Intelligence Security Check System Using Face Recognition Algorithm: A Review

[1]Lateefah Abdul-azeez, [2]Abiodun Musa Aibinu, [3]Sodiq Olanrewaju Akanmu, [4]Momoh-Jimoh E. Salami, [5]Taliha Abiodun Folorunso

***Abstract*— One of the famous biometric in use is facial recognition, which uses the statistical measurement of an individual face features to discover or determine his/her identity. Humans are prone to errors or mistakes, therefore, using only security personnel cannot give us a perfect security mechanism. This paper explains the importance of biometric and also present various methods in which biometric applications can be applied in solving various problems. It focuses on face recognition and face detection techniques which include Principle Components Analysis Hidden Markov Model (HMM) (PCA), Principal Component Analysis (PCA) and the Discrete Wavelet Transform (DWT). It briefly explains how the use of the symmetry of the face can be used for recognition, the combination of audio and video in face recognition and also show that a face can be detected in a video. It also shows the various strengths and weaknesses of each method used.**

Keywords—— biometric, face recognition, security, identification, verification

INTRODUCTION

Biometric which combines two Greek words which are "bio" which means life and "metrics" which stands for measurement. It involves two distinctive modes which identification are (answers the question "who you are") and verification (answers the question "are you really who you claim to be"). Biometric is an automatic recognition of an individual which is based on their biological e.g. DNA, fingerprint, vein, face etc. or behavioral features e.g. keystroke, face, DNA, fingerprint, vein etc. [1,2,3]

The most popular biometric trait employed by human for personal recognition today is the face, it uses the physical unique facial feature for recognition either from an image or video [1]. It is suitable for public spaces and uses. Face recognition is gradually becoming a common biometric (life measurement) traits used for identification and verification.

some of the uniqueness of biometric traits are, it cannot be shared to others, it is impossible to steal, it is specially attached to the owner and it is difficult to alter or compromise. This gives it an edge and makes it the best technique for authentication, authorization, identification and verification compared to other techniques such as password, PIN, pattern etc.

In 1960s the development of semi-automated systems emerged in respect to face recognition technology started in which the administration needs to locate the feature points such as the eyes, mouth, nose etc., in [3].

The most common approaches that provides solutions to face recognition are based on either: 1) the place or point and shape of facial features, example are the spatial eyes, eyebrows, mouth, nose, and chin and their relationships or 2) the entire(global) analysis of the face image that represents a face that carried the combination of a number of canonical faces, in [1]. It uses the physical unique facial feature for recognition either from an image or video.

Several problems occur in real time recognition. Moreover, time is also a serious agent in this regard. Time is directly proportional to the size (scope) of the data (images), humans face also has identical features such as the eyes, nose, lips, eyebrow etc. in [3]

In the process of using face detection algorithm, several images of the individual have to be captured in several angles with a distinct expression of the face, in [7]. Face detection algorithm using MATLAB programming language. The person faces the camera for few seconds for face capture, it captures the facial features of the face, put it inside a frame and give it a caption which can be the full name of the person. A database will be developed containing different images and their information. The captured image will be compared with what is stored in the database as the system runs a quick search on the database for available information on it. This information can be the name, tribe, nationality, school, place of work etc. of the image.

Face recognition is a technique that is passively used without the involvement or consent of the person compared to other biometric traits such as fingerprint, which involves active participation of the person in question. Such techniques are needed especially in security agencies, such as the military, or financial institutions like banks etc.

Face recognition are excellent technique for the purpose of surveillance. It can be used to search for criminal or wanted faces, missing persons and so on. In fighting terrorism, face recognition technology has played a vital role in contributing positively to providing solutions to the problem. It helps to easily and automatically identify the culprit.

Using other identification process such as password, fingerprint, iris etc. face recognition provides better security especially in authentication.

