Technique to Generate Face and Palm Vein-Based Fuzzy Vault for Multi-Biometric Cryptosystem

N. Lalithamani[1] and Dr. M. Sabrigiriraj[2]
[1]*Assistant Professor(SG), Amrita School of Engineering*
Amrita Vishwa Vidyapeetham, Amritanagar(PO), Ettimadai, Coimbatore – 641 112.
n_lalitha@cb.amrita.edu
[2]*Head of the Department, Department of Computer Science and Engineering*
SVS College of Engineering, Coimbatore – 642 109.
sabari_giriraj@yahoo.com

Abstract. Template security of biometric systems is a vital issue and needs critical focus. The importance lies in the fact that unlike passwords, stolen biometric templates cannot be revoked. Hence, the biometric templates cannot be stored in plain format and needs strong protection against any forgery. In this paper, we present a technique to generate face and palm vein-based fuzzy vault for multi-biometric cryptosystem. Here, initially the input images are pre-processed using various processes to make images fit for further processing. In our proposed method, the features are extracted from the processed face and palm vein images by finding out unique common points. The chaff points are added to the already extracted points to obtain the combined feature vector. The secret key points which are generated based on the user key input (by using proposed method) are added to the combined feature vector to have the fuzzy vault. For decoding, the multi-modal biometric template from palm vein and face image is constructed and is combined with the stored fuzzy vault to generate the final key. Finally, the experimentation is conducted using the palm vein and face database available in the CASIA and JAFFE database. The evaluation metrics employed are FMR (False Match Ratio) and GMR (Genuine Match Ratio). From the metric values obtained for the proposed system, we can infer that the system has performed well.

Key words: multimodal biometric cryptosystems, biometric template security, palm vein feature extraction, face feature extraction, fuzzy vault, secret key.

1. Introduction

Biometric technology offers to identify people through physical measurements of unique human characteristics or behavior. In other words, we all have unique personal attributes that can be used for distinctive identification purposes, including a fingerprint, the pattern of a retina, and voice characteristics. Biometric technology offers the promise of an easy, secure method to make highly accurate verifications of individuals. It guarantees a means of identification that cannot be stolen, lost or forgotten, are being increasingly demanded in security environments and applications like access control and electronic transactions. By replacing Passwords, biometric techniques can potentially

Machine GRAPHICS & VISION 23(1/2):97–114, 2014. DOI: 10.22630/MGV.2014.23.1.6 .

prevent unauthorized access to or fraudulent. However, even the best biometrics to date is still facing numerous problems, some of them inherent to the technology itself. Multibiometrics are a relatively new approach to overcome these problems by having multiple samples of a single biometric trait (called multi sample biometrics) or samples of multiple biometric traits (called multi-source or multimodal biometrics) [5].

The use of biometric data in the context of identity attribute verification poses several non trivial challenges because of the inherent features of the biometric data. In general, two subsequent readings of a given biometrics do not result in exactly the same biometric template. Therefore the matching against the stored template is probabilistic. Storing biometric templates in repositories along with other personally identifiable information introduces security and privacy risks [6]. Those databases can be vulnerable to attacks by insiders or external adversaries and may be searched or used for purposes other than the intended one. If the stored biometric templates of an individual are compromised, there could be severe consequences for the individual because of the lack of revocation mechanisms for biometric templates [26].

In many medical practices, X-ray and ultrasonic scanning are used to form vascular images. This is not acceptable for general purpose biometric applications in the real world. Therefore, obtaining the palm vein pattern images in a fast and non-invasive manner is the key challenge in a vein pattern biometric system [10]. The personal identification using hand and palm vein has gained more and more research attentions these years as it seems a better biometric feature that finger print and other modalities [4,14]. Palm print recognition is getting popular in personal authentication because it provides robust features from a large palm area and the palmprint image can be captured with a cost effective device. In general, a typical palm print acquisition device operates under visible light and can acquire three kinds of features: principle lines (usually the three dominant lines on the palm), wrinkles (weaker and more irregular lines) and ridges (patterns of raised skin similar to fingerprint patterns). A resolution of about 100 dpi (dots per inch) [2,3] can be used to acquire principal lines and wrinkles while a higher resolution, usually 500 dpi, is required to acquire ridge features. However, such a high resolution will increase significantly the computational cost to extract ridge features because of the large image size of palm, and hence prevents the system from being implemented in real time. Therefore, most of the palmprint base systems capture low resolution palmprint images using CCD (charge coupled device) cameras and many algorithms have been proposed for feature extraction and matching [11,12,17,18,20]. Face is another biometric modality is used regularly these days and has been researched to have better results.

The main challenge for embedded versions is to provide a secure storage of the reference template. Embedded devices are vulnerable to eavesdropping and attacks. Thus alternative protection mechanisms need to be investigated. Recently, a novel cryptographic technique called the fuzzy commitment scheme has been proposed for biometric

authentication [1]. The scheme integrates well known error control coding methods and cryptographic techniques to construct a novel type of cryptographic system. Instead of an exact, unique decryption key, a reasonable close witness can be accepted to decrypt the commitment. This characteristic makes it possible for protecting the biometric data using traditional cryptographic techniques [25].
In this paper, we have designed and developed a face and palm vein-based fuzzy vault technique that improves the multimodal biometric template security especially. Initially, the preprocessing steps are applied to both palm-vein and face images for enhancement and smoothing. Then, the features of two biometric images are extracted by finding the common unique points in the images and the extracted features are combined along with chaff points for generating multimodal biometric template. Finally, the multimodal biometric template and the input key are used to generate the fuzzy vault. For decoding, the multimodal biometric template from palm vein and face image will be constructed and it is combined with the stored fuzzy vault to generate the final key. Finally, the experimentation will be conducted using the palm vein and face database available in the CASIA and JAFFE database.

