A Survey of Automated Biometric Authentication Techniques

Keerti Arse[1]
[1]Department of Computer & Science Engineering
[1]Saveetha School of Engineering Saveetha University

Abstract— Biometric identification refers to the automatic identification of a person by analyzing their physiological or behavioral characteristics. Since many physiological and behavioral characteristics are unique to an individual, biometrics provides a more dependable system of authentication than ID cards, keys, passwords, or other standard systems. A wide range of organizations are using automated person authentication systems to improve customer fulfillment, operating efficiency as well as to secure difficult resources. Now a day an increasing number of countries including India have decided to adopt biometric systems for national security and identity evil prevention, which makes biometrics an important component in security-related applications such as logical and physical access control, forensic investigation, IT sector, identity crooked protection, and terrorist prevention. Various biometric authentication techniques are available for identifying an individual by measuring fingerprint, hand, face, signature, voice or a combination of these traits. New biometric algorithms and technologies are proposed and implemented every year. This paper aims to give a brief overview of the field of biometrics and summarize various biometric identification techniques including its strengths and week.

Key words: Biometric Authentication, Fingerprint, Palm Print

I. INTRODUCTION

Authentication is mainly based on that (e.g. finger prints, iris, face) or that you can produce (e.g. handwriting or voice).Most common authentication system are smart card and password, pin. This technology must also have some disadvantages unsolved problem or may be some security concern. Mainly a pattern reorganization system which identify the person by identifying the authenticity of particular physiological characteristics that have a person. Physiological features are related to shape of body

Like hand geometry, palm print, DNA, iris reorganization, retina etc. A biometric authentication system is print, face recognition, fingerprint, DNA, iris recognition, retina and odor. Behavioural characteristics are related to the behaviour of a person, such as typing rhythm, gait, and voice. Seven such factors to be used when assessing the suitability of any trait for use in biometric authentication: Universality, Uniqueness, Permanence, Measurability, Performance, Acceptability and circumvention.

II. BIOMETRIC AUTHENTICATION SYSTEM

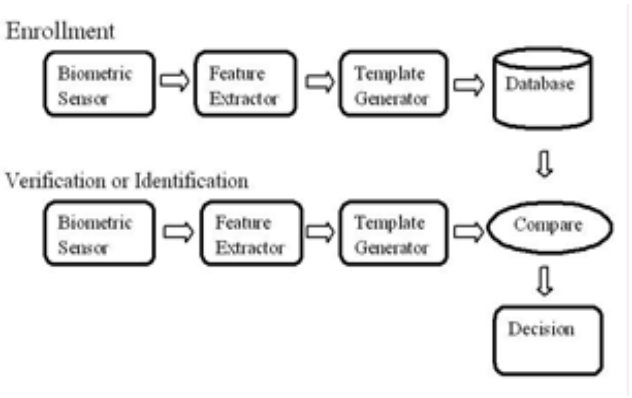

Fig. 1: Biometric Authentication System

The study of biometric explores ways to distinguish between individuals using physical characteristics and person traits .the most common physical characteristics explore and used are facial features, eyes (iris and retina), finger prints, and hand geometry. Hand writing and voice are examples of personal traits which could we used to distinguish between individual ls. Finger prints and face reorganization are the two most common used characteristics to distinguish between individual.

An important distinction between biometric verification and identification lies in that verification is a one-to-one comparison, while identification is a one -to-many searches in a database. They perform different functions since verification is used to confirm one's identity and identification is used to find one's identity.

III. OVERVIEW OF BIOMETRIC AUTHENTICATION TECHNIQUES

There are number of physiological and behavioural characteristics are used in automated biometric authentication system. Each biometric characteristic has its own strengths and weaknesses, and the choice depends on the application. No single biometric characteristic is expected to effectively meet the requirements of all the applications.

