Performance Analysis of Multimodal Biometric System Authentication

George Chellin Chandran . J [1]
Research Scholar
Dr. M.G.R. Educational and Research Institute
Dr. M.G.R. University

Dr. Rajesh. R.S [2]
Associate Professor
Department of Computer science & Engineering.
Manonmaniam Sundaranar University

Abstract-- Traditional identity verification in computer systems are done based on Knowledge based and token based identification these are prone to fraud. Unfortunately, these may often be forgotten, disclosed or changed. A reliable and accurate identification/verification technique may be designed using biometric technologies. Biometric authentication employs unique combinations of measurable physical characteristics--fingerprint, facial features, iris of the eye, voice print, hand geometry, vein patterns, and so on--that cannot be readily imitated or forged by others. Unimodal biometric systems have variety of problems such as noisy data, intra-class variations, restricted degree of freedom, non-universality, spoof attacks, and unacceptable error rates. Multimodal biometrics refers the combination of two or more biometric modalities in a single identification system. The purpose of this paper is to identify whether the integration of iris and fingerprint biometrics overcome the hurdles of unimodal biometric system. This paper discusses the various scenarios that are possible to improve the performance of multimodal biometric systems using the combined characteristics such as iris and fingerprint, the level of fusion (multimodal fusion) is applied to that are possible and the integration strategies that can be adopted in order to increase the overall system performance. Information from multiple sources can be consolidated in three distinct levels [1]: (i) feature extraction level; (ii) match score level; and (iii) measurement level, (iv) decision level.

Index Terms--*Cross over point, Decision fusion, Equal error rate, Face recognition, Fingerprint recognition, false acceptance rate, false rejection rate, Iris recognition, Multimodal biometric, Receiver operating characteristics, Result Analysis, Templates.*

1. Introduction

Multimodal biometric systems are those that employ more than one physiological or behavioral characteristic for enrollment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multi-modal biometric systems are looked to as a means of (a) reducing false acceptance rates and false rejection rates, (b) providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and (c) combating attempts to spoof biometric systems through non-live data sources such as fake fingers. Identifying a person is becoming critical in our immeasurably interconnected society. The need for reliable, legitimate method for determining an individual's identity technique is essential to increase security level in the area where reliable authentication is needed. Most biometric systems deployed in real-world applications are unimodal, i.e., they rely on the evidence of a single source of information for authentication (e.g., single fingerprint or face or iris)[20]. These systems are subject to problems such as: (i) noisy data (due to dirty sensor or environment poorly illuminated) (ii) Intra-class variations (due to incorrect interaction with sensor ie: incorrect facial pose). (iii) Inter-class similarities (due to overlap ie: In a biometric system comprising of a large number of users, there may be inter-class similarities). (iv) Non-universality (due to incorrect data ie: the biometric system may not be able to acquire meaningful biometric data). (v) Spoof attacks: this type of attack is especially relevant when behavioral traits such as signature or voice are used. However, physical traits such as fingerprints are also susceptible to spoof attacks. In this paper, the limitations imposed by unimodal biometric systems is overcome by multimodal biometric systems which include multiple sources of information and are expected to be more reliable. The proposed system uses multiple biometric traits of an individual to establish identity. Brunelli et al. [24] use the face and voice traits of an individual for identification. Since, all the biometric technology has their own strengths and weaknesses and each are well suited for particular applications here no single Biometric technology will dominate every area of the Biometric industry. A biometric authentication system operates in two approaches: Enrollment and Authentication. During enrollment user's biometric data are acquired using a biometric read and stored in a database. The stored biometric template is tagged with a user identity to facilitate authentication. In the authentication phase, a user's biometric data is once again acquired and the system uses it to either verify the claimed identity of the

