CANCELLABLE MULTIMODAL BIOMETRIC USER AUTHENTICATION SYSTEM WITH FUZZY VAULT

S.R.Soruba Sree
Research Scholar, Dept. of Computer Science
PSGR Krishnammal College for Women
Coimbatore
sorubasree@gmail.com

Dr. N. Radha
Asst.Professor, Dept. of Computer Science
PSGR Krishnammal College for Women
Coimbatore

Abstract—**Biometrics refers to authentication techniques that rely on humans physical and behavioral characteristics that can be automatically checked. Biometric based authentication system provides robust security and ease of use than conventional methods of verification system. Multimodal biometric system is one of the major areas of study identified with large applications in recognition system. Unimodal biometric systems challenge with a wide variety of problems such as noisy data, Intra-class variations, non-universality, and spoof attacks. Some of these limitations can be solved in multimodal biometric system. In proposed work, face and fingerprint biometric traits are used for multimodal biometric authentication system. Biometric traits are transformed using distortion algorithm. After the transformation processes pre-processing of images are done to improve the clear visibility of images. The extractions of minutiae features from fingerprint are achieved using Crossing Number concept and the face features are extracted using the Local Binary Pattern algorithm. To combine both the face and fingerprint features feature level fusion is used. In order to provide additional security to the proposed work the fuzzy vault is introduced by adding duplicate values and having a secret key to lock and unlock the system. Fuzzy vault and distortion acts as an additional layer of security in multimodal biometric user authentication system.**

Keywords-Multimodal, Cancelable, Fusion, Fuzzy vault, Biometrics, Security

I. INTRODUCTION

Biometric traits can be obtained from humans through sensors it is restored as images or signals. So biometric plays an important role in authentication system. Biometric based person recognition overcomes the difficulties of knowledge-based and object based approaches. Locks and keys are generally a physical access to a building, a few pin codes that can be easily stolen by by malicious individuals. Because for access control based on keys or badges the authentication factor is something you have, there is no real guarantee that the person entering your building is the individual that was granted access in the first place.

Biometric authentication system can be broadly divided into two groups, based on the type of biometric trait they use

- Physical Factor, examples are fingerprint recognition and iris recognition
- Behavioral Factor, examples are voice pattern recognition and keystroke dynamics

Noisy sensor information, Intolerable fault rates constrained degrees of freedom are challenges in the Unimodal-biometric trait that utilized in User authentication systems. Such these troubles are the obstacles for the progression of the individual matcher's operational significance. More number of proofs of a single person can able to solve these issues that are utilized in Multi-biometric systems [1]. Overall security in the Multimodal biometric is improved by improving the recognition process and also by reducing the error rates those results better than the uni-modal authentication system. One of the momentous issues in biometric authentication system is protecting the template of the user which is usually stored in a database or smartcard.

First step in proposed system is distortion transformation. One of the solutions to the biggest problem in biometric like achieving its substitution or cancellation in the case of data compromise is to save the original biometric trait separately and use the distorted images for processing. This results in better protection of biometric trait and reduces the leakage of the original biometric trait. The process of creating the distorted image is called transformation.

To combine the multiple biometrics fusion techniques is used for combining the obtained biometric trait. There are five levels image fusion techniques. They are

978-1-4673-6680-9/16/$31.00 ©2016 IEEE

1. Sensor level- This fusion combines raw biometric information that can account for inter-class and intra-class variability and facilitate decision making based on the fused raw data.
2. Feature level- Feature sets extracted from multiple biometrics is combined in feature level fusion
3. Score level- The match score is the similarity between the input and template biometric feature vectors.
4. Decision level- Fusion at this level is carried out only when the decision outputs by the individual biometric matchers are available.
5. Rank level- This method consolidates more than two identification results to enhance the reliability in personal identification.

In proposed work feature level fusion is used for fusing the features extracted from multiple biometric traits.

II. RELATED WORKS

Lots of recent works are based on the multimodal biometric traits like fingerprint, finger vein; palmprint, face, and iris are used along with the fuzzy vault to give more security to the biometrics system. Here are some of the related works of multimodal biometrics system.

- R.Vinoth Kanna et. al [2] proposed a multimodal biometrics with fuzzy vault in which fingerprint and ear are used as biometrics. For the evaluation FAR, FRR, GAR and Accuracy were measured by changing the key value. In this work facilitated better accuracy value of 98.815%.

