IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 3, Issue 10, October 2023

Impact Factor: 5.731

Information Extraction for Touch Free Biometric Authentication System from Large Databases using Deep Learning Algorithm

Dhanaraj Jadhav[1] and Dr. Jaibir Singh[2]

PhD Scholar, Department of Computer Science and Engineering[1]

Associate Professor, Department of Computer Science and Engineering[2]

Om Prakash Jogender Singh University, Rajgarh (Sadulpur), Churu, Rajasthan, India

Abstract: *Users' privacy must be strictly protected because smartphones have become an essential tool for storing sensitive data. This may be performed by using the most accurate and trustworthy bio-metric authentication techniques available, like iris, voice, facial and fingerprints cognizance. This paper presents a way to develop and test biometric recognition system for smartphones. Touch-less biometric recognition system is an implementation of biometric verification and identification system on mobile phones that utilizes mobile phone cameras and microphone to acquire the biometrics of the user. Once the data is captured, they are pre-processed using standard pre-processing algorithm to obtain the skeleton. This is used to extract true minutiae eliminating all the false minutiae. The usage of mobile phones for biometric recognition makes it quite convenient and feasible for everyone. Also, touch-less system has a lot of advantages over touch-based ones and hence, they become a more popular choice.*

Keywords: Deep Sparse Filter, Iris recognition, Face recognition, Biometrics, Machine learning, Identity authentication, Fingerprint classification, Eigenfaces, Picture pre-purifying, Arbitrarily Forest, Support-vector-machine, Hough transform, Face detection, Fisher faces, Singularity feature, Android application, Voice feature, Visible Light.

I. INTRODUCTION

Biometric identification systems have become one of the most important systems for recognizing people's identities nowadays. It has aided security in a variety of areas, including banking transactions, Aadhar identity, high security wireless access, biometric attendance, and approved personnel identification for access to restricted locations. Traditional identification system made the use of id cards or passwords, however they might be stolen, lost or forgotten impending a threat to security system. The recognition systems which employ those traits inherent to humans can probably decrement fraudulent cases. Biometric systems have the advantage of user convenience as opposed to cards, codes keys etc.

1.1 Iris Recognition

Many current iris recognition technologies are extremely accurate. However, the majority of them rely on photos captured by an infrared camera, which comes at a significant price for smartphone consumers. As a solution, using built-in cameras in mobile phones that utilise visible light (VL) imaging is suggested. Enrolment and verification are the two main purposes of an iris recognition system. The segmentation step begins with the smartphone camera capturing the eye, followed by the iris borders being located. Normalisation is the process of converting an iris picture into a fixed-size pattern. The algorithm extracts and compares the pattern's features to the pattern's features. Another decision-making template that has been put in a database (accept or reject). Because visible-wavelength photos include more noise, such as reflections, illuminations, and less iris texture features than infrared images, using the smartphone's built-in camera typically demands certain pre-processing processes before iris segmentation.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 3, Issue 10, October 2023
Impact Factor: 5.731

1.2 Voice Recognition

Because the vocal organs they utilise to communicate, such as the lungs, mouth cavity, and nasal cavity, vary in shape and size, different people have different voice quality. Its biometric authentication application also requires this feature. Voice has a few key advantages over other biological characteristics: non-contact, low-cost technology, broad application, and ease of use. There are two aspects to a speech recognition authentication system: registration and authentication. Users must first register, then get a unique registration code (used for reading the contents), and last gather & enter audio. Audio material is initially detected after successful capture of voice segments. If it meets the predefined information, given procedure include processing, speciality withdrawal, model training, matching & authentication.

1.3 Face Recognition

Bio-metric authentication technique, particularly human facial cognizance, has been a famous field of study in previous 10 years. Due to the rapid growth of smart phones, facial cognizance system implementation on smart device platforms like ANDROID has become a hot topic. One of the main hurdles to facial cognizance for smart device processing is the issue of fluctuations in facial images taken in an uncontrolled setting. Another computational restriction of smart device platforms.

