2009 Second International Conference on Computer and Electrical Engineering

Biometric Authentication Techniques and its Future Possibilities

Debnath Bhattacharyya[1], Rahul Ranjan[1], Poulami Das[1], Tai-hoon Kim[2], Samir Kumar Bandyopadhyay[3]
[1]Computer Science and Engineering Department
Heritage Institute of Technology
Kolkata, India
{debnathb, rahul.sdabahar,dasp88}@gmail.com

[2]Hannam University
Daejeon, Korea
taihoonn@empal.com

[3]Department of Computer Science and Engineering
University of Calcutta, Kolkata, India
skb1@vsnl.com

***Abstract*—Advances in the field of Information Technology also make Information Security an inseparable part of it. In order to deal with security, Authentication plays an important role. This paper presents a review on the biometric authentication techniques and some future possibilities in this field. In biometrics, a human being needs to be identified based on some characteristic physiological parameters. A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. By using biometrics it is possible to confirm or establish an individual's identity. The position of biometrics in the current field of Security has been depicted in this work. We have also outlined opinions about the usability of biometric authentication systems, comparison between different techniques and their advantages and disadvantages in this paper.**

Keywords-biometric; authentication; recognition; IRIS; voice.

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. Compared to other biometric, iris is protected from the external environment behind the cornea and the eyelid. No subject to deleterious effects of aging, the small-scale radial features of the iris remain stable and fixed from about one year of age throughout life [5].

II. BIOMETRIC PAST, PRESNT AND FUTURE

In this paper, we have tried to 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.

A. Past

European explorer Joao de Barros recorded the first known example of fingerprinting, which is a form of biometrics, in China during the 14th century.

In 1890, Alphonse Bertillon studied body mechanics and measurements to help in identifying criminals.

Karl Pearson, an applied mathematician studied biometric research early in the 20th century at University College of London.

In the 1960s and '70s, signature biometric authentication procedures were developed.

978-0-7695-3925-6/09 $26.00 © 2009 IEEE
DOI 10.1109/ICCEE.2009.103

B. *Present*

Biometrics authentication is a growing and controversial field in which civil liberties groups express concern over privacy and identity issues. Today, biometric laws and regulations are in process and biometric industry standards are being tested. Face recognition biometrics has not reached the prevalent level of fingerprinting, but with constant technological pushes and with the threat of terrorism, researchers and biometric developers will stimulate this security technology for the twenty-first century. In modern approach, Biometric characteristics can be divided in two main classes:

- Physiological are related to the shape of the body and thus it varies from person to person Fingerprints, Face recognition, hand geometry and iris recognition are some examples of this type of Biometric.
- Behavioral are related to the behavior of a person. Some examples in this case are signature, keystroke dynamics and of voice. Sometimes voice is also considered to be a physiological biometric as it varies from person to person.

Recently, a new trend has been developed that merges human perception to computer database in a brain-machine interface. This approach has been referred to as cognitive biometrics. Cognitive biometrics is based on specific responses of the brain to stimuli which could be used to trigger a computer database search.

C. *Future*

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 thermograph , 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 vain 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 because this technique can have some good low level implementation.

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. TECHNIQUES

Numerous promising techniques are available, proposed and in practice. These are Finger Print Technology, Face Recognition Technology, Retina Technology, Hand Geometry Technique, Speaker Recognition Technique, Signature Verification Technique, Palm print, Hand Vein, DNA, Thermal Imaging, Ear Shape, Body Odor, and Keystroke Dynamics. Here in this paper, details of IRIS Technology is discussed.

IRIS recognition method uses the iris of the eye which is colored area that surrounds the pupil. Iris patterns are unique and are obtained through video based image acquisition system. Each iris structure is featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings [1].

Figure 1. Image of Iris.

Localization of the iris is an important step in iris recognition because, if done improperly, resultant noise (e.g., eyelashes, reflections, pupils, and eyelids) in the image may lead to poor performance, shown in figure 2.

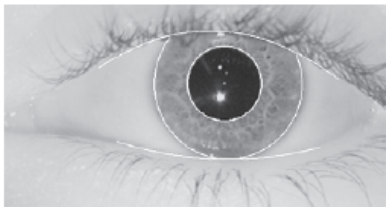

Figure 2. White outlines indicate the localization of the iris.

An iris-recognition algorithm first has to identify the approximately concentric circular outer boundaries of the iris and the pupil in a photo of an eye. The set of pixels covering only the iris is then transformed into a bit pattern that preserves the information that is essential for a statistically meaningful comparison between two iris images, (figure 1 shows an IRIS Image). The iris pattern is taken by a special gray scale camera in the distance of 10- 40 cm of camera. Once the gray scale image of the eye is obtained then the software tries to locate the iris within the image. If an iris is found then the software creates a net of curves covering the

iris. Based on the darkness of the points along the lines the software creates the IrisCode. Here, two influences have to take into account. First, the overall darkness of image is influenced by the lighting condition so the darkness threshold used to decide whether a given point is dark or bright cannot be static, it must be dynamically computed according to the overall picture darkness. Secondly, the size of the iris changes as the size of the pupil changes. Before computing the iris code, a proper transformation must be done.

To perform the recognition, two IrisCodes are compared, (figure 4 shows an IrisCode). The amount of difference between two IrisCodes — Hamming Distance (HD) — is used as a test of statistical independence between the two IrisCodes. If the HD indicates that less than one-third of the bytes in the IrisCodes are different, the IrisCode fails the test of statistical significance, indicating that the IrisCodes are from the same iris. Therefore, the key concept to iris recognition is failure of the test of statistical independence. In decision process, the matching software takes two iris codes and compute the hamming distance based on the number of different bits. The hamming distances score (within the range 0 means the same IrisCodes), which is then compared with the security threshold to make the final decision. Computing the hamming distance of two iris codes is very fast (it is the fact only counting the number of bits in the exclusive OR of two iris codes). We can also implement the concept of template matching in this technique. In template matching, some statistical calculation is done between a stored iris template and a produced. Depending on the result decision is taken [2, 3, 4].

