Fingerprint and Face Recognition: Application to Multimodal Biometrics System

Wong Kin Fatt[1], Kushsairy AK[1], Haidawati Nasir[2], Sairul I Safie[3], Noor N.M[4]
[1]BMI, [2]MIIT, [3]MITEC, Universiti Kuala Lumpur.
[4]UTM Razak School, School of Engineering and Advance Technology.
wong.kin@s.unikl.edu.my

***Abstract*—Multimodal biometrics systems combine different unimodal biometric sources to achieve high recognition accuracy. By overcoming the limitation of unimodal biometric systems in this paper, a multimodal biometric recognition system which combines two modalities, fingerprint and face based on score level fusion is proposed. For fingerprint trait, the features are built based on the minutiae points of ridge area, while Local Binary Patterns (LBP) is used for face trait. The procedures of pre-processing, features extraction and matching are proceeding independently to obtain the individual matching scores. Afterwards, the two calculated results are combined by a matching score level fusion scheme to make the final decision on declaring the person as genuine or an imposter.**

***Index Terms*—Multimodal Biometric System; Fingerprint Recognition; Face Recognition; LBP; Minutiae; Fusion.**

I. Introduction

Nowadays, security system becomes more important than ever. It based on personal identity to recognize a person for purpose of means of access to physical and virtual domains. And, it is improved over time from traditional identification system to unimodal biometrics recognition system and then to multimodal biometrics recognition system.

The multimodal biometrics recognition system combines and integrates unimodal biometrics to become a better system to deter spoofing. Generally, biometrics refers to physiological or behavioral feature of a user. The physiological characteristics are related to the shape of the body such as fingerprint, palm veins, palm print, hand geometry, face, iris, retina, DNA, tooth, odor or scent, and etc. On the other hand, behavioral characteristics are related to the pattern of behavior of a person such as typing rhythm, gait, voice, signature, soft biometric information (gender, ethnicity and eye color, height, weight, tattoo, age, scar, mark) and etc.

The fusion of fingerprint and face recognition can form a good combination for a multimodal biometric system. As the fingerprint recognition is the most popular physiological characteristic used for authentication and authorization in biometric system. While, the facial recognition is more suitable for wide range surveillance and security applications. In this paper, Minutiae-based approach is used for obtaining the feature for fingerprint and Local Binary Patterns (LBP) approach for the face trait.

The paper is organized as follows. In Section 2, we describe the methods and procedures of the proposed system. In Section 3, we show the fusion score level of fingerprint and face matching method. In Section 4, we compare the results between the fusional and individual biometric traits. Finally, the summary and conclusions of this paper are shown in Section 5.

A. Previous Work

The multimodal biometric system in [1] is used to overcome the limitation of unimodal biometric system by enhance real time verification and reliability rate. The feature of face extract by Laplacian approach, while fingerprint by DFB approach.

A minimization of data storage by space specified tokens to encrypt the face image and encode into fingerprint image [2]. It provides a solution from spoofing in term of accuracy verification.

II. The Multimodal Biometrics System

A. The Fingerprint Recognition System

Basically, the fingerprint is formed by the combination of ridges and valleys (or furrows) on the surface of the finger. Ridges are the lines that create fingerprint pattern and shown as dark areas of the fingerprint. Valleys are the spaces between the ridges and shown as white areas of the fingerprint (as shown in Figure 1) [3]. The steps involved in fingerprint recognition using minutiae-based method after image acquisition are binarization, thinning, minutiae extraction, minutiae matching [4].

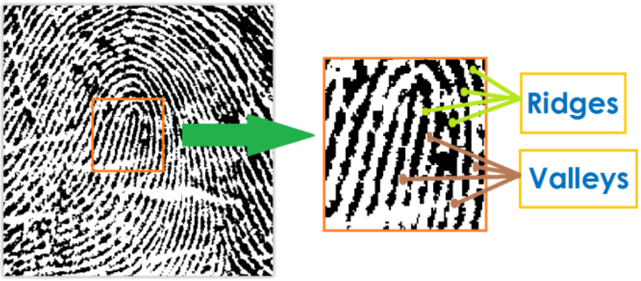


Figure 1: Ridges and valleys of a fingerprint [3]

a. Binarization

The binarization process convert the captured fingerprint image from grayscale to binary data (as shown in Figure 2).

