Enhancing the Performance of Identification System Based on Score Level Fusion

Subhash V.Thul[#1], Anurag Rishishwar[#2], Bhagwat Kakde[#3]
[#1]PG Scholar, [#2]Asst. Professor, [#3]Asst. Professor
Department of Electronics & Communication
RKDF Institute of Science & Technology, Bhopal-462047, Madhya Pradesh, INDIA
[1]subuthul@gmail.com
[2]anurag.rishishwar@gmail.com
[3]bhagwatkakde@yahoo.co.in

***Abstract*— Biometric recognition, or simply biometrics, refers to the use of distinctive anatomical and behavioural characteristics or identifiers (e.g., fingerprints, face, iris, voice, hand geometry) for automatically recognizing a person. In unimodal biometric systems the recognition accuracy has to contend with a variety of problems such as background noise, noisy data, non-universality, spoof attacks, intra-class variations, inter-class similarities or distinctiveness, interoperability issues. In this paper a multimodal biometric system that integrates multiple traits of an individual for recognition has been described, which is able to alleviate the problems faced by unimodal biometric system while improving recognition performance. A multimodal biometric system can be developed by combining iris and face at match score level using simple sum rule. The match scores are normalized by min-max normalization. The identification and verification by this system is much more reliable and precise than the individual biometric systems.**

***Keywords*— Multimodal Biometric System, Iris recognition, Fingerprint recognition, Score level fusion, Sum rule**

I. INTRODUCTION

A generic biometric system consists of four modules namely sensor module, feature extraction module, matcher module and decision module In a multimodal biometric system, fusion can be performed depending upon the type of information available in any of these modules. According to Sanderson and Paliwal [1] various levels of fusion can be classified into two broad categories: fusion before matching and fusion after matching as shown in Fig.1. Fusion prior to matching includes fusion at the sensor and feature extraction levels and fusion after matching includes fusion at the match score and decision levels. It is generally believed that a fusion scheme applied as early as possible in the recognition system is more effective. The amount of information available to the system gets compressed as one proceeds from the sensor module to the decision module [2].

Fusion at the sensor level faces the problem of noise in raw data which gets suppressed in the further levels. Fusion at the feature level involves the consolidation of feature sets corresponding to multiple biometric traits. Since the feature set contains richer information about the raw biometric data than the match score or the final decision, so integration at this level is expected to provide better authentication results. However, it is difficult to achieve integration at the feature

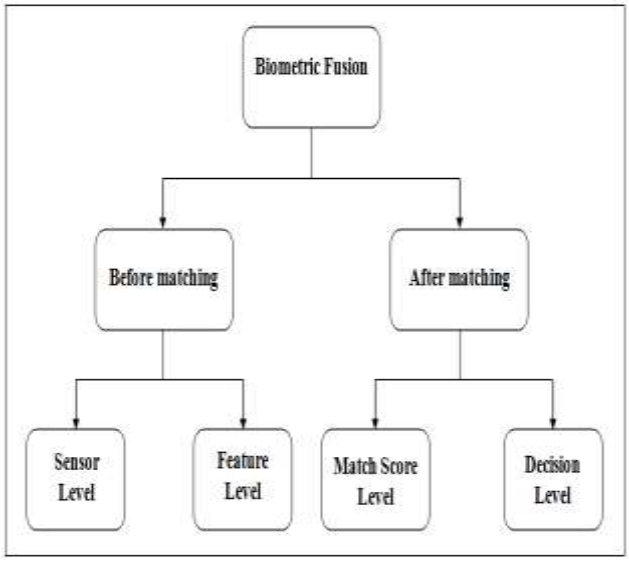

Fig. 1 Classification of levels of fusion

level because the relationship between the feature sets of different biometric systems may not be known, the feature representations may not be compatible, concatenating two feature vectors may result in a feature vector with very large dimensionality and a significantly more complex matcher might be required in order to operate on the concatenated feature set [3]. Next to the feature sets, the match scores output by the different matchers contain the richest information about the input pattern and also it is relatively easy to access and combine the scores. Therefore, fusion at the match score level is the most common approach in multimodal biometric systems. Fusion at the decision level contains the least 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 [4]. Integrating multiple traits can significantly improve the recognition performance of a biometric system besides improving population coverage, deterring spoof attacks, and reducing the failure-to-enroll rate.