The rest of the paper is organized as follows: A brief review of researches related to the proposed technique is presented in section 2. The proposed biometric storage using fuzzy vault technique is presented in Section 3. The detailed experimental results and discussions are given in Section 4. The conclusions are summed up in Section 5.

2. Brief Review of Related Works

Literature presents lot of works related to biometric recognition and template storage. Here, some of works related to these are reviewed in this section. Abhilasha Bhargav et al. [26] have presented biometrics-based identifiers for digital identity management. They presented algorithms to reliably generate biometric identifiers from a user's biometric image which in turn was used for identity verification possibly in conjunction with cryptographic keys. Their algorithm captured generic biometric features that ensured unique and repeatable biometric identifiers. They also ensured security and privacy of the biometric data. K. Nandakumar [21] has presented a fingerprint cryptosystem based on minutiae phase spectrum. He proposed a minutiae representation known as the Binarized Phase Spectrum (BiPS), which was a fixed-length binary string obtained by quantizing the Fourier phase spectrum of a minutia set. He secured the BiPS representation using a fuzzy commitment scheme employing turbo codes. He also proposed a technique for aligning fingerprints based on the focal point of high curvature regions.

Dr. S. Ravi and Mahima S. [27] have presented several significant strides in facial expression recognition and its applications. At first, the facial expression was measured by virtue of its position. The results for this procedure was far from accurate because static nature and deficient of intensity measurements. The facial EMG has made a radical transformation in the calculation of automatic variation in onset and offset of facial expression. The shortfall owing to static nature has been rectified with the insertion of facial expression recognition by image sequence. The expressive expression where mapping is carried out with ratio images, made it probable to calculate the transformation of one person's expression by calculating expression ratio image to produce more expressive facial expressions of any other person. Ghandi et al. [16] have presented a technique to detect facial emotion by employing a modified Particle Swarm Optimization algorithm, which they named as Guided Particle Swarm Optimization (GPSO). The technique engages tracking the activities of Action Units (AUs) located at suitable points on the face of a subject. Two dimensional rectangular shaped search spaces were defined around each of the action units and particles were then described to contain a constituent in each domain, efficiently building a 10-dimensional search space inside which particles fly in search of a solution. Multiple swarms were employed where each swarm had a target emotion.

Peng Li et al. [23] have presented an alignment-free fingerprint cryptosystem based on fuzzy vault scheme. They introduced an alignment-free fingerprint cryptosystem based on fuzzy vault scheme was developed fusing the local features, known minutia descriptor and minutia local structure, which were invariant to the transformation in fingerprint capturing. The proposed fingerprint cryptosystem avoided the alignment procedure and improved the performance and security of the fuzzy vault scheme at the same time. David Zhang et al. [20] have presented online joint palmprint and palmvein verification method for increasing the anti-spoof capability of the system. Yiding Wang et al [25] have presented hand-dorsa vein recognition based on partition local binary pattern. They introduced hand-dorsa vein recognition method based on Partition Local Binary Pattern (PLBP). The method employed hand-dorsa vein images acquired from a low-cost, near infrared device. After preprocessing, the image was divided into sub-images. LBP uniform pattern features were extracted from all the sub-images, which were combined to form the feature vector for token vein texture features. The method was assessed using a similarity measure obtained by calculating the distance between the feature vectors of the tested sample and the target sample.

Maleika Heenaye et al. [22] have presented feature extraction of dorsal hand vein pattern using a fast modified PCA algorithm based on Cholesky decomposition and Lanczos technique. Principle Component Analysis (PCA) was a successful method which was originally applied on face biometric. They modified PCA using Cholesky decomposition and Lanczos algorithm to extract the dorsal hand vein features. This modified technique decreases the number of computation and hence decreases the processing time. The eigenveins were successfully computed and projected onto the vein space. Zhenhua Guo et al. [19] have presented palmprint based verification method. They proposed a unified distance measure and provided some principles for determining the parameters of the unified distance. They showed that, using the same feature extraction and coding methods, the unified distance measure got lower equal error rates than the original distance measures. Zhenhua Guo et al. [28] have presented empirical study of light source selection for palmprint recognition. They analyzed that most of the current palmprint recognition systems used an active light to acquire images, and the light source was a key component in the system. Although white light was the most widely used light source, little work had been done on investigating whether it was the best illumination for palmprint recognition. They studied the palmprint recognition performance under seven different illuminations, including the white light. A large database showed that white light was not the optimal illumination, while yellow or magenta light could achieve higher palmprint recognition accuracy than the white light.

Xiangqian Wu et al. [24] have presented a biometric system based on hand vein. They presented a hand vein recognition system, which extracted and combined the dorsal, palm and finger vein for personal recognition. In the proposed system, the whole infrared frontal and back images of a hand were initially captured. Secondly, the Region Of Interest (ROI) of dorsal, palm and finger vein images were cropped. Thirdly, the veins in each ROI were extracted and matched by using multi-scale 2-D Gaussian matched filter. Finally, the matched distances were fused to form the final distance for decision by employing SVM classifier.

3. Proposed Technique to Generate Face and Palm Vein-Based Fuzzy Vault for Multi-Biometric Cryptosystem

Template security is an important concern in biometric systems because unlike passwords, stolen biometric templates cannot be revoked. Due to these reasons, biometric templates should not be stored in plaintext form and fool-proof techniques are required to securely store the templates such that both the security of the application and the users' privacy are not compromised by adversary attacks. However, a multi-biometric system requires storage of multiple templates for the same user corresponding to the different biometric sources. Hence, template security is even more critical in multi-biometric systems where it is essential to secure multiple templates of a user.

