IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Review on Biometric Authentication Methods

Mr. Mule Sandip S.[1], Mr.H.B.Mali[2]

Student, ENTC Department, SITS Narhe, Pune, India[1]

Asst.Prof. ENTC Department, SITS Narhe, Pune, India[2]

Abstract: There have been several studies on the different kinds of biometrics authentication systems which uses person's physiological and behavioral characteristics. So authentication serves first step towards security concern. Biometric have widely used over existing methods due their significant response for secure identification. Biometrics is the preventive solution for unauthorized access due to traditional password or smartcard based authentications. Biometric uses fingerprint, eye patterns (IRIS recognition), hand geometric, facial expression, voice recognition, and signature analysis etc. With the use of unique characteristics of person; various biometrics authentication devices have been developed and in use. Various software/hardware companies are developing such authentication for better security of sensitive, confidential information's here the paper proposes the brief review on different biometric person identification methods.

Keywords: Authentication, Biometrics, password, smartcards, IRIS.

I. INTRODUCTION

Biometric Authentication is any process that validates the identity of a user who wishes to sign into a system by measuring some intrinsic characteristic of that user. The traditional methods involving passwords and PIN numbers do not require the candidate to be present there at the time of authentication, while biometrics techniques does not require password ,PIN numbers or any RFID cards. It prevents fraud usage of ATMs, mobiles, PCs, smart cards etc. The characteristics are measurable and unique. Identity verification occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the verification biometric data obtained from the user is compared to the user's data already stored in the database. Identification (also called search) identification occurs when the identity of the user is a priori unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all. In biometric-based authentication, a legitimate user does not need to remember or carry anything and it is known to be more reliable than traditional authentication schemes. Biometric authentication offers a convenient, accurate, irreplaceable and high secure alternative for an individual, which makes it has advantages over traditional cryptography-based authentication schemes [1].

There are basically two kinds of biometric systems:

1. Automated identification systems operated by professionals (e.g., police Automated Fingerprint Identification Systems – AFIS). The purpose of such systems is to identify an individual in question or to find an offender of a crime according to trails left at the crime scene. Enrolled users do not typically have any access to such systems and operators of such systems do not have many reasons to cheat.

2. Biometric authentication systems used for access control. These systems are used by ordinary users to gain a privilege or an access right. Securing such a system is a much more complicated task.

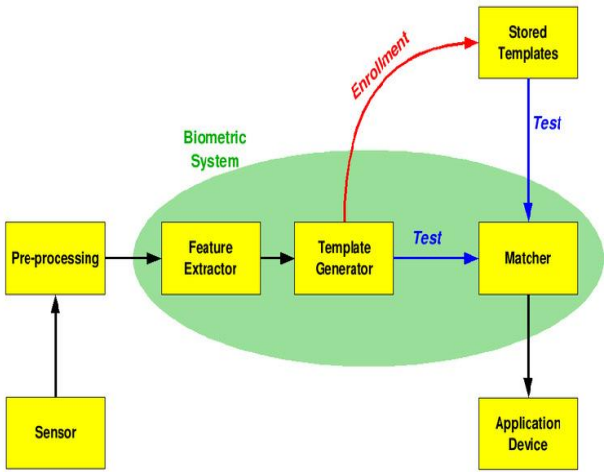

Fig.1.The model of Biometric System

Figure 1 gives the basic model of biometrics system [11]. Typical biometric system comprises of sensor like transducer to convert data to digital form. Biological templates have generated through digital image processing algorithms. Then with the use of database these templates are compared with other saved templates; these are performed by matching algorithms .Finally decision process will determine the correct authentication.

The purpose of this paper is to give a look at the use of biometrics technology to determine how secure it might be in authenticating users, and how the users job function or role would impact the authentication. The advantages of biometric authentication definitely look very attractive, there are also many problems with biometric authentication that one should be aware of. We will be exploring many of the technologies and applications that make up the field of "biometric authentication" – what unites them and what differentiates them from each other.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

II. LITERATURE REVIEW

Normally Identification or authentication can be implemented by following methods as shown in figure 2.

