Multimodal Biometrics Recognizer: A Comparisonof Feature Fusion & Matching Score Fusion

Karnati Sathwika[1], Chava Swathika[2], Dr. M. Selvi[3]
[1,2]*Computer Science and Engineering Sathyabama Institute of Science and Technology Chennai, India*
[3]M.E., Ph.D. *Computer Science and Engineering Sathyabama Institute of Science and Technology Chennai, India*

Abstract—**Due to its widespread uses in the surveillance system, human identification is now being given a lot of attention. Unimodal authentication like speech and facial recognition are used in most individual biometric identification. Unimodal biometric systems have drawbacks, especially when dealing with outliers and incorrect data. Because of its many advantages, including increased safety versus traditional unimodal biometric & remarkable identification accuracy, multifunctional authentication technologies are receiving increasing attention from academics. So, this work in the paper creates a biometric recognition method that employs both facial & fingerprints identification. CNN & ORB algorithms are used to create a multibiometric person identification system. The next step is a matched score level synthesis built on the Balanced Tally, which brings together the disparate aspects. If fusion score is higher than that of the threshold t, the validation procedure is fulfilled. The technique is rigorously tested on many datasets from the UCI ML Repository Database, including one real-world dataset using state-of-the-art methods. The suggested methodology shows great promise in the area of facial detection.**

Keywords—: **Biometric, facial, fingerprint, CNN, ORB, identification, unimodal**

I. INTRODUCTION

Biometric systems, which use a person's distinctive physiological or behavioural features to verify their identity, have seen rapid growth in popularity in recent years. Biometric systems have the benefit of being more secure than conventional means of identification like credentials and PINs since they are harder to fabricate or mimic. Multimodal biometrics is the use of more than one biometric feature in a single system to increase security and trustworthiness. The system's overall performance andresilience may be enhanced by merging the data from different senses, such as facial & fingerprint identification. Through this work, we want to create a biometric modalities system that incorporates both facial and fingerprint identification. Scoring fusion methods will be used to mergedata from the two platforms to boost the system's efficacy. The benefits of this strategy include mitigating the limitations of one modality with those of another.

The system's face detection and recognition functionality will be built to be resilient in the face of environmental challenges like shifting illumination and a moving subject's perspective. The fingerprint identification system will bebuilt to be resilient against environmental and user-related conditions that degrade fingerprint images, such as damp or filthy fingertips. In recent years, a new subject of industrial engineering has emerged, and its products are poised to soon command substantial consumer demand. It's been dubbed "biometrics" for short. Pioneers in this field want to build gadgets that can recognise a person by their "biological" traits, such as their voice, movement dynamics, facial features, body features, retinal or iris pattern. Because each individual is uniquely crafted by Mother Nature, no two people will ever be exactly same. Biometric technologies rely on this trait to uniquely identify each individual.

Simply said, a biometric is a set of algorithms that canauthenticate a user's possession of a unique based on physiological trait. In order to create a functional biometric technology, it is necessary to take into account a number of factors. One must first be registered in the system for his biometric template to be recorded. This form is then saved in an encrypted format in a centralised database or on the user's card reader. As soon as it becomes necessary to identify a certain person, the corresponding template is fetched. A biometric system may function as either a verification or identification system, depending on the

requirements of the situation. Recently, biometrics has become more important in the realm of IT security. Rather of relying on a user to remember a passcode or swipe a card,biometric identification systems use an analysis of a person's unique identifying traits to verify their identity automatically.

This project's overarching objective is to develop a biometric identifier that will be used in a variety of settings, such as but not restricted to safety, authentication protocols, & cash activity. The platform's efficacy & dependability will be measured against industry norms and actual information.