In our technique, we make use of biometric modalities of face and palm print of a person. The input biometric image is initially pre-processed and feature extracted. Features from both the biometric modalities are then combined to have the combined biometric feature vector, to which the chaff points and secret key points are added to have the fuzzy vault. In the test phase, the test person's face and palm vein biometric images are matched to the fuzzy vault and if matched, secret key is extracted by the technique. The technique is split into four phases: a) Pre-processing, b) Combined feature vector generation, c) Fuzzy vault generation and d) Test case.

3.A. Pre-Processing Phase

The input face and palm vein images are pre-processed before its feature extracted so as to have better results. Pre-processing makes the image fit for further processing of feature extraction and gets rid of the noise and blur in the input image. The pre-processing methods involved in face and palm vein are almost same except in few steps. Palm vein image is initially done by cropping, which is absent in processing of face image. The other difference is that edge detection is used in face image instead of motion filter which is used in palm vein image. The block diagram of the pre-processing phase is given in Figure 1.

Cropping refers to removal of unwanted areas from the input image so as to obtain the image with area of interest. In our case, the inner part of the input palm vein is only required, hence we remove other parts including fingers form the image. Image Scaling is the process of enhancing the smoothness, sharpness and resizing a digital image. The main objective of the scaling is to rescale the input image size to a standard size and as a result of image scaling different size images are resized to a single standard size. Image scaling makes the further processing easier. The resized images are then type converted to double precision format. Double precision is a computer number format that store in

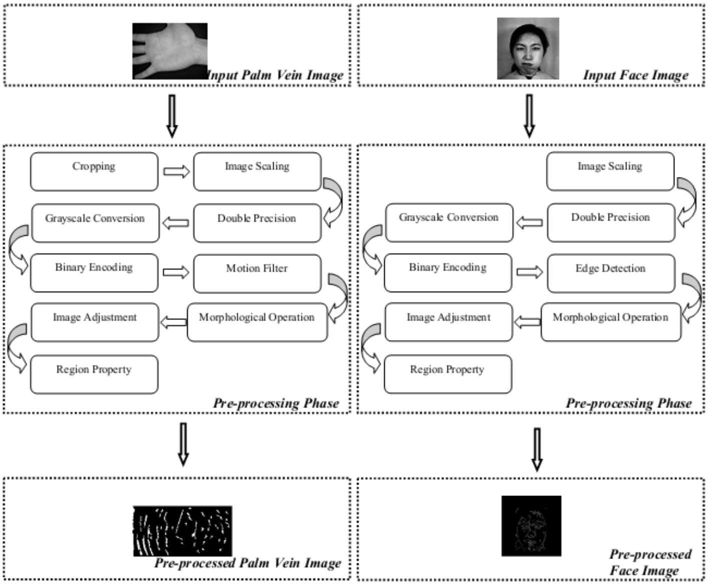

Fig. 1. Block Diagram of the Pre-Processing Phase

two adjacent storage locations. A double-precision number, also called as a double, may be defined to be an integer, fixed point or floating point.

The input images in RGB format are then converted to grey scale images. Greyscale images are composed exclusively of shades of grey, varying from black to white based on intensity value. The grey image is then binary changed where the image is converted to binary format. A binary image has only two possible values for each pixel which is either digits zero or one which are typically represented by the black and white colours. The binary image is motion filtered in case of palm vein image where the linear motions of the images are approximated. Motion filtering is carried with the help of line smoothing process. Smoothing of the image is to build an approximating function that effort to detect vital patterns, while leaving out noise. Here, the image pixels are modified so that the noise pixels are reduced and smoother image is obtained. Here, the smoothed values can be written as a linear transformation of the observed values. In case of face image, the edge detection is carried out to find out the edge points in the input face image. Edge detection for face is vital as features have to be extracted from the face area and not from the outside area. Detection of face edge also results in extraction of points form face edges which is a property of the individual's face as the shape of face varies from person to person.

The image is enriched through image adjustments where various parameters are decided for adjusting the images such as image intensity levels, brightness and colour balance. These parameters improve the quality of the image which in turn yields better feature extraction. Morphological Operation is employed subsequently which is defined by image processing operations that process images based on shapes is a broad set of morphology. The output image is based on a comparison of the corresponding pixel in the input image with its neighbor's and the value of each pixel in a morphological operation. We add pixels to the boundaries of objects in an image and we make use of dilation in morphological process for both palm vein image as well as face image. Set-theoretic processes like union and intersection are employed to describe morphological operations. The two inputs for the morphological operation are binary image and structuring element. Initially the image Im is adjusted for contrast and intensity and is subsequently converted to the binary form Im_b. The enhanced image is obtained through the morphological operation 'imerod' that utilizes the structuring element Sa using the equation:

$$Im_b \Theta Sa = \bigcap_{j \epsilon Sa} A_{-j}$$

The above equation is employed for computing the erode function. The maximum intensity pixels of the image alone are selected by using morphological operation. Hence, adjusted image is additionally improved by exploiting the morphological operation.

The image obtained after the morphological operation will have many unwanted pixels in it, so in order to filter out those we use the region property. The palm veins will not only have required lines but also some other unwanted small lines and pixels. Hence, these unwanted elements are filtered out from the image for better feature extraction using region property. Similarly in the face image, unwanted elements are removed from the image using region property.

