International Journal of Computational Intelligence and Informatics, Vol. 2: No. 3, October - December 2012

Enhancing the Security and Privacy of Multi Modal Biometric System

A Pethalakshmi
Associate Professor and Head
Department of CS, MVM Govt Arts College (W),
Dindigul, India
pethalakshmi@yahoo.com

A P Caroline Hirudhaya
Research Scholar
Manonmaniam Sundaranar University
Tirunelveli, India
carol_aps@yahoo.co.in

***Abstract*- Person authentication is done mostly by using one or more of the following means as text passwords, personal identification numbers, barcodes and identity cards. The technology has been improved to secure the privacy via biometrics. Unimodal biometrics are normally used to provide personal authentication. In this paper multimodal biometrics, combination of palmprint, hand geometry, knuckle extraction and speech are applied to authentication with improved security. In this paper we propose a new approach in multimodal biometrics by applying Least mean square algorithm, which is one of the adaptive filtering algorithm to preserve the privacy.**

Keywords- Unimodal biometrics, multimodal biometrics, secure adaptive filtering, Least mean square algorithm

I. INTRODUCTION

A. Authentication

Nowadays people are connected electronically with the out bounding trends of internet, e-commerce and m-commerce. A network is established electronically among individuals, organizations, etc. To connect through the internet the individuals have to establish the identity. That is known as person identification or person authentication. This is essential for the access of network and reliable transactions. Person authentication can be done by different methods like knowledge, token, and biometric (e.g., face, gait). Person authentication is usually done through text passwords, personal identification numbers, barcodes and identity cards. These identification methods do not change their value with respect to time and also unaffected by the environment. The major drawback of them is that they can be easily misused or forgotten. When the services increase it is unmanageable to remember the authentication secrets for different services. In order to avoid all these drawbacks the use of biometric features for person authentication is preferred. Any physiological and/or behavioural characteristics of human can be used as biometric feature for the authentication as they have the properties of universality, distinctiveness, permanence, collectability, circumvention, acceptability and performance. Password or card can be shared, forgotten or stolen, but not the biometric.

B. Biometric System

Making combinations of digits or stealing the card is easier but the acquisition of biometric is more complex. Hence, biometric is more secure compared to PIN and password. Book keeping can be avoided as biometric can be used for most of the applications, but passwords are desirable to be different for different applications. Any one of the human physiological or behavioral characteristic can be used as a biometric characteristic (indicator) to make personal identification. Commonly in use biometric features include speech, face, signature, finger print, handwriting, iris, DNA, Gait, etc.

C. Multimodal Biometric system

When biometric systems uses single source of information then they are called as unimodal systems. When they combine multiple sources of information (like face, fingerprint and iris) they are called multimodal biometrics. 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.

ISSN: 2349 - 6363

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

II. LITERATURE SURVEY

Hong and Jain [5] proposed an identification system based on face and fingerprint, where fingerprint matching is applied after pruning the database via face matching. Kittler et al. [2] have experimented with several fusion techniques for face and voice biometrics, including sum, product, minimum, median, and maximum rules, among them they noted that the sum rule is not significantly affected by the probability estimation errors and this explains its superiority.

Brunelli and Falavigna [3] used hyperbolic tangent (tanh) for normalization and weighted geometric average for fusion of voice and face biometrics. Ben-Yacoub et al. [4] considered several fusion strategies, such as support vector machines, tree classifiers and multi-layer perceptrons, for face and voice biometrics. The Bayes classifier is found to be the best method. Ross and Jain [1] combined face, fingerprint and hand geometry biometrics with sum, decision tree and linear discriminant-based methods.

III. PROPOSED ALGORITHM

The research on multimodal biometrics reveals various new aspects of the specified area. It shows that the existing multimodal biometric systems were developed by combining speech, palmprint, signature, fingerprint , iris 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 person. These characteristics obtained from the user are fused together and used for further identification. We propose LMS algorithm, one of the secure adaptive filtering algorithms is applied to the data to preserve the privacy. The hand images are captured using 3-D digital camera for the extraction of palmprint, hand geometry and knuckle extraction. The speech is recorded through microphone in a closed environment.