II. LITERATURE SURVEY

Farmanabar & Toyagar [6] used a strategy that used several concepts, both functionality and match point total, to demonstrate the reliability of their detection method. Systems based on one's fingerprints or face were employed.In order to pick features, a meandering search technique was utilised to find an appropriate and optimum subset that included palm- print and face retrieved characteristics. By doing so, we can minimise the computational cost of processing features while improving speed. Using the sum rule approach, we successfully merged match scores at many levels. Later, the research's findings were put to the test on a simulated multimedia repository comprised of libraries including both palm prints and facial images from the Ck+ visage and Uniformly distributed random palmprintprojects. With an efficiency of 98.17%, the suggested method significantly exceeded previous materials are available or face multifunction technologies. Whencompared to other cutting-edge techniques, this one holds itsown.

Motameed[7] suggested another identification approach for authentication that uses a combination of a person's ear and palm traits. The technique for feature extraction was focused on particle swarm optimization (PSO). Its two primary characteristics are the usage of Discreet Wavelet & Dct. This program's being the consisted of three stages: (1) picture capture, (2) well before, and (3) image separation and normalisation of the eye but instead thumb. The data also were retrieved, and a fusion of methods was performed. The last stage was making a call using information from the Pa & Ppo classifications. According to the experimental findings, appears that this Wrapper method of feature selection may provide very effective recognition results with a minimal set of characteristics.

For both multilingual and symmetrical systems, Raghavendrah&Dorizi [8] suggested an efficient feature method of selection for biometric identification. So, we utilised AIPSO to choose Based On gabor values for the face and fingerprint paradigms separately, and then to merge these features in a single space using the Log Gabor representation of both modalities. The projection space for the features chosen by KDDA is taken into account in the event of a classification purpose for the two approaches.The experimental findings reveal that AIPSO outperforms other methods such as AdaBoost, SFFS, Conventional PSO, and GA by a factor of 5% & reduces the the system's size by62%.

For the purpose of adaptively guaranteeing the intended performance, Kanhangaad[9] have suggested a promisingsolution to the continuous improvement of biometric authentication. To best integrate the choices made by each unique biometric sensor, the authors suggest a method that uses particle swarm optimization (PSO). To minimise a specified cost function, the suggested method chose a fusionrule and sensor operating points. To achieve the best possible performance for the required degree of security, Kumaar[10] have created a flexible system that combines different biometrics. Multiple biometric modalities, including iris and palmprint scans, facial and vocal recognition, and DNA fingerprinting, have been tried. Contrary to the feature - level technique, the testing findings demonstrated that the suggested score-level strategy achieved pretty steady performance with a lower number of repetitions.

An adaptive multimodal biometric fusion technique based on pretrained and PSO was suggested by LMezai&FHachouff[11]. Score-based fusion is done, with a modified PSO used to determine the most accurate belief functional and its values. The findings provide sufficient impetus for further exploration into the use of optimization methods in the pretrained.

The feature selection approach proposed by Vijaykumar N. and Irfan Ahmed M. [12] is likewise based on PSO. Inaddition to using KNN & Naive Bayes classification techniques, they

also made use of DCT, Psf, Fft, association based image feature engineering, feature merging, Pso optimization feature selection, and Pso optimization functionality extraction. According to the obtained data, the classification rate is increased by 4.3% compared to theDCT-NB and by 1.81% compared to the Gabor-NB whenthe two Naive Bayes methods are fused together. Similarly, compared to DCTKNN and Gabor-KNN, the suggested fusion with KNN significantly increased the rate of recognized by 3.05percent vs 2.42%. Relatively recently, PHSilva[13] offer a profound backpropagation algorithm optimised from either a method based for face recognition, with the goal of attaining remarkable representation for just the iris modality. A periocular image was already available to them, and now they have the iris representation that was offered after some fine-tuning.

They evaluate this method of fusion in terms of features in comparison to the three fundamental laws of matching functions: sum, multi, and min. The eye & periocular area and a real-world setting are both covered in the outcomes. Data from the NICE.II event indicated that pretrained representations for the iris modality were able to attain a new position, with a tendency to result of 1.22 and a Dat dey of 13.56 percent. So when synthesis is performed atthe document level using PSO on the periorbital & pupil modality, they achieved state-of-the-art results, with a tendency to result of 4.45 as well as an EER of 6.55%, respectively.