- V.Evelyn Brindha et. al [3] proposed a multimodal biometrics template security using fingerprint and palmprint based fuzzy vault in which single template and query minutia are used for encoding and decoding. Error rates are measured in order to determine the accuracy. This technique yielded good scores having FNMR of 88% and FMR of 12%.

- A.Muthukumar et. al [4] proposed a multimodal biometric authentication using fingerprint and iris with particle swarm optimization in which fuzzy vaults are combined with two individual biometric to form the cryptosystem by generating the polynomial construction using chaff points. The genuine acceptance rate was increased for authentication and security.

- Chulhan lee et. al [5] proposed a cancelable fingerprint templates using minutiae-based bit-strings. This method generates bit-strings by mapping the minutiae into a predefined 3D array using the coordinates of each minutia. The performance was ideal when each user had a different PIN and two templates from the same fingerprint were not matched when the corresponding PINs were different.
- Geetika et. al [6] proposed a multimodal system with fuzzy vault in which iris and retina. Fuzzy vault is one of the most comprehensive mechanisms in which it is implemented with iris and retina to enhance the system performance. Accuracy of the system was 98%. By changing the key size accuracy level of the system changes.

- Meenakshi et. al [7] proposed a fuzzy vault framework to secure both iris and retina template. The research work is formed by combining fuzzy vault with feature points extracted from retina and iris. This work measures the security of the resultant vault by using min-trophy. The idea of fuzzy vault secures the biometric template as well as the secret data at the same time.

- Mitul D Dhameliya et. al [8] proposed a multimodal biometric recognition system based on fusion of palmprint and fingerprint. Individual score of two traits are fused at feature level and features were extracted using Gabor filter. The GAR of the system was 87%.

- Mohamed Addolahi et. al [10] proposed a multimodal biometric system fusion using fingerprint and iris with fuzzy logic in which decision level fusion is used. A fuzzy logic method is used for fusion to obtain better performance of 98% with FAR of 2% and FRR of 2%.

- Om prakash verma et. al [17] proposed a palmprint based fuzzy vault system for securing cryptographic key. Palm print images suggest its possible usage in an automated palm print based key generation system. The system is very critical in terms of precision required for proper implementation. Reconstruction of polynomial of high power with at most accuracy is somewhat very tedious job and method really lags in this phase. Performance of the system was 92% with FAR of 6% and FRR of 4%.

III. METHODOLOGY

1. Distortion Transformation

Transformation is the process of changing the angle of image from one angle to other angle so that, the transformed image is used for evaluation and original image is

stored for further purpose. Distortion in image is caused by either a characteristic of the lens or the position of camera in relation to the subject. In proposed work, For transformation purpose distortion algorithm is used in image to change the angle from one position to another for evaluation purpose. Face and fingerprint images were rotated at 90^0 with distortion transformation algorithm.

1. At one time rotate all the pixels of the image to guarantee the orientation equals 90^0 and obtain the converted pixel

2. **Angle=a*(exp(-(x*x+y*y)/(b*b))** ------- (1)
   u=cos(angle)*x+sin(angle)*y ------- (2)
   v=-sin (angle)*x+cos(angle)*y ------- (3)
   Where, a is amount of rotation and b size of effect

3. Resultant images are set of transformed images.

4. By storing the distorted images, for further process distorted images are used by securing the original biometric traits.

Distortion algorithm is applied both on fingerprint and face images and all the process in proposed system is done with the distorted image.

2. Binarization

Binary images are mostly used to extract minutiae from fingerprint. The processes of converting original images into binary images are called Binarization process. Intensity value of enhanced image is represented as I(x,y) at pixel position (x,y). Threshold value is represented as Tp. BW(x,y) represents the binary image obtained from equation 4.

$$BW(x,y) = \begin{cases} 1, & if\ I(x,y) \geq T_p \\ 0, & Otherwise \end{cases} \quad \text{------ (4)}$$

3. Thinning

To remove the foreground pixels from the binary images thinning process is used on the skeleton images. It can be used for several applications, but is particularly useful for skeletonization. In this mode it is commonly used to tidy up the output of the edge detectors by reducing all lines to single pixel thickness. Both the input and output of the thinning process are binary images.

4. Crossing-Number concept

Crossing Number (CN) concept is most widely used concept for extracting the minutiae features from the fingerprint. Skeleton image is used for CN concept to extract minutiae where the ridge flow pattern is eight connected. To scan the local neighborhood of each ridge in an image uses 3*3 windows. In the eight-neighborhood half the sum of the differences between pairs of adjacent pixels are calculated to obtain CN value.