A. Palmprint

a) 3-D palmprints extracted from the range images of the hand (region between finger valleys and the wrist) offer highly discriminatory features for personal identification. We employ the SurfaceCode 3-D palmprint representation. This is a compact representation, which is based upon the computation of shape index at every point on the palm surface. Based upon the value of the shape index, every data point can be classified in to one of the nine surface types. The index of the surface category is then binary encoded using four bits to obtain a SurfaceCode representation.

b) 2-D Palmprint Personal authentication based upon 2-D palmprint has been extensively researched and numerous approaches for feature extraction and matching are available. We employ the competitive coding scheme. This approach uses a bank of six Gabor filters oriented in different directions to extract discriminatory information on the orientation of lines and creases on the palmprint. 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. .

B. Hand Geometry

a) 3-D features extracted from the cross-sectional finger segments have been 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 (in terms of unit normal vector) computed at every data point on these finger segments constitute the feature vectors.

b) 2-D Hand Geometry 2-D hand geometry features are extracted from the binarized intensity images of the hand. The hand geometry features 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.

C. Dynamic fusion strategy

Normally the palmprint and hand geometry scores extracted from the pose corrected range and intensity images are combined together. But Pose correction of the image may lead to loss of information around the finger edges and, therefore, results in incomplete (partial) region of interest for finger geometry feature extraction. Hence we use the orientation information, estimated in the pose normalization step for every probe

hand to selectively combine palmprint and hand geometry features. The dynamic combination identifies and ignores those poor hand geometry match scores by using the estimated orientation of the hand.

D. Extraction of Knuckles

The finger geometry parameters are extracted from the hand images acquired are employed to locate the gray level pixels belonging to the four individual fingers. These finger pixels are used to extract the knuckle regions. 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 defines the line of symmetry of the finger-strip region. The length of the strip is taken to be the length of the finger. The width of the strip is taken to be the minimum distance between the base points of the finger. With this length and width, the Region Of Interest (ROI) pixels for each of the four fingers are extracted symmetrically on both sides of the symmetry line. In total six finger geometry features are 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, and finger area. The normalization of extracted geometrical features is essential because of the variation in their 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. It may be noted that the finger images extracted from each hand image vary in size. We applied two methods for extracting knuckle regions from the segmented fingers.

Method A: In this approach, 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 x 100 pixels is extracted symmetrically from the middle finger at a distance of one-third the length from the tip of the finger. Likewise, 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.

Method B: Another method is applied 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. In the knuckle region, the density of intensive pixels is very high. This region can be extracted on either side of the central line. Hence, a 80 ×100 pixel highly dense region is extracted centrally from the base part of the finger. That is a region with mostly edge elements along the finger symmetry line, In the same way, fixed regions of size 50× 100 pixels are extracted from little and index fingers.

E. Speaker Feature extraction

The fMAPLR is a linear regression function that projects speaker dependent features to speaker independent ones, that is known as an affine transform. It consists of two sets of parameters, bias vectors and transforms matrices. The former, representing the first order information, is more robust than the latter, the second-order information. We propose a flexible tying scheme that 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. We utilize a maximum *a posteriori* (MAP) algorithm for the estimation of feature transform parameters that further alleviates the possible numerical problem.
If a speech utterance spoken by a speaker is represented by a sequence of feature vectors, which are - dimensional vectors. We define the fMAPLR function that maps the speaker's feature vector to a speaker independent feature vector as follows:

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

Here three sets of parameters are applied, that are 1) the GMM parameter set, 2) the hyper parameter set, and 3) the fMAPLR parameter set are 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.

An important issue in speaker recognition is the intraspeaker intersession variability such as the channel effects. In the feature domain, the variability in feature vectors can be normalized by methods such as feature mapping.

a) Estimation of Hyper parameters

The hyperparameters and the GMM parameters are estimated together to maximize the likelihood on the background data. The estimation is carried out by using the method of alternative variables, in where the hyperparameters are updated iteratively in multiple steps, each estimating one subset of hyperparameters by fixing the other hyperparameters.

