Development of a New Framework for Enhancing Security in Fingerprint and Finger-Vein Multimodal Biometric Authentication Systems

Richa Jani
Student
College of Technology and Engineering
Udaipur

Dr. Navneet Agrawal
Associate Professor
College of Technology and Engineering
Udaipur

Dr. Sunil Joshi
Professor
College of Technology and Engineering
Udaipur

ABSTRACT
A biometric is a unique feature, a measurable trait or characteristic which is utilized in automatically identifying or verifying the identity of a human being. An assortment of inevitable shortcomings has been faced by unimodal biometric recognition like Limited discriminability, noisy biometric data, Upper bound in performance and Lack of permanence, consequence dilapidation of exactness and performance of the system. Multimodal biometrics consolidates the two or more biometric features into a single detection. Problems transpired in unimodal recognition can be alleviated by using multimodal biometric systems that fuse evidence from scores of multiple biometric systems and characteristically provide better recognition as compared to unimodal biometric systems. Biometric authentications exploit inimitable combination of measurable physical Characteristics- fingerprint, finger vein features, voice print, iris of the eye, and so on- that cannot be willingly imitated or forged by others.

This paper proffers the match score level of fusion with feature extraction that can be espoused to consolidate the scores attained by fingerprint and finger-vein and new technique fusion with alignment that are credible and the integration strategic that can be espoused to overlapped the features attained by fingerprint and vein.

Fusion techniques include processing biometric modalities successively until an adequate match is obtained.

Keywords
Fingerprint, finger-vein, multimodal biometrics, score level fusion, fusion with alignment

1. INTRODUCTION
Necessitate for consistent user verification methods has augmented in the wake of heightened concern about security and hasty advancements in communication, networking and Mobility. Biometrics is an automated method of recognizing a person, based on physiological or behavioral assets. Physiological biometrics is based on measurements and data collected from direct measurement of a part of the human body. Fingerprint, retina-scan, iris-scan, facial recognition and hand geometry are physiological biometrics. Behavioral characteristics are based on an action got by a human being. Voice recognition, signature-scan and keystroke scan are most important behavioral biometric technologies.

Generally biometric authentication system consist of five major components namely, sensor, feature extractor, template database, matcher, and decision unit .Sensor works as a interface between the user and the authentication system which is used to scan the biometric trait of the user. The scanned biometric data is processed by the feature extractor module to extract the feature sets. The extracted feature set is stored in a database as a template by the user‘s uniqueness information in enrollment phase. The matcher module accepts two biometric feature sets from template and query, respective as inputs and provides a match score signifying the similarity between the two sets. Finally, the identity decision is taken by the decision module [6].

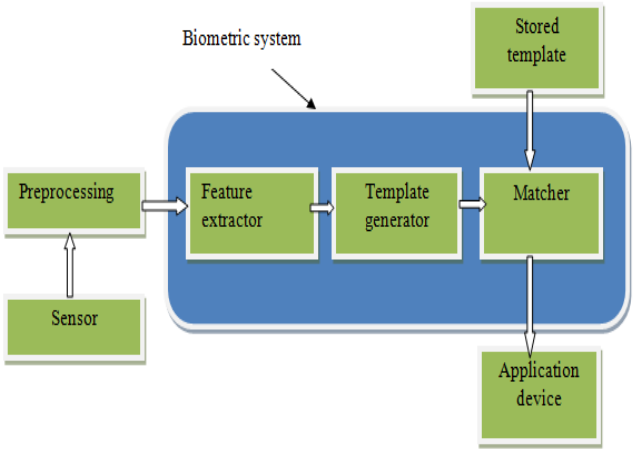


Fig 1. Block diagram of general biometric system

An variety of predictable limitations has been faced by unimodal biometric recognition like Limited discriminability, noisy biometric data, Upper bound in performance and Lack of permanence, consequence dilapidation of performance and correctness of the system.

In order to overcome these problems and to accomplish better recognition performance multimodal biometric systems has been developed which combined various sources of biometric information.

