A MULTI-MODAL BIOMETRIC SYSTEM COMBINING FACE AND IRIS

Radhika Sarmokaddam
M Tech II (Computer Sci.)
Yashavantrao Chavan College of Engineering
Nagpur, 441110, Maharashtra
Email:sarmokaddamradhika@gmail.com

Prof. Praful Barekar
(Deptt. of Computer Technology)
Yashavantrao Chavan College of Engineering
Nagpur, 441110, Maharashtra
Email:praful.barekar20@gmail.com

Abstract :

Multimodal biometric systems are considered the simplest way to reduce the constraints raised by single traits. In our system, we've got developed an algorithm that extracts the features from face and iris for person authentication. Face is one among the foremost widely used biometric features due to its ease of capture on the other hand iris recognition is one among the foremost accurate biometric modalities having verification results near 98%. Human faces and irises are often considered as important biometric traits in many applications like airport management boards, criminal investigation. Additionally, since the face and iris modalities are acquired at the same time using constant camera, the proposed theme is motivated to construct a sturdy multimodal biometric system. so the proposed theme can be applied much in individual and multimodal face-iris recognition systems by extracting facial features and then fusing them with iris patterns. For the extraction of face feature we are exploiting local Binary Patterns (LBP) approach. The iris features are extracted using Daugman's Gabor filters based approach. Exploiting this info, we've got developed a multi-modal (combining face and iris) system based on score level and decision level fusion to efficiently fuse face and iris modalities.

Keywords— Authentication, Biometrics, Fusion levels, Multimodal biometric systems, Recognition methods

1. INTRODUCTION

A. Biometrics

The system that automatically identifies and authenticates the user based on their behavioral and biological characteristics is termed as biometrics [1], [2]. Some examples of biometric characteristics are fingerprint, iris, face (2D and 3D), retina, palm print, hand veins, ear, DNA, voice, signature, gait, typewriting patterns, etc. These characteristics are denoted as biometric traits or modalities. Since the biometric traits are intrinsically guaranteed to the person, they'll be used to establish his identity with high degree of confidence. A classical biometric system involves 2 distinct phases: enrollment and recognition/comparison. during enrollment, biometric info (such as fingerprint image or voice data) is captured by exploiting specific sensors. This info is processed using exclusively designed algorithms to get important features. These features are used to produce a reference biometric template for the user. The features could also be depicted as a fixed dimension feature vector (e.g., iris code), or a feature set of variable dimension (e.g., fingerprint minutiae). This reference biometric template is needed at the time of authentication for comparison purposes and hence, the biometric templates for all such registered users are keep in a central template info for more comparisons. At the time of recognition/comparison, a recent sample of the biometric measurement is captured and similar method, up to obtaining applicable features, is followed. These options are compared with the stored templates.

Typically, biometric systems will operate in 2 characteristic modes:
(a) Recognition mode – wherever the system answers the question, 'who is the client?'
(b) Authentication mode – wherever the system answers the question, 'is the user truly who he's claiming to be?'
In another word, during recognition, the information extracted from the recent biometric knowledge is compared with all the stored templates and therefore the identity of the person to which the biometric data belongs is decided. In authentication, the one who needs to get verified provides his identity along with his biometric information. A one-to-one comparison is carried out between the knowledge} extracted from the recent

biometric data and therefore the stored template similar to the provided identity and therefore the results of this comparison is either accepted or reject. A central template database is needed for a recognition system because all the templates are required during the process of comparison. The foremost important advantage of biometry over the strategies is that it cannot be stolen, misplaced or forgotten. Moreover, it's difficult to spoof biometric traits, due to greater accurateness and higher robustness of biometric recognition. Biometric solutions become admired and preferred ways to analysis individual characteristics for security – recognition and authentication - purpose. It could not be duplicate or imitated and abused.

B. Multi-Biometrics

Biometric fusion incorporates a history of over thirty years. Over one biometric come together to analyze high performance multi-biometric recognition system. Multi-biometrics has focused on some issues associated with unimodal this create its some advantages over unimodal biometry like recognition accuracy, privacy and biometric information enrollment.

