ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

Biometric Methods of Face Recognition: A Mirror Review

Gursharan Singh
Department of Computer Science
Lovely Professional University
Phagwara, India
gursharan.16967@lpu.co.in

Vishal
Computer Science and Engg.
Lovely Professional University
Phagwara, India
vishal.11615139@lpu.in

Simarjit Singh Malhi
Department of Computer Science
Lovely Professional University
Phagwara, India
simarjit.15976@lpu.co.in

Salil Batra
Department of Computer Science
Lovely Professional University
Phagwara, India
salil.16836@lpu.co.in

Gagandeep Singh
Department of Computer Science
Lovely Professional University
Phagwara, India
gagandeep.17672@lpu.co.in

Makul Mahajan
Department of Computer Science
Lovely Professional University
Phagwara, India
makul.14575@lpu.co.in

***Abstract*-- Biometric recognition refers to an electronically controlled authentication of an individuals based on a characteristic extracted by vector from their physiology and action character traits. Biometric identification systems should provide a reliable personal recognition system for either confirming or deciding an individual's identity. Such a system's applications include security of computer systems, secure online banking, credit cards, smart phones, secure building access, social services and health. By using biometrics, a person could be detected based on "who they are" instead of using "what they have" (card, token, key) or "what they know" (password, PIN).With the world pacing towards the digital era, security becomes a key feature, authentication being a major concern. Biometric techniques like face recognition are increasingly advancing. This paper presents a comparison and analysis is done on two face recognition techniques are OpenCV, SVM, Gabor features, OpenCV and Machine Learning.**

Keywords— Biometrics, Face Recognition, Machine Learning, OpenCV, SVM, Gabor features

1. INTRODUCTION

Today's era is the digital era, with almost all the tasks being performed via computers. With the world pacing towards technology, computers have become the primary accessory in business and corporations [1]. With e-commerce at its peak, companies like amazon, flipkart would not function without computer networks. Computer Networks helps stay connected and communicate across the globe. Without computer networks or the intricately formed web of networks, the internet the virtual companies will cease to exist. Thus, there is a pressing need to provide network security, authentication systems in systems.

Hence, a major point to think about is - how to secure a computer network system. Confidentiality, Integrity and Availability renowned as the CIA triad are the three pillars of Information Security. Therefore, Security must be enforced keeping these features in mind. Confidentiality refers to the feature which ensures data can be accessed only by authorized personnel. Integrity is the feature that assures that data transmitted by a sender has been received without any alterations. Availability ensures that resources are accessible to authorized user at any point of time. If an adversary floods a network with malicious requests, a system must be able to cop-up with rather than resulting in a denial of service to legitimate users. Several security features must be considered while securing a network, one of them being biometrics authentication. Biometrics is derived from the two Latin words, 'Bios' meaning human and 'metrikos' meaning measure. Thus, biometrics is the technique of measuring an individual's physiological as well as behavioral features in order to correctly identify them, thus acting as an authorization system [1].

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

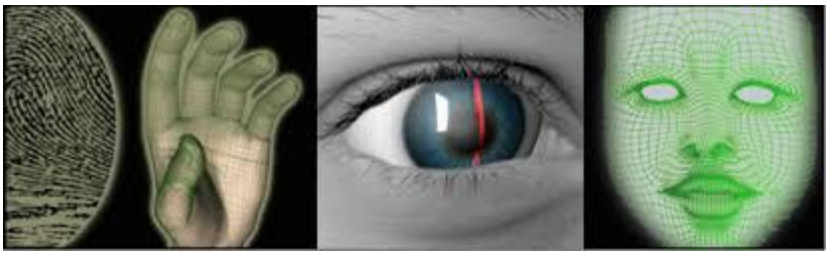

Figure 1 Biometric Recognition System

Firstly, the individual's sample is collected, followed by feature extraction to create a template which is stored in the system database and matched against, every time a person attempts to access the system. Biometrics deals with something you are, a part of your identity which is used for authentication and cannot be stolen, altered or duplicated.

II. LITERATURE REVIEW

Boatwright et. al. performed a survey on biometrics and explore about biometrics [1]. Author explained about the importance and working of biometrics in securing computer networks. Authors have explained about various biometric techniques in brief. Future of Biometrics is vast and bright. Future of Biometrics depends upon user acceptancy.