3.B. Combined Feature Vector Generation Phase

In this phase, the features points extracted from the face and palm vein images (Figure 2). The extracted features are added with the randomly generated chaff points for the user to generate the combined feature vector. For any person, respective face images and palm vein images are taken as the input and the respective features are extracted from these images. Feature extraction is carried out based on finding out the unique points from the images of the concerned person. Suppose for a person i, let the input palm images be represented by $P_i = \{p_{i1}, p_{i2}, ..., \ p_{iNp}\}$, where Np is the total number of palm vein images available for the person. Similarly, let the input face images of the person i be represented by $F_i = \{f_{i1}, f_{i2}, ..., f_{iNf}\}$, where Nf is the total number of face images available for the person. From all the input palm images of the user, the feature points are extracted which are the common unique points in all the images. That is, if a point ep denoted by co-ordinates (x, y) is common to all images $p_{i1}, p_{i2}, ..., p_{iNp}$, then point

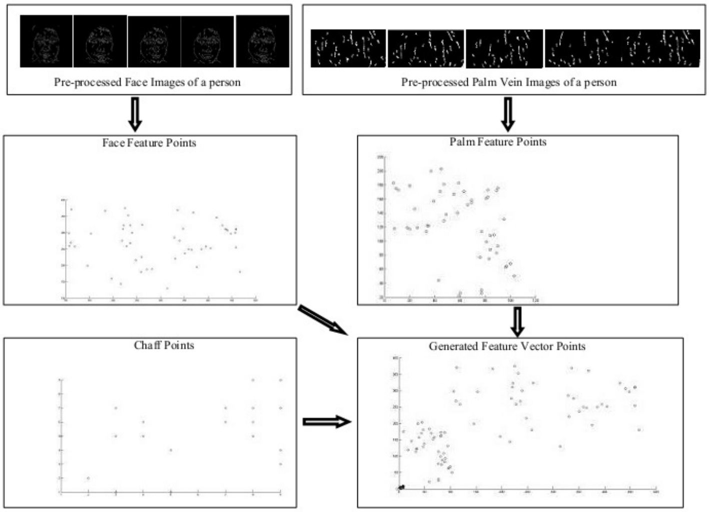
Pre-processed Face Images of a person
Pre-processed Palm Vein Images of a person
Face Feature Points
Palm Feature Points
Chaff Points
Generated Feature Vector Points

Fig. 2. Block Diagram of Combined Feature Vector Generation Phase. Face Feature Points Range Y axis-100 to 400, X axis-100 to 500, Palm Feature points Y axis- 0 to 220, X axis-0 to 120 Chaff Points Range Y axis-1 to 9, X axis-1 to 9, Generated feature points Y axis- 0 to 400, X axis-0 to 500.

$ep\,(x,y)$ is taken as a palm image feature point. Similarly, all other common unique points from the input palm images of the person are found out and let the extracted feature points from be represented as $Ep_i = \{ep_{i1}, ep_{i2}, ..., ep_{iNep}\}$, where Nep is the total number of palm feature points extracted for person i. Similarly, the feature points are extracted from the face images of the person by finding out the common unique points from the input face images of the person. Let the extracted feature points from be represented as $Ef_i = \{ef_{i1}, ef_{i2}, ..., ef_{iNef}\}$, where Nef is the total number of face feature points extracted for person i.

For any person, apart from the face and palm feature points, some additional random points are added known as chaff points. Chaff points are added to improve the security while forming the combined feature vector. Let the chaff points for person i be represented as $Ec_i = \{ec_{i1}, ec_{i2}, ..., ec_{iNec}\}$, where Nec is the total number of chaff points added. Chaff points are randomly added for the person. The combined feature vector is formed by combining the feature points from face, palm and the chaff points. Hence the combined feature vector for a user i can be represented as $E_i = \{Ep_i, Ef_i, Ec_i\}$, which can be expanded to $E_i = \{ep_{i1}, ep_{i2}, ..., ep_{iNep}, ef_{i1}, ef_{i2}, ..., ef_{iNef}, ec_{i1}, ec_{i2}, ..., ec_{iNec}\}$ and the total number of extracted points in the combined feature vector is $Nep+Nef+Nec$. In our technique, though we extract all the common points, we make use of only some points in order to reduce the complexity and time of execution. Here we limit the extracted points from face and palm to 50 and number of chaff points to 20 so as to have total of 120 points in the combined feature vector for a person. Selection of these 50 points from each modality is carried out on based on first come first serve basis. That is first 50 unique common points found out from each of face and palm would form the feature vector. Feature vector also includes 20 chaff points to make a total of 120 points.

3.C. Fuzzy Vault Generation Phase

Fuzzy vault improves the security of template security by the addition of secret key concept into the feature vector. Initially, the input key is encoded to have the respective points which are added to the points of the feature vector to have the fuzzy vault points. The number of secret key points generated is directly dependent on the number of digits in the secret key and if secret key is 4 bit long, then 4 points will be added to the feature vector to form the fuzzy vault. Block diagram of the fuzzy vault generation is given in Figure 3.

