A Survey of Biometric Fusion and Template Security Techniques

C.Prathipa, Dr.L.Latha

Abstract— **Unimodal biometric has many problems like noisy data, intra class variation; inter class similarity, non-universality and spoofing which cause the system to be less accurate and secure. To overcome these problems and increase the level of security, biometric research enrolled multimodal biometrics into the field. Iris and palm print recognitions are considered to be the best recognition system since their false match and non-match rates are very small which implies high accuracy. Password hardening provides additional level of security provided to the template which in turn provides revocability. In this paper, features of iris and palm print are fused by feature level fusion and security is provided by password hardened fuzzy vault.**

***Index Terms*— Fuzzy vault, Iris, Palm print, Password hardened fuzzy vault, Segmentation.**

I. INTRODUCTION

Automatic personal recognition is becoming much essential nowadays. The number of different applications is in use for the same like physical access control, telebanking, teleshopping, etc. Conventional recognition methods have few lacking while biometric recognition systems are more powerful and secure.

The different biometrics is iris, palm print, finger print, ear, hand geometry, face, retina, signature, voice etc. Biometric identification can be classified in to two classes: the first class is called physiological which is interested in shapes of the body like face, palm print, finger print, iris, and vein. The second is behavioural that are related to activities of a person like signature and voice [2]. The multibiometric system has many advantages over the unibiometric systems because they address the issue of non-universality. It becomes difficult for an attacker to spoof the multibiometric traits of an individual.

The iris recognition system is considered as the one of the most important ways for providing security in airports, research laboratories and government organizations. The iris is the annular part between the black pupil and white sclera which is the most part that researches are going on recently. The iris pattern is the most constant part in human body that does not change throughout the human life, with the data-rich substantial structure that can improve the accuracy. The iris recognition system generally includes the following steps 1) iris preprocessing includes segmentation, normalization and image enhancement 2) feature extraction 3) fusion and matching [7].

Palm print has got its role in personal recognition due to its ease of acquisition, high user acceptance and reliability. A palm print contains typical features like standard lines, wrinkles, ridges and valleys on the surface of the palm. Compared to other metrics palm print has several advantages: (1) low-resolution imaging 2) low intrusiveness 3) high user acceptance 4) Stable feature lines. Generally palm print features contain following steps 1) image acquisition 2) preprocessing 3) feature extraction 4) fusion 5) matching [6].

The important part in multimodal biometrics is the combination of two or more modalities is said as Fusion. The fusion can be feature level fusion, score level fusion, pixel level fusion, Decision level fusion. Since features contain richer information of biometric trait, the feature level fusion provides much better accuracy than the decision level and score level fusion [4] [1]. Fuzzy vault is a cryptographic construct proposed by Jules and Sudan. This scheme is more suitable for applications where biometrics and cryptography is applied together. Thus, Fuzzy vault frame work has advantages of both biometrics and cryptography. Fuzzy vault eliminates key management problems as compared to other practical cryptosystems [14]. Password hardened fuzzy vault improved security than the fuzzy vault scheme [19].

II. FUSION

A Preprocessing

Image preprocessing is very important step in the image recognition to do removal of image noise. The brightness in the image may not be uniformly distributed because of non-uniform illumination, so the acquired image has to be preprocessed to extract the ROI (Region of Interest). All the metrics contain their own steps of preprocessing.

Zhongliang [1] preprocessed the iris image which consists of iris segmentation from eyelids and sclera. Normalization of iris is done for extracting a particular block to process it further and image denoising is done to improve the clarity. The next step can be image enhancement which enlightens the image brightness which facilitates the feature extraction.

Aruna and Anu H Nair [2] gave a concept on iris and palm print fusion, which includes preprocessing of both iris and palm print. The Segmentation process takes place where iris is separated from eye lids and sclera. Further, there are two steps in the process of removing the pupil area 1) Adaptive thresholding and 2) Morphological operation. In the palm print preprocessing, the grey-level image is transformed into binary form by Binarization method [6]. Cropping is applied to crop the region necessary in particular using the masking method. Image enhancement is done using the Histogram equalization method.

Manuscript received Oct, 2014.

