ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 6, June 2019

A Study on Various Biometric Techniques

[1] Siji Joju, [2] Aswin Kumar P.M, [3]Akhil Chandran.N, [4]Nibin Sasidharan
[1][2][3][4] Mtech CSE Students

Abstract: This papers discusses and gives a brief overview of the popular physical and behavioral biometric techniques used in identification and recognition of users to create secure systems. Biometrics gains significant importance in this technical world and it means analysis of biological data. It is defined as the technology of analyzing individual person based on physiological, behavioral or morphological traits such as face, fingerprint, iris, retina, voice, and signature etc,. It is possible to establish one's identity with the help of biometric techniques. Today biometric have been successfully deployed in various fields like forensic science, security, identification and authorization system. For the last three decades, lot of research work has to be carried out for the growth of biometric system based on fingerprint, voice, iris, face, etc, but recently new biometrics has been come up. To provide a comprehensive survey, this paper presents an overview to various biometric systems, their applications, limitations and the different type of biometrics recognition systems.

Index Terms— Biometric Techniques, Face recognition, Identification.

1. INTRODUCTION

The question of "how to identify a Human by a machine" has always intrigued researchers until it was found that it may do by expoiting the unique biological trait of a human being. For this reason most security systems try to identify a person by his unique biological traits which cannot be copied. Using Biometric passwords overcomes this problem since it uses the unique biological trait of a particular user that cannot be copied or stolen or replicated. The human face itself can serve as an unique biometric key, apart from that, the eye, iris, fingerprint, hand geometry , voice, DNA, retina are among the few other examples of objects that have been found useful to serve as the biometric key, because of their uniqueness from person to person.

II. BIOMETRIC TECHNIQUES

1. Fingerprint Recognition:

Fingerprint recognition is a process that tires to find a match between fingerprints of users from its existing database. There are three basic fingerprint ridge patterns of the arch, loop, and the cycle:

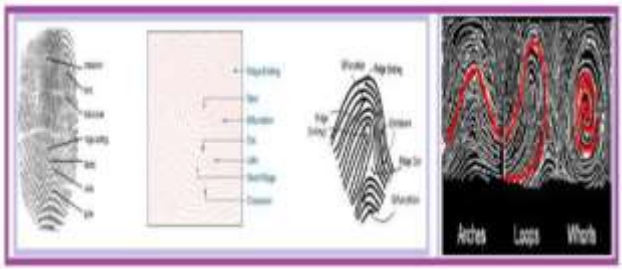
i. Arch: The ridges enter from one side of the finger, rise in the centre forming an arc, and then exit the other side of the finger.

ii. Loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side.

iii. Whorl: Ridges form circularly around a central point on the finger.

The main features of the fingerprint ridge of minutia.

Minutia: ridge end, bifurcation, and a short ridge (or dot). At the end of the ridge, which is close to a ridge? Bifurcations are points at which only the ridge of a ridge between the two splits. A small ridge (or dot) is significantly shorter than the length of the ridge that the average fingerprint ridge top. And a small part of the analysis of patterns of fingerprints is very important, since no two fingers have been shown to synchronize. Adjust the algorithm to authenticate the applicant's Fingerprints are used to compare the fingerprints of previously stored template. Be directly compared with the original image so that it is a candidate image or certain features must be compared A model - based algorithms in, template type, size, and orientation patterns are aligned in the fingerprint image. Candidate fingerprint image template and the degree to which they are graphically compared with a matched set.



