ISSN No. 0976-5697

Volume 7, No. 2, March-April 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Robust Multimodal Biometric System Integrating Iris, Face and Fingerprint using Multiple SVMs

Sheetal Chaudhary
Post Doctoral Fellow
Department of Computer Science & Applications
Kurukshetra University, Kurukshetra, INDIA

Rajender Nath
Professor
Department of Computer Science & Applications
Kurukshetra University, Kurukshetra, INDIA

Abstract: This paper presents a robust multimodal biometric recognition system integrating iris, face and fingerprint based on match score level fusion using multiple support vector machines (SVMs). Here, multiple support vector machines are applied in parallel fashion to overcome the problem of missing biometric traits. It considers every possible combination of all the three biometric traits (iris, face and fingerprint) individually. Each possible combination of biometric traits has a separate SVM to combine the available match scores to generate the final decision. Existing multimodal biometric recognition systems are based on the assumption that the set of biometric traits to be integrated is always present as a whole at the time of authentication. But sometimes it is not possible due to some unavoidable circumstances (e.g. injury may be caused, person may be under some medical treatment, corresponding trait may be missing etc.). The performance of the proposed system is evaluated on a public dataset demonstrating its recognition accuracy regarding FAR (False Accept Rate) and FRR (False Reject Rate).

Keywords: support vector machine (SVM), score level fusion, iris recognition, face recognition, fingerprint recognition, receiver operating characteristic (ROC) curve.

I. INTRODUCTION

Unimodal biometric systems have to compete with a variety of problems such as noisy data, intra-class variations, inter-class similarities or distinctiveness, non-universality, spoof attacks, interoperability issues [1]. Multimodal biometric recognition systems are estimated to be more reliable due to the presence of multiple, rather independent pieces of facts [2]. Depending upon the data presented by multiple sources of biometric information, a multibiometric system can be classified into five types of systems i.e. multiple sensor, multiple algorithm, multiple instance, multiple sample and multimodal systems as shown in figure 1.

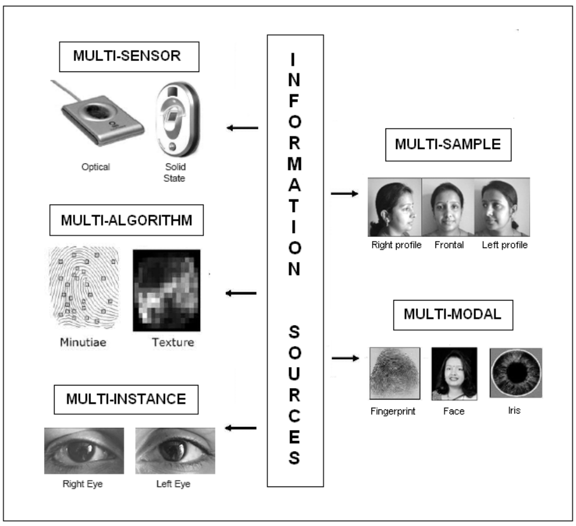

Figure 1. Multiple sources of biometric information for fusion

Multimodal biometric systems address noisy data problem by providing multiple sensors and multiple traits. Intra-class variations and inter-class similarities can be avoided with multiple samples and multiple instances of same trait. To address the problem of non-universality they provide sufficient population coverage with multiple traits. They also prevent spoof attacks since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user at the same time. They also impart fault tolerance to biometric applications so that they keep on working even when certain biometric sources become unreliable (due to sensor or software malfunction or deliberate user manipulation) [3].

A general biometric system consists of four modules - sensor module, feature extraction module, matcher module and decision module. According to Sanderson and Paliwal [4] various levels of fusion can be classified into two broad categories: fusion before matching and fusion after matching. This classification is based upon the fact that once the matcher of a biometric system is invoked, the amount of information available to the system significantly decreases. Fusion prior to matching includes fusion at the sensor level and feature extraction level. Fusion after matching includes fusion at the match score level and decision level. In general, it is believed that a fusion scheme applied as early as possible in the recognition system is more effective since the amount of information available to the system gets compressed when one proceeds from the sensor module to the decision module.