Although the storage requirements, processing time and the computational demands of a multimodal biometric system are much higher than a unimodal system, the above mentioned advantages present a compelling case for deploying multimodal systems in large-scale authentication systems. The organization of the paper is as follows:

Section II discusses the related work. Section III describes the architecture of the proposed system integrating iris and fingerprint at the match score level. Results and discussion are given in section IV. Finally, the summary and conclusions are given in the last section V.

II. RELATED WORK

A lot of work has been done in the last years 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. A variety of articles can be found, which propose different approaches for unimodal and multimodal biometric systems. Multimodal biometric systems are based on different biometric features and/or introduce different fusion algorithms for these features. Many researchers have demonstrated that the fusion process is effective, because fused scores provide much better discrimination than individual scores. Such results have been achieved using a variety of fusion techniques. Toh et al. [5] combined hand geometry, fingerprint and voice by using global and local learning decision as fusion approach. The accuracy performance is 85% to 95%. Viriri and Tapamo [6] introduced a multimodal approach including iris and signature biometrics at score level fusion with False Reject Rate (FRR) 0.008% on a False Accept Rate (FAR) of 0.01%. Fierrez-Aguilar and Ortega-Garcia [7] proposed a multimodal approach including face, a minutiae-based fingerprint and online signature with fusion at the matching score level. The fusion approach obtained Equal Error Rate (EER) of 0.5. Luca et al. [8] used fingerprint and face to be fused at the match score level. PCA and LDA are used for the feature extraction and classification. Mean rule, product rule and Bayesian rule are used as the fusion techniques with FAR of 0% and FRR of 0.6% to 1.6%. Meraoumia et al. [9] presented a multimodal biometric system using hand images and by integrating two different biometric traits palmprint and finger-knuckle-print (FKP) with EER = 0.003 %. Rodriguez et al. [10] used signature with iris by using sum rule and product rule as the fusion techniques. Neural Network is used as the classification technique with EER below than 2.0%. Kartik et al. [11] combined speech and signature by using sum rule as fusion technique after the min max normalization is applied. Euclidean distance is used as the classification technique with 81.25% accuracy performance rate. Aggithaya et al. [12] proposed a personal authentication system that simultaneously exploits 2D and 3D Palmprint features. The sum rule classifier achieves the best EER of 0.002. Feng et al. [13] combined face and palmprint at feature level by concatenating the features extracted by using PCA and ICA with the nearest neighbor classifier and support vector machine as the classifier. Kisku et al. [14] proposed a multibiometric system including face and Palm print biometrics at feature level fusion. The system attained 98.75% recognition rate with 0% FAR. Kazi and Rody [15] presented a multimodal biometric system using face and signature with score level fusion. The results showed that face and signature based bimodal biometric system can improve the accuracy rate about 10%, higher than single face/signature based biometric system.

III. PROPOSED MULTIMODAL SYSTEM

It is evident that a single biometric trait is not enough to meet the variety of requirements including matching performance and recognition accuracy imposed by several large-scale authentication systems. Multimodal biometric recognition systems appear more reliable due to the presence of multiple, independent pieces of data. They seek to alleviate the shortcomings encountered by unimodal biometric systems by integrating the data presented by multiple biometric traits. In this paper, we develop a fused iris-fingerprint recognition system which overcomes a number of inherent difficulties of the individual biometrics. The integrated system also provide anti spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously.

A. Image Acquisition and Feature Extraction:

The images of two traits (iris and fingerprint) are acquired using appropriate sensors. The feature extraction of these traits carried out with suitable methods is discussed below:

1) Iris Feature Set Extraction:

A general iris recognition system is composed of five basic steps: image acquisition, segmentation, normalization, feature extraction and matching. Fig. 2 shows a schematic diagram of these basic steps in the process of iris feature set extraction.

Segmentation is a process of finding the precise location of the circular iris. The iris region is bounded by two circles. To detect these two circles the Circular Hough transform (CHT) has been used [16]. The size of the iris varies from person to person, and even for the same person, due to variation in illumination, pupil size and distance of the eye from the camera. These factors can severely affect iris matching results. In order to get accurate results, the localized iris is transformed into polar coordinates 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 $[0,2\pi]$ [17, 18]. Once the iris image has been located, the iris image is encoded into a phase code or Iris Code that is the 2048-bit binary representation of an iris. Gabor filter with isotropic 2D Gaussian function can be used for rotation invariant classification for feature extraction. The matching score is generated by computing the hamming distance between stored Iris Code records with current image. It is a measure of the

variation between the Iris Code record for the current iris and the Iris Code records stored in the database.