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 6, June 2019

2. Iris Recognition:

Iris recognition is a biometric identification system that uses the eyes of a person, which is unique, complex and has random patterns can be seen from some distance to the video images of the irises mathematical pattern - Recognition technology used. Do not be confused with other, less common, visual – based technology, retina scan, iris recognition technology; the camera is sensitive to infrared illumination with a rich, complicated structure of the iris in the image. Matching the speed and ultimate prevention of false matches in addition to the benefits of an iris recognition, an internal, protected, as part of the eye is still visible on the outside of the iris stability. Black iris biometric identification for the human body model has been described as part of the reason:

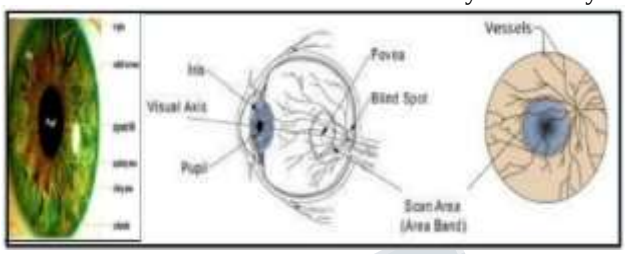
A. This is an internal organ that is a very transparent and sensitive membrane (cornea) is better protected against damage and wear

B. Iris is mostly flat, and the geometric configuration of the two complementary muscles (sphincter papillae and dilator papillae) is controlled only by controlling the diameter of the pupil. It is much more predictable than the bow shape, for example, that face. Similar to a photograph of an iris scan, and about 10 cm to a few meters away from the place can be.

The comparison of two iris code can be computed by the hamming distance based on the difference in the number of bits and it is very fast. Also the template matching technique can be used and it uses the statistical calculation to match the stored iris template and the obtained iris template. The iris recognition is applied in the following areas: border control, passports and Identity cards and other government purposes, database access, login authentication, aviation security, hospital security, controlling access to restricted buildings, areas, homes and prison security.

3. Retina Biometrics:

The Retinal scan biometric is based on the distinctive patterns on a person's retina, which is significantly different from the iris recognition. It is older than the Iris scanning which also uses the part of the eye. There is a unique pattern called the blood vessels at the rear side of the eye, which covers the 65% of the inner surface of the eyeball. The retina is a thin tissue which is made up of neural cells and situated as the innermost layer of the eye.



Even identical twins have distinct patterns of retina and it is stable throughout the life. It is impossible to fake the retina and it decays so quickly after the death and can be accessed only from a living person. The retina templates are typically 40 to 96 bytes. It has an error rate of 1 in 10,000,000 . The Enrollment and scanning of retina are intrusive and slow. Retina biometrics is used in Government, military and banking.

4. Face Recognition:

This process tries to automatically detect and match a face from a digital image or a video frame from a video source with the existing databases. The facial image database is compared with the facial features. It is commonly used in security systems, fingerprint or eye iris recognition systems, and these can be compared to other Biometrics. These features are then used to search for other images with features for matching.

Face recognition is an emerging subject which gets dynamic and constant improvement. Face Recognition has attracted the Researchers in the field of Security, Psychology, Optics, Neural Networks, Machine learning, Image Processing, Computer Vision and Pattern Recognition. It has expanded not by Engineers but also by Neuroscientists and the most important application is Image Analysis and Understanding.

ISSN (Online) 2394-2320

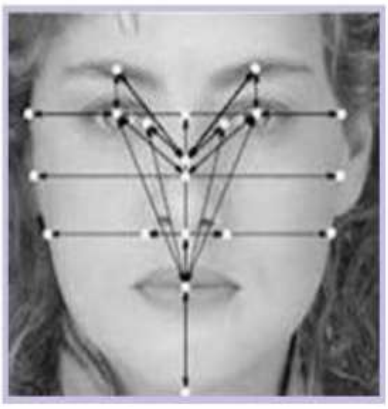
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 6, June 2019

Face recognition is a non-intrusive and popular method. The dimensions, ratio and other physiological attributes of the face form the basis for the Face recognition. Based on the size, location and the shape of the facial traits such as nose, lips, eyes, chin, jaw and their spatial relationships the humans recognize and distinguish faces. Researchers use both specific and general features for facial recognition. Face recognition can be carried out in the following ways .

i. Facial metric: The location and shape of facial attributes are measured. For example, distance between nose to lip or pupil to chin

ii. Eigen faces: The overall face image is analyzed i.e., collection of weights describing the canonical faces.

iii. Skin texture analysis: Technique of face recognition along with other visual details of skin. Finding the location of the unique spots, lines and patterns in a person's skin.