Manuscript received March 5, 2009
Manuscript revised March 20, 2009

user or identify who the user is. While verification involves comparing the acquired biometric information with only those templates corresponding to the claimed identity, identification involve comparing the acquired biometric information against templates corresponding to all users in the database [22].The table - i Compares the Biometric Technologies fingerprint and iris based on five characteristics namely universality, uniqueness, permanence, performance and Collectability. Although there has been many researches on multimodal biometrics are on the venue by combining different biometrics technologies, however not much work is focused on the combination of fingerprint and iris. In this paper we examine the scenario for integrating fingerprint and iris using Decision level fusion The evidence provided by the FRR & FAR minimizes the error rate and proven that the system performance is more reliable for future authentication. The rest of the paper is organized as follows: section 2 gives the brief overview of fingerprint and iris recognition systems, Section 3 suggest the overview of proposed technology. Section 4 discus the implementation parts, Section 5 provide the experimental result, Section 6 present the result analysis and Section 7 concludes the document.

Table i : Comparison based on Fingerprint & Iris characteristics

Biometric aspects	Universality	Uniqueness	Permanence	Performance	Collectability
FingerPrint	**Medium**	**High**	**High**	**High**	**Medium**
Iris	**High**	**High**	**High**	**High**	**Medium**

2. Existing Methodology

2.1 Biometric Identification 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 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 enrollment and testing. During enrollment 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 pre-processing: 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.

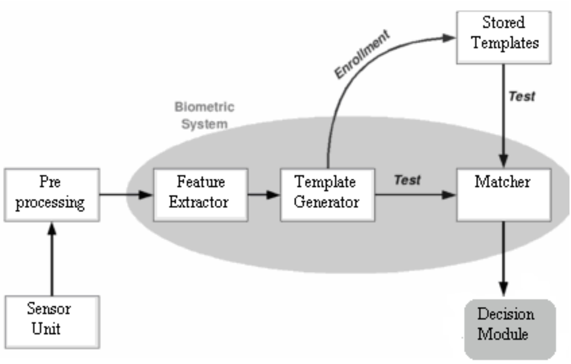

Fig. 1 Block diagram represents a simple Biometric system

3. Proposed Approach

The design of a multimodal biometric system is strongly dependent on the application scenario. A number of multimodal biometric systems have been proposed but they are differ from one another in terms of their architecture, the number and choice of biometric modalities, the level at which the evidence is accumulated, and the methods used for the integration or fusion of information. The proposed system adopts multiple biometric traits of an individual, to establish the identity. The system employs multiple sensors to acquire data pertaining to fingerprint and iris. The independence of the traits ensures the improvement in performance. The system operates on five stages. (a) Stage–1, the multiple Sensor captures the raw biometric data and can be processed and integrate to generate a new data from which features can be extracted, as shown in fig. (ii) (b) Stage–2, the preprocessor unit extract the necessary features that are subject to interest. (c) Stage–3, template will be generated for the extracted features. (d) Stage–4, Decision fusion integrates multiple cues (e) Stage -5 the input data will be compared with database data for matching. Finally if matching is genuine authentication occurs if not authentication denied.

3.1 Proposed System Performance

The performance of the proposed system is determined by its accuracy. False Accept Rate (FAR) and False Reject Rate (FRR) are two widely used standard metrics to determine the accuracy of a biometric system. The FAR is the percentage of imposters that are incorrectly granted access and FRR is the percentage of valid users who are incorrectly denied access.

3.2 Purpose

The main purpose of the proposed system is to reduce the error rate as low as possible and improve the performance of the system by achieving good acceptable rate during identification and authentication.

4. Implementation

The promise of biometric technology for countering security threats Biometric authentication employs unique combinations of measurable physical characteristics--fingerprint, facial features, iris of the eye, voice print, hand geometry, vein patterns, and so on--that cannot be readily imitated or forged by others to determine or verify a person's identity. Initially the raw biometric data pertaining to multiple sensors are obtained. In our proposed system since we are using multiple biometric characters of an individual to establish identity. Here, we employ multiple sensors to acquire data pertaining to different characters. The independence of the characters ensures good and reliable performance. Provide high level security by integrating the patterns by Decision level fusion.