Multibiometric systems depend on representing each client by multiple sources of biometric information [11]. Based on the nature of these sources, a multibiometric system can be classified into one of six categories, Multi-algorithm systems, Multi-sensor systems ,Multi-instance systems, Multi-sample systems, Hybrid systems and Multimodal systems Hybrid systems[12]. The technique for implementation of this kind of systems requires the use of information fusion theory. There are three major fusion techniques: fusion at the feature extraction level, matching score level, and decision level.

To enhance the system performance of multimodal biometrics system this paper spotlightes on recognition of fingerprint and finger-vein at score level fusion (sum rule method) and introduce a general framework for the individual's authentication based on fusion with alignment method where minutiae obtained from each individual biometric feature will be fused together such that at least one or two minutiae will be overlapped.

The formation of this paper is as follows. In section II we elucidate multimodal biometrics system that is used in our work. In section III, Proposed method is enlightened. In section IV experimental results are publicized. Finally, the conclusions of this paper are exposed in section V.

2. MULTIMODAL BIOMETRIC SYSTEM

In order to overcome these problems and to accomplish better recognition performance multimodal biometric systems has been developed which combined various sources of biometric information.
The technique for implementation of this kind of systems requires the use of information fusion theory. There are three major fusion techniques: fusion at the matching score level , feature extraction level and decision level.

In this paper, the fingerprint and finger-vein biometric traits are selected to erect multimodal biometric system, because fingerprint recognition is one of the most well known and published biometrics and fingerprint consists of ridges (lines across fingerprints) and valleys (spaces between ridges). The pattern of the ridges and valleys is unique for each individual whereas vein pattern is an internal structure of finger so it provides a very high accuracy rates.

2.1 Fingerprint Recognition

Fingerprint-based identification is the oldest method, which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. The major minutiae points in fingerprint are: ridge ending, bifurcation, and short ridge or dot. [13]

The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges or dots are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

Fingerprint recognition mainly contains image preprocessing, feature extraction, matching. In order to extract fingerprint minutiae accurately, we do a series of pre-processing. Fingerprint matching based on point pattern can be approached in two stages. In the first stage, two matching fingerprints should be aligned by finding rotation and translation parameters of the two fingerprints. In the second stage, aligned fingerprints will be matched [3].

2.2. Finger-Vein Recognition

The finger veins structures are hidden; it is enormously tricky to filch the finger-vein patterns of an individual without their knowledge, therefore offering a high extent of privacy. Second, finger-vein biometrics exploits to offer strong ant spoofing competence as it can also ensure liveness in the existing fingers during the imaging[8].

Fingerprint systems, but adapted to the own characteristics of vein patterns [10]. The image of vein shown below:

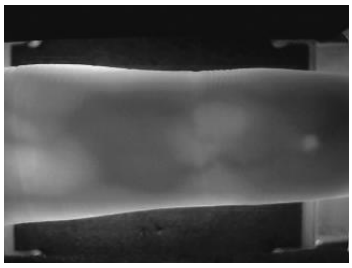


Fig 2. Finger vein

3. PROPOSED FRAMEWORK

Multimodal Biometrics System robustly depends on the application circumstances and refers to the use of a grouping of two or more biometric traits in an identification system. The proposed system espoused identification based on multiple biometrics represents a promising trend of an individual, to recognize the identity. The most convincing reason to merge different modalities is to enhance the recognition rate.

