Biometric Authentication System & its future trends

Aditi Gupta[1], abhilash Kumar[2]

[1] Scholar , College Of Computing Science And Information Technology (TMU)

[2] Assistant Professor, College Of Computing Science And Information Technology (TMU)

[1]aditigupta418@gmail.com

[2] AbhilashKumar21@gmail.com

***Abstract*— Authentication is the process of validating the identity of a person based on certain input that the person provides. Authentication has become a major topic of research due to the increasing number of attacks on computer networks around the globe. This paper focuses on biometric authentication systems in use today and in the upcoming days. We believe this paper will provide basic security researchers some useful insight whilst designing better biometric systems. Now a day the Biometric is becomes the most popular technique due to its liability. Because of need of high security systems we are also using the biometrics broadly. Another feature of biometric is its efficiency, authentication and authorization. It is very easy to use and handle. In this paper the review of Biometric System is provided. The main steps involve in biometrics is: Fingerprint Recognition and Face Recognition.**

***Keywords*— Authentication, Biometrics, Face, Iris, Multimodal, Retina**

I. Introduction

The biometric system is a growing technology and is fundamentally a pattern recognition system. Now a day, the biometric system becomes faster, easy to use, precise, trustworthy & economical over traditional knowledge based method. As we know, through personal experience or through reports in different media, software system, hardware system, is using biometric data for authentication become more & more common, and which has been widely used in forensics, secured access & prison security. The biometric attributes can be divided into two classes. The first class includes physical attribute like (fingerprint, iris & retina, palm & hand, face, face thermo gram etc) and second class includes behavior attribute like (signature, voice, movement, characteristics (key press, lips & hand movement, walk etc.)

Now we discuss on fingerprint sensors in laptop (see figure 1 on the next page). Mostly bank start using biometric authentication systems there exist even video stores and another work, but they are not widely used now-a-days.

Figure 1: Fingerprint sensor integrated in a laptop[1]

Authentication system must be used for some advantage, although no one spend their precious money for the research and development of this technology. So what are the advantages of this technique? Does the use of biometric data make system more secure? Many more questions running in my mind like what the disadvantage of this technique? Why this technique not widely used at the present time? Write this paper to find the correct and meaningful answers of these types of questions.

This paper divided into three parts.

1 part describes the short introduction of biometric system and especially fingerprints & face recognition. 2 parts describe different type of aspects for biometric authentication system which provides specific answer of the following

questions. Finally the 3 part provide the conclusion and references.

II. Biometrics – what is it?

Following definition of biometric system found by the internet on the page of Wikipedia “Biometrics is the study of automated method for uniquely recognizing humans based upon one or more intrinsic or behavioral traits”[1]. In the other word, A biometric system is a pattern recognition system that is used for define a features set in the form of specific data, and comparing the features set in the database.

The following are 2 biometric areas:-

A. Fingerprint Recognition

B. Face recognition

A. *Fingerprint Recognition:-*

Fingerprint biometric concept commonly used to uniquely identifying a person as another of a document since a long time. Fingerprint biometric used in numerous application that include civilian and commercial application like civil services, military, forensics, driver license registration, medicine, education, law enforcement, UIDAI, etc. This technique most widely used today and the future.

Fingerprint processing using image recognition algorithms, take fingerprint using scanned first. There exists different finger print scanner, e.g. optical, thermal and capacitive. Figure 2 show the different categories of fingerprint like (loop, whorl, and twin loop).

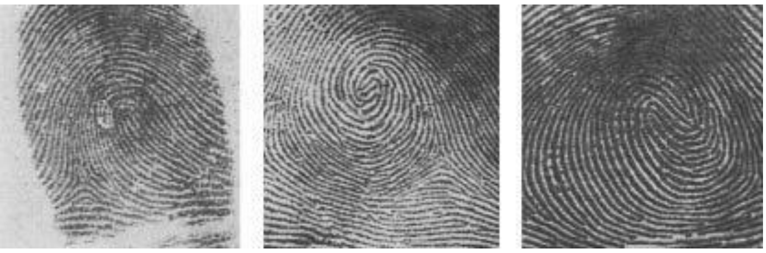

Figure 2: The picture shows 3 different categories of fingerprints - left loop, whorl and twinloop.[4]

B. *Face Recognitioon* :-

The method of distinguishing one individual form another is an ability of virtually every human. Algorithms for face recognition usually use the shape and location of facial attributes to distinguish between different faces. The face recognition systems usually use only the gray scale information. Color is mostly use for locating the face because every person has a some facial attributes like (eyes, nose, chine, lips, head etc.)

