ISSN No. 0976-5697

Volume 6, No. 6, June - July 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Privacy Preserving in Multimodal Biometrics Via Piecewise Polynomial Filtering Function

A.Pethalakshmi
Associate Professor and Head of the Department,
Dept of CS, MVM Govt Arts College (W),
Dindigul, India

A.P.Caroline Hirudhaya
Research Scholar
Manonmaniam Sundaranar University
Tirunelveli, India

Abstract: Confirming the identity of a person is the important criteria to access through the confidential services on the net. The confirmation of identity is done through various methods like passwords, pin numbers, and biometrics features. The field of identification using biometrics expands from unimodal biometrics to multimodal biometrics. In multimodal biometrics the modalities may differ. In this paper three modes of biometric traits are combined using various fusion techniques. We propose piecewise polynomial filtering function to enhance the privacy of the system.

Keywords: biometrics, traits, fusion techniques, piecewise polynomial filtering

I. INTRODUCTION

A. *Authentication:*

Nowadays with the blooming trends of internet, e-commerce and m-commerce people are becoming more and more connected through electronic network. A network is established electronically throughout the world among individuals, and organizations. The ability to automatically establish the identity of individuals is known as person identification or person authentication which is essential for the access of network and reliable transactions. Person authentication can be performed by different methods like knowledge, token, and biometric (e.g., speech, face). Person authentication is done mostly using: text passwords, personal identification numbers, barcodes and identity cards.

The merit of these schemes is that they do not change their value with respect to time and also unaffected by the environment in which they are used. The main demerit of them is that they can be easily misused or forgotten. Also, Day by day more services are being offered over the electronic devices and internet. Hence it becomes unmanageable to keep track of the authentication secrets for different services. When an alternative is analyzed to overcome all these demerits biometric features for person authentication comes to bloom. Either or both the physiological and behavioural characteristics of human can be used as biometric feature. The biometric feature possesses the properties like universality, distinctiveness, permanence, acceptability and performance. Password or card can be shared, forgotten or stolen, but not the biometric.

B. *Biometric System:*

Acquisition of biometric is more complex compared to making combinations of digits or stealing the card. In this way, biometric is more secure compared to PIN and password. Passwords are desirable to be different for different applications, but same biometric can be used for most of the applications and hence avoids book keeping. Any human physiological or behavioral characteristic can be used as a biometric characteristic to make personal identification Some of the commonly used biometric features include speech, face, signature, finger print, handwriting, iris, DNA, Gait, etc.

C. *Multimodal Biometric system:*

Biometric system used for personal identification can be classified into two categories. One is unimodal biometric system and multimodal biometric system. Biometric systems based on single source of information are called unimodal systems. Multimodal biometric systems, which combine information from multiple modalities (like face, fingerprint and iris). Multimodal biometric systems can achieve better performance compared with unimodal systems. The information from the multiple sources are integrated either in the earlier stage of the process or in the later stage of the process.

The rest of this paper is organized as follows: Section 2 reviews the supported literature. Section 3 presents a description of the proposed system. Section 4 is illustrated with the experimental results. The efficiency and effectiveness of the algorithm were discussed. Finally, Section 5 concludes the paper with enhancement that can be extended.

II. LITERATURE REVIEW

Anil Jain et al [1] introduced a multimodal biometric system by combining fingerprint, face and speech which proved a better reliability than the unimodal biometric system.

K.Sasidhar et al [2] had examined large face and fingerprint data sets by using various normalization and fusion techniques. The results of their study showed that the performance of multimodal biometric system is higher than the performance of unimodal system.

A.K. Jain et al [3] emphasis fusion of the multiple modalities at the match score level due to the reason of its easiness to access and combine the scores presented by the different modalities. Rukhin and alioutov [4] proposed fusion based on a minimum distance method for combining rankings from several biometric algorithms. Kittler et al. [5] compared the various fusion methods and found that the sum rule outperformed many other methods, Verlinde et al. [6] and Fierrez-Aguilar et al. [7] did the comparison on various fusion methods. While Fierrez-Aguilar et al. [8] and Gutschoven and Verlinde [9] designed learning based strategies using support vector machines.

J.P. Baker and D.E. Maurer [10], applied Bayesian belief network (BBN) based architecture for biometric fusion applications. Bayesian networks provide united probabilistic framework for optimal information fusion. Bigun et al. [11] developed a statistical framework based on Bayesian statistics to integrate the speech (text dependent). Hong and Jain associated different confidence measures with the individual matchers when integrating the face and fingerprint traits of a user [12]. They also suggest an indexing mechanism wherein face information is used to retrieve a set of possible identities and the fingerprint information is then used to select a single identity. A commercial product called BioID [13] uses the voice, lip motion and face features of a user to verify the identity. Aloysius George used Linear Discriminant analysis (LDA) for face recognition and Directional filterbank (DFB) for fingerprint matching.