***C.Prathipa**, Computer Science and Engineering, Anna University/ Kumaraguru College of Technology, Coimbatore, India, / 9500593632.*

***Dr.L.Latha**, Computer Science and Engineering, Anna University/ Kumaraguru College of Technology, Coimbatore, India, 9345439969.*

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

Mohd Sharimie Mohd Ansari [3] proposed a concept that contains preprocessing of finger vein and finger geometry. The first step is image acquisition, which can be done by a capturing device that contains a near-infrared LEDs and camera. The finger separation is carried out on detecting the boundary lines in the finger boundary. The non-uniform brightness of the image is adjusted by Laplacian mask and the overall image contrast is enhanced by the canny edge detection method. Duraiswamy and Jegadeesan [4] had a work on preprocessing of fingerprint and iris. The obtained fingerprint image is subjected to the very common enhancement technique Histogram equalization [2]. The ridge structures are crucial for a finger and palm print, Hence Wiener Filter is applied to advance the clarity of image with the ridge structures unchanged. Then the image segmentation is done to extract the ROI (Region of Interest) which takes a chance for image enhancement again for extracting the complete and readable features in the near future. It is done using the Gaussian Low-pass filter and Gabor filter.

Mahesh and Shanmukaswamy [6] proposed an approach on palm print and speech signals, where they obtained a binary image by converting grey scale image of the fingerprint into binary image using Binarization method [2]. The key positioning points in a fingerprint image is detected by the automatic detection method and rotated to a degree θ and cropped to extract the local Region of interest. Ola M Aly and Hoda M Onsi [7] proposed a work on three metrics iris, palm print and finger knuckle. Here they have separated iris from pupil and sclera using the Daugman's integro-differential operator. Palm print preprocessing is carried out to extract the sole features of palm print like standard lines, wrinkle and crease.

Maleika Heenaye and Mamode Khan [8] had an experiment on multimodal hand vein, they have used the dorsal feature of hand vein and palm vein in their work. The image attainment is carried out with the capturing device CMOS digital camera, an infrared filter and an LED. The preprocessing is done after this for the extraction of region of interest and it is subjected to the image enrichment by Wiener filter [4] and smoothening filter. This in turn leads to the uniform elucidation of the image where feature extraction is simply easier.

B. Feature Extraction

Zhongliang [1] proposed a concept on feature extraction by using Wavelet Based Contour let Transform (WBCT). In their view, the proposed method reproduces the iris image in a better way and improves the recognition rate. Dr.P.Aruna and Anu H Nair [2] proposed a method on feature extraction in palm print using Sobel operator code. Hence Sobel-palm print features are obtained in the result of feature extraction. Mohd Assari and Shahral [3] had their work on finger geometry feature extraction with a new feature Width Centroid Contour-Distance (WCCD). This method combines the breadth of finger and the centroid distance to form feature from finger geometry which improves accuracy better than the existing method.

K. Duraisamy and A.Jegadesan [4] experiment the feature extraction process of finger print and iris, here they initially Binarization is applied to the image and make the features easy to extract. Then morphological operators are used to remove the surplus noises and Ridge Thinning Algorithm is applied to extract the minutiae features. The feature extraction of iris is done using 1D Gabor wavelets of Log-Gabor filter which extracts the iris image and their surface in precise way.

Zhang and Lui [5] proposed feature extraction in the palm print using the six-dimensional Gabor filter. Their magnitude in different orientations detects the features of different dimension. The palm vein features are extracted using the Gaussian filters [4]. Mahesh and Shanmukaswamy [6] proposed their work on extracting the features of speech signal by converting speech waveform into parametric representation which will consists if lower information rate. The palm print image is subjected to 2D Low-pass Gaussian filter [4] and then Haar wavelet decomposition is done in 1D form to extract the features which will be both in horizontal and vertical directions.

Ola M Aly and Hoda [7] projected an idea with iris, palm print and finger knuckle. Here the feature of iris and palm print biometric is extracted by using the Log-Gabor filter [4]. The significant features of finger knuckle are extracted using the Linear Discriminant Analysis (LDA) and thereby the dimensionality of the image is also reduced. Heenaye and Khan [8] had their work in feature extraction from hand vein and palm vein. The dorsal features are extracted in both the metrics by representing the images in the Independent Component Analysis (ICA).

