International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072

Sum Rule Based Matching Score Level Fusion of Fingerprint and Iris Images for Multimodal Biometrics Identification

Subhash V.Thul[1], Anurag Rishishwar[2], Neetesh Raghuwanshi[3]

[1]PG Scholar, ECE Department, RKDF Institute of Science & Technology Bhopal, Madhya Pradesh, INDIA
[2,3]Asst. Professor, ECE Department, RKDF Institute of Science & Technology Bhopal, Madhya Pradesh, INDIA

Abstract – *Basic aim of a biometric system is automatically discriminate between subjects as well as protects data. It also protects resources access from unauthorized users. In biometric system physical or behavioral traits are used for recognition purpose. A multimodal biometric identification system we fuse two or more physical or behavioral traits. Multimodal biometric system improves the accuracy. In a multimodal biometric system each biometric trait processes its information independently then the processed information is combined using appropriate fusion scheme. The comparison of data base template and the input data is done with the help of Euclidean-distance matching algorithm. If the templates are match we can allow the person to access the system.*

Key Words: **Biometric, Fusion, Fingerprint Recognition, Iris Recognition, Multimodal**

1. INTRODUCTION

An automated method which recognizes a person based on his/her physiological or behavioral characteristic is called biometrics. A biometric system could be either a verification system or an identification system depending on the application. A verification system compares the acquired trait with the template of the claimed identity pre-stored in the system. The verification system will either accept or reject the claimed identity. A verification system performs one-to one matching. In contrast, an identification system identifies an individual by searching potentially, the entire template database for a match. This kind of a system performs a one-to-many matching. The identification system can either establish the person's identity with some level of accuracy or fail if the individual does not exist in the enrolled database. Biometric technologies include dynamic signature verification, iris scanning, face recognition, DNA recognition, voice recognition and fingerprint identification. Biometric identification is superior to lower technology identification methods in common use today - namely passwords, PIN numbers, key-cards and smart cards. PINs (personal identification numbers) were one of the first identifiers to offer automated recognition. However, this means recognition of the PIN, implies recognition of the PIN but not the person to whom they belong. Similar analogy can be extended to cards and other tokens. The token recognition is easy but is not 100% fake-proofs. It carries a threat of being stolen and recreated. The primary use of physical objects or behaviors based on memory has a clear set of problems and limitations. Objects are often lost or stolen and a behavior based on memory is easily forgotten. Identity cannot be guaranteed, privacy is not assumed and inappropriate use cannot be proven or denied. These limitations decrease trust and increase the possibility of fraud. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions.

Biometric-based techniques are able to provide for confidential financial transactions and personal data privacy. A biometric cannot be easily transferred between individuals. The scalability for integrating biometrics into a variety of processes can be extended if the verification procedures are made more user-friendly. The most basic definition of biometrics is that it is a pattern recognition system, which establishes and validates an individual's identity based on a specific and unique biological characteristic. Biometric-based authentication applications include workplace, network, and entry access, single sign-on, application logon, data safeguarding, remote access to resources, transaction security and Web security. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than conventional methods (e.g. usage of Passwords or Personal Identification number). The reason being using biometric nullifies the need to carry or remember any password or PIN. Moreover, biometrics is something that are unique to one and only one person. The rising popularity and inexpensiveness of such methods make the technology more acceptable. Biometric characteristics can be classified into two broad categories:

Physiological – based methods verify a person's identity by means of his or her physiological characteristics such as fingerprint, facial features, DNA, hand geometry, palm print, iris pattern.

Behavioral – based methods performs the authentication task by recognizing people's behavioral patterns such as typing rhythm and voice print.