Rutovitz's definition of crossing number for a pixel P is given by

$$C_n(P) = (\frac{1}{2})\sum_{i=1}^{8} |P_i - P_{i+1}| \quad \text{------- (5)}$$

Where p_i is the binary pixel value in the neighborhood of p with p_i= (0 or 1) and $p_1=p_9$. The crossing number $c_n(p)$ at a point p is defined as half of cumulative successive differences between pairs of adjacent pixels belonging to the 8-neighborhood of P. For a pixel p, its eight neighborhood pixels are scanned in an anti-clockwise direction as follows

$$\begin{matrix} P_4 & P_3 & P_2 \\ P_5 & P & P_1 \\ P_6 & P_7 & P_8 \end{matrix} \quad \text{--------- (6)}$$

Then the pixels are classified according to the property of their CN value.

- The point is defined as bifurcation if central value is 1 and has more than one 1 value at neighbor.
- The point is called termination if central value of pixel is 1 and its neighbor has only 1 value.

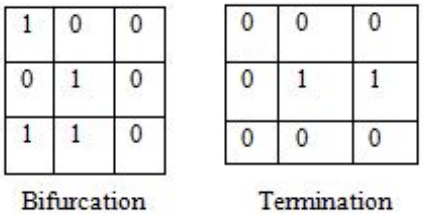

Fig. 1 Bifurcation and termination classification

5. Local Binary pattern

Local binary pattern operator was proposed by ojala to encode the pixel-wise information in textured images. Binary numbers are considered as a result of the LBP operator that labels the pixels of an image by thresholding the neighborhood of each pixel. Two most important properties of Local Binary Patterns are

1. Robustness
2. Computational Simplicity

The basic local binary pattern operator was introduced by Ojala et al. It is based on the assumption that texture has locally two complementary aspects, a pattern and its strength.

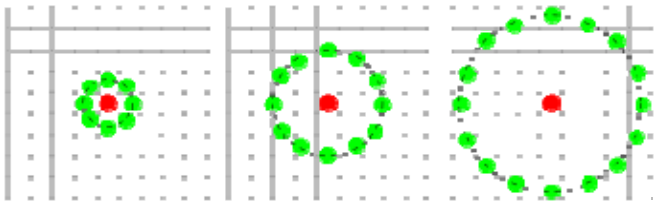

Fig. 2 working model of LBP

The process of LBP labeling the pixels of images is by thresholding the pixels of an image 3*3 neighborhood with central value and converts the result into binary number using the equation 7.

$$LBP_{p,r} = \sum_{n=0}^{p-1} s(x_{r,n} - x_{0,0})2^n, \quad s(x) = \begin{cases} 1, x \geq 0 \\ 0, x < 0 \end{cases}$$

--- (7)

1) The grey values of neighbors which do not lie on precisely in a pixel location may be estimated by interpolation.
2) Given N*M image, let $LBP_{p,r}(i,j)$ identified LBP pattern of each pixel (i,j), then the image is represented by the histogram vector of length k

$$\underline{h}(k) = \sum_{i=1}^{N} \sum_{j=1}^{M} \delta(LBP_{p,r}(i,j) - k)$$

-- (8)

6. Feature level fusion

Feature points extracted from both fingerprint and face is fused using feature level fusion. Both features are concatenated and stored for authentication purpose. The concatenated feature point set has better discrimination power than the individual feature vectors.

7. Fuzzy vault

The proposed multimodal biometric fuzzy vault includes combined feature points from face and fingerprint. The feature points extracted from both fingerprint and face images are fused together in feature level fusion and projected on the polynomial using the proposed algorithm.

