

Evolution of Biometric Technology

Sourav Biswas ^[1], Sameera Khan ^[2]

Amity School of Engineering & Technology ^[1]

Assistant Professor ^[2], Amity School of Engineering & Technology

Amity University Chhattisgarh

India

ABSTRACT

Biometrics is a Technology that can carry out the identification and authentication according to the physiological or behavioral characteristics. The biometrics has the reliability, security, safety and so on. With such a vast development of computer technology and the needs of increasing information security, biometrics became more and more important. Firstly, the paper makes a brief overview presentation on various types of biometric identification technology; Secondly, biometric technology in information security in the application and development prospects are also analysed.

Keywords:- Biometrics, Face, Iris , personal authentication , automated speech recognition , palm print ,finger print.

I. INTRODUCTION

Traditional identity has two ways. One is owned by the user through the various items (such as keys, certificates, known as markers) to be certified, this authentication method, which we call identity-based markers. But this identity is neither safe, can't ensure each other's identity. The other is owned by the knowledge which the users have, such as passwords or card test, ID number, etc. certification. Such authentication is the earlier operations in the computer network to confirm the identity of the process and produce solutions. This authentication method, simply speaking, is for "According to the information you know to prove your identity"[3]. Static password means that is the user's password is set by the user. The user will not login the network until he or she enter the correct password. Smart card (IC card) is a built-in IC chip, the chip has the user-related data, smart card manufacturers by special equipment through a dedicated, hardware cannot be copied. Smart cards are carried by the legitimate users, login to the smart card into a dedicated reader to read the information, to verify the user's identity. Smart card data is static. SMS password is the form according to the request of the SMS contains six random dynamic password authentication system, it sends the messages to the customer's mobile phone. When the Customers login or trade certification in time to enter this dynamic password authentication to ensure system security. Dynamic passwordcard is the client handheld terminal which used to generate dynamic password, the mainstream is based on the time synchronization mode, every 60 seconds change a dynamic password, the password once effective, it produced six figures a dynamic way of a secret certification. USB Key is a USB interface, hardware device, built-in single chip or smart card chip that can store the user's key or digital certificate, use the built-in password algorithm USB Key user identity authentication. Electronic

digital signature, also known as encryption, can distinguish between real data, fake data, and the data had been tampered with [1] . However, these authentication methods have inconvenient, unsafe and unreliable and other defects. The marker system of identification, certificates, keys and other convenient marker carry, easy to lose and forgery, so the whole system security performance degradation, at the same time as documents, smart cards, or other markers USBKEY increase with frequency of use will cause varying degrees of wear and tear, which will affect the accuracy of identification, while the cost of replacement of more expensive markers. Also users may forget their password or account hackers stealing passwords and other information intentionally, and thus can affect the security of the system. To overcome these shortcomings, the biometrics rises along.

II. BIOMETRIC TECHNOLOGY

A. The brief introduction of Biometrics

Biometrics is the technical term refers to metrics related to human characteristics. Biometrics identification is used in computer science as a form of identification and access control method. It is also used to recognize individuals in groups that are under surveillance.

Biometric identifiers are the measurable, distinctive characteristics used to label and describe someone. Biometric authenticators are often categorized as physiological vs behavioural characteristics. Physiological characteristics are related to the body shape. Behavioural characteristics are related to the behaviour pattern of a person, including typing, rhythm, gait, and voice. Some researchers have coined the

term behaviometrics to describe the latter class of biometric technologies.

Error-Rates

False rejection rate (FRR) is one of the most important specifications in any biometric system. The FRR is defined as the percentage of identification instances in which false rejection occurs. It is also known as Type-I error

- **False acceptance rate (FAR)** is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts. It is also known as Type- II error.
- **Average Error Rate (AER)** is the average of type1 and type2.
- **Equal Error Rate (EER)** is the location on a ROC or Detection Error Trade-off curve where the FAR and FRR are equal. Smaller the value of EER, better is the performance of the system.

B. Steps in Biometric Authentication.

A Biometric verification basically uses some mechanism and database in which the few specimen. Steps involved in verification process –

- Gets specimens for the creation of database.
- Extract the various features of images stored in database.
- Use these features to educate and prepare the classifier.
- Get the unknown specimens and extract the features.
- Perform the matching with the specimens in the database.
- Do the classification to see whether match is found or not.