Adrian Rhesa Septian Siswanto et. al. proposed the implementation of face recognition system using open-cv [2]. Open-cv is image processing library use to process and capture images from live camera, photo or videos. To recognize a face some features of face like width of mouth and eye are extracted from images in training process and tested against same person's other images.

Marian Stewart Bartlett et. al. suggested a new way to implement facial recognition using Machine learning [3]. Author used Facial Action Coding System (FCAS) to recognize facial actions and facial expressions. Person's mood can also be recognized i.e. if person is sad then algorithm can predict that person is sad after recognition of face.

Liping Yuan et. al. Proposed another approach of implementing facial recognition using neural networks based on TensorFlow [9]. TensorFlow is a framework for deep learning and it is open source. This way is more accurate than other methods proposed and proved by many researchers. CNN (Convolutional Neural Network) was used to find and verify the displacement, scaling and other features.

Sun et. al. Presented a new scheme to face detection using deep learning [8]. Author achieved faster recognition using faster framework RCNN. Number of strategies are applied some of them are hard negative mining, feature concatenation, training of multi scale model , pre-raining model and achieved state-of-the-art results.

Jun Qin et. al. Described a novel approach for face detection which is based on Gabor Featured Key point [4] and SVM "Support Vector Machine". A human face was represented in computable dimensional space using the Gabor features for key points. Result shows better performance received from Experiments on AT&T databases and FERET with SVM method.

Kruti Goyal et. al. Used open computer vision in face detection and face tracking. It is an application of face recognition system [7]. To understand the algorithm easily author performed a tabular comparison. Algorithms were compared in terms of space paradigm and time paradigm.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

Erno Makien et. al. Presented a way to classify the gender of an individual by using face recognition method [6]. SVM helped in achieving better classification rate. Classification rate depends upon automatic and manual alignment methods. Neural network and Adaboost also predicted good classification rate almost same.

Unsang Park et. al. Explained one of the applications of face recognition: Age Invariant [5]. If a person uses face recognition as biometrics security of its system, then with age face of person changes and create False Rejection error. So, the main challenge is to make a system which cannot be affected by facial aging and predicts the correct result. Authors proposed 3D aging modeling technique.

Abhijit Punnappurath et. al. Found a drawback of existing systems that they cannot capture non uniform image clearly and recognize the face [10]. So, author proposed a new approach so that image can be captured and recognized clearly in non-uniform blurring situations. Authors converted the blurred face to convex combinations of focused face and then performed the analysis.

III. BIOMETRIC TECHNIQUES

Biometric techniques are methodologies using which authentication can be performed, Biometric Techniques can be broadly categorized in two classes-Physiological Biometrics as well as behavioral biometrics [1].