.

C. Fusion

Fusion at this level can be applied by extracting the features from diverse modalities or same modality. Feature extraction level means the combination of different feature vectors that are obtained from numerous sensors of same biometric trait or multimodal traits. When the feature vectors are identical, A single feature vector can be designed with "and","or","xor", or other operations. When the feature vectors are non-identical we can concatenate them in to sole vector.

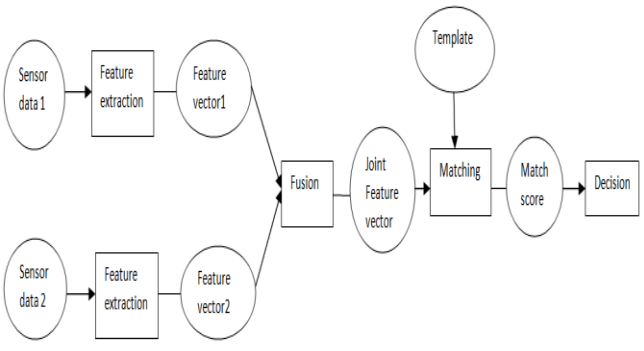

Fig 1 Feature Level Fusion

Dr.P.Aruna and Anu Nair [2] proposed their work with four different fusion methods for the iris and palm print biometrics. The four fusion methods experimented here. Principle Component Analysis (PCA) is a vector space transforms used to diminish the multidimensional data sets into lowers dimensional for a study. The Discrete Wavelet

 All Rights Reserved © 2014 IJARCET

Transform (DWT) is wavelets- based and a multi-scale advance used to handle the image resolutions. The IHS is one of the frequently used fusion system that is used for sharpening of the image. Laplacian Pyramid consists of breakdown of images where at each set a low level pyramid is constructed. After fusion, the quality of fusion is calculated with some measures like PSNR (Peak Signal Noise Ratio), MSR (Mean Square Error) etc. The trial results expose that DWT is the superior fusion method compared to other methods.

Mohd Assari and Affendi Rosdi [3] anticipated fusion of finger vein and finger geometry based on the score level fusion. The templates are matched and score of different metrics are calculated and score normalization [5] is done to make the scores in a common range. Then the normalized scores are fused by the Weighted SUM rule and then stored in the database. Dr. K. Duraiswamy and A. Jegadesan [4] had their work on fusion of fingerprint and iris, where they have three different steps which follow the fusion 1) Shuffling of individual feature vectors 2) Concatenation of shuffled feature vector 3) Merging of concatenated feature vectors. This method of fusion decreases the vulnerability of the templates.

Zhang and Lui [5] planned a notion on fusion of palm print and palm vein based on their score levels. Here the test sum and weighted sum of the palm print and palm vein are intended and fusing those scores with the average level combination. The quality of the combined image depends on the weights assigned to each metric during computation. Mahesh and Shanmukaswamy [6] proposed fusion of speech signal and palm print by calculating the scores of each metric with the mean of absolute difference between the two feature vectors. Then the scores are merged by weighted sum technique [3].

Ola M Aly and Hoda Onsi [7] proposed the fusion of iris, palm print and finger knuckle by the calculating the scores and normalizing them using Min-max normalization. Here they have tried three different score level combinations for the under taken metrics, product rule, average rule [5], weighted sum rule [3]. For different combination of metrics different fusion rules produce good results. Hence it is our best part to analyze the results and decide on best fusion rule. Heenaye and Khan [8] proposed their work on fusion of multimodal hand vein based on fusion of score. The obtained scores are normalized using Min-max normalization [7]. Here they have used sum-rule based fusion [3] [6] which gives good result for the under taken metrics by reducing the FAR (False Acceptance Rate) and increasing the FRR (False Rejection Rate).

III. Security Techniques

Basic security provision for the protection of biometric template has become much important nowadays. The biometric template stored in the database requires to be protected to avoid it from fake authentication, avoid spoofing, cross matching across the databases, etc. Hence the reliability and privacy of biometric templates can be enlarged. Biometric template security system can be classified to 1) Feature transformation approach 2) Biometric cryptosystems. In the feature transform approach, Transformation function is used whose parameters are typically derived from the random key. The feature transform can be further classified in to 1) salting 2) non-invertible transform. Some of the encryption techniques had been projected for the guard of stored template based on the above mentioned classification like fuzzy commitment, fuzzy vault, and password hardened fuzzy vault, etc.