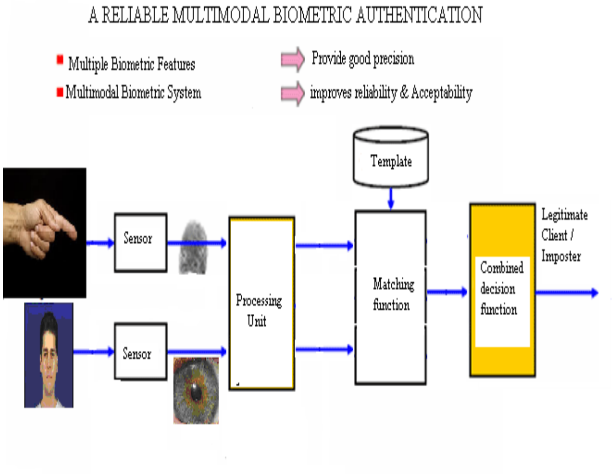
A RELIABLE MULTIMODAL BIOMETRIC AUTHENTICATION
Multiple Biometric Features
Multimodal Biometric System
Provide good precision
improves reliability & Acceptability
Template
Sensor
Sensor
Processing Unit
Matching function
Combined decision function
Legitimate Client / Imposter

Fig. 2 Proposed system an overview

4.1 Fingerprint Recognition

Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. Solid state sensors overcome this and other technical hurdles because the coated silicon chip itself is the sensor. Solid state devices use electrical capacitance to sense the ridges of the fingerprint and create a compact digital image. Once the image has been captured fingerprint image processing must be carried out:

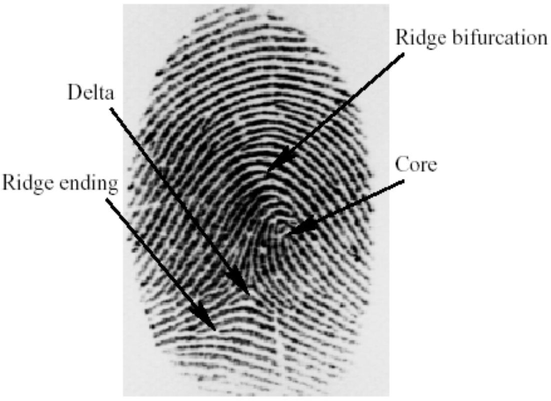

Fig. 3 Structure of Fingerprint

(a) Recognition of aspects – the finger print is represented as a series of ridges and valleys with local discontinuities in the ridge flow pattern called minutiae. (b)Ridge extraction - The ridges are extracted by eigen space representations using minimum distance classifier.(c)Matching fingerprints - The matching is the process two fingerprint images are compared and the resemblance between the two geometrics are measured.

4.2 Iris Recognition

Fingerprint recognition is the technology that verifies the identity of a person based on the fact that everyone has unique fingerprints. It is one of the most heavily used and actively studied biometric technologies. A person's iris is fully developed within 18 months after birth, and is protected by eyelashes, eyelids and the retina. Its shape hardly changes so that it has higher consistency compared to other biometric characteristics. Its higher uniqueness in shape than a face or fingerprints ensures that an authentication system using the iris is immensely reliable. Personal identification using iris is composed of two parts: obtaining the iris image and recognizing it. Firstly, the system performs the function of obtaining the iris image suitable to iris recognition. The second part is comprised of two stages: extracting the iris area from the image and creating an iris code, and perform a match based on the iris characteristics.

(a) Recognition – occurs by obtaining an eye image from an input device is the first stage of personal identification using the iris. The device is comprised of a camera to capture the image and lighting & image sensors to grab correct iris patterns. In particular, the device is closely related to the system's overall performance. General iris input devices are using multi-wavelength infrared rays to prevent iris patterns from being affected by external light. Unlike face recognition, close-up photographing is required to obtain appropriate resolution of the eye image since an eye is smaller than a face. In the case of close-up photographing, it is difficult to set a clear focus due to low depth of field. To obtain a clear image, the shutter speed of a camera and capture speed of an image sensor should be fast. The infrared rays used to capture the iris image have low intensity, and are known to be non-harmful to humans.(b) Iris Extraction - After capturing the eye image, the iris area should be correctly extracted from it. Detecting the inner boundary of the iris against the pupil and the outer border of the iris against the sclera finishes the process.