Generation of points for the secret key is based on the below mentioned designed mechanism which provides security to the combined face and palm vein templates. The x-coordinates of the secret key points are the digit itself and the y-coordinate is the next odd number in case if the digit is odd and next even number in case of an even digit. Suppose the input key is of size Nk and the key is represented by $K_i = K_{i1}K_{i2}...K_{iNk}$, where K_{ij} is the j^{th} digit of the i^{th} person secret key. Taking a digit K_{ij} in the secret key, corresponding point KL_{ij} is formed by co-ordinates (K_{ij}, L_{ij}), where L_{ij} is the

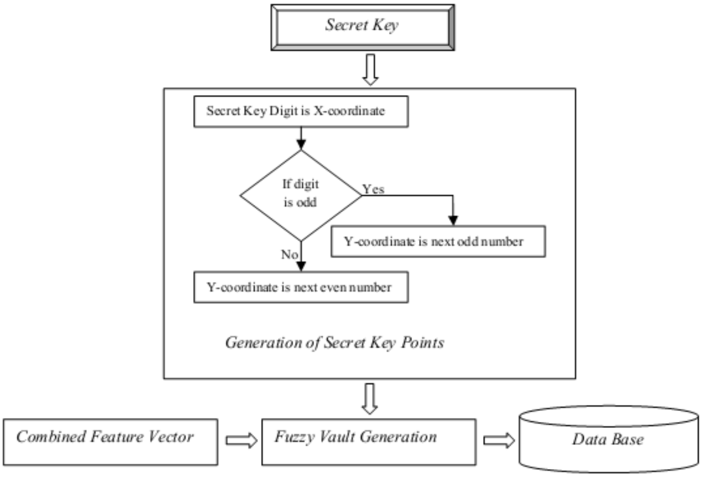
Secret Key
Secret Key Digit is X-coordinate
If digit is odd
Yes
No
Y-coordinate is next odd number
Y-coordinate is next even number
Generation of Secret Key Points
Combined Feature Vector
Fuzzy Vault Generation
Data Base

Fig. 3. Block Diagram of the Fuzzy Vault Generation Phase

next odd number after K_{ij} when K_{ij} is odd and L_{ij} is the next even number after K_{ij} when K_{ij} is even. Similarly all the points for each of the secret key digit are formed in the similar manner so as to result in points $EK_i = \{KL_{i1}, KL_{i2}, ..., KL_{iNK},\} = \{(K_{i1}, L_{i1})\,(K_{i2}, L_{i2})\,...\,(K_{iNk}, L_{iNk})\}$. These points are added to the concatenated vector to form the fuzzy vault which is given by $FV_i = \{E_i, EK_i\}$, which can be expanded to form $FV_i = \{Ep_i, Ef_i, Ec_i, KL_{i1}, KL_{i2}, .., KL_{iNk}\}$. The feature vector can be represented by

$$FV_i = \{ep_{i1}, ep_{i2}, .., ep_{iNep}, ef_{i1}, ef_{i2}, .., ef_{iNef}, ec_{i1}, ec_{i2}, .., ec_{iNec}, KL_{i1}, KL_{i2}, .., KL_{iNk}\}.$$

Hence, the total number of points in the fuzzy vault is $Nep + Nef + Nec + Nk$. In our technique, we employ secret key of size 4 so as to generate total of 124 points in the fuzzy vault. Each of the person will have a corresponding fuzzy vault and all the fuzzy vaults formed $FV_i \; for \; 0 < i < Np$ are stored in the database, where Np is the total number of persons.

3.D. Test Case Phase

In this phase, a test person's face and palm images are given as input which is preprocessed and feature extracted to form the combined feature vector. The input feature vector is compared to the fuzzy vaults in the database and if matched, the secret key is generated to confirm with the person and authentication is provided. Block diagram of test case phase is given in Figure 4.

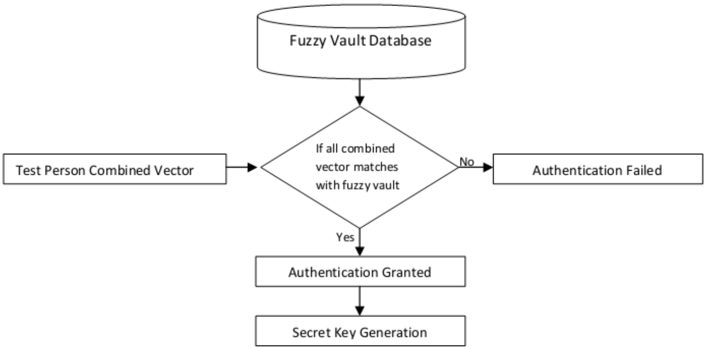

Fig. 4. Block Diagram of the Test Case Phase

Let the input person's feature vector points be represented by $E_t = \{Ep_t, Ef_t, Ec_t\}$, which is compared to fuzzy vault in the database,$FV_i \ for \ 0 < i < Np$. If all the points feature vector of the test person matches into the fuzzy vault, then the person is granted authentication else the authentication is denied. Once all the points in test person feature vector matches with the fuzzy vault form the database, then certain points in the fuzzy vault will be still be left alone. These points are the secret key points and the x-coordinate of these points will give the secret key of the person. Suppose $(K_{i1}, L_{i1})\,(K_{i2}, L_{i2})\,...\,(K_{iNk}, L_{iNk})$, then the secret key is $KL_{i1}, KL_{i2}, ..., KL_{iNk}$. The generation of key for the person is a second confirmation of the person and improves the template security.

