

An Improved Biometric Fusion System of Fingerprint and Face using Whale Optimization

Tajinder Kumar¹

Department of Computer Science
& Engineering
IKG Punjab Technical University
Kapurthala, Punjab, India

Shashi Bhushan²

Department of Computer Science
and Engineering, Chandigarh
Group of College, Landran,
Punjab, India

Surender Jangra³

Department of Computer Science,
GTBC, Bhawanigarh, Punjab, India

Abstract—In the field of wireless multimedia authentication unimodal biometric model is commonly used but it suffers from spoofing and limited accuracy. The present work proposes the fusion of features of face and fingerprint recognition system as an Improved Biometric Fusion System (IBFS) leads to improvement in performance. Integrating multiple biometric traits recognition performance is improved and thereby reducing fraudulent access. The paper introduces an IBFS comprising of authentication systems that are Improved Fingerprint Recognition System (IFPRS) and Improved Face Recognition System (IFRS) are introduced. Whale optimization algorithm is used with minutiae feature for IFPRS and Maximally Stable External Regions (MSER) for IFRS. To train the designed IBFS, Pattern net model is used as a classification algorithm. Pattern net works based on processed data set along with SVM to train the IBFS model to achieve better classification accuracy. It is observed that the proposed fusion system exhibited average true positive rate and accuracy of 99.8 percentage and 99.6 percentage, respectively.

Keywords—Biometric fusion; face recognition; fingerprint recognition; feature extraction; feature optimization; classifier

I. INTRODUCTION

The unimodal biometric systems are prone to the inconsistencies scores and outliers [1]. However, fusion biometric systems or multi model systems play a crucial role in providing accuracy, security, universality and cost-effectiveness. Various research papers has focused on the face and fingerprint-based fusion system, but classification accuracy has not been achieved so far. This work aims to present a new biometric system that overcomes the problem of authenticity and employs fusion of faces and fingerprint traits [2]. The paper organizes in following sections: Section 2 defines the existing work in fingerprint and face biometric traits in the form of related work. Section 3 presents the formulation of multimodal fusion system. In Section 4, experimental results are considered, and Section 5 states the vital conclusions.

II. RELATED WORK

Nagar et al. had studied the fusion of three biological features (fingerprint, face and iris). It has been proved that multi-biometric systems show a great similarity check and possess high security although it requires a large storage space to save multiple templates of the input data. Here fuzzy vault and fuzzy commitment model was used to form a biometric encryption system framework [3]. A lot of work has

been implemented in the fields of biological key using unimodal biometric system in which algorithm utilized user-key and biometrics authentication [4]. The Dialog Communication Systems developed BioID which is a multimodal identification system that uses three different features: voice, face and lip movement-to recognize people [5]. The present work involves the design of new soft biometric database with a human face, body with clothing attributes at three different distances for investigates indirect influence on the soft biometric fusion [6]. Thereafter authors has been designed multimodal biometric approach and validated on three chimeric multimodal databases such as face, fingerprint and Iris. The performance of this work has been analyzed in terms of Decidability Index (DI), Equal Error Rate (EER), and Recognition Index (RI). Present approach outperforms existing methods by achieved an accuracy of 99.5%, an EER of 0.5% [7]. A novel multi-modal biometric system based on face and fingerprint resolves the issues like noise sensor data, non-universality, susceptibility to forgery and deficiency of invariant representation. The fingerprint matching has been performed through alignment-based elastic algorithm. To get the improved feature extraction, extended local binary patterns (ELBP) has been utilized. This work has been examined on FVC 2000 DB1, FVC 2000 DB2, ORL (AT&T) and YALE databases and accomplished 99.59% of accuracy [8]. The authors have introduced and examined the concepts of dual authority with authentication-based scheme on the basis of biometric along with its influencing factors of recognition rate in biometrics. However the singular model authentication approach does not guarantee the security of jurisdictions in a common regulatory area. By increasing the number of experiments, the average time for face recognizing reduces and leading to the stable value and the rate of recognition to be 92.2%. The authors has explored the ways to enhance the performance of rank identification in Automated Fingerprint Identification Systems (AFIS) while only a partial latent fingerprint has been made available. The preset work approach exploits extended fingerprint features (unusual/rare minutiae) not commonly considered in AFIS. This novel approach has combined with existing minuate-based matcher. A realistic forensic fingerprint casework database comprising of rare minutiae features obtained from Guardia Civil, the Spanish law enforcement agency has been utilized here [9]. The authors have presented a novel multimodal biometric fusion system using three different biometric modalities such as face, ear and gait based on speed-up-robust-feature (SURF) descriptor including genetic algorithm (GA). ANN has been utilized to

classify the biometric modality. The work has been observed on three databases namely AMI ear, Georgia Tech face and CASIA Gait database. Before fusion, SURF features have been optimized through GA and further cross-validated using ANN [10]. The authors have presented two level score level fusion method for the merger of scores being obtained from the cancel-able template of various biometric characteristics. The framework has been run on two virtual databases. The results have shown that the proposed amalgamation have optimized better performance than the uni-biometric system [11].