Recognition accuracy: Its accuracy is best as compared to the unimodal biometric system [21]. The multi-biometric system is predicted to be additional accuracy and reliableness because of the multiple, biometric traits independency and hard to forge all of them [19, 18]. Because the combination of every of the biometric identifiers offers some additional proof regarding the genuineness of an identity claim, one will have additional confidence within the result. As an example, 2 persons might have the similar signature patterns; in this case, the signature verification system can produce large FAR for that system. Addition of iris recognition system with the signature verification system might solve the matter and minimizes the FAR [17]. Experiments have shown that the accuracy of multimodality will reach close to 100% in identification.

Privacy: Multimodal biometric systems increase opposition to certain kind of vulnerabilities. It checks from stolen the templates of biometric system as at the time it stores the 2 characteristics of biometric system within the info [22]. As an example, it might be additional challenge for offender to spoof many alternative biometric identifiers [17]. Further, once 2 or additional modalities are used for authentication, it results in become difficult to spoof the biometric system.

Biometric data enrollment: Multimodal biometric systems will tackle the matter of non-universality. Just in case of inconvenience or poor quality of a selected biometric data, alternative biometric identifier of the multimodal biometric system is used to capture data. As an example, a face biometric identifier is used in a multimodal system (involves fingerprint of general labors with many scars within the hand) [17]. Multi-biometric system additionally addresses the matter of noisy data effectively (i.e. sickness affecting voice, scar affecting fingerprint). They permit indexing or filtering of huge biometric databases, and is robust to noise. Thus, it provides universal coverage and improves matching accuracy [16, 18, 23].

Multi-biometric systems have 2 basic categories: synchronous and asynchronous. In synchronous, 2 or additional biometry combined within one authorization method. On the other hand, asynchronous system uses 2 biometric technologies in sequence (one after the other) [24]. Multimodal biometric systems will operate in 3 completely different modes [19];

- *Serial Mode (cascade mode)* – Every modality is examined before subsequent modality is investigated. The overall recognition period is minimized, because the total number of possible identities - before using subsequent modality - can be reduced.
- *Parallel Mode* – sensed/captured data from multiple modalities are utilized in simultaneous way to perform recognition. Then the results are combined to create final judgment.
- *Hierarchical Mode* – individual classifiers are combined during a hierarchy -tree like- structure. This mode is most popular once an oversized range of classifiers are expected.

Depending on the sources of information, the multi-biometric system can be called as [3]:

- *Multi-sensor systems:* The information of identical biometric obtained from completely different sensors are combined for all. For instance, opposite information associated with fingerprints are often gain using different kinds of sensors (like optical and capacitive sensors). Data obtained is then integrated using sensor level fusion technique [16].

- *Multi-modal systems:* More than one biometric attribute is used for user identification. For instance, the data obtained using face and iris options or different are often integrated to determine the identity of the user [24].
- *Multi-instance systems:* Multiple instances of one biometric attribute are captured. As an example, pictures of the left and right irises are often used for iris recognition. If one device is used to accumulate these pictures during a consecutive manner, the system are often created very price effective, because it doesn't need multiple sensors. Moreover, it doesn't integrate extra feature extraction and matching components [20].
- *Multi-sample systems:* Multiple samples of a same biometric attribute are used for the enrollment and recognition. As an example, together with the frontal face, the left and right profiles are captured. But, it needs multiple copies of sensors, or the user might wait a longer period of time to be detected or a mixture of each [16].
- *Multi-algorithm systems:* Multiple totally different approaches to feature extraction and matching algorithms are applied to one biometric attribute. But, these are additional complicated due to application of various algorithms [19].
- *Hybrid systems:* It is a system that integrates over one of the above mentioned multi-biometric systems. As an example, 2 face recognition algorithms are often combined with 2 iris recognition algorithms. Such systems are going to be multi-modal and multi-algorithmic system.