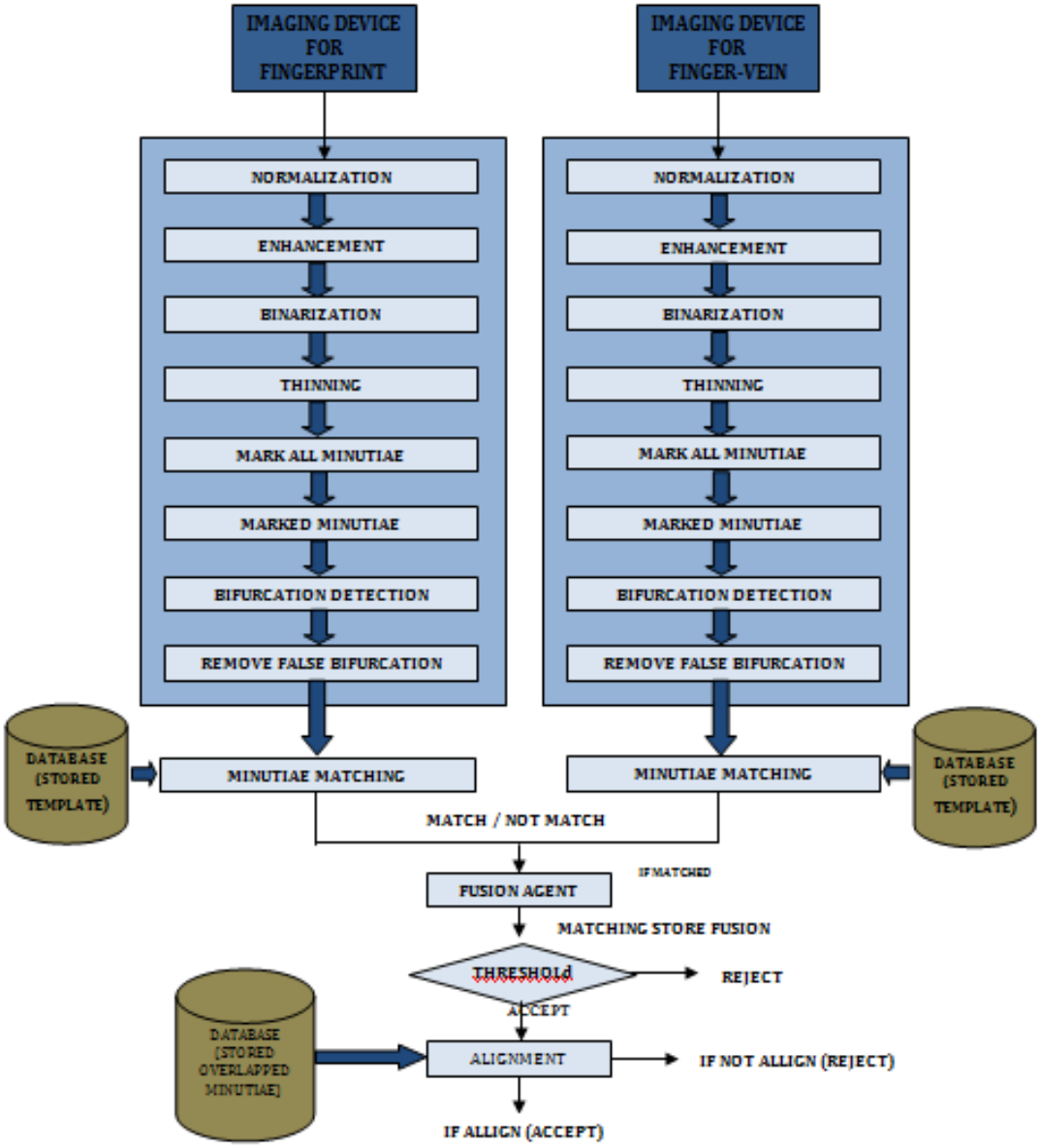


Fig 3: Proposed Method

In This pattern the two templates extracted from the fingerprint and vein pattern are stored in a database in the enroll phase. In the identification phase, the templates are extracted from the finger and vein, matched with entries in the database to accept or reject the individual.

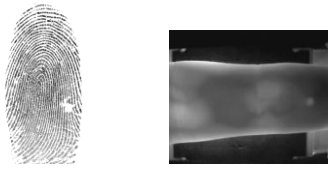
For Matching Score calculation, number of correctly matched corner points for two images are considered. Total number of correctly matched points for a pair of images is taken as matching score for that pair. In decision making there will be one more threshold for combined matching score for two fingers and vein. If matching score is more than the threshold that pair will be chosen as matched pair and authentication will granted.