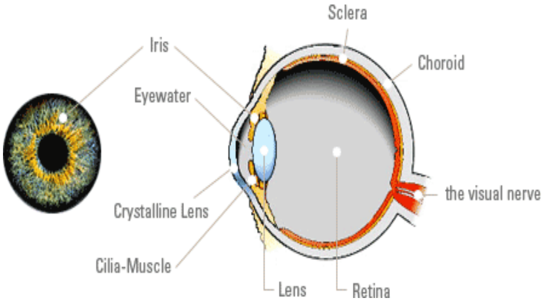

Fig. 4 Structure of Iris

Both borders of the iris are determined by approximating them into a circle based on the premise that they are circle-shaped. For the circle detection, extract the inner/outer boundaries of the iris after performing the preprocessing on the eye image, or change "hoop transformation" that is widely used for the detection of the same-shape line. In general, a Circular Edge Detector is commonly used. However, the outer boundary of the iris could have a non-circular shape. The feature extraction method using the Gabor Wavelet transformation, which is commercialized and recognized for its good performance, is introduced here. After the iris area is extracted, the area is divided into 8 small ring areas. The gray values of the iris patterns are calculated clockwise or counter-clockwise and the iris feature data in actual use can be obtained through the Gabor Wavelet transformation of the value.

4.3 Level of fusion

In multimodal biometric system there are Four possible levels of information fusion. They are fusion at the sensor level, feature extraction level, matching score level and decision level. Sensor level fusion is unusual because fusion at this level requires that the data obtained must be compatible, which is rare in case of biometric sensors. Fusion at the feature level is also not always possible because the feature sets of multiple modalities may be incompatible or inaccessible. Fusion at matching score level is generally complex in logic and requires lengthy enrolment time Fusion at the decision level is generally preferred because Decision fusion integrates multiple cues improve the accuracy of a recognition system

4.3.1 Decision fusion

Decision fusion integrates multiple cues of fingerprint and iris inorder to improve the accuracy of recognition system [25], [24], [10]. Generally, multiple cues may be integrated at one of the following three different levels [24]: i) Abstract level; the output from each module is only a set of possible labels without any confidence associated with the labels; in this case, the simple majority rule may be employed to reach a more reliable decision. ii) Rank level; the output from each module is a set of possible labels ranked by decreasing confidence values, but the confidence values themselves are not specified; iii) Measurement level; the output from each module is a set of possible labels with associated confidence values; in this case, more accurate decisions can be made by integrating different confidence measures to a more informative confidence measure. In our system, the decision fusion is designed to operate at the measurement level. Each of the top n possible identities established by the iris recognition module is verified by the fingerprint verification module. In order to carry out such a decision fusion scheme, we need to define a measure that indicates the confidence of the decision criterion and a decision fusion criterion. The confidence connected with different results may be characterized by the genuine distribution and the impostor distribution, which are used to establish two error rates: i) false acceptance rate (FAR), which is defined as the probability of an impostor being accepted as a genuine individual and ii) false reject rate (FRR), which is defined as the probability of a genuine individual being rejected as an impostor. The graph in fig 5 shows the relationship between these variables. The cross over error rate is the point at which the FRR and FAR are equal. In the context of personal identification, the required FAR value and FRR value should be less than the cross over error rate to obtain genuine authentication.