The problem of combination of information presented by multiple biometric sources from any of the types mentioned above is known as information fusion. Multimodal biometric fusion combines the differentiated aspect from different biometric traits to support the advantages and minimizes the shortcomings of the individual aspects [19]. The first drawback of information fusion is to choose the type of information that ought to be united and also the choice of technique for fusion. In multimodal biometrics, the fusion scheme may be classified as[3]:

- Sensor Level – information coming from different sensors is combined.
- Feature Level – the biometric information extracted in the form of features is combined.
- Score Level – match scores of individual biometric comparisons are combined.
- Decision Level – the results of individual biometric comparisons are combined.
- Rank Level – when the output of each biometric system is a subset of probable matches (i.e., identities) arranged in decreasing order of confidence, the fusion can be done at the rank level. This is appropriate in a recognition system where a rank may be assigned to the top matching identities.

C. Literature Review

Multimodal systems combine the evidence given by totally different body traits for establishing identity. For instance, some of the earliest multimodal biometric systems utilised face and voice features to establish the identity of an individual (Brunelli and Falavigna [4]). Physically uncorrected traits (e.g., fingerprint and iris) are expected to lead to better improvement in performance than correlate traits (e.g., voice and lip movement).

Because of these reasons, we opted for combination of face and iris. Iris is known to possess very high recognition accuracy. Since our focus is on combining face and iris, thus we tend to focused on such literature only. Some of the systems doing face-iris combinations are represented below.

The fusion of face and iris modalities may be a biometric approach that has gained increasing attention over the past decade, likely because of the popularity of the individual modalities, similarly because the natural connection between them. Despite this recent trend, only a few studies are done on fusion of face and iris biometry from a single device.

The most common methodology of multi-biometric fusion is score-level fusion. Zhang et al. [5] approach the problem of fusing face and iris biometry under near-infrared lighting using a single sensor device. Frontal face images are acquired using a ten megapixel CCD camera. The eigenface algorithm and Daugman’s algorithm are used to perform face and iris recognition, respectively, and score-level fusion is accomplished via the sum and products rules after min-max normalization. Various different score-level fusion approaches are tested on chimeric datasets. chen and Te Chu use an unweighted average of the outputs of matchers based on neural networks [6]. Wang et al. [16] test weighted average, linear discriminant analysis, and neural networks for score fusion.

Another common approach to biometric fusion is feature level fusion through concatenation. Rattani and Tistarelli work out SIFT features for chimeric face and iris images and concatenate the resulting feature vectors [7]. the quantity of matching SIFT features between 2 vectors (measured by euclidean distance) is used as a match score for that comparison. Son and Lee extract features for face and iris images based on a Daubechies wavelet transform [8]. Concatenation is used to make a joint feature vector, and euclidean distance between feature vectors are used to generate match scores.

Eskandari and Toygar [9] given an iris-face combination system within which they used LBP for face and Linear Discriminant Analysis feature for iris. They provided in depth experimental results to prove the effectiveness of combining iris with face. However, their focus is on score level fusion and various score normalisation techniques.

Score normalisation is one of the necessary aspects of the fusion. an intensive review of various score normalisation strategies is given by jain et al. [10]. An intensive review of multi-biometric systems generally is often found in Mane and Jadhav [11]. Awalkar, Kanade, Jadhav and Ajmera [25] given the approach Multi-modal with Multi-algorithmic to create sturdy system but it becomes difficult because of application of various algorithms and it becomes expensive in terms of time and hardware price as it uses multi modal.

2. MULTI-MODAL SYSTEM COMBINING FACE WITH IRIS

As seen earlier, combining more than one biometric modalities will have several benefits. In this section, we proposed a multi-modal system. In our proposed system we choose the operation in serial mode due to its advantage - the overall recognition period is minimized, because the total number of possible identities - before using subsequent modality - can be reduced. we use the multi-biometric system in terms of multi modal system (combining face and iris) because of possible User Inconvenience means when multiple identifiers have to be compelled to be provided users need to wait for it and if we combine face and iris the waiting time of user ought to reduced. Face & Iris biometrics can be proposed as a closed to best multimodal system. universality is high in each the cases, collectability is high and medium for face and iris respectively, acceptability is high just in case}} of face and low in case of iris & circumvention is high within the face whereas there in no probabilities of circumvention in case of iris, so that they are compliment of one another, that's why they will creates a extremely accurate fusion.