III. PROPOSED MULTI-MODAL FUSION SYSTEM

This section covers the architecture of the proposed biometric system which is based on fingerprint and face. The simulation of proposed work includes the improved finger print recognition system, frame work of improved biometric fusion system and improved face recognition system is as follows:

A. Database

Quality data mining is the first and the most key aspect of any prediction model. The data sets used in the proposed work represents the collection of face and fingerprint images. Fingerprint images have been collected from FVC fingerprint database and face images were collected from Georgia Tech face database . Fingerprint data corresponds to high resolution gray scale images in *.tif format. Face images are found in *.jpeg format and are represented by 150 pixels square matrix. Database has collection of images with variation of lighting and scale.

B. Framework of IBFS

The multi-modal bio-metric system deals with improvement of the performance by using enhancement of quality of the input data. It is employed to enhance the accuracy and security of the bio-metric recognition systems. Thus, multi-modal fusion systems has proved to be more accurate . Multi-modal systems also provide knowledge about the sample being entered by applying liveness detection techniques. Spoofing is thus far easily detected.

There are various ways to measure the efficiency of IBFS.

- 1) Collectability: Provides the manner in which the person's trait is measured and processed.
- 2) Uniqueness: Determines the uniqueness of the user through the recognition of bio-metric system.
- 3) Performance: It provides the Robustness, accuracy, speed and fault handling achieved using system.
- 4) Universality: The requirements for unique characteristics of each person in the world is known. These cannot be reproduced.
- 5) Permanence: Provides the time frame for recording the personal trait in the database

In this work, IBFS fusion architecture taken into consideration. More information is contained in the feature set about the input bio-metric data than the matching score or the output decision of a matcher. When fusion is done at the feature level better recognition results are generated. To do this first step requires pre-processing of the data. However, there is difficulty in pre-processing which is to acquire a better quality

of input image for bio-metric system. This paper proposes a new method to increase the accuracy of IBFS and optimizes the accuracy of bio-metric traits, which is disturbed in case of noisy data. It uses the fusion levels algorithms between face and fingerprints recognition system [12] [13]. The first system is created combining the fingerprint verification with the Atmospheric Light Adjustment (ALA). It uses Whale Optimization based on minutiae feature extraction technique. The second system used in the multi-modal makes use of face verification by employing Whale optimization based on Maximally Stable Extremal Region (MSER) extraction technique. Both the systems together are then trained using pattern net. Fingerprints are considered and accepted mostly for the identification of person due to their uniqueness and nature of immutability. Even stored and classified using SVM for better accuracy. In this work, the traits of face and finger are considered. Fig. 1 shows the framework of proposed IBFS.

1) *Framework of Proposed IFPRS*: A fingerprint refers to the assortment of furrows and ridges found on the tip of a finger. In local parlance ridge pattern is known as oriented texture pattern comprising of orientation and dominant frequency. Capturing the orientation and dominating frequency of ridges in fingerprint, leads to a distinct representation of this texture [14]. These are commonly categorized into five different types: whorl, left loop, right loop, arch, and tented arch. Fingerprints are considered and accepted mostly for the identification of person due to their uniqueness and nature of immutability. Laptops and smart phones are using this technology in the form of a password to unlock the screen. It is used in residential system for attendance and time. For most recognition systems, problems arise for identifying fingerprints of same type. In general recognition systems employ neural networks to detecting the minutiae's, and the ridge ends in fingerprints. This helps in matching the fingerprint. The problem lies in feature extraction as extracted features vary in length. The second difficulty is due to irrelevant noise caused while obtaining the fingerprint in the online mode from the biometric sensor. A lot of noise is added in the fingerprint images. This results difficulties in formulating a classification system. These difficulties are overcome by using pre-processing, feature extraction, optimization before using classification of biometric features.

Fingerprint Pre-processing: In case of image analysis fingerprint pre-processing provides great results. The main features used in fingerprint pre-processing are subdivided into two types local and global features. The Local features use the minutiae information whereas the secondary features employ the local area information which does not vary with global transformation. The global features include type, number, and the position containing the singularities that includes geometrical and spatial relationship of attributes of size, ridge lines, and shape of the fingerprints [15]. The pre-processing steps applied on the uploaded fingerprint images for enhancing the quality is described below:

Conversion using Color: Color conversion helps in finding the luminance of the fingerprint image which further used in extraction process [16].