III. CREATING FINGERPRINT CODE

The fingercode is constructed using the following methods:

a) Background removal in the capturing procedure by meansof pane wise normalisation, Quantization, filters, andsubsampling [3].

b) Pinpointing the centre of the cone using a maximumcavity estimate [4].

c) Tessellating a spherical zone centred on the origin.

d) Adjustment of each sector individually, then applying a spatially distributed banks of Bloch filtering with a generic shape (see (1)) [5].

$$G(x, y; f, \theta) = \exp\left\{\frac{-1}{2}\left[\frac{x'^2}{\delta_x^2} + \frac{y'^2}{\delta_{y'}^2}\right]\right\}\cos(2\pi f x') \quad (1)$$

With $x' = x\sin\theta + y\cos\theta$ and $y' = x\sin\theta - y\cos\theta$.

Where f is the frequency of the sine plane wave along the direction θ from the x-axis, and δ_x and δ_y are the space constants of the Gaussian envelope along X' and Y' axes, respectively.

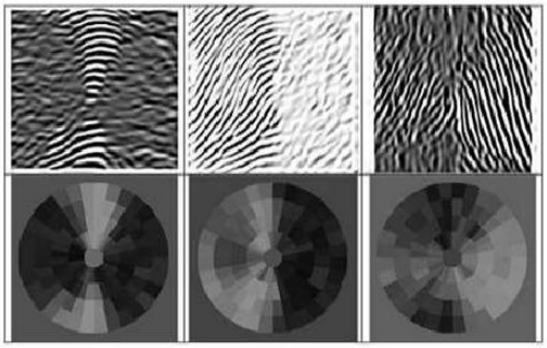

Fig.1. Here we have filtered examples of the photos at 0 degrees, 5 degrees, 22.5 degrees, and 45 degrees, along with the appropriate feature vectors.

IV. FACIAL RECOGNITION

CNN facial detection is a method for finding and recognising faces in still and moving media. CNNs are a form of deep learning algorithm that excel at automatically learning characteristics from the input, making them ideal for image & video analysis. Facial detection using a CNN requires first training the model on a dataset of tagged faces. Following this, the CNN may utilise the taught characteristics to identify faces in fresh media. After a CNN detects a face in a picture, another CNN is used to extractthe face's traits and find a matching face in a dataset.

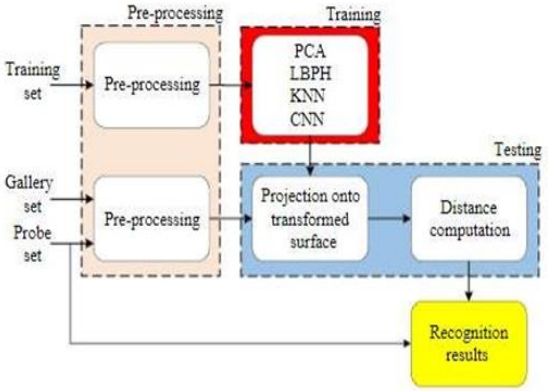

Fig.2. Facial Recognition System

Pre-trained models such as MTCNN, VGG-Face, OpenCV's dl face detector, etc., are readily

accessible. For optimalperformance on a given job or data set, these models may be tweaked. In general, CNNs are very effective methods of face recognition, and have found usage in fields as diverseas security, monitoring, & human contact. Just after exhibit pictures have been preprocessed, the term referring description are calculated by comparing the featurevectors from the portfolio with the subset. When comparing photographs from a gallery to one from a probe, facial recognition programs must account for large differences in lighting. The resemblance between query and benchmark setpictures is computed to provide the term referring definition for the test dataset. Resemblance scores between the probe and gallery photos' reference-based descriptor are used to rate the collection photographs.