2. LITERATURE SERVEY

One of the biggest challenges facing society today is confirming the true identity of a person. Biometrics has been around for many years. Vincenzo Conti et al. [1] used a frequency based approach for features fusion in fingerprint and iris multimodal biometric identification systems. They have come up with an innovative multi-modal biometric identification system based on iris and fingerprint traits. The paper is itself benchmark in advancement of multi-biometrics, offering an innovative perspective on features fusion. Using frequency-based approach results in a homogeneous biometric vector that integrates iris and fingerprint data. Consecutively, a hamming-distance based matching algorithm can be coupled with the unified homogenous biometric vector. Yang F. et al [2] used Fingerprint, palm print, and hand geometry to implement personal identity verification. Unlike other multimodal biometric systems, these three biometric features can be taken from the same image of hand. They implemented matching score fusion to establish identity, performing first fusion of the Fingerprint and palm-print features, and later, a matching-score fusion between the multimodal system and the unimodal palm-geometry. F. Besbes, et al [3] proposed a multimodal biometric system using finger-print and iris features. They use a hybrid approach based on fingerprint minutiae extraction and iris tem-plate encoding through a mathematical representation of the extracted iris region. This approach is based on two recognition modalities and every part provides its own decision. The final decision is taken by considering the unimodal decision through a ―AND‖ operator. Asim Baig et al [4] used a single hamming distance matcher for fingerprint- iris fusion based identification system. They proposed a framework for multimodal biometric identification system which provide smaller memory footprint and faster implementation than the conventional systems. This framework has been verified by developing a fingerprint and iris fusion system which utilizes a single Hamming Distance based matcher. Such systems provide higher accuracy than the individual uni-modal system. Gaurav Bhatnagar et al [5] presented a new watermark embedding technique based on Discrete Wavelet transform (DWT) for hiding little but important information in images. Sumit Shekhar et al [6] proposed a multimodal sparse representation method, which represents the test data by a sparse linear combination of training data, while constraining the observations from different modalities of the test subject to share their sparse representations. Kittler et al. [7] have experimented with several fusion techniques for face and voice biometrics. Ben-Yacoub et al. [8] considered several fusion strategies, such as support vector machines, tree classifiers and multi-layer perception, for face and voice biometrics. Maryam et al. [9] proposed fusion of face and iris to obtain a robust recognition system .in That study the proposed method use Local Binary pattern local feature extractor an subspace linear discriminant analysis global feature extractor on face and iris respectively. Face and iris scores are normalized using tanh normalization, and then weighted sum rule is applied for the fusion. Mohamed et al. [10] multimodal biometric system fusion using fingerprint and iris are proposed, decision level is used for fusion and each biometric result is weighted for participate in final decision .fuzzy logic is used for the effect of each biometric result combination. The proposed method has achieved high accuracy comparing with unimodal systems. L.Latha et al. [11] have used left and right irises and retinal features, and after matching process the scores are combined using weighted sum rule. To validate their approach, experiments were conducted on the iris and retina images obtained from CASIA and VARIA database respectively. Wang Yuan et al [12] proposed a real time fingerprint recognition system in their paper "A Real Time Fingerprint Recognition System Based on Novel Fingerprint Matching Strategy". In this paper they have presented a new real time recognition system based on a novel fingerprint minutiae matching algorithm. Jagadeesan, et al. [13] prepared a secured cryptographic key on the basis of Iris and Fingerprint Features. Minutiae points were extracted from Fingerprint. Similarly texture properties were extracted from Iris. Feature level fusion was further employed. Monwar *et.al* [14] has discussed rank level fusion of face, ear and signature with principal component analysis and fisher's linear discriminant analysis for matching purpose. Kartik et al. [15] 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. Rodriguez et al. [16] 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%. Toh et al. [17] combined hand geometry, fingerprint and voice by using global and local learning decision as fusion approach. The accuracy performance is 85% to 95%. Meraoumia et al. [18] 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 %. Xifeng Tong et al. [19] presented a method, thinning is the process of reducing thickness of each line of patterns to just a single pixel width. The requirements of a good algorithm with respect to a fingerprint are i) the thinned fingerprint image obtained should be of single pixel width with no discontinuities ii) Each ridge should be thinned to its central pixel iii) Noise and singular pixels should be eliminated iv) no further removal of pixels should be possible after completion of thinning process. Bhupesh gaur et al., [20] proposed Scale Invariant Feature Transformation (SIFT) to represent and match the fingerprint. By extracting characteristic SIFT feature points in scale space and perform matching based on the texture information around the feature points. The combination of SIFT and conventional minutiae based system achieves significantly better performance than either of the individual schemes. Vatsa *et al.*[21] applied a set of selected quality local enhancement algorithms to generate a single high-quality iris image. A support-vector-machine-based learning algorithm selects locally enhanced regions from each globally enhanced image and combines these good-quality regions to create a single high-quality iris image.

3. MULTI-BIOMETRIC SYSTEM

Some people have poor quality fingerprints, their face image depends on lighting, their voice can get hoarse due to cold, and also original image of iris projected on a lens can make different biometric authentication systems. All these disadvantages can be overcome with multi-biometric systems which combine the results of two or more biometric characteristics independent from each other. Uni-modal biometric systems are affected by many problems like noisy sensor data, non- universality, lack of individuality, lack of invariant representation and susceptibility to circumvention due to which the uni-modal biometric systems error rate is quite high that makes them unacceptable for security applications. Such types of problems can be alleviated by using two or more uni-modal biometrics as multi-biometric systems.