$$GrayIm = 0.299 * R_1 + 0.587 * G_2 + 0.114 * B_3 \quad (1)$$

Where GrayIm: Gary image

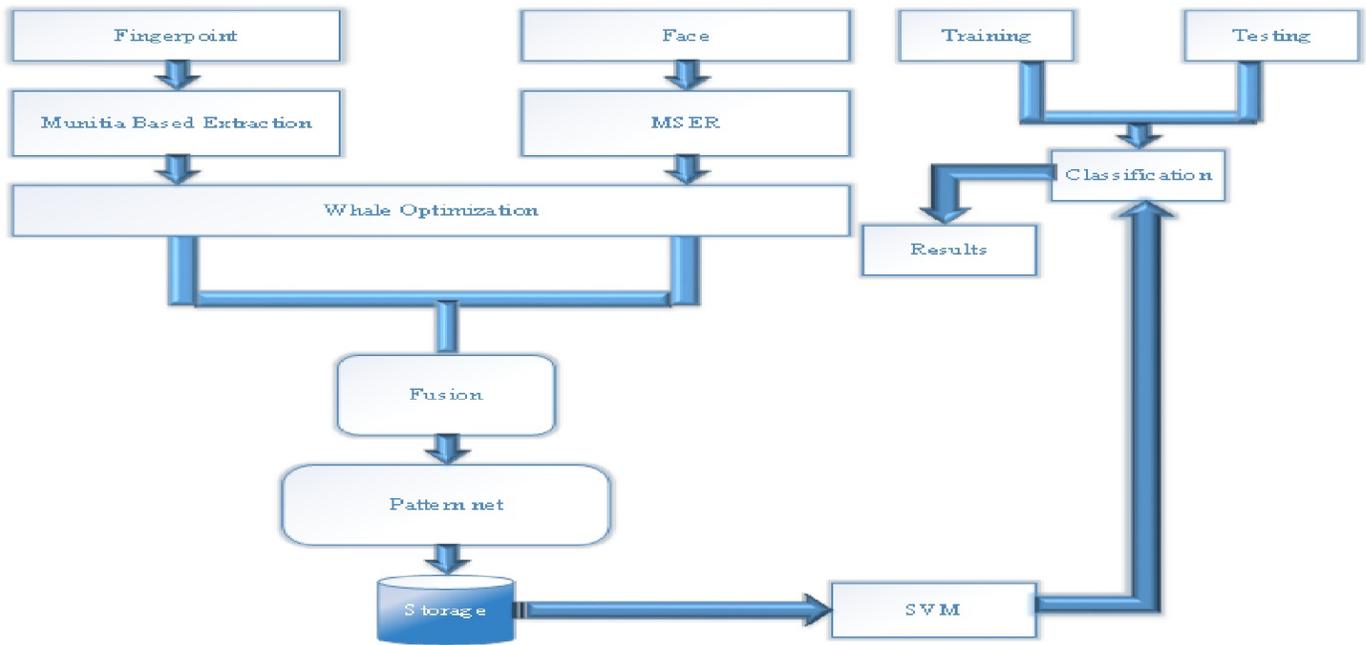


Fig. 1. Framework of Proposed IBFS.

R₁: Red image component
G₂: Green image component
B₃: Blue image component

Image Enhancement: To fix specific pixel points in the image enhancement is used. For improving the quality of fingerprint ALA image enhancement technique is used. This algorithm helps to find the exact minutiae feature of fingerprint.

Algorithm 1: ALA Algorithm

1. Input: Image_{gray}
2. Define variable: Img = double(Image_{gray})
3. Determine: [Image_{height}, Image_{width}, Image_{plane}] = size(Image_{gray})
4. Assign Variables: patch_{size} = 15 // here parts of images are considered
5. pad_{size} = 7 // it demonstrates the extra boundary
6. Determine: P_{mask} = padarray(I, [pad_{size}, pad_{size}]) // generates empty mask of pad_{size}
7. For each j value in Image_{width}
8. For each i value in Image_{height}
9. Construct: patch_{matrix} = pmat(i_{value}:(i_{value}+ patch_{size}- 1), (j_{value}+ patch_{size}- 1), All)
zmat(i_{value}, j_{value}) = min(patch_{matrix} (:))
10. end for
11. end for
12. Apply: A = atmosLight(double(Img), zmat, plane) //applies Atmospheric Light adjustment
13. Image_{Opt} = 1 - zmat

14. Image_{enhance} = Zeros(size(Img)) //creates an empty matrix of size of I

15. for each ind_{value} inplane

16. Image_{enhance}(:,:,ind) = (A(ind) + (Img(:,:,ind) / (max(Image_{opt}, 0.1))))
//where 0.1 is the lightening coefficient

17. end for

18. Output: Image_{enhance}

Fingerprint Feature Optimization (FOP): FOP results in optimizing and reducing the number of features in the data set. It includes selection of features, variable and attributes . These selection techniques are employed for simplifying the models for easy understanding and interpretation by the users.

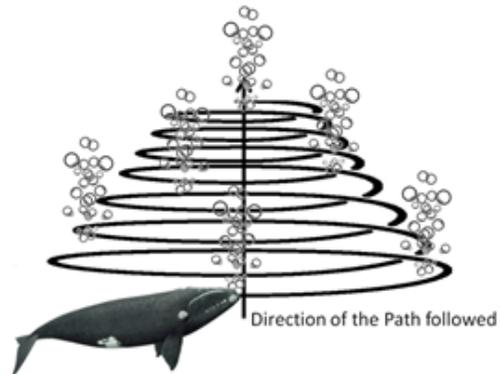


Fig. 2. Whale Optimized Algorithm Inspired by Behavior of Whales.