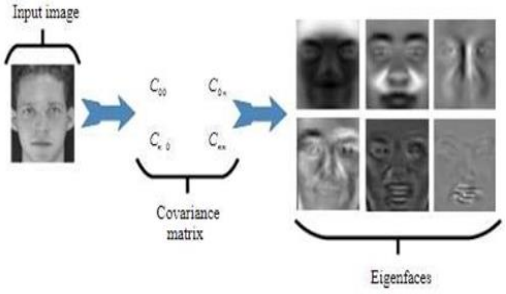

Fig.3. Illustration of the pca algorithm's building blocks

V. BIOMETRIC SYSTEMS WITH MULTIPLE MODALITIES

In order to assess more than one kind of biometric trait,multi - biometric system utilizes data from various sensors. When compared to other methods, it excels at both the identifying and security tasks. As a result of its various benefits, it has found widespread use in a variety of contexts. For instance, the Indian government just mandatedthat all citizens get a "Aadhar card" to serve as a form of identification. Therefore, in this procedure, they collect data on two biometric features, namely a person's irises and fingerprints. We encounter situations like these often during the course of a normal day. Only one enrolment, confirmation, and identity systems have significant drawbacks, as we have shown. The advantages of a multisensory system outweigh these disadvantages. Gains in speed, precision, safety, and sturdiness are among the benefits you'll get. The primary goals of multi-biometric authentication are the reduction of the prevailing exchange rate.Rates of erroneous acceptance, rejection, and nonenrollment are calculated (FTE).

It is considered false approval if an unenrolled user is granted access. Similar, a mistaken reject occurs when a registered user is denied access. In certain cases, the user is unable to join owing to issues such as damage or a lack of required attributes. There are a number of factors that may lead to these occurrences, including noise in the data, intra- class differences, and others. All these rate may be lowered, therefore, by using various techniques in a multimodal fingerprint scanner. Biometric identification may take many different forms, including multi-algorithmic systems that use several methods, multi-instance systems that choose from many individuals with the same features, and tri systems that use multiple sensors. In biometric technology, the merging of many inputs occurs at multiple stages, thus the sheet strategy.

VI.PROPOSED WORK

Algorithms used in our system

A. ORB

We present the Oriented FAST and Rotated BRIEF (ORB) algorithm for use in the feature extraction and matching processes of the multimodal biometric system's face & fingerprints identification subsystems. Combining the FAST corner detector with the BRIEF descriptor creates the ORB algorithm. As its name suggests, FAST (Features from Accelerated Segment Test) is a corner detector that can swiftly and accurately identify corners in an image. In a compact binary form, BRIEF (Binary Robust Independent Elementary Features) is a descriptor that may express the appearance of a corner. The ORB algorithm is a quick and effective feature extraction approach since it combines these two strategies to simultaneously extract corners and their descriptions.

The ORB method also has an orientation component that may be used to flip the identified corners to a more conventional setting. Matching algorithms may benefit from this since features will always be presented in the same orientation, regardless of the viewpoint from which theywere captured. After characteristics have been retrieved, they will be compared using a matching algorithm to determine how similar the face & fingerprint pictures are. Inthis project, we'll apply

a matching method based on Hamming distance, a way to quantify the dissimilarity among 2 input strings. As the ORB method only produces binary characteristics, the Spacing is well suited to evaluate them.

After a similarity score has been determined for both the face & fingerprint modalities, a score level fusion approach will be used to merge the data from the two modalities to boost the system's overall efficiency. The combined totalwill be used to make a final call. The multimodal biometric system's face as well as fingerprint recognition elementswill use the ORB algorithm for extracting features & matching, with features being teamed utilising Hammingdistance and an ultimate decision being made using the fused score acquired via the based method fusion technique.

