

Biometric Authentication

Shinju Kelotj¹ Aishwarya Swamy²

^{1,2}Department of Information Technology

^{1,2}Model College, Khambalpada, India

Abstract— Over the last few years a new area of engineering science has been established whose products are likely to create a large market in the near future. It has been called "biometrics". The pioneers of this new domain intend to construct devices which would allow identification of a person on the basis of his/her "biological" characteristics: voice, dynamics of movements, features of face and other parts of the body, retina or iris pattern. Nature has made human beings with different characteristics which may vary from one person to another. This property is made use of by Biometric technology to distinctly identify each person. Biometric system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Several important issues must be considered in designing a practical biometric system. First, a user must be enrolled in the system so that his biometric template can be captured. This template is securely stored in a central database or a smart card issued to the user. The template is retrieved when an individual needs to be identified. Depending on the context, a biometric system can operate either in a verification (authentication) or an identification mode. Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification offers several advantages over traditional methods involving ID cards (tokens) or PIN numbers (passwords) for various reasons: (i) the person to be identified is required to be physically present at the point-of-identification; (ii) identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased integration of computers and Internet into our everyday lives, it is necessary to protect sensitive and personal data. By replacing PINs (or using biometrics in addition to PINs), biometric techniques can potentially prevent unauthorized access to ATMs, cellular phones, laptops, and computer networks. Unlike biometric traits, PINs or passwords may be forgotten, and tokens like passports and driver's licenses may be forged, stolen, or lost.

Keywords: Breast Cancer; Breast Cancer Detection; Medical Images; Machine Learning

I. INTRODUCTION

Information security is concerned with the assurance of confidentiality, integrity and availability of information in all forms. There are many tools and techniques that can support the management of information security. But system based on biometric has evolved to support some aspects of information security. Biometric authentication supports the facet of identification, authentication and non-repudiation in information security.

Biometric authentication has grown in popularity as a way to provide personal identification. Person's identification is crucially significant in many application and the hike in credit card fraud and identity theft in recent years

indicate that this is an issue of major concern in wider society. Individual passwords, pin identification or even token based arrangement all have deficiencies that restrict their applicability in a widely-networked society.

Biometric is used to identify the identity of an input sample when compared to a template, used in cases to identify specific people by certain characteristics. Possession based: using one specific "token" such as a security tag or a card and knowledge-based: the use of a code or password. Standard validation systems often use multiple inputs of samples for sufficient validation, such as particular characteristics of the sample. This intends to enhance security as multiple different samples are required such as security tags and codes and sample dimensions. So, the advantage claimed by biometric authentication is that they can establish an unbreakable one-to-one correspondence between an individual and a piece of data.

In this paper, we present a detail survey on Biometric Authentication and we hope that this work will definitely provide a concrete overview on the past, present and future aspects in this field.

II. SCOPE

A biometric system can provide two functions. One of which is verification and the other one is Authentication. So, the techniques used for biometric authentication has to be stringent enough that they can employ both these functionalities simultaneously. Currently, cognitive biometrics systems are being developed to use brain response to odor stimuli, facial perception and mental performance for search at ports and high security areas. Other biometric strategies are being developed such as those based on gait (way of walking), retina, Hand veins, ear canal, facial thermogram, DNA, odor and scent and palm prints. In the near future, these biometric techniques can be the solution for the current threats in world of information security.

Of late after a thorough research it can be concluded that approaches made for simultaneous authentication and verification is most promising for iris, finger print and palm vein policies. But whatever the method we choose, main constraint will be its performance in real life situation. So, application of Artificial System can be a solution for these cases. We have given emphasis on the Iris recognition. According to us, after detection of an iris pattern, the distance between pupil and the iris boundary can be computed. This metric can be used for the recognition purposes because this feature remains unique for each and every individual. Again, an artificial system can be designed which will update the stored metric as the proposed feature may vary for a particular person after certain time period.

After doing the manual analysis of the above discussed method, we have got a satisfactory result. Due to the dynamic modification of the proposed metric, the rejection ration for a same person reduces by a lot. The work is being carried out to make the system viable.

