

A Review on Iris and Fingerprint Fusion Authentication Systems

Dhara Heble¹, Rupali Nikhare²

Student, Information Technology, Pillai College of Engineering, New Panvel, India¹

Asst. Professor, Computer Engineering, Pillai College of Engineering, New Panvel, India²

Abstract: There are many combinations possible for the multi biometric fusion authentication systems. In this paper, we focus our study on Iris and Fingerprint fusion authentication systems. With advancement in technology, now a days, more biometric combinations are possible for better precision. Some references quoting combinations of face and ear are also discussed to quote these advancements compared to the traditional and usual biometric combinations of iris and fingerprints.

Keywords: Iris, Fingerprint, Fusion, Multimodal, Biometric Authentication.

I. INTRODUCTION

In current global environment, any personal data can be accessible by anyone. There are all chances for hacking of template by intruder. This hacking can be controlled with unimodal or multimodal biometric systems, as they recognise a person uniquely. Unimodal / Biometric Systems have many limitations with regard to precision in identification / authentication of personal data. This occurs especially with noisy data, spoof attacks and unacceptable error rates. In multimodal biometric system, two or more biometric traits are fused together for identification. This fusion can be done at four different levels, viz. raw data, detector level, Feature level, score level.

II. BIOMETRIC SYSTEM FOR PERSONAL IDENTIFICATION

Biometric system is used for identification purpose of a specific person. Two types of attributes are followed in this process, viz. physical and biological. Fingerprint, face recognition, palm, voice are the physical attributes. Gait, keystroke etc are the biological attributes. The changes, if any, made by the intruder with the template are not be accepted by the biometric system.

In multimodal biometric system, (Eg. fusion of Fingerprint and Iris), such physical and biological attributes are fused together for precise identification of a particular person. This system comprises of three modules viz. Feature extraction, fusion of multimodal biometric template creation and cryptographic key creation.

The traditional multimodal biometric approach has better accuracy and stability of the system than individual unimodal components. It costs higher than Unimodal approach. Because of multiple sensors or multiple algorithms or both leading to requirement of larger memory footprint and slower processing speeds.

With these merits and drawbacks, it is the need of the hour to opt for multimodal system than Unimodal one.

III. FINGERPRINT – IRIS FUSION APPROACH

Asim Baigetal[1], in their research paper on Fingerprint – Iris fusion based Identification System using a Single Hamming Distance matcher, state that the efficacy of a biometric authentication system is measured by the accuracy of the system and by the error rates viz. False Accept Rate (FAR) and the False Reject Rate (FRR). Desired values of Far and FRR should be closed to zero in real systems as far as possible. Some biometric applications demand robustness and accuracy higher than any single biometric trait. The overall security of the multimodal system is always better. Multimodal biometric approach is a logical extension to the unimodal approach. They provide promising results.

Pooja Choudhari et al[2], in their research paper on Fusion of Iris and Fingerprint Images for Multimodal Biometrics Identification, proposed an approach for cryptographic key generation from multimodal biometrics, aiming for security-conscious customers. In their proposal, cryptographic key generation is planned with Feature extraction from fingerprint, Feature extraction from iris, Fusion of fingerprint and iris features and Generation of cryptographic key from fused features.

IV. PROTOTYPE SYSTEM DEVELOPMENT

After obtaining image of two biometric templates, feature extraction is done from the biometric traits and stored in database. Now comparison of template with the one stored in database can be done to get result of matching score.

The authors tested the database for 800 subjects and found that the level of accuracy had increased in multimodal system is efficient than unimodal system.

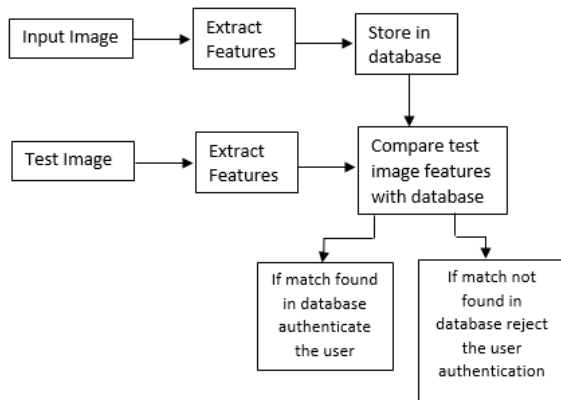


Fig. 1 Biometric Authentication System

They further revealed that selective encryption method gives better results for multimedia data and is useful compression of encrypted images on web.