A. Fingerprint:

It is known since a long time that finger prints of human

Is unique, they can be distinguish by the epidermal ridge and furrow structure of each finger which is used to categorized finger prints. . Fingerprints of identical twins are different and also the prints on each finger of the same person. For electronically processing finger prints using image recognition algorithm, a finger print has to be scanned first. There exists different finger print scanner e.g. capacitive, optical and thermal, each using different technology. Most fingerprint matching systems are based on four types of fingerprint representation schemes: grayscale image, phase image, skeleton image and minutiae. Due to its distinctiveness, compactness, and compatibility with

features used by human fingerprint experts, minutiae-based representation has become the most widely adopted fingerprint representation scheme.

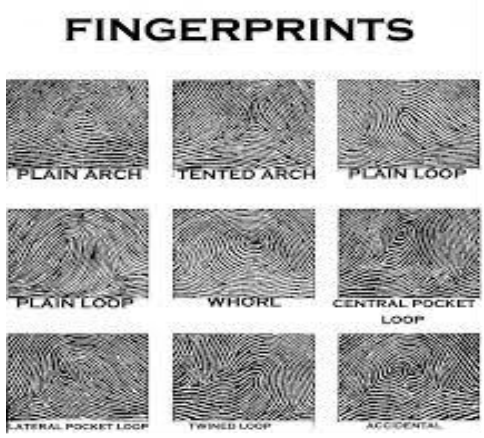

Fig. 2: Finger prints

B. Palm Print:

A palm print refers to an image acquire of the palm region of hand. Like fingerprints, palms of the human hands have unique pattern of ridges and valleys. . Human palms also contain additional distinctive features such as principal line and wrinkles. And epidermal ridges its differ to a fingerprints .in that it also contain other information such as texture ,marks which can be used when comparing one palm to another palm .and it can be

Used for criminal, forensic or commercial application.

C. Hand Geometry:

Hand geometry is a biometric technique, which identifies person through hand instrument .some geometry structure related to a human hand (e.g. length and width of hand) are related invariant to individual. and the main advantages of hand geometry is acquisition convenience and good verification and suitable for medium and low security application. the hand based biometric system can be employed in those application which do not require extreme security but where robustness and low cost are primary issue. Hand geometry based identification systems utilize the geometric features of the hand like length and width of the fingers, diameter of the palm. Since hand geometry is not very distinctive it cannot be used for determination of an individual from a large population, but it can be used in a verification mode. Further, hand geometry information may not be invariant during the growth period of children.

D. Iris:

Iris is the best authentication process available today .it is generally conceded that iris recognition is the most accurate coupling this high confidence authentication with factors like outlier group size, speed. the iris extremely visible colored ring around pupil of every size is absolutely unique. iris is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupil and thus the amount of light reaching the retina. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. The main advantages of this are the smallest outlier population of all biometrics and iris pattern and structure exhibit long Term.

Fig. 3: Iris

E. Face:

Some facial recognition software algorithm identifies the face by extracting features from an image of a subjective face. face recognition capture information about the shape of face .this information is then used to identify distinctive features on the face such as counter of eye sockets , nose and chin .it uses to visualize details of the skin as captured in standard digital or scanned images. this technique is called skin texture analysis turns the unique lines, pattern and spot apparent in a person skin to a mathematical space. Hum Face Recognition algorithms can be divided into two main approaches, geometric, which looks at distinguishing features(the location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships), or photometric. This technique uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin. Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. This technique, called skin texture analysis, turns the unique lines, patterns, and spots apparent in a person's skin into a mathematical space.

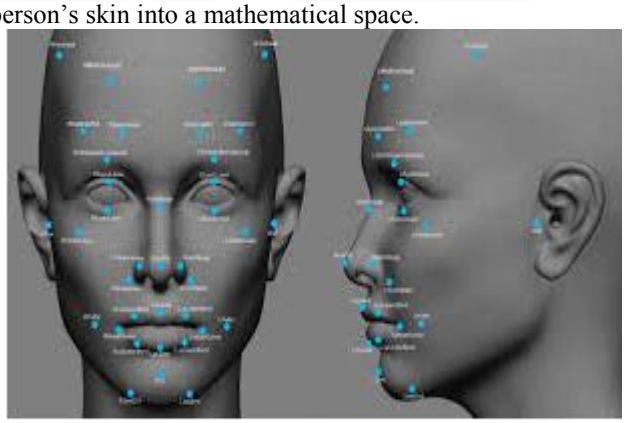

Fig. 4: Face

F. Ear:

Researchers have suggested that the shape and appearance of the human ear is unique to each individual and relatively little change occurs during the lifetime of an adult. The ear recognition approaches are based on matching the distance of salient points on the pine from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.

