Decision Fusion based Person Identification System using Fingerprints and Facial Image with Template Matching

A. K. M. Akhtar Hossain

Professor, Dept. of Computer Science & Engineering,
University of Rajshahi, Bangladesh.
Email: akh_ru_cst [AT] yahoo.com

ABSTRACT— ***In this research, it has been developed a prototype biometric system which integrates facial images and fingerprints. The system overcomes the limitations of face recognition systems as well as fingerprint recognition systems. The integrated prototype system operates in the identification mode with an admissible response time. The identity established by the system is more reliable than the identity established by a face recognition system. In addition, the proposed decision fusion scheme enables performance improvement by integrating multiple features with different confidence measures. Experimental results demonstrate that the system performs well. It meet up the response time as well as the accuracy requirements.***

Keywords — Prototype Biometrics, False Acceptance Rate (FAR), False Reject Rate (FRR), Decision Fusion, Template database.

1. INTRODUCTION

A biometric system uses multiple applications to capture different types of biometrics. This allows the integration of two or more types of biometric recognition and verification the systems in order to meet stringent performance requirements. A multimodal system could be, for instance, a combination of fingerprint verification, face recognition, Iris identification, voice verification and smart card or any other combination of biometrics. This enhanced structure takes advantage of the proficiency of each individual biometric and can be used to overcome some of the limitations of a single or two biometric. A multimodal system can combine any number of independent biometrics and overcome some of the limitations presented by using just one or two biometric as verification tool. For instance, it is estimated that 5% of the population does not have legible fingerprints, a voice could be altered by a cold and face recognition systems are susceptible to changes in ambient light and the pose of the subject [3][9]. A multimodal system, which combines the conclusions made by a number of unrelated biometrics indicators, can overcome many of these restrictions. Unlike single Biometrics methods of authentication a Multimodal biometric system uses multiple bio-applications to capture and store different types of biometric signatures. Using this method allows the integration of two or more types of biometric verification systems in order to increase the performance and reliability of security systems and to meet required security standards. Multimodal systems are generally more vital to fraudulent technologies, because it is of the opinion that it is more difficult to forge or copy multiple biometric characteristics than to forge a single biometric.

2. IDENTIFICATION ACCURACY OF BIOMETRIC SYSTEMS

Due to intra class variations in the biometric characteristics, the identity can be established only with certain confidence. A decision made by a biometric system is either a “genuine individual” type of decision or an “impostor” type of decision [11], [12],[13],[14]. For each type of decision, there are two possible outcomes, true or false. Therefore, there are a total of four possible outcomes:

a) A genuine individual is accepted
b) A genuine individual is rejected
c) An impostor is accepted
d) An impostor is rejected

Outcomes 1 and 3 are correct, whereas outcomes 2 and 4 are incorrect. The confidence associated with different decisions may be characterized by the genuine distribution and the impostor distribution, which are used to establish two error rates:

a) False acceptance rate (FAR), which is defined as the probability of an impostor being accepted as a genuine individual and
b) False reject rate (FRR), which is defined as the probability of a genuine individual being rejected as an impostor.

FAR and FRR are dual of each other. A small FRR usually leads to a larger FAR, while a smaller FAR usually implies a larger FRR. Generally, the system performance requirement is specified in terms of FAR [1][9]. A FAR of zero means that no impostor is accepted as a genuine individual.

In order to build a biometric system that is able to operate efficiently in identification mode and achieve desirable accuracy, an integration scheme which combines two or more different biometric approaches may be necessary. For example, a biometric approach that is suitable for operating in the identification mode may be used to index the template database and a biometric approach that is reliable in deterring impostors may be used to ensure the accuracy. Each biometric approach provides a certain confidence about the identity being established. A decision fusion scheme which exploits all the information at the output of each approach can be used to make a more reliable decision.

3. PROPOSED SYSTEM ARCHITECTURE

User verification systems that use a single biometric indicator often have to contend with noisy sensor data, restricted degrees of freedom, non-universality of the biometric trait and unacceptable error rates. Attempting to improve the performance of individual matchers in such situations may not prove to be effective because of these inherent problems. Multi-biometric systems seek to alleviate some of these problems and drawbacks by providing multiple evidences of the same identity. These systems help achieve an increase in performance that may not be possible using a single biometric indicator.