1.4 Fingerprint Recognition

Biometric identification methods based on fingerprints are extensively used. The fingerprint of each person is unique and does not change over time. Ridges and valleys make up a fingerprint. A valley is defined as the space between two adjacent ridges, whereas a ridge is a continuous curved line. In order to match other fingerprints, certain features must be recovered during fingerprint analysis. Almost every image of a fingerprint is of poor quality. Noise can deform or impair each object's skin qualities (temperature, skin humidity), fingerprints, finger position (Fingerprint Angle & Area), and coercion (Too Strong/Weak) while rolling out samples.

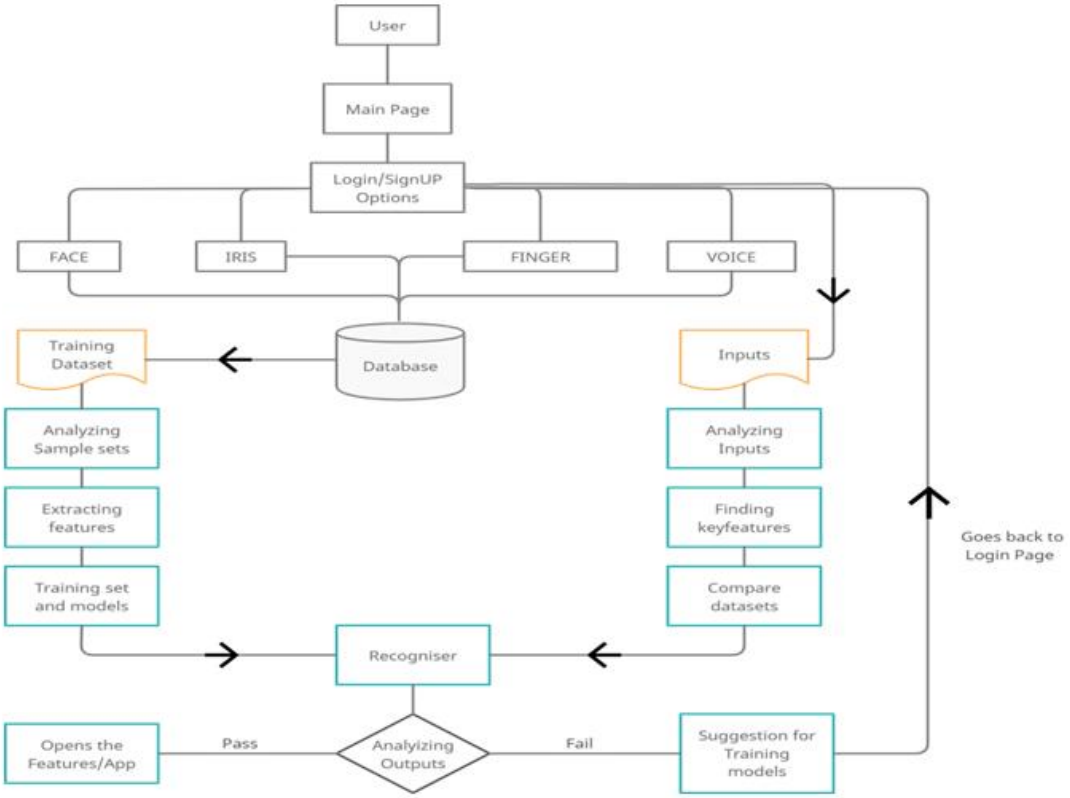

Figure 1. System Data Flow Diagram

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 3, Issue 10, October 2023
Impact Factor: 5.731

II. RELATED WORK

2.1 Iris

The created technique aims to identify people based on their iris texture. Enrolment and verification are the two fundamental functions of the system. The system must initially be able to perform these functions. From the captured eye image, crop the iris region. The Haar Cascade is used to complete this operation. The accuracy achieved by the classifier is 86 percent. During the segmentation procedure, the iris is pre-processed. Various sounds are reduced using the image. Following that, the iris and pupillary margins are segmented. The Hough transform is circular. The average accuracy for this stage is 78.25 percent. The iris image is normalised using the Rubber Sheet model. To extract features from the iris picture, Deep Sparse Filtering is performed. Finally, the features are recorded in a template in the enrolment function and matched with a template in the verification function. The City Block formula is used to match features in order to make a judgement (Accept/Reject). The Equal Error Rate, which was 0.18, was used to determine the system's correctness. In addition, the system is put through its paces online with the use of a custom interface. The system is practical and functional at all times. It does, however, require certain enhancements in order to achieve more efficiency and accuracy.

