A Novel Multimodel Feature Extraction for Authentication Approach Using Iris Image

R.Ashwinkumar
Ph.D (Research Scholar), Department of Computer Science,
Erode Arts & Science College (Autonomous), Erode, Tamil Nadu, India.
Email: ahaashwin@gmail.com
Dr.S.Pannirselvam
Research Supervisor & Head
Department of Computer Science, Erode Arts & Science College (Autonomous), Erode, Tamil Nadu, India.
Email: pannirselvam08@gmail.com

Abstract— Identity authentication is the most essential and required task in the real world environment which make use of biometric model to authenticate the persons in the real time. Biometrics usage to authenticate the system requires is a more burden process where the existences of fake images are exists. In the existing work, this problem is over come by introducing the multi model based authentication system in which wrong authentication due to fake images is reduced considerably. In the existing work, score level fusion is done using the triangulation based method which will combine the multi bio metrics (dual iris, thermal face and normal face) to authentication single person. However the authentication of system based on identity information might be more complex in case of presence of noises present in the given input images. Due to the noises resides in the images, the efficient and accurate matching of test input image with the database images might fail. The performance of combined multi bio metric authentication is improved by replacing the triangulation based method with min-max score level fusion approach which will lead to efficient processing. Thermal image enhancement is done before feature extraction to provide the optimal compilation of finding the fake images. The experimental tests have been conducted in the Matlab simulation environment which provides a flexible and convenient environment for the testers to execute the system. The performance evaluation conducted were proves that the proposed methodology provides better result than the existing system in terms of improved accuracy and successful authentication system.

Keywords— DCT, WALSH, HAAR, RCF.

1. INTRODUCTION

A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioural characteristic".

Multimodal biometric systems are those that utilize more than one physiological or behavioural characteristic for enrolment, 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

Reducing false non-match and false match rates. Providing a secondary means of enrolment, verification and identification if sufficient data cannot be acquired from a given biometric sample and Combating attempts to fool biometric systems through fraudulent data sources such as fake fingers. A multimodal biometric verification system can be considered as a classical information fusion problem i.e. can be thought to combine evidence provided by different biometrics to improve the overall decision accuracy.

Abstract level: The output from each module is only a set of possible labels without any confidence value associated with the labels; in this case a simple majority rule may be used to reach a more reliable decision.

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.

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 values.

2. RELATED WORKS

Ismail [1] comprehensively categorizes image quality measures, extend measures defined for gray scale images to their multispectral case and propose novel image quality measures. Subjective tests are tedious, time consuming and expensive and the results depend on various factors such as the observer’s background, motivation, etc. The statistical behavior of the measures and their sensitivity to coding artifacts are investigated via analysis of variance techniques. Their similarities or differences are illustrated by plotting their Kohonen maps.

Samir [2] proposes a new technique for generating synthetic iris images. The background texture is first generated using a texture synthesis scheme based on a single primitive element. Then, features of the iris such as the radial and concentric furrows, collarets and crypts are added to the synthetic images. Line integral convolution is used to impart texture to the radial furrows.

Anil [3] reliable identity management system is urgently needed in order to combat the epidemic growth in identity theft and to meet the increased security requirements in a variety of applications ranging from international border crossings to securing information in databases. Establishing the identity of a person is a critical task in any identity management system. Surrogate representations of identity such as passwords and ID cards are not sufficient for reliable identity determination because they can be easily misplaced, shared, or stolen. Biometric recognition is the science of establishing the identity of a person using his/her anatomical and behavioural traits.

Matthew [4] discussed that with the exception of the identity mapping, pixel value mappings leave behind statistical artifacts which are visible in an image's pixel value histogram. These artifacts as the intrinsic fingerprint of a pixel value mapping. By observing the common properties of the histograms of unaltered images, this work able to build a model of an unaltered images pixel value histogram. This model to identify diagnostic features of a pixel value mapping's intrinsic fingerprint. Because a number of image processing operations are in essence pixel value mappings, this work propose a set of image forgery detection techniques which operate by detecting the intrinsic fingerprint of each operation. At lower quality factors, however, noise detection appears to become more difficult.