III. PROPOSED WORK

So far the research on multimodal biometrics brings out various aspects of the specified area. It shows that the multimodal biometric systems were developed by combining speech, signature, fingerprint and face etc. In this paper, the proposed work focuses on a multimodal biometric system by combining palm print, hand geometry, knuckles and speech of a single person. Hand images both on the palm side and the dorsum side are captured using 3-D camera. The speech of the person is recorded using microphone in a closed environment. These traits obtained from the user are fused together and used for further identification.

A. Hand Geometry and Palmprint:

The 3-D and 2-D hand geometry and3-D and 2-D palmprint of a person were extracted. The pose corrected range and intensity images are processed to locate regions of interest (ROI) for hand geometry and palmprint feature extraction [14]. These features are fused together dynamically as follows.

a. 3-D Palmprint & 3-D Palmprint:

3-D palmprints are being extracted from images of the hand offer highly discriminatory features for personal identification. Features contained in the 3-D palmprint are primarily local surface details in the form of depth and curvature of palmlines and wrinkles. We employ the SurfaceCode 3-D palmprint representation. This compact representation is based upon the computation of shape index at every point on the palm surface.

2-D palmprint has been extensively researched and numerous approaches for feature extraction and matching are available. In this work, we employ the competitive coding scheme. Six Gabor filtered images are used to compute the prominent orientation for every pixel in the palmprint image and the index of this orientation is binary encoded to form a feature representation (CompCode).

b. 3-D Hand Geometry & 2-D Hand Geometry:

3-D features extracted from the cross-sectional finger segments are highly discriminatory and useful for personal identification. For each of the four fingers (excluding thumb), 20 cross-sectional finger segments are extracted at uniformly spaced distances along the finger length. Curvature and orientation are computed at every data point on these finger segments constitute the feature vectors [14].

2-D hand geometry features are extracted from the binarized intensity images of the hand. The hand geometry features utilized in this work include finger lengths and widths, finger perimeter, finger area and palm width. Measurements taken from each of the four fingers are concatenated to form a feature vector. The computation of matching score between two feature vectors from a pair of hands being matched is based upon the Euclidean distance.

c. Fusion Of Hand Geometry And Palm print:

In this approach, we develop a simple but efficient approach for combining palmprint and hand geometry scores that are simultaneously extracted from the pose corrected range and intensity images. For every probe hand, the orientation information estimated in the pose normalization step is utilized to selectively combine palmprint and hand geometry features. The proposed dynamic combination approach attempts to identify and ignore the poor hand geometry match scores using the estimated orientation of the hand.

B. Extraction of Knuckles:

The finger geometry parameters extracted from the hand images previously are employed to locate the graylevel pixels belonging to the four individual fingers. The located finger pixels are used to extract the knuckle regions for feature extraction [15]. First, four additional points are located from the finger contour. Two of them are one-third of the distance between the fingertip and the base points of the finger and the other two are two-thirds of the distance. The line joining the middle points of the line segments and defines the line of symmetry of the finger-strip region. The length of the strip is chosen to be the length of the finger. The width of the strip is chosen to be the minimum distance between the base points of the finger. With this length and width, the ROI pixels for each of the four fingers are extracted symmetrically on both sides of the symmetry line.

A total of six finger geometry features is computed from each of the fingers, resulting in a total of 24 finger geometry features. These include one finger length, three finger widths, finger perimeter, finger area. The normalization of extracted geometrical features is essential because of their varying ranges and order. Then the knuckles are to be extracted.

Min-Max normalization

$$x'_{ik} = \frac{x_{ik} - \min(x_{ik})}{\max(x_{ik}) - \min(x_{ik})}$$

Z-score normalization

$$x'_{ik} = \frac{x_{ik} - \alpha}{\beta}$$

Once the finger regions are segmented, the knuckle regions are located for the extraction of reliable features.

The knuckle regions from the segmented fingers can be extracted in two ways.

In one way, a fixed size knuckle region of the finger is extracted based on the finger length. For example, along the central line of the finger, a region of fixed size 80 x100 pixels is extracted symmetrically from the middle finger at a distance of one-third the length from the tip of the finger. Similarly, a region of 50 ×100 pixels is extracted from little and index fingers while a region of 80× 100 is extracted from the ring finger.

Another way is investigated to further improve the localization of the region of interest. The canny edge detector is first applied on the extracted finger image. The density of the high intensity pixels in the resultant image is used for ROI extraction. . The extracted knuckle region will be fused with other features.