Voice -

On the Android smart phone platform, this thesis investigates and constructs a speech biometric authentication system. The properties of the speech database, as well as the voice recognition and authentication system flow, are discussed first. The voice cypher is then generated using a random shuffling technique. Following that, the MFCC-based voice feature extraction algorithm is shown. The voiceprint feature model is efficiently trained utilising voice segment data using GMM in this work. The system authentication success rate is between 89 and 96 percent at 5 training samples, and the time required lies in 210 and 320 milliseconds, exhibiting high accuracy and real-time performance.

Face

The creation and development of an open-source facial identification system for the ANDROID that works well on smartphones. The experiment on real-world face photos yielded 93.8 percent accuracy with Eigenfaces and 96.0 percent with Fisher faces after face detection and ROI pre- processing. More useful functions, other face recognition technologies, such as deep learning-based face recognition, may be combined with the X Face system in the future, such as facial expression recognition or gender recognition.

Finger

Machine learning is becoming increasingly significant in practical applications. As a result, scientists are exploring and creating increasingly advanced machine learning technologies. Fingerprint categorization is one of the applications that is gaining popularity. Reference investigates a solution to the fingerprint classification problem. This effort will lower the variation of the element directions by segmenting the fingerprint into sections. The segmentation of the directed image is used to create a relation graph. The resultant graph is compared to a model graph, which can be used to graph matching algorithms. A method using analytical singularities and ridges linking singular spots is proposed in Reference. Due to low image quality, determining correct placements of distinctive features is difficult. The author uses rigid tracing and curve features to classify fingerprints.

III. MAJOR TECHNIQUES USED FOR DIFFERENT MODELS

3.1 Iris

Support Vector Machine Algorithm

A typical Guided Learning technique for handling classification and regression issues is the Support Vector Machine (SVM). However, it is usually utilised to tackle classification issues in Machine Learning. Every data item is presented as a point in N-Dimensional space (Where N is number of features), with the value of every feature being the result of the Support Vector Machine Algorithm for a given position. Then, to complete classification, we choose the hyper-plane that best differentiates the 2-classes. Simply explained, SV are the co-ordinates of each and every

observation. The SVM classifier acts as a border between the two classes (hyper-plane and line).

Normalization:

Normalization is a data pre-processing technique for converting numerical data to a common scale without changing the shape of the data. When we feed data into a machine learning or deep learning system, we usually modify the numbers to a balanced scale. Including some fairly advanced algorithms for processing photos in low-light settings or with a cluttered background.

Voice -

Hidden Markov Model

A probabilistic model called Hidden Markov model is used to explain or infer the probabilistic features of any randomly chosen process. It simply means that an observed occurrence would be assigned. Let's pretend that the system being modelled is a Markov chain, and that there are some hidden states in the process. Hidden states, in this situation, are a process that is dependent on the primary Markov process/chain. HMM's major purpose is to observe a Markov chain's hidden states in order to learn about it. In the case of a Markov process X with hidden states Y, the HMM establishes that the probability distribution of Y for each time stamp must not be influenced by the history of X at that time.

Artificial Neural Network

Calculates features that reveal the spectral content of the voice by dividing the waveform into frames (regions of high energy at specific frequencies). At each frame, a neural network (sometimes known as multilayer perception/ MLP) organises the input into phonetic categories. To match the neural network output scores to target words, Viterbi search is performed.