*b) Estimation of fMAPLR Parameter*s

By computing the given hyper parameters and the GMM parameters, the fMAPLR parameters are estimated. Similar to the estimation of hyper parameters, we adopt the method of alternative variables to estimate.

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

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

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

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

F. Fusion techniques

Here in this paper, we have experimented various fusion strategies. The results which are the outcome of various fusion techniques are analyzed. We have applied data level fusion, feature level fusion and match score level fusion for combining palmprint, hand geometry, knuckle extraction and speech.

a) Data level fusion, also called pixel level fusion, combines several sources of raw data to produce new raw that is expected to be more informative and synthetic than input. It is the low level fusion.

b) Feature level fusion, is the one in which the data obtained from each biometric modality is computed as a feature vector. It is intermediate level fusion. It can compress data for processing. As the extracted features have a direct relationship with decision. The result of fusion has more feature information required for decision making.

c) Matching score level fusion is the most commonly used biometric information fusion strategy because matching scores are easily available and because they retain sufficient information to distinguish genuine matching from impostor matching. Generally, a multi-biometric system based on the matching score level fusion works as follows: each subsystem of the multi-biometric system exploits one biometric trait to produce a matching score. Then these matching scores are normalized and integrated to obtain the final matching score or final decision for personal authentication. We have employed sum rule, serial rule and weighted sum rule in this level of fusion.

Serial rule: Let $X = (X_1,..., X_d)$ and $Y = (Y_1,..., Y_d)$ Y Y be vector sets of three different modal features. Then the fusion features in serial rule were $Z = (Z_1,..., Z_d)$. Here d is the number of samples. The i^{th} fusion feature is (x_i^1 ... x_i^m , y_i^1 ... y_i^m). Here x_i^m denotes the m^{th} dimension of the i^{th} vector.

Sum rule: Let $X = (X_1,..., X_d)$ and $Y = (Y_1,..., Y_d)$ Y Y be vector sets of two different modal features. Then the fusion features in serial rule were $Z = (X_1 + Y_1, X_d + Y_d)$. Here d is the number of samples. The i^{th} fusion feature is (x_i^1 ... x_i^m , y_i^1 ... y_i^m). Here x_i^m denotes the m^{th} dimension of the i^{th} vector

Weighted sum rule: Let $X = (X_1,..., X_d)$ and $Y = (Y_1,..., Y_d)$ Y Y be vector sets of two different modal features. Then the fusion features in serial rule were $Z = (X_1 + wY_1, X_d + wY_d)$. Here

d is the number of samples. The i[th] fusion feature is (x_1^1 +w y^1... x_1^m +w y^m). Here x_1^m denotes the m[th] dimension of the i[th] vector.

We employ data level fusion, feature level fusion and match score level fusion in this paper. First, 2-D, 3-D palmprint and 2-D, 3-D hand geometry features are combined by using dynamic fusion strategy. Then it is combined with knuckle extraction and speech extraction by using the above mentioned fusion techniques. This is illustrated in figure 1.