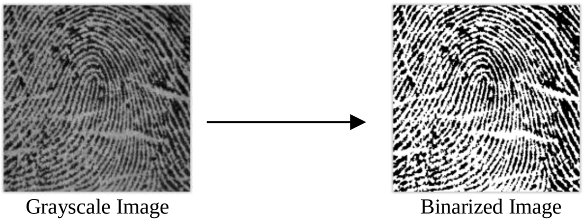
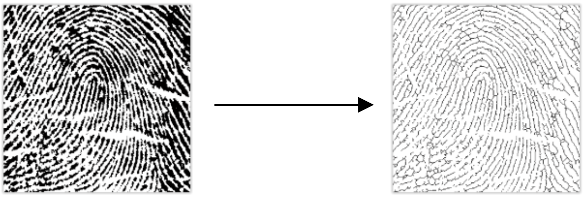


Figure 2: Binarization of fingerprint

b. *Thinning*

The binarized image is thinned to reduce the thickness of ridges to one pixel width for precise location of minutiae extraction as thinning does not change the location of the minutiae points compared to the original fingerprint (as shown in Figure 3).



Binarized Image

Thinned Image

Figure 3: Thinning of fingerprint

c. *Minutiae Extraction*

Generally, the minutiae features of the fingerprint among the ridges are ridge endings and bifurcations. These two basic minutiae features fit one another together to form lake, independent ridge, point or island, spur and crossover (as shown in Figure 4) [5].

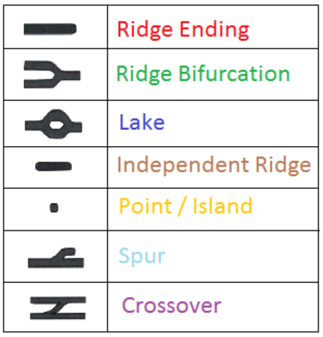


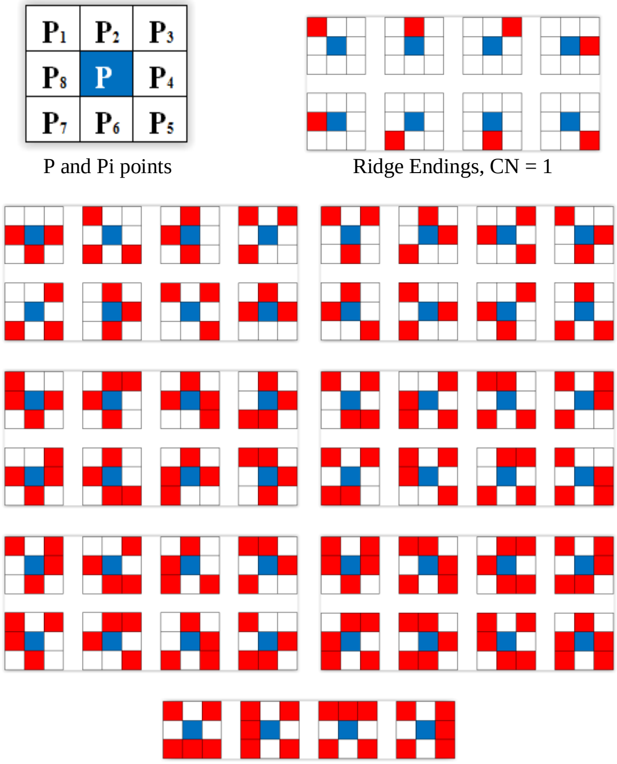
Figure 4: Minutiae Features [5]

The fingerprint features extraction is basically based on these two basic minutiae as they can be easily detected by only looking at points that surround them. The process of features extraction is as follows:

1. The minutiae points such as ridge endings and bifurcations are extracted by referring to the 3 x 3 neighbourhood pixels of neural network. The crossing number, CN (1) is used to determine and differentiate ridge endings and bifurcations through the neighborhood, P_i at center point, P. P_i is a binary number and P_9 is set as P_1 for the close loop sake (as shown in Figure 5).

$$CN = \frac{1}{2}\sum_{i=1}^{8}|P_i - P_{i+1}| \quad (1)$$

2. Filter the false minutiae according to a certain distance between ridge ending and bifurcation which form the typical minutiae such as lake, independent ridge, point or island, spur and crossover (as shown in Figure 4). An 11 x 11 closed curve is formed based on any point of ridge ending or bifurcation as center. If there is a ridge ending or bifurcation other than center minutiae found within the closed curve, then this said center minutiae will treat as false minutiae (as shown in Figure 6).
3. The minutiae points are then stored to form a feature structure set.