MFCC

Windowing the signal, using the DFT, obtaining the log of magnitude, and then wrapping the frequencies on Mel scale, followed by applying the inverse DCT & all part of the MFCC feature extraction approach. The MFCC coefficient is a characteristic value for feature extraction that may be generated in the Mel frequency domain. It exploits the human auditory edge effect to simulate the feeling of numerous frequencies in Ears. Mel frequency explains the non-linear aspects of human perception of external sound frequency and expression may be used to approximate its relationship to real frequency. 2595* log (1+f / 700) Mel(f)3.

Face-

LBPH Algorithm

Because Eigenfaces and Fisher faces both take a holistic approach, each image's features are distinct from those of other photos, rather of depicting the high-dimensional vector, the LBPH method illustrates the local attributes of the objects. As a result, updating the classifier may be done without having to retrain the entire database of faces.

Colour Segmentation

Face detection using skin colour detection in colour photos is a common and useful technique. Each pixel was identified as skin or non-skin in the skin colour detection procedure based on its colour component values. According to the literature, colour segmentation can be done in a variety of ways, including some fairly advanced algorithms for processing photos in low-light settings or with a cluttered background.

Morphological Image Processing

Pixels are added or subtracted from images during morphological processing. The structure and shape of the things are studied in order to identify them. Binary convolution and correlation are the core processes in this processing, which are based on logical rather than mathematical calculations. The core operations are dilation and erosion, and the rest of

the operations and algorithms are built around them. The minimum and maximum operators are used to extend morphological processing to grey level images.

CNN:

CNNs are a sort of deep learning neural network that uses convolutional neural networks. Consider CNN to be a machine learning system that can take an input image and assign importance (learnable weights and biases) to distinct aspects/objects in the image, as well as distinguish between them. CNN extracts feature from photographs to obtain information. The components of any CNN are as follows:

- As the input layer, a grayscale image is used.
- A binary or multi-class labelling system is used as the output layer.
- Hidden layers include convolution layers, Relog (rectified linear unit) layers, pooling layers, and a fully linked Neutral Network.
- It's important to remember that Artificial Neural Networks (ANNs), which are made up of a lot of neurons, are incapable of extracting features from photos. A convolutional and pooling layer mix is used in this case. Similarly, classification is impossible with the convolution and pooling layers, necessitating the deployment of a fully linked Neural Network.

Fiducial Point Detection:

Fiducial points are marks you make on your specimen to assist you align successive sections. Fiducial points and contours can be placed or traced.The requirements are identical. Fiducial points are points that can be found in every component of the building you're re-creating.

Finger -

Minutia Extraction Algorithm:

Most fingerprint minutia extraction methods use the skeletonization procedure to decrease each ridge to one pixel width. On the thinned ridge skeleton, the termination points and bifurcation points are found by counting the number of neighbouring pixels and identifying the termination points and bifurcation points. If there is only one neighbour, the end points are chosen, and if there are more than two, the bifurcation points arechosen.

Binarization and Thinning:

The fingerprint image must be in binary format to extract minutia, with black pixels corresponding to foreground ridge structures and white pixels corresponding to background non-ridge structures or troughs. Binarization converts a grey-scale image to a binary image, which improvesthe contrast between hills and valleys and makes tiny point extraction easier.

Gabor Filtering:

The combination of the Orientation Image and the Ridge Frequency Image aids in the construction of an even symmetric Gabor Filter. A 2D Gabor filter is a sinusoidal plane wave modulated by a Gaussian envelope tuned to a particular frequency and direction. When adjusted to the local ridge frequency structure, such a filter provides the best response. It improves local contrast by enhancing ridges and suppressing non ridge structure. An even symmetric Gabor filter is formed when a Gaussian modulates a cosine wave, and it is a genuine portion of the Gabor function.

Image Segmentation:

Segmentation is the process of separating ridges and troughs in the foreground of a fingerprint picture from a descriptive or non-descriptive backdrop. The background areas are those that are outside the fingerprint boundary and do not contain any fingerprint information, thus they must be segmented out. The minutia extraction algorithm will produce false minutia if background information is allowed, and the matching will deteriorate as a result. When the camera flash light falls on the finger image during touchless acquisition, the foreground finger image brightenswhile the

background darkens. As a result, the foreground image has a higher grey-scale covariance than the background, and segmentation canbe done using covariance thresholding.