There is another technique that is similar to FOP and used

for dimensionality reduction .The difference lies in creating new combination of features whereas feature optimization only excludes and includes the features. The Whale algorithm is used as feature optimization technique. Fig. 2 depicts the inspiration taken from the biological behavior of the whales which corresponds to the typical path followed by Whale Algorithm to achieve an optimized solution.

There are two phases of the algorithm, exploitation and exploration phase. In the exploitation phase whale follows the spiral path to encircle the prey as shown in Fig. 2. In the second phase, prey is randomly searched.

Mathematical explanation of Exploitation Phase:

Prey encircling: It works on two assumptions, firstly, that the target prey is the principal candidate for achieving the most favorable solution. Secondly, other search mediators continuously change their positions in response to search agent. This behavior is represented as follow:

$$Pw_{(itr+1)} = Pp_{itr} - A_{coeffvect} * D_{vect} \quad (2)$$

$$D_{vect} = |B_{coeffvect} * Pp_{itr} - Pw_{itr}| \quad (3)$$

Where, Pp_{itr} is the whale's last position at iteration 'itr' also corresponding to the prey position, $Pw_{(itr+1)}$ is the whale's present position, distance between prey and whale is represented by D_{vect} , $A_{coeffvect}$ and $B_{coeffvect}$ are coefficient vectors represented as follows:

$$A_{coeffvect} = 2 * A_{vect} * r_{vect} + A_{vect} \quad (4)$$

$$B_{coeffvect} = 2 * r_{vect} \quad (5)$$

In order to shrink the search space corresponding to the spiral path followed by the whale, the value of A_{vect} is reduced thereby decreasing the oscillating range of A

Updating Spiral Path Position: Let us consider the whale position coordinates as (Pw,Qw) and prey position coordinates as (Pp,Qp). The spiral path followed by the whales is represented as follows:

$$Pw_{(itr+1)} = exp^{CR} * cos(2\pi R) * Dp_{vect} + Pp_{itr} \quad (6)$$

$$D_{vect} = |B_{coeffvect} * Pp_{itr} - Pw_{itr}| \quad (7)$$

Where, C represents the constant that determines the logarithmic shape of the spiral path and R is the random variable lie between -1 and +1. There always lies a 50% chance that the search mechanism will follow a spiral or shrinking encircling design. The selection is done as follows:

$$Pw_{(itr+1)} = \begin{cases} Pp_{itr} - A_{coeffvect} * D_{vect} & \text{if } R < 0.5 \\ exp^{CR} * Dp_{vect} + Pp_{itr} & \text{if } R \geq 0.5 \end{cases} \quad (8)$$

Mathematical explanation of Exploration Phase. In search phase, position of the search agent is determined in respect to the randomly selected search gents and not with respect to the best search agent. This mechanism corresponds to the strengths of WOA to deal with the shortcoming associated with the local optimization problems. The model is represented as follows:

$$Pw_{(itr+1)} = Pw_{rand} - A_{coeffvect} * D_{vect} \quad (9)$$

$$D_{vect} = |B_{coeffvect} * Pw_{rand} - Pw_{itr}| \quad (10)$$

Where, Pw_{rand} represent the position of a random whale within the population. The Whale optimization algorithm is as follows:

Algorithm 2: Whale Optimization Algorithm

1. Input: F_{points} //Feature points of fingerprint Image_{enhance}
2. Output: Image optimized //optimized feature points
3. Initialize parameters: Itr // Search agents, L_{BN} //lower bound of "N" variables

U_{BN} //upper bound of "N" variables

F_{fit} //fitness function

4. Calculate: $T=size(F_{points})$ // size of the input image

5. for each i value in T

6. Calculate: $F_{pointsselected} = \sum_{i=1}^T F_{points}(i_{value})$

// value for selected F-point in terms of N

7. Calculate:

$$F_{pointsthreshold} = \frac{\sum_{i=1}^T F(i)}{Length(F_{points})}$$

$F_{pointsthreshold}$ is threshold which should be achieved by supervisor N with respect to threshold F-Points

8. Calculate: Fitness

$$F_{fit} = \begin{cases} False, & F_{pointsselected} < F_{pointsthreshold} \\ True, & F_{pointsselected} \geq F_{pointsthreshold} \end{cases}$$

Calculate: $Opt_{value} = WOA(F_{fit}, N, L_{(BN)}, U_{BN})$

end for

While Itr \neq max(T)

Assign: $F_{points} = Opt_{value}$

End while

Output: Image optimized = optimize(F-points) //optimized fingerprint image

2) *Framework of Proposed IFRS:* Face recognition helps in contributing to the IBPS. Bio-metrics of face help in identifying persons of interest and are used to verify their identities. It also helps in gathering the demographic data on large amount of people [17]. This has led to increase in demand for retail marketing. Fig. 3 describes the framework of proposed IFRS. Face is a complex multidimensional structure. There is a need to enhance the input data and computing it with better recognition techniques. Pre-processing of data helps in the feature extraction and optimization and overcome the difficulties faced during face recognition.