AsimBaiget al[1]. In their research paper on Fingerprint – iris fusion based Identification System using a Single Hamming Distance matcher, state that the effectiveness of a biometric authentication system is measured by the accuracy of the system and by the error rates, viz. False Accept Rate (FAR) and the False Reject Rate (FRR). FAR identifies the number of times an imposter is classified as a genuine user by the system. FRR, contradictory to FAR, measures misidentifications of a genuine user as an imposter. Theoretically, FAR and FRR should be as close to zero as possible. But in real systems, this is not possible.

Multimodal Biometric System is, truly speaking, a logical extension to the unimodal approach. Multimodal biometric approaches often provide promising results where robustness and accuracy are highly needed as it reduces FAR and FRR. Also, this approach is harder to circumvent and overall security of the whole system is improved.

Fingerprint of an individual is composed of ridges and furrows. They have same width, they run parallel. Minutia Are the features on ridges. Minutia types, viz. Termination, bifurcation, etc. on fingerprint image are mostly significant. In case of each human being, finger print of his each finger has a permanent uniqueness. This property is being used for recognition of an individual.

For the purpose of identification, bifurcations and terminates are stored as one feature. Each minutia is stored with three parameters X, Y by assigning respective decimal number and its tangent angle is assigned a floating point number. One pixel coordinate is stored for each minutia.

Iris is a circular diaphragm. It consists of a number of layers. Epithelium layer contains dense color cells. It determines the color of iris. Stromal layer consists of blood vessels. The external visible surface is a multi-layered iris consisting of two zones. Each zone differs in color. These two zones are divided by the collarets. This iris is located between cornea and lens of the human eye. Iris controls the amount of light entering in the eye through the pupil. It has an average diameter of 12 mm. Pupil size goes to 10% to 80% of the iris diameter. This is

how iris pattern of each human being is distinct, hence is used in identification of an individual.

[1]Empirically proved that multimodal biometrics improves performance in respect to increasing accuracy and decreasing False Accept Rates. Jain et al [7] provided a fingerprint, fusing face and speech based multimodal authentication system. By doing rank level fusion in a parallel mode at post matching stage, they used minutiae based approach to detect fingerprint, Eigen face-based approach to detect faces. They also incorporated text dependent speaker recognition system using Hidden Markov Model (HMM) to detect Voice.

In another model, Wang et al[3], in order to identify users, provided comparison between multiple fusion techniques, at rank level, using weighted sum, a Fisher discriminant analysis and neural network based classifier. Fusion of face and iris was done, and an Eigen face-based approach was followed to detect faces by employing an algorithm characterizing local variations in iris for matching.

Bowyer et al[8] worked with multiple samples of face from same and different sources. With this, he created a multimodal system using four different 2D images and a single 3D face image from each user were used for verification, in parallel at matching score level using sum, product or the minimum value rule.

Mohamad Abdolahi et al[9], in their research paper entitled Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic, in the beginning, authors have once again described limitations of Unimodal Biometric System and have advocated to go for Multimodal Biometric System.

Fuzzy logic is used for the effect of each biometric result combination in Multimodal Biometric System. While studying related work in this technology, the authors have reported about some of important outcomes of other researchers.

