint such as ridge direction and pattern type. Fingerprint ridge contains details like pattern, minutia points or pores and ridge contours. These features are extracted from the fingerprint which is given as input and the template is formed.

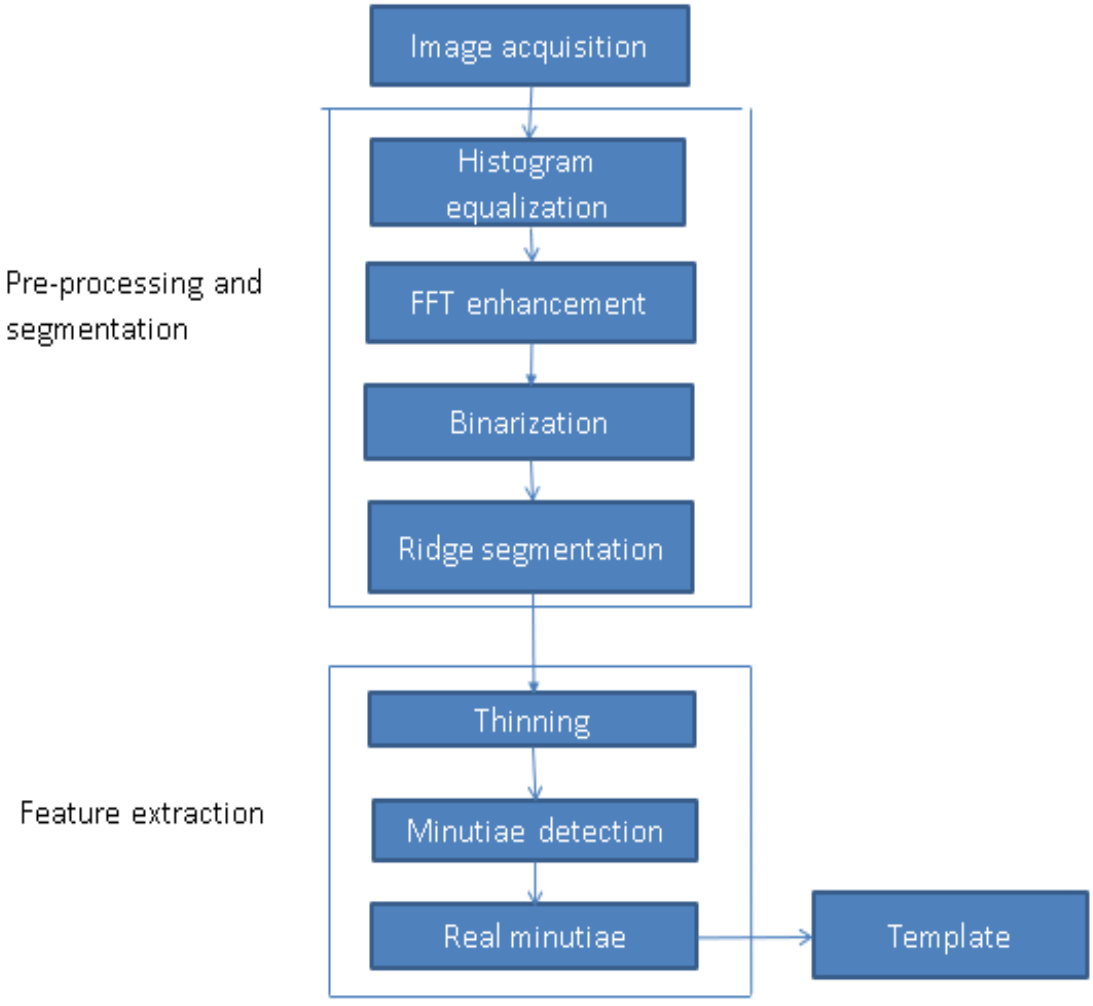

Figure 2: Fingerprint Feature Extraction Block Diagram

B. IRIS TEMPLATE FORMATION

IMAGE ACQUISITION

Image acquisition is the process of acquiring the iris image.

EDGE DETECTION

Canny edge detection is used for edge detection. This algorithm runs in several steps. In smoothing, the image is blurred to remove noise. In finding gradients, the edge is marked when the large magnitude of gradient of image is detected. In non-maximum suppression the local maxima and marked it as edges. Then the threshold is applied to determine potential edge. At last, the edges are determined by suppressing all edges that are not connected to strong edge.

PUPIL DETECTION

In pupil detection method is used to detect the pupil and it can raise the accuracy of iris recognition. The Canny edge detection method is to find the pupil boundaries from the captured image. This gives the effective edges of eye so we can get the exact pupil edge to detect the image.

SEGMENTATION

In segmentation, it is desired to distinguish the iris texture from the rest of the image. An iris is normally segmented by detecting its inner (pupil) and outer (limbus) boundaries is done by active-contour methods.