3. DRAWBACKS IN THE EXISTING SYSTEM

The above research methodologies concentrates on finding the similarity of the authors based on gait sequences and author bio metric sequences. Single biometrics is used for authentication of users. Feature extraction and analysis are done in the synthetic manner. From these literatures it is clear that the authentication of the persons would be more difficult in the real world environment where the there is presence of more security threats. Gait sequence based authentication would be more complex process and also user with same manners can hack the system easily. Statistical measure based authentication system cannot support the authentication permission in the real time dynamic environment.

4. PROPOSED METHODOLOGY

The various problems that reside in the existing methodology are the noisy elements presents in the images might lead to the failure in the bio metric authentication process and also triangulation based score level fusion does not provide an optimal decision which is more complex process that leads to computational overhead.

In the existing system, multi biometric based authentication is used. The bio metrics used in this work are dual iris, normal face and the thermal faces. The features from these images are extracted and the feature fusion is done for iris, normal face and thermal face features. Then score level fusion is combining the feature details of the images. Finally, fake image is identified from the output retrieved from the score level fusion approach.

4.1 MULTI BIOMETRIC BASED AUTHENTICATION

In the existing work, multi biometric authentication is done to prevent the malicious user authentication. The multi biometric that are considered in this work dual iris and the thermal face image.

4.2 FEATURE EXTRACTION IN THE IRIS IMAGES

In the existing research work, feature extraction in the iris code images are done by using the 1D log filter based feature extraction. Relations between activations for a specific spatial location are very distinctive between objects in an image. Furthermore, important activations can be extracted from the Gabor space in order to create a sparse object representation. Gabor filters have been used extensively in a variety of image processing problems, such as fingerprint enhancement and iris recognition.

4.3 FEATURE EXTRACTION IN THERMAL FACE IMAGES

The thermal feature extraction is done by using (2D)2FPCA feature extraction approach. The existing (2D)2LDALPP method effectively combines alternative 2DLDA with alternative 2DLPP. The feature extraction is split into two steps: firstly, the column directional information is extracted by applying alternative 2DLDA; secondly, the feature matrix is inversed and alternative 2DLPP is used to extract the row directional information.

4.4 FEATURE EXTRACTION IN VISIBLE FACE IMAGES

Multilinear principal component analysis (MPCA) is a mathematical procedure that uses multiple orthogonal transformations to convert a set of multidimensional objects into another set of multidimensional objects of lower dimensions. There is one orthogonal (linear) transformation for each dimension (mode) hence multilinear. This transformation aims to capture as high a variance as possible, accounting for as much of the variability in the data as possible, subject to the constraint of mode-wise orthogonality.

4.5 FEATURE LEVEL FUSION FOR BOTH VISIBLE AND THERMAL FACES

Almost every biometric system consists of four major parts – sensor, feature extraction, comparison, and the final decision. In order to address specific parts of the process, we use a slightly more complex pipeline structure. The numbers in the following list refer directly to the numbers.

1. The detection of facial features involves the localization of important facial landmarks. These landmarks are used in subsequent steps. In this paper, we are using manually annotated data, because precise detection of facial features is still a challenge. Moreover, we are focusing on algorithm performance, rather than detection accuracy.
2. The face can be normalized into some predefined position by affine transformation, based on the detected points (2D-warping). The other solution (3D-projection) involves a 3D model that is adapted to the input image.
3. Some of our testing databases contain the IR images, captured in dynamic range mode. Due to this fact, intensity normalization is needed.
4. The feature vector extraction is a simple vectorization of the normalized image. The other possibility is the application of a filter bank. Either the Gabor filter or the Laguerre-Gaussian filter banks may be used.
5. In order to reduce space dimensionality, as well as to increase inter-class variability and/or reduce redundancy, the feature vector may optionally be passed onto some statistical projection technique.

6. Feature vector post-processing involves additional processing of the feature vector. For example, a selection of the best components (in terms of recognition performance) may be used. Individual components may obtain weights, or the components may be normalized.
7. A comparison of two processed faces (feature vectors) is accomplished by calculating the distance between them. Any distance-metric function may accomplish this task. In our paper, we are using Euclidean, cosine, city-block (Manhattan, sum of absolute differences), and correlation metric.
8. The final decision is simply a thresholding of the achieved comparison score.

