Indian J.Sci.Res. 14 (2): 142-147, 2017 ISSN: 2250-0138 (Online)

A COMPARATIVE ANALYSIS OF DIFFERENT TECHNIQUES FOR TRIPLE LEVEL BIOMETRIC AUTHENTICATION FOR HUMAN

ROHIT SRIVASTAVA[a1] AND PRATEEK SRIVASTAVA[b]

[ab]Department of Computer Science and Engineering, School of Engineering, Sir Padampat Singhania University, Udaipur, Rajasthan, India

ABSTRACT

Biometric identification process is used for recogniting and identifying a person for various applications. The process can be done by using single Biometric feature or a combination of Biometric features. If the identification is done by using a single Biometric feature (face iris finger , palm etc) then the system is called as Unimodal and if a combnation of Biometric is used then it is called as Multimodal. In multimodal system various drawbacks of Unimodal system (Noisy Data , Multiple vectors etc) are removed. The main goal of the proposed work is to design a framework that will provide authentication based upon three level authentication for a person. Earlier works in this field are explained in different statistical models based on different authentication schemes. They tried to estimate the predictable output values with known historic data. In those procedures, they tried to authenticate with the help of transformations and analysis.In the proposed method a mechanism is developed in which if one biometric trait gets failed then the other biometic traits can be used for authentication.

KEYWORDS: Principal Component Analysis, Face Recognition, Fingerprint Recognition, Miniutae Matchnig, Score Fusion, Palmprint Recognition

A biometric system refers to a pattern recognition system that have ability to acquires biometric data from an individual [1]. The requirements of enhanced security in biometric based upon the authentication of a person has led us to an interesting area. Those biometrics systems that are based on single information source are called "Uni-modal Systems" [2]. Unimodal biometrics have many implicit problems in their applications. The major difficulty with uni-modal biometric technology is that it is not perfect suited for all applications [3]. Limitations of uni-modal biometric systems even though these systems offers a reliable solution for secured verification and it is commonly used in numerous commercial systems in practice; it suffers from following limitations: Sensed data noise, intra-class variation, intra-class similarities, spoof attacks and non-universality [4]. Hence, it is not possible to achieve desired performance by single biometric system. One of the methods to solve these problems which are encountered in single biometric system is to make use of multi-modal authentication biometric systems. This model combines information from multiple modalities to dictate a decision [2].

This paper presents the review of multimodal biometrics. This includes a brief introduction about multimodal biometrics. In this paper, various fusion techniques of multi-modal biometrics have been discussed. In this paper a fusion technique is proposed based on face,fingerprint and palmprint biometric traits. After capturing features preprocessing is done and features are extracted for feature level fusion. Biometric Fusion is classified into 5 categories:

(a) Sensor Level Fusion: This is also referred to as image level or pixel level fusion. This is possible only if multiple samples are fused that are taken using the same sensor. If multiple sensors are used then the data from different sources must be compatible. The raw data contains a lot of information but at the same time it is corrupted by noise.

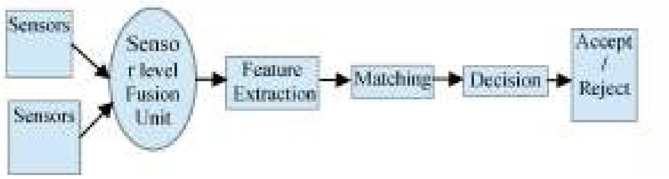
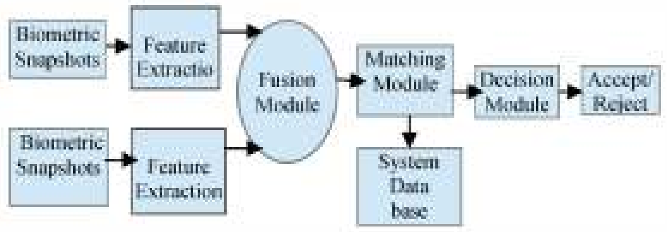


Figure 1: Sensor Level Fusion[3]

(b) Feature Level Fusion: In this fusion the data from different sources are separately processed, features are extracted and a joint feature vector is computed for matching against the stored template. The fusion can be easily accomplished if the features are extracted using same algorithm otherwise it becomes tedious .