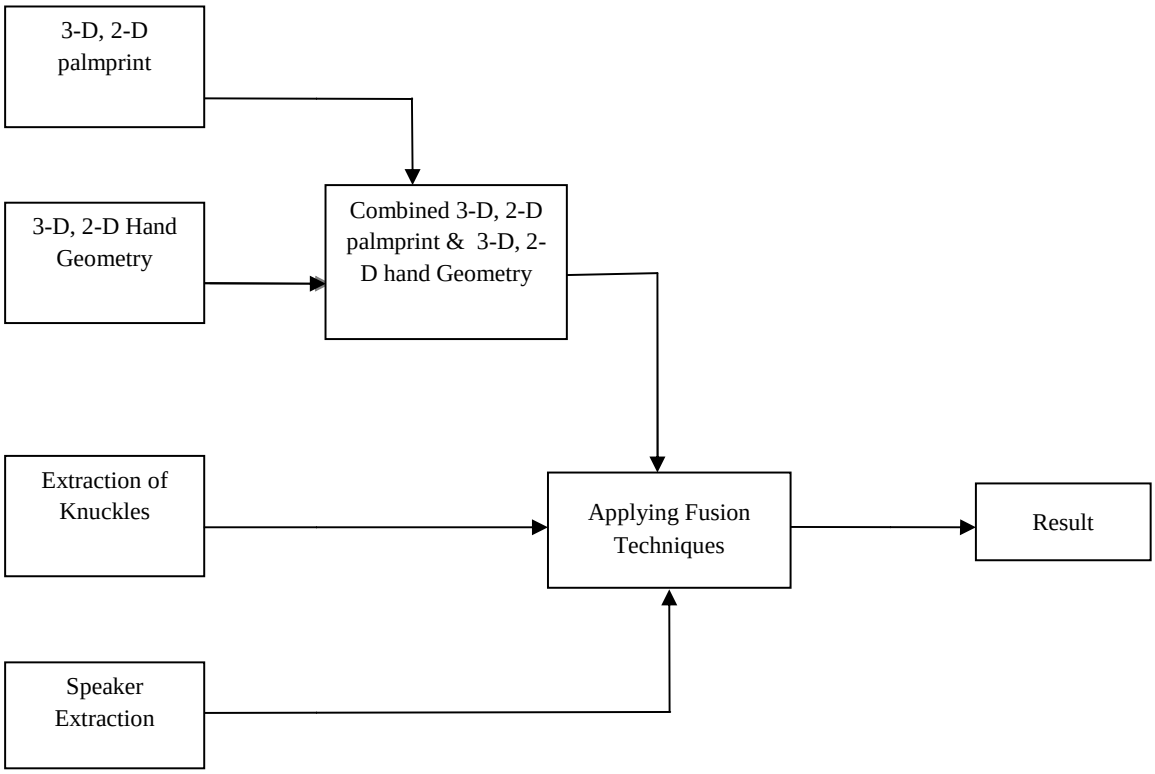

Figure 1 Fusion of modalities

IV. AN IMPROVED PRIVACY PRESERVING APPROACH FOR MULTIMODAL BIOMETRICS

a. *Secure Adaptive Filtering*

Instead of sending full raw data, we are sending the encrypted privacy preserving data by using the secure adaptive filtering techniques. In our new approach, we employ Least Mean Square (LMS) algorithm, which is one of the adaptive filtering algorithm. The characteristic of this algorithm is that it comprise only linear operations, while having an essentially nonlinear behavior due to their adaptive nature. Thus, it can be assumed that homomorphic processing can yield a quite efficient solution.

There are no complete homomorphic cryptosystems is in use. The major contribution in this scenario is Gentry's poly-time and poly-space fully homomorphic cryptosystem, whose constant factors make it impractical. Hence, using only homomorphic processing implies resorting to interactive protocols for performing multiplications between encrypted values, or for any other more complex operation. The inputs to the secure protocol must be quantized prior to encryption. So, it is necessary to work in fixed point arithmetic, keeping a scale factor that affects all the values under encryption. This factor will increase with each encrypted multiplication, limiting the number of allowed iterations of the adaptive algorithm, until the encrypted numbers cannot fit the cipher, when it is said that the cipher blows up.

There are two approaches for devising a private LMS protocol, depending on whether the output is either disclosed or given in encrypted form. The simplest approach is the one in which the output of the LMS algorithm can be disclosed to both parties; in this case, a secure protocol could be quite efficient, as the problem of the increased scale factor can be easily solved by requantizing the outputs in a clear way after every iteration without any additional overhead. It requires only homomorphic additions and multiplications and interactive

multiplication gates. Nevertheless, besides its simplicity, this scenario is of no interest due to the fact that disclosing the output gives both parties all the necessary information for retrieving the other party's private input and rendering the privacy-preserving solution unnecessary and unusable.

Algorithm 1 Homomorphic Processing (HP) PrivateLMS Protocol

Inputs: $\mathcal{A}$: $d_n, \boldsymbol{w}_0$; $\mathcal{B}$: $u_n, \boldsymbol{w}_0$
Outputs: $[\![y_n]\!]$.