B. Convultional Neural Network

CNN technique is proposed here to be used as the approachfor classification and feature extraction in the face plusfingerprint recognition sections of the multimodal biometricsystem. A convolutional neural network (CNN) is anexample of a deep learning algorithm with the purpose of doing image processing. It is made up of several layers ofneurones that have been taught to identify certain characteristics in given pictures. The retrieved features fromthe CNN may be utilised for classification and recognition. We'll utilise a convolutional neural network (CNN) modelthat has previously trained on a huge dataset of face photos for the system's facial recognition functionality. A featurevector representing facial features will be extracted from the face picture with the help of a convolutional neural network (CNN) and fed into a classifier. The facial picture will be used to train a classifier that can then determine which person it depicts relying on their feature space. The system's fingerprint identification functionality will be provided by a convolutional neural network (CNN) specifically trained to recognise fingerprints. The convolutional neural network (CNN) will be taught to identify fingerprints by their distinctive minutiae points. The fingerprints will be classified when the CNN has extracted the characteristic points.

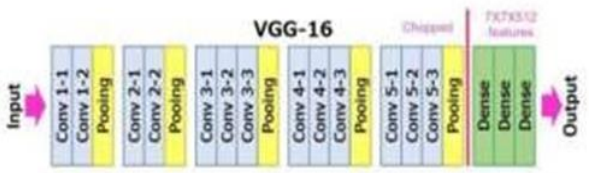

Fig.2. Architecture of VGG

After characteristics have been retrieved, they will be compared using a matching algorithm to determine how similar the face & fingerprint pictures are. Here, we'll utilise the Euclidean distance—a measure of dissimilarity between two feature vectors—as the basis for our matching technique.

After a similarity score has been determined for the face & fingerprint modalities, a match score fusion approach willbe used to merge the data from the two modalities to boost the system's overall performance. The combined total will be used to make a final call. The multimodal biometricsystem's face & biometric fingerprint constituents will use the Classification algorithm as the methods for feature extraction & categorization, functionality will be compared using Distance function, and indeed the final call will be based on the fused marks obtained from the score levelconvolution.

Approaches followed -

In this work, we describe a methodology for comparing two multi - biometric fusion devices that use varying sets of biometric modalities (iris, finger print).

Level 1: Features The complexity of the resulting fusedinput vectors tends to be high, and it may also include superfluous or duplicate data. Both the time it takes to classify data and the amount of space it takes up are inflated when dealing with feature vectors that are too big. Here on out, feature choice is essential for cutting down on processing time and boosting identification precision. Toachieve the best possible integration of features at several levels, we offered two different approaches (PSO). The first plan extracts characteristics from each sensory source independently (iris, palm print). As a further step, we combined the feature maps. Ultimately, the Pdc wasemployed on the combined feature space to narrow down the candidates to the most relevant ones.

However, input vectors normalisation is performed sincethere may be large variances in the length & spread of the fusion extracted

features of matrices. Product normalisation (also known as scope) aims to individually normalise each feature piece to the domain of 0–1 by adjusting the average & variance of the attribute values [24].

$$S_i' = \frac{Si - \mu}{\delta} \quad (1)$$

Where:
S_i' is the normalized matching scores
S_i is the vector to be normalized, and i is the no of classes
μ and δ are the mean and the variance of the fused feature respectively.

System 2 extracts characteristics from biometric techniques such as irises, palms, and knuckles independently. The PSO was then used to choose the best characteristics from each measurement. After that, we normalised and combined the efficient feature sets.