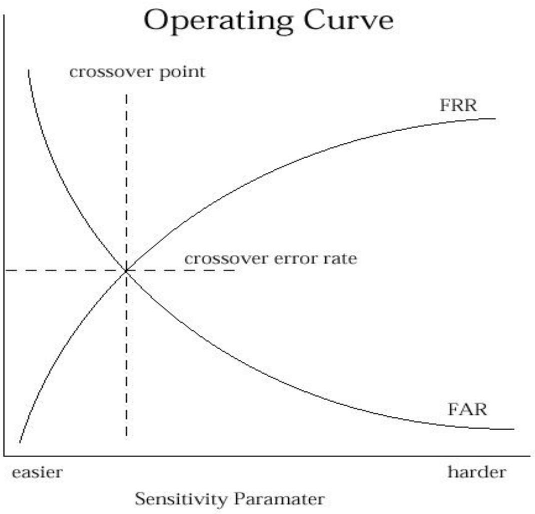

Fig. 5 shows the relationship between FRR & FAR

4.4 Decision Policy

The decision subsystem implements system policy by directing the database search, determine "matches" or "non-matches" based on the distance measures received from the pattern matcher, and ultimately make an "accept/reject" decision based on the system policy. Such a policy could be to declare a match for any distance lower than a fixed threshold and "accept" a user on the basis of this single match, or the policy could be to declare a match for any distance lower than a user-dependent, time-variant, or environmentally-linked threshold and require matches from multiple measures for an "accept" decision. The policy could decide the good-guys and bad-guys alike.

5. Experimental Results

A set of 10 iris images and fingerprint images were acquired from 60 users, to evaluate the performance of the proposed technique. In this experiment the ROC curve that summarizes the matching performance by plotting the False Rejection Rate (FRR) against the False Accept Rate (FAR) at various thresholds. The Equal Error Rate (EER) using match score level fusion is 3.5 & 3.0 respectively with respect to Table ii & iii. The receiver operating characteristic (ROC) curves of the individual matchers and the likelihood ratio based on fusion rule for these databases are shown in Fig. 6 & 7. As expected, likelihood ratio based fusion leads to significant improvement in the performance. At a false accept rate (FAR) of 0:001%, the improvement in the genuine Acceptance is achieved. FAR & FRR exits when the threshold level is >0.1

6. Result Analysis

Table ii Result analysis of genuine acceptance

Threshold	Finger	Irris	Finger & Irris
0.0	1	2	1
0.5	1	6	1
1.0	1	9	1
1.5	4	10	4
2.0	5	10	5
2.5	7	10	7
3.0	8	10	8
3.5	9	10	9
4.0	9	10	9

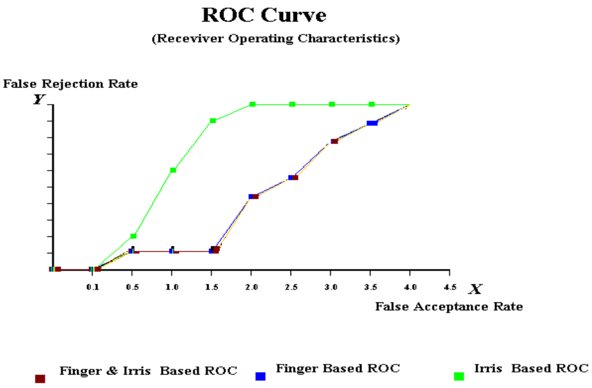

Fig. 6 ROC in case of genuine acceptance

Table iii Result analysis of imposter

Threshold	Irris	Finger	Finger & Irris
0.0	3	1	1
0.5	7	2	2
1.0	10	4	4
1.5	10	7	7
2.0	10	8	8
2.5	10	8	8
3.0	10	9	9
3.5	10	9	9
4.0	10	9	9