A. Fuzzy Vault

The well prominent example of biometric cryptosystems is the Fuzzy vault framework which is a biometric template protection technique where the biometric features are represented as an unordered set. The concept of fuzzy vault framework can be explained further as, Let P denotes the biometric template with k elements. The user must select a key U and it encodes it in the form of polynomial Q of degree r and evaluates the polynomial Q on all elements in P. Now the genuine points on P are concealed by including the chaff points (random points). The genuine points and chaff points together comprise a vault V or also called as helper data. Hence the user's biometric data is secured with the configuration of vault.

During the authentication, the user must provide their biometric query template denoted by P'. If the P' overlaps sufficiently with P then the user can spot many points in V that lie on the polynomial. If the difference between the P and P' is more than the particular predestined threshold value then the Reed-Solomon decoding can be applied to reconstruct the polynomial. If the polynomial is successfully restructured and the secret key is able to be reproduced from the polynomial then the authentication will be successful. If the P and P' does not overlap considerably and reconstruct the polynomial properly, then the authentication will not be successful. The fuzzy vault support can be done many mixture of multimodal biometrics.

Abhisekh Nagar, Karthik Nagar and Anil A.K Jain [9] have proposed an approach on improving the recognition rate and securing the biometric template based on the method called Finger print Fuzzy vault. The minutiae descriptors are used to extract the ridge orientations and frequency information. The method consists of two main steps 1) Fuzzy vault encoding, where the securing of minutiae location and path using the fuzzy vault takes place 2) Securing ordinate values, where the ordinate values of the vault are secured using the minutiae descriptors using the fuzzy commitment approach. The experimental approach reveals that usage of minutiae descriptors increases the identification progress and security accordingly. The False acceptance rate decreases to the acceptable level without change in the genuine acceptance rate.

Y.J.Chin, T.S.Ong, A.B.J Teoh, K.O.M Goh [10] proposed a Hybrid template defense procedure with finger print and palm print. Feature extraction is done in two steps 1) Non-overlapping blocks based fusion. 2) Random tiling. The Gabor filter [7] [5] is used in the feature mining to some degree. The feature level fusion is done based on the wavelet decomposition and matching is based on hamming distance. The proposed template protection technique is equal-probable 2^n discretization which produces zero EER with the under taken metrics when compared to other protection technique like Biophasor and Random tailing. This method shows better performance in the experiment with the

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

multimodal biometrics than in the use of Unimodal biometrics.

Peng Li, Xin Yang, Jie Tian [11] proposed an approach on alignment free cryptosystem by extracting the local features like minutiae descriptors and minutiae local structure since these two are the only features that are invariant to the rotation and translation. The fusion strategy uses three rules as separated rule, product rule and sum rule. The similarity of local features between stored template and query template is calculated for knowing similarity measure. The Alignment-free cryptosystem is planned since the alignment of stored and query biometric in the encrypted domain is a tough task. It consists of Alignment-free vault encoding is done for both features with chaff generation [13] technique and polynomial encoding to create helper data. Then the Alignment-free vault decoding is done further. The sum rule performs best than the others and the proposed method works well for the smaller database than the larger database.

Abhisekh Nagar, Karthik Nandhakumar [12] proposed a method on multibiometric cryptosystem using the three popular biometrics finger print, face and iris. Here the various templates of an user are secluded using distinct secure sketch, for that two well known biometric cryptosystems Fuzzy Vault[1][3] and Fuzzy Commitment scheme are used. An embedding algorithm is proposed and implemented for all the three metrics and fusion is done. The fuzzy vault encoding and decoding [1][3] and fuzzy commitment is done for all the three metrics in Real multimodal database and virtual multimodal database. It is observed that the different fusion method using different metrics with the implementation of cryptosystems produces varied positive results.