$\mathcal{A}$	$\mathcal{B}$
Initialize $\texttt{carriedFactor}= 2^{n_f}$, $\texttt{updateFactor}= 2^{3n_f}$.	
Encrypt inputs and send $[\![d_n]\!]$ to $\mathcal{B}$.	
for $k = 1$ **to** N_{iter}	
	Perform the vector multiplication $[\![y_k]\!] = [\![\boldsymbol{w}_k]\!] \cdot \boldsymbol{u}_k$. Scale $[\![d'_k]\!] = [\![d_k]\!] \cdot \texttt{carriedFactor}$. Obtain $[\![e'_k]\!] = \mu \cdot ([\![d'_k]\!] - [\![y_k]\!])$. Perform the scalar multiplication $[\![\boldsymbol{\Delta w}_k]\!] = [\![e'_k]\!] \cdot \boldsymbol{u}_k$. Update the coefficients vector $[\![\boldsymbol{w}_{k+1}]\!] = [\![\boldsymbol{w}_k]\!] \cdot \texttt{updateFactor} + [\![\boldsymbol{\Delta w}_k]\!]$.
Update $\texttt{carriedFactor}=\texttt{carriedFactor} \cdot \texttt{updateFactor}$.	
	Output $[\![y_k]\!]$.
endfor	

The private output scenario is more realistic, and it is the one on which we will focus, as it corresponds to the case where the LMS block can be used as a module of a more complex system whose intermediate signals must not be disclosed to any party. Several secure solutions for privacy-preserving adaptive filtering that involve homomorphic processing, garbled circuits, and interactive protocols, in order to overcome the limitations of the three technologies, while profiting from their respective advantages. The least mean squares (LMS) algorithm is a prototypical example of a relatively simple but powerful and versatile adaptive filter.

V. EXPERIMENTAL ANALYSIS

The hand images on the palm side and dorsum side is taken by 3 D camera and the speech is recorded through microphone in a closed environment. These images are processed to extract palm print, hand geometry, knuckle and speech pattern. These features are fused together using various fusion techniques. Initially, we combine 2-D, 3-D palmprint and 2-D, 3-D hand geometry features by using dynamic fusion strategy. Then the palmprint and hand geometry features are combined with knuckle extraction and speech extraction. We have applied various fusion techniques like data level fusion, feature level fusion, sum rule, serial rule and weighted sum rule. These fusion techniques are applied on raw data at the first level. In the second level least mean square (LMS) algorithm, a simple, powerful and versatile adaptive filter is applied to the biometric features. Then the data are fused using various fusion techniques. The results obtained from the raw data and the data with LMS algorithm are analyzed. The error rate and accuracy level varies with fusion strategies in both the levels.

When we employ raw data the serial rule shows better accuracy level, and the error rate is less. But the accuracy is lesser in data level fusion, and the error rate is more. While the data is subjected to secure adaptive filtering by using LMS algorithm and fused together by applying various fusion techniques, weighted sum rule over perform others. It shows higher accuracy level and lesser error rate.

The graphs (Figure 2 and 3) show the accuracy level for raw data and the error level for raw data without LMS algorithm respectively. The figure 4 illustrate graph ,which shows the accuracy level for filtered data with LMS algorithm and figure 5 illustrates graph, which shows the error level for filtered data by using LMS algorithm.

In general biometric system can be evaluated by false negative rate, false positive rate, true positive rate and true negative rate. On analyzing the above results application of serial rule found to be more effective on raw data without using LMS algorithm, but weighted sum rule is found to be more effective on filtered data with LMS algorithm. The accuracy level is high when Least Mean Square algorithm is applied. The table is illustrated with the comparative values of fusion techniques applied to raw data and filtered data with LMS algorithm.