B. Some types of biometric technology

- Fingerprint Recognition

Fingerprint recognition refers to the method of identifying the identity of an individual based on the comparison of two fingerprints [3]. It is developed based on the fact that no two

individuals can have same finger prints [10]. Fingerprint identification is also known as dactyloscopy or also hand identification is the process of comparing two examples of friction ridge skin impression a from human fingers, palm or toes [2]. Fingerprints offer an infallible means of personal

identification. Other personal characteristics may change, but fingerprint can never mark differently unless your palm structure is burnt completely.

Fingerprint recognition is one of the most well-known biometrics, and it is by far the most used solution for authentication of any individual on computerized systems. The reasons for fingerprint identification being so popular are the ease of acquisition, established use and acceptance when compared to other technology of biometrics, and fact that there are numerous sources of this biometric on each individual.

Challenges: The recognition rate of finger print based biometric recognition system degrades greatly when the finger is wet and wrinkled [11].



- Palm Print Identification

Palm print recognition is a biometric identification method based on the unique patterns of various characteristics in the palms of individual's hands. Palm prints are counterparts to fingerprints recognition, including similar details.



As in the case with fingerprint scan, palm scanners use optical, thermal or tactile ways to bring out the details in the pattern of ridges and branches (called bifurcations) in an image of a human palm, along with other details including

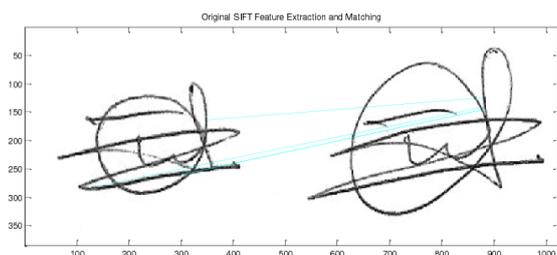
scars and creases [3]. Those three methods rely on visible light, heat-emission and pressure analysis respectively. Palm scanners may require that individuals touch their hands to a screen or it may have contactless authentication.

The first recorded application of handprint recognition was in 1858, when Sir William Herschel recorded the print of an Indian civil service employees working under him [5].

Challenges: research must be advanced to address the impact of wet and wrinkle palm on the recognition rate.

- Signature Recognition

Signature recognition is one of the authentication technique which used for various purposes in day to day life especially in banks, legal procedures, government formalities etc. Signatures are a behavioural biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories [6].



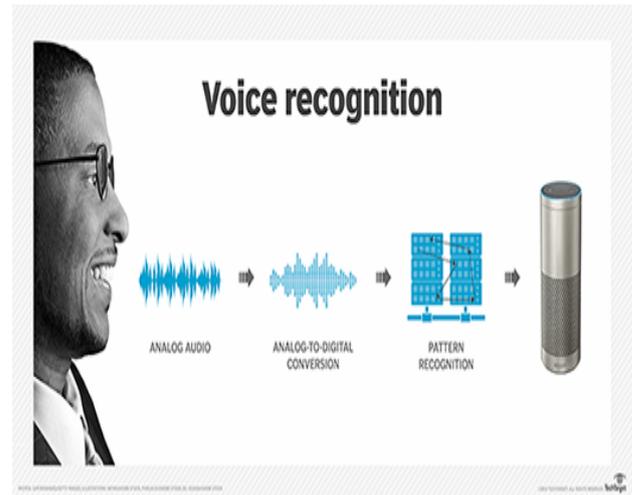
Challenges: Long term reliability, cost and lack of accuracy are the main issues to be addressed in this technology [11].

- Speech recognition

Speech recognition is also known as automatic speech recognition or computer speech recognition which means understanding voice of the computer and performing any required task or the ability to match a voice against a provided or acquired vocabulary [15].

These physiological characteristics of human speech are invariant for an individual, but the behavioural part of the speech of a person changes over time due to age, medical conditions (such as a common cold), and emotional state and so on [6].

Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel [6].