It has been introduced a prototype integrated biometric system which makes personal identification by integrating facial images and fingerprints. The prototype integrated biometric system shown in **Fig.1** operates in the identification mode. The proposed system integrates three different biometric Approaches (face recognition and fingerprint recognition) and incorporates a decision fusion module to improve the identification performance.

4. DESIGN ISSUES OF THE DEVELOPED MULTIMODAL BIOMETRIC SYSTEM

i. **Choice and number of biometric indicators**: The proposed system uses three biometric (facial image and fingerprint) indicator to identify a person.
ii. **Fusion level**: Decision fusion which integrates multiple cues has proved beneficial for improving the accuracy of a recognition system [11], [12], [18]. Generally, multiple cues may be integrated at one of the three different levels which are discussed in Multimodal Biometric system. In our system, the decision fusion is designed to operate at the decision level. Each biometric system makes its own recognition decision based on its own feature vector. A majority vote scheme can be used to make the final recognition decision.
iii. **Fusion Methodology**: Fusion methodology means the techniques which are used to make final decision of a multimodal system. Our system uses a conjunctive rule based methodology which is discussed below.

Mode of operation: A multimodal biometric system can operate in one of three different modes which are discussed in multimodal biometric system. The system has been used parallel mode of operation where information from facial image and fingerprint are used simultaneously to perform recognition.

5. FACE RECOGNITION

The system is initialized by first acquiring the training set. Eigenvectors and Eigenvalues are computed on the covariance matrix of the training images [4][5][6]. The M highest eigenvectors are kept. Finally, the known individuals are projected into the Eigen face space, and their weights are stored. Once the eigenfaces are created, identification becomes a pattern recognition task. When an unknown face or new facial image is found, project it into the eigenspace. To recognize the face, the Euclidean distance is measured between the unknown image's position in eigenspace and all the known face positions in eigenspace. Select the face closest in eigenspace to the unknown face as the match.