The architecture of a multi-biometric system depends on the sequence through which each biometrics are acquired and processed. Typically these architectures are either serial or parallel. In the serial architecture, the result of one modality affects the processing of the subsequent modality. In parallel design, different modalities operate independently and their results are combined with appropriate fusion method. Multi-biometric systems use five different methods for solving single biometric disadvantages:

Multi-sensor: using two or more sensors for obtaining data from one biometric (Fingerprint image with two optical and alter sound sensors).

Multi-presentation: several sensors capturing several similar body parts. (Multi fingerprint image from multi finger of one person).

Multi instance: the same sensor capturing several instances of the same body part. (Different position face image).

Multi- algorithm: the same sensor is used but its input is processed by different algorithm and compares the results.

Multi-modal: using different sensors for different biometrics and fusion the results. (Like fusion iris and fingerprint code as multi-biometric).

For combining two or more uni-modal biometrics and making a multi-biometric system, two or more acceptance results must be combined as fusion. Fusion strategies can be divided into two main categories: premapping fusion (before the matching phase) and postmapping fusion (after the matching phase). The first strategy deals with the sensor level fusion, feature level fusion. Usually, these techniques are not used because they result in many implementation problems. The second strategy is realized through fusion at the decision level, based on some algorithms, which combine single decisions for each component of the system. Furthermore, the second strategy is also based on the matching-score level, which combines the matching scores of each component system. A generic biometric system has 4 important modules: (a) the sensor module which captures the trait in the form of raw biometric data; (b) the feature extraction module which processes the data to extract a feature set that is a

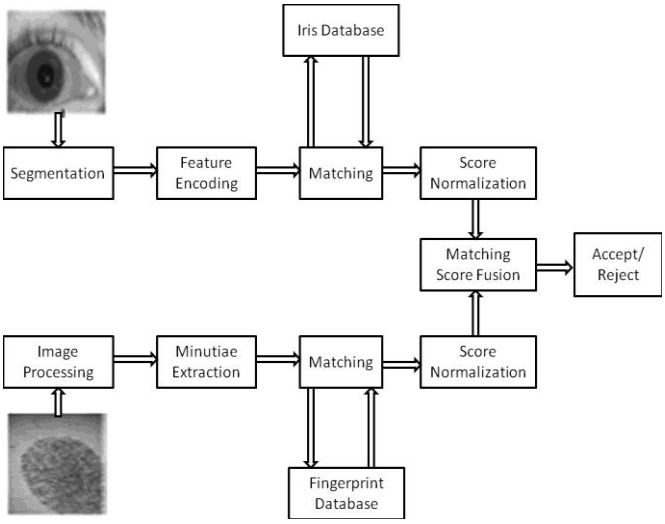


Fig 3.1: Schematic diagram of multibiometric system

compact representation of the trait; (c) the matching module which employs a classifier to compare the extracted feature set with the stored templates to generate matching scores; (d) the decision module which uses the matching scores to either determine an identity or validate a claimed identity. Figure (i) is the representation of a conventional biometric system. The main operations that the system can perform are enrolment and testing. During enrolment biometric information of an individual are stored, during test biometric information are detected and compared with the stored ones. The first block (sensor) is the interface between the real world and our system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics we want to consider. The second block performs all the necessary preprocessing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing some noise), to use some kind of normalization, etc. In the third block we have to extract the features we need. This step is really important: we have to choose which features to extract and how to do it, with certain efficiency to create a template. After that, we are matching the input pattern and the Data base pattern using pattern matching technique.

Finally Authentication occurs based on pattern matching. System is divided into three sub-systems:- Fingerprint recognition, Iris recognition, Fusion techniques:

3.1 Fingerprint recognition

Fingerprint recognition involves the following four steps: 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:

1) ***Binarizing:*** In this step the colors of the image are binaries so that the output image consists of only two colors, black and white.

2) ***Thinning:*** After the fingerprint image is converted to binary form, submitted to the thinning algorithm which reduces the ridge thickness to one pixel wide, demonstrates that the global thresholding technique is effective in separating the ridges (black pixels) from the valleys (white pixels). The results of thinning show that the connectivity of the ridge structures is well preserved, and that the skeleton is eight-connected throughout the image.