1. Token can be produced from a multitude of different physical objects. Human intervention requires for identification process for manual based tokens such as paper passport and identity cards. Automated tokens do not require human intervention in the identification process; the identity is verified by a system/computer such as magnetic-stripe cards, memory cards, or smart cards.

2. By means of passwords, PIN numbers sometimes authentication have processed.

3. Biological physical or behavioural characteristics such as IRIS, Finger-paint, Palm vain, LIP motion, audio and signature analysis based authentication have been developed now days.

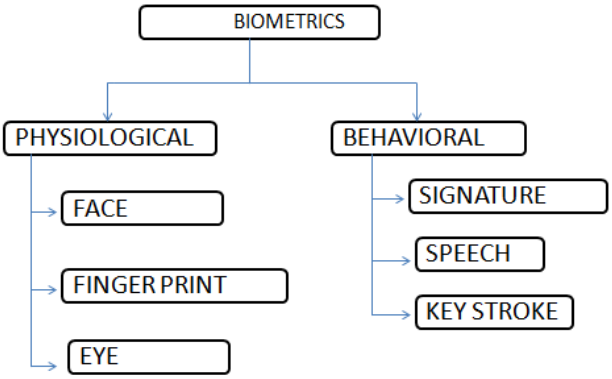

Fig.2.Classification of biometrics

Having identified the required qualities and measures for each quality, it would seem a straightforward problem to simply run some experiments, determine the measures, and set a weighting value for the importance of each, thereby determining the "best" biometric characteristic.

Different biometrics authentication methods have reviewed as follows:

A. *Fingerprints Identification*

This is the oldest biometric authentication approach. It analyzes finger characteristics. The first is by scanning optically the finger. The other method is by using electrical charges that determines which parts of the finger are directly in contact with the sensor. Each fingerprint has some characteristics, such as curves, bifurcations, deltas. One set of these characteristics is unique for each person.

Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques find the minutiae points first and then map their relative placement on the finger. Minutiae are individual unique characteristics within the fingerprint pattern such as ridge endings, bifurcations, divergences, dots or islands. In the recent years automated fingerprint comparisons have been most often based on minutiae. The problem with minutiae is that it is difficult to extract the minutiae points accurately when the fingerprint is of low quality. This method also does not take into account the global pattern of ridges and furrows. The correlation-based method is able to *correlation* overcome some of the difficulties of the minutiae-based approach. *Based* However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.

B. *Eyes feature recognition*

There are two methods using the eyes characteristics for authentication.

The first is based on the retinal recognition. The user has to look in a device that performs a laser-scanning of his retina. The device analyzes the blood vessels configuration of the acquired retinal picture. This blood vessels configuration is unique for each eye. The device is not friendly, because you have to fix a point while a laser is analyzing your eye.

The second method is based on the iris recognition. The scan is done by a camera. Unlike the retinal method, you don't need to be close to the device to be authenticated. The acquired picture is analyzed by the device, and contains 266 different spots. Moreover iris is stable through the whole life. The 266 spots are based on characteristics of the iris, such as furrows and rings [9]. The iris patterns are obtained through a video-based image acquisition system. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes.

The main drawback of the retina scan is its intrusiveness. The method of obtaining a retina scan is personally invasive. A laser light must be directed through the cornea of the eye. Also the operation of the retina scanner is not easy.

C. *Face recognition*

A simple camera or a web cam with good resolution use in face recognition, after capturing face image the device computes a digital representation based on some features of the face. The representation is compared with one which is stored in a database, and if there is a match, the user is authenticated. It is easy to implement and cheap authentication method with unique recognition.

Facial recognition in visible light typically models key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. The accuracy of the face recognition systems improves with time, but it has not been very satisfying so far.

D. *Voice recognition*

The user speaks in a microphone, and voice is recorded and computed. It is done by using some frequency analysis of the voice. It can be useful to authenticate someone through a telephone, and it allows users to work on a remote location. It is less accurate than other biometrics authentication methods, and some errors can occur [9].