Fusion at the sensor level faces the problem of noise in raw data that gets suppressed in the further levels. Fusion at the feature level combines feature sets corresponding to multiple biometric traits. It is expected to provide better authentication results as the feature set contains richer information about the raw biometric data than the match score or the final decision. But , fusion at this level is difficult to achieve because of the following reasons: (i) the feature sets of multiple biometric traits may be incompatible (e.g. minutiae set of fingerprint and eigen-coefficients of face) (ii) the relationship between the feature spaces of different biometric systems may not be known (iii) concatenating two feature vectors may result in a feature vector with very large dimensionality leading to the curse of dimensionality problem and (iv) a more complex matcher might be required in order to operate on the concatenated feature set [5]. Thus fusion at the sensor or feature levels requires additional processing complexity. After feature sets, the match scores contain richest information about the input pattern. It is relatively easy to access and combine the match scores. Hence, fusion at the match score level is the most common approach in multimodal biometric systems [6]. Fusion at the decision level contains the least amount of information i.e. the final output by the system. It is carried out only when the decisions output by the individual biometric matchers are available since most commercial biometric systems provide access to only the final decision output by the system [7].

The rest of the paper is organized as follows. In section 2 related works are presented. Section 3 describes the architecture of the proposed system and fusion performed at the match score level. In section 4 results are discussed. Finally, the summary and conclusions are given in Section 5.

II. RELATED WORK

Fusion of multiple biometric traits for human recognition has established significant attention in last years. A lot of work has been done in the field of multimodal biometrics yielding mature hybrid biometric systems. Fusion at the match score level has been extensively studied in the literature and is the dominant level of fusion in biometric systems. Feng et al. [8] combined face and palmprint at feature level. Fusion is performed by concatenating the features extracted by using PCA and ICA with the nearest neighbor classifier and support vector machine as the classifier. Luca et al. [9] combined fingerprint and face at the match score level. They used PCA and LDA for the feature extraction and classification, Fusion was performed using techniques like mean rule, product rule and bayesian rule with FAR of 0% and FRR of 0.6% to 1.6%. Meraoumia et al. [10] presented a multimodal biometric system by integrating palmprint and finger-knuckle-print (FKP) with EER = 0.003 %. Kartik et al. [11] combined signature and speech by using sum rule at the match score level. For normalization, min max technique is applied and euclidean distance is used as the classification technique with 81.25% accuracy performance rate. Rodriguez et al. [12] combined signature and iris by using product rule and sum rule as the fusion techniques. Neural Network is used as the classification technique with EER below than 2.0%. Kisku et al. [13] proposed a multimodal biometric system integrating face and palmprint at feature level. The system attained 98.75% recognition rate with 0% FAR. Toh et al. [14] combined hand geometry, fingerprint and voice by using global and local learning decision as fusion approach with accuracy performance of 85% to 95%. Fierrez-Aguilar and Ortega-Garcia [15] proposed a multimodal system integrating face, fingerprint and online signature at the match score level with Equal Error Rate (EER) of 0.5. Viriri and Tapamo [16] proposed a multimodal biometric system integrating iris and signature at the match score level with False Reject Rate (FRR) 0.008% on a False Accept Rate (FAR) of 0.01%. Kazi and Rode [17] proposed a multimodal biometric system combining face and signature at the match score level. The results showed that this bimodal biometric system can improve the recognition accuracy rate about 10% higher than single face or signature based biometric system.

III. PROPOSED WORK

A biometric recognition system based exclusively on single biometric trait is often not able to meet the system performance requirements. Multimodal biometric systems are likely to enhance the recognition accuracy of a personal authentication system by integrating the facts presented by multiple sources of information. Although multimodal fusion techniques improves the matching performance and recognition accuracy of biometric systems but their performance degrades if any one of the biometric trait (traits offered at the time of enrollment) is unavailable or missing during authentication. Thus, a fusion strategy based on multiple support vector machines (SVM) is presented in this paper which overcomes the difficulty of missing traits encountered by existing multimodal systems.

A. Image Acquisition and Feature Set Extraction

The raw samples of three traits (iris, face and fingerprint) are acquired using appropriate sensors. The feature set extraction of these traits is carried out with appropriate feature extraction methods and is discussed below:

(i) Iris Feature Set Extraction: The iris feature set extraction consists of four basic steps - image acquisition, segmentation, normalization and feature extraction. Fig. 2 [18] shows a schematic diagram of the steps involved in the process of iris feature set extraction.