George S Eskander and Eric [13] Granger proposed an approach for securing the offline signature images with the bio-cryptographic systems. Although Fuzzy vault [1][3][4] has proved success in the physiological biometrics like face, finger print and iris[1][4], it has not been experimented with the behavioral biometric trait like signature. Fuzzy vault encoding and decoding is done with the offline signature images. The feature extraction is based on Extended-Shadow-Code (ESC) and Directional Probability Density Function (DPDF), while ESC detects the spatial information and DPDF detects the directional information in the signature images. A Boosting Feature Selection (BFS) technique is described in two steps that are used for Feature selection. The anticipated procedure is also counting the user-based feature selection and population based feature selection. Matching is calculated based on the similarity score computation between the extracted features. The tentative results confirm that the proposed method decreases the FAR (False Acceptance Rate) and increases the FRR (False Rejection Rate)

Fang Enbo, Han Caiyun [14] had proposed an approach on Auto-aligned fuzzy vault since the mechanical alignment of templates is difficult. Auto-aligned sharing fuzzy finger print vault which is based on the Geometric Hashing is to deal with the automatic configuration in the multiple-control fuzzy vault with a compartmented organization. The geometric hashing is a technique to compete the geometric features against the database, it does preprocessing at enrollment phase and acknowledgment at the verification phase. With hash table set up at the time of verification the geometric hashing makes a quicker authentication in less time. Multiple-control fuzzy vault (MCFV) is a conservatory of single-control fuzzy vault (SCFV), the MCFV which allows numerous user can have admittance to a single secret. The proposed multi-control fuzzy vault contains threshold, compartmented multi-level contact structures. Auto-aligned sharing fuzzy vault is based on the multiple-control fuzzy vault with the compartmented structure. But on comparing the original MCFV with Auto-aligned fuzzy vault, the later method produces very high accuracy and verification because of the incorporation of geometric hashing. Finally, an auto-alignment of finger features is achieved in the domain of a multiple-control fingerprint fuzzy vault with the compartmented structure.

Mohamed Khalil-Hani, Muhammad N. Marsono [15] have proposed an approach on the generation of chaff points for the security of fuzzy vault[1][3][4]. The security of fuzzy vault depends on the degree of polynomial and amount of chaff points added. Chaff points generation is needed during the fuzzy vault encoding and they must be removed from the vault exactly during the fuzzy decoding. Clancy proposed a chaff generation algorithm which is more compute-intensive and so has higher complexity. A new fast chaff generation algorithm had been proposed which overcomes the disadvantage of existing Clancy algorithm. In the proposed algorithm, Boundary points are created around each genuine point at a predefined distance. The Boundary matrix is created to store the boundary points. When new points enroll in to the vault, new boundary points are created and stored in the boundary matrix. The proposed method on analysis shows that it can provide better security to the vault Also it is proved to be much less compute intensives, since the algorithm contains operations like addition, subtraction and multiplication. The complexity of the present system is O (n^3) while the complexity of the future system is O (n^2).Hence the fast chaff generation algorithm is considered to be providing better security to the vault.

Tohari Ahmed and Song Wong [16] proposed a work on cancellable finger print template, which is a biometric template protection technique, which does not need registration. The cancellable template stores only the altered feature as an alternative of the original feature. The renovation can be done either in the signal field or feature field. But the feature field renovation is more secured. The proposed method uses the pair-polar coordinate based pattern design method. The work consists of steps as minutiae point generation from the finger print. Template generation is carried out with the proposed design method and the random vector is generated using the sector-mapping. Sector-mapping is many-to-one, so that it is feasible to find the random vectors in the original sector. Matching is done with the criteria that, features match if they satisfy the specified conditions. Only the changed features are stored in the template and hence the proposed method prevents the want for finger print registration, which is a demanding issue in template security.

V Evelyn Brindha [17] proposed an approach on creation of fuzzy vault with the features of palm print and finger print. The samples of finger print and palm print is preprocessed and features are extracted using the Gabor filter [7] [5]. The features are fused using the feature-level fusion. Then the Fuzzy vault [9] encoding with the two samples is carried out during the enrollment. Then during the authentication stage, the fuzzy vault decoding is carried out. As the result FMR decreases to 12% and FNMR increases to 88%.Hence the proposed method yields a good result.