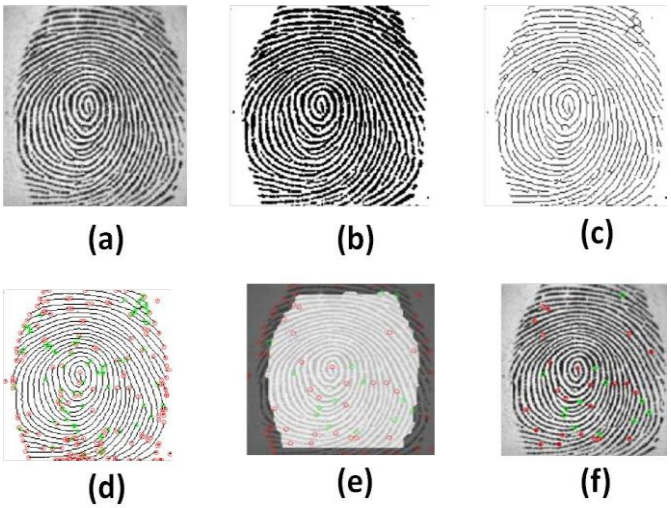
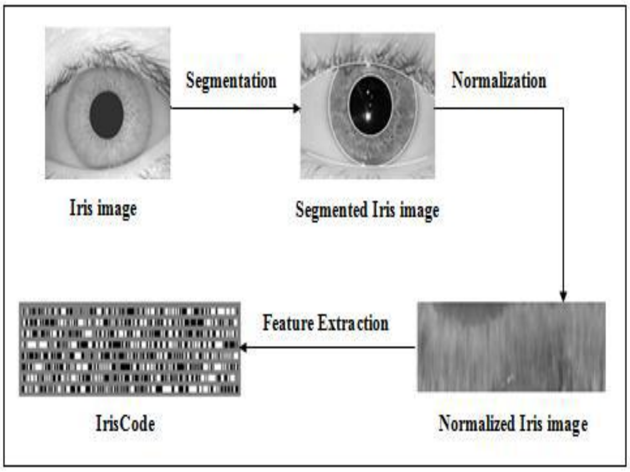


Fig.3- (a) Input image (b)Binarized image (c)Thinned image (d)Ridge end+Bifurcation (e)Common Region of ROI and Image (f)Final Minutiae

3) ***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 neighborhood 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-neighborhood. Using the properties of the CN as, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point.

4) ***Matching:*** The algorithm that we have applied to match two fingerprints involves calculating hamming distance between each ridge end and all other ridge ends and similarly between all bifurcations and then taking the average for both and at last add the results for achieving high accuracy and precision level. This process is applied on both the images and the results of the two images are compared to give the percentage match between the two images.

3.2 Iris recognition



1) ***Iris segmentation:*** It is a significant module in iris recognition. It comprises of two steps 1) canny edge detection technique 2) The parabolic Hough transform. The iris image is first fed as input to the canny edge detection algorithm that produces the edge map of the iris image for boundary estimation. The exact boundary of pupil and iris is located from the detected edge map using the Hough transform. Hough transform has been enhanced to find positions of arbitrary shapes, usually circles or ellipses. For the parameters of circles passing through every edge point, votes are being casted in Hough space, from the obtained edge map. These parameters are the centre coordinates x and y, and the radius are capable to describe the circle in accordance with this equation:

$$x^2 + y^2 = r^2 \quad \text{.......................................} (1)$$

2) ***Iris normalization:*** Once the segmentation module has estimated the iris's boundary, the normalization module uses image registration technique to transform the iris texture from Cartesian to polar coordinates. Daugman`s Rubber Sheet Model is utilized for the transformation process.

3) ***Feature encoding:*** Feature encoding extracts the underlying information in an iris pattern and generates the binary iris template that is used in matching. The normalized 2D form image is disintegrated up into 1D signal, and these signals are made use to convolve with 1D Gabor wavelets. The frequency response of a Log-Gabor filter is as follows,

$$G(f) = \exp\left(\frac{-\left(\log\left(\frac{f}{f_0}\right)\right)^{\wedge}2}{2\left(\log\left(\frac{\sigma}{f_0}\right)\right)^{\wedge}2}\right) \quad \text{..................................} (2)$$

Where f_0 indicates the centre frequency and σ provides bandwidth of the filter. The Log-Gabor filter generates the biometric feature (texture properties) of the iris.

4) ***Matching:*** we are using Hamming distances (HD) to calculate the matching scores between two iris templates.