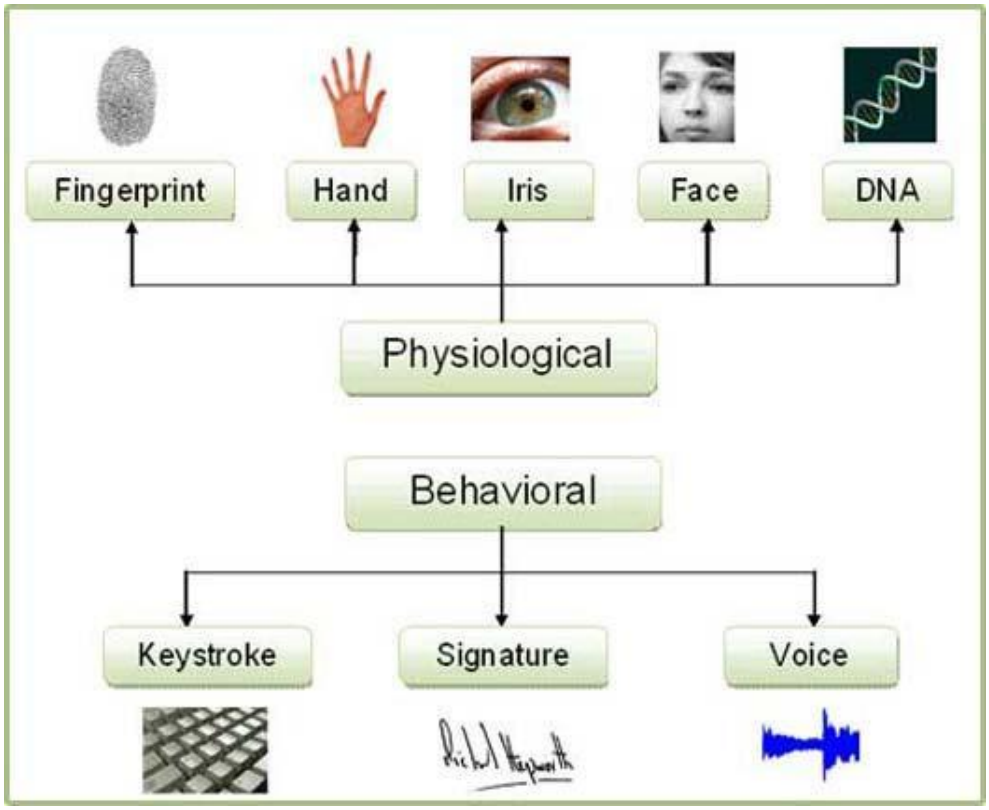

Figure 2 Biometric Techniques

A. Iris Biometrics

Iris is a circular portion of the eye which controls the size of pupil [1]. The imaging of an iris is easy and it is well protected from environmental adversities thus making it a feasible biometric technique. Spoofing of the iris is very difficult making this technique an efficient as well as fast biometric technique. It is used in the banking sector in order to manage access to highly critical areas. Replicating the features of iris is difficult.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

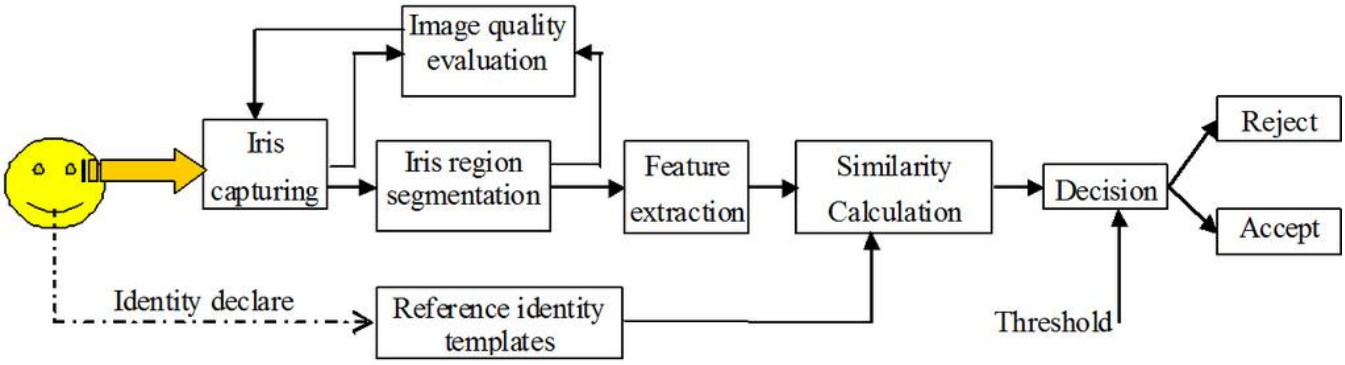

Figure 3 Iris Biometrics Method

However, a German company C'T attempted to do so, involving the replica of an iris. The attempt was successful and the impersonator gained access to the system.