III. LITERATURE REVIEW

European explorer Joao de Barros recorded the first known example of fingerprinting, which is a form of biometrics, in China during the 14th century. Chinese merchants used ink to take children's fingerprints for identification purposes.

In 1890, Alphonse Bertillon studied body mechanics and measurements to help in identifying criminals. The police used his method, the Bertillonage method, until it falsely identified some subjects.

The Bertillonage method was quickly abandoned in favor of fingerprinting, brought back into use by Richard Edward Henry of Scotland Yard.

Karl Pearson, an applied mathematician studied biometric research early in the 20th century at University College of London. He made important discoveries in the field of biometrics through studying statistical history and correlation, which he applied to animal evolution. His historical work included the method of moments, the Pearson system of curves, correlation and the chi-squared test.

In the 1960s and '70s, signature biometric authentication procedures were developed, but the biometric field remained fixed until the military and security agencies researched and developed biometric technology beyond fingerprinting.

IV. METHODS

We have already stated that there exist two kind of biometric characteristics. So, techniques for biometric authentication have been developed based on these characteristics. Details of different techniques are discussed below.

A. Finger Print Technology

A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the on the palmar (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin.

These ridges are sometimes known as "dermal ridges" or "dermal ". The traditional method uses the ink to get the finger print onto a piece of paper. This piece of paper is then scanned using a traditional scanner. Now in modern approach, live finger print readers are used. These are based on optical, thermal, silicon or ultrasonic principles [22],

B. Face Recognition Technology

A facial recognition technique is an application of computer for automatically identifying or verifying a person from a digital image or a video frame from a video source. It is the most natural means of biometric identification [6].

Facial recognition technologies have recently developed into two areas and they are Facial metric and Eigen faces.

Facial metric technology relies on the manufacture of the specific facial features (the system usually look for the positioning of eyes, nose and mouth and distances between these eatures), some other available techniques for biometric authentication are described below.

C. Palmprint:

Palmprint verification is a slightly different implementation of the fingerprint technology. Palmprint scanning uses optical

readers that are very similar to those used for fingerprint scanning, their size is, however, much bigger and this is a limiting factor for the use in workstations or mobile devices [40, 15].

D. Hand Vein:

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. 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

E. DNA:

DNA sampling is rather intrusive at present and requires a form of tissue, blood or other bodily sample. This method of capture still has to be refined. So far the DNA analysis has not been sufficiently automatic to rank the DNA analysis as a biometric technology. The analysis of human DNA is now possible within 10 minutes. As soon as the technology advances so that DNA can be matched automatically in real time, it may become more significant. At present Biometric Systems DNA is very entrenched in crime detection and so will remain in the law enforcement area for the time being [2, 4, 16].

V. CONCLUSION

While biometric authentication can offer a high degree of security, they are far from perfect solution. Sound principles of system engineering are still required to ensure a high level of security rather than the assurance of security coming simply from the inclusion of biometrics in some form.

The risks of compromise of distributed database of biometrics used in security application are high- particularly where the privacy of individuals and hence non-repudiation and irrevocability are concerned. It is possible to remove the need for such distributed databases through the careful application of biometric infrastructure without compromising security.

The influences of biometric technology on society and the risks to privacy and threat to identify will require mediation through legislation. For much of the short history of biometrics the technology developments have been in advance of ethical or legal ones.

Careful consideration of the importance of biometrics data and how it should be legally protected is now required on a wider scale.

REFERENCES

- [1] Smart Cart Alliance Identity Council (2007): Identity and Smart Card Technology and Application Glossary, <http://www.smartcardalliance.org>, as visited on 25/10/2008.
- [2] Jain, A. K.; Ross, A. & Pankanti, S., "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics And Security, Volume 1, issue 2, Jun. 2006, pp 125 – 144.

- [3] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems", *IEEE Trans. Pattern Anal. Mach. Intell.*, Volume 28, issue 1, Jan. 2006, pp. 3–18.