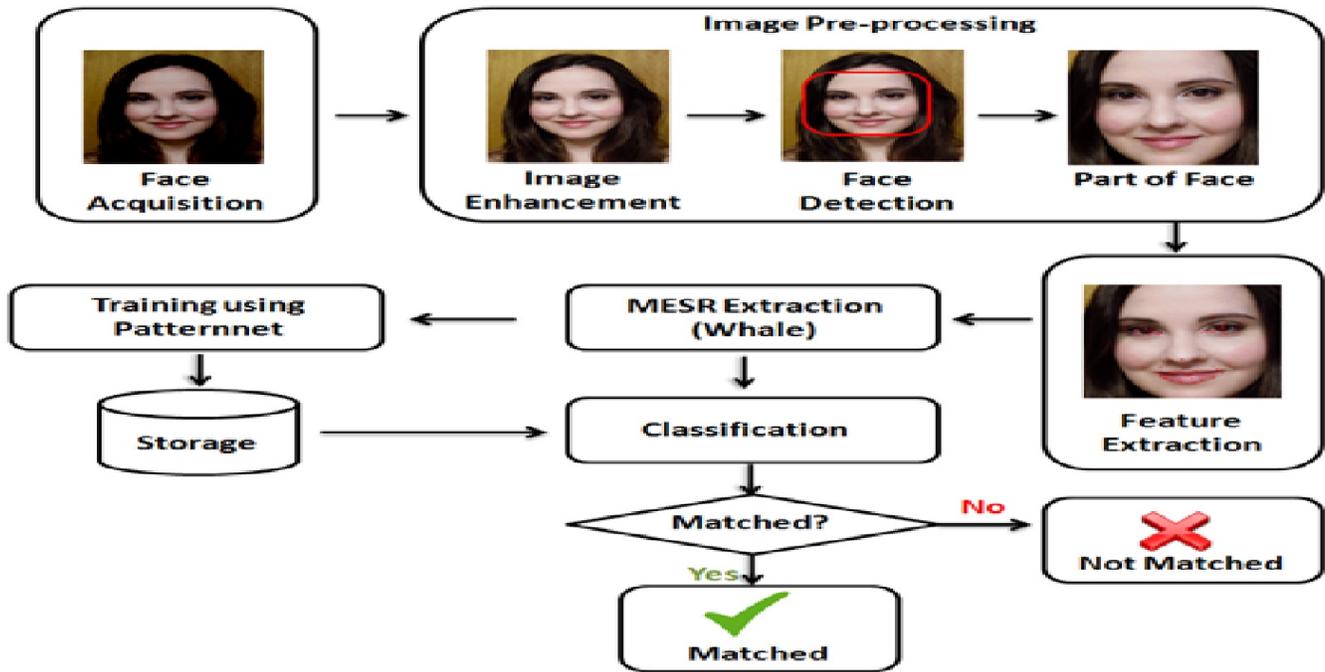


Fig. 3. Framework of Proposed IFRS.

3) *Face image pre-processing*: Facial feature point detection provides many applications such as recognition of face, tracking hallucination, animation and 3D analysis [18]. The first process of pre-processing includes Face data acquisition (FDAQ) which includes uploading the captured face images. FDAQ Algorithm extracts the Region of Interest (RoI). The pre-processing algorithm is given as:

Algorithm 3: Pre-Processing for IFRS

1. Input: $Image_{face}$ //upload image for face recognition
2. for each i_{value} in $Image_{face}$
3. Apply: $Image_{resize}=Resize(Image_{face}(i))$
4. Apply: $image_{detect}=FaceDetector(image_{face}(i))$
5. Calculate: $Image_{bound}=boundary(Image_{detect})$ //find boundary of face detection image
6. Calculate: $Image_{th}=Threshold(Image_{detect})$ //calculate threshold
7. Calculate: $Image_{gray}=GrayConversion(Image_{detect},Image_{th})$
8. Calculate: $Image_{RoI}=crop(Image_{gray},Image_{bound})$
9. end for
10. Output: $image_{RoI}$ //pre-processed face image

This procedure helps to obtain the pre-processed RoI image. MSER Extraction applied after pre-processing helps in finding optimized features.

4) *MSER extraction*: MSERs are used to detect blobs in images. The blobs can be a symbol, text character and content that the MSER algorithm identifies. It reduces the computational overhead by identifying the regions of the image that contains text as to determine whether a region is a true

character or not [19]. Having the property of performing well on homogeneous regions it works well in this case. It provides robustness for large scale images and helps in improving matching performance. In such a case, it performs best when applied in proper strategy. This works as one of the fastest region detectors. Algorithm 4 provides the steps needed to implement MSER.