4. Results and Discussions

The proposed technique to generate face and palm vein-based fuzzy vault for multi-biometric cryptosystem is evaluated and analyzed in this section. Section 4.1 gives the experimental set up and the evaluation metrics employed. In section 4.2, data set description is given and in section 4.3 it gives the data set preparation. The experimental results are discussed in section 4.4 and performance analysis is made in section 4.5. Comparative performance is given in section 4.6

4.1. Experimental set up and evaluation metrics

The proposed technique is implemented in MATLAB on a system having 6 GB RAM and 2.6 GHz Intel i-7 processor. For determining the accuracy and efficiency of the technique, the error rates are measured and analyzed. NGRA (Number of Genuine Recognition Attempts) gives the number of attained matches. Rejection of face and palm print images F_{ij} may happen due to various reasons and all these rejections are summed up to have REJ_{ENROLL}.

$$GMR\left(t\right) = \frac{gms}{NGRA}$$

Here, gms is the genuine matching score. In addition with, each of the face and palm images $K_{1i}, i = 1, 2, ..., 10$ is matched against with the first set of face and palm print images from database $F_{ik}(i < k \leq 10)$ and the corresponding Impostor Matching Score (ims) is calculated. The number of matches (denoted as NIRA - Number of Impostor Recognition Attempts) is $\left(\left(50X49\right)/2\right) = 1225$ only if,$REJ_{ENROLL} = 0$.

$$FMR\left(t\right) = \frac{ims}{NIRA}$$

Furthermore, the $FMR\left(t\right)$ (False Match Rate) and $GMR\left(t\right)$ (Genuine Match Rate) are calculated from the above distributions for t ranging from 0 to 1.

4.2. Dataset description

Face image The Japanese Female Facial Expression (JAFFE) Database [30] contains 213 images of 7 facial expressions (6 basic facial expressions + 1 neutral, Figure 5, bottom) posed by 10 Japanese female models. Each image has been rated on 6 emotion adjectives by 60 Japanese subjects.

Palm print CASIA Palm-print Image Database [29] contains of 5,502 palmprint images captured from 312 subjects. For each subject, images are obtained for both the left and right palms (Figure 5, top). All the images are 8 bit gray-level JPEG files.

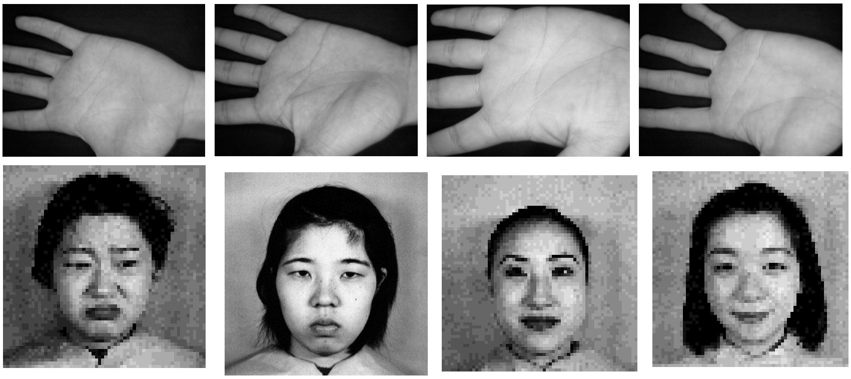

Fig. 5. Images of the face and the palm print taken from the respective databases

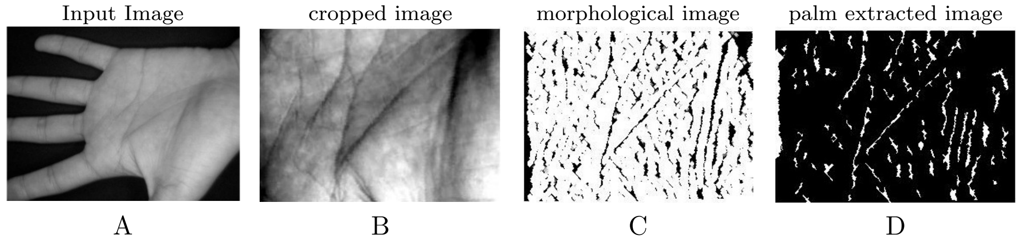

Fig. 6. Palm image outputs at various stages

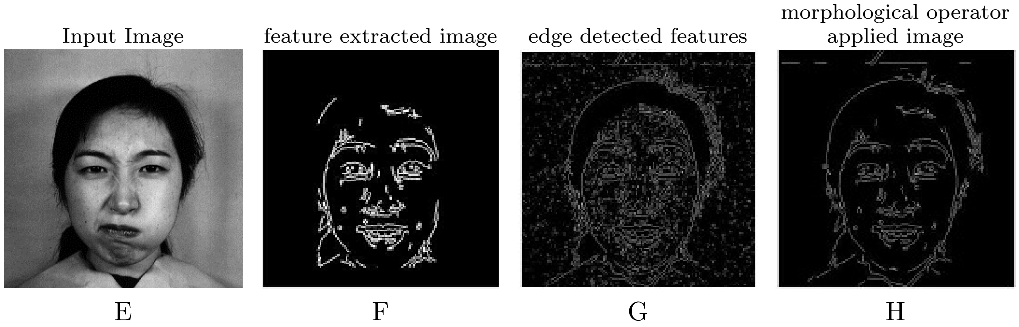

Fig. 7. Face image outputs at various stages

4.3. Dataset preparation

The fact that we are taking the face and palm print from different databases, the face and the palm print will not be of the same person. But as we have to evaluate the proposed technique with both the palm and face image, we approximate the corresponding images from different databases to be of a single person. That is, one image from the hand vein database and another image from the palm print database is combined together to form a single persons biometrics.

4.4. Experimental Results

The section gives the image at different stages of execution. For palm print, the images at six different stages are given. Here Fig. 6 gives the palm images at various stages; A gives the input image which cropped to have B. The morphological image obtained is given by C, and D gives the extracted palm print image. Figure 7 gives the face images at different stages: E gives the input face image, F – the feature extracted image, G shows the edge detected features, and H – the morphological operator applied image.