4.6 Algorithm

Input: Thermal Face Image, normal face image, Dual iris image
Output: Authentication result

Step 1: Retrieve the thermal face image from the database.
Step 2: Enhance the thermal image by eliminating noises and improving the contrast.
Step 3: Extract the features from the image using 2LDPP.
Step 4: Calculate the feature fusion score of thermal face image.
Step 5: Retrieve the normal face image from the database.
Step 6: Extract the features from the image using MPCA.
Step 7: Calculate the feature fusion score of normal face image.
Step 8: Retrieve the dual iris image from the database.
Step 9: Extract the features using 1D gabor filter approach.
Step 10: Calculate the fusion score of the iris features.
Step 11: Compute score fusion value by integrating the feature score values of dual iris and the thermal face image.
Step 12: Output whether the person is authenticated or not.

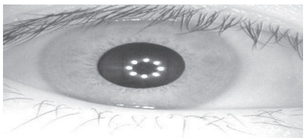
5. EXPERIMENTAL RESULTS

MATLAB is an interactive software package which was developed to perform numerical calculations on vectors and matrices. It is a high performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notations. It is an interactive system whose basic data element is an array that does not require dimensioning. This allows formulating solutions to many technical computing problems, especially those involving matrix representations, in a fraction of the time it would take to write a program in a scalar non-interactive language.

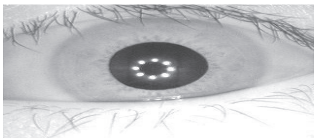
MATLAB stands for Matrix Laboratory. It was written originally to provide easy access to matrix software developed by the linear system package, Eigen system package. It is complimented by a family of application-specific solutions called toolboxes. It contains a high-level programming language which makes it quite easy to code complicated algorithms involving vectors and matrices. It can do quite sophisticated graphics in two and three dimensions. Image processing toolbox is a collection of MATLAB functions that extend the capability of the MATLAB environment for the solution of Digital Image Processing.

5.1 MULTI BIOMETRIC SAMPLE DATABASE

The sample biometrics images that are considered in this work for secured authentication of persons who are trying to access information is given as follows: These bio metrics improves the authentication security in terms of various difference resides between the biometrics that are proposed.



Iris Right Image



Iris Left Image

5.2 PROCEDURE FOR IDENTITY FUSION BASED AUTHENTICATION

A complete procedure of the authentication an person in terms of multiple bio metrics that are gathered from the users are given as follows:

Feature Extraction in biometrics
Feature level Fusion creation
Score level Fusion Calculation
Authenticate the person

6. PERFORMANCE EVALUATION

6.1 Accuracy

Accuracy is defined as the correctness of authentication of the persons who are entering into field without error. The accuracy of authentication of system should be high, so that the retrieval can be done without wrong authentication. The accuracy is calculated as follows:

$$\text{Accuracy} = \frac{(\text{True positive}+\text{True negative})}{(\text{True positive}+\text{True negative}+\text{False positive}+\text{False negative})} \text{------------(1)}$$

6.2 True positive rate (TP)

The recall or true positive rate (TP) is the proportion of positive cases that were correctly identified, as calculated using the equation

$$\mathrm{TP} = \frac{d}{c+d} \qquad \text{---------(2)}$$

6.3 False positive rate (FP)

The false positive rate (FP) is the proportion of negatives cases that were incorrectly classified as positive, as calculated using the equation:

$$\mathrm{FP} = \frac{b}{a+b} \qquad \text{---------(3)}$$

6.4 False negative rate (FN)

The false negative rate (FN) is the proportion of positives cases that were incorrectly classified as negative, as calculated using the equation:

$$\mathrm{FN} = \frac{c}{c+d} \qquad \text{---------(4)}$$

a is the number of correct predictions that an instance is negative b is the number of incorrect predictions that an instance is positive

c is the number of incorrect of predictions that an instance negative

d is the number of correct predictions that an instance is positive

6.5 Precision

Precision is the percentage of ability of system to authentication person in the correct manner. The precision value indicates that the ability of system to correct prediction made among the total number of prediction. The precision value is calculated as follows:

Precision =True Positive / (True Positive + False Positive)-------(5)

6.6 Recall

Recall value is determined based on the retrieval of information at true positive prediction, false negative. Recall in this context is also referred to as the True Positive Rate. In that process the fraction of relevant instances that are retrieved.