LITERATURE REVIEW

In [1], protection of information element using behavioral traits was introduced. This paper discussed, a multi-biometric machine which performs in exceptional modes: serial modes, parallel mode, or hierarchical mode turned into used. The output of one biometric trait in the operation of serial mode was commonly used to slim down the wide variety of feasible identities earlier than the nest trial. In the operation of parallel mode, statistics from multiple tendencies changed into used simultaneously to carry out recognition. In the hierarchical structure likewise, character categorizers were blended in a shape similar to a tree. This proposed machine used the empirical performance

dimension which assessment performed an essential role in knowing if the existing biometric machine was suited or not, or if it required additional improvement. Even though, it has issue in recognizing facial pictures taken from two extensively specific point and beneath one-of-a-kind illumination conditions (that is, varying temporal contexts). More so, same twins couldn't be reliably outstanding using the face facts alone. And there was greater trouble in acting an aggregate at the traits level which is at a result of the connection among characteristic spaces of various biometric designs won't be regarded as a result of this, the traits representations won't be well matched. Significant result achieved turned into that it reduced the overall recognition time. It additionally ensured information safety due to the inherent capability for efficaciously linking people to records and the performances determined in numerous test situations recommended that biometric authentication has extensive scope for development.

Efficient facial recognition system based totally on Hidden Markov Model (HMM) along with the handiest type "Haar" of the Discrete Wavelet Transform (DWT) was developed in [2]. A novel technique became added for selecting the training snap shots implemented with the aid of selecting the photos which have the odd identifying numbers from the database the usage of the DWT and HMM model. The recognition rating become accomplished with the usage of Hidden Markov Models to layout a facial detection and recognition machine. For face detection, a fixed snap shot was used inside the training of 1 HMM, while face recognition, every person inside the database was represented by means of an HMM version of the face. The proposed technique that was used is an effective group of record vectors which is based at the sunder out of the KLT coefficients.

The use of vertical symmetry of human face for half of way face recognition was introduced in [3]. This system used the mathematical model for locating the symmetry. The method hired in this goes as follows: detection of the front view of the face in photograph using Haar Cascade Classifier; cropping and saving the facial area from the picture; scaling the faces to cause them into the same in size; conversion of the picture from RBG into the grey scale and subsequently equalizing the face with the help of filter. For verifying the performance of the method, the application of Principle Component Analysis (PCA) on each of the whole face and segment of face was employed. The result indicated that segment of the faces has been enough for the recognition of an individual. Recognition was accomplished via taking the measurement of the euclidean space covered among the gallery photograph and the probe photo. Faces verification using the PCA, the experimental outcomes were very much promising because it minimizes the time spent and assets which include memory consumption and computation.

[4] used a process for getting bits from face photographs in such a way that every snap shot that look alike will manufacture an almost identical sequence of bit. The methodology worried the stairs for normalizing a face picture, after which from the normalize image of the face a bit string was built. The resulting bit string was used to reconstruct the deduced cryptographic key. The strength of this work lies in evaluating the biometric hashing for 5 famous face detection methods inclusive of PCA, FLD, WT, WT-FMT, and WT-PCA. The saved errors-correcting parameters, if taken, could be composed for the user's or client's biometric, this makes it less secure. Nevertheless, this method become not effortlessly practical to creating cryptographic keys originating from the surfaces of 2-D. The method has produced efficient and accurate outcomes for facial recognition and detection system. In respect of variations accuracy in lightening situations and complicacy performance turned into average. It also allowed fast implementation because the face template is broken into quick observable vectors.

In [5], a proposed client-server model and to compare it with the current client -server models for facial recognition was discussed. This system involves of 2 major aspects: the cellphone side (client aspect) as well as the Matlab aspect (server aspect). The connector among these two seemed as the Tomcat Server. On the Cellular Phone aspect was Java Application. The server aspect alternatively was Matlab together with: consumer database, authentication engine, biometric profile and authentication management. Authentication manager had general control of the authentication device, deterring both whilst authentication ought to take place and the present-day state of security. Authentication machine authenticates users, and a biometric profile generates and train the applicable biometric template. Database carries records or information about customers/users, compatibility, information about which mobile devices are configured to work with the structure, in conjunction with a listing of supported biometric system, in this example the PCA is more suitable. Mobile telephone was connected in wireless with a server side and it communicated to standard wireless protocols 802.11 (CSMA/CA). This paper presented development in client-server implementation for cell face recognition made through adding the privet key to have stable and safe network model when transmitting the biometric information over the network. In conjunction to that, an improved processing energy storage ability of cellular cellphone gadgets in real‐time face recognition for cell phones had been now not unimaginable and implementing PCA common accuracy of 88.88% was accomplished. Moreover, advancement have been made by including the privet key to have safe network model whilst transmitting the biometric statistics over the network. Nonetheless, the technique faces a low popularity time rate and accuracy.