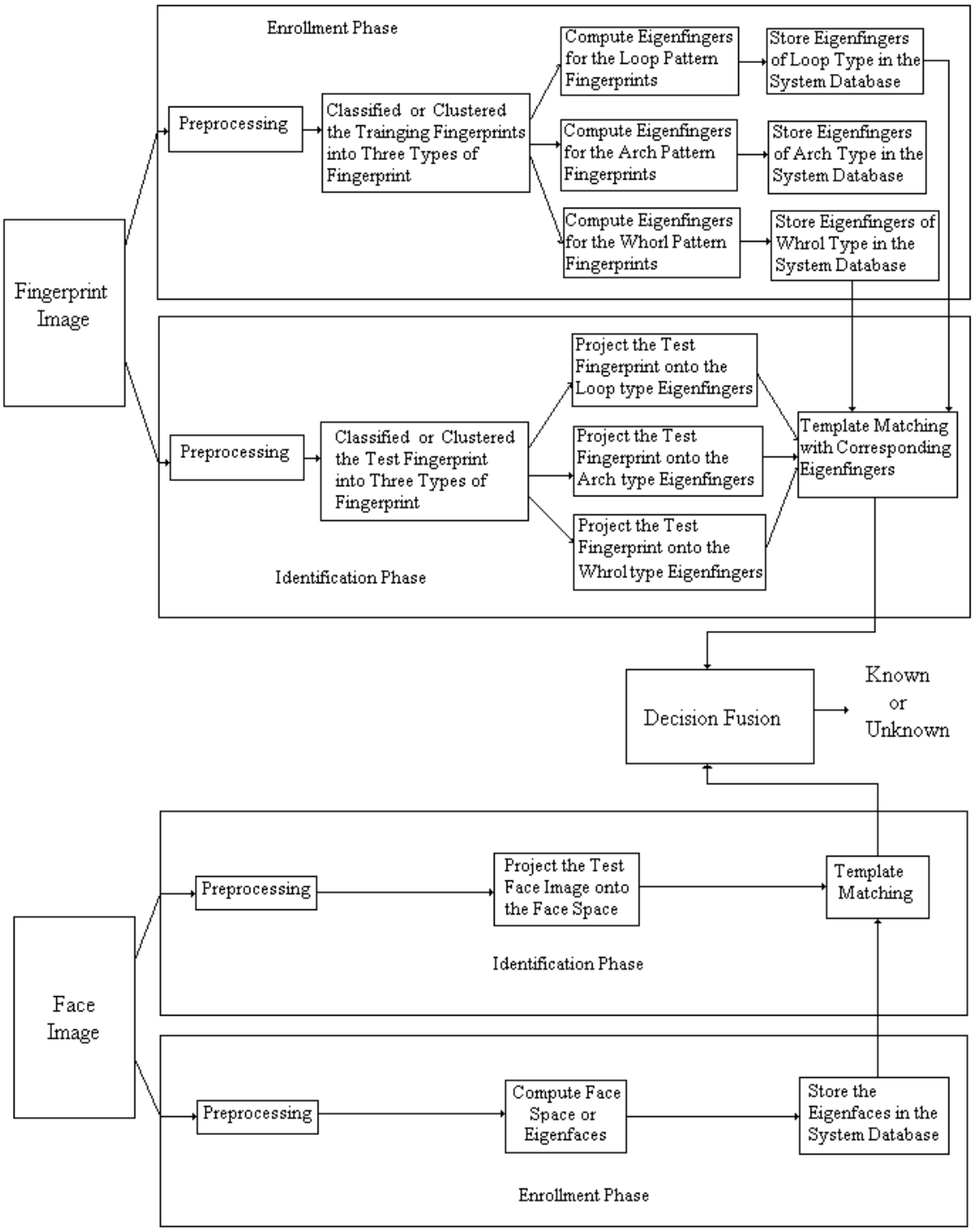

Fig.1: Proposed Diagram of the Multimodal System

Let a facial image I(x, y) be a two-dimensional N by N array of intensity values or a vector of dimension N^2. A typical image of size 256 by 256 describes a vector of dimension 65,536, or equivalently, a point in 65,536-dimensional space [6]. Consider our training set of images of 100 by 100 pixels. Images of faces, being similar in overall configuration, will not be randomly distributed in this huge space thus can be described by a relatively low dimensional subspace. The main idea of principal component analysis is to find the vectors which best account for the distribution of the face images within the entire image space. These vectors define the subspace of the face images, which we call "face space". Each vector of length N^2, describes an N by N image, and is a linear combination of the original face images. Because these vectors are the eigenvectors of the covariance matrix corresponding to the original face images, and because they are face like in appearance, we refer to them as "eigenface".

Steps for eigenfaces / eigenspace calculation:

1. The first step is to obtain a set S with M face images. Each image is transformed into a vector of size N and placed into the set.

$$S = \{\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4, \Lambda\ \Lambda\ \Lambda\ , \Gamma_M\}$$

2. Second step is to obtain the mean image Ψ.

$$\Psi = \frac{1}{M}\sum_{n=1}^{M}\Gamma_n$$

Fig. 2: Example Average Image.

3. Then find the difference Φ between the input facial image and the mean image

$$\Phi_i = \Gamma_i - \Psi$$

4. Next seek a set of M orthonormal vectors, u_n, which best describes the distribution of the data. The k_{th} vector, u_k, is chosen such that

$$\lambda_k = \frac{1}{M}\sum_{n=1}^{M}\left(u_k^T \Phi_n\right)^2$$

is a maximum, subject to $\mathbf{u}_l^T\mathbf{u}_k = \delta_{lk} = \begin{cases} 1 & \text{If l=k} \\ 0 & \text{Otherwise} \end{cases}$

where u_k and λ_k are the eigenvectors and eigenvalues of the covariance matrix C

5. The covariance matrix C has been obtained in the following manner

$$C = \frac{1}{M}\sum_{n=1}^{M}\Phi_n\Phi_n^T$$
$$= AA^T$$
$$A = \{\Phi_1, \Phi_2, \Phi_3, \Lambda\ \Lambda\ \Lambda\ , \Phi_n\}$$

6. To find eigenvectors from the covariance matrix is a huge computational task. Since M is far less than N^2 by N^2, we can construct the M by M matrix L= A^TA, where $L_{mn} = \Phi_m^2\Phi_n$

7. Find the M eigenvectos, v_l of L.

8. These vectors (v_l) determine linear combinations of the M training set facial images to form the final eigenvectors or eigefaces u_l

$$u_l = \sum_{k=1}^{M} v_{lk}\Phi_k \qquad l = 1,2,\Lambda\ \Lambda\ \Lambda\ , M$$

After computing the eigenvectors or eigenfaces and eigenvalues on the covariance matrix of the training images, the M eigenvectors are sorted in order of descending eigenvalues and chosen to represent eigenfaces or eigenspace. The following are the first four eigenfaces of our set of training face's images in the order of eigenvalues.