But the different is, every person facial structure is unique from another. So the facial technique, works like to identify a unique personality. Now this concept includes into a biometrics system.

The facial recognition technology has recently developed into two areas:

- Eigen faces
- Facial metrics

Those technologies usually look for the positioning of nose, eyes, mouth and show the distance between the entire facial attribute. To make this technology more successful and widely used to resolve the problems.

But the drawback is, these techniques not recognize additional aspect like Glasses, makeup, hairdressing and the ageing of faces can be a problem.

III. . Biometric authentication

A. *Authentication:-*

Before going more detail, first of all describe the general view of biometric authentication system. Show the figure3 to easily understand and helpful how to keep a system secure.

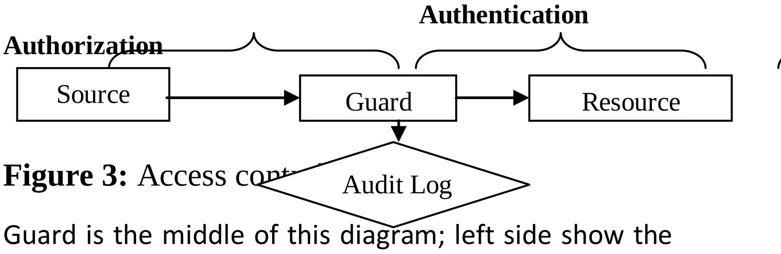

Figure 3: Access co

Guard is the middle of this diagram; left side show the source and right side show the resource. Guard uses authentication information for requesting the source and authorization info to a system and claims the particular identification that belongs to specific data. For example :- if the biometric system take a finger print if the person, and save the info in the data base, now give the unique enrollment number to identify the unique identity to of the person. Now the testing phases using enrollment number & password of the person to recognize the identity.

B. *Performance and security considerations:-*

As we all know old systems get only replaced by new ones, if the new systems have some advantages. For example if they are faster, more secure, cheaper or easier to use. So this section has a look at the performance and the security of biometric authentication systems, before the next section discusses some more advantages and disadvantages. The performance of a biometric authentication system is difficult to measure. The accuracy of a system is a strong factor which can indicate a good or a bad performance. Other factors like speed, storage, cost and ease-of-use should be considered as well.

C. *Advantage and Disadvantage*

Besides the already mentioned concerns about accuracy and security of biometric authentication systems there are some more disadvantages which are shortly mentioned in the following paragraphs. But besides all disadvantages the advantages which make biometric systems so desirable are described in the second half of this section.

Acceptability is one more disadvantage of biometric authentication systems. New systems can only be successful if they are accepted. In the case of biometric authentication systems some people are concerned about their acceptance in society.

“Many people hesitate using fingerprints for authentication because fingerprints are associated with criminals. Other people would never use iris scanner, because they are very harmful for eyes”. [7]

Another disadvantage is the high cost of biometric authentication technologies. Some articles[2] claims that “Biometric systems do impose the highest costs of any authentication technology.” The high cost results on the one hand from higher costs for hardware and software and on the other hand from high costs for integrating biometric authentication into the current network. [7]

The varying reliability of biometric systems is another disadvantage, which is already shortly mentioned above. The biometrics of people can change when they age or suffer physical injuries or diseases. This might for example affect their fingers or their eyes. In addition to that environmental conditions might affect the reliability of biometric systems. Background noise for example might hinder voice recognition systems or a cut in a finger might result in not being able to access a system using fingerprint recognition.[2]

One more disadvantage not yet mentioned, is the problem of integrating biometric authentication into corporate infrastructures. According to the article of Clare Hist[2] the support for platforms and applications is very limited and current standards are not or only poorly supported.

Besides all mentioned disadvantages, biometric authentications systems are very desire-able because of the following advantages.

The most obvious advantage is that biometric data can’t get lost, stolen, duplicated or forgotten like keys or access cards. They also can’t be forgotten, compromised, shared, observed or guessed like passwords, secret codes or PINs [9]. In addition to that people can’t write them down (“25% of the people appear to write their PIN on their ATM card” [3]) which would make is easy for other people to steal it. People also don’t have to change the data used for authentication every three months like we sometimes have to do with passwords. Therefore authentication systems using biometric data are more convenient to use.