Multimodal biometric fusion combines the differentiated aspect from different biometric traits to support the benefits and minimizes the shortcomings of the individual aspects. The aim of fusion is to formulate the correct function that may optimally combine the data provided by the biometric subsystems. In our approach we tend to use both rank level and score level fusion.

A. Feature Extraction from Face Image using Local Binary Patterns (LBP)

For extracting features from face image, we are using the Local Binary Pattern (LBP) histogram approach first proposed by [17]. The local binary patterns capture local face features. The LBP operator shown in Fig. 1 is centred at every pixel in the image. The centre pixel value acts as a threshold and the surrounding eight pixels are binarized. The binary values are taken in clock-wise manner to form an 8-bit number which is then converted to an integer and placed at the centre pixel's location. In this way, we obtain a new image called LBP image. The LBP image is then divided into blocks and histograms of these blocks are calculated. These histograms are concatenated to form a single feature vector. If the binary number has maximum of 2 transition from 0 to 1 or 1 to 0, then it is called uniform LBP. There are only 58 such values for 8-bit numbers. Other values are replaced by a constant number. Thus there are only 59 possible values in the LBP image. Therefore the total feature vector length is equal to the total number of blocks*59. For face recognition, LBP histogram features of two images are compared using the Chi square distance metric shown in Equation (1).

$$X^2(X,Y) = \sum_{i=1}^{n} \frac{(xi - yi)^2}{(xi + yi)} \qquad (1)$$

Here $X = \{x1, x2, ..., xN\}$ and $Y = \{y1, y2, ..., yN\}$ are the feature vectors and N is their dimension. Nearest neighbour classifier can be used to take the accept/reject decision.