[1] Corresponding author

Figure 2: Feature Level Fusion[3]

(c) Score level fusion: Score level fusion is the combination of scores matched from th output of the individual matcher. These matching scores indicate the approximation of of identification of sample image form the database. The matching score is rich in information next to the feature vector and also it is easy to access these values and combine them.

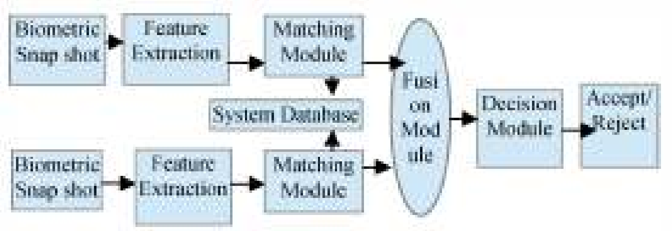


Figure 3: Score Level Fusion[3]

(d) Rank Level Fusion: Rank level fusion is based on ranking of the output of the enrolled identities. The matched identities are sorted in descending order of matching statistics. Ranks gives a clear information regarding the decision-making process compared to just identify the best match, but they reveal less information as compared to score level. Just like score match the ranking outputs are comparable so, the normalization process is not required.

(e) Decision level fusion: The decision level or abstract level fusion is possible only when the output from individual biometric matchers is available. The output from the different matchers are fused using the "AND" and "OR "rules. The output of the "AND" rule is a "match" only when the input test sample is matched with the stored templates at the output of each matcher. Whereas, the "OR" rule outputs a "match" decision even if one of the matcher+ decides that the input test sample matches with the stored templates.

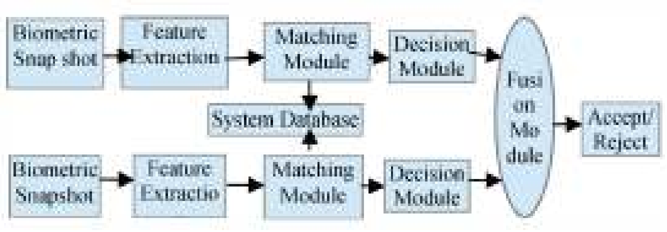
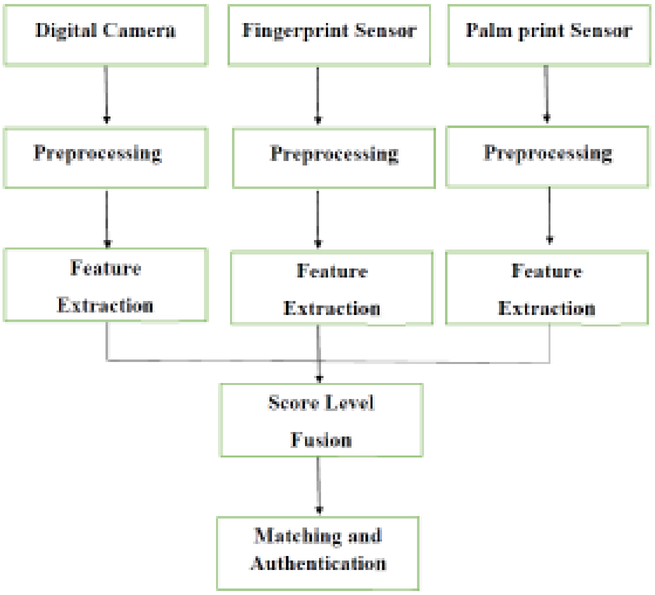


Figure 4: Decision Level Fusion[7]

Artificial Neural Networks (ANN) has been are having a great usage in authentication systems and also provides automation to the system.. The advantages of these models of the neural network are to be seen in increase in approximation and cost reduction. Artificial Neural Networks takes part as an important task in support of the analysis of the big data sets in various forms of authentication.

SYSTEM BLOCK DIAGRAM



PROPOSED METHODOLOGY

Fingerprint Identification

The fingerprint identification is made of three main steps, namely the preprocessing, the feature extraction and the comparison step.