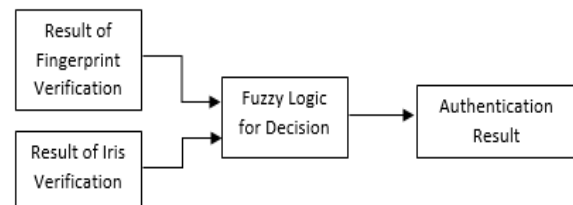


Fig. 2 Fuzzy Logic at Decision Level of Multimodal Authentication System

Brunelli and Falavigna[10] used hyperbolic tangent (tanh) for normalization. They also used weighted geometric average for fusion of voice and face biometrics. Hong and Jain proposed an identification system based on face and fingerprint. The fingerprint matching is applied after pruning the database via face matching. Kittler et al. have experimented with many fusion techniques for face and voice biometrics. Ben-Yacoub et al, for face and voice biometrics, studied many fusion strategies, viz. support

vector machines, tree classifiers and multi-layer perception, and Bayes classifier.

V. ADVANCE FEATURES IN PRECISE PERSONAL IDENTIFICATION

Ross and Jain as quoted in [6] combined face, fingerprint and hand geometry biometrics with sum, decision tree and linear discriminant-based methods. It is observed that sum rule outperforms others.

Ujwalla Gawande et al. [6], in their research paper on Fingerprint-Iris Fusion Based Multimodal Biometric System Using Single Hamming Distance Matcher, state that each biometric feature has its own strengths and weaknesses. Based on application, we choose a particular pattern for personal recognition. Due to robustness, distinctiveness, availability, accessibility and acceptability, multimodal biometric system specific application oriented multimodal biometric system is selected for personal recognition. These qualities of multimodal biometric system make them reliable and popular with improved template security. Proper feature sets from different biometric sources when used with appropriate fusion scheme, give precise personal recognition.

A single biometric indicator alone can't investigate whether integration of face and palmprint biometrics can give better performance or not. Considering Principal Component Analysis (PCA) and Independent Component Analysis (ICA) in the context of feature vector fusion, Ross and Jain presented separately various levels of integration in score level fusion strategies of multimodal biometric systems and novel fusion at feature level for face and palm print. They observed significantly improved performance.

Dass, Nandakumar & Jain [7] conducted an experiment with fusion of face, fingerprint and hand geometry. They employed product rule and couple method. With this, they proposed an approach to score level fusion in multimodal biometrics systems. Both fusion rules showed better performance than individual recognizers.

Kittler et al. As mentioned in [6] proposed a framework for multimodal biometric fusion. It was based on utilization of a single matcher implementation for both modalities.

Feature vectors were created independently for each sensor. They were compared to the enrolment templates. In Fusion, at the Matching Score Level, they were stored separately for each biometric trait. Each subsystem computed its own matching score based on the proximity of feature vector and template. These individual scores were finally combined into a total score. The final score was passed to the decision module.

This framework was designed to provide improved performance over the unimodal systems. It was demonstrated through the development of a fingerprint and iris based multimodal biometric identification system with score level fusion. Both modalities utilized the same matcher module. Due to this, the memory footprint of the system got reduced. They analyzed Common theoretical framework for combining classifiers using sum rule,

median rule, max and min rule under the most restrictive assumptions. They observed that sum rule outperforms better over other classifiers' combination schemes.

In another paper entitled Decision Level Fusion Based Multimodal Biometric System by V. SIREESHA, K. SANDHYARANI [3], the authors reported that IRIS is one of the best biometric parameter. An efficient recognition technique is proposed to reduce the space complexity; enhancing recognition accuracy within a limited number of classes was proposed. An accuracy of 99.73% was achieved within 1500 classes in 3.6 seconds. Compared to existing Iris recognition techniques, on ideal iris sets, a nonideal iris recognition was proposed. This technique extracts half of the Iris part. This segmentation gave 90% recognition accuracy. The iris segmentation was achieved within 1.8 seconds. The performance of Iris recognition system depended on the inter dependability and separation of the features.

For improving recognition accuracy of a biometric system, the number of features extracted from the biometrics should be increased. This will enhance the processing time. MAHMOUD. Y. SHAMS et al. [4] pointed out that in case of injury to a person, when more than two or more biometric parts are used in biometric fusion, the chances of precise recognition are increased. Second advantage of this multiple fusion is eradicating spoof attacks.