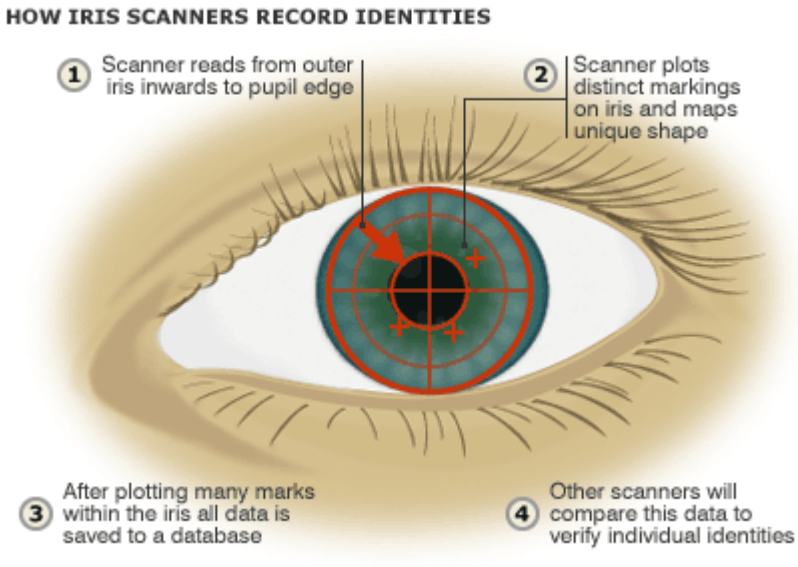

Figure 4 Iris Identification

B. Palm Vein and hand Vein Biometrics

Hand vein and palm vein biometric technique involves capturing the vein patterns over the hand as well as palm using infrared imaging and creating a template, which access as a novel feature in authenticating an individual [1]. No two individual possess the same vein pattern hence it is a reliable biometric technique. The size of arm or hand may change with age but the vein pattern remains unchanged. Experiments involving the collection of data from different parts of the hand, including back side of hand, back side of palm and wrist back side. Nevertheless, capturing wide veins in the back of the hand is more fitting, it is vulnerable to environmental factors and the condition of the nervous system and does not provide a clear picture quality [16].

On the other hand, when detecting vein patterns on the back side of hand, palm and wrist, near-infrared imaging produces images of good quality. The biometric element considered here is the palm vein. The apps include points of bifurcation and starting points. Because other cryptographic keys are prone to theft or guess, keys created from the biometric entity are preferable as they are attached to the consumer. The Finger vein authentication system used in this work is based on the Max Curvature Points (MCP)

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

[14] as a system of extraction of features and as a comparator comparison. This choice is made by taking into account the high efficiency and few processing features of the MCP system [15].

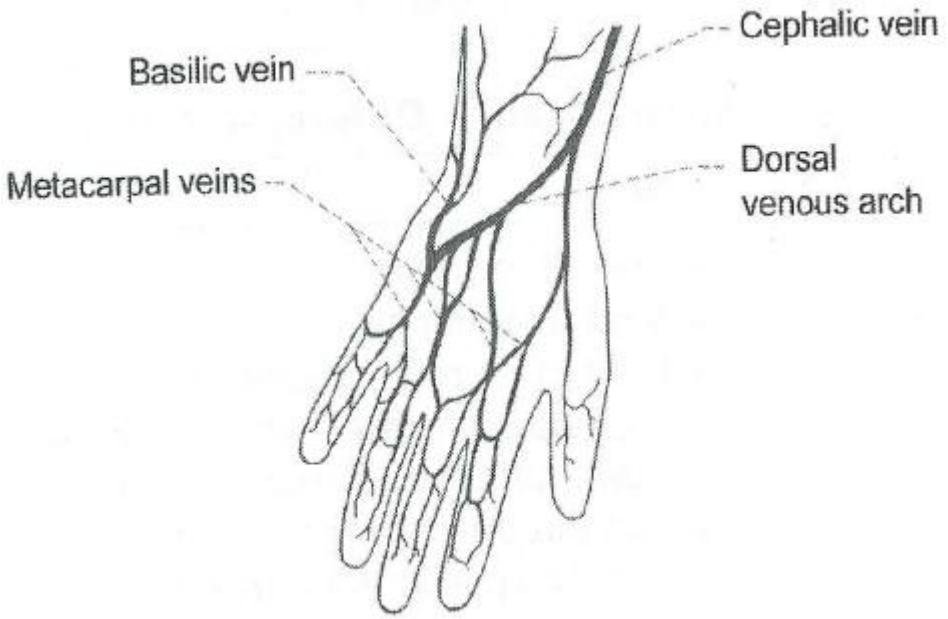

Figure 5 Vein Biometrics

C. **Voice Biometrics**

Voice biometrics involves extraction of three traits called phonemes i.e. intonation, pronunciation and pitch of human voice [1]. The three of them together distinguish one individual from another. The voice biometric can be categorized as both, physiological as well as behavioral. However, it is not an efficient biometric technique since the voice acoustics can vary depending on the environment, age as well as health of the person. The voice can also be mimicked by an imposter to gain unauthorized access.