5. Voice Biometrics / Speaker Recognition Biometrics

Today, the voice recognition biometrics is most significant research area. Voice biometrics also known as speaker recognition biometrics. It is shown in the figure 19. They are used for the applications based on telephone. Almost, human voice features are distinct for every individual as well as for twins also and voice could be replicated perfectly The voice recognition relies on how the person speaks and the focus is on the speech produced by the vocal features not on the pronunciation or the sound. There is no need of any extra special and costlier hardware. The acoustic pattern traits of the speech are used by voice recognition to differentiate the individuals and these patterns consists of both behavioural patterns (speaking style, voice pitch) and physical (shape and size of the throat and mouth) . The vocal tract is not affected even by cold and so there will be no adverse impact on the accuracy.

6. Hand Geometry Biometrics

Hand geometry is a biometric method that identifies users by the shape of their hands. Hand geometry readers to a user's hand along many dimensions, and measurement criteria to compare the size of a file to be saved. Sustainable hand geometry device the early 1980s, after you have finished creating the first biometric hand geometry has been used to broad-teller machines. In the field of biometrics, the Researchers found that human hand, particularly human palm, has some features that may be used for personal authentication. These features include the density of the palm, width and length of the fingers, etc. and these measurements are not unique. The shape of the hand becomes stable in the later stage of life. Only the features of hand are not sufficient for authentication.

7. Signature Verification:

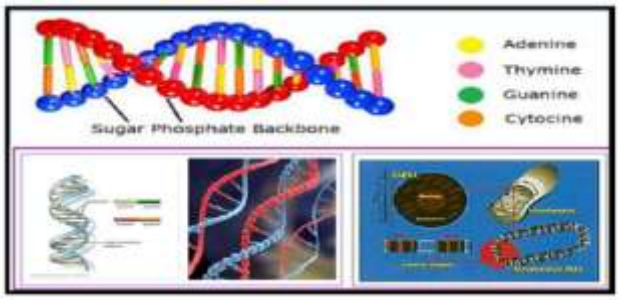
Handwriting recognition and the ability to get a computer, such as paper documents, photographs, touch-screens and other devices, such as the sources from which intelligible handwritten input. Text of a paper image of an optical scanning (optical character recognition) or intelligent word recognition by a fragment from the "off line" sensed it. Otherwise, the pen tip to the "line" sensed to be a pen - based on the computer screen. Off-line handwriting recognition to write a letter code that computers and automated text processing application to convert the image is usable. Off-line handwriting recognition more difficult, as different people have different handwriting styles. Automatic online handwriting recognition to convert the text as it is involved in a special digitizer or PDA, where a sensor break-up on the cutting edge of switching pen-up/pen-down as it is written.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 6, June 2019

8. DNA Biometrics:

A DNA-binding domain (DBD), a motif that is independently folded protein domain that is at least one double or single stranded DNA is recognized. DNA binding domain of one or more additional domains is often part of a larger protein, consisting of various actions. DNA with the DNA binding domain and copy function due to the structure, repair, storage, and the DNA methylation status of the change, biological role.

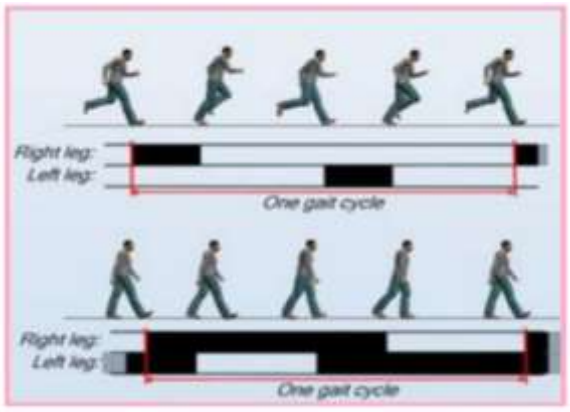


The control of gene expression of involved in DNA binding domain contains. Most of the cellular signaling cascades, as described in the final output of gene regulation.