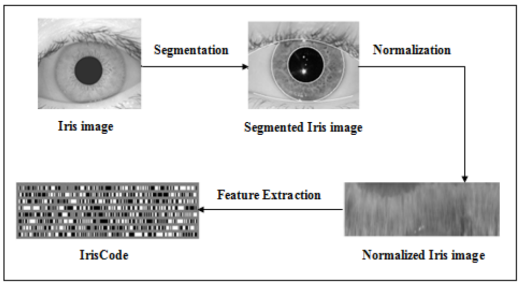

Figure 2. Steps involved in iris feature set extraction

First of all segmentation is carried out to find the precise location of the circular iris. The region of iris is surrounded by two circles. To recognize these two circles the Circular Hough transform (CHT) has been used [19]. There are several factors that severely affects iris matching results such as variation in illumination, size of the pupil and distance of the eye from camera. These factors are responsible for varying size of the iris from person to person, and even for the same person. To get accurate results, it is necessary to reduce these factors by transforming the localized iris into polar coordinates. It is accomplished by remapping each point within the iris region to a pair of polar coordinates (r, θ) where r is in the interval [0,1] with 1 corresponding to the outermost boundary and θ is the angle in the interval $[0,2\pi]$ [20, 21]. After the iris image has been located, it is encoded into a IrisCode which is the 2048-bit binary representation of the iris. For feature set extraction, gabor filter with isotropic 2D gaussian function can be used. The hamming distance between stored IrisCode record and current IrisCode record is calculated to generate the matching score. It measures the variation between the IrisCode record for the current iris image and the IrisCode records stored in the database by comparing each of the 2048 bits against each other [21, 22].

(ii) Face Feature Set Extraction: The face feature set extraction process is preceded by a face detection process during which the location and spatial extent of the face is determined within the given image. To recognize human faces, the prominent characteristics on the face like eyes, nose and mouth are extracted together with their geometry distribution and the shape of the face [23]. Human face is made up of eyes, nose, mouth and chin etc. There are differences in shape, size and structure of these organs, so the faces are differ in thousands ways, and we can describe them with the shape and structure of these organs in order to recognize them. These feature points and relative distances between them make some patterns in every input signal. These characteristic features are called eigenfaces in the facial recognition domain (or principal components). Once the boundary of the face is established and feature points are extracted, the eigenface approach [24] is used to extract features from the face as shown in figure 3[25]. In this approach a set of images that span a lower dimensional subspace is computed using the principal component analysis (PCA) technique [26]. The feature vector of a face image is the projection of the original face image on the reduced eigenspace. The matching score is generated by computing the Euclidean distance between the eigenface coefficients of the template and the detected face**.**

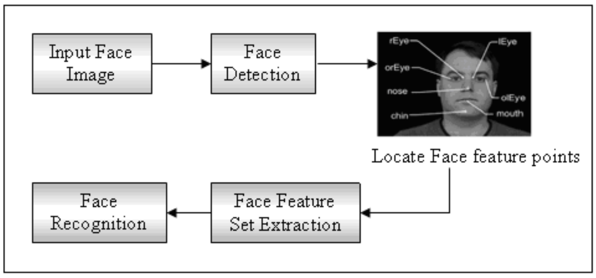

Figure 3. Steps involved in face feature set extraction

(iii) Fingerprint Feature Set Extraction: The fingerprint pattern is basically the combination of ridges and valleys on the surface of the finger. The lines that create fingerprint pattern are called ridges and the spaces between the ridges are called valleys or furrows. Once a high-quality image is captured, there are several steps required to convert its distinctive features into a compact template. This process is known as feature extraction. The major steps involved in fingerprint feature set extraction are image acquisition, image enhancement, extraction of ridges, thinning of ridges and minutiae points extraction [27] as shown in figure 4[25]. The goal of fingerprint enhancement is to increase the clarity of ridge structure so that minutiae points can be easily and correctly extracted. The enhanced fingerprint image is binarized and submitted to the thinning algorithm which reduces the ridge thickness to one pixel wide for precise location of endings and bifurcations. Minutiae localization begins with this processed image. The processed image is used to extract minutiae points which are the points of ridge endings and bifurcations. The location of minutiae points along with the orientation is extracted and stored to form a feature set. The minutiae based matching consists of finding alignment between the template and the input minutiae sets that result in the maximum number of minutiae pairings [28].