ISSN 2229-5518

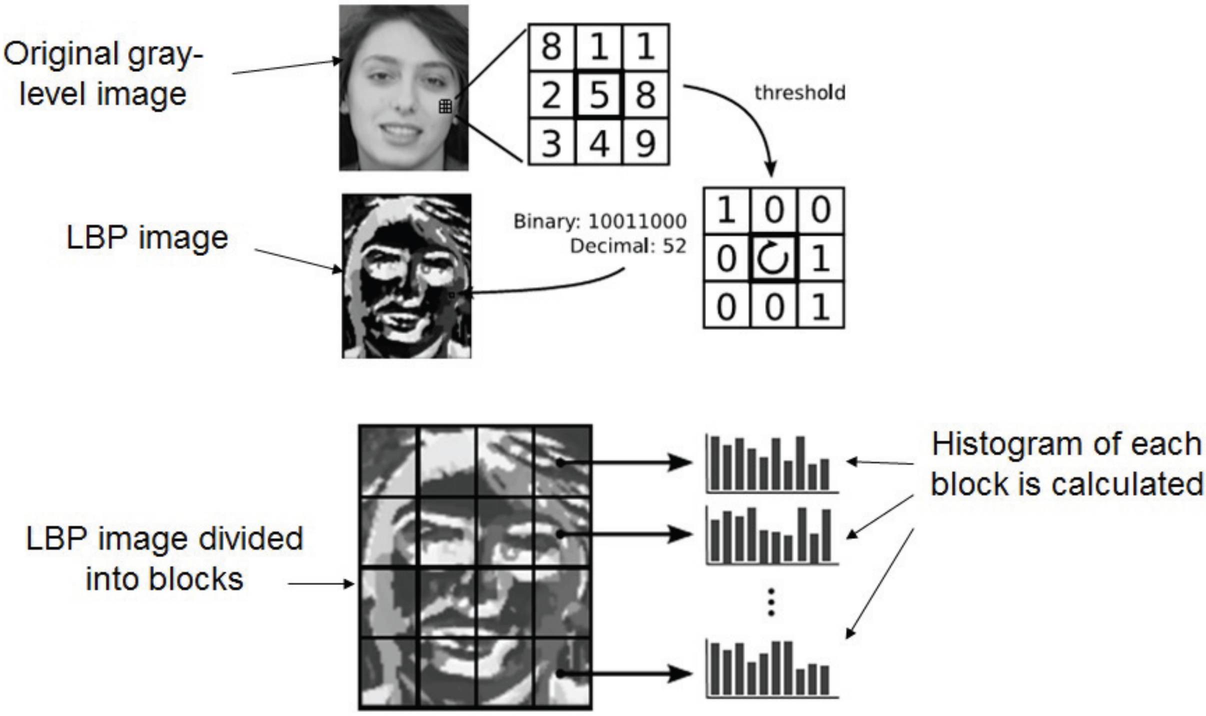
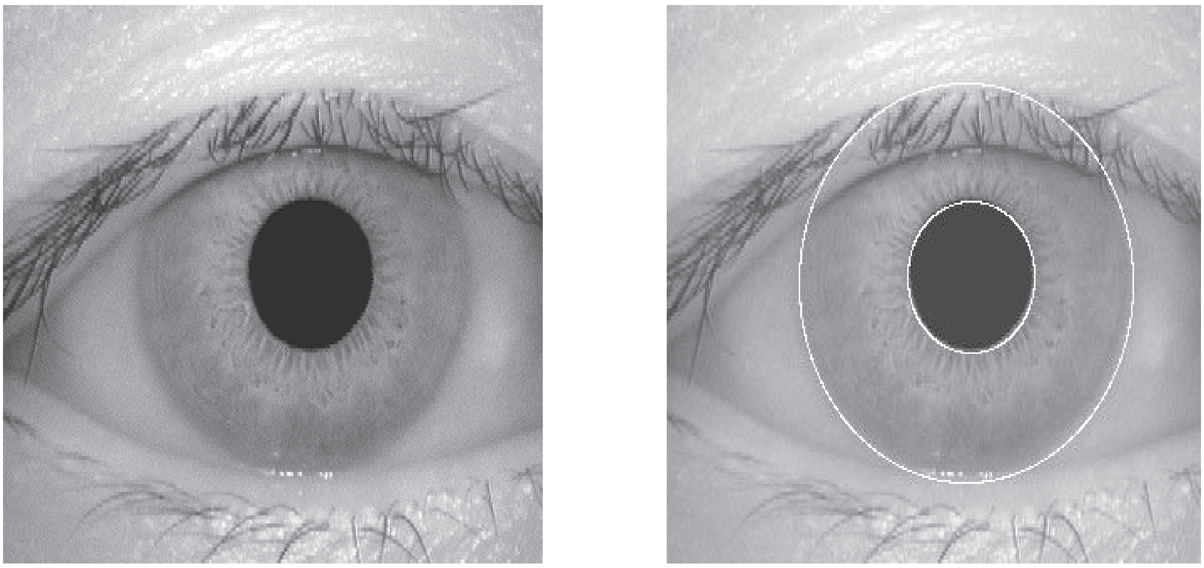


Fig.1. Basic diagram showing the steps of a facial image using LBP (image taken from [15]).

B. **Feature Extraction from iris using Daugman's algorithm**

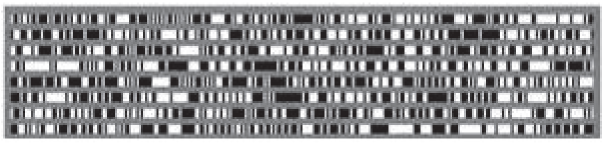
Daugman's algorithm is used for extracting binary iris code features from iris images. Figure 2 shows an iris image at different processing levels. We have taken Libor Masek's implementation [12] of this algorithm as a starting point. The circular iris region first needs to be detected correctly using a process called iris segmentation. The segmented circular iris region is then converted into a rectangular image of fixed size using Daugman's rubber sheet model [13], [14]. Generally, the size of the normalized images is 240 × 20 pixels. The normalized image is decomposed using Gabor filters and phase information from the decomposed images is binarized and concatenated to form a one-dimensional binary iris code.