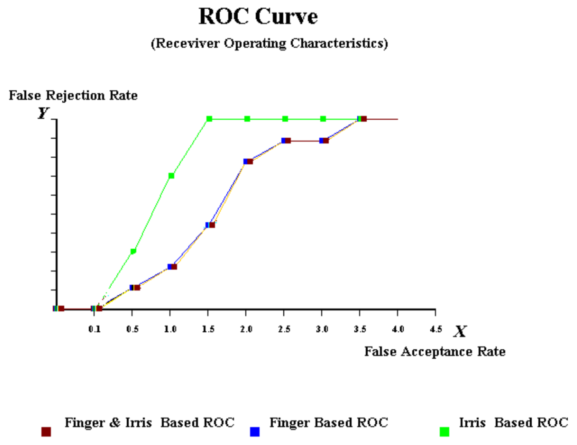

Fig 7 : ROC in case of imposter

7. Design Issues

A variety of factors should be considered when designing a multimodal biometric system. First is the growing international threat to security. second reason for growing interest in biometrics is the increasing threat to security that comes with the ubiquitous information society. The third reason biometric techniques are attracting attention is the apparent need to replace conventional authentication methods with more robust biometric authentication. The Proposed system uses the Combination of Biometric technologies because all the biometric technology has their own strengths and weaknesses and each are well suited for particular applications here is no single Biometric technology will dominate every area of the Biometric industry. The system choose a Biometric by considering factors such as (a) the choice of biometric traits, (b) integration of multiple biometric traits, (c) the methodology adopted to integrate the information, (d) highest level of security & reliability, (e) mobility, (f) safe and user friendliness, and (g) the cost versus matching performance.

8. Conclusion

There is no security system that is completely out of spoofing. Every system is subject to breakable. The techniques used to prevent the attacks help to increase the time, and cost. Fingerprints can be easily forged from touched surfaces and can be copied in a small amount of time using readily available materials. All the liveness detection mechanisms in fingerprint systems can be easily overwhelmed using wafer thin gelatin and silicon artificial fingerprints. But it is very difficult to fake the iris systems because they use physiological reactions to changing illumination conditions for liveness detection. A physical modeling of iris device will be needed to defeat them which are very hard and expensive. Also a fake iris printed on a contact lens can be easily detected using a check to see special properties introduced by the printing. So iris systems can be used for high security applications and network security. But iris and retina systems are very expensive and their user acceptability is low compared to face and fingerprint recognition systems. This makes them a bad choice for common applications. Biometric systems using fingerprints and face are sufficiently robust to be used as an authentication system for time and attendance and access control for low security systems No biometric system is optimal. The decision to which biometric is to be used should be made on the basis of the type of application and the level of security. Multimodal biometric systems address several problems present in unimodal system. Multimodal biometric systems are those that utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multi-modal biometric systems are looked to as a means of (a) reducing false acceptance and false rejection, (b) providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and (c) combating attempts to spoof biometric systems through non-live data sources such as fake fingers. The performance of multimodal biometric system shows great promise to personal identity in the biometric authentication society.

References

[1] Wayman, J., Jain, A.K., Maltoni, D., Maio, D.: Biometric Systems: Technology, Design and Performance Evaluation.Springer (2005)

[2] Feng, X., Pietik¨ainen, M., Hadid, A.: Facial Expression Recognition with Local Binary Patterns and Linear Programming. Pattern Recognition and Image Analysis 15 (2005) 550-552

[3] A. K. Jain, K. Nandakumar, and A. Ross, \Score normalization in multimodal biometric systems," Pattern Recognition , 2005.

[4] M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. K. Jain, multimodal biometric authentication methods: A Cots approach," in Workshop on Multimodal User Authentication (MMUA), pp. 99{106, 2003.

[5] D. Maio and D. Maltoni. Direct gray scale minutia detection in fingerprints. Transactions on PAMI, 19(1), 1997.

[6] D. Maio, D. Maltoni, A. K. Jain, and S. Prabhakar. Handbook, Fingerprint Recognition. Springer Verlag, 2003.

[7] A. Vetro and N. Memon, "Biometric System Security," Tutorial presented at Second International Conference on Biometrics, Seoul, South Korea, August 2007.

[8] Y. Sutcu, Q. Li, and N. Memon, "Secure Biometric Templates from Fingerprint-Face Features," in Proceedings of CVPR Workshop on Biometrics, Minneapolis, USA, June 2007.

[9] W. J. Scheirer and T. E. Boult, "Cracking Fuzzy Vaults and Biometric Encryption," in Proc. of Biometrics Symposium, September 2007.

[10] j. Kittler, Y. Li, J. Matas and M.U. Sanchez, "Combining evidence in multimodalpersonal identity recognition systems", Proc. First Int'l Conf. Audio Video based Personal Authentication, pp. 327-334, Crans-Montana, swizerland, mar. 1997.