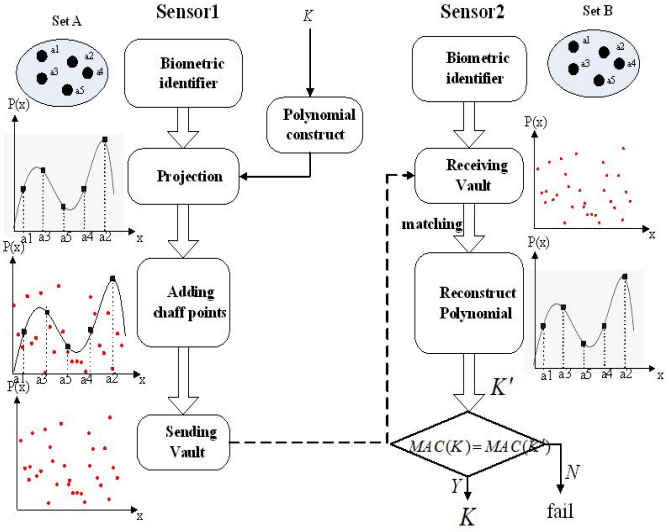

Fig. 3 working of fuzzy vault

Step 1: Polynomial P is selected by the user that will encode the secret K and also evaluates the polynomial on all elements in X.

Step 2: Chaff points i.e additional dummy minutiae points which do not lie on the original polynomial p are add to make confusion to the hacker even if he has the original acces to the stored templates.

Step 3: A special polynomial is generated using a reed Solomon Codeword. All valid codeword's are exactly divisible by the generator polynomial.

Step 4: Both the templates and secret key are secures concurrently by encoding the complete information about template X and secret K points lying on P Since the points lying on P. By providing another biometric sample the user can able to recover the secret key K from the vault V.

Step 5: Let the query be represented as another unordered set *X*'. If *X*' overlaps considerably with *X*, then the user can identify many points in *V* that lie on *P*.

Step 6: It is possible to decode the secret K if adequate number of points on *P* can be identified and are able to recreate P. If *X*' does not overlap considerably with *X*, it is infeasible to reconstruct *P* and the authentication is unsuccessful.

Step 7: Even when X and X' are not exactly same the secret can be retrieved from the vault, this scheme is referred to as a fuzzy vault.

IV. EXPERIMENTAL RESULT

The proposed system is evaluated in MATLAB R2014a.100 faces and 100 fingerprint images that are obtained. Evaluation of the system is done by measuring False Acceptance Rate [FAR], false rejection rate [FRR] and accuracy. As cancellable distortion is applied on the input images, the transformed image is processed by preserving the original biometric data. By using distortion algorithm original image can be secured and used if any biometric templates are stolen. Fuzzy vault act as an additional layer of security to authentication system. So that, the security of the system is also increased with low FAR of 2%, FRR of 1.8% and high GAR with 98.1%. Secret key size of the fuzzy vault is 8. Accuracy level changes once the secret key size of the vault is being changed. The results of the proposed system are mentioned in Figure 2.

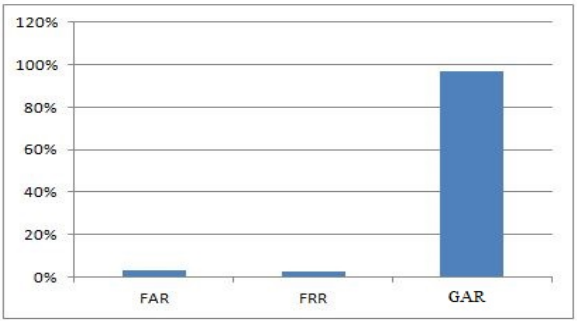

Fig. 4 Performance of the cancelable system with fuzzy vault

Proposed Techniques	FAR	FRR	GAR
Cancelable authentication system	*3%*	*2.8%*	*97.1%*
Cancelable authentication system with fuzzy vault	*2%*	*1.8%*	*98.1%*

Table 1 Summary of the research work

Table 1 justifies the performance analysis of proposed techniques. Cancelable authentication system without fuzzy vault is less secure when compared with the performance of the cancelable authentication system with fuzzy vault. The proposed technique done with fuzzy Vault results with high GAR and with low FAR and FRR