(a) raw iris image (b) segmented iris image

ISSN 2229-5518

(c) normalized iris image



(d) binary features code extracted from normalized image

Fig. 2. Illustration of processing of an iris image: (a) raw iris image, (b) segmented iris image, (c) normalized iris image, and (d) binary features code extracted from normalized image[25]

The iris codes obtained from the reference and test iris images are compared using the normalized Hamming distance. The normalized Hamming distance formula is as shown in Equation (2). The range of this Hamming distance is between (0,1).

$$\text{Normalized Hamming distance} = \frac{(\text{code } A \Theta \text{code } B)}{(code\ A)} \qquad (2)$$

C. Proposed Methodology for Face and Iris Biometrics

Figure 3shows a block diagram depicting the proposed approach with the fusion method for face and iris.

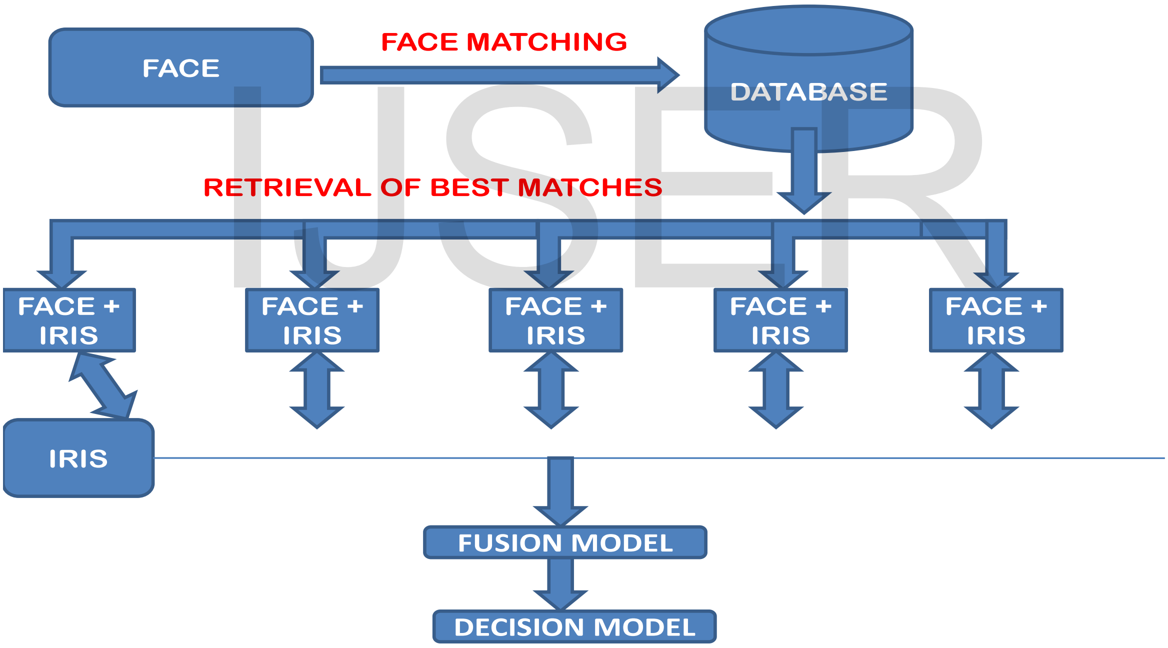


Fig.3. Block Diagram of Proposed Approach

The templates in case of score level fusion are stored independently. At the time of recognition, fresh biometric data from an individual is captured; features/templates are extracted from the data individually and compared with the respective stored templates. The comparison scores obtained from these individual comparisons are then combined using weighted sum technique using formula shown in Equation (3).

$$\text{Final score weighted} = \alpha 1 \text{score1} + \alpha 2 \text{score2} \qquad (3)$$

In equation (3), score1 and score2 are the comparison scores of iris and face respectively and α1 and α2 are the weights applied for iris and face respectively. If α1 > α2, then it means iris is given more weight than face and vice versa. Note that, α1 + α2 = 1. However, a difficulty with score level fusion is that the range of scores of various biometric data is not uniform. For example, the distance between two iris samples is calculated using normalized Hamming distance and therefore, it is in the range of (0,1). On the other hand, the face LBP feature

ISSN 2229-5518

vectors are compared using Chi square distance. Both of these distance outputs are not in any standard range. Therefore, before using score level fusion, it is required to perform score normalization so that all the scores to be combined are in a standard range. There are multiple methods for score normalization as described in [10].