[11] P N Belhumeur, J P Hespanha, and D J Kriegman, "Eigenfaces vs. fisherfaces: Recognition using class specific linear projection", IEEE Trans. on Pattern Analysis and Machine Intelligence, 19(7), pp. 711-720, 1997.

[12] Jain, A., and Pankanti, S., "Fingerprint Classification and Matching". Handbook for Image and Video Processing, A.Bovik (ed.), Academic Press, April 2000.

[13] S. Prabhakar, A. Jain, and S. Pankanti. Learning fingerprint minutiae location and type. volume 36, pages 1847–1857, 2003.

[14] Richard W. Hamming. Error Detecting and Error Correcting Codes Bell System Technical Journal 26(2):147-160, 1950.

[15] E. Newham, The Biometric Report. New York: SJB Services, 1995.

[16] Eigenvalues function Mathematica documentation

[17] A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics. Springer, 2006.

[18] A. Kholmatov and B. Yanikoglu, "Realization of Correlation Attack Against the Fuzzy Vault Scheme," in Proc. of SPIE Symposium on Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, vol. 6819, San Jose, USA, January 2008.

[19] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based Fuzzy Vault: Implementation and Performance," IEEE Trans. on Info. Forensics and Security, vol. 2, no. 4, pp. 744–757, December 2007.

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

[21] M. Golfarelli, D. Maio, and D. Maltoni, "On the error-reject tradeoff in biometric verification systems," IEEE Trans.on Patt. Anal. and Mach. Intell., vol.19, pp. 786–796, July1997.

[22] A. Ross and A. K. Jain, "Information fusion in biometrics," Pattern Recognition Letters, vol. 24, pp. 2115–2125, Sep 2003.

[23] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, "Is independence good for combining classifiers?," in Proc. of Int'l Conf. on Pattern Recognition (ICPR), vol. 2, (Barcelona, Spain), pp. 168–171, 2000.

[24] R. Brunelli and D. Falavigna, "Person identification using multiple cues," IEEE Transactions on PAMI, vol. 12, pp. 955–966, Oct 1995.

[25] E. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert conciliation for multimodal person authentication systems using Bayesian Statistics," in First International Conference on AVBPA, (Crans-Montana, Switzerland), pp. 291–300, March 1997.

[26] L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal identification," IEEE Transactions on PAMI, vol. 20, pp. 1295–1307, Dec 1998.

[27] R. W. Frischholz and U. Dieckmann, "Bioid: A multimodal biometric identification system," IEEE Computer, vol. 33, no. 2, pp. 64–68, 2000.

[28] J.L. Wayman, "Technical Testing and Evaluation of Biometric Identification Devices" in A. Jain, etal (eds), Biometrics: Personal Identification in a Networked Society, (Kluwer Academic Press, 1998)

[29] C. Frenzen, "Convolution Methods for Mathematical Problems in Biometrics", Naval Postgraduate School Technical Report, NPS-MA-99-001, January 1999

ABOUT THE AUTHORS

Mr. J.George Chellin Chandran, received his B.E degree in Electronics and Communication Engineering from Manonmaniam Sundaranar University in the year 1994 and M.E degree in Computer Science and Engineering from Madurai Kamaraj University in the year 2000. Presently doing Ph.D in Dr. MGR Educational and Research institute. He is working as Principal in Sri Jayaram Engineering College, cuddalore. He has more than 14 years experience in the field of education and administration. He is a member of ISTE, CSI, AIMA, IEEE, ACM.

Dr. R. S Rajesh received his B.E and M.E degrees in Electronics and Communication Engineering from Madurai Kamaraj University, Madurai, India, in the year 1988 and 1989 respectively, and completed his Ph.D in Computer Science and Engineering at Manonmaniam Sundaranar University, Tirunelveli, India in the year 2004. In September 1992 he joined in Manonmaniam Sundaranar University where he is currently working as Associate Professor in the Computer Science and Engineering Department. He got more than 18 years of PG teaching and Research experience. His current research interests include Digital image processing, Biometric Security, Wireless networks, Mobile and Pervasive computing and Parallel Computing.