The preprocessing is divided into two main steps which are the normalization of the fingerprint image, and the location and the framing of the central point of the fingerprint image. The normalization is used to eliminate the effects of noise and distortion when capturing the image from the fingerprint sensor. The original image is normalized by its mean M and its variance VAR, the matrix G (I) given by equation indicates the normalized grayscale image and G (i, j) is its value at pixel (i, j). Where M_0 and VAR_0 are the desired mean and variance values, respectively.

$$G(i,j) = \begin{cases} M_0 + \sqrt{\dfrac{VAR_0(I(i,j) - M)^2}{VAR}}, \text{if } I(i,j)>M \\ M_0 - \sqrt{\dfrac{VAR_0(I(i,j) - M)^2}{VAR}}, \text{otherwise} \end{cases}$$

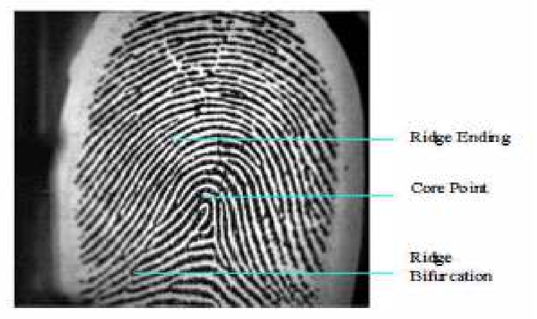


Figure 5: A Fingerprint Image[4]

The following step is used to locate and frame the central point of the fingerprint. The central point detection algorithm is summarized as follows:

- Estimate the orientation field
- Calculate the field strength of the loop at each point in the orientation field, using the expanded field of the hidden orientation.
- Normalize the resistance loop field row in a range from 0 to 1.
- Perform a thresholding on the field loop to locate both the kernel and the center of the region.

In order to extract the relevant features of the fingerprint, the Gabor filter was applied on the framed part of the fingerprint following 8 different directions θ that is (0°, 22.5°, 45°, 67.5°, 90°, 112.5°,135°, 157.5°). The results are complex values which were encoded in order to obtain a binary vector of size 1024, representing the main features of the fingerprint image.

B. Fingerprint Verification (Gabor Filter approach):

For identifying details in a fingerprint image Gabor filters are to be used..Matching of two fingerprint images is done on the basis of Euclidean Distance.The matching of two images can be enhanced for performance by the combination of score decisions based on different fingerprint features. [21]

C. Feature Extraction from Face Image using Local Binary

Patterns (LBP)

For extracting face features Local Binary Pattern (LBP) histogram approach is used . It captures local face features. As shown in Fig. 6 LBP is centered at every pixel in the image. It acts as a threshold value for all the surrounding binarized pixels.By using clockwise direction 8 bit number is generated and placed at centre pixel location . In this way a new image called LBP image is obtained . 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

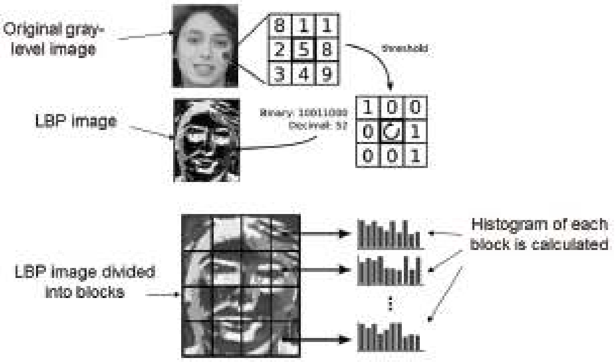

Original gray-level image
8 1 1
2 5 8
3 4 9
threshold
LBP image
Binary: 10011000
Decimal: 52
1 0 0
0 1
0 0 1
LBP image divided into blocks
Histogram of each block is calculated

Figure 6: Face Print Identification using LBP Approach

Transition from 0 to 1 or 1 to 0, then it is called uniform LBP. For face recognition, LBP histogram features of two images are compared using the Chi square distance metric shown in Equation .

$$\chi^2(X,Y)=\sum_{i=1}^{N}\frac{(x_i-y_i)^2}{(x_i+y_i)}$$

Here X and Y are the feature vectors and N is their dimension. Nearest neighbour classifier can be used to take the accept/reject decision.