Black Hole search method:

The method of Black Hole search is used to determine the pupil's centre and area. Because the pupil is the darkest part of the picture, this approach applies a threshold segmentation method to find it. To begin, a detection threshold for dark areas in the iris picture is established. "Black holes" are what the dark spots are called. The global picture is used to compute the black hole's centre of mass. The total number of black holes in the region is represented by the pupil area. The circle area formula may be used to compute the pupil's radius. For iris images with dark iris, the black hole search approach is ineffective. Instead of the pupil, the black iris region would be observed

Bisection Technique

The bisection approach is used in both circumstances to determine the pupil's centre. The outer and inner margins of the iris are established using the pupil's centre as a reference. To get edge information, the iris picture is initially subjected to edge detection. The method of bisection is used to create perpendicular lines from any two places on the same edge component to the centre point. The pupil's centre is determined by the place with the most line intersections. The radius of a virtual circle created around the pupil's centre is increased between a particular range. The inner and outer borders of the iris are made up of the two virtual circles with the largest edge points. Non-uniform illuminations and glassware reflections have an impact on the bisection procedure. A result, pinpointing the iris inner border is challenging. To eliminate the high intensity regions created by illuminations and reflections, a discrete circular active contour method-like image pre-processing technique is required.

IV. PAPER PUBLICATION SUMMARY

Year of Publication	Title	Summary
2021	Types of Authentication Safety Practices among Internet Users.	One of the most significant strategies for keeping information secure in smart devices is the authentication mechanism. Three key themes emerged from the conclusions of the study: Password Authentication, Biometric Authentication, Multi- factor Authentication.
2020	Research Paper on Biometrics Security.	The quality of fingerprints acquired from mobile phone cameras is resolution dependent, at first sight it seems to be a drawback, but the rising technology trends that provide best resolution cameras in cheaper phones makes resolution dependency, less of a problem.
2018	Voice Biometric Identity Authentication Android-based smart phone system.	This research focuses on the relevant ideas and algorithms for a voice identity authentication system, as well as the Android implementation of the system.
2018	Voice Biometric: A Technology for Voice Based Authentication.	This paper demonstrated the usefulness of forensic linguistic in the security critical areas. In addition, it has also discussed about the techniques to be used to develop such type of systems.
2017	Developing iris recognition system for smartphone security	Work of an iris system for smartphones develop and tested. Method relies on visible-wavelength eye pictures, which are captured by the smartphone's camera.