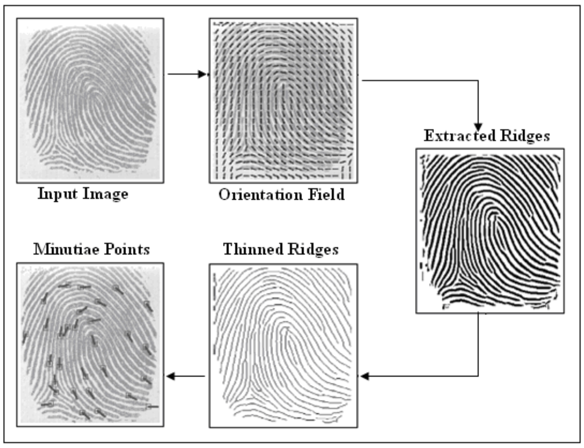

Figure 4. Steps involved in fingerprint feature set extraction

B. *Architecture of Proposed System*

Figure 5 shows the architecture of proposed multimodal biometric recognition system integrating iris, face and fingerprint at match score level. Individual recognition system of iris, face and fingerprint involves image preprocessing, feature extraction, matching and decision-making respectively. It can be seen from the architecture that initially the raw images of available biometric traits are acquired using appropriate sensors from the person to be authenticated. Further, these images are processed by corresponding feature extraction modules to generate biometric templates. These templates are then fed to the corresponding matcher modules where they are matched with templates stored in the corresponding databases taken during the enrollment phase. The match scores produced by the available individual biometrics are then passed to the fusion module. Now, fusion module will choose an appropriate SVM from multiple parallel SVMs to carry out fusion depending upon the match scores obtained from current available biometric traits. The chosen SVM will perform fusion of available matching scores to generate a fused matching score which is then passed to the decision module for final decision. Decision module utilizes the fixed threshold to declare a person as genuine or an imposter.

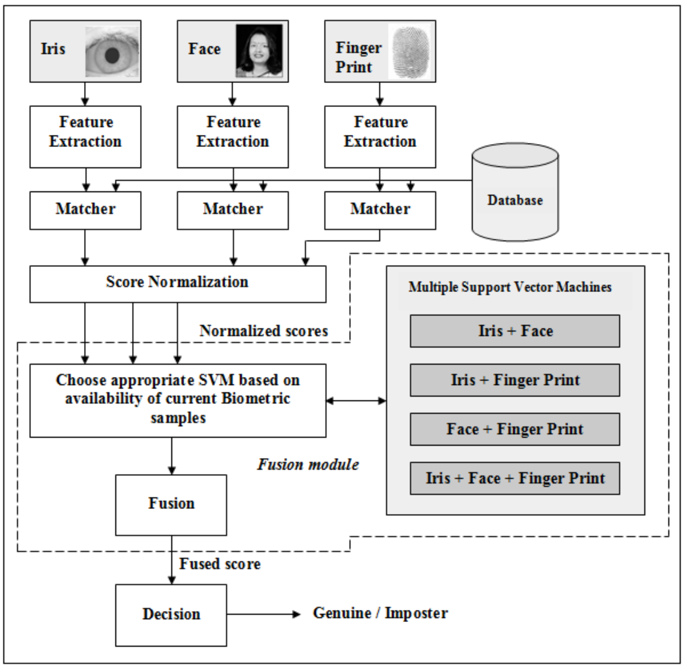

Figure 5. Architecture of proposed multimodal biometric system integrating iris face and fingerprint

(i) Score normalization: Let MS_{iris}, MS_{face} and MS_{finger} are the matching scores generated by iris, face and fingerprint biometrics respectively. The proposed fusion strategy integrates iris, face and fingerprint at match score level. The primary step involved in fusion is score normalization. The matching scores output by the three biometrics are heterogeneous because they are not on the same numerical range. So, score normalization is needed to transform these scores into a common domain prior to combining them [29]. The normalization of the three matching scores is done by min-max rule which transforms all the scores into a common range [0, 1]. The normalized scores generated by min-max equation [29] are given below:

$$N_{iris} = \frac{MS_{iris} - \min_{iris}}{\max_{iris} - \min_{iris}}$$

$$N_{face} = \frac{MS_{face} - \min_{face}}{\max_{face} - \min_{face}} \qquad (1)$$

$$N_{finger} = \frac{MS_{finger} - \min_{finger}}{\max_{finger} - \min_{finger}}$$

where [$\min_{iris}$, $\max_{iris}$], [$\min_{face}$, $\max_{face}$] and [$\min_{finger}$, $\max_{finger}$] are the minimum and maximum scores for iris, face and fingerprint biometrics respectively.

where N_{iris}, N_{face} and N_{finger} are the normalized matching scores of iris, face and fingerprint biometrics respectively.