The most important advantage is that biometric authentication systems can increase the security of the system, if the accuracy is high, the hardware used can’t be cheated easily and if it is used together with other authentication methods. Clare

Hist states for example that biometrics used in conjunction with smart cards "can provide strong security for PKI credentials held on the card."[2]

In addition to that biometric authentication systems reduce costs because it is possible to eliminate overheads resulting from password management[2]. The reason for this is that people can't forget their passwords anymore and so the queries at help desks become less. Besides reducing the mentioned overhead this also saves money because there are no more costs for distributing new passwords in a secure way.

IV. CONCLUSION AND OUTLOOK

. There seem to exist more disadvantages than advantages for using biometric authentication systems. This is one reason why such systems are not yet widely used. But the advantages mentioned above are so important and people want to benefit from them that the disadvantages will be more and more reduced in the future. However, some sort of trade-offs, like between the FA rate and the FR rate will always need to be made.

The discussion above shows that biometric authentication is an interesting topic that a lot of research is going on in this area and that it can be used for secure systems despite all disadvantages. At the moment it is recommended to combine biometric authentication with any other authentication technology. Such multi-factor authentication systems are always more secure and it is also common practice to use combinations of different authentication methods. ATMs require for example a PIN and a bank card with additional authentication information saved on a chip.

When talking about biometric data questions about the privacy of personal data come up automatically. This paper has not considered this topic but there are many articles dealing with these concerns. It is a difficult topic but it is obvious that biometric authentication systems have to store the biometric samples in a secure way and it has to be ensured that such data cannot be used otherwise. The best would be if biometric data is kept under the control of the person to which it belongs. This could be done for example by saving the biometric sample only on a smart card which is used in combination with the biometric in an authentication process.

To sum up it can be clearly said that the usage of biometric authentication will in-crease more and more in the future. This will be supported among other things by the steady improvement of the technologies and the reduction of the prices for hardware and software. Biometric authentication can and probably will be used in many areas, for example ATMs, access to Personal Computers, PDAs and mobile phones, DRM systems, access to buildings and cars and many more we can't even think about.

ACKNOWLEDGEMENT

I would like to thank Er Deepanshu Sharma, for his generosity, hard work and his kind support. He completely helped me finding the topic for this research paper as well as spelling and logical errors. Without him, I wouldn't be able to do this research work. Thanks to him a lot.

REFERENCES

[1] Wikipedia: The Free Encyclopedia.Biometrics.URL:http://en.wikipedia.org/wiki/Biometrics.

[2] Clare Hirst. The pros and cons of using biometric systems in business. Technical Report G00126400, Gartner, March 2005.

[3] Anil Jain, Lin Hong, and Sharath Pankanti. Biometric identification. Commun. ACM, 43(2):90–98, 2000.

[4] Anil K. Jain, Lin Hong, Sharath Pankanti, and Ruud Bolle. An identity-authentication system using fingerprints. In Proceedings of the IEEE, volume 85 of 9, pages 1365–1388, September 1997.

[5] J. Ortega-Garcia, J. Bigun, D. Reynolds, and J. Gonzalez-Rodriguez. Au-thentication gets personal with biometrics. Signal Processing Magazine, IEEE, pages 50–62, March 2004.

[6] P.J. Phillips, A. Martin, C.L. Wilson, and M. Przybocki. An introduction to evaluating biometric systems. Computer, 33:56–632, February 2000.

[7] Nataliya B. Sukhai. Access control & biometrics. In InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development, pages 124–127, New York, NY, USA, 2004. ACM Press.

[8] Lisa Thalheim, Jan Krissler, and Peter-Michael Ziegler. Body check. c't, November 2002. translated by Robert W. Smith.

[9] John D. Woodward. Biometrics: Privacy's foe or privacy's friend? In Proceedings of the IEEE, volume 85 of 9, pages 1480–1492, September 1997.

[10] 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.

[11] Geetika, Manavjeet Kaur " Fuzzy Vault with Iris and Retina: A Review" International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 4, April 2013.

[12] Anil. K.Jain, Arun Ross, Salil Prabhakar, "An introduction to biometric recognition", IEEE Transactions on circuits and systems for video technology, vol. 14, no. 1,pp 67-80, Jan 2004.

[13] N. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM System Journal, 40:614– 634, 2001.

[14] K. Takahashi, S. Hirata, H. Hino, and M. Mimura. Method, system and program for authenticating a user by biometric information. Google Patents, 2007.

[15] A. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, and J. Wayman. Biometrics: a grand challenge. In Proceedings of the 17th International Conference on Pattern Recognition, pages 935–942, 2004.