Recall =TP / (TP+FN) --------------(6)

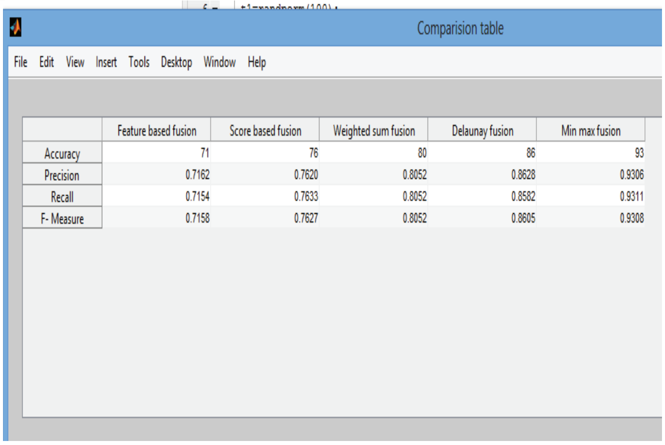
6.7 F-Measure

The F-Measure computes some average of the information retrieval precision and recall metrics

$$\text{F-measure}=\frac{2*precision.recall}{precision+recall} \qquad \text{---------------(7)}$$

To evaluate the overall performance of the proposed system in terms of accurate authentication of the persons based on their correct bio metric system is conducted in the MATLAB simulation environment. The different performance parameters are considered for the efficient comparison of the proposed approach with the existing approach in order to prove their performance improvement in terms efficient authentication.

Table 6.1 shows the performance metrics values that are considered for evaluating the proposed with the existing approach which are obtained in the MATLAB simulation environment. The comparison of the proposed methodology with the various existing approaches and its actual performance metrics values are listed in the table 6.1.



	Feature based fusion	Score based fusion	Weighted sum fusion	Delaunay fusion	Min max fusion
Accuracy	71	76	80	86	93
Precision	0.7162	0.7620	0.8052	0.8628	0.9306
Recall	0.7154	0.7633	0.8052	0.8582	0.9311
F- Measure	0.7158	0.7627	0.8052	0.8605	0.9308

Table 6.1. Performance measure values of proposed and various existing researches