Recognizing the face from a video that comprise faces of people was the work in [6]. In this paper, video sequences had been taken as inputs. The technique changed into primarily based on monitoring-and-recognition, which attempted to resolve uncertainties in monitoring and recognition simultaneously in a uniformed probabilistic framework. This device has the potential to understand a face from a video but with low monitoring and recognition accuracy. Even though, the inability to handle tremendous appearance modifications because of pose and illumination variations is one of its weaknesses. However, the result

obtained supplied better overall performance over other protection system as accuracy become above ninety percent, and one hundred percent recognition was accomplished.

The authors in [7], developed a system that detected and identified faces of humans to resolve security issues. It used a real-time facial recognition software for reading a video using a camera which is attached to the system processing the software program. It detected any person's face that is in facing the digital camera, after which checked if this individual face is present in a group of face photos within the database employing the face recognition technique. The device had three predominant obligations for facial recognition specifically: document control, access control, and database retrieval. After checking out on several cases, at the end of it, it obtained an accuracy of about 98% of face detection and about 90% accuracy of face recognition. Also, the Graphical User Interface implementation of the algorithm become accomplished to check and validate the device.

In [8], the automated switching of magnetic door lock system employing microcontroller primarily based on face recognition become evolved. The device was divided into two components. The first component of the machine was totally the GUI based face recognition device at the same time the second component was the microcontroller hardware implementation. The master control slave unit for PIC16F877A microcontroller was the GUI based face recognition device. In this device, a recognized photograph was converted into eight-bit signal as an American Standard Code for Information Interchange (ASCII) using a communication port which is serial to the circuit of microcontroller. Then, the serial signal became changed to CMOS degree signals with the use of MAX232. The signal obtained was then analyzed by means of the microcontroller to lock or release the magnetic lock. The device may be stepped forward to emerge as fully automatic face recognition device by means of including some other feature that robotically seize photo with the aid of a sensor while there is the presence of an individual there at the entrance location. The outcomes and functions on ground for the designed system present that the transfer of statistics all the way from the GUI to the microcontroller became effectively performed after the photo was identified. The image testing became identical with the schooling image that allows you to flip OFF the magnetic lock at door and finally allowed person to go into the room. The matched image was the photo selected by way of consumer, even as they entered picture changed into the photograph traced by way of the device which was effectively finished.

The automatic surveillance in commercial transportation of automobile using security audio-video monitoring system was developed in [6]. The system contains six modules along with three novel ones, that is, Face Recognition and Monitoring responsible for recognizing and monitoring faces of humans when been focused to cameras; Audio event recognition detecting peculiar audio precursor occasions that are for recognizing scenarios which have been predefined by clients; and Audio-Video Scenario Detection for acting excessive level interpretation of the discovered items with the aid of the both that is audio and video occasions which focused mainly on spatio-temporal reasoning. The audio-video event recognition algorithm recognized which scenario have been persisting with the use of radical video occasions detected by means of the primitive video occasion recognition module and the audio activities which are detected by using the audio occasion detection module. The occasion template contained the listing of bodily items involved within the primitive state. These bodily items partly instantiated the scenario template. To apprehend an occasion which is comprised of sub-activities, given the event template partially instantiated, the recognition set of rules decided on (if wished) a fixed of bodily items matching the closing physical variables of object of the occasion version. The step by step instructions then was returned within the beyond for any identified state/event previously that suits the initial component of the occasion model. If the two identified components confirmed the occasion model constraints, the occasion changed into said to be diagnosed. The SAMSIT device was examined on two sets of recorded audio-video streams. These units had been then found out on a train (TER 75700) ready with 4 cameras dealing with each different and 4 microphones mounted along the corridor. The database used in the learning system become composed of 3959 faces under numerous pose and lights situations and audio-video surveillance platform capable of mechanically understand excessive degree human behaviours concerning individuals the usage of both audio and video statistics. There had been two principal difficulties bobbing up inside the audio-video popularity: the synchronization among audio and video activities, in addition to the actual-time recognition. The audio-video monitoring scheme was able digitlly apprehend excessive level of human behaviors regarding people with the use of each audio and video information that is beneficial. This device ought to recognize effectively 5 numerous scenarios distinct by way of end-users. Among them, the situation "vandalism of window" became the most efficaciously recognized.