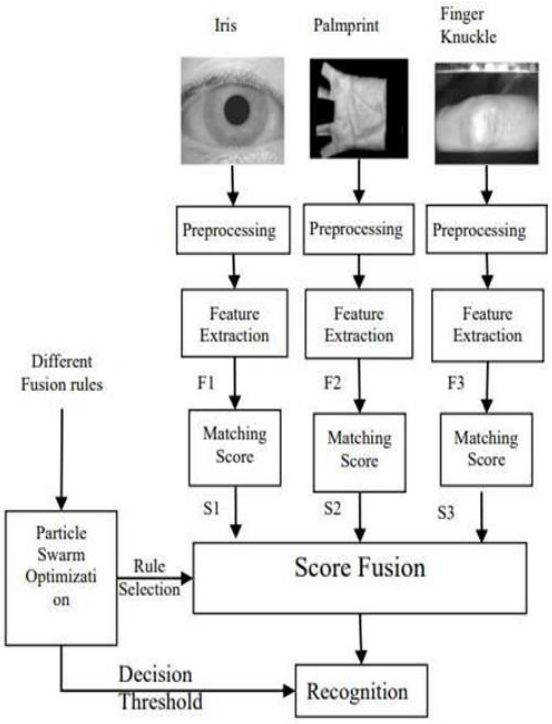

Fig.3. A better fusion of score levels is offered.

Level 2 : The most often used fusion strategy in the academic papers is key - point melting. The suggested approach, uses Pso Algorithm to optimally fuse comparable scores at many levels. Each fingerprint is processed independently to generate its feature maps. Afterwards, a fitting score is determined for each biomechanical specimen using the appropriate standards.

VII.CONCLUSION AND FUTURE WORK

As a result of its accuracy and convenience, biometric systems have found widespread usage in automated human verification and identification. However, there are significant shortcomings in monotonic identification technologies due to serious security threats. Thus, in this lecture, we will explore the topic of modal identification technologies, which take use of a combination of many different biometric identifiers. Score-level fusion is only onekind of fusion that has been considered. Several strategies for fusing scores that have been explored in the book are also described. In this work, we offer a system that uses a cnn classifier to make predictions.

These days, authentication is often performed using some kind of secret code like a PIN or password, which is inherently insecure. One viable option is provided by biometry. By instead or in alternative to using passcode & PIN codes, biometrics should be employed. A user will be validated by his/her biometric features and he/she will be simply acknowledged or rejected. Whether or not his or her biometrics are verified determines whether or not the request is approved. The biometrical key might play some function by substitution or upgrading of standard PIN. Our proposed biometric key might provide even more secure system access than a PIN. Many individuals write there PIN upon certain paper or straight on smart card! You can't just jot down a biometric key or piece of knowledge like a PIN number, and biometrics often have a lot more randomness than PINs do. There are more uses for biometrics besides replacing PINs and passwords. More could be obtained. Because it is so difficult to identify and extract continually the same or virtually its same traits, current biometric authentication isn't suitable for use in encrypted reasons. Features are developing and maturing throughout time. Therefore, it is important to do some coarse found success (granularity change; to prevent the change of position of some characteristic) and subsets calculation (to assure the repetition of some portion of the features).

While there are other level fusion techniques, score level merging stands out for its numerous benefits. In order to improve detection capability, it is recommended to execute fusion at the corresponding score level, since this level of information includes more material and is also more realisticand applicable. Thus, our future endeavours should centreon developing a means of using the score-level fusion classifying approach. The superior performance of the CNN

classifiers justifies its selection.

REFERENCES

[1] A. Ross," An Introduction to Multibiometrics", appeared in proc.of the 15th European Signal Processing Conference (EUSIPCO),September 2007.

[2] A. Ross, and A. K. Jain, "Information Fusion in Biometrics". Pattern Recognition Letters, 2003,

[3] M. Faundez-Zanuy, "Data fusion in biometrics". IEEE Aerospace and Electronic Systems Magazine, vol. 20, pp. 34-38 2005.

[4] J. Kennedy, R. C Eberhart "A discrete binary version of the particle swarm algorithm". In Proceedings of the IEEE International Conference on Computational Cybernetics andSimulation, pp. 4104 – 4108. (1997).

[5] X. Wang, J. Yang, X. Teng, W. Xia and B. Jensen, "Feature selection based on rough sets and particle swarm optimization". Pattern Recognition Letters, vol. 28. pp. 459–471. (2007).