 All Rights Reserved © 2014 IJARCET

Devesh Harahan and Om Prakash [18] proposed a new approach fuzzy cryptosystem with palm print. Generally, the secret key in the asymmetric cryptographic area is confined with the help of fuzzy vault formed by randomizing the palm print with the secret key. Here in the proposed method uses polynomial construction on the secret key by using two functions, matching function, injective function. Most randomized palm features are obtained using the PCA (Principle Component Analysis) and the polynomial construction is carried out. The PCA mapping is also done further and the random chaff points [13] are generated and added to the vault, hence the vault is encoded. The experimental results reveal the proposed method works well for the palm print than the finger print. The security of the fuzzy vault depends on the quantity of the polynomial, higher the degree higher the security.

B. Password Hardened Fuzzy Vault

Password hardened fuzzy vault is introduced to conquer some of the boundaries of fuzzy vault. Some of the restrictions of fuzzy vault are, if the vault is compromised then the same biometric data cannot be used to assemble a new vault with diverse keys, polynomial and random chaff points. Fuzzy vault is prone to cross-matching of templates with various databases and hence it cannot be easily revoked. As the biometric features are of non-uniform character, it becomes easy for an attacker to utilize them and extend attacks based on study of points in the vault. As the chaff points are more than the genuine points, it is probable for an attacker to alternate few points with the help of his own biometric feature. Therefore both the valid user and the attacker are validated by the vault using the same biometric character. This results in the increased FAR (False Acceptance Rate)

To beat some of these limitations Password is added as the supplementary layer of security to the vault and increasing the user-privacy. Password hardening provides security and revocability to the biometric templates. It is very difficult for an attacker to cooperate both the vault and the combined password at the same time. A password is derived from the user biometric and a password of user's own interest is created. The user generated password and soft biometric password are combined to form the transformation password. Password is divided into blocks and permuted with the biometric features. Hence the security is added to the vault.

Farid Benhammadi, Kadda Beghdad Bey [19] planned an approach on password hardened fuzzy vault for finger print. In the proposed method, the feature called Minutiae-pair wise is extracted based on the minutiae pair wise extraction algorithm. The extracted features are distorted into Plate-model-fingerprint. Minutiae pair wise matching is done with the use of Breadth First Search (BFS) and Bipartite graph. The maximum resemblance is calculated with the Cardinality measure. Then the password hardened fuzzy vault scheme is implemented. The extracted feature is divided into quadrant and the password of user- interest is permuted with the password and biometric feature. Hence new transformed feature is obtained. They are further divided into quadrants and Angular and Radial transformation is carried out. The obtained new feature is encoded into the vault with the addition of chaff points. Further for the fuzzy decoding, password and the user biometric is required. Only then the user will be authenticated with the maximum template match score. Thus the password hardening provides revocability and prevents cross-matching.

V.S. Meenakshi and G.Padmavathi [20] proposed a concept regarding Password hardened fuzzy vault with iris, retina and finger print. The security of the password hardened scheme is measured with the min-entropy. Extraction of feature points from finger print, iris and retina are carried out. The canny edge detection is used to subtract the iris and Hough transformation is then used first to iris/sclera boundary and then to the iris/pupil boundary. Histogram equalization is used to boost the image contrast. Thinning and joining morphological operations are performed on the retinal image and also these operations are done to enhance the contrast of vascular patterns. Then the password hardened fuzzy vault is implemented by the transformation of biometric features with the user defined password. Three different passwords are used for three different metrics and transformed in to new features. Then fuzzy vault encoding and decoding are carried out. The security of the password hardened fuzzy vault is measured with the min-entropy. Also the security of the scheme depends on the number of chaff points [13] are added and also if the degree of polynomial is higher, higher the security.

IV. CONCLUSION

The iris and palm print biometric are unique and stable for every individual than other biometric like fingerprint, voice etc. The feature level fusion is preferred since the exact matching can be done. Provision of security to the template is much essential nowadays. Fuzzy vault is good encryption techniques that can provide security to the stored template for a good extent since it can efficient overcomes the key management problem. Password hardened fuzzy vault provides a supplementary layer of protection provided to the encrypted template.