The system developed in [9] involved face recognition system of 2D/ 3-D survey. It makes use of the following strategies: Linear/nonlinear projection approach, the neural networks, Gabor filters and wavelets, Fractals and iterated functions system, and Thermal and hyperspectral. Face recognition appears to be an amazing compromise between reliability and social popularity and helps to balance protection and privacy. This approach mentioned in preceding sections addressed only segment of existing open questions and a method capable of offering the best performances under any situations does not exist yet. However, the technique for face recognition poses numerous threats to civil rights with the reasons that, firstly it impinged on the privacy of harmless human beings when false positives had been investigated and lastly the face-template records might be stolen and changed.

[10] was a process to protect the facial biometric trait throughout detection time. It based totally on picture-based (statistical) face recognition with the use of the 2DPCA set of rules. The transformation of biometric data in to a

cancellable domain using a polynomial function accompanied with matrices that are co-occurrence. Original facial pictures had been converted non-linearly through a polynomial function that has parameters which can be changed based on the issuing model of the stable cancellable template. Co-occurrence matrices have been also used to improve the accuracy of protection and recognition using a transform to generate a distinctive feature vector. The proposed approach has excessive in flexibility proving terms of creating a new relationship among in independent co-variance matrices. More so, it has both protection and accuracy of biometric information. Using the 2DPCA set of rules for recognition that has no modifications, the accuracy became better to 96% by using 3% extra compared with the initial biometric records.

In [11], used DCT-based feature characteristic vectors for recognition of the face was developed. It consisted of 3 elements: a pre-processing step to segment the records and extract crucial regions or features of the face, the feature choice process, and lastly the classification. The preliminary face recognition algorithm explained in this paper was VQ-based with minimum distance classifier. A codebook of characteristic vectors was figuring out for everyone from the training set. DCT-based function vectors have the extra attraction that the recognition can be done directly at the bit stream of compressed photos. The preliminary recognition effects have been encouraging and produced result however, the correctness of less expensive and much less intrusive systems needed improvement. In the case of registration, computerized landmark localization, artefact removal, scaling, and removal of mistakes because of occlusions, glasses, beard, and so on have been had to be worked out. However, the popularity charges for a database of 500 pix showed promising results.

In [12], the management for security of cellular equipment using facial recognition was developed. It centered on face verification involving four parts, which are before processing, traits extraction, characteristic equivalence and after processing. As for enrolment, three parts had been mentioned that is before processing, characteristic extraction and database registration. Otherwise characteristic vectors might be exclusive from each other, which could purpose hassle inside the characteristic matching degree. The database was used in verification to fit the data with the characteristics vector extracted from the input picture. The set of rules became developed to have portability, and assist 4 predominant environments, firstly, Symbian OS, secondly, Embedded linux. ITRON and lastly, BREW.

The authors in [13] presented the techniques and applications that can be utilized in face recognition. The commonplace strategies like matching using a holistic technique, characteristic extraction approach and hybrid methods were discussed in the paper. In the approach of holistic, whole of the face area is taken into consideration as input records into face capturing device. Eigenfaces is a great example of holistic methods, they are used extensively as an approach for recognition of the face, independent component analysis, Principal Component Analysis (PCA), Linear Discriminant Analysis, amongst others. In traits-based (structural) methods, local traits inclusive of mouth, nostril and eyes had been first off extracted with their positions, and local records (geometric and/or appearance) were given right into a structural classifier. Hybrid face recognition structures used a mixture of holistic and feature extraction techniques. Applications and examples of this proposed method are face Identification, access identification, security, image database investigation, general identification verification, as well as surveillance. Feature extraction technique has a challenge which is characteristic "restoration", which involved the exact time the device attempted to fetch traits that is not visible by the eye because of the huge variations. The problem with the device was that now not all techniques and application were captured. Be that as it can, it provided higher knowledge on face recognition techniques and application.

[14] used Hidden Markov Models to design a facial detection and recognition system. For face recognition, a group of photos was used in HMM training, while each person within the database has a representation by a face model of HMM for face recognition. This version used an effective group of observation vectors which is based on the fetching of the KLT coefficients. It yielded efficient and correct results for face detection and recognition system. More so, this technique regarded to have a promising method for face detection. It hence allowed fast implementation because of the face template needs to be broken into quick remark vectors.