D. Palmprint Identification (Left and Right Palmprint):

For Palmprint identification a combination of left palmprint and right palmprint image has been used. For the proposed methodology a framework for fusing left palmprint and right palmprint image is developed. For this framework to successfully identify palmprint image a fusion of three kinds of score is required.Two scores can be generated by using left and righr palmprint image whereas for third score a specific algorithm is proposed.

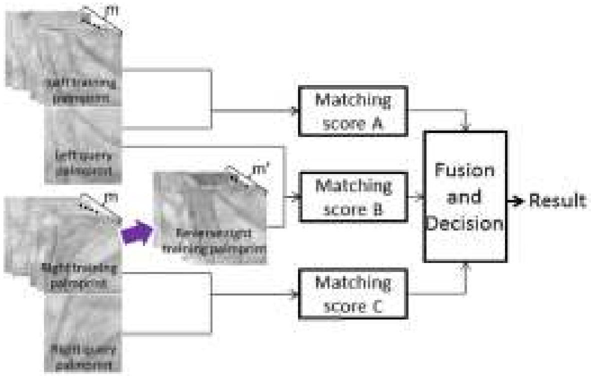


Figure 7: Procedure for Palmprint fusion[7]

Corelation Between the Left and Right Palmprints

Left palmprint and Right palmprint images are similar to each other .In Fig. 8 left palmprint images of four different subjects is taken. Again the right palmprint image and reverse palmprint image is also taken in the figure [Fig 7] As depicted from the figure it is inferred that left palmprint and the reverse right palmprint image of the same subject are similar in nature.

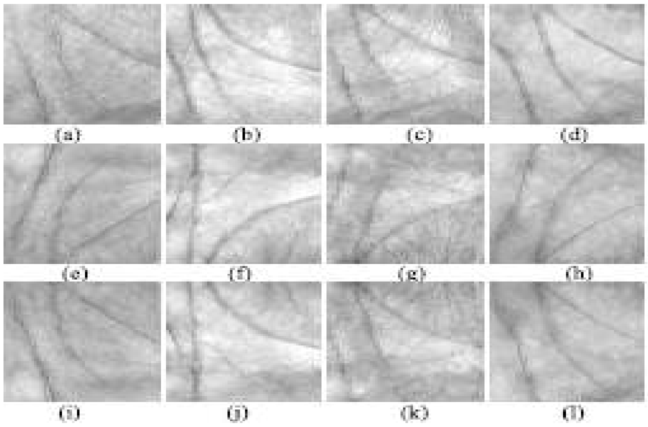


Figure 8: Palmprint images of four subjects.

Fig. 9 shows the principal lines images of the left palmprint, reverse right palmprint shown in Fig. 8.

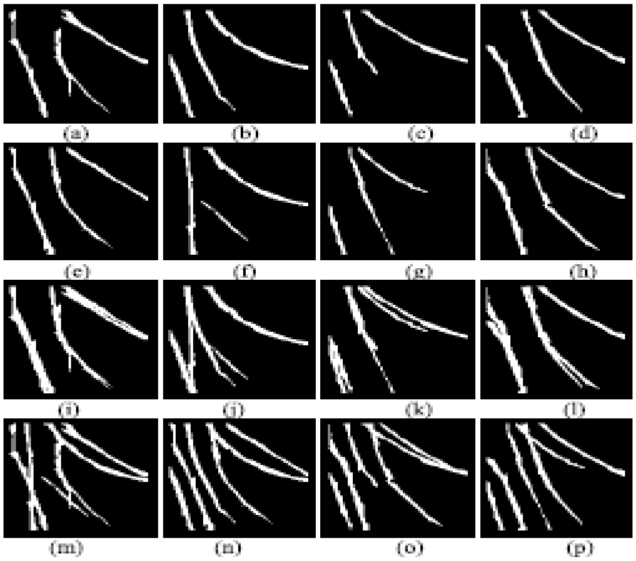


Figure 8: Principal lines images.

According to the fiure [Fig. 9 (i)-(l)] we can see that principal lines of palmprint image for a same subject palmprint images of left and reverse right are almost similar in shape and position but for different persons is is different[Fig. 9 (m)-(p)]. So accoding to this result it can be concluded that the this feature of palprint images can be deployed for palmprint verification.