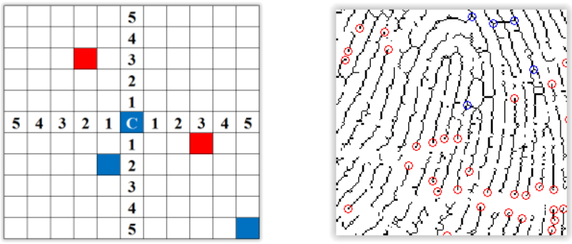


P and Pi points

Ridge Endings, CN = 1

Ridge Bifurcations, CN = 3

Figure 5: Minutiae Features



Blue = Ridge Bifurcation, Red = Ridge Ending, Distance = 5

Figure 6: False Minutiae Filtering

d. *Minutiae Extraction*

The minutiae-based method compares the similarity between the input (I) and template (T) minutiae sets. The matching score is calculated by Equation (2).

$$MS\_Finger = \frac{Matching\_Minutiae}{Max(NT\ , NI)} \quad (2)$$

where:

NI = total number of minutiae in the input matrix

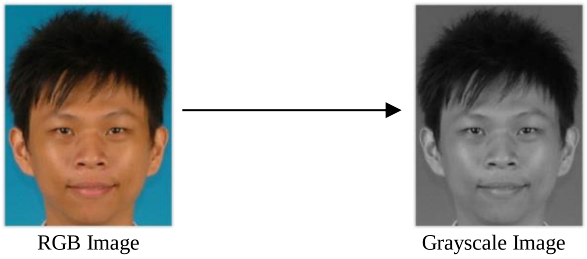
NT = total number of minutiae in the template matrix

B. *The Face Recognition System*

Human faces differ in thousand ways and we can describe them with the shape and structure of the organs such as eyes, nose and mouth in order to recognize them. So, the face recognition system extracts these facial organs together with their geometry distribution and the shape of the face [6] to measures the dimension, area and angle of organs that located on a face [7] to distinguish a person by Local Binary Patterns (LBP) [8] [9]. The steps involved in face recognition using LBP method after image acquisition are grayscale transformation, LBP features extraction, LBP histogram matching.

a. Grayscale Transformation

The captured facial image is converted from RGB into grayscale image (as shown in Figure 7).



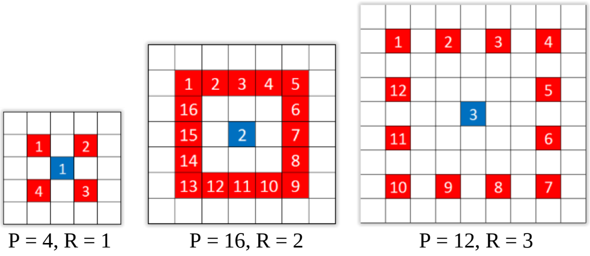
RGB Image

Grayscale Image

Figure 7: RGB to Grayscale

b. LBP Features Extraction

Local Binary Pattern LBP(P, R) is a method that is using circular neighborhoods to get the bilinear interpolating values of all sampling points around a centre point for any radius and any number of sampling points (as shown in Figure 9). The sampling points, P are equal pixels spacing on the edge of a circle with radius, R. The face features extraction is basically based on the circularly symmetric neighbour set that can be extended to consider different neighbourhood sizes [10]. For instance, LBP(16, 4) uses only 16 neighbours on a circle of radius 4 (as shown in Figure 8).



P = 4, R = 1

P = 16, R = 2

P = 12, R = 3

Figure 8: LBP circle neighbour-sets

The process of features extraction:

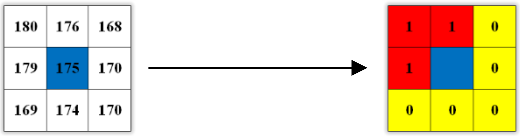
1. The intensity of the center point of the LBP(P, R) compare with each sampling point to obtain the uniform (binary) code. The uniform values are assigned with 1 when the intensity of sampling points are greater than or equal to the intensity of centre point and 0 for those intensity smaller than centre point (3) (4) (as shown in Figure 9).