Major or minor groove of DNA by DBD DNA recognition, may occur during or sugar – phosphate backbone DNA can. DNA recognition by proteins specific to each type of function is like.

9. Gait Biometrics:

Gait analysis, to assess if, and to walk in their ability to affect people with medical conditions are used. This is usually in sports biomechanics from the athlete to perform more efficiently and with the posture-related or movement-related problems used to help identify. Survey quantification, i.e. the measurable parameters of gaits and the introduction of the analysis, as well as an explanation encompasses, i.e. different conclusions about its gates to the animal (health, age, size, weight, speed, etc.) drawing.



10. Ear Recognition:

Human ear can be used to recognize a person. The biological pattern and structure of an ear of a human vary from person to person. The ear of every person has a unique pattern and structure. By this pattern a person can be identified. This pattern is unique biological trait of every human. The researchers use this biological uniqueness to identify a person uniquely. The technology may use a secondary identification and recognition system. The shape of the ear is used to perform identification by the Ear geometry recognition. It is recommended that the characteristics and the shapes of the human ear are generally distinct

III. COMPARISON OF BIOMETRICS

The comparison of the different biometric methods by considering the various factors. The biometric features of face, voice, fingerprint, iris, hand geometry, retina, keystroke, gait, signature and DNA have the characteristics like Universality, Uniqueness, Permanence, Performance, Collectability or Measurability, Acceptability and Circumference. These characteristics are distinct for each biometric type. These can be measured in High, Medium and Low denoted by H, M, and L, respectively. Any human physiological or behavioural features can serve as a biometric

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 6, June 2019

characteristic as long as it satisfies these requirements. Table 8 compares the biometric features based on different factors.

IV. DISCUSSIONS

Biometric authentication becomes highly promising since human physical characteristics are much more difficult to forge. The security code, passwords, hardware keys, smart card, magnetic stripe card, ID cards, physical keys can be lost, stolen, duplicated or left at home. Passwords can be forgotten, shared or observed and people have to remember a multitude of passwords like ATM PIN, mail password etc.

For variety of application biometrics authentication is fast, easy, accuracy, reliable and less expensive. Nowadays, biometrics uses non-invasive methods for identification of individuals. Image acquisition, pre-processing, feature extraction and template storing in the system database are the stages involved in the processing of biometric system. The comparison of the input query image features and stored features are done for authentication during verification.

The noisy sensor data, spoof attacks, interclass similarity and intra-class variations are the limitations. To increase the performance accuracy and to design a biometric system or to propose a new approach to the existing system, one has to understand the basic biometric system, its parameters, limitations, biometric scenario, biometric characters used for an application, types of errors and existing approaches. Any biometric system is not an optimal system. Always there is a need for improving the accuracy and performance of the biometric system.

IV. CONCLUSION

This paper briefly reviews the present's notions and ideas associated with the biometric techniques for recognition of users of system. Biometric systems for today's high security applications must meet stringent performance requirements. The fusion of multiple biometrics helps to minimize the system error rates. Fusion methods include processing biometric modalities sequentially until an acceptable match is obtained. More sophisticated methods combine scores from separate classifiers for each modality.

REFERENCES

[1] K. Karu, A.K. Jain, Fingerprint classification, Pattern Recognition 29 (3) (1996) 389–404

[2] A. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," IEEE Trans. Pattern Anal. Machine Intell, vol. 19, pp 302–314, 1997. X. Jiang, W. Y. Yau, "Fingerprint minutiae matching based on the local and global structures", ICPR2000, vol. 2, 2000, pp 1042-1045.

[3] Xuejun Tan, Bir Bhanu, "Fingerprint matching by genetic algorithms", Pattern Recognition, vol. 39, 2006, pp. 465 – 477.

[4] W. Zhao, R. Chellappa, A. Rosenfeld, P.J. Phillips, Face Recognition: A Literature Survey, ACM Computing Surveys, 2003, pp. 399-458

[5] John Daugman, How Iris Recognition Works, IEEE Transactions on circuits and systems for video technology, vol. 14, no. 1, january 2004, pp 21 – 30