- Iris Recognition Technology

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of a human's eyes, whose complex patterns are unique and can be seen from some distance. It has been estimated that the probability that two irises would be identical by random chance is approximately 10 to the power (-35) [14].

Retinal scanning is a ocular-based biometric technology that uses the unique pattern on a human's retina blood vessels and is often confused with iris recognition process. Iris recognition uses video camera technology with subtle near IR illumination to acquire images of the detail-rich, intricate structures of the iris which are visible externally. Although John Daugman patented the first actual algorithms to perform iris recognition, published the first papers about it and gave the first live demonstration [7].

Challenges: The recognition rate degrades if eyes are covered by some occlusions like contact lens , water droplet etc [11].

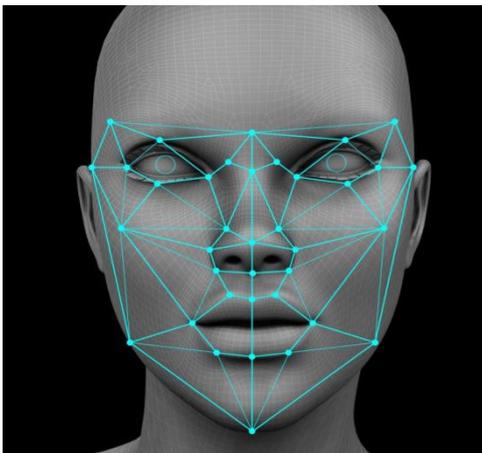


- Face Recognition Technology

Face recognition technology is based on people's facial features, the input face image or video stream. First of all, to determine whether it is the face, if face, each face is further given the location, size and various location information of the main facial organs. Based on this information, and further

extraction of each face implied in identity, and with the known face compared to identify each face's identity.

Regional Characteristics of the algorithm is face knowledge technology is widely used in an algorithm, which combines the computer image processing technology and bio-statistical theory in one, using computer image processing techniques to extract image features from the video point, the use of biometrics analysis of the principle of mathematical models that facial feature template. Uses of facial features have been built and tested template of those who study the characteristics of a face, according to results of the analysis to give a similar value.



The main function modules include: face capture and tracking capabilities; face recognition; human face modelling and retrieval; real man identification function; image quality testing.

Challenges: The presence of doppel-gangers, face rotation, illumination problem etc [11].

C. Other types of Biometric

There are also some other biometrics such as ear contour recognition, hand gesture recognition, human body temperature infrared spectra of recognition, like face recognition, retina recognition, gene identification, palm vein scanning and so on.

D. Literature Survey

In recent years, multimodal fusion has gained much attention of many researchers due to the benefit it provides for various multi biometric analysis tasks. Lots of research is done on biometrics in the past few years.

Asima Akber Abbasi, M.N.A. Khan and Sajid Ali Khan [17] In their work they have shown that the eye iris detection method of this implemented system of eye A biometric system is an automatic identification system based on a unique

template or feature matching. Biometric system is one of the methods that is used now a days as an useful authentication system. Iris recognition system is among the most reliable and unique biometric identification system. The approach in this paper is to create an authentication biometric system using iris recognition with parallel approach.

Sukhwinder Singh, Ajay Jatav [18] In their work they have shown eye iris Is Used In High Security Areas. Some Of The Applications Of Iris Recognition System Are Border Control In Airports And Harbours', Access Control In Laboratories And Factories, Identification For Automatic Teller Machines (Atms) And Restricted Access To Police Evidence Rooms. This Paper Provides A Review Of Major Iris Recognition Researches. Iris identification was considered one of the most robust ways to identify humans. It provides enough Degrees-of-Freedom for accurate and safe recognition. Iris is considered the most unique, data rich physical structure on the human body. It works even when people were sunglasses or contact lenses.

Essam-Eldean F. Elfakhrany, Ben Bella S. Tawfik [20] In their work they have shown eye iris Reliable and unique identification of people is a difficult problem; people typically use identification cards, usernames, or passwords to prove their identities, however passwords can be forgotten, and identification cards can be lost or stolen. Biometric methods, which identify people based on physical or behavioural characteristics, are of interest because people cannot forget or lose their physical characteristics in the way that they can lose passwords or identity cards. Biometric systems have been developed based on fingerprints, facial features, voice, hand geometry, handwriting, the retina, and the one presented in this work, the iris. Iris is difficult issue because of pre-processing and segmentation phases.