2017	Biometric Voice Authentication Auto-Evaluation System.	We create a unique approach to analyse the statistical disadvantages of randomly picked biometric voices from the TIMIT speech database by using the AWGN MATLAB function with varied SNR levels to offer an assessment report based on FAR and FRR biometric measurements. By empirically running the algorithm on half of the biometric voices in the database, we uncovered some voices that can resist the AWGN and make the system safer.
2016	Face Recognition on Mobile Platforms.	The application is written in standard C++11 and may be produced for usage on both a PC and a smartphone. Although the complete application logic operates at 12 frames per second on a smartphone without any optimization, there is a considerable performance loss on mobile devices. Because the implementations are for x86/x64 processors rather than ARM processors, future optimization and tuning of the settings will be necessary. This is backed up by the fact that smartphone CPU usage is presently between 35 and 45 percent, indicating that the device still has plenty of resources. Because images with resolutions higher communication between the user interface and the application logic should be enhanced, as VGA are transmitted and transformed slowly. For example, a frame from the application logic may be stored by uploading it to an OpenGL texture and then showing it on the UI side with a GL Surface View.
2015	Face based authentication on Mobile devices.	We investigate how well modern in this study, photo set-based approaches are integrated with fiducial point-based characteristics to provide active authentication on cell phones. To capture the sorts of changes that are predicted to be present with mobile devices, a dataset of 750 videos was gathered during three sessions with varying lighting conditions. The films in the dataset indicated the following: that smartphone face videos had a specific set of characteristics and issues. To improve the effectiveness of the face detection phase and reduce false positives, we took use of since the user's face is continuously near to the phone.
2014	Touchless Fingerprint biometric survey of 2D and 3D technologies.	Touchless recognition systems are classified as two types: 2D data and 3D models. Most of the two-dimensional systems use a single camera and use enhancement and resolution normalisation methods to create touch-equivalent pictures. These systems are usually less costly than three dimensional technologies, but they have issues with perspective deformations and non-constant sample resolution. Multiple- view setups, structured lighting methodologies, and photometric stereo tactics may all be used to create three dimensional systems. The three-dimensional models that are created might have various levels of detail. Touch equivalent pictures are computed in these systems using "unwrapping" techniques, which transfer three-dimensional data into two- dimensional space. These algorithms might be based on assumptions about the shape of the finger (parametric algorithms) or on examination of local fingerprint features (non-parametric techniques).
2008	A Review of Iris Recognition Algorithms.	This document gives a survey of well-known iris recognition studies. There are three phases to the algorithms employed in iris recognition: image template, Pre-processing matching and feature extraction Each

		algorithm's effectiveness. The effectiveness of each stage is evaluated. Iris recognition is becoming more popular. Because of its dependability and correctness If the iris recognition does not work, Algorithms have been tuned for specialised low-cost devices. It will be used in a variety of applications as hardware.
2006	Biometric Authentication using Voice.	Traditional access methods have a number of drawbacks, including the possibility of loss, theft, or illegal lending. Furthermore, they have no control over the customer's true identity and rely on the user to remember codes or passwords. Because the biometric key is produced based on the individual's unique features, it is immune to the previously mentioned issues. However, there are additional issues to consider. Another issue is that a person's voice can be copied. We think that a trustworthy system should be able to recognise which parts of the speech signal are impossible to replicate and use them as a key point during the verification phase.

Table 1 Paper Publication Comparison

V. CONCLUSION

An open-source biometric identification system for the Android platform was designed and implemented. is described in this paper, and it works well on Android mobile phones. It is now possible to obtain biometric images from a smartphone without the use of a dedicated and more expensive device, extract minutiae from the pre-processed image, and execute matching using secure mobile – webserver connection. Because of the simplicity and feasibility, obtaining biometric images from devices such as mobile phones, which are now owned by practically everyone, is becoming a more common choice. Furthermore, mobile phone cameras offer a deeper depth of 3D resolution than dedicated devices. This provides additional information about the biometric factor, which improves the accuracy of matching FAR and FRR rates that are falling. Experiments with more datasets gathered using mobile phone cameras will be conducted in the future. Using higher performance devices for the training step can improve the accuracy of biometric factor detection. The matching step be improved by including a step to deal with corruption or experimenting with deep learning algorithms We plan to make the system available as an API component that can be used to lock cell phones or any application that requires a high level of authorisation in the future. Additionally, scanning the factors rather of recording images will improve the photo quality.

REFERENCES

[1]. R. Wildes, IEEE. [Iris Recognition: - An Emerging biometric technology], (proceeded by IEEE, sept 1997).

[2]. S. Olatinwo; O. Shoewu & O. Omitola. [IRIS RECOGNITION TECHNOLOGY: IMPLEMENTATION, APPLICATION, AND SECURITY CONSIDERATION], Nov 2013 {Fall}.

[3]. L. ELREFAEI; D. HAMID; A. BAYAZED; S. BUSHNAK & S. MAASHER. [Developing Iris Recognition System for Smartphone Security]. 21 JUL 17 @ Springer Science & Business Media.

[4]. R. Fatt; Y. Haur Tay & K. Ming Mok. [A Review of Iris Recognition Algorithms]. Computer Vision & Intelligent System Group University of Tunku Abdul Rahman, Sept 2008.