Fig. 5: Ear

G. DNA:

Humans have 23 pairs of chromosomes containing their DNA blueprint. One member of each chromosome pairs comes from their mother and other chromosomes from their father. Every cells in a human body contain a copies of this DNA, the large majority of DNA does not differ from person to person. the main benefit of DNA recognition is accuracy and the disadvantages is DNA matching is not done in real time. Deoxyribonucleic acid (DNA) is a molecule that takes the genetic instructions used in the development and functioning of all known living organisms and many viruses. DNA testing is a technique with a very high degree of accuracy. It is the most distinct biometric identifier available for human beings except for monozygotic twins. DNA does not change throughout a person's life; therefore its permanence is incontestable. The recent process is done by obtaining DNA samples are quite intrusive, requiring some form of tissue, blood or other bodily sample. Forensic scientists use DNA in blood, semen, skin, saliva or hair found at a crime scene to identify a matching DNA of an individual. In DNA profiling, the lengths of variable sections of repetitive DNA, such as short tandem repeats and mini satellites, are compared between people.

Fig. 6: DNA

IV. INDIA'S UNIVERSAL IDENTIFICATION PROGRAMME

India is currently implementing its Universal Identification (UID) program to provide a unique identification number based on biometric identifiers to each of its 1.25 billion citizens. The government will then use the information to issue identity cards the word which is popularly known as *Andhra Card*. The physical count began on February 2011. The Universal ID program is administered by the Unique Identification Authority of India (UIDAI). Although it is in early stages, the UID program is already the largest biometric identification program in the world with more than 200 million people enrolled as of January 2012[19].

V. CONCLUSION

In this age of digital impersonation, biometric techniques are being used increasingly as a hedge against identity theft. The premise is that a measurable physiological or behavioral characteristic is a more reliable indicator of identity than legacy systems such as passwords and PINs. The principal objective of this paper is to give an overview of the fast developing and exciting area of automated biometrics. Various biometric authentication techniques are presented that are either currently in use across a range of environments or still in limited use or under development or still in the research realm.

REFERENCES

[1] Jain, A.K.; Bolle, R.; Pankanti, S., eds. (1999). Biometrics: Personal Identification in Networked Society. Kluwer Academic Publications. ISBN 978-0-7923-8345-1.
[2] James Wayman, Anil Jain, Davide Maltoni and Dario Maio, "An Introduction to Biometric Authentication Systems". In Biometrics: Technology, Design and performance evaluation. Springer Publications. ISBN 978-0-7923-8345-1
[3] Qinghan Xiao. Biometrics—Technology, Application, Challenge and Computational Intelligence Solutions, May 2007 | Ieee Computational Intelligence Magazine.
[4] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004.
[5] Naser Zaeri, Minutiae-based Fingerprint Extraction and Recognition, Biometrics, Edited by Jucheng Yang, ISBN 978-953-307-618-8.
[6] D. Zhang and W. Shu, "Two novel characteristic in palmprint verification: Datum point invariance and line feature matching," Pattern Recognit., vol. 32, no. 4, pp. 691–702, 1999.
[7] Kresimir Delac, Mislav Grgic, "a survey of biometric recognition methods", 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June 2004, Zadar, Croatia.
[8] Williams, Mark. "Better Face-Recognition Software". Retrieved 2008-06-02.
[9] Bonsor, K. "How Facial Recognition Systems Work". Retrieved 2008-06-02.
[10] A. Iannarelli. Ear Identification. Paramont Publishing Company, 1989.