C. *Speaker Feature extraction:*

The fMAPLR is a linear regression function that projects speaker dependent features to speaker independent ones, also known as an affine transform. It consists of two sets of parameters, bias vectors and transforms matrices. In this paper a scheme is proposed, which allows the bias vectors and the matrices to be associated with different regression classes, such that both parameters are given sufficient statistics in a speaker verification task [16].

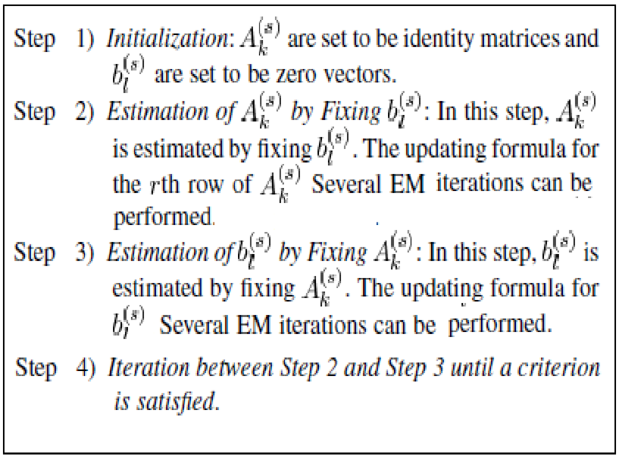
If we assume that a speech utterance spoken by a speaker is represented by a sequence of feature vectors, we define the fMAPLR function that maps the speaker's feature vector to a speaker independent feature vector as follows:

$$y_t \triangleq \mathcal{F}(y_t^{(s)};\Theta^{(s)}) = A_k^{(s)} y_t^{(s)} + b_l^{(s)}$$

We have three sets of parameters, that are 1) the GMM parameter set, 2) the hyper parameter set, and 3) the fMAPLR parameter set. GMM and hyper parameter sets are estimated on the background data, and fMAPLR parameter is estimated on the speaker's data. We jointly estimate the hyper parameters and the GMM parameters to maximize the likelihood on the background data.

a. *Estimation of fMAPLR Parameters:*

The hyper parameters and the GMM parameters are provided and the fMAPLR parameters are estimated by maximizing the posterior. Similar to the estimation of hyper parameters, we adopt the method of alternative variables estimation [15, 16]. It is estimated with the following steps.



Step 1) *Initialization*: $A_k^{(s)}$ are set to be identity matrices and $b_l^{(s)}$ are set to be zero vectors.

Step 2) *Estimation of $A_k^{(s)}$ by Fixing $b_l^{(s)}$*: In this step, $A_k^{(s)}$ is estimated by fixing $b_l^{(s)}$. The updating formula for the rth row of $A_k^{(s)}$ Several EM iterations can be performed.

Step 3) *Estimation of $b_l^{(s)}$ by Fixing $A_k^{(s)}$*: In this step, $b_l^{(s)}$ is estimated by fixing $A_k^{(s)}$. The updating formula for $b_l^{(s)}$ Several EM iterations can be performed.

Step 4) *Iteration between Step 2 and Step 3 until a criterion is satisfied.*

D. *Fusing the modalities:*

All these features have to be fused to form a multimodal biometric system. There are various fusion techniques available now to fuse the individually obtained components [15]. The raw data obtained from different modalities are fused together. We also applied Piecewise polynomial filtering function for enhancing privacy-preserving of the data and then those data are fused together. We have employed the fusion techniques as data level fusion, feature level fusion, serial rule, sum rule, and weighted sum rule.

IV. ENHANCING PRIVACY PRESERVING APPROACH

A. *Piecewise polynomial filtering function:*

Here we propose a new Piecewise polynomial filtering function for enhancing privacy-preserving of the data. This function introduces a basis of the corresponding linear space and then applies the linear combinations of these basis functions.

If we have a strictly increasing sequence $\xi := (\xi_i)_{i=1\ldots l}$ of knots $\xi_i \in$ R and polynomials P_i, i = 1…l, each of order k (i.e., of degree < k), then we define a piecewise polynomial function of order k by

$$f(x) := \begin{cases} 0, & x < \xi_1 \\ P_i(x), & \xi_i \leq x < \xi_{i+1}\,, \\ P_l(x), & x \geq \xi_l\,. \end{cases} \quad , \qquad i = 1$$

The function and its derivatives may or may not be continuous at the knots ξ_i. It is easy to see that the set of piecewise polynomial functions of order k defined for a fixed knot sequence generates a linear space.