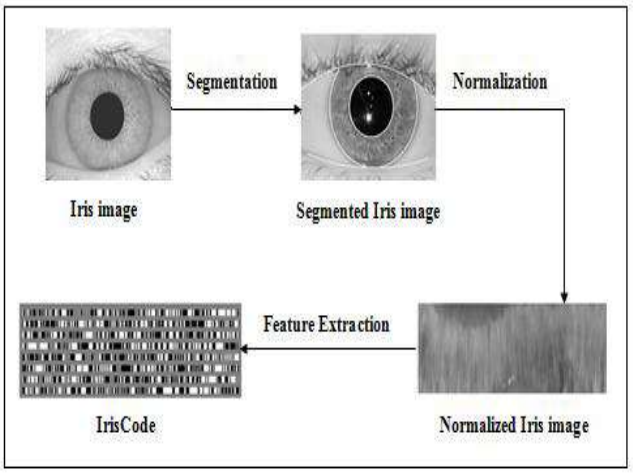

Fig. 2 Steps involved in iris feature set extraction

2. Acquisition of Fingerprints:

The acquisition of a fingerprint can be done off-line or on-line. In the off-line acquisition the image is typically obtained by smearing ink on the fingertip and creating an inked impression of the fingertip on the paper. After this procedure, the fingerprint is digitized by an optical scanner or a high resolution camera. This kind of fingerprint is often called rolled fingerprint. A very important kind of off-line fingerprint image is the latent fingerprint: a partial fingerprint image lifted from a crime scene by a forensic expert. Compared to a rolled fingerprint, the latent is most of the times of bad quality and hard to process. In the on-line acquisition, the fingerprint is acquired by using a fingerprint scanner without any kind of ink. A typical fingerprint scanner comprises:

1) A sensor to read the ridge pattern on the finger surface;
2) An A/D (Analog to Digital) converter to convert the signal;
3) An interface module responsible for communicating with external devices. Almost of all existing sensors belong to one of the following families: optical, solid state and ultrasound. These sensors are also called touch sensors. With the aim of reducing the cost, recently another sensing method has been proposed: the sweep sensor, where the finger is swept over the sensor. This is very common in mobile devices. The main parameters characterizing the acquisition of a digital fingerprint image. Here we will consider three of them: resolution, area and number of pixels.
   i. Resolution: It denotes the number of pixels per inch (dpi). 500dpi is the minimum resolution for scanners.
   ii. Area: is the size of the rectangular area sensed by a fingerprint scanner and expressed in inch^2.
   iii. Number of pixels: It is the number of pixels in a fingerprint image. If Res is the resolution, h is the height of the sensing area and w the weight of the sensing area, the number of pixels is given by (Res * h) x (Res * w).

One of the methods towards verifying a fingerprint is to find out the minutiae in the image of a fingerprint. The two features of a minutia are ridge endings and bifurcation points. A ridge ending is the point where a ridge ends, and a bifurcation point is where two ridges meet and continue as a single ridge.

1) Pre-processing: The pre-processing of the image involves taking the image and applying various processes on the image so that it can easily be processed to find out the ridge endings and bifurcation points. The two major steps in the pre-processing are:

- *Binarizing:* In this step the colours of the image are binarized so that the output image consists of only two colours, black and white.
- *Thinning:* After the fingerprint image is converted to binary form, submitted to the thinning algorithm which reduces the ridge thickness to one pixel wide.

2) Minutiae extraction: The most commonly employed method of minutiae extraction is the Crossing number (CN) concept. This method involves the use of the skeleton image where the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighbourhood of each ridge pixel in the image using a 3*3 window. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighbourhood. Using the properties of the CN as, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point.

3) Post processing: After above process too many minutiae have been detected on the edge of the image. This is because those points passed the processing test of being ridge ends, but actually they are not ridge ends but only the points beyond which the image was not scanned. So now these false minutiae have to be filtered out and removed. Any pair of ridge or bifurcation points is removed if it is found that the distance between the two is smaller than a certain number of pixels.

4) ROI extraction: (ROI) is the area of an image, which is importance for extraction of minutiae points. At first, the fingerprint image is divided into non-overlapping blocks. Then, the gradient of each block is computed. The standard deviation (SD) of gradients in X and Y direction are calculated and summed. The block is filled with ones only if the resultant value exceeds the threshold value, else the block is filled it with zeros.
This region is simply a mask that is applied on the above image that removes the focus on the edge minutiae.

5) Matching: The algorithm that applied to match two

fingerprints involves calculating Euclidian distance between each ridge and all other ridge ends and similarly between all bifurcations and then taking the average for both and at last adds the results for achieving high accuracy and precision level.