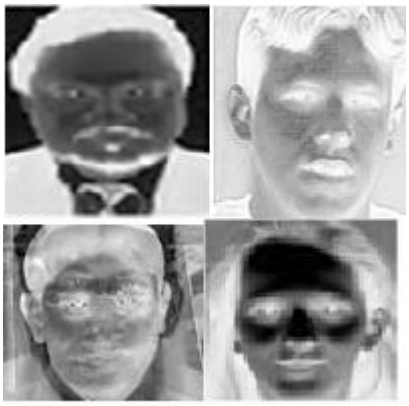

Fig. 3: Eigenfaces for the Example Image Set.

Finally, Project each of the original facial images into eigenspace. This gives a vector of weights representing the contribution of each eigenface to the reconstruction of the given image.

6. FINGERPRINT RECOGNITION

The system is initialized by first acquiring the training set. The training set fingerprints are classified into three types of fingerprint [8][9]. Eigenvectors and eigenvalues are computed on the covariance matrix of each type of training fingerprint. The M highest eigenvectors are kept for each type of fingerprint. Finally, the known individuals are projected into the corresponding Eigen fingerprint space, and their weights are stored. Once the eigenfingers of type of fingerprint are created, identification becomes a pattern recognition task. When an unknown fingerprint or new fingerprint is found, classify of cluster it among one of the three types of fingerprint and project it into the corresponding class fingerprint eigenspace. To recognize the fingerprint, the Euclidean distance is measured between the unknown fingerprint's position in eigenspace and all the known fingerprint positions in eigenspace. Select the fingerprint closest in eigenspace to the unknown fingerprint as the match.

Let a finger image I(x, y) be a two-dimensional N by N array of intensity values or a vector of dimension N^2. A typical image of size 256 by 256 describes a vector of dimension 65,536, or equivalently, a point in 65,536-dimensional space [6]. Consider our training set of images of 100 by 100 pixels. Images of one type fingers, being similar in overall configuration, will not be randomly distributed in this huge space thus can be described by a relatively low dimensional subspace. The main idea of principal component analysis (PCA) is to find the vectors which best account for the distribution of the finger images within the entire image space. These vectors define the subspace of the finger images, which we call "eigenspace". Each vector of length N^2, describes an N by N image, and is a linear combination of the original finger images. Because these vectors are the eigenvectors of the covariance matrix corresponding to the original finger images, and because they are finger like in appearance, we refer to them as "eigenfinger".

Steps for eigenfingers / eigenspace calculation:

1. The first step is to obtain a set S with M finger images. Each image is transformed into a vector of size N and placed into the set.

$$S = \{\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4, \Lambda\ \Lambda\ \Lambda\ , \Gamma_M\}$$

2. Second step is to obtain the mean image Ψ.

$$\Psi = \frac{1}{M}\sum_{n=1}^{M}\Gamma_n$$

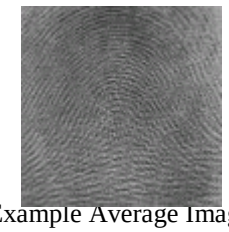

Fig.4 Example Average Image.

3. Then find the difference Φ between the input fingerprint image and the mean image

$$\Phi_i = \Gamma_i - \Psi$$

4. Next seek a set of M orthonormal vectors, u_n, which best describes the distribution of the data. The k_{th} vector, u_k, is chosen such that

$$\lambda_k = \frac{1}{M}\sum_{n=1}^{M}\left(u_k^T \Phi_n\right)^2$$

is a maximum, subject to $\mathbf{u}_l^T \mathbf{u}_k = \delta_{lk} = \begin{cases} 1 & \text{If } l=k \\ 0 & \text{Otherwise} \end{cases}$

where u_k and λ_k are the eigenvectors and eigenvalues of the covariance matrix C