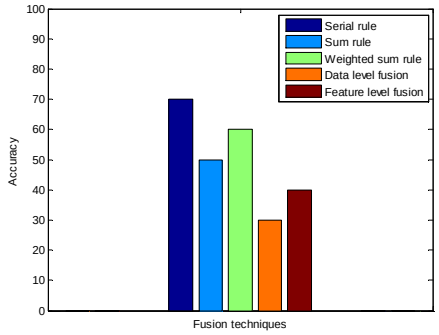

Figure 2. Accuracy level for raw data

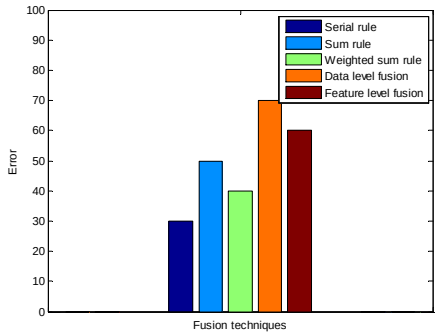

Figure 3. Error level for raw data

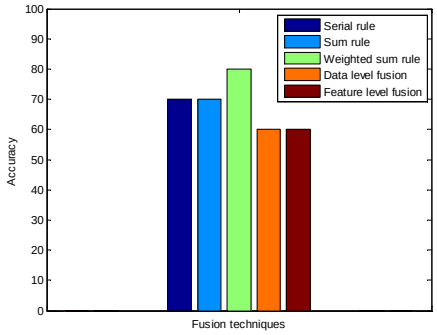

Figure 4. Accuracy level for data applied with LMS Algorithm

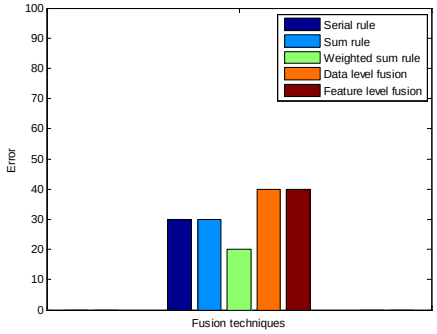

Figure 5. Error level for data applied with LMS Algorithm

Table 1: Performance Comparison of fusion techniques on raw data and data applied with LMS algorithm

FUSION TECHNIQUES	False negative rate		False positive rate		True positive rate		True negative rate	
	With LMS	Without LMS (raw data)	With LMS	Without LMS (raw data)	With LMS	Without LMS (raw data)	With LMS	Without LMS (raw data)
SERIAL RULE	1%	2%	2%	1%	3%	3%	4%	4 %
SUM RULE	2 %	1%	1%	4-5%	4 %	3%	3 %	2 %
WEIGHTED SUM RULE	1%	0%	1%	4-5%	4 %	3%	4%	3 %
DATA LEVEL FUSION	1 %	3%	3%	4-5%	2 %	1%	4%	2 %
FEATURE LEVEL FUSION	1 %	3%	3%	3-4%	3%	2%	3%	2 %

VI. CONCLUSION

We have developed a multimodal biometric system by combining palmprint, hand geometry, knuckle feature and speech. Various fusion strategies like serial rule, sum rule, weighted sum rule, data level fusion and feature level fusion are applied to these biometric traits. These fusion techniques are applied to raw data. We employed LMS algorithm, an adaptive filtering algorithm to data for securing the privacy of the data. The data are subjected to various fusion techniques. The data subjected to secure adaptive filtering by using LMS algorithm shows higher accuracy level. In future, We can combine these biometric features using other privacy preserving algorithm to enhance the security level in authentication. In future, we will extend our research with combining different biometric modalities and various other techniques to enhance the security.

REFERENCES

[1] A. Ross, A.K. Jain, "Information fusion in biometrics", Pattern Recognition Letters, vol 24, No 13, pp 2115–2125 , 2003.
[2] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, "On Combining Classifiers", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 3, pp. 226-239, 1998.
[3] 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
[4] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of Face and Speech Data for Person Identity Verification", *IEEE Trans. Neural Networks*, vol. 10, no. 5, pp. 1065-1075, 1999.