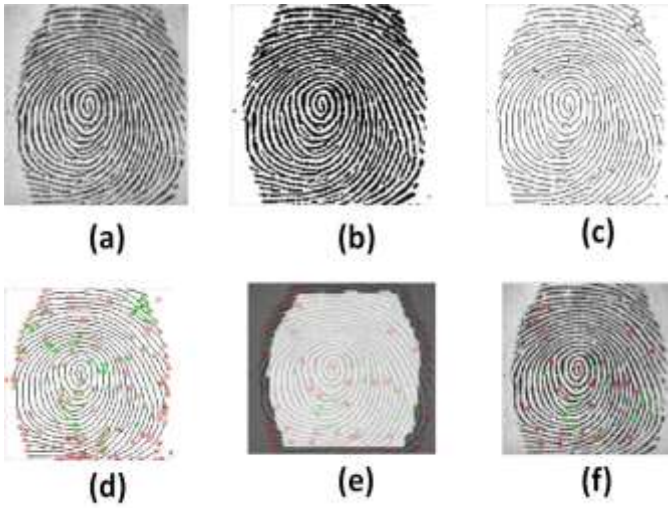

Fig. 3: (a) Input image, (b) Binarized image, (c) Thinned image, (d) Ridge end+Bifurcation, (e) Common region of ROC and Image, (f) Final Minutiae.

B. Architecture of Proposed System

The structural design of proposed multimodal biometric recognition system integrating iris and fingerprint is shown in Fig.5. In the operational phase, the two biometric sensors capture the images individually from the person to be identified and converts them to a raw digital format, which is further processed by the feature extraction modules individually to produce a compact representation that is of the same format as the templates stored in the corresponding databases taken during the enrolment phase. The two resulting representations are then fed to the two corresponding matchers. Here, they are matched with templates in the corresponding databases to find the similarity between the two feature sets. The match scores generated from the individual biometrics are then passed to the fusion module to perform fusion at match score level using simple sum rule.

1) Fusion: The first step involved in fusion is score normalization. Since the match scores output by the two biometric traits (iris and fingerprints) are heterogeneous because they are not on the same numerical range, so score normalization is done to transform these scores into a common domain prior to combining them. Here, min-max normalization is used to transform all these scores into a common range [0, 1]. The two normalized scores are fused using sum rule to generate final match score. Finally, fused matching score is passed to the decision module where a person is declared as genuine or an imposter. The normalized scores are obtained by following min-max equation [18]:

$$S_i' = \frac{S_i - S_{min}}{S_{max} - S_{min}}$$

Where S_i' is the normalized matching score, S_i is the matching score, S_{min} is the minimum match score and S_{max} is the maximum match score for i^{th} biometric trait. In order to combine the match scores output by the two individual matchers (iris and fingerprint), simple sum rule is used and its equation is given below [18]:

$$Sum = \sum_{i-1}^{n} S_i$$

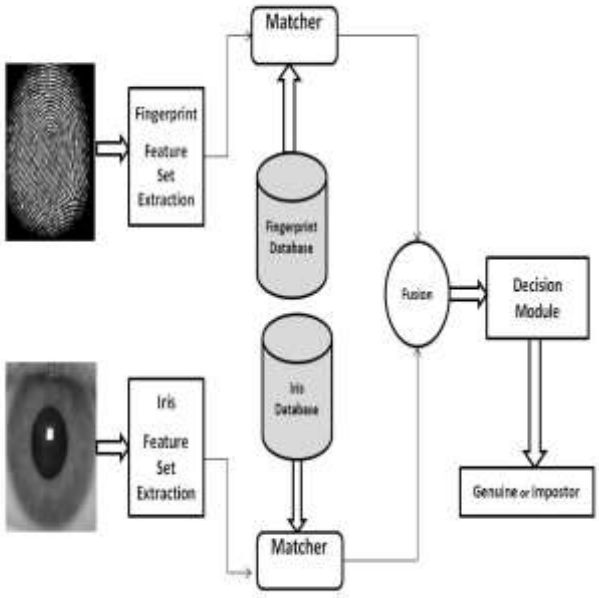

Fig.5: Architecture of proposed multimodal biometric recognition system integrating fingerprint and iris

IV. EXPERIMENTAL RESULTS

False Accept Rate (FAR) and False Reject Rate (FRR) are two widely used standard metrics to determine the accuracy of a biometric system.