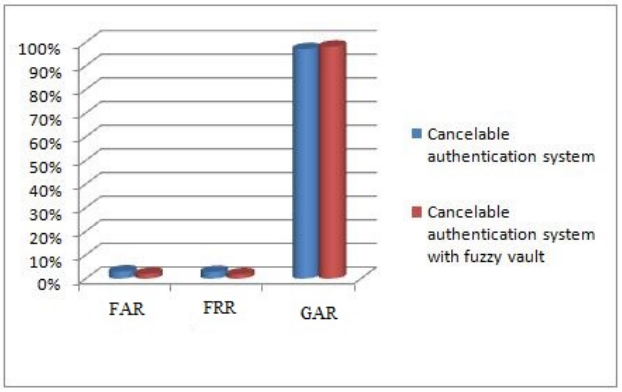

Fig. 5 Summary of the research work

V. CONCLUSION

The proposed technique aims to improve the template security by the use of fuzzy vault. In proposed work, for effective human recognition system with distorted image, the biometric images follows pre-processing, feature extraction, fusion and fuzzy vault. Multimodal system with face and fingerprint was effectively implemented in Matlab. For the evaluation of the research work FAR, FRR and accuracy are calculated. Accuracy was measured by changing the secret key size. Fuzzy vault is done to improve the accuracy and to decrease the FAR and FRR which will improve the level of security in user authentication. Thus, the experimental result of the proposed system achieved secured recognition and authentication result when compared with the other traditional methods. In future, Different cancelable algorithm can be used to generate new template and Usages of different transformation methods for template security enable us to improve the level of security.

REFERENCES

[1]. A. Ross, A.K.Jain, “Information fusion in biometrics”, Pattern recognition letters, 2003, Vol.24,No.3, pp2115-2125.

[2]. R.Vinoth Kanna, Dr.Amitabh Wahi,” Fuzzy vault based multimodal biometric human recognition system with fingerprint and ear”, Journal of theoretical and applied information technology, 2014, Vol.59 No.2, pp 304-316.

[3]. V.Evelyn Brinda, AM Natrajan," Multi-modal biometric template security: Fingerprint and palmprint based fuzzy vault", Journal of Biometrics and Biostatistics, 2012, Vol.3, No.6, pp1-6.

[4]. A.Muthukumar, C.Kasthuri, S.Kannan,"Multimodal biometric authentication using particle swarm optimization algorithm with fingerprint and iris", ICTACT journal on image and video processing, 2012, Vol.02, No.03, pp 369-374.

[5]. Chulhan Lee, Jaihie Kim, "Cancelable fingerprint templates using minutiae-based bit-strings", Journal of network and computer applications, 2010, Vol.3, No.5, pp 236-246.

[6]. Geetika, Manavjeet Kaur, "Fuzzy vault with iris and retina", International Journal of advanced research in computer science and software Engineering, 2013, Vol.3, No.4, pp 294-297.

[7]. V.S.Meenakshi, Dr.G.Padmavathi,"Retina and iris based multimodal biometric fuzzy vault", International Journal of computer applications, 2010, Vol.1, No.29, pp 67-73.

[8]. Mitul Dhameliya, Jitendra Chaudhari, "A Multimodal biometric recognition system based on fusion of palmprint and fingerprint", International journal of Engineering trends and technology, 2013, vol.4, No.5, pp 1908-1911.

[9]. Shekar S., Patel, Chellappa R., "Joint sparsity – based robust multimodal biometrics recognition", In proceeding of computer vision-ECCV 2012, Springer, 2012, pp 365-374.

[10]. Jain, A.K.Prabakar, Pankati s, "Filterbank- based fingerprint matching", IEEE Transactions on Image processing, 2000, pp 846-859.

[11]. A.K.Jain, A.Ross, "An introduction to biometric recognition", IEEE Transaction on circuits and system for video technology, 2004, Vol.14, No.3, pp 4-20.

[12]. T.Sim, S.Zhang, R.Janakiraman, "Continuous verification using multimodal biometrics", IEEE transaction on pattern analysis and machine intelligence, 2007, Vol.29, No.4, pp 687-700.

[13]. Ojala, Pietikien, Harwood, "A comparative study of texture measures with classification based on featured distributions", Pattern recognition, 1996, Vol.29, No.6, pp 51-59.

[14]. Paul, "Multimodal cancelable biometrics", Cognitive informatics and cognitive computing IEEE 11th international conference, 2012, Vol.4, No.2, pp 43-49.

[15]. Karthik Nandakumar, Abhishek Nagar, Anil.K.Jain, "Hardening Fingerprint fuzzy vault using password", International conference on biometrics, 2007, Vol.3, No.3, pp 35-41.

[16]. A.K.Jain, A.Ross, S.Pankati, "Biometrics: A tool for information security", IEEE Transactions on information forensics and security, 2006, Vol.1, No.2, pp125-143.

[17]. Om Prakash verma, Devesh Bharathan, "A new palmprint based fuzzy vault system for securing cryptographic key", International Journal of Information and Electronics and engineering, 2012, Vol.2, No.2, pp 289-292.