In the proposed framework firstly left palmprint images and then right palmprint images are used for score calculation for each sample class After the matching score generation for each class is generated final fusion is performed for to obtain the identification result.

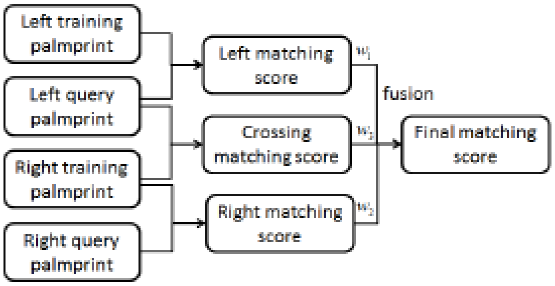


Figure 9: Fusion at the matching score level[4]

After obtaining all three scores final matching score is generated. Depending on the all the three matching scores ,final matching score is generated. After obtaining first and second score the third kind of score is calculated by performing crossing matching between the left and right palmprint. For an ith matcher wi (i = 1, 2, 3), which denotes the weight assigned to the ith matcher, score can be adjusted and viewed as the importance of the corresponding matchers.

In the proposed method a strategy is introduced in which crossing matching score is given to the fusion methodology. When w3 = 0, the proposed method is equivalent to the conventional score level fusion. Thus a performance enhancement is there for the proposed method compared to conventional methods by tuning the weight coefficients.

Fusion procedure for Biometric Features:

1) Score Normalization

For resizing the matching scores to a criterion between 0 and 1 Normalization is done. For both the scores normalization is done by:

$$N_{face} = MS_{face}-min_{face} / max_{face}- min_{face} \quad \_\_\_ \ (3)$$

$$N_{fingerl} = MS_{fingerl}-min_{fingerl} / max_{fingerl}-min_{fingerl} \quad \_\_\_ \ (4)$$

$$N_{finger2}= MS_{finger2}rmin_{finger2}/ max_{finger2}rmin_{finger2} \quad \_\_\_ \ (5)$$

$$N_{palm} = MS_{palm}-min_{palm} / max_{palm}-min_{palm} \_\_\_ \ (6)$$

Where min_{face} and max_{face} are the minimum and maximum scores for Face recognition and $min_{finger1}$and $max_{finger1}$ are the resultset values obtained from applying minutiae matching over fingerprint image. $min_{finger2}$ and $max_{finger2}$ are the resultset values obtained from applying Gabor filter over fingerprint image and min_{palm} and max_{palm} are the corresponding values obtained from palmprint image .

2) Fusion

The normalized values from finger , face and palm print images are fused using sum rule as -

$$MS = m*N_{face} + n*N_{finger1} + p *N_{finger2}+ q * N_{palm} \_ \ (7)$$

where m, n, p and q are four weight values that are assigned using the feature vector. If the value of matching score is less than the actual score it can be easily misleaded . So the value value of weight is assigned linearly.

CONCLUSION

As per the current proposed system accuracy rate in multimodal biometric system is greater than single biometric system. After experimentation it can be seen that the accuracy of system would increase on combination of multiple biometric features. The Genuine Acceptance Rate is also improved using multibiometric recognition and Neural Network approach. Also the system can be developed using five level biometric traits in future.

ACKNOWLEDGMENT

I take immense pleasure in expressing my humble note of gratitude to my guide Dr. Prateek Srivastava, Assistant Professor, Department of Computer Science and Engineering, SPSU, Udaipur, Rajasthan, India for his remarkable guidance and technical suggestions.

REFERENCES

Aizi K., Ouslim M. and Sabri A., 2015. “Remote Multimodal Biometric Identification Based on the Fusion of the Iris and the Fingerprint”, IEEE transactions on Information and Forensics, **12**(6).

Lee T. and Bong D., 2016. “Face And Palmprint Multimodal Biometric System Based on Bit-Plane Decomposition Approach”, In Proc. International Conference on Consumer Electronics-Taiwan, **114**(21).

Telgad R., Deshmukh P. and Siddiqui A., 2014. “Combination Approach to Score Level Fusion for Multimodal Biometric System By Using Face and Fingerprint” , In Proc. International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India.