[15] introduced the use of 3-D for biometric software face recognition. The proposed method used two techniques particularly the stereo acquisition and structural light approach. In stereo acquisition approach, more than one cameras that have been located and adjusted have been employed to accumulate snapshots of a person occurring the same time. Each factor has a depth information which has been computed from geometrical fashions and by fixing a correspondence problem. The structural light approach involved a light sample projected at the face, where the distortion of the pattern shows depth facts. It categorized and summarized the applicable 3D face recognition based on the primary representation used in the recognition set of rules for example, the curvatures and surface features, factor cloud and meshes, depth map, profile, evaluation by synthesis and mixtures of representations. Nonetheless, correctness of inexpensive and intrusive-free structures needed to be stepped forward, and temporal sequences must be taken into consideration. For registration, automated landmark localization, artifact removal, scaling, and elimination of errors are taken into consideration because of beard, occlusions, glasses, and many others. Had to be worked out. However, the end result obtained confirmed that statistics fusion become in the three-D face reputation, which assisted in biometric software of face detection. A single training instance case for a realistic structures, should be put into account, whilst for publicly to be had 3D datasets were important to encourage additional research on those topics.

Frontal-view face detection and facial feature extraction using color, shape and symmetry-based cost functions

turned into presented in [13]. A primarily based supervised pixel colour classifier was used to mark all pixels that had been inside a pre-exact distance of skin shade which was calculated from a training set of patches of the skin. This coloration-category map was then refined by using Gibbs random field version model-based filters to define pores and skin regions. An ellipse model was match to the centre of the eyes, tip of the nose, and centre of mouth inside ellipses whose element ratio become much like that of a face. The paper helped to describe the algorithm for recognizing human faces with the use of colour and shape statistics after which localizing the eyes, nostril and mouth via using symmetry-primarily based fee features. However, there was no right software program optimization and the set of rules was restrained to frontal facials views, and therefore could not yield meaningful outcomes on profile. The situations did not present any serious limitation in security type applications wherein the character would ought to stroll past a camera or display a photo badge to get entry to a specific place. Nevertheless, the algorithm changed into an effective way in identifying faces and facial traits, in which the face sample shows as the front view and the two eyes had been seen in the act.

The authors in [16] utilized micro functions, which include facial marks (e.g., freckles, moles, and scars) to improve face recognition and retrieval overall performance. The method in this paper employed using Active Appearance Model (AAM) to find and segment primary facial features (e.g., eyes, nose, and mouth). This was accompanied via Laplacian-of-Gaussian (LoG) and morphological operators used to locate facial marks. It also used FERET and a Mugshot face database for comparing the proposed mark-based matcher. FERET (Mugshot) database consisted of 426 (1,225) photographs belonging to 213 (671) specific topics, wherein 213 (554) of the topics in the database had reproduction snap shots. It supplemented the characters in a present face matcher and enabled matching or retrieval from a partial or profile face photograph with marks. The end result obtained confirmed that using facial marks improved the rank-1 identity accuracy of a contemporary face reputation system from 92.96% to 93.90% and from 91.88% to 93.14%, respectively. However, there has been need to enhance the mark primarily based photograph retrieval and matching accuracy.

Finally, the paper presented in [17] was on the quality of photo assessment for detection of fake biometric relevant to fingerprint, iris and face detection. This work involved a singular software program-primarily based on fake detection approach which is used in more than one biometric system to identify several forms of access which are fraudulent. The objective of the system proposed was to improve the safety of biometric detection scheme, by means of adding evaluation in a speed, user pleasant and intrusive-free way, via the application of Image Quality Assessment (IQA). The approach which was proposed provided totally low level of complexity which made it best applicable for actual-time application, the use of 25 general picture satisfactory capabilities fetched from one picture (that is, equal obtained for verification purposes) to differentiate among valid and data. The training effects obtained on publicly available data sets of finger-print, iris and a pair of-D face, confirmed that the proposed technique become highly competitive compared to other new ways and the evaluation of the whole photo satisfactory of real biometric data found out distinctly treasured information that can be very correctly used to discriminate them from faux developments. This work has presented the excessive capacity of quality photograph assessment which are used for securing the biometric software against various attack.

CONCLUSION

This paper introduced biometric technology which is an area that is fast growing, how it can be applied to solve different problems ranging from security issues such as terrorism, kidnapping, theft among others. It shows that it is the best technique for authentication, verification, identification and authorization.

The intelligent security check system using face detection algorithm has been presented, how images will be captured, processed, compared with what is in the database and display available metadata related to the image. It will have a high accuracy facial recognition rate. The hypothesis will be tested on 50 different images.