$$LBP_{P,R} = \sum_{i=1}^{P} U(g_i\,, g_c) * 2^i \qquad (3)$$

$$U(g_i\,, g_c) = \begin{cases} 1 & if\ g_i \geq g_c \\ 0 & if\ g_i < g_c \end{cases} \qquad (4)$$

g_i = intensity of sampling points
g_c = intensity of center point

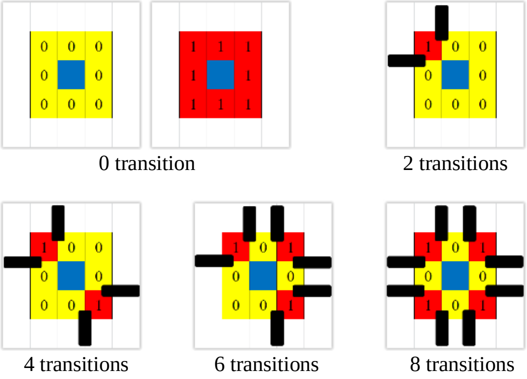
2. A filtering will be performed to reduce the noise. It'll keep 58 + 1 uniform patterns out of 256 uniform patterns in LBP(8, R). Therefore, there are 58 uniform patterns for 0 and 2 transitions. The rest are treated as non-uniform code and label as 1 uniform pattern (as shown in Figure 10).
3. The uniform code is then converted to decimal number known as LBP code (as shown in Figure 11) to obtain the LBP image shown in Figure 12. The LBP code determine by sum up all multiplication between uniform code and binary base accordingly.
4. The LBP image is divided to a number of regions and transforms them to individual histogram according to LBP code. These region histograms are collected to form a final histogram known as LBP labels (as shown in Figure 13).
5. The histogram of face is then stored to form a feature structure set.



180	176	168
179	175	170
169	174	170

1	1	0
1		0
0	0	0

Figure 9: Conversion of uniform code



0 transition

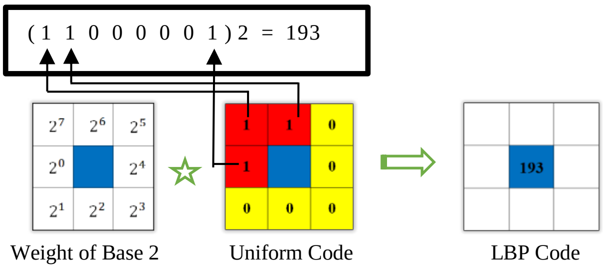
2 transitions

4 transitions

6 transitions

8 transitions

Figure 10: The transition within the uniform cord



(1 1 0 0 0 0 0 1) 2 = 193

2^7	2^6	2^5
2^0		2^4
2^1	2^2	2^3

1	1	0
1		0
0	0	0

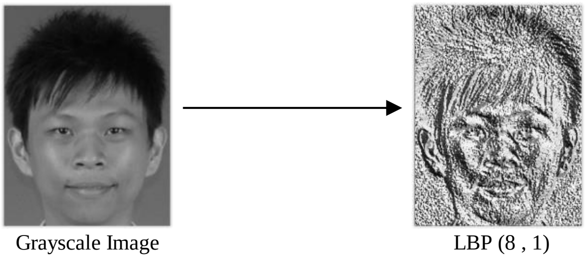
	193	

Weight of Base 2

Uniform Code

LBP Code

Figure 11: Transformation of LBP code



Grayscale Image

LBP (8 , 1)

Figure 12: Example of LBP image

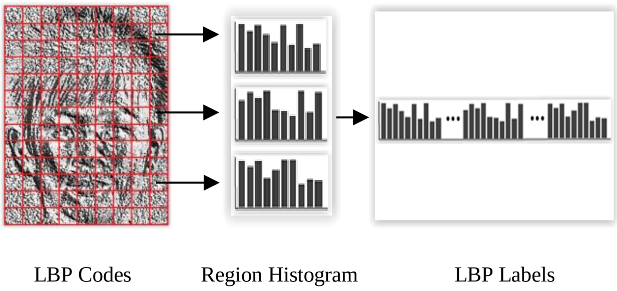


Figure 13: LBP Histogram

c. LBP Matching

The LBP method compare the dissimilarity between the LBP label of input (I) and template (T). The matching score is calculated by Equation (5) [11].

$$MS\_Face\_Dissimilarity = \sum_{n=1}^{N} \frac{|I_n - T_n|}{I_n + T_n} \quad (5)$$

In this paper, similarity score is considered. So, the matching score of dissimilarity will be converted to similarity score by Equation (6) [11].

$$MS\_Face = 1 - MS\_Face\_Dissimilarity \quad (6)$$

III. The Fusion Score Level

Figure 14 shows the block diagram of the proposed multimodal biometric recognition system integrating fingerprint and face. This system involves image pre-processing, feature extraction, matching and decision-making. In operational side, two biometric sensors individually capture two biometric characteristics from a person. The captured images are then processed by two feature extraction modules and generate matching scores respectively.