[6] Farmanbar, M., & Toygar, Ö. (2015). Feature selection for the fusion of face and palmprint biometrics. Signal, Image and Video Processing, 1-8.

[7] Motamed, S., Broumandnia, A., & Nourbakhsh, A. (2013). Multimodal Biometric Recognition Using Particle Swarm Optimization-Based Selected Features.

[8] Raghavendra, R., & Dorizzi, B. (2011, November). A novel adaptive inertia particle swarm optimization (AIPSO) algorithm for improving multimodal biometric recognition. In Hand-Based Biometrics (ICHB), 2011 International Conference on (pp. 1-6). IEEE.

[9] V. Kanhangad, A. Kumar, and D. Zhang, "Comments onan adaptive multimodal biometric management algorithm," IEEE Trans. Sys. Man & Cybern., Part-C , vol. 38, no. 5,pp. 438-440, 2008.

[10] A. Kumar, V. Kanhangad and D. Zhang, " A new framework for adaptive multimodal biometrics managemen", IEEE Transactions on Information Forensics and Security, vol. 5, pp. 92-102, Mar. 2010

[11] Mezai, Lamia, and Fella Hachouf. "Adaptive multimodal biometric fusion algorithm using particle swarm optimization and belief functions." 2016 4th International Conference on Biometrics and Forensics (IWBF). IEEE,2016.

[12] Vijaykumar, N., and MS Irfan Ahmed. "Multimodal biometric system using particle swarm based feature selection." 2017 International Conference on Algorithms,Methodology, Models and Applications in Emerging Technologies (ICAMMAET). IEEE, 2017.

[13] Silva, Pedro H., et al. "Multimodal Feature Level Fusion based on Particle Swarm Optimization with Deep Transfer Learning." 2018 IEEE Congress on Evolutionary Computation (CEC). IEEE, 2018.

[14] J. Kennedy and R. Eberhart, "Particle swarm optimization". IEEE Int. Joint Conf. on Neural Networks, Perth, Australia. (1995).

[15] M. Clerc and J. Kennedy, "The Particle Swarmexplosion, stability, and convergence in a multidimensional somplex space," IEEE Trans. Evolutionary Comp., vol. 6, p. 58-73, 2002.

[16] J. Kennedy, R. Eberhart. "A discrete binary version of the particle swarm algorithm". Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, Vol.5, pp. 4104–4108, 1997.

[17] A. Pour, K. Faez, and R. Amirfattahi "Multimodalbiometric system using face, ear and gait biometrics", 10th International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010).

[18] T. Sabareeswari and S. Stuwart," Identification of a person using multimodal biometric system", International Journal of Computer Applications vol. 3, no.9, 2010.

[19] Chinese Academy of Science Institute of Automation, Database of the Eye Grayscale Images. http://www.sinobiometrics.com

[20] PolyU Palmprint Database, http://www.comp.polyu.edu.hk/~biometrics/

[21] L. Zhang, "Finger-Knuckle-Print: A new Biometric Identifier", ICIP, Cairo, Egypt, 2009.

[22] Madane, M., & Thepade, S. (2016). Score Level Fusion Based Bimodal Biometric Identification Using Thepade'sSorted n-ary Block Truncation Coding with Variod Proportions of Iris and Palmprint Traits. Procedia Computer Science, 79, 466-473.

[23] Singh, V., Kant, C., & tech Scholar, M. An Efficient Multi-Modal Biometric Authentication System Using Face, Iris and Finger Knuckle Print.(2015)

[24] Meraoumia, A., Chitroub, S., & Bouridane, A. (2011, June). Fusion of finger-knuckle-print and palmprint for an efficient multi-biometric

system of person recognition. In 2011 IEEE International Conference on Communications (ICC) (pp. 1-5). IEEE.
[25] Mayya, A., & Saii, M. Iris and Palmprint Decision Fusion to Enhance Human Recognition. International Journal of Computer Science Trends and Technology (IJCST), 5, 42-46. (2017)