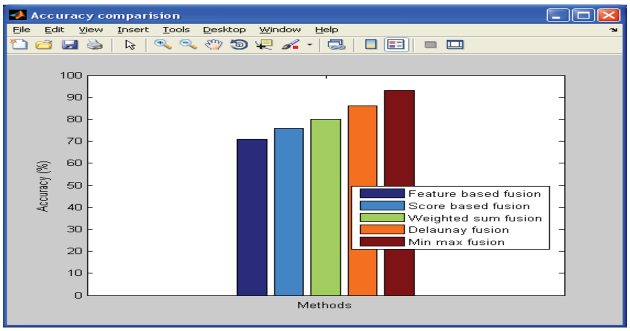


Figure 6.1 Comparison of Accuracy parameter of different research methods

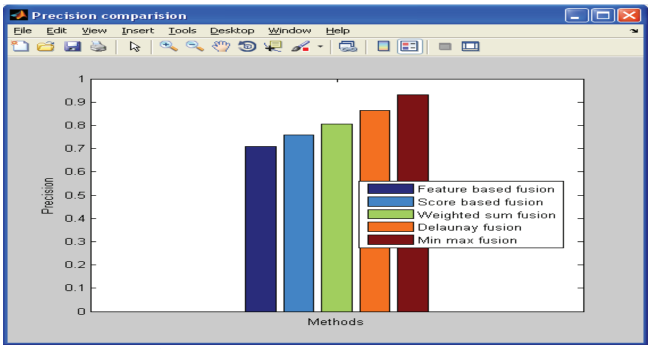


Figure 6.2 Comparison of Precision parameter of different research methods

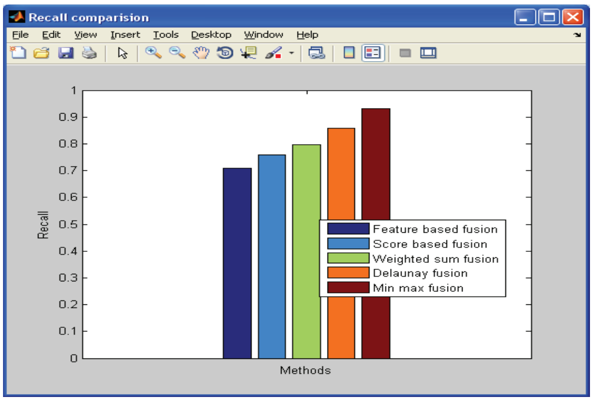


Figure 6.3 Comparison of Recall parameter of different research methods

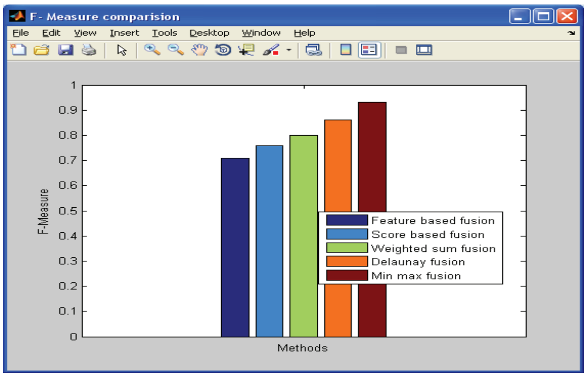


Figure 6.4 Comparaison of F-Measure parameter of different research methods

7. CONCLUSION

Identity based authentication is the most essential process in most of the real world application which started to use bio metric based authentication for the secured environment. In this work secured multi bio metric based system is done in which bio metrics are authorized in the secured manner. Biometric considered are dual iris, normal face image and the thermal face. Thermal face is enhanced before feature extraction to improve the matching rate. The fusion of features is done with the consideration of the various segmentation details. The min max based approach is used to fuse the multi bio metric features from which the security is enhanced considerably. Experimental results prove that the proposed methodology provides better result than the existing work.

8. REFERENCES

[1] Matthew C. Stamm, and K. J. Ray Liu," Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 3, September 2010.

[2] Samir Shah and Arun Ross, "Generating Synthetic Irises By Feature Agglomeration", Proceedings of International Conference on Image Processing (ICIP), (Atlanta, USA), October 2006.

[3] Ismail avcas, Bulent saker, khalid shayid, "Statistical evaluation of image quality measures", Journal of Electronic Imaging 11(2), 206–223, April 2002.

[4] Raffaele Cappelli, Alessandra Lumini, Dario Maio and Davide Maltoni, "Fingerprint Image Reconstruction from Standard Templates", IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 29, No. 9, September 2007

[5] Siwei Lyu, and Hany Farid, "Steganalysis Using Higher-Order Image Statistics", IEEE Transactions On Information Forensics And Security, Vol. 1, No. 1, March 2006.

[6] Gian Luca Marcialis, Aaron Lewicke, Bozhao Tan, Pietro Coli, Fabio Roli, "First International Fingerprint Liveness Detection Competition—LivDet 2009", Image analysis and processing, Volume 5716, pp 12-23, 2009.

[7] Anmin Liu, Weisi Lin, and Manish Narwaria, "Image Quality Assessment Based on Gradient Similarity", IEEE Transactions On Image Processing, Vol. 21, No. 4, April 2012.

[8] Kristin Adair Nixon Valerio Aimale Robert K. Rowe, "Spoof Detection Techniques", published in handbook of biometrics.

[9] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainenm, "Can Gait Biometrics be Spoofed?", Pattern Recognition (ICPR), PP: 3280 – 3283, 11-15 Nov. 2012.

[10] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric Template Security", Hindawi Publishing Corporation, EURASIP Journal on Advances in Signal Processing, Volume 2008, Article ID 579416.