DOI 10.17148/IJARCCE.2015.41157

Speaker verification focuses on the vocal characteristics that produce speech and not on the sound or the pronunciation of the speech itself. The vocal characteristics depend on the dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanisms of the human body.

The system typically asks the user to pronounce a phrase during the enrollment; the voice is then processed and stored in a template (voiceprint). Later the system asks for the same phrase and compares the voiceprints. Currently there are three major international projects in the field of voice technology: PICASSO, CASCADE and Cost 250.

E. *Signature analysis*

The signature analysis is a biometrical authentication solution. The device is a tactile screen. The parameters that are computed for the authentication are the shape of the signature, the time taken to do it, the stroke order and the pen pressure. With the computation of these parameters, the system provides to you a unique authentication method. It is virtually impossible to reproduce in the same way somebody else's signature. It is easy to implement and quite cheap.

This technology uses the dynamic analysis of a signature to authenticate a person. The technology is based on measuring speed, pressure and angle used by the person when a signature is produced. One focus for this technology has been e-business applications. The accuracy of the signature dynamics biometric systems is not high; the crossover rate published by manufacturers is around 2%.

F. *Handprints recognition*

This method is based on the recognition of the handprints. The device is a scanner that extracts a picture of a user's hand. Some characteristics like length of the fingers, distance between them or their relative position are computed. These characteristics are compared with the saved database and result will be displayed [1]. This method is not much complex as compared with IRIS or signature analysis type methods.

These methods are most commonly based either on mechanical or optical principle. Optical hand geometry scanners capture the image of the hand and using the image edge detection algorithm compute the hand's characteristics. There are basically 2 sub-categories of optical scanners. Devices from the first category create a black-and-white bitmap image of the hand's shape. This is easily done using a source of light and a black-and-white camera. The bitmap image is then processed by the computer software.

G. *DNA Analysis*

This method is based on a DNA analysis. To perform a DNA analysis the user has to give some of his cells such as skin hair etc. Analyzing DNA takes a long time. Everyone is unique through his DNA. But it can be easily fooled, because anyone can steal a hair [4].It will maybe become the most efficient in crime department to identify criminal. DNA sampling is rather intrusive at present and requires a form of tissue, blood or other bodily sample.

H. *Palm print Recognition*

Palm print is inner part of hand. Palm prints possess features such as principal lines, orientation, minutiae, singular points etc. Also palm print modality is unique. Palm print recognition is used in civil applications, law enforcement and many such applications where access control is essential. Palm has features like geometric features, delta point's features, principal lines features, minutiae, ridges and creases. Principal lines are heart line, head line and life line [6].

Palm print contains three principal lines which divides palm into three regions: Interdigital, Hypothenar and Thenar. An Inter-digital region lies above the Heart line. The Thenar lies below the Life line. And Hypothenar is between Heart and Life line. From palm print principal lines, minutiae, ridges features can be extracted for identification.

Hand vein geometry is based on the fact that the vein pattern is distinctive for various individuals. The veins under the skin absorb infrared light and thus have a darker pattern on the image of the hand taken by an infrared camera [8].The hand vein geometry is still in the stage of research and development. One such system is manufactured by British Technology Group. The device is called Veincheck and uses a template with the size of 50 bytes.

I. *LIP motion based authentication*

Personal authentication is based on LIP motion only. It is composed of a password embedded in the lip movement and the underlying characteristic of lip motion. Subsequently, a lip-password protected speaker verification system aiming at holding a double security is established. That is, the claimed speaker will be verified by both of the password information and the underlying behavioral biometrics of lip motions simultaneously. Accordingly, the target speaker saying the wrong password or an impostor who knows the correct password will be detected and rejected [2].

Discriminative Analysis of Lip Motion Features for Speaker Identification and Speech-Reading gives explicit lip motion information, instead of or in addition to lip intensity and/or geometry information, for speaker identification and speech-reading within a unified feature selection and discrimination analysis framework. But the principal feature components representing each lip frame are not always sufficient to distinguish the biometric properties between different speakers; hence it is quite tedious complex method to implement.