3.1 Score Level Fusion

The inputs to the matchers are fingerprints and finger-veins images, joined with the identity claimed by the subject to be authenticated. Matching scores are independently computed by the individual's fingerprint and finger-vein matchers. Then, their scores are normalized. A suitable score-level fusion rule is applied to the normalized scores. Finally, the commonly adopted threshold-based decision is made: if the combined score exceeds a fixed acceptance threshold, The subject is classified as a "genuine user" (the claimed identity is "verified") otherwise he/she is classified as an "impostor".
In this paper the simple weighted fusion is used as a score fusion approach and the fusion scores (S) is computed as follows,

$$Z = M1\ Z1 + M2\ Z2 \qquad (1)$$

Where Z1 and Z2 are fingerprint matching score and finger vein matching score, M1 and M2 are their weights, Z is the fusion score. The weights Z1 and Z2 are varied over the range [0, 1], such that the constraint M1+M2=1 is satisfied.



Fingerprint Finger-vein

Fig 4: Fingerprint and finger-vein of one finger

3.2 Proposed Method (Fusion with Alignment)

- We have proposed one more authentication step that is alignment method to enhance the security as well as recognition rate. Alignment can be done using rotation and translation techniques .First minutiae obtained from fingerprint and finger-vein are fused together such that at least one or two minutiae will be overlapped by using rotation and translation method and the information (angle, left and top movement) about this overlapping stored in database.
- Query images will overlap with the help of database information. If they overlapped then matching occurs and high level security is found to determined real or fake user. The proposed system's performance is determined its accuracy. The main widely used standard metrics to determine the accuracy of a system are:
  - False accept rate (FAR)
  - False reject rate (FRR)
  - Genuine acceptance rate (GAR)

4. IMPLEMENTATION AND RESULTS

This research work is implemented with the help of MATLAB R2012a. In this research work first both the fingerprint and finger-vein recognition is done with minutiae extraction and then matching scores are consolidated together to get the multimodal biometrics. Further alignment also has been done to enhance the result of proposed work.

Table 1.Comparison of Fusion Recognition Rate

M1	M2	Fusion recognition rate(%)
0.90	0.10	90
0.80	0.20	91
0.77	0.23	92
0.70	0.30	94.15
0.66	0.34	96.20
0.60	0.40	96

4.1 False Accept Rate (FAR)

The false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts. [14]

4.2 False rejection rate (FRR)

The false rejection rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. FRR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts. [14]

4.3 Equal error rate (EER)

Equal error rate is the value at which false rejection rate and false acceptance rate is approx equal.

4.4 Genuine acceptance rate (GAR)

The Genuine Acceptance Rate is depending on FRR. As FRR increases GAR decreases and vice-versa. The GAR value can be determined as –

$$GAR=100–FRR \quad (2)$$

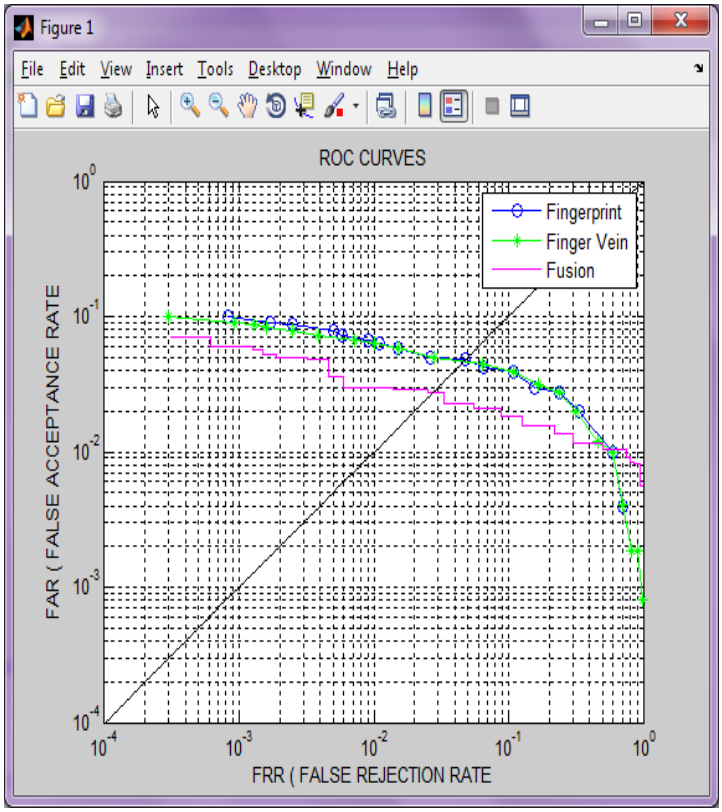


Fig 5: ROC curves (Fusion method)

Table 1 shows the recognition rate of multimodal biometric authentication based on the score fusion of fingerprint and finger vein when M1 =0.66 and M2=0.34, along with the recognition rate of single biometric including fingerprint recognition and finger vein recognition. The receiver operating curve of score fusion, along with the receiver operating curve of fingerprint recognition and finger vein recognition are plotted in Figure 5.