Additional techniques can be added for verification and authentication of images. The future work can be focused on extraction of information from the internet instead of relying solely on database. The extraction of the facial feature and ability to recognize it irrespective of the expression, aging and pose will also be recommendation in future.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 2, pp. 125–143, 2006.

[2] H. R. Farhan, "Face Recognition using DWT with HMM," *Proc. 19998 IEEE Int. Conf. Acoust. speech signal Process.*, vol. 30, no. 1, pp. 142–154, 2012.

[3] A. kumar singh and G.C Nandi, "Face Recognition Using Facial Symmetry," in *proceedings of the Second International Conference on Computational Science, engineering and Information Technology*, 2012, pp. 550–554.

[4] D. C. L. Ngo, A. B. J. Teoh, and A. Goh, "Biometric hash: High-confidence face recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 6, pp. 771–775, 2006.

[5] E. Kremic, A. Subasi, and K. Hajdarevic, "Face Recognition Implementation for Client Server Mobile Application using PCA," in *proceedings of the ITI 2012 34th International Conference on Information Technology Interfaces, Cavtat*, 2012, pp. 435–440.

[6] V. Vu, G. Davini, M. Thonnat, Q. Pham, N. Allezard, P. Sayd, J. Rouas, and V. Vu, "Audio-Video Event Recognition System For Public Transport Security ebastien Ambellouis , Amaury Flancquart To cite this version :," in *International conference on Crime detection and Preventation (ICDP 2006)*, 2006, pp. 414–419.

[7] M. Owayjan, A. Dergham, G. Haber, N. Fakih, A. Hamoush, and E. Abdo, “Face Recognition Security System,” in *elliithy K., Sobh T. (eds) New Trends in Networking, Computing, E-Learning, Systems Sciences and Engineering. Lecture Notes i electrical Electronics*, 2015, pp. 343–348, vol. 312.

[8] H. Hassan, R. Abu, B. Ahmad, and T. Fawwaz, “Face Recognition Based on Auto-Switching Magnetic Door Lock System Using Microcontroller,” in *2012 International Conference on System Engineering and Technology September 11-12, 2012, Bandung, Indonesia*, 2012, pp. 28–34.

[9] A. F. Abate, M. Nappi, D. Riccio, and G. Sabatino, “2D and 3D face recognition: A survey,” *Pattern Recognit. Lett.*, vol. 28, no. 14, pp. 1885–1906, 2007.

[10] M. A. Dabbah, W. L. Woo, and S. S. Dlay, “Secure Authentication for Face Recognition,” in *proceeding of the 2007 IEEE Symposium on Computational Intelligence in Image and Signal Processing*, 2007, no. Ciisp, pp. 121–126.

[11] C. P. and X. Zhang, “face recognition using DCT based system vector.pdf,” in *1996IEEE International Conference on acoustics, Speech, and Signal Processing Conference Proceeding*, 1996, pp. 2144–2147, vol. 4.

[12] Y. Ijiri, M. Sakuragi, and S. Lao, “Security Management for Mobile Devices by Face Recognition,” in *7th international conference on mobile data management*, 2006, pp. 49–49.

[13] D. N. Parmar and B. B. Mehta, “Face Recognition Methods & Applications,” *int. J.Computer Technol. Appl.*, vol. 4, no. 22229–6093, pp. 84–86, 2013.

[14] A. V. N. and M. H. H. III, “face detection and recognition using hidden markov models,” in *proceedings 1998 International Conference on Image Processing ICIP98*, 1998, pp. 141–145, vol. 1.

[15] L. Akarun, B. Gökberk, and A. A. S. Salah, “3D face recognition for biometric applications,” in *13th European Signal Processing Conference, EUSIPCO 2005*, 2005, pp. 1–5.

[16] A. K. J. and U. P. Park, “Facial marks: soft biometric for face recognition" Anil K. Jain and Unsang Park Department of Computer Science and Engineering Michigan State University, East Lansing, MI 48824,” in *16th IEEE International Conference on Image Processing (ICIP), Cairo*, 2009, pp. 37–40.

[17] J. Galbally, M. Member, and J. Fierrez, “for Fake Biometric Detection: Application to Iris, Fingerprint and Face Recognition,” vol. 2, pp. 710–724, 2014.