[5]. S. Arslan Ali; M. ALI Shah; T. A. Javed; M. Abdullah; M. Zafar. [IRIS RECOGNITION_ SYSTEM IN SMARTPHONES WITH LIGHT-VERSION RECOGNITION ALGO]. Proceeded in 23rd International Conference on automation, university of Huddersfield, Sept 2017.

[6]. R. Vyas; T. Kanumuri; G. Sheoran & P. Dubey. [Effi-cient Features for Smartphone based Iris Recognition]. TURK J ELEC & COMP ENG (2019).

[7]. A. NITHYA & Dr. LAKSHMI. [Iris Recognition Techniques: A Literature Survey]. International Journal of applied Engineering & Research; Jul 2015.

[8]. S. Attarawala & Prof. S. Nirmanik. [Iris Recognition System]. jetir May 2020.

[9]. Haiqing li; Z. Sun; M. Zhang; L. Wang; L. Xiao & T. Tan. [A brief survey on recent progress in iris recognition].

[10]. M. De Marsicoa, M. Nappi & H. Proença. [Mobile iris challenge evaluation part II], Pattern recognition letters: April 2017.

[11]. MARKOV MODEL]; Dec 2008. 1. K Brunet; K Taam; E Cherrier; N Faye & C Rosenberger. [Speaker recognition for mobile user authentication; an android solution]. sept 2013.

[12]. MANUELA MARZOTTI AND CRISTINA NARDINI. 'BIOMETRIC AUTHENTICATION USING VOICE'.

[13]. Nilu singh; Alka Agrawal & R. Khan. [VOICE-BIOMETRIC:A TECHNOLOGY for VOICE - AUTHENTICATION]. ENGINEERING AND MEDICINE – JULY-2018.

[14]. S. Trewin; Cal Swart; L. Koved; J. Martino; K. Singh & S. Bendavid. [BIOMETRIC-AUTHENTICATION ON MOBILE DEVICE: A STUDY OF USERS EFFORT, ERROR & TASK DISRUPTION].

[15]. R. Tanwar; K. Singh & S. Malhotra; [An Approach TO Ensure Security WIth Voice Authentication System]; International journal of recent technology and engineering JAN-2019.

[16]. X. Zhang; Q. Xiong; Y. Dai & X. Xu; [VOICE BIOMETRIC IDENTITY AUTHENTICATION SYSTEM BASED ON ANDROID SMART PHONE]; international conference on computer and communications ieee [IV] 2018.

[17]. Prof. Dr. S. Sadkhan; Dr. B. Al-shukur & A. Matter; [BIOMETRIC VOICE AUTHENTICATION AUTO-EVALUATION SYSTEM]. Annual conference on new trends in information & communications technology applications (7 – 9) MAR 2017.

[18]. R. maduranga jayamaha; M. senadheera; N. gamage; P. weerasekara; G. dissanayaka & N kodagoda; [HUMAN VOICE AUTHENTICATION SYSTEM USING HIDDEN

[19]. Shah F. Darwaisha; E. Moradiana; T. Rahmanib; M. Knauer. [BIOMETRIC IDENTIFICATION ON ANDROID SMARTPHONES]. department of comp & sys-sci, stockholm university, SWEDEN GERMANY.

[20]. K. Bertok & A. Fazekas; [FACE RECOGNITION ON MOBILE PLATFORMS]. (VIIth) IEEE INTERNATIONAL CONFERENCE (COGNITIVE INFOCOMMUNICATIONS); OCT 16-18; POLAND.

[21]. J. HU; L. Peng & L. Zheng; [X-FACE: A FACE RECOGNITION SYSTEM FOR ANDROID MOBILE PHONES]. 2015 IEEE (IIIrd) INTERNATIONAL CONFERENCE ON CYBER-PHYSICAL SYSTEMS, NETWORKS & APPLICATIONS.