Table 2. Fusion with alignment (FAR andFRR values)

Dataset	FAR(False acceptance rate)	FRR(False rejection rate)
1	0.8	0.0023
2	0.5	0.0023
3	0.1	0.0026
4	0.05	0.0078
5	0.002	0.0131
6	0.0019	0.026
7	0.0018	0.052
8	0.0015	0.078
9	0.001	0.1184

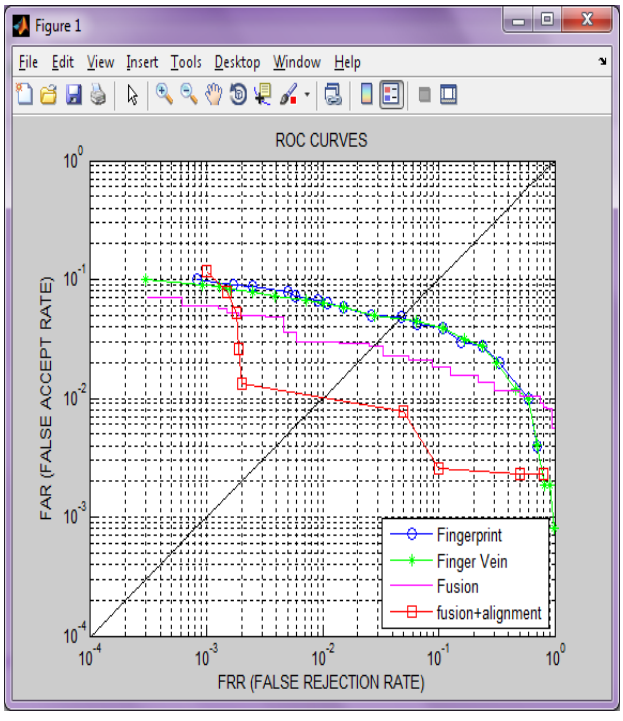


Fig 6:ROC curve((proposed(fusion+alignment) method)

To summarize the matching performance using ROC (Receiver Operating System), we have plotted the False Rejection Rate (FRR) against the False Accept Rate. Here, we have shown four different results as only for fingerprint image, only for finger vein image, fusion of both fingerprint and finger vein image and the proposed work i.e. fusion with alignment. As expected fusion with alignment method leads to significant improvement in the performance. We obtained equal error rate 1.80% which results in 98.2% genuine acceptance rate (recognition rate) which is quite enhanced thansimple score level or feature level fusion.

We can conclude from these results that the integration of fingerprint and finger vein leads to an improvement in recognition performance.

Table 3. comparison between the proposed method and previous fusion method

Method	GAR(Genuine acceptance rate %)	FAR(False acceptance rate %)	FRR(False rejection rate %)
Fusion (feature level)(yang,y. *et al.* 2012)	**95.81**	**2.52**	**6.78**
Matchscorelevel(Yongming, y. *et al.*2012)	**93.50**	**5.33**	**6.92**
Fusion(Score level)	**98**	**3.34**	**5**
Fusion(score level)+alignment(proposed)	**98.2**	**2.232**	**3.125**
Fusion (feature level)(yang,y. *et al.* 2012)	**95.81**	**2.52**	**6.78**

Table 3 shows that the proposed method fusion+alignment gives better accuracy than existing technique but apart that there are various limitations in proposed method in current scenario that there will be increase in code complexity with respect to time as well as cost of thesystem. A large circuit area is required to implement on hardware. Further this recognition rate will increase by using dynamic weight fusion+alignment technique.