NORMALIZATION

Once the segmentation module has estimated the iris's boundary, the normalization module uses image registration technique to transform the iris texture from cartesian to polar coordinates. The process, often called iris unwrapping, yields a rectangular entity that is used for subsequent processing.

FEATURE EXTRACTION:

We first detect the pupil its boundary is a closed, continuous and smooth curve, which is near-circular. Once pupil is extracted, iris is located and iris texture is considered as iris feature. We here use a method proposed by daugman.

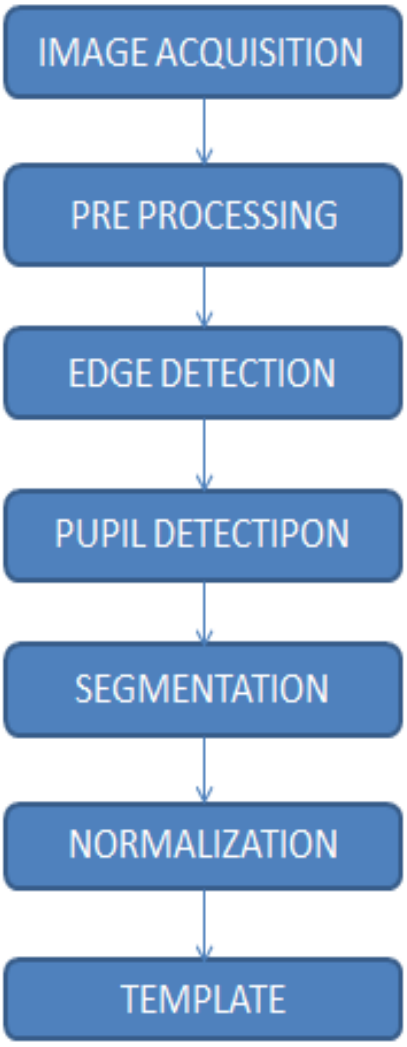

Figure 3: Iris Feature Extraction Block Diagram

C. FACE TEMPLATE FORMATION

IMAGE ACQUISITION:

Face scan technology can acquire faces from static camera or video which generates images of sufficient quality.

SEGMENTATION:

Images are cropped such that the ovoid facial image remains and colour images are converted into grayscale characteristics.

EXTRACT FEATURE

Features utilized are those least likely to change significantly over time like upper ridges of the eye socket, areas around the cheek bone sides of the mouth, nose shape and position of major features relative to each other.

DETECT FACE

It can detect the distance facial features like between the eyes, width of the nose, shape of the cheekbones, length of jawlines.

REMOVAL SPIKES

Spikes are caused mainly by specular regions. In the case of faces, the eyes, nose tip and teeth are three main regions where spikes are likely to occur. The eye lens sometimes forms a real image in front of the face causing a positive spike.

FILTER NOISE

Removal of surface noise is particularly important as a pre-processing step in some methods of extraction of the differential properties of the surface, such as normal and curvatures.

LOCALIZED FIDUCIAL POINTS & CORRECT POSE

A common approach to pose correction uses fiducial points on the 3D face. Three points are necessary to normalize the pose to a canonical form. Often these points are manually identified, however, automatic detection of such points is desirable particularly for online verification and identification processes.