1. The FAR is the percentage of imposters that are incorrectly granted access

$$FAR = \frac{False\ Matches}{No.\ of\ Impostors\ Attempt}$$

2. FRR is the percentage of valid users who are incorrectly denied access

$$FRR = \frac{False\ Rejection}{No.\ of\ Genuine\ User\ Attempt}$$

The results are tested on iris and fingerprint images. For the purpose allowing comparisons two levels of experiments are performed. At first level iris and fingerprints algorithms are tested individually. At this level the individual results are computed and an accuracy shown in table 1. It is found to be 94.36% and 92.06% respectively. However in order to increase the accuracy of the biometric system as a whole the individual results are combined at matching score level. At second level of experiment the matching scores from the individual traits are combined and final accuracy shown in Table 2.

Table 1: Figures showing individual accuracy

Trait	Algorithm	Accuracy	FAR	FRR
Iris	Gabor Filter	94.34	4.82	6.21
Fingerprint	Minutiae	92.08	3.15	4.73

Table 2: Figures showing fusion accuracy

Trade	Fusion	Accuracy	FAR	FRR
Without normalization	Sum rule	97.6	2.19	4.35
With normalization	Sum rule	98.67	1.23	2.65

V. CONCLUSION

Biometric features are unique to each individual and remain unaltered during a person's lifetime. These features make biometrics a promising solution to the society. Unimodal biometric systems fail in case of lack of proper biometric data for a particular trait. In that case the system rejects genuine identity of person. This results in increasing false rejection rate. So an efficient algorithm is required to avoid this drawback. Fingerprint and iris are two strong biometrics which gives good performance than any other biometric. To process fingerprint and iris we apply an efficient algorithm and matching scores are calculated for individual biometric trait. Then fusion of matching scores is used because matching scores contain sufficient information to make genuine and impostor case distinguishable and they are relatively easy to obtain.

REFERENCES

[1] 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.
[2] A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics, New York: Springer, 2006.
[3] 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.
[4] A.K. Jain, A. Ross, Multibiometric systems, Communications of the ACM, Special Issue on Multimodal Interfaces, Vol. 47, January 2004, 34-40.
[5] 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.
[6] S. Viriri and R. Tapamo, "Integrating Iris and Signature Traits for Personal Authentication using User-Specific Weighting", 2009.
[7] 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.
[8] 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
[9] 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.
[10] 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
[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] V. Aggithaya, D. Zhang and N. Luo "A Multimodal biometric authentication system based on 2D and 3D palmprint features", Proc. of SPIE Vol. 6944 69440C-1- 2012.
[13] 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.
[14] 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
[15] 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.
[16] 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.
[17] K. Dmitry, "Iris Recognition: Unwrapping the Iris", The Connexions Project and Licensed Under the Creative Commons Attribution License, Version 1.3. (2004).

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

[19] Bhupesh Gour, T. K. Bandopadhyaya and Sudhir Sharma, *"Fingerprint Feature Extraction usingMidpoint Ridge Contour Method and Neural Network*", International Journal of Computer Science and Network Security, vol. 8, no, 7, pp. 99-109, (2008).

[20] G. Aguilar, G. Sanchez, K. Toscano, M. Nakano, and H. Perez, Mul-timodal biometric system using fingerprint,‖ in Proc. Int. Conf. Intell. Adv. Syst. 2007, pp. 145–150. DOI: 10.1109/ICIAS.2007.4658364

[21] F. Besbes, H. Trichili, and B. Solaiman, "Multimodal biometric system based on fingerprint identification and Iris recognition," in *Proc. 3rd Int.IEEE Conf. Inf. Commun. Technol.: From Theory to Applications (ICTTA2008)*, pp. 1–5. DOI: 10.1109/ICTTA. 2008. 4530129.

[22] Prince,Manvjeet K., "Fingerprint matching system using level 3 feature",*Intrrnational journal of engg science and tech* Vol.2(6),2010,2258- 2262.

[23] R. Snelick, U. Uludag, A. Mink, M. Indovina, A. Jain, Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems, IEEE Trans- actions on Pattern Analysis and Machine Intelligence 27 (3) (2005) 450–455.

[24] M. Vatsa, R. Singh, and A. Noore, "Improving iris recognition performance using segmentation, quality enhancement, match score fusion, and indexing," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 38, no. 4, pp. 1021–1035, Aug. 2008.

[25] A. Nagar, S. Rane, and A. Vetro, "Privacy and security of features extracted from minutiae aggregates," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, Dallas, TX, Mar. 2010, pp. 524–531.