[5] L. Hong and A.K. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, 1998.
[6] A.K. Jain, A. Ross, S. Prabhakar, "An introduction to biometric recognition", IEEE Transactions on Circuits Systems Video Technology. Vol 14, pp 4–20, 2004
[7] A.K. Jain, A. Ross, "Multibiometric systems", Communications of the ACM, Vol 47, pp 34–40, 2004.
[8] L. Hong, A.K. Jain, S. Pankanti, "Can multibiometrics improve performance? in: Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies, NJ, USA, pp. 59–64, 1999.
[9] C. Sanderson, K.K. Paliwal, "Information fusion and person verification using speech and face information", Research Paper IDIAP-RR 02-33, IDIAP, September 2002.
[10] S.S. Iyengar, L. Prasad, H. Min, "Advances in Distributed Sensor Technology", Prentice-Hall, Englewood Cliffs, NJ, 1995.
[11] A. Ross, A.K. Jain, "Multimodal Biometrics: An Overview", 12th European Signal Processing Conference (EUSIPCO), Vienna, Austria, pp. 1221- 1224, 9/2004
[12] K. Woods, K. Bowyer, W.P. Kegelmeyer, "Combination of multiple classifiers using local accuracy estimates", IEEE Transactions on Pattern Analysis and. Machine Intelligence, vol 19,pp 405–410, 1997.
[13] K. Chen, L. Wang, H. Chi, "Methods of combining multiple classifiers with different features and their applications to text-independent speaker identification", International Journal on Pattern Recognition and Artificial Intelligence. Vol 11, No 3, pp 417–445, 1997.
[14] L. Lam, C.Y. Suen, "Application of majority voting to pattern recognition: an analysis of its behavior and performance", IEEE Trans. Systems Man Cybernet. vol 27, no.5, pp. 553–568, 1997.
[15] L. Xu, A. Krzyzak, C.Y. Suen, "Methods for combining multiple classifiers and their applications to handwriting recognition", IEEE Trans. Systems Man Cybernet. vol 22,no.3,pp. 418–435, 1992.
[16] T.K. Ho, J.J. Hull, S.N. Srihari, "Decision combination in multiple classifier systems", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol 16, no 1,pp. 66–75, 1994.
[17] Y. Wang, T. Tan, A.K. Jain, "Combining face and iris biometrics for identity verification", in: Proceedings of Fourth International Conference on AVBPA, Guildford, UK, pp. 805–813, 2003.
[18] P. Verlinde, G. Cholet, "Comparing decision fusion paradigms using k-NN based classifiers, decision trees and logistic regression in a multi-modal identity verification application", in: Proceedings of Second International Conference on AVBPA, Washington, DC, USA, pp. 188–193, 1999.
[19] V. Chatzis, A.G. Bors, I. Pitas, "Multimodal decision-level fusion for person authentication", IEEE Trans. Systems Man Cybernet. Part A: Systems Humans, vol 29, no.6, pp. 674–681, 1999.
[20] J.P. Baker, 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.
[21] S. Prabhakar, A.K. Jain, "Decision-level fusion in fingerprint verification", Pattern Recognition, vol 35,no. 4, pp. 861–874, 2002.
[22] E.S. Bigun, J. Bigun, B. Duc, S. Fischer, "Expert conciliation for multimodal person authentication systems using Bayesian statistics", in: Proceedings of First International Conference on AVBPA, Crans-Montana, Switzerland, pp. 291–300, 1997.
[23] R. Snelick, M. Indovina, J. Yen, A. Mink, "Multimodal biometrics: issues in design and testing", in: Proceedings of Fifth International Conference on Multimodal Interfaces, Vancouver, Canada, pp. 68–72, 2003.
[24] A.K. Jain, A. Ross, "Learning user-specific parameters in a multibiometric system", in: Proceedings of International Conference on Image Processing, New York, USA, pp. 57–60, 2002.
[25] P. Verlinde, P. Druyts, G. Cholet, M. Acheroy, "Applying Bayes based classifiers for decision fusion in a multi-modal identity verification system", in: Proceedings of International Symposium on Pattern Recognition "In Memoriam Pierre Devijver", Brussels, Belgium, 1999.