5. CONCLUSION

Several of the problems present in unimodal systems are gracefully addressed by the multimodal biometric systems by merging multiple sources of information. In multimodal systems an assortment of fusion levels and scenarios are feasible. Match score level fusion is most efficient due to easy in accessing and consolidating matching scores. The proposed method added one more authentication stage (fusion with alignment) to provide better security than existing system. In many applications such as border entry/exit, general recognition, access control and network security, multi-modal biometric systems are looked to as a means of (a) if sufficient data cannot be attained from a given biometric sample, providing a secondary means of enrollment, verification, and identification and (b) plummeting false acceptance and false rejection, (c) combating attempts to spoof biometric systems through non-live data sources such as fake fingers. The performance of proposed multimodal biometric system shows great assurance to individual identity in the biometric authentication society.

This paper proffers the score level of fusion with feature extraction that can be espoused to consolidate the scores attained by fingerprint and vein and new approach fusion with alignment that are credible and the integration strategic that can be espoused to overlapped the features attained by fingerprint and vein.

We have proposed an efficient minutiae extraction algorithm for fingerprint recognition as well as finger-vein recognition. The proposed method is predominantly efficient for verifying low-quality fingerprint images that could not be recognized appropriately by conventional techniques and attained 98.2% accuracy whereas unimodal biometric system such as fingerprint identification system produces 96%.and match score level fusion produces 98%.

6. REFERENCES

[1] Miura, N. , Nagasaka, A. and Miyatake, T.2004. Feature extraction of finger vein patterns based on repeated line tracking and its application to personal identification. 194–203.

[2] Kaur, M.,Singh, M.,Girdhar, A.and Sandhu,P.S. 2008.Fingerprint Verification System using Minutiae Extraction Technique. World Academy of Science, Engineering and Technology . 497-502 .

[3] Feifei, C. and Gongping, Y. 2011.Score Level Fusion of Fingerprint and Finger Vein Recognition. Journal of Information Systems . 5723-5731.

[4] Kang, B.J.andPark,K.R.2010.Multimodal biometric authentication based on the fusion of vein and geometry of single finger. The Institution of Engineering and Technology .209-217..

[5] Aboalsamh,A.H.2011. a multi biometric system using combined vein and fingerprint identification. international journal of circuits, systems and signal processing.29-36 .

[6] Garje, P.D.and Agrawal,S.S 2012. Multibiometric Identification System Based On Score Level Fusion. IOSR Journal of Electronics and Communication Engineering (IOSRJECE)**.** 07-11.

[7] Marcialis,G.L. and Roli,F. Score-level fusion of fingerprint and face matchers for personal verification under "stress" conditions.

[8] Gowtham,P.,Sindhu,C.,Sudheer Kumar,Chandra Sekhar, and Abdullah , M.S.2013.identification of finger images using score-level fusion.international journal of engineering science invention . 12 -23.

[9] yadav,S.S, Gothwal ,J.K.and R.Singh2011. Multimodal Biometric Authentication System:Challenges and Solutions.Global Journal of Computer Science andTechnology..

[10].Antonio, J.U., Hartung, d.,Pascual, j.e.s and R.S.Reillo, **"**vascular biometrics based on a minutiae extraction approach".

[11] O.M. Aly,H.M. Onsi,G.I. Salama,and Mahmoud, T.A.2012. multimodal biometric system using iris, palmprint and finger-knuckle. International Journal of Computer Applications . 1-6.

[12] Xiangy,W.,.DesaiyPaul,afengWangz,and Peng T.A Prototype Biometric Security Authentication System Based Upon Fingerprint recognition.

[13] Kekre,H.B.,Thepade,H.D., Maloo.A.Eigenvectors of Covariance Matrix using Row Mean and Column Mean Sequences for Face Recognition.International Journal of Biometrics and Bioinformatics (IJBB). 42-50.

[14] Ajay Kumar, and Yingbo Zhou2012. Human Identification Using Finger Images. IEEE Transactions on Image Processing.

[15] Ross,A., Nandakumar,K. and Jain.A.K. 2006. Handbook of Multibiometrics. Springer, New York, USA, 1st edition, 2006.