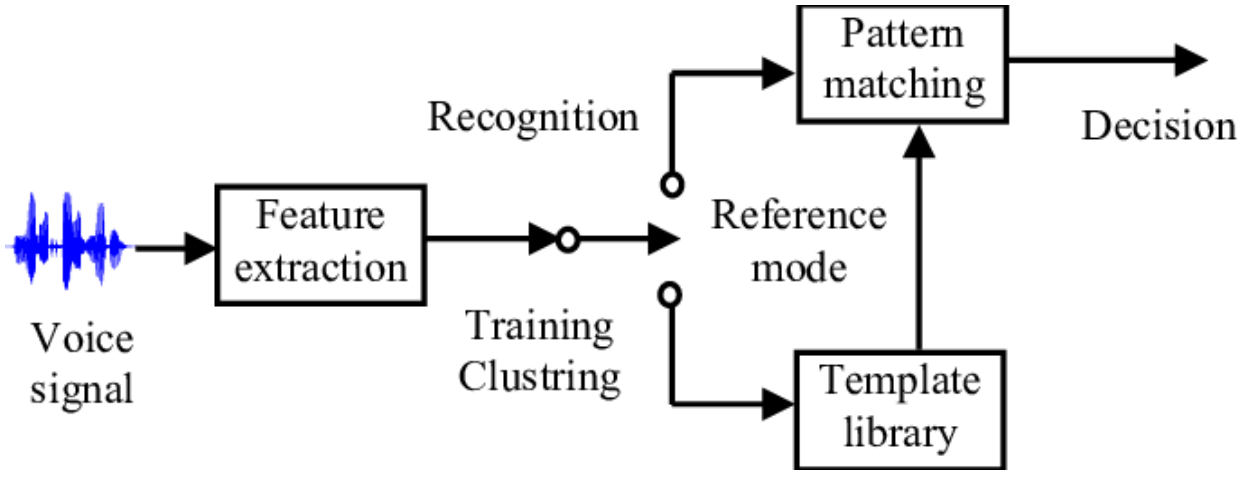

Figure 6 Voice Recognition Method

User verification voice biometrics is a task in which the goal is to operate speaker verification easily, robustly and safely. Examining the use of state-of - the-art text-independent and text-dependent speaker verification technologies for user authentication [17].

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

D. Retina Biometrics

Retina is the portion of the eye where image is formed and located at the posterior part of eye. Retina is composed of thin issues of neural cells [1]. Is also known as ocular based techniques. The retinal scan involves casting a beam of infrared light into the human eye. This beam traces a path over the retina. The blood vessels over the retina absorb light with varying amount of reflection. Thus, variations are captured ad stored in digitalize form in the system database. *E*.

E. Face Recognition

Face recognition is commonly used biometric technique which captures facial images and extracts certain features based on the images to uniquely identify a person [1]. It is commonly used in several gadgets and gizmos like smartphones, laptop and many more. It involves extraction of facial coordinates, dimensions of eyes, mouth, pupil, and creating a template which is further used to match against every time user demands system access [2].