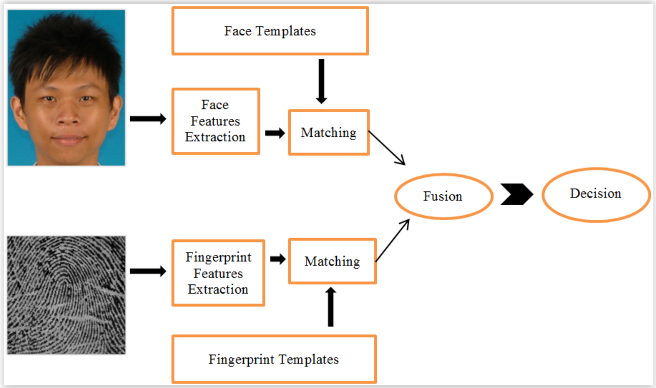


Figure 14: Block-diagram of multimodal biometric system

The two similarity matching scores combine and pass to fusion module to generate a fusion matching score by sum rule (7) [12].

$$MS\_Fusion = MS\_Finger + MS\_Face \quad (7)$$

Lastly, the fusion matching score pass to the decision module and compare against a threshold value to recognize the person as genuine or an imposter.

IV. Results and Discussion

The databases that are used in this work are UPEK Fingerprint Database and GUFD Face Database. 30 samples from each database are selected to run 4 cycles in the system respectively. For the personal data, the sample of fingerprint randomly matches with the sample of face and take it as a user.

Table 1 shows the result of the proposed multimodal biometrics system. The fusion approach (98.1%) provides a higher matching result if compare to the standalone fingerprint (91.6%) and face (87.4%) recognition system.

Table 1
Recognition Result

Trait	Method	Accuracy (%)	Sample
Fingerprint	Minutiae	91.6	30 x 4
Face	LBP	87.4	30 x 4
Fusion	Sum Rule	98.1	30 x 2 x 4

The performance of a biometric system is commonly evaluated by the Receiver Operating Characteristic (ROC) curve. The ROC curve corresponds to a graphical visualization of the probability of False Accept Rate (FAR) against probability of False Reject Rate (FRR) for different values of the decision threshold.

FAR is the percentage of imposters that incorrectly get accepted by the system with a matching score greater than or equal to threshold, meanwhile FRR is the percentage of genuine that incorrectly get rejected by the system with a matching score less than threshold. Moreover, the True Accept Rate (TAR) is the percentage of genuine that gets accepted by the system (8).

$$TAR = 1 - FRR \quad (8)$$

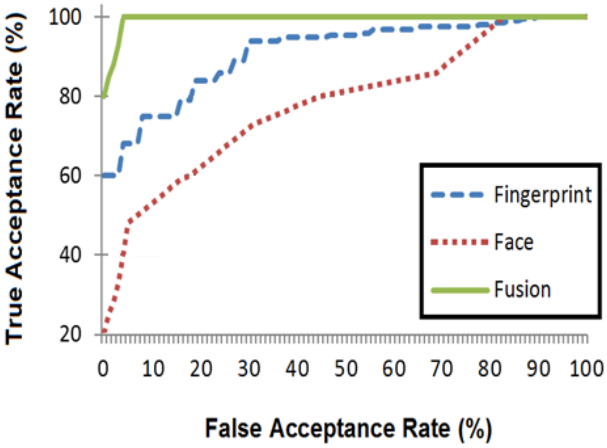


Figure 15: Receiver Operating Characteristic, ROC curve

Thus, the ROC curve of this proposed method is plotted with TAR versus FAR (as shown in Figure 15) by using matching scores for different users at different thresholds for better expression.

It is observed from the ROC curve that the performance gain obtained from the fusion system is higher when compare to the two individual traits (fingerprint, face) as it is evident from the ROC curves in Figure 15.