[22]. W. deng; X. Zhang & Z. jiang. [A MOBILE APPLICATION OF FACE RECOGNITION BASED ON ANDROID PLATFORM]; 2020 (16TH) INTERNATIONAL CONFERENCE ON COMPUTATIONAL INTELLIGENCE & SECURITY

[23]. Prof. H. Soliman; A. Saleh & E. Fathi. [FACE RECOGNITION IN MOBILE DEVICES]. INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS, JUL-2013.

[24]. M. E. FATHY; V. M. PATEL & R. CHELLAPPA. [FACE-BASED ACTIVE AUTHENTICATION ON MOBILE DEVICES]. @ IEEE ICASSP 2015.

[25]. V. Ravibabu & Dr. N. Krishnan. [A VARY APPROACH TO FACE RECOGNITION VERITABLE MECHANISMS FOR ANDROID MOBILE AGAINST SPOOFING]. 2014 IEEE international conference on computational intelligence & computing research.

[26]. H. Baqeel & S. Saeed; [FACE DETECTION AUTHENTICATION ON SMARTPHONES: END USERS USABILITY ASSESSMENT EXPERIENCES]; Department of computer science, college of computer science and information technology, @2019 IEEE.

[27]. M. Zulfiqar; F. Syed, M. Jaleed Khan & K. Khurshid. [DEEP FACE RECOGNITION FOR BIOMETRIC AUTHENTICATION]. (1ST) INTERNATIONAL CONFERENCE ON ELEC., COMM. AND COMPUTER ENGINEERING (ICECCE) (24th) - (25th) JUL- 2019.

[28]. G. Dave; X. Chao & K. Sriadibhatla. [FACE RECOGNITION IN MOBILE PHONES]. Dept of Elec Engg Stanford university Stanford, USA.

[29]. G. Hassan & K. Elgazzar. [THE CASE OF FACE RECOGNITION ON MOBILE DEVICES]. IEEE WIRELESS COMMUNICATIONS & NETWORKING CONFERENCE 2016 SERVICES, APPLICATIONS & BUSINESS.

[30]. A. K. JAIN; Lin Hong; Sharath Pankanti; & RUUD BOLLE: IEEE. [AN IDENTITY-AUTHENTICATION SYSTEM USING FINGERPRINTS]. PROCEEDINGS OF THE IEEE, Sept 1997.

[31]. Zhang rui & Zheng yan IEEE. [A SURVEY ON BIOMETRIC AUTHENTICATION: TOWARD SECURE AND PRIVACY- PRESERVING IDENTIFICATION]. DEC 27- 2018, JAN 16, 2019.

[32]. Huong T. Nguyen & Long T. Nguyen. [FINGERPRINTS CLASSIFICATION THROUGH IMAGE ANALYSIS AND MACHINE LEARNING METHOD]. 11 NOV 2019.

[33]. S. Milshtein; A. Pillai; A. Shendye; C. Liessner & M. Baier. [FINGERPRINT RECOGNITION ALGORITHMS FOR PARTIAL AND FULL FINGERPRINTS]. 2008 IEEE.

[34]. Meet H. Haria & prof. V. M. Gadre. [Touchless Fingerprint Recognition System]. DEPT OF ELEC ENGG, INDIAN Institute of Technology Bombay.

[35]. Ruggero D. Labati; A. Genovese; V. Piuri; F. Scotti; [TOUCHLESS FINGERPRINT BIOMETRICS: A SURVEY ON 2-D AND 3-D TECHNOLOGIES]. DEPT OF COMPUTER SCIENCE UNIVERSITITY, ITALY.

[36]. J. Priesnitz; C. Rathgeb; N. Buchmann; C. Busch & M. Margraf; [AN OVERVIEW OF TOUCHLESS 2-D FINGERPRINT RECOGNITION]. (2021)

BIOGRAPHY

Dhanaraj Jadhav is a Research Scholar in the CSE Department, Om Prakash Jogender Singh University, Rajgarh (Sadulpur) Churu - Rajasthan. He received MTech in CSE degree in 2015 from JNT University, India. His research interests are Computer Networks, Machine Learning, Deep Learning etc.