III.SUMMARY

1. Advantages of the biometric authentication

The major advantage of the biometrics is that you can forget a password or lost an access card but impossible to forget your fingerprint, signatures and other biological features.

Advantage of biometric authentication systems may be their speed. The authentication using an iris-based identification system may take 2 (or 3) seconds while finding your key ring, locating the right key and using it may take some 5 (or 10) seconds. You save time and resources [11].

An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. Encoding and decision-making are tractable.

2. Disadvantages of the biometric authentication

The general drawback in this authentication scheme is that you cannot apply biometric identification process for deformed people such as visually impaired people have difficulties using iris or retina based techniques, Fingerprint recognition for person who has no hands etc. Some characteristics as your face can also be changed with the age.

The accuracy of iris scanners can be affected by changes in lightning. Deformation non-elastically as pupil changes size. Iris scanners are significantly more expensive than some other form of biometrics. Iris recognition is susceptible to poor image quality.

Different biometric samples of the same person may or may not be same. After the implementation, any failure of the biometric system and maintenance cost is also a big challenge.

IV. CONCLUSION

Proper design and implementation of the biometric system can indeed increase the overall security. It is necessary to trust the input device and make the communication link secure. Facial recognition systems are often deployed at frequently visited places to search for criminals.

Fingerprint systems are used to find an offender according to trails left on the crime spot. Infrared thermographs can point out people under influence of various drugs.

Biometric systems successfully used in non-authenticating applications may but also need not be successfully used in authenticating applications.

Biometrics implies that you have to face some ethics and law considerations. Palm print recognition is an emerging field and only limited works were carried out which paves way for the researchers to invent new methods to reduce the error rates and to improve the accuracy and speed of the system. Palm print recognition is an emerging field and only limited works were carried out which paves way for the researchers to invent new methods to reduce the error rates and to improve the accuracy and speed of the system. Cyber-crimes have been increasing everywhere hence it is expected to provide more significant secure identification with the help of biometric systems for protecting identities and transaction. Finally you have to select best option for authentication depending on level of security and requirements. For successful implementation of biometric technology, the biometric system must be error free so that it will increase the acceptance rate.

REFERENCES

[1] Ashbourn, J., Biometrics: Advanced Identity Verification: The Complete Guide. Springer Verlag, London, 2000: Springer. 201.
[2] 2. Learning Multi-Boosted HMMs for Lip Password Based Speaker Verification Xin Liu, Member, IEEE, and Yiu-ming Cheung, Senior Member, IEEETrans.on Information Forensic and Security,vol:9,No:2Feb.2014.
[3] 3. E. Newham, *The biometric report*, SBJ Services, 1995
[4] B. Schneier: *The Uses and Abuses of Biometrics*, Communications of the ACM, August 1999.
[5] Krishneswari, K., Arumugam, A. (2010) 'A Review on Palm Print Verification System', International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM), ISSN: 2150-7988 Vol.2 (2010), pp.113-120
[6] Krishneswari, K., Arumugam, A. (2010) 'A Review on Palm Print Verification System', International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM), ISSN: 2150-7988 Vol.2 (2010), pp.113-120.
[7] R. H. Hill, Retina identification, in A. Jain, *et al.* (eds) *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Press, 1999.
[8] David Mulyono, and Horng Shi Jinn, "A Study of Finger Vein Biometric for Personal Identification", Proceedings of the IEEE International Symposium on Biometrics and Security Technologies (ISBAST 2008), pp. 1-8, 2008.
[9] J. Perkins, FT-IT: New services will keep eye on security: biometrics. *Financial Times* (London), February 21, 2001, Wednesday Surveys ITC1.
[10] S.Pruzansky,Pattern-matching procedure for automatic talker recognition. *J. Acoust. Soc. Am*., **35**, 354–358, 1963.
[11] Dugelay, J.L., et al., Recent Advantages in Biometric Person Authentication, in ICASSP International Conference on Acoustics, Speech and Signal Processing. 2002: Orlando, Florida, USA.
[12] Common Criteria for Information Technology Security Evaluation, v 2.1, 1999.

DOI 10.17148/IJARCCE.2015.41157