(ii) Fusion strategy: After score normalization, multiple SVM [30] based fusion strategy is applied to overcome the limitation of missing biometric traits. Multiple SVMs are parallel and each SVM correspond to a possible combination of biometric traits being considered. This fusion strategy integrates three biometric traits i.e. iris, face and fingerprint. Thus, four combination of traits i.e. {iris, face}, {iris, fingerprint}, {face, fingerprint}, {iris, face, fingerprint} are possible. Each combination contains two or three biometric traits. Accordingly four SVMs (one for each combination of traits) are arranged in parallel fashion as shown in figure 5. Fusion module selects an appropriate SVM to carry out fusion from multiple SVMs depending upon the status of current available traits. If only one biometric trait is available then it will behave just like a unimodal biometric system and no fusion can be performed.

The matching scores generated by the matchers of current available biometric traits are combined to generate the final matching score. It is produced by the chosen SVM for final decision by performing fusion of the current available traits. If the final matching score is greater than the decision threshold, the person to be authenticated is accepted as a genuine person. And, if it is less than the decision threshold, the person to be authenticated is rejected as an imposter.

IV. RESULTS AND DISCUSSION

This paper proposes a robust multimodal biometric recognition system integrating iris, face and fingerprint. Fusion of three biometric traits is carried out at the matching score level. Here, multiple parallel SVM based fusion strategy is employed to generate the final decision. MATLAB is used to evaluate the effectiveness of proposed fusion strategy. The sample biometric data for iris was taken from CASIA database [31] and for face, fingerprint was taken from NIST website [32] respectively.

The proposed fusion strategy uses multiple parallel SVMs to address the limitation of existing multimodal fusion techniques. These techniques are based on the assumption that all the biometric traits being considered in the system are always available and user provides biometric data for every trait at the time of authentication. These techniques are also not flexible enough to add new biometric trait to the system. It will require data to be gathered for this trait from all the persons already registered in the system and thus modifying the entire fusion architecture. In contrast, multiple SVMs based score level fusion provides flexibility for new trait to be added to the system without affecting the persons already enrolled in the system and without affecting the existing SVMs. An additional SVM can be added to the fusion module to consider the new combination of traits.

The performance of a biometric system is represented by the ROC (Receiver Operating Characteristic) curve which plots the probability of FAR (False Accept Rate) versus probability of FRR (False Reject Rate) for different values of the decision threshold [2]. FAR is the percentage of imposter pairs whose matching score is grater than or equal to threshold and FRR is the percentage of genuine pairs whose matching score is less than threshold. The ROC curve plot is a visual characterization of the trade-off between the FAR and the FRR. The point on the ROC curve where FAR = FRR is known as the EER (Equal Error Rate) point. The value at this point indicates that the proportion of false acceptances is equal to the proportion of false rejections. The lower the equal error rate value, the higher the accuracy of the biometric system. Figure 6 shows the ROC curves for the proposed multimodal system. It represents one ROC curve corresponding to the fusion of iris, face and fingerprint with EER 0.19% and another three ROC curves corresponding to the cases when iris, fingerprint and face are missed with EERs 1.1%, 0.43% and 0.54% respectively. Even though the performance shown by ROC curves corresponding to the missing biometric trait cases is slight worse than the case when all the three traits are available but multiple SVM based fusion strategy effectively overcomes the limitation of missing traits. Hence, it is clear that SVM fusion based multimodal system is more realistic than existing multimodal systems which require that person to be authenticated must provide every biometric trait.