Yong D., Bhowmik S. and Magnago F., 2015. “An effective Power Quality classifier using Wavelet Transform and Support Vector Machines”, Expert Systems with Applications, **42**(15):60-75.

Radha N. and Kavitha A., 2012. " Rank Level Fusion Using Fingerprint and Iris Biometric", Indian Journal of Computer Science and Engineering (UCSE) ISSN: 0976-5166, **2**(6).

Wang J.G., Toh K.A., Sung E. and Yau W.Y., 2007. "A Feature level Fusion of Appearance and Passive Depth Information for Face Recognition", Source: Face Recognition, Book edited by:Kresimir Delac and Mislav Grgic, ISBN978-3-902613-03-5, pp.558, I-Tech, Vienna, Austria.

Razzak M.I., Alghathbar M.K.K.K. and Yusof R., 2011. "Multimodal Biometric Recognition Based on

Fusion of Low Resolution Face and Finger Veins" , International ournal of Innovative Computing, Information and Control ICIC International 2011 ISSN 1349-4198, **7**(8):4679-4689.

Xu Y., Zhu Q., Zhang D. and Yang J.Y., 2011. “Combine crossing matching scores with conventional matching scores for bimodal biometrics and face and palmprint recognition experiments,” Neurocomputing, **74**(18): 3946–3952.

Jain A.K. and Feng J., 2009. “Latent palmprint matching,” IEEE Trans. Pattern Anal. Mach. Intell., **31**(6):1032–1047.

Jain A.K., Ross A. and Prabhakar S., 2004. “An introduction to biometric recognition,” IEEE Trans. Circuits Syst. Video Technol., **14**(1):4–20.

Xu Y., Zhu Q., Zhang D. and Yang J.Y., 2011. “Combine crossing matching scores with conventional matching scores for bimodal biometrics and face and palmprint recognition experiments,” Neurocomputing, **74**(18):3946–3952.

Telgad R.L. and Deshmukh P.D.,"Computer Aided Technique for Finger Print Image Enhancement and Minutiae Extraction "U.C.A., **75**(17).

Kumar A., Senior Member, IEEE, Sumit Shekhar," Personal Identification Using Multibiometrics Rank-Level Fusion", IEEETransactions On Systems, Man, And Cybernetics-PART C: Applications And Reviews.

Besbes F., Trichili H. and Solaiman B., 2008. Multimodal biometric system based on Fingerprint identification and Iris recognition,1I in Proc. 3rd Int. IEEE Conf. Inf. Commun. Techno!.: From Theory to Applications (ICTTA 2008), pp. 1-5. DOl: 10.1109/ ICTT A2008.4530129.

Rattani A., Kisku D.R., Bicego M., Member, IEEE and M. Tistarelli," Feature level fusion of face and finger Biometric".

Radha N. and Kavitha A.," Rank Level Fusion Using Fingerprint and Iris Biometric", Indian Journal of Computer Science and Engineering (UCSE) ISSN: 0976-5166, **2**(6).

Jain A.K, 2000. Fellow, IEEE, Salil Prabhakar,Lin Hong, and Sharath Pankanti, "Filterbank-Based Fingerprint Matching", IEEE transactions on Image processing, **9**(5).

Wang J. and Cheng J., 2010. "Face Recognition Based on Fusion of Gabor and 2DPCA Features", In International Symposium on Intelligent Signal Processing and Communication Systems, pp. 1-4.

Hancock P. 1. B., Bruce Y. and Burton A. M., 1997. "Testing Principal Component Representations for Faces", Proc. of 4th Neural Computation and Psychology Workshop.

Shlens J., 2005. "A Tutorial on Principal Component Analysis", Systems Neurobiology Laboratory, Ver.2.

Zhujie Y.L.Y., 1994. Face recognition with Eigen faces. Proc.IEEE Int!. Conf. Industrial Techno!. Pp: 434-438.

Patil S.S., Chandel G.S. and Gupta R., 2016. "Fingeprint Image Enhancement Techniques and Performance Evaluation of the SDG and FFT Fingerprint Enhancement Techniques ", International Journal of Computer Technology and Electronics Engineering (JJCTEE), ISSN 2249-6343, **2**(2):184-190.