Senbhaga S [21] In their work they have shown eye iris presents a new iris segmentation framework which can robustly segment the iris images acquired using near infrared or visible illumination. The proposed approach exploits multiple higher order local pixel dependencies to robustly classify the eye region pixels into iris or non-iris regions. Face and eye detection modules have been incorporated in the unified framework to automatically provide the localized eye region from facial image for iris segmentation.

Mojtaba Najafi, Sedigheh Ghofrani [16] In their work they

have shown eye new feature extraction method according to ridge let transform for identifying the iris images is provided. At first, after segmentation and normalization the collarets area of iris images has been extracted. Then we improve the quality of image by using median filter, histogram equalization, and the two dimensional (2-D) Wiener filter as well. Finally, ridge let transform is employed for extracting features and then, the binary bit stream vector is generated.

D R Prithvi, R Madhu [19] D R Prithvi, R Madhu "Recognition Using Secret Key in Iris Feature Extraction and Palm Print Features" Proceedings of AECE-IRAJ International Conference, Tirupati, India, ISBN: 978-81-927147-9-0, 14th July 2013.] In their work they have shown methods are more reliable and capable than single knowledge-based techniques which are a uni-modal system. Due to its applications as well as features the theoretical challenges of multimodal biometric has drawn more and more attention in recent years. They show that integration of iris and palm print biometrics with secure key can achieve higher performance that which may not be possible using a single biometric indicator alone.

Savita Borole, Prof. S. D. Sapkal [22] A novel descriptor for iris recognition is proposed by using dual-tree complex wavelet feature and Support Vector Machine (SVM). SVM is used as a classifier and some kernel functions are tested in the experiment. In this they compared with the k-NN and Naïve Bayes classifier to demonstrate the efficiency of the proposed technique. The 2D DT-CWT is extracted from the iris images and train the support vector machine (SVM) as iris classifier

III. FUTURE SCOPE

As the biometric technology grows and expands, the various methods are also being developed in order to identify a person accurately. Trends have begun to emerge in the following important areas [13].

- Fingerprint and Palm print identification technologies together will be the main biometric in the foreseeable future that law enforcement depends on [12].
- Facial recognition will have increase intelligence and investigative use. However, law enforcement may not use facial recognition for evidence in the near future [12].
- Palm prints may be used with increased investigation in a few years.
- Multimodal biometrics, also called bio fuse, cataloguing is merging two or more biometrics together to achieve maximum accuracy of authentication.

- International cooperation is a major trend. As the cooperation is the backbone of law enforcement agencies, biometric data needs to be shared among them.
- Acquiring passive biometric data will also be the future trend of biometrics. Capturing and matching biometrics passively without human interaction is very exciting
- Progress on biometric Ear Recognition, DNA recognition, Body odour recognition and many more.

IV. CONCLUSION

The 21st century is information technology, network technology, the century is out of the traditional techniques of human bondage, more freedom's century. In order to information, freedom of the characteristics of century, the biometric authentication technology, as the late 20th century, began to flourish in high-tech, will occupy in social life more and more important position, and fundamentally change our way of life. At the same time, it can ensure the security of personal information as possible to prevent all types of criminal and economic crimes

REFERENCE

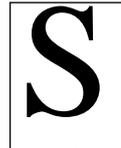
- [1] "Biometric Identity Management System". UNHCR. Retrieved 2015-11-02.
- [2] "Biometric System- A Review" .Abhilash Kumar Sharma¹, Ashish Raghuwanshi², Vijay Kumar Sharma³
- [3] "The Evolution of Biometrics" Panpan Li, Renjin Zhang.
- [4] Palm vein recognition using a high dynamic range approach Emanuela Piciucco, Emanuele Maiorana¹, Patrizio Campis
- [6] "An Introduction to Biometric Recognition". Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Salil Prabhakar, Member, IEEE.
- [7] Essam-Eldean F. Elfakhry, Ben Bella S. Tawfik, "IRIS" Recognition using Conventional Approach" IEEE 9th International Colloquium on Signal Processing and its Applications, 8 - 10 Mac, 2013.
- [8] Biometrics and Face Recognition Techniques, Renu Bhatia
- [9] A Review on Offline Signature Recognition and Verification Techniques, Sameera Khan, Avinash Dhole
- [10] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. (2003), Handbook of Fingerprint Recognition, New York: SpringerVerlag
- [11] Study on Biometric Authentication Systems, Challenges and Future Trends: A Review, Krishna Dharavath¹, F. A. Talukdar², R. H. Laskar