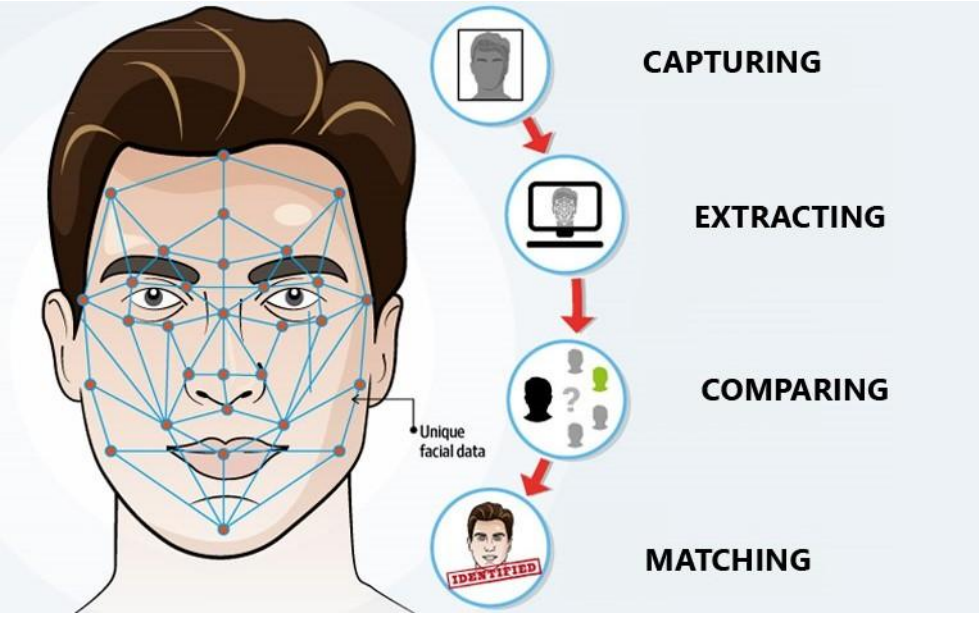

Figure 7 Face Recognition

The various phases involved in face recognition are as follows:
Phase 1: Face detection
In the image that is captured, a face needs to be detected, irrespective of the dimension or place. A high-end filtering strategy is used for face detection and filtering faces is performed using classifiers.

Phase 2: Face normalization and Feature Extraction
The anthropometric system finds approximate location facial features such as nose, eyes and mouth. The entire process is performed again to predict such features and are matched against collocation statistic to discard wrongly located features.

Phase 3: Facial Recognition

Anchor points are generated by applying geometric features in the facial image. After that, the face recognition process is begun. It is done by finding local facial appearance representation at each of

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

the anchor points. Preparation of the set. Each subject will be sitting behind them in a seat with a dark foundation to limit the impression of light. The collaboration of all subjects means that they use the equivalent present during the procedure to obtain a decent set of preparations. Be that as it may, during the process, there is no photometer used. The main problem during the process of securing the preparation set is the light that comes from a window in the room. In order to limit the lighting impact from that window, we tried to take all the preparation set straight in a similar time with the expectation that during the process the light force from the window would not change.
Prepared face recognition calculations inside OpenCV are allowed to operate directly against the c amera. It is necessary to download the latest version of OpenCV.

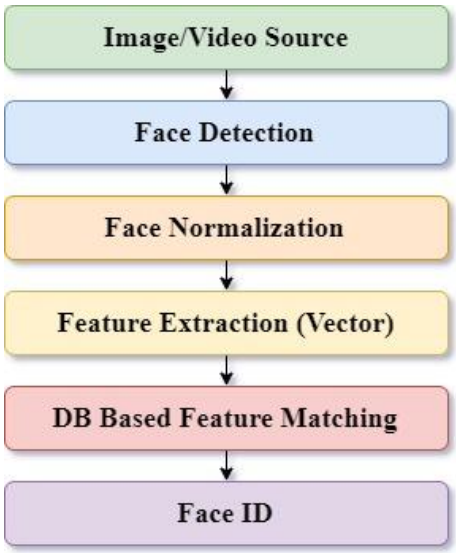

Figure 8 Steps in Facial Recognition Method

There are many techniques to implement face recognition.
Some of them are discussed here.

1. Face Recognition using Open CV
2. Face Recognition using Machine Learning

1. Face Recognition using Open-CV

Open-CV stands for Open Computer Vision. This can be implemented in any programming language like C++ or Python. Both programming Languages have pre-installed libraries in System [2].

Authors found False Match Rate (FMR), False Non-Match Rate (FNMR), Receiver Operating Characteristics (ROC) as performance metrics for the biometrics system for face recognition. Equal value between acceptance and rejection error is Equal Error Rate (EER). Author compared the performance on these parameters.