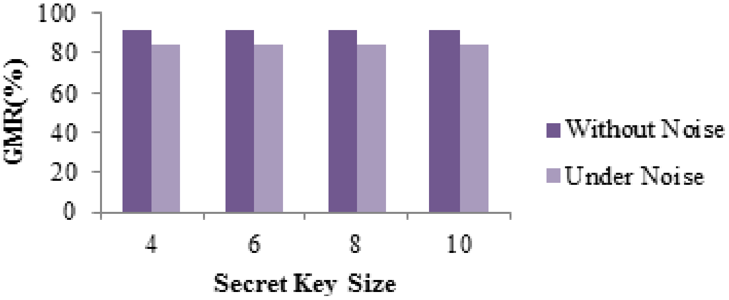

Fig. 8. Plot of GMR values

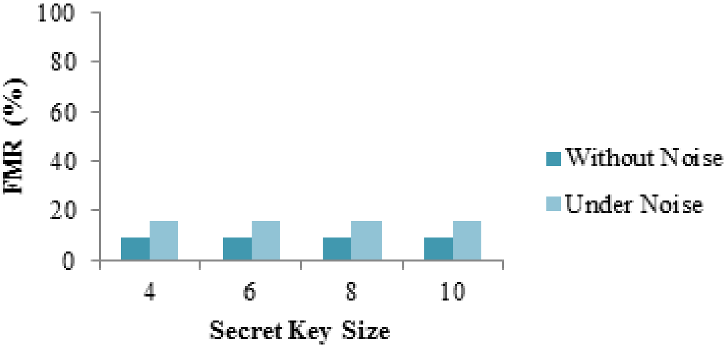

Fig. 9. Plot of FMR values

4.5. Performance analysis

The evaluation metric values of GMR and FMR obtained for the proposed technique is discussed in this section. The study is made in presence and in absence of noise and also by varying the key size of the secret key. Table 1 gives the evaluation metric values obtained without noise and Table 2 gives the values with noise. The noise added is the salt and pepper noise. GMR and FMR values are plotted in Figures 8 and 9, respectively.

Inferences from the Tables 1 and 2, Figures 8 and 9 are as follows.

- Table 1 gives the evaluation metric values of GMR and FMR obtained without noise and Table 2 gives the obtained values with noise.
- Figure 8 gives the GMR plot and Figure 9 gives the FMR values.
- The values are obtained by varying the key word size and values are taken for key word size at 4, 6, 8 and 10.

Tab. 1. Evaluation metrics obtained without noise

		Secret Key Size			
		4	6	8	10
Evaluation	**GMR**	91%	91%	91%	91%
Metrics	**FMR**	09%	09%	09%	09%

Tab. 2. Evaluation metrics obtained under noise

		Secret Key Size			
		4	6	8	10
Evaluation	**GMR**	84%	84%	84%	84%
Metrics	**FMR**	16%	16%	16%	16%

- All cases irrespective of neither the key size nor noise, obtain a high GMR and low FMR which clearly indicates the effectiveness and stability of the proposed technique.

4.6. Comparative Analysis

Various papers related to biometric authentication and recognition uses different biometric modalities, extraction techniques, authentication techniques, evaluation metrics, image quality and image resolutions. Some of the techniques along with modalities and evaluation metric employed and the respective results are given in Table 3. From the table, we can see that our proposed technique has produced good results.

5. Conclusion

This paper presents a technique to generate face and palm vein-based fuzzy vault for multi-biometric cryptosystem. Input images are pre-processed using various processes to yield images fit for further processing. The technique is split into four phases: a) Pre-processing, b) Combined feature vector generation, c) Fuzzy vault generation and d) Test case. The experimentation is conducted using the palm vein and face database available in the CASIA and JAFFE database. The evaluation metrics used is FMR (False Match Ratio) and GMR (Genuine-Match Ratio) and from the values obtained we have inferred that our proposed technique have performed well.

Tab. 3. Comparative analysis for various methods

Paper	**Mechanism**	**Modality**	**Evaluation Metrics**
Fuzzy Vault for Fingerprints [8]	Fuzzy Vault based Authentication	Fingerprint	False Reject Rate (FRR)= 21%
			Genuine Accept Rate (GAR)=79%
Multispectral Palm Image Fusion for Accurate Contact-free Palmprint Recogniton [15]	Curvelet Transform based Recognition	Palm Print	Discriminating Index (d)= 5.9608
			Equal Error Rate (EER)= 0.58%
Fingerprint-Based Fuzzy Vault:Implementation and Performance [13]	Fuzzy Vault based Authentication	Fingerprint	False Accept Rate (FAR)=0.08%
			Genuine Accept Rate (GAR)=85%
A Study of Hand Vein Recognition Method [9]	Feature Point Extraction based Recognition	Hand Vein	Pass Ratio (PR) = 99.1%
			Rejection Rate(RR)=0.9%
Our proposed technique	Fuzzy Vault based Authentication	Face and palm vein	GMR=91%
			False Match Rate(FMR)= 09%

References

1999

[1] A. Juels and M. Wattenberg, A fuzzy commitment scheme, 6th ACM Conference on Computer and Communications Security New York, pp.28-36, 1999.

2003

[2] C. Han, H. Cheng, C. Lin and K. Fan, Personal authentication using palm-print features, Pattern Recognition, 36, pp. 371-381, 2003.

[3] D. Zhang, W. Kong, J. You and M. Wong, Online palmprint identification, IEEE Transactions on Pattern Analysis and Machine Intelligence, 25, pp. 1041-1050, 2003.