So to avoid the score normalization time, in our system, we combined the rank level and score level fusion. The experimental details are given in the next section.

3. EXPERIMENTAL EVALUATION AND RESULTS

A. Performance analysis of Biometric Systems

The biometric systems used in this work generate feature vectors which are compared using various distance metrics. The binary feature vectors obtained from the reference and test biometric samples are compared using the normalized hamming distance. The LBP face features are compared using the Chi square distance. In general, if the 2 feature vectors are extracted from images belonging to the same person (genuine comparison), the distance between them is close to minimum. On the other hand, if the feature extracted are from totally different persons (impostor comparison), then the feature vectors are like random and disagree by a large distance. Comparison with a threshold value results in an accept/reject decision. There may be 2 errors within the decision process: false acceptance when an pretender is accepted and false rejection when a real user is rejected by the system. The performance of a biometric system may also be summarized with one number, where the FAR=FRR, this point is denoted as Equal Error Rate (EER), Retrieval time.

B. Discussion concerning Face and Iris database

For our experiments on face modality, the IMM Frontal dataset is used which contains 120 face images, images of 12 persons in 10 totally different expressions. For iris, we have used the CASIAv1 database. In this info, there are 756 images of irises of 108 individuals which are captured using the OKI sensor. The images are captured in 2 sessions, three in initial session and four within the second. We tend to take only 120 iris images; this can be done in order to match the maximum number of users available in IMM database. For evaluating the proposed systems, we tend to create a hybrid database by pairing face and iris image from the 2 databases described above. Thus we've got created 120 users.

C. Results for Face- Iris Multi-modal

Before evaluating the multi-modal system, we tend to first present the results of the uni-modal biometrics systems. The experiments were performed for each biometric modality individually. For face modality, (Table1) two separate experiments are performed one each for Gabor filters based} features and LBP based features (so we choose LBP in our proposed system).The results are reported in terms of Recognition Rate. The results of the uni-biometrics based systems as well as the proposed system are reported in Table 2 in terms of retrieval time of result.

No. of faces in DB	No. of input face image compared with DB	Recognized image	Unrecognized image	Recognition rate
25	25	19	06	76% (Gabor)
25	25	21	04	84% (LBP)

Table 1: Comparison of Gabor and LBP

.

System	Retrieval Time
Face(LBP)	78SEC
Iris(Daugman's)	67SEC
Face+Iris+Score	57 SEC
Face+Iris+Rank+Score (Proposed System)	53 SEC

Table 2: Verification Results of the Uni- as well as Multi-Modal Biometric Systems in terms of retrieval time

4. CONCLUSIONS

In this paper, we developed a multi-modal biometric system by combining face and iris. For face, we used two types of features: Gabor filters based and Local Binary Patterns (LBP) based. We performed extensive experiments to evaluate the system on publicly available databases using standard well defined protocol, then after experimentation we choose LBP for our proposed system. The iris features are extracted using the Daugman's algorithm which results in binary features. We achieved significant improvement in the authentication performance in terms of accuracy without hampering the speed.

REFERENCES

[1] A. K. Jain, P. Flynn, and A. Ross, Eds., *Handbook of Biometrics*. Springer, 2008.

[2] ISO/IEC CD 2382.37, "Information processing systems Vocabulary Part 37 : Harmonized Biometric Vocabulary," 2010.

[3] A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*, ser. International Series on Biometrics. Springer, 2006.

[4] R. Brunelli and D. Falavigna, "Person identification using multiple cues," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 17, no. 10, pp. 955–966, 1995.