3.3 Range normalization

The scores generated by a biometric system can be either similarity scores or distance scores, one need to convert these scores into a same nature. Normalization maps the raw matching scores to interval [0, 1] and retains the original distribution of matching scores except for a scaling factor. Given that max(X) and min(X) are the maximum and minimum values of the raw matching scores, respectively, the normalized score is calculated as

$$x' = \frac{x - \min(X)}{\max(X) - \min(X)} \quad \text{..} (3)$$

3.4 Sum rule based score level fusion

The procedure for sum rule-based fusion is stated as following.
After we get a set of normalized scores($x_1, x_2, \ldots, x_m$) from a particular person (here the index i=1,….,m indicates the biometric matcher), the fused score fs is evaluated using the formula,

$$fs = w_1 x_1 + \ldots + w_m x_m \quad \text{..} (4)$$

The notation w_i stands for the weight which is assigned to the matcher–i, for i=1,…, m. There are many choices of how to calculate these weights based on some preliminary results. In the next step, the fused score fs will be compared to a pre- specified threshold t. If $fs \geq t$, then a person declares as to be genuine otherwise, declare as an impostor.

4. CONCLUSIONS

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. Enlarging user population coverage and reducing enrollment failure are additional reasons for combining these multiple traits for recognition. An efficient algorithm using the phase-based image matching is particularly effective for verifying low-quality fingerprint images that could not be identified correctly by conventional techniques. Log-Gabor filter is effective method than any other technique to extract feature from iris image capture. Fusion can be applied to enhance the performance of system and security level.

REFERENCES

[1] Vincenzo Conti, Carmelo Militello, Filippo Sorbello, "A Frequency-Based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems", IEEE transactions on systems, man and cybernetics- Part C: Applications and Reviews, Vol. 40, No. 4, July 2010

[2] Yang F. and Ma B. (2007) *4th IEEE International Conference on Image and Graphics*, *Jinhua*, 689-693.

[3] F. Besbes, H. Trichili, and B. Solaiman, ―Multimodal biometric sys-tem based on fingerprint identification and Iris recognition,‖ in Proc. 3rd Int.IEEE Conf. Inf. Commun. Technol.: From Theory to Applica-tions (ICTTA 2008), pp. 1–5. DOI: 10.1109/ICTTA.2008.4530129.

[4] Asim Biag, Ahmed Bouridane, Faith Kurugollu and Gang Qu, "Fimgerprint- Iris Fuion based Identification System using a Single Hamming Distance Matcher", 2009 Symposium on Bio-inspired Learning and Intelligent Systems for Security.

[5] Gaurav Bhatnagar, Q.M. Jonatihan Wu, Balasubramanian Raman, "Biometric Template Security based on Watermarking", Elsevier, 2010.

[6] Sumit Shekhar, Student Member, IEEE, Vishal M. Patel, Member, IEEE, Nasser M. Nasrabadi, Fellow, IEEE, "Joint Sparse Representation for Robust Multimodal Biometrics Recognition", IEEE, 2013

[7] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, "On Combining Classifiers", IEEE Trans. PAMI, vol. 20, no. 3, pp. 226-239, 1998.

[8] 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.

[9] Maryam Eskandari and O'nsen Toygar. 2012 Fusion of face and iris biometrics using local and global feature extraction methods. Signal, Image and Video Processing, pages 1–12.

[10] Mohamad Abdolahi, Majid Mohamadi, and Mehdi Jafari. 2013. Multimodal biometric system fusion using fingerprint and iris with fuzzy logic. International Journal of Soft Computing and Engineering, 2(6):504 510.

[11] L Latha and S Thangasamy. 2010. A robust person authentication system based on score level fusion of left and right irises and retinal features. Procedia Computer Science, 2:111–120.

[12] Wang Yuan, Yao Lixiu nad Zhou Fugiang, "A Real Time Fingerprint Recognition System Based On Novel Fingerprint Matching Strategy", Electronic Measurement and Instruments, 2007. ICEMI '07. 8th International Conference, July 2007.

[13] Jagadeesan A., Thillaikkarasi T., Duraiswamy K. (2011) *European Journal of Scientific Research*, 49(4), 488-502.

[14] Md. Maruf Monwar & Marina, L. Gavrilova, (2009). Multimodal biometric system using rank-level fusion approach. *IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics*, Vol. 39, No. 4, pp. 867-878.

[15] 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.

[16] 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.

[17] 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

[18] 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.

[19] Xifeng Tong, Songbo Liu, Jianhua Huang, and Xianglong Tang, "*Local Relative Location Error Descriptior-Based Fingerprint Minutiae Matching",* the Journal of the Pattern Recognition Letters, vol. 29, pp. 286-294, (2008).

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

[21] 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.