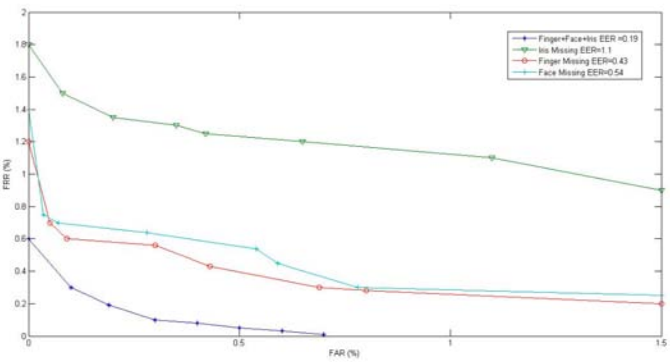

Figure 6. ROC curves for proposed system

Table I. Accuracy of all SVMs

Traits		Accuracy
A	SVM for { Iris, Face, Finger}	99.8%
B	SVM for { Iris, Face}	99.43%
C	SVM for { Iris, Finger}	99.02%
D	SVM for { Face, Finger}	97.653%

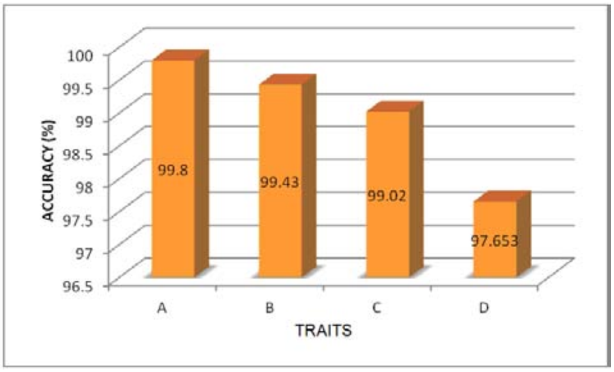

Figure 7. Bar chart showing accuracy of each SVM

Table 1 describes the average accuracy of every SVM employed in proposed system. It is clear from the table that SVM for {Face, Finger} has the lowest accuracy because face and fingerprint both has less reliability than iris. And SVMs that include iris biometric appear extremely accurate. Accuracy of every SVM is also represented with the help of bar chart in fig. 7 showing that the use of multiple SVMs does not affect the accuracy of multimodal fusion. Multimodal fusion achieves better accuracy and increased reliability of human authentication than unimodal systems. Thus, multimodal biometrics is an effective way to improve accuracy of human authentication. Proposed multiple SVM based technique appears to be robust and also retains high accuracy against missing biometric traits.

V. CONCLUSION

In this paper, a robust multimodal biometric recognition system is proposed which addresses the problem of missing biometric traits. It integrates three biometric traits (iris, face and fingerprint) at match score level. Here, a fusion strategy based on multiple parallel support vector machines (SVMs) is applied. It considers all possible combinations of available biometric traits. An appropriate SVM is chosen from multiple SVMs according to the current available biometric traits to perform fusion. In contrast, the existing multimodal fusion techniques are based on the assumption that all the biometric traits involved in fusion are made available at the time of authentication. If a biometric trait is unavailable or missed, the accuracy of multimodal systems degrades. Thus, the proposed fusion strategy effectively overcomes the missing trait drawback of existing systems by employing multiple SVMs. Experimental results show that the proposed fusion strategy is more robust, fault tolerant, flexible and provide better population coverage particularly when some of the biometric traits are unavailable. Future work will be focused on integrating liveness detection with multimodal biometric systems since it will provide a better solution for increased security requirements.

VI. REFERENCES

[1] Arun Ross and Anil K. Jain, "Multimodal biometrics: An overview", appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004.

[2] A.K. Jain, A. Ross, S. Prabhakar, "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol.14, 2004, 4-20.

[3] Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, VOL. 1, NO. 2, JUNE 2006

[4] C. Sanderson and K. K. Paliwal, Information Fusion and Person Verification Using Speech and Face, Information. Research Paper IDIAP-RR 02-33, IDIAP, September 2002.

[5] A. Ross and R. Govindarajan, "Feature Level Fusion Using Hand and Face Biometrics", In Proceedings of SPIE Conference on Biometric Technology for Human Identification II, volume 5779, pages 196–204, Orlando, USA, March 2005.

[6] A.K. Jain, A. Ross, Multibiometric systems, Communications of the ACM, Special Issue on Multimodal Interfaces, Vol. 47, January 2004, 34-40.

[7] L. Hong, A. Jain & S. Pankanti, "Can Multibiometrics Improve performance", Proceedings of AutoID 99, pp. 59-64, 1999.

[8] G. Feng, K. Dong, D. Hu and D. Zhang, "When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy," in Biometric Authentication. vol. 307, 2004.

[9] Gian Luca Marcialis and Fabio Roli, "Serial Fusion of Fingerprint and Face Matchers", M. Haindl, MCS 2007, LNCS volume 4472, pp. 151-160, © Springer-Verlag Berlin Heidelberg 2007.