- [12] L. Hong, A. K. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Trans. Pattern Analysis Machine Intell.*, Vol. 20, pp. 1295-1307, December 1998
- [13] Massimo Tistarelli and Marks Nixon, "Advances In Biometrics", Springer-Verlag Berlin Heidelberg 2009, ISBN 03029743
- [14] P. W. Hallian "Recognizing human eyes" *Geometric methods computer vision*, vol. 1570, pp. 214-216, 1991.
- [15] Automatic Speech Recognition: A Review Preeti Saini, Parneet Kaur
- [16] Mojtaba Najafi and Sedigheh Ghofrani "A New Iris Identification Method Based on Ridge let Transform" *International Journal of Computer Theory and Engineering*, Vol. 5, No. 4, August 2013.
- [17] Sukhwinder Singh, Ajay Jatav "A closure looks to Iris Recognition system" *IOSR Journal of Engineering (IOSRJEN)* eISSN: 2250-3021, p-ISSN: 2278-8719 Vol. 3, Issue 3 (Mar. 2013).
- [18] Asima Akber Abbasi, M.N.A. Khan and Sajid Ali Khan "A Critical Survey of Iris Based Recognition Systems" *Middle-East Journal of Scientific Research* 15 (5): 663-668, 2013.
- [19] D R Prithvi, R Madhu "Recognition Using Secret Key in Iris Feature Extraction and Palm Print Features" *Proceedings of AECE-IRAJ International Conference, Tirupati, India*, ISBN: 978-81-927147-9-0, 14th July 2013.
- [20] Essam-Eldean F. Elfakhrany, Ben Bella S. Tawfik, "IRIS Recognition using Conventional Approach" *IEEE 9th International Colloquium on Signal Processing and its Applications*, 8 - 10 Mac, 2013.
- [21] Senbhaga S "A Survey on Iris Segmentation using Distantly Acquired Face Images" *International Journal of Scientific & Engineering Research*, Volume 4, Issue 5, May-2013 118 ISSN 2229-5518.
- [22] Savita Borole, Prof. S. D. Sapkal "Extraction of Dual Tree Complex Wavelet Feature for IRIS Recognition" *International Journal of Advanced Research in Computer and Communication Engineering* Volume 2, Issue 7, July 2013
- [23] Sameera Khan, Megha Mishra, and Vishnu Kumar Tiwari. "Effect and Uses of Synthetic Data Generation in Inverse Biometric Problem." 2018 *International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*. IEEE, 2018.
- [24] Sameera Khan, Avinash Dhole, A Review on Offline Signature Recognition and Verification Techniques,

International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 6, June 2014

- [25] Sameera Khan, Avinash Dhole, An Offline Signature Recognition And Verification System Based On Neural Network, *IJRET: International Journal of Research in Engineering and Technology*, Volume: 03 Issue: 11 | Nov-2014

BIOGRAPHIES



Saurav Biswas is a student of B.TECH CSE in Amity School of Engineering & Technology, Amity University Chhattisgarh. He has research interest in soft computing technologies and biometric technology.



Sameera Khan is an Assistant Professor in the Amity school of Engineering & Technology, Amity University Chhattisgarh, Raipur. She is pursuing PhD from Chhattisgarh Swami Vivekanand Technical University. She received her Master OF Technology (CSE) from the same University and Bachelor of Engineering (CSE) in 2008 from Raipur Institute of Technology, Raipur affiliated to Pt. Ravishankar University, Raipur (C.G). Her research interest are Digital Image Processing, Biometric Technology, Artificial neural network and cognitive science.