This linear space is called as $P_{k,\ \xi}$. When using the piecewise polynomial functions as filter kernels, we require the right-most polynomial P_l to be zero, since the kernels must have finite support.

V. EXPERIMENTAL RESULTS

The different modalities like palm print, hand geometry, knuckle extraction and speech extraction are combined to form a multimodal biometric system. We have applied various fusion techniques on the raw data and privacy preserved data, which is applied with piecewise polynomial filtering function. The graph I and 2 shows the accuracy level and error level for raw data respectively. Likewise the graphs 3 and 4 represent the accuracy level and error level respectively for data with piecewise polynomial function.

The accuracy is higher when serial rule is applied. The accuracy is lower when data level fusion is applied. Likewise the error rate is lower when applying serial rule, but it is higher in case of data level fusion.

While the features are combined together and applied cryptography techniques the accuracy level and error rate varies. Here the accuracy level is higher when weighted sum rule is used. Likewise the error rate is lower while using weighted sum rule.

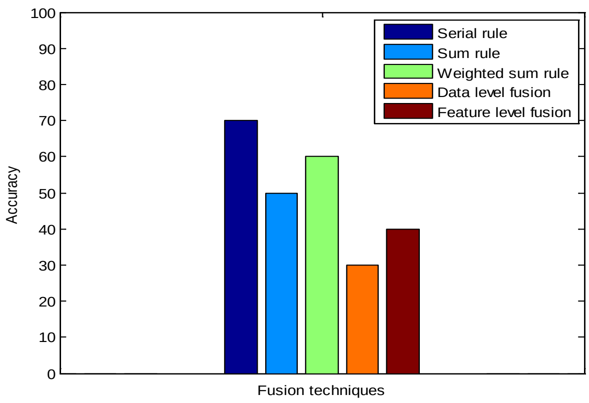


Figure 1: Accuracy level for raw data

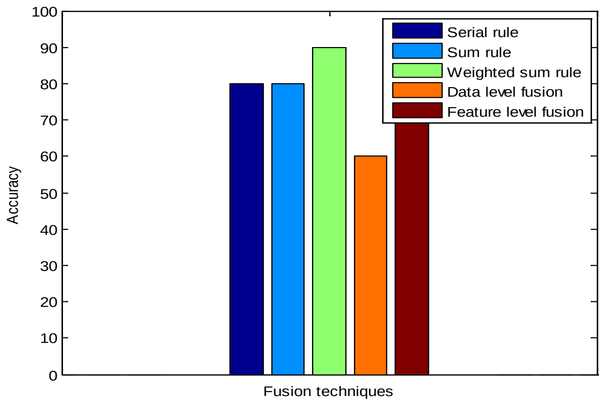


Figure 2: Error level for raw data

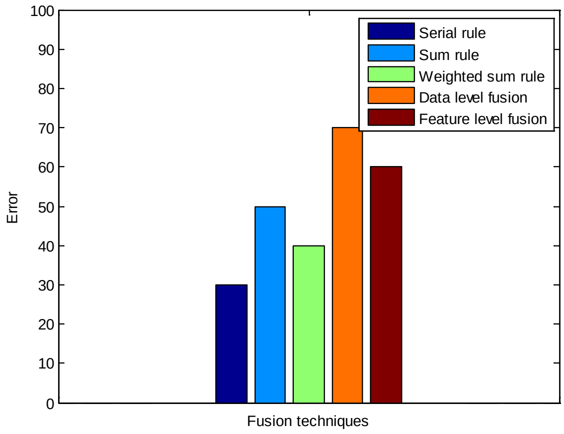


Figure 3: Accuracy level for privacy preserved data

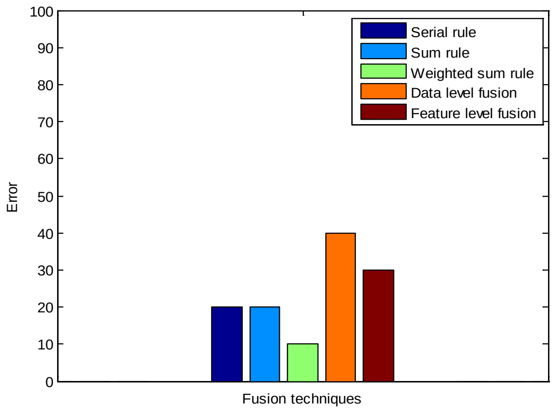


Figure 4: Error level for privacy preserved data

The biometric system is evaluated by false negative rate, false positive rate, true positive rate and true negative rate. The table 1 is illustrated with comparative values of fusion techniques for raw data and privacy preserved data subjected to piecewise polynomial data.