[5] Z. Zhang, R. Wang, K. Pan, S. Li, and P. Zhang, "Fusion of near infrared face and iris biometrics," in *Advances in Biometrics, Lecture Notes in Computer Science*,, 2007, pp. 172–180.

[6] C. H. Chen and C. T. Chu, "Fusion of face and iris features for multimodal biometrics," in *Advances in Biometrics, Lecture Notes in Computer Science*,, 2005, pp. 571–580.

[7] A. Rattani and M. Tistarelli, "Robust multi-modal and multi-unit feature level fusion of face and iris biometrics," in *Advances in Biometrics, Lecture Notes in Computer Science*, 2009, pp. 960–969.

[8] B. Son and Y. Lee, "Biometric authentication system using reduced joint feature vector of iris and face," in *6th International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA03)*, 2003.

[9] M. Eskandari and O. Toygar, "Fusion of face and iris biometrics using local and global feature extraction methods," *Signal, Image and Video Processing*, vol. 8, no. 6, pp. 995–1006, 2014.

[10] A. Jain, K. Nandakumar, and A. Ross, "Score Normalization in Multimodal Biometric Systems," *Pattern Recognition*, vol.38, pp. 2270–2285, 2005.

[11] V. M. Mane and D. V. Jadhav, "Review of Multimodal Biometrics: Applications, challenges and Research Areas," *International Journal of Biometrics and Bioinformatics (IJBB)*, vol. 3, no. 5, pp. 90–95, 2009.

[12] L. Masek, "Recognition of human iris patterns for biometric identification," Bachelors Thesis, 2003.

[13] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148–1161, November 1993.

[14] ——, "How Iris Recognition Works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, pp. 21–30, January 2004.

[15] D. Maturana, D. Mery, and A. Soto, "Face recognition with local binary patterns, spatial pyramid histograms and naive bayes nearest neighbour classification," in *Proceedings of the 2009 International Conference of the Chilean Computer Science Society*, 2009.

[16] H. AlMahafzah and M. Z. AlRwashdeh, "A Survey of Multibiometric Systems," International Journal of Computer Applications vol. 43, no. 15, pp. 36-43, 2012

[17] M. L. Gavrilova and M. M. Monwar, "Current Trends in Multimodal Biometric System Rank Level Fusion," in Pattern Recognition, Machine Intelligence and Biometrics, ed: Springer, 2011, pp. 657-673.

[18] R. Singhal, N. Singh, and P. Jain, "Towards An Integrated Biometric Technique," International Journal of Computer Applications, vol. 42, no. 13, pp. 20-23, 2012.

[19] G. Amirthalingam, "A Multimodal Approach for Face and Ear Biometric System," International Journal of Computer Science Issues (IJCSI), vol. 10, no. 5, pp. 234-241, 2013.

[20] M. S. Ahuja and S. Chabbra, "A Survey of Multimodal Biometrics," International Journal of Computer Science and its Applications, vol. 1, no. pp. 157-160, 2011.

[21] S. Kalra and A. Lamba, "A Survey on Multimodal Biometric," International journal of computer science and information technologies, vol. 5, no. 2, pp. 2148-2151, 2014.

[22] M. A. P. C. Mr. Rupesh Wagh, "Analysis of Mutlimodal Biometrics with Security Key," International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE). vol. 3, no. 8, pp. 1363-1365, 2013.

[23] A. Meraoumia, S. Chitroub, and A. Bouridane, "Multimodal Biometric Person Recognition System based on Iris and Palmprint Using Correlation Filter Classifier," in *Proc. of the Second International Conference on Communications and Information Technology*, Hammamet, Tunisia, June 26-28, 2012, pp. 782-787.

[24] M. Deriche, "Trends and Challenges in Mono and Multi biometrics," presented at the Image Processing Theory, Tools and Applications, 2008. IPTA 2008. First Workshops on, Sousse, 2008. pp. 1-9.

[25] Awalkar, Kanade, Jadhav, Ajmera, “A Multi-modal and Multi-algorithmic Biometric System Combining Iris and Face”, *International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology, Dec 16-19, 201*, pp.496-501.