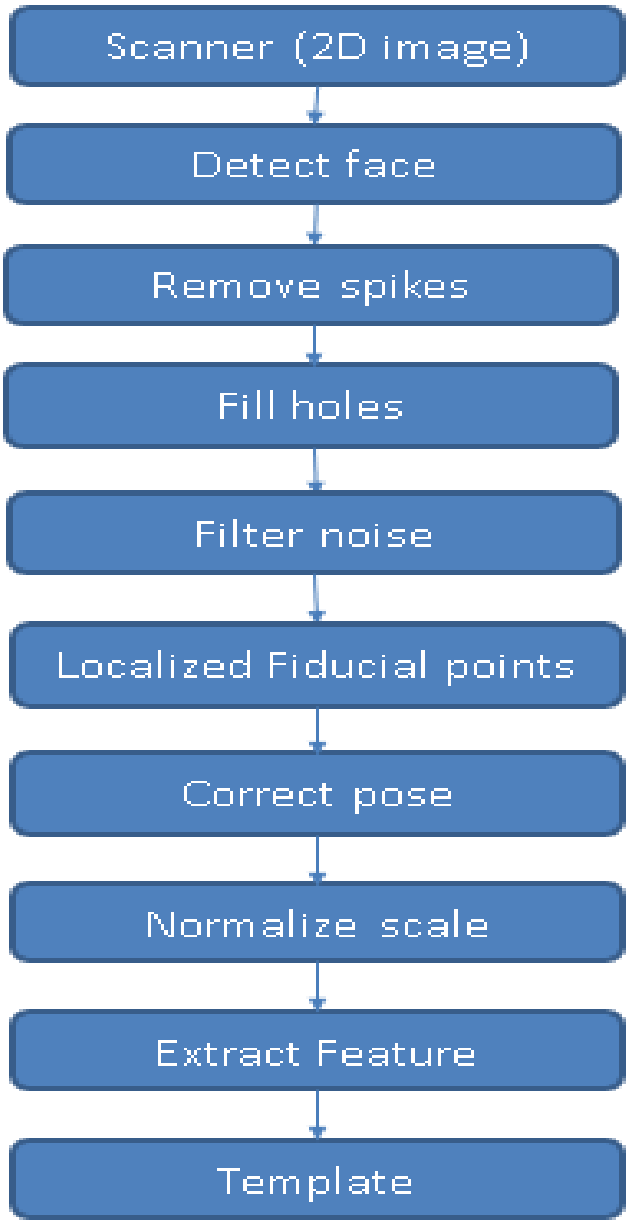

Figure 4: Face Feature Extraction Block Diagram

D. FUSION

The extracted feature vector of all the biometric traits which we use in our project, represent the individual traits. So we fuse these feature vectors to obtain the multibiometric template. This fusion process can be done in four stages and the survey on types of fusion is discussed in [8]. In our project we use feature level fusion.

- **Sensor level fusion** is combining of sensory data or data derived from disparate sources such that the resulting information has less uncertainty than would be possible when these sources were used individually.

- **Feature level fusion:** a single template of higher dimensionality is generated from the individual templates extracted from each characteristic, hence comprising more discriminative information than each single template

- **Score level fusion**: each unimodal system returns an individual similarity score, which are normalized to a common range and combined in order to obtain a more accurate system.

- **Decision level fusion**: each unimodal system returns an individual accept/reject decision, which are fused in order to increase the accuracy of the system.

E. ENCRYPTION

It is a form of encryption that allows computation on cipher texts, generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. The purpose of homomorphic encryption is to allow computation on encrypted data.

There are two types of encryption method Fully homomorphic encryption and partially homomorphic encryption. The encryption scheme is said to be Fully homomorphic if it supports arbitrary computational on ciphertexts. It is said to be partially homomorphic encryption if only certain operations can be performed. In comparison to partially homomorphic encryption scheme are more powerful but slower.

In our project, we use Paillier- ElGamal algorithm which is the combination of Paillier and ElGamal algorithm and these algorithm are homomorphic algorithm. When these two algorithms are fused, it gives more privacy to the biometric template and we can also perform operations on the cipher text itself.

IV. CONCLUSION

In this project, we have implemented the Paillier-ElGamal cryptosystem in multi model biometrics to ensure the template with more privacy preservation technique. The solution is very useful for biometric data security and the template is very secure so that it cannot be misused. And also practical analysis of the irreversibility and unlinkability of the protected templates is done.

V. REFERENCE

1. Marta Gomez-Barrero, Javier Galbally, Aythami Morales, Julian Fierrez.” Privacy-Preserving Comparison of Variable-Length Data with Application to Biometric Template Protection”, IEEE Access, Volume: 5, Year: 2017.

2. RupeshWagh, Saurabh Darokar, ShubhamKhobragade , Assistant Professor Dr. BabasahebAmbedkar College of Engineering and Research Nagpur, India, “Multimodal Biometrics Features with Fusion Level Encryption”, IJESC, Year: 2017.

3.Cai Li, Jiankun Hu, Josef Pieprzyk, Willy Susilo, “A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion”, IEEE Transactions on Information Forensics and Security, Volume:10, Issue: 6, Year: 2015.

4. Enrique ArgonesRua, Emanuele Maiorana, Jose Luis Alba Castro and Patrizio Campisi “Biometric Template Protection Using Universal Background Models: An Application to Online Signature”, IEEE Transactions on Information Forensics and Security, Volume: 7, Issue: 1, Year: 2012.

5. Cai Li; Jiankun Hu; Josef Pieprzyk; Willy Susilo, "A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion", IEEE Transactions on Information Forensics and Security, Volume:10, Issue: 6, Year: 2015.

6. R. Agrawal and R. Srikant, "Privacy-preserving data mining," Proc.ACM Sigmod record, vol. 29, issue: 2, pp. 439–450, Year: 2000.

7. Y. Lindell and B. Pinkas, "Privacy preserving data mining," Journal of Cryptology, vol. 15, issue: 3, pp. 177–206, 2002.

8. Lavinia MihaelaDinca, Gerhard Petrus Hancke, "The Fall of One, the Rise of Many: A Survey on Multi-Biometric Fusion Methods" IEEE Access, Volume: 5, Year: 2017.