Algorithm 4: MSER Algorithm

1. Input: $Image_{RoI}$ // upload image
2. Calculate: $[R.C]=size(Image_{RoI})$
3. for each r_{value} in R
4. for each c_{value} in C
5. Calculate: $Image_{intensity}=intensity(Image_{RoI}(r,c))$
6. Calculate: $Image_{components}=component(Image_{intensity}(r,c),8)$
7. $Image_{th} = stable(Image_{components})$
8. $Filter_{points} = filter(Image_{th})$
9. Check: if $Image_{th} == True$
10. $MSER_{points} = Filter_{points}$
11. end if
12. end for
13. end for
14. Assign: $F_{points} = MSER_{points}$
15. Output: F_{points}

5) *Optimization of features of face:* To generate the unique feature sets optimization is applied. Optimization generates best features which are used for face detection. Using Whale algorithm, MSER points are optimized.

C. Training of Proposed Model

The training of the system is done using pattern net. To train the proposed system, Pattern net is used with the optimized feature set. Both systems fuse together to provide the training data for the model. This is called Optimized Pattern net, which is used to leverage the filters in the last convolution layer of a convolution neural network . This helps to find locally consistent visual patches. The visual patterns are discovered efficiently due to Pattern net. To enhance the classification accuracy of the system SVM is used along with Pattern net in the recognition system.

IV. RESULTS

Table I summarizes the images and the stages of image processing in IFPRS and IFRS bio-metric fusion model. Column 2 labels the image processing stages and column 3 and column 4 corresponds to the respective image processing results of IFPRS and IFRS

Experimental evaluation of performance of bio-metric fusion model: The Precision, Recall, F-measure, and Accuracy are calculated while considering confusion matrix parameters for evaluating the performance of machine learning in our proposed model using following formulas:

- 1) Precision

$$Precision = \frac{T_{positive}}{T_{positive} + F_{positive}} \quad (11)$$

- 2) Recall

$$Recall = \frac{T_{positive}}{T_{positive} + F_{negative}} \quad (12)$$

- 3) F_{measure}

$$F_{measure} = \frac{precision * recall}{precision + recall} \quad (13)$$

- 4) Accuracy

$$Accuracy = \frac{T_{positive} + T_{negative}}{T_{positive} + T_{negative} + F_{positive} + F_{negative}} \quad (14)$$

Table II summarizes the performance parameters obtained for the bio-metric fusion system over a range of image samples. It is observed that with the increase number of image samples , there is an increase in the number of true positive results which predicts the better performance of classification model.

The parameters, namely, TP, TN, FP, FN are essential for predicting the performance of machine learning classification. Fig. 4 represents the number of image samples used in the bio-metric fusion model. These are plotted on X-axis against the measurements of confusion matrix parameters in percentiles on Y-axis. It is observed that with increase in the number of image samples increases in the number of TP and corresponding reduction in the number of TN, FP and FN values. Initially when 10 image samples are used the TP observed is 70% with

TN, FP and FN as 10% each. As the sample size increases to 100, TP rises to 95% and TN, FP and FN falls to 2%, 1% and 2% respectively. Further it is observed that when the sample size increases to 500, the system achieved improved TP of 99.2% with traces of TN, FP and FN corresponding to 0.4%, 0.2%, and 0.2% respectively. In other words, the plot implies the prevalence of least error in the proposed bio-metric fusion model. Fig. 5 evaluates the precision, sensitivity and accuracy

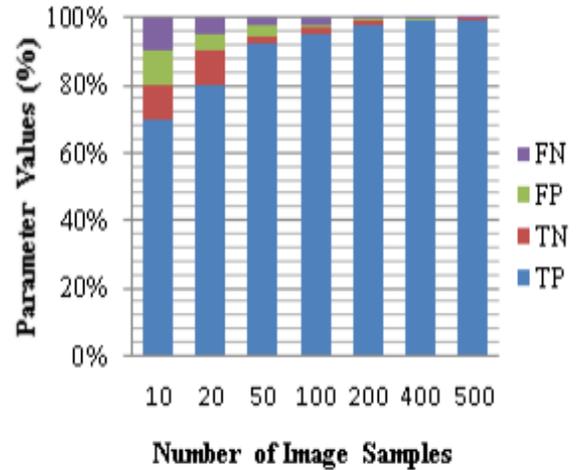


Fig. 4. Confusion Matrix Parameters Expressed in Percentiles.