5. The covariance matrix C has been obtained in the following manner

$$C = \frac{1}{M}\sum_{n=1}^{M}\Phi_n\Phi_n^T$$
$$= AA^T$$
$$A = \{\Phi_1, \Phi_2, \Phi_3, \Lambda\ \Lambda\ \Lambda\ , \Phi_n\}$$

6. To find eigenvectors from the covariance matrix is a huge computational task. Since M is far less than N^2 by N^2, we can construct the M by M matrix $L = A^TA$, where $L_{mn} = \Phi_m^2\Phi_n$
7. Find the M eigenvectos, v_l of L.
8. These vectors (v_l) determine linear combinations of the M training set finger images to form the eigenfingers u_l

$$u_l = \sum_{k=1}^{M} v_{lk}\Phi_k \qquad l = 1,2,\Lambda\ \Lambda\ \Lambda\ , M$$

After computing the eigenvectors and eigenvalues on the covariance matrix of the training images, the M eigenvectors are sorted in order of descending eigenvalues and chosen to represent eigenspace. Now the M´ significant eigenvectors of the L matrix are chosen as those with the largest associated eigenvalues. The eigenfingers span an M´-dimensional subpace of the original N^2 image space. In Many of our test cases, based on M=25 finger images of each type of fingerprint, M´ = 9 eigenfingers have been used. We have discussed the Arch type's finger print here. The number of eigenfingers of each class to be used is chosen heuristically based on the eigenvalues. The following are the eigenfinger which have been used of our system in the order of eigenvalues.

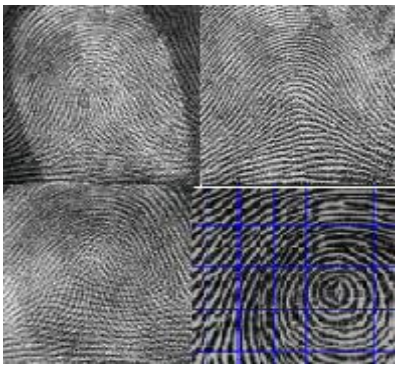

Fig. 5: Eigenfinger for the Example Image Set.

Finally, Project each of the original images into eigenspace. This gives a vector of weights representing the contribution of each eigenfinger to the reconstruction of the given image.

7. EXPERIMENTAL RESULTS AND DISCUSSIONS

The experimental results of the proposed system have shown in the Table-1 & 2. In summary of the results of the system have been identified with fingerprint individually 94% (in average), and with the facial image the accuracy was 92.75 % (in average).The proposed prototype system (integrating face and fingerprint) accuracy was 97% (in average). The system experimental results also exposed that the accuracy was decreasing with increasing of the sample trait.

The proposed multimodal biometric can provide the following characteristics and benefits

- More reliable if one of the human traits is damaged e.g., if fingerprint is not available so other trait like face can be used for identification.
- It enhanced identification performance.
- It can improve population coverage by reducing the failure to enroll rate.

Table.1: Person Identification Results

No of Person	Identification with Facial image	Identification with Fingerprint	Identification by Integrating Face and Fingerprint
50	94%	95%	98%
100	93%	95%	97%
150	93%	94%	97%
200	91%	92%	96%
Average	92.75%	94%	97%

Table.2: False Reject Rate and False Acceptance Rate Result

No of Person	False reject rate with Facial Image	False reject rate with Fingerprint	False reject rate by Integrating Face and Fingerprint	False Accept rate with Facial image	False Accept rate with Fingerprint	False Accept rate by Integrating Face and Fingerprint
50	3%	2%	2%	3%	2%	1%
100	4%	3%	3%	4%	3%	1.5%
150	5%	4%	3%	4%	3%	2%
200	6%	4%	4%	4%	3%	2%
Average	4.5%	3.25%	3%	3.75%	2.75	1.625%

8. CONCLUSION

The proposed system integrates two different biometric approaches (face recognition and fingerprint recognition) and incorporates a decision fusion module to improve the identification performance. Firstly, It has been developed a person identification system using face that uses principal component analysis or eigenface technique. Then a person identification systems using fingerprint has been developed. The system has been worked in parallel mode of operation, where information from face and fingerprint were used simultaneously to perform recognition process. In this system, the decision fusion were designed to operate at the decision level. Each biometric system were performed its own recognition decision based on its own feature vector. Conjunctive rule based methodology has been used to make the final recognition decision. Experimental results demonstrate that the system was functioning very well. The response time as well as the accuracy of the system was minimal.