Open-CV uses Haar Cascades to recognize the faces. There are many Haar Cascades are available in library for different purposes. Frontal face Haar Cascades is used to recognize the front of the face only. If one wants to recognize the whole face, then default profile Haar Cascades will be used.

Two highlights will be made for the case study of the Attendance System; "Gather Face Information" and "Recognition of attendance." Gather Face Data is working to collect face pictures from a few understudies that will use this application in a continuous condition and prepare all the face pictures in order to produce a superior result of closeness. To turn on the

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

built-in webcam, customers (understudies) are required to provide their legitimate understudy ID.

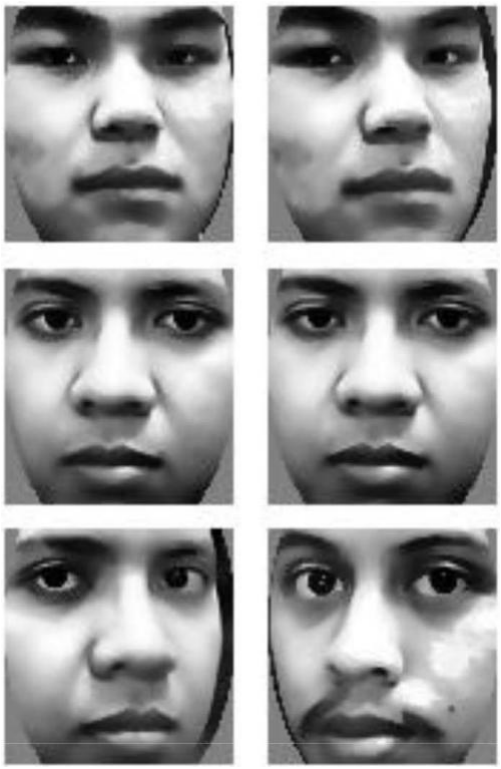

Figure 9 Sample Preparing Set

In spite of face acknowledgment low exactness contrast with other advance biometrics, for example, iris and unique finger impression. Face recognition can be an assistive framework planning to assist in the application of multi-modular biometrics as one of the most characteristic biometrics, "simple to collect." Eigenface is the calculation of [mal face acknowledgment to be updated in the application of Attendance System. ROC bends of Eigenface calculation's presentation dominated the Fisher face calculation's presentation utilizing the current preparing set.

2. Face Recognition using Machine Learning

Machine Learning is a growing technology. Machine Learning can be used to face recognition. Authors directed observational examinations of AI techniques applied to this issue, including examination of acknowledgment motors and highlight choice strategies [3]. Best outcomes were gotten by choosing a subset of Gabor channels utilizing AdaBoost and after that preparation Bolster Vector Machines on the yields of the channels chose by AdaBoost. The mix of AdaBoost and SVMs upgraded both speed and precision of the framework. The framework introduced here is completely programmed and works continuously.

SVM was used to detect and predict facial expressions [4]. SVM is the only algorithm that was well suited for this task. Adaboost was used to detect and predict emotion classification. Adaboost and SVM both were compared in this technique.

The highlights utilized for the Adaboost feeling classifier were the individual Gabor channels. This gave 9xXx48x48= 165,888 potential highlights.

Adaboost isn't just a quick classifier, it is additionally an element choice method. A preferred position of highlight choice by Adaboost is that highlights are chosen dependent upon the highlights that have as of now been chosen. In highlight choice by Adaboost, each Gabor channel

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

is a treated as a wJeak classifier. Adaboost picks the best of those classifiers, and after that lifts the loads on the guides to weight the mistakes more. The following channel is chosen as the one that gives the best execution on the mistakes of the past channel. At each progression, the picked channel can be appeared to be uncorrelated with the yield of the past channels.

IV. CONCLUSION

After analyzing and reading and a lot of research it can be concluded that Machine Learning approach is faster than using OpenCV and provide more accurate result on same preparing dataset. Machine Learning approach gave 93.3% accuracy.

V. FUTURE SCOPE

Biometric authentication will be necessity in coming years. It might be of great importance in an authenticated use of government agencies. The use of biometrics will only grow in the future as the technology and criminals continue to improvise. This multimodal system can be used efficiently by improving technology and increasing hardware costs. A deep analysis can be done by considering other techniques also like Deep Learning, Neural Networks based on TensorFlow etc.