Table 2
Performance of the Proposed System

Biometrics	Biometrics Parameters						
	1	2	3	4	5	6	7
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	H
Signature	L	L	L	H	L	H	L
Voice Print	M	L	L	M	L	H	L
Thermo gram	H	H	L	H	M	H	H
Retinal Scan	H	H	M	L	H	L	H
Vein	H	M	M	M	H	M	L
Fingerprint + Face	H	H	H	M	H	M	L

H = High, M = Medium, L = Low

Table 2 shows the performance of the proposed system based on seven parameters below [13] to decide whether a human trait can be used as biometric or not. In the proposed system, the two traits (fingerprint and face) are fused to increase the performance of the system.

1. Universality means every individual should have the biometric trait and characteristic.
2. Distinctiveness ensures that every individual should be distinguishing in terms of the biometric traits when compared between each other.
3. Permanence means the biometric trait of an individual should be remaining constant over a period of time such as aging and other variance.
4. Collectability means data gathering process and techniques should be as simple as possible which without any inconvenience to the user.
5. Performance relates to accuracy, speed and robustness of the technology used.
6. Acceptability means the user acceptance without objection to the collection of the biometric and the ease and convenience of use of the technology.
7. Circumvention relates to the ease with which the biometric trait can be deceived with a substitute to cheat the system.

V. Conclusions

Biometric features are unique to each individual and remain unaltered during a person's lifetime. The fingerprint features are extracted by minutiae-based method and face by local binary pattern, to generate the matching scores respectively. These two scores of biometric traits combined and carried out the final matching score by fusion method. The system will base on the fusion matching score to define the owner.

[14]

The proposed multimodal biometric system based on the fusion of fingerprint and face performs much better than the unimodal biometric systems of fingerprint and face which using the same technique. However, there is still room for improvement in fusion approach. As the weight of sum rule might improve the accuracy of the recognition system. The fingerprint recognition system can perform better than face recognition system; therefore it might get a higher weight in order to increase the performance of the multimodal biometrics system.

Acknowledgement

This research was supported by grant from FRGS/1/2014/TK03/02/1.

References

[1] Aloysius George. 2008. Bizarre Approaches for Multimodal Biometrics. IJCSNS *International Journal of Computer Science and Network Security*, 8(7).

[2] B. Prasana Lakshmi & A. Kannammal. 2009. Secured Authentication of Space Specified Token with Biometric Traits – Face and Fingerprint. *IJCSNS International Journal of Computer Science and Network Security*, 9(7).

[3] Davide Maltoni and Dario Maio. 2009. *Handbook of Fingerprint Recognition*. Springer.

[4] N. Zaeri. 2011. Minutiae-based Fingerprint Extraction and Recognition. Biometrics. Dr. Jucheng Yang (Ed.), ISBN: 978-953-307-618-8, *InTech*.

[5] D. Maltoni, D. Maio, A. K. Jain, S. Prabahakar. 2003. Handbook of Fingerprint Recognition. *Springer*.

[6] Dirk Colbry, George Stockman, and Anil Jain. Detection of Anchor Points for 3D Face Verification.

[7] Ilker Atalay. Brief Introduction to Pattern Recognition; Face Recognition; Face Recognition Using EigenFace.

[8] T. Ojala, M. Pietikainen, and D. Harwood. 1996. A Comparative Study of Texture Measures with Classification Based on Feature Distributions. *Pattern Recognition*.

[9] T. Ahonen, A. Hadid, and M. Pietikainen. 2006. Face Description With Local Binary Patterns: Application To Face Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*.

[10] T. Ojala, M. Pietik¨ainen, and T. M¨aenp¨a¨a. 2002. Multiresolution Gray-Scale and Rotation Invariant Texture Classification With Local Binary Patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24:971–987.

[11] R. Shyam, Y.N. Singh. 2015. Face Recognition Using Augmented Local Binary Pattern And Bray Curtis Dissimilarity Metric. *2nd International Conference on Signal Processing and Integrated Networks (SPIN)*, 779-784.

[12] Timo Ahonen, Abdenour Hadid, Matti Piesetikainen. 2006. Face Description With Local Binary Patterns: Application to Face recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 28(12): 2073-2041.

[13] S. Ravi, Dattatreya P. Mankame. 2013. Multimodal Biometric Approach Using Fingerprint, Face and Enhanced Iris Features Recognition. *International Conference on Circuits, Power and Computing Technologies*, 1143-1150.