9. REFERANCES

[1] L. Hong and A. K. Jain, "Classification of Fingerprint Images," 11th Scandinavian Conference on Image Analysis, June 7-11, Kangerlussuaq, Greenland, 1999.

[2] L. Hong and A. K. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 20, No. 12, pp. 1295-1307, Dec 1998.

[3] R. W. Frischholz and U. Dieckmann, "Bioid: A Multimodal Biometric Identification System", IEEE Computer, Vol. 33, No. 2, pp. 64-68, 2000.

[4] M. Turk and A. Pentland, "Eigenfaces for Recognition," J. Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, 1991.

[5] R. Chellappa, C. Wilson, and A. Sirohey, "Human and Machine Recognition of Faces: A Survey," Proc. IEEE, vol. 83, no. 5, pp. 705– 740, 1995.

[6] M. Turk, A. Pentland. "Face Recognition Using Eigenfaces". In Proc. IEEE Conf. on Computer Vision and Pattern Recognition, pp. 586-591, 1991.

[7] D. Valentin, H. Abdi, A.J. O'Toole, and G. Cottrell, "Connectionist Models of Face Processing: A Survey," Pattern Recognition, vol. 27, no. 9, pp. 1,209–1,230, 1994.

[8] A.K.M. Akhtar Hossain, "Fingerprint Identification System Using Artificial Neural Computing Models", Ph.D. Thesis, Department of Computer Science and Engineering, University of Rajshahi, Bangladesh, January 2006 .

[9] A. K. M. Akhtar Hossain & S.K. Ahmed Kamal , "An Approach To Extract Fingerprint Feature Using Grid-Mapping Technique And To Match Through BackPropagation Neural Network", Scientific Journal founded in 1997, Bulletin of Donetsk National University, 004.932.721, ISSN 1817-2237, PP-412-418, Ukraine, 2/2005 .

[10] A. K. M. Akhtar Hossain and S. K. Ahmed Kamal, "Grid Mapping Features based Fingerprint Verification System" Proceedings of 8th International Conference on Computer and Information Technology, Islamic University of Technology (IUT), Gazipur, Dhaka, Bangladesh, PP-1052-1057, ISBN 984-32-2873-1, ICCIT-2005.
[11] R. Brunelli and D. Falavigna, "Personal Identification Using Multiple Cues," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 17, no. 10, pp. 955–966, Oct. 1995.
[12] J. Kittler, Y. Li, J. Matas, and M.U. Sanchez, "Combining Evidence in Multimodal Personal Identity Recognition Systems," Proc. First Int'l Conf. Audio Video-Based Personal Authentication, pp. 327–334, Crans-Montana, Switzerland, Mar. 1997.
[13] Xiaohui Cheng, Cuina Zhang, and Maojie Zhou, "Rotation Invariant Texture Spectrum-Based Image Retrieval Algorithm", IEEE 2nd International Conference on Software Engineering and Service Science (ICSESS), Pages: 602 - 605, 2011.
[14] Jinfeng Yang and Xu Zhang, "Feature-Level Fusion of Fingerprint and Finger-Vein for Personal Identification", Pattern Recognition Letters 33, Pages 623–628, 2012.
[15] AK Jain, K Nandakumar, A Nagar, in Security and privacy in biometrics. Fingerprint Template Protection: From Theory to Practice (Springer London), pp. 187–214, Year 2013.
[16] Ahmed M. Hamad, Rasha Salah Elhadary, Ahmed Omar Elkhateeb, " Multimodal Biometric Identification Using Fingerprint, Face and Iris Recognition", International Journal of Information Science and Intelligent System, 3(4): 53-60, 2014.
[17] Subhas Barman, Debasis Samanta and Samiran Chattopadhyay, Fingerprint-based crypto-biometric system for network security, EURASIP Journal on Information Security, 3 April 2015.
[18] Ashraf Aboshosha, Kamal A. El Dahshan, Eman A. Karam, Ebeid A. Ebeid, Score Level Fusion for Fingerprint, Iris and Face Biometrics, International Journal of Computer Applications, Volume 111 - Number 4, Year of Publication: 2015.