Figure 3. Iris Scanner (2100 Model).

Iris scanner(fig 3) is biometric scanner used to identify the approximately concentric circular outer boundaries of the iris and the pupil in a photo of an eye. The set of pixels covering only the iris is then transformed into a bit pattern that preserves the information that is essential for a statistically meaningful comparison between two iris images.

Figure 4. IrisCode.

IV. APPLICATIONS

Biometric authentication is highly reliable, because physical human characteristics are much more difficult to forge then security codes ,passwords ,hardware keys sensors ,fast processing equipment and substantial memory capacity, so the system are costly. Biometric-based authentication applications include workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and Web security. The promises of e-commerce and e-government can be achieved through the utilization of strong personal authentication procedures. Secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometric technologies are expected to play a key role in personal authentication for large-scale enterprise network authentication environments, Point-of-Sale and for the protection of all types of digital content such as in Digital Rights Management and Health Care applications. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics is anticipated to pervade nearly all aspects of the economy and our daily lives. For example, biometrics is used in various schools such as in lunch programs in Pennsylvania, and a school library in Minnesota. Examples of other current applications include verification of annual pass holders in an amusement park, speaker verification for television home shopping, Internet banking, and users' authentication in a variety of social services.

V. EVALUATION

When it is time to use the biometric authentication, the degree of security is concerned. In this paper, we have discussed the various types of biometric authentication techniques. In this section, we will evaluate different techniques and find degree of security. Table I shows the comparison of various techniques.

Iris patterns have a high degree of randomness in their structure. This is what makes them unique.

Iris technology can't be easily artificially duplicated because of its unique properties .There is closed connection from iris to the human brain and it is said to be one of the first parts of the body to decay after the death. Therefore, it is very difficult to create an artificial iris to fraudulently bypass the biometric systems if the detection of the iris liveness is working properly. Table II shows the advantage of the use of IRIS Technology.

VI. DISCUSSION

A. Benefits of using IRIS Technology

i. The iris is a thin membrane on the interior of the eyeball. Iris patterns are extremely complex.
ii. Patterns are individual (even in fraternal or identical twins).
iii. Patterns are formed by six months after birth, stable after a year. They remain the same for life.
iv. Imitation is almost impossible.

v. Patterns are easy to capture and encode.

B. *Limitations of Person Recognition by IRIS Technology*

i. Blind persons may have difficulty in getting themselves aligned with the iris camera at arm's length, because some such systems rely on visual feedback via a mirror or LCD display to guide the user into alignment with the camera.

ii. Persons with pronounced nystagmus (tremor of the eyes) may have difficulty in presenting a stable image; however, some iris cameras now use stroboscopic (flashed infrared) illumination with very fast camera integration times, on the order of milliseconds, so tremor becomes unimportant for image capture.

iii. A person must of course have an eye, with an iris. According to the US National Eye Institut, the condition of aniridia (lack of an iris) occurs in 1.8 of 100,000 births. Because it is genetically linked, the condition usually affects both eyes according to the UK's Royal National Institute for the Blind, but its incidence covers a wide spectrum of partial conditions such as just chronically enlarged pupils. Iris recognition requires the pupil to have a diameter less than about 75% of the iris.

Iris recognition has both the potential to be a convenience enhancer (including an access enhancer), but also the potential to be an obstacle or excluder if improperly configured or installed without consultation and guidance from disabled persons. Because it allows hands-free, automatic, rapid and reliable identification of persons, it can facilitate access for persons unable to engage in the standard mechanical transactions of access. But it must not presume universal uniformity among persons and their bodies. The variability of persons is, after all, the heart and soul of biometric technology.

VII. 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] Sanjay R. Ganorkar , Ashok A. Ghatol , "Iris Recognition: An Emerging Biometric Technology", In Proc. of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation, Greece, Feb. 2007, pp. 91 – 96.

[2] A. K. Jain, A. Ross, and S. Pankanti, "Biometric: A Tool for Information Security", IEEE Trans. Information Forensics and Security, Volume 1, No. 2, Jun. 2006, pp. 125–144.

[3] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds., "Biometric Systems: Technology, Design and Performance Evaluation", New York: Springer Verlag, 2005.

[4] J. Daugman, "The importance of being random: statistical principles of iris recognition", Journal of Pattern Recognition, Elsevier, Volume 36, No. 2, Feb. 2003, pp. 279–291.

[5] Christel-Loic Tisse, Lionel Torres and Michel Robert, "Person Identification Technique Using Human Iris Recognition", International Conference on Vision Interface, May 27-29, 2002, Calgary, Canada, pp. 294-299.

TABLE I. COMPARISON OF VARIOUS BIOMETRIC METHODS.

Biometric	**EER**	**FAR**	**FRR**	**Subjects**	**Comments**
face	NA	1%	10%	37437	varied light, indoor /outdoor
finger print	2%	2%	2%	25000	rotation and exaggerated skin distortion
hand geometry	1%	2%	2%	129	with rings and improper placement
iris	.01%	.94%	.99%	1224	indoor environment
keystrokes	1.8%	7%	.1%	15	during 6 months period
voice	6%	2%	10%	30	text dependent and multilingual

TABLE II. ADVANTAGE OF IRIS TECHNOLOGY.

Method	**Coded Pattern**	**Misidentification rate**	**Security**	**Applications**
Iris Recognition	Iris pattern	1/1,200,000	High	High-security facilities