2004

[4] C. L. Lin and K. C. Fan, Biometric Verification Using Thermal Images of Palm-Dorsa Vein Patterns, IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 2, pp. 199-213, 2004

[5] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, Biometric cryptosystems: issues and challenges, Proc. of the IEEE, vol. 92, no. 6, pp. 948-960, 2004.

2005

[6] R. Dhamija and J. D. Tygar, The battle against phishing: Dynamic security skins, In Proceedings of the Symposium on Usable Privacy and Security ACM Press, pp. 77-88, 2005.

[7] Shenglin Yang and Ingrid Verbauwhede, Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme, In Proceeding of IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 5, pp. 609-612, 2005.

[8] Umut Uludag, Sharath Pankanti, and Anil K. Jain, Fuzzy Vault for Fingerprints, Lecture Notes in Computer Science, Vol. 3546, pp. 310-319, 2005.

[9] Yuhang Ding, Dayan Zhuang and Kejun Wang, A Study of Hand Vein Recognition Method, In Proceedings of the IEEE International Conference on Mechatronics & Automation, pp. 2106-2110, 2005.

2006

[10] Lingyu Wang and Graham Leedham, Near- and Far- Infrared Imaging for Vein Pattern Biometrics, In Proceeding of IEEE International Conference on Video and Signal Based Surveillance, pp. 52, 2006.

2007

[11] P. H. Hennings-Yeomans, B. V. K. Kumar, and M. Savvides, Palmprint classification using multiple advanced correlation filters and palm-specific segmentation, IEEE Transactions on Information Forensics and Security, 2, pp. 613-622, 2007.

[12]] D. Hu, G. Feng, and Z. Zhou, Two-dimensional locality preserving projections (2DLPP) with its application to palmprint recognition, Pattern Recognition, 40, pp. 339-342, 2007.

[13] Karthik Nandakumar, Anil K. Jain and Sharath Pankanti, Fingerprint-Based Fuzzy Vault: Implementation and Performance, IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, pp. 744-757, 2007.

[14] Yi-Bo Zhang, Qin Li, Jane You and Prabir Bhattacharya, Palm Vein Extraction and Matching for Personal Authentication, Advances in Visual Information Systems, vol. 4781, pp. 154-164, 2007.

2008

[15] Ying Hao, Zhenan Sun, Tieniu Tan and Chao Ren, Multispectral Palm Image Fusion For Accurate Contact-Free Palmprint Recognition, In proceedings of IEEE International Conference on Image Processing, pp. 281-284, 2008.

2009

[16] Bashir Mohammed Ghandi, Ramachandran Nagarajan and Hazry Desa, Classification of Facial Emotions using Guided Particle Swarm Optimization I, International Journal Computer and Communication Technology, Vol. 1, No. 1, pp. 36-46, 2009.

[17] Su, C. (a), Palm extraction and identification, Expert Systems with Applications, 36, pp. 1082-1091, 2009.

[18] Su, C. (b), Palm-print recognition by matrix discriminator, Expert Systems with Applications, 36, pp. 10259-10265, 2009.

2010

[19] Zhenhua Guo, Wangmeng Zuo, Lei Zhang and David Zhang, palmprint verification, Neurocomputing, vol. 73, no. 4-6, pp. 944-950, 2010.

[20] David Zhang, Zhenhua Guo, Guangming Lu, Lei Zhang, Yahui Liu and Wangmeng Zuo, Online joint palmprint and palmvein verification, Expert Systems with Applications, 2010.

[21] K. Nandakumar, A fingerprint cryptosystem based on minutiae phase spectrum, IEEE International Workshop on Information Forensics and Security, pp. 1-6, 2010.

[22] Maleika Heenaye-Mamode Khan, Naushad Mamode Khan and Raja K. Subramanian, Feature Extraction of Dorsal Hand Vein Pattern using a fast modified PCA algorithm based on Cholesky decomposition and Lanczos technique, World Academy of Science, Engineering and Technology, vol. 61, 2010.

[23] Peng Li, Xin Yang, Kai Cao, Xunqiang Tao, Ruifang Wang and Jie Tian, An alignment-free fingerprint cryptosystem based on fuzzyvaultscheme, Journal of Network and Computer Applications, vol. 33, no. 3, pp. 207-220, 2010.

[24] Xiangqian Wu, Enying Gao, Youbao Tang and Kuanquan Wang, A Novel Biometric System Based on Hand Vein, In proceedings of 5th International Conference on Frontier of Computer Science and Technology (FCST), pp. 522-526, 2010.

[25] Yiding Wang, Kefeng Li and Jiali Cui, Hand-dorsa vein recognition based on partition Local Binary Pattern, In Proceeding of IEEE 10th International Conference on Signal Processing, pp. 1671-1674, 2010.

[26] Abhilasha Bhargav, Anna Squicciarini, Elisa Bertino, Xiangwei Kong and Weike Zhang, Biometrics-Based Identifiers for Digital Identity Management, In Proceedings of the 9th Symposium on Identity and Trust, pp. 84-96, 2010.

2011

[27] Christopher Alvino, Christian Kohler, Frederick Barrett, Raquel E. Gurb, Ruben C. Gurb and Ragini Verma, Study of the Changing Trends in Facial Expression Recognition, International Journal of Computer Applications, Vol 21, No. 5, pp. 0975-8887, May 2011.

[28] Zhenhua Guo, David Zhang, Lei Zhang, Wangmeng Zuo and Guangming Lu, Empirical study of light source selection for palmprint recognition, Pattern Recognition Letters, vol. 32, no. 2, pp. 120-126, 2011.

[29] Palm print database. Online: `http://www.idealtest.org`.

[30] Face database. Online: `http://www.kasrl.org/jaffe.html`.