M. I. Razzak et al [11] selected some faces having minimum Euclidean distance, with more similarity. They entered faces and finger veins to the system. Using Linear Discriminant Analysis (LDA) method, extraction of these biometric organs was done. The FAR was reduced to 0.000026 and Genuine Acceptance Rate (GAR) increased to 97.4%.

Dass, Nandakumar & Jain [7], in their paper entitled "Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint", followed an approach, of matching biometric recognition of iris and fingerprint with monomodal system. They did matching with fuzzy and classical algorithms, followed by exhaustive and intensive tests on database of iris and fusion matrix. The results were inspiring.

VI. SUMMERY

In current global environment, any personal data can be accessible by anyone. There are all chances for hacking of template by intruder. Biometric system is used for identification purpose of a specific person using fingerprint, face recognition, palm, voice, etc.

Single Hamming Distance matcher, cryptographic key generation from multimodal biometrics, biometric authentication system, useful compression of encrypted images on web with an GAR as high as 99.7%, just a few seconds, Linear Discriminant Analysis (LDA) method, product rule and couple method

VII. CONCLUSION

Multimodal biometric system, such physical and biological attributes are fused together for precise identification of a particular person. Unimodal Biometric Systems have many limitations with regard to precision in identification / authentication of personal data. Multimodal systems control FAR and FRR. Selective encryption method with Linear Discriminant Analysis (LDA) method gives better results for multimedia data and provides useful compression of encrypted images on web with an GAR as high as 99.7 %, just a few seconds. However, more than iris and finger prints, when fused, provide still better precision to identify precisely in normal case as well as when one of the organs is damaged.

REFERENCES

- [1] Asim baig, Ahmed Bouridane, "Iris Fusion based identification system using a single hamming distance matcher", International general of bioScience and Bio-technology, vol. 1, pp. 1, December 2009.
- [2] PoojaChoudhari et al.;Fusion of Iris and Fingerprint Images for Multimodal Biometrics Identification,IOSR Journal of Engineering (IOSRJEN)Vol. 04, Issue 08 (August. 2014), ||V2|| PP 01-04
- [3] Yunhong Wang, Tieniu Tan, Anil K. Jain, Combining face and iris biometrics for identity verification, Proceedings of the 4th international conference on Audio- and video-based biometric person authentication, June 09-11, 2003, Guildford, UK
- [4] SIREESHA, K. SANDHYARANiet al.: Decision Level Fusion Based Multimodal Biometric System, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5, Issue 5, May 2016
- [5] Mahmoud. Y. Shams, Ahmad. S. Tolba, Shahenda. H. Sarhan: Face, Iris, And Fingerprint Multimodal Identification System Based On Local Binary Pattern With Variance Histogram And Combined Learning Vector Quantization, Journal of Theoretical and Applied Information Technology 15th July 2016. Vol.89. No.1
- [6] Tiwalade O. Majekodunmi, Francis E. Idachaba, Mohamad Abdolahietal, :A Review of the Fingerprint, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technologies, Proceedings of the World Congress on Engineering 2011 Vol II WCE 2011, July 6 - 8, 2011, London, U.K.
- [7] UjwallaGawande et al.: Fingerprint-Iris Fusion Based Multimodal Biometric System Using Single Hamming Distance Matcher, International Journal of Engineering Inventions Volume 2, Issue 4 (February 2013) PP: 54-61
- [8] Dass, Nandakumar& Jain: Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint, The Scientific World JournalVolume 2014 (2014), Article D 829369, 13 pages
- [9] Kevin W. Bowyer, and Patrick Flynn:Fusion of Face and Iris Biometrics Ryan Connaughton
- [10] Mohamad Abdolahi, Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic, International Journal of Soft Computing and Engineering (IJSC), Volume-2, Issue-6, January 2013
- [11] Brunelli and Falavigna: Person Identification using multiple cues, Ieee Transactions On Pattern Analysis And Machine Intelligence, Vol. 17, No. 10, October 1995
- [12] Muhammad Razzak, Multimodal biometric recognition based on fusion of low resolution face and finger veins, International Journal of Innovative Computing, Information and Control, Volume 7, Number 8, August 2011 pp. 4679-4689