VI. REFERENCES

[1] Boatwright, M., & Luo, X. (2007). What do we know about biometrics authentication? *InfoSecCD'07: Proceedings of the 4th Annual Conference on Information Security Curriculum Development*, 205– 209. https://doi.org/10.1145/1409908.1409942

[2] Siswanto, A. R. S., Nugroho, A. S., & Galinium, M. (2014). Implementation of face recognition algorithm for biometrics-based time attendance system. *Proceedings - 2014 International Conference on ICT for Smart Society: "Smart System Platform Development for City and Society, GoeSmart 2014", ICISS 2014*, 149–154. https://doi.org/10.1109/ICTSS.2014.7013165

[3] Bartlett, M. S., Littlewort, G., Lainscsek, C., Fasel, I., & Movellan, J. (2004). Machine learning methods for fully automatic recognition of facial expressions and facial actions. *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, *1*, 592–597.

[4] Qin, J., & He, Z. S. (2005). An SVM face recognition method based on Gabor-featured key points. *2005 International Conference on Machine Learning and Cybernetics, ICMLC 2005*, (August), 5144–5149.

[5] Park, U., Tong, Y., & Jain, A. K. (2010). Age-Invariant Face Recognition, *32*(5), 947–954.

[6] Makinen, E., & Raisamo, R. (2008). Evaluation of gender classification methods with automatically detected and aligned faces. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *30*(3), 541–547. https://doi.org/10.1109/TPAMI.2007.70800

[7] Detection, F. (2017). Face Detection and Tracking Using OpenCV, 1–4.

[8] Sun, X., Wu, P., & Hoi, S. C. H. (2018). Face detection using deep learning: An improved faster RCNN approach. *Neurocomputing*, *299*, 42–50. https://doi.org/10.1016/j.neucom.2018.03.030

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

[9] Yuan, L., Qu, Z., Zhao, Y., Zhang, H., & Nian, Q. (2017). A convolutional neural network based on TensorFlow for face recognition. *Proceedings of 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference, IAEAC 2017*, 525–529. https://doi.org/10.1109/IAEAC.2017.8054070

[10] Punnappurath, A., Rajagopalan, A. N., Taheri, S., Chellappa, R., & Seetharaman, G. (2015). Face Recognition Across Non-Uniform Motion Blur, Illumination, and Pose. *IEEE Transactions on Image Processing*, *24*(7), 2067–2082. https://doi.org/10.1109/TIP.2015.2412379

[11] Lu, J., Liong, V. E., Zhou, X., & Zhou, J. (2015). Learning Compact Binary Face Descriptor for Face Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *37*(10), 2041–2056.

[12] Fan, H., Cao, Z., Jiang, Y., Yin, Q., & Doudou, C. (2014). Learning Deep Face Representation, 1–10. Retrieved from http://arxiv.org/abs/1403.2802

[13] K. Delac ; M. Grgic (2014). A survey of biometric recognition methods, International Symposium on Electronics in Marine, 953-7044-02-5

[14] N. Miura, A. Nagasaka, T. Miyatake, "Extraction of finger-vein patterns using maximum curvature points in image profiles", *IEICE Transactions on Information and Systems*, vol. 90, no. 8, pp. 1185-1194, 2007.

[15] R. Raghavendra, K. Raja, J. Surbiryala, C. Busch, "Finger vascular pattern imaging; a comprehensive evaluation", *Asia-Pacific Signal and Information Processing Association 2014 Annual Summit and Conference (APSIPA)*, pp. 1-5, Dec 2014.

[16] L. Wang and G. Leedham, "Near- and Far- Infrared Imaging for Vein Pattern Biometrics," *2006 IEEE International Conference on Video and Signal Based Surveillance*, Sydney, Australia, 2006, pp. 52-52.
doi: 10.1109/AVSS.2006.80

[17] Aronowitz, Hagai / Hoory, Ron / Pelecanos, Jason / Nahamoo, David (2011): "New developments in voice biometrics for user authentication", In *INTERSPEECH-2011*, 17-20.

Copyright © 2019Authors