Table 1 : Comparison of raw data and privacy preserved data

FUSION TECHNIQUES	False negative rate		False positive rate		True positive rate		True negative rate	
	data with Piecewise polynomial function	Raw data	data with Piecewise polynomial function	Raw data	data with Piecewise polynomial function	Raw data	data with Piecewise polynomial function	Raw data
SERIAL RULE	1 %	2%	1 %	1%	4 %	3 %	4 %	4 %
SUM RULE	1 %	1%	1 %	4-5%	4 %	3 %	4 %	2 %
WEIGHTED SUM RULE	0 %	0%	1 %	4-5%	4 %	3 %	4 %	3 %
DATA LEVEL FUSION	2-3 %	3%	2 %	4-5%	3 %	1 %	3 %	2 %
FEATURE LEVEL FUSION	1 %	3%	2 %	3-4%	3 %	2 %	4 %	2 %

VI. CONCLUSION

We have fused the data from different modalities like palmprint, hand geometry, knuckle extraction and speech extraction. The raw data obtained from different modals are combined by using various fusion techniques. We have also applied piecewise polynomial filtering function to preserve the privacy of the data for enhancing the security level. The performances were analyzed for raw data and privacy preserved data. The data subjected to piecewise polynomial function shows the higher accuracy level. Weighted sum rule gives the better performance in privacy preserved data. In near future various combination of biometric features can be implemented. We can use various fusion techniques in combining the biometric features.

VII. REFERENCES

[1]. Anil Jain, Lin Hong, and Yatin Kulkarni,"A Multimodal biometric system using Fingerprint, Face and Speech"

[2]. K.Sasidhar, Vijaya L Kakulapati, Kolikipogu Ramakrishna and K.KailasaRao, "Multimodal Biometric Systems –Study To Improve Accuracy And Performance", International Journal of Computer Science and Engineering Survey, Vol 1, no 2, pp 54-61,November 2010.

[3]. A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition". IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.

[4]. L. Rukhin, and I. Malioutov, “Fusion of biometric algorithms in the recognition problem”. Pattern Recognition Letter, pp. 26, 679–684, 2005.

[5]. Kittler, “On combining classifiers”. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20 (3), pp. 226–239, 1998.

[6]. P. Verlinde, G. Chollet, and M. Acheroy, “Multimodal identity verification using expert fusion”. Information Fusion, vol. 1 (1), pp. 17-33, 2000.

[7]. J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, “Fusion strategies in multimodal biometric verification”. In Proceedings of International Conference on Multimedia and Expo (ICME ’03), vol.3 (6–9), pp. 5–8, 2003.

[8]. J. Fierrez-Aguilar, “Kernel-based multimodal biometric verification using quality signals”. Biometric Technology for Human Identification, Proceedings of the SPIE, vol. 5404, pp. 544–554, 2004.

[9]. B. Gutschoven, P. Verlinde, “Multimodal identity verification using support vector machines (SVM)”.Proceedings of the Third International Conference on Information Fusion, vol. 2, pp. 3–8, 2000.

[10]. J.P. Baker, and D.E. Maurer, “Fusion of biometric data with quality estimates via a Bayesian belief network”. Proceedings of the Biometric Symposium, Arlington, VA, pp. 21–22, 2005.

[11]. E.S. Bigun, J. Bigun, B. Duc, and S. Fischer, “Expert conciliation for multimodal person authentication systems by Bayesian statistics”. First International Conference AVBPA Proceedings, Springer Lecture Notes in Computer Science, vol. 1206, pp. 291–300, 1997.

[12]. L. Hong and A. K. Jain, “Integrating faces and fingerprints for personal identification”. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, pp. 1295– 1307, Dec 1998.

[13]. R. Brunelli and D. Falavigna, “Person identification using multiple cues”. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 12, pp. 955–966, Oct 1995.

[14]. V. Kanhangad, A. Kumar, and D. Zhang, “Combining 2-D and 3-D hand geometryfeatures for biometric verification,” in Proceedings of IEEE Workshop Biometrics, Miami, FL, pp. 39–44, Jun. 2009.

[15]. A. Pethalakshmi and A.P. Caroline Hirudhaya**,** “Enhancing the Security and Privacy of Multi Modal Biometric System”**,** International Journal of Computational Intelligence and Informatics, Vol 2, no.3, December 2012.

[16]. Donglai Zhu, Bin Ma, and Haizhou Li, “Joint Map Adaptation of Feature Transformation and Gaussian Mixture Model for Speaker Recognition”, Institute for Infocomm Research, A*Star, 1 Fusionopolis Way, Singapore.