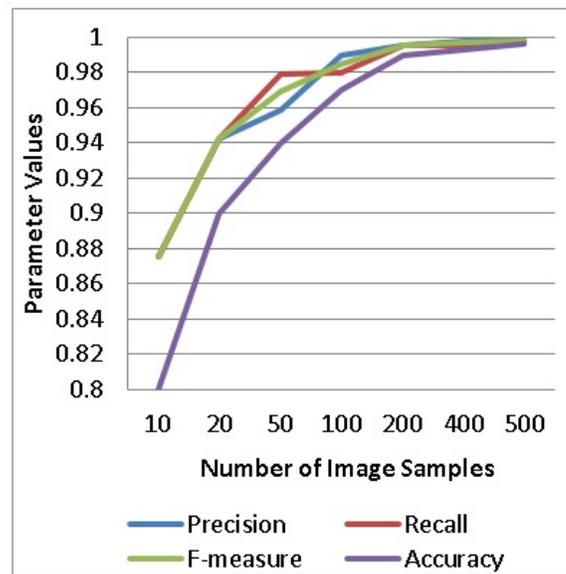


Fig. 5. Parametric Plot of Precision, Recall, Fmeasure and Accuracy.

of sampling and classification in the proposed model over the range of image samples. The plots shows that for a sample of 10 images, the precision is only 0.875. Further, as the sample size is increased to 50, 200 and 500 the precision also increases from 0.95 to 0.995 and 0.998. This trend shows a improvement of 12.3% in precision. Similar trend is observed in case of recall value or the true positive rate. The recall for a sample

TABLE I. IMAGES AT VARIOUS STAGES IN IFPRS AND IFRS.

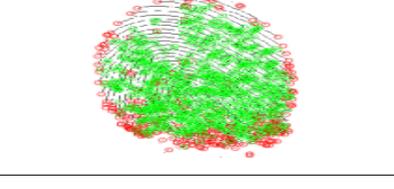
S.No	Stages of Images	IFPRS	IFRS
1.	Original Uploaded Image		
2.	Pre-Processed Image		
3.	ROI Recognition Image		
4.	ROI Enhanced Image		
5.	Optimized Image		

TABLE II. COMPUTED RESULTS.

Number of Image Samples	TP	TN	FP	FN	Precision	Recall	F-measure	Accuracy
10	7	1	1	1	0.875	0.875	0.875	0.800
20	16	2	1	1	0.942	0.942	0.942	0.900
50	46	1	2	1	0.959	0.979	0.969	0.940
100	95	2	1	2	0.990	0.980	0.985	0.970
200	196	2	1	1	0.995	0.995	0.995	0.990
400	396	1	1	2	0.998	0.995	0.997	0.993
500	496	2	1	1	0.998	0.998	0.998	0.996

of 10 images is only 0.875. But as the sample size is increased to 50, 200 and 500 the recall value also increases from 0.979 to 0.995 and 0.998. Hence the system sensitivity increases with increase in the number of input sample images. In case of F-measure, the observed value for 10 images is 0.875. As the number of image samples increases to 50, 200 and 500, this leads to increases the accuracy to 0.969, 0.995 and 0.998. The results show that the system achieved on average precision, recall and f-measure of 99.8% each. Accuracy is an important parameter to predict the correctness of results predicted by the proposed model. The plots show that the initial accuracy of the system is only 0.80 which record a step rise till the sample size is 200 and system attains an accuracy of 0.97. This further

gets accentuated to 99 % for a sample size of 500 images. The performance of the bio-metric fusion system is also evaluated against similar literature cited hybrid approaches. Kumar and Zhang had evaluated the effectiveness of SVM, NN and FFN for feature extraction and classification and conclude SVM to be best approach among others employed in the study [20]. Similar work was also carried on by Kremic and Subasi who employed Random Forest Tree (RFT) with SVM to enhance the performance of their proposed approach [21]. The authors in the current study considered these existing studies for the evaluation of the proposed system in terms of accuracy. Table III and Fig. 6 shows that the recognition accuracy of 89% was achieved by Kumar and Zhang using

SVM classifier [20] and maximum face recognition accuracy of 97.94% was attained when SVM classifier was powered with the employment of RFT by Kremic and Subashi [21]. In comparison to these prediction results, our proposed biometric fusion model demonstrated an average accuracy of 99.6% when a combination of WOA and SVM is used.

TABLE III. ACCURACY EVALUATION WITH EXISTING WORK

Reference Work	Approach used	Accuracy
Proposed Work	WOA + SVM	99.60%
Kumar and Zhang, 2006	SVM	89%
Kremic and Subasi, 2016	RFT + SVM	97.94%

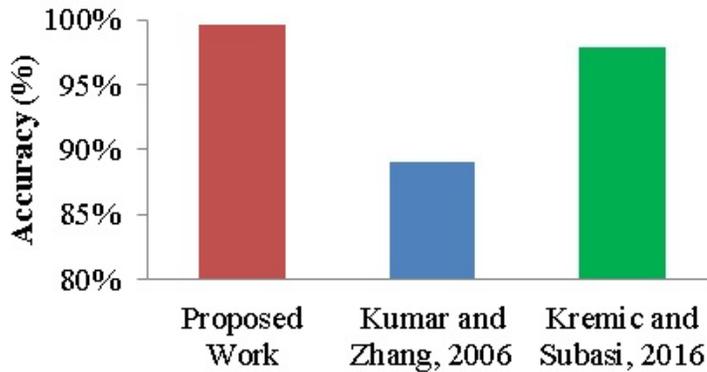


Fig. 6. Accuracy Comparison with Existing Work.