REFERENCES

[1] Kyle O.Baliey, James O Okolika, Gilbert L Peterson, "User identification and authentication using multi-modal behavioral biometrics", *Computer society, 2014*.

[2] Anu H nair and Dr.P.Aruna, "image fusion technique for iris and palm print biometric system", *Journal of theoretical and applied information technology.vol.no.3, 2014.*

[3] Mohd sharimie, Mohd Assari, Shahral A suandi, Bhaktiar Affendi Rosdi, "Fusion of band limited phase only correlation and width centroid counter distance for finger based Biometric", *Expert system with application, 2014.*

[4] Dr .K.Durai swami and A. Jegadesan, "Feature level fusion of fingerprint and iris", *International journal of computer science and information security, 2010*.

[5] David Zhang, Yahui Liu, Lei Zhang, "Online Joint Palm print And Palm vein verification", *Expert system with Applications, Science Direct, 2010*.

[6] P.K. Mahesh and M.N. Shanmukaswamy,"Fusing speech signal and palm print feature for a secured authentication system", *ITACT journal on image and video processing, 2011*.

[7] Ola M. Aly, Hoda M. Onsi, Gouda I. Salama, Tarek A. Mahmoud, "Multimodal Biometric System Using Iris, Palm

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

Print and Finger-Knuckle", *International Journal of computer Applications, 2012.*

[8] Maleika Heeneya and Mamode Khan, "A multimodal hand vein biometric based on score level fusion", *International Symposium on robotics and intelligent sensors, 2012.*

[9] Abhisekh Nagar, Karthik Nandha Kumar, Anil A. K Jain, "A hybrid biometric cryptosystem for securing finger print minutiae template", *Pattern recognition Letters, 2010.*

[10] Y.J. Chin, T.S. Ong, A.B.J.Teoh, K.O.M.Goh, "Integrated Biometrics Template Protection Technique based on finger print and palm print Feature level fusion", *Information Fusion, 2013*.

[11] Peng Li, Xin Yang, Jie Tian, Kai Cao, "An Alignment-Free finger print cryptosystem based on fuzzy vault scheme", *Journal of network and computer applications, 2010.*

[12] Abhisekh Nagar, Karthik Nandha Kumar, Anil A.K. Jain, "Multibiometric cryptosystem based on feature-level fusion", *IEEE Transaction on information Forensics and Security, 2012.*

[13] George S. Eskander, Robert Soberin, Eric Granger, "A bio-cryptographic system based on offline signature images", *Information sciences, 2014.*

[14] Fang Enbo, Han Caiyun, "Auto-aligned sharing fuzzy finger print vault", *School of electronics and information engineering, 2012.*

[15] Mohamed Khali-Hani, Muhammad N. Marsono, Rabia Bakhteri, "Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm", *Feature generation computer . Systems, 2013.*

[16] Tohari Ahmed and Song Wang," Pair-polar Coordinate based cancelable finger print template*", Pattern recognition, Science direct, 2011.*

[17] V Evelyn Brindha, A.M Natarajan, "Fingerprint and palm print based fuzzy vault", *journal of biometrics and biostatistics, 2012*.

[18] Om Prakash Verma and Devesh Harahan, " A New Palm print Based Fuzzy Vault system for securing cryptographic key", *International Journal of Information and Electronics Engineering, 2012.*

[19] Farid Benhammadi, Kadda Beghdad Bey, "Password hardened fuzzy vault for finger print authentication system*", Image and vision computing, 2014.*

[20] V S. Meenakshi and G.Padmavathi, "Security analysis of Password Hardened multimodal biometric fuzzy vault with combined feature point extracted from finger print, iris and retina for high security applications", *science direct, 2010.*

C.Prathipa pursuing her Master of Engineering at Kumaraguru College of Technology, Coimbatore, India. She Completed her Bachelor in Engineering at KGISL Institute of Technology, Coimbatore. Her research interest is in the field of Biometrics and Networks.

Dr.L.Latha Associate Professor at Kumaraguru College of Technology, Coimbatore, India. She has an experience over 18 years in the field of Teaching. Her research interests are towards the area of Biometrics, Image Processing and Information Security.

 All Rights Reserved © 2014 IJARCET