[10] A. Meraoumia, S. Chitroub and A. Bouridane, "Fusion of Finger-Knuckle-Print and Palmprint for an Efficient Multi-biometric System of Person Recognition", IEEE ICC 2011.

[11] Kartik.P, S.R. Mahadeva Prasanna and Vara.R.P, "Multimodal biometric person authentication system using speech and signature features," in TENCON 2008 - 2008 IEEE Region 10 Conference, pp. 1-6, Ed, 2008.

[12] Rodriguez.L.P, Crespo.A.G, Lara.M and Mezcua.M.R, "Study of Different Fusion Techniques for Multimodal Biometric Authentication," in Networking and Communications. IEEE International Conference on Wireless and Mobile Computing, 2008.

[13] D. Kisku, P. Gupta and J. Sing, "Multibiometrics Feature Level Fusion by Graph Clustering", International Journal of Security and Its Applications Vol. 5 No. 2, April, 2011.

[14] Toh.K.A, J. Xudong and Y. Wei-Yun, "Exploiting global and local decisions for multimodal biometrics verification," Signal Processing, IEEE Transactions on Signal Processing, vol. 52, pp. 3059-3072, 2004.

[15] J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez Rodriguez, " A comparative evaluation of fusion strategies for multimodal biometric verification," in Proc. 4th Int, Conf,Audio-video-based Biometric Person Authentication , J. Kittler and M. Nixon, Eds., vol. LNCS 2688, pp. 830–837, 2003.

[16] S. Viriri and R. Tapamo, "Integrating Iris and Signature Traits for Personal Authentication using User-Specific Weighting", 2009.

[17] M. Kazi and Y. Rode, "multimodal biometric system using face and signature: a score level fusion approach" ,Advances in Computational Research, Vol. 4, No. 1, 2012.

[18] S. Chaudhary, R. Nath, "A New Template Protection Approach for Iris Recognition", In Proceedings of 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), IEEE Xplore, pp. 1-6, September 2015.

[19] R. Wildes, J. Asmuth, G. Green, S. Hsu, and S. Mcbride. "A System for Automated Iris Recognition", Proceedings IEEE

Workshop on Applications of Computer Vision, Sarasota, FL, USA, 1994.

[20] K. Dmitry, “Iris Recognition: Unwrapping the Iris”, The Connexions Project and Licensed Under the Creative Commons Attribution License, Version 1.3. (2004).

[21] R. Schalkoff., “Pattern Recognition: Statistical, Structural and Neural Approaches”, John Wiley and Sons Inc., pp. 55-63 (2003).

[22] J. Daugman. “Statistical Richness of Visual Phase Information: Update on Recognizing, Persons by Iris Patterns”. International Journal of Computer Vision, 45(1): 25-38, 2001.

[23] Dirk Colbry, George Stockman, and Anil Jain, Detection of Anchor Points for 3D Face Verification.

[24] M. Turk and A. Pentland, “Eigenfaces for recognition,” Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, Mar. 1991.

[25] S. Chaudhary, R. Nath, “A Multimodal Biometric Recognition system Based on Fusion of Palmprint, Fingerprint and Face” In Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing, IEEE Xplore, pp. 596-600, October 2009.

[26] Lu, X.; Wang, Y. & Jain, A.K. (2003), Combining Classifiers for Face Recognition, In IEEE Conference on Multimedia & Expo, Vol. 3, pp. 13-16.

[27] L. Hong, Y. Wan, and A. K. Jain, “Fingerprint image enhancement: Algorithm and performance evaluation,” IEEE Trans. Patt. Anal. Machine Intell., vol. 20, pp. 777-789, Aug. 1998.

[28] A.K. Jain, S. Prabhakar, and L. Hong, A multichannel approach to fingerprint classification, PAMI, 21 (4):348–359, 1999.

[29] A. K, & A. Ro. Jain, K. Nandakumar , Score Normalization in multimodal biometric systems. The Journal of Pattern Recognition Society, 38(12), 2005, 2270-2285.

[30] B. Schölkopf, A.J. Smola. Learning with Kernels. MIT Press, Cambridge, MA, 2002.

[31] Chinese Academy of Sciences, Center of Biometrics and Security Research, Database of Eye Images. http://www.cbsr.ia.ac.cn/IrisDatabase.htm

[32] National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