V. CONCLUSION

The authors propose an Improved Bio-metric Fusion System for face and fingerprint recognition in the present work. The system makes use of WOA approach as an optimization technique along with MSER for extracting feature points of the images. Pattern net has been used along with SVM to enhance the accuracy of classification in the proposed fusion system. The resultant recognition system shows an instrumental TP value of 99.2% with minor TN, FP and FN values of 0.4%, 0.2%, and 0.2% respectively. It is also observed that the proposed system demonstrates an average precision, recall and f-measure of 99.8% each with an average recognition accuracy of 99.6%. The overall result achieved an improvement of 12.3% for precision, recall and f-measure and an outstanding enhanced accuracy of 91.6% when a larger data set of images is employed for training the proposed system.

REFERENCES

[1] Dwivedi, R. and Dey, S., 2018. Score-level fusion for cancellable multi-biometric verification. *Pattern Recognition Letters*.

[2] Connor, P. and Ross, A., 2018. Biometric recognition by gait: A survey of modalities and features. *Computer Vision and Image Understanding*, 167, pp.1-27.

[3] Nagar, A., Nandakumar, K. and Jain, A.K., 2011. Multibiometric cryptosystems based on feature-level fusion. *IEEE transactions on information forensics and security*, 7(1), pp.255-268.

[4] Wu, Z., Tian, L., Li, P., Wu, T., Jiang, M. and Wu, C., 2018. Generating stable biometric keys for flexible cloud computing authentication using finger vein. *Information Sciences*, 433, pp.431-447.

[5] Frischholz, R.W. and Dieckmann, U., 2000. BioID: a multimodal biometric identification system. *Computer*, 33(2), pp.64-68.

[6] Nixon, M.S., Guo, B.H., Stevenage, S.V., Jaha, E.S., Almodhahka, N. and Martinho-Corbishley, D., 2017. Towards automated eyewitness descriptions: describing the face, body and clothing for recognition. *Visual Cognition*, 25(4-6), pp.524-538.

[7] Gupta, K., Walia, G. S., & Sharma, K. 2020. Quality based adaptive score fusion approach for multimodal biometric system. *Applied Intelligence*, 50(4), pp.1086-1099.

[8] Aleem, S., Yang, P., Masood, S., Li, P., and Sheng, B. 2020. An accurate multi-modal biometric identification system for person identification via fusion of face and fingerprint. *World Wide Web*, 23(2), pp.1299-1317.

[9] Krish, R. P., Fierrez, J., Ramos, D., Alonso-Fernandez, F., & Bigun, J. 2019. Improving automated latent fingerprint identification using extended minutia types. *Information Fusion*, 50, pp.9-19.

[10] Mehraj, H., & Mir, A. H. 2020. Feature vector extraction and optimization for multimodal biometrics employing face, ear and gait utilizing artificial neural networks. *International Journal of Cloud Computing*, 9(2-3), pp.131-149.

[11] Hussein, I.S., Sahibuddin, S.B., Nordin, M.J. and Sjarif, N.B.A., 2019. Multimodal palmprint technology: A review. *Journal of Theoretical and Applied Information Technology*, 97(11), pp.2882-2896.

[12] Dwivedi, R. and Dey, S., 2019. A novel hybrid score level and decision level fusion scheme for cancellable multi-biometric verification. *Applied Intelligence*, 49(3), pp.1016-1035.

[13] Jain, L.C., Halici, U., Hayashi, I., Lee, S.B. and Tsutsui, S. eds., 1999. *Intelligent biometric techniques in fingerprint and face recognition (Vol. 10)*. CRC press.

[14] Zewail, R., Elsafi, A., Saeb, M. and Hamdy, N., 2004, July. Soft and hard biometrics fusion for improved identity verification. In *The 2004 47th Midwest Symposium on Circuits and Systems*, 2004. MWSCAS'04. (Vol. 1, pp. 1-225). IEEE.

[15] Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S., 2009. *Handbook of fingerprint recognition*. Springer Science & Business Media.

[16] Sing, J.K., Dey, A. and Ghosh, M., 2019. Confidence factor weighted Gaussian function induced parallel fuzzy rank-level fusion for inference and its application to face recognition. *Information Fusion*, 47, pp.60-71.

[17] Saini, M. and Kapoor, A.K., 2016. *Biometrics in Forensic Identification: Applications and Challenges*. *J Forensic Med*, 1(108), p.2.

[18] Wang, N., Gao, X., Tao, D., Yang, H. and Li, X., 2018. Facial feature point detection: A comprehensive survey. *Neuro computing*, 275, pp.50-65.

[19] Natarajan, P., Sikka, A. and Prasad, R., Amazon Technologies Inc, 2016. *Image processing using multiple aspect ratios*. U.S. Patent 9,418,283.

[20] Kumar, A. and Zhang, D., 2006. Personal recognition using hand shape and texture. *IEEE Transactions on image processing*, 15(8), pp.2454-2461.

[21] Kremic, E. and Subasi, A., 2016. Performance of random forest and SVM in face recognition. *Int. Arab J. Inf. Technol.*, 13(2), pp.287-293.