International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Study of Biometric Authentication Systems and Their Security

Dr. Vikash Kumar Singh[1], Devendra Singh Kushwaha[2], Roshni Tiwari[3]

[1]Head (I/C) Dept. of computer Science IGNTU Amarkantak (M.P.), India

[2]Assistant Professor Faculty of Vocational Educational IGNTU Amarkantak (M.P.), India

[3]Department of Computer Science, IGNTU Amarkantak (M.P.), India

Abstract: ***A biometric system is fundamentally a pattern recognition system that recognizes a person by determining the authentication by using his different biological features i.e. Fingerprint, retina-scan, iris scan, hand geometry, and face recognition are leading physiological biometrics and behavioral characteristic are Voice recognition, keystroke-scan, and signature-scan. Biometrics is a growing technology, which has been widely used in forensics, secured access and prison security. This paper deals with the design of a biometric security system based upon the fingerprint and speech technology. In this paper different biometrics techniques such as Iris scan, retina scan and face recognition techniques are discussed. We would like to outline our opinions about the usability of biometric authentication systems. We outline the position of biometrics in the current field of computer security.***

Keywords: Biometric, Biometric techniques, Eigen face, Face recognition

1. Introduction

This paper summarizes our opinions and findings after several years of studying biometric authentication systems and their security. Our research on security and reliability issues related to biometric authentication. Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic.

The past of biometrics includes the identification of people by distinctive body features, scars or a grouping of other physiological criteria, such like height, eye color and complexion. The present features are face recognition, fingerprints, handwriting, hand geometry, iris, vein, voice and retinal scan. Biometric technique is now becoming the foundation of a wide array of highly secure identification and personal verification. As the level of security breach and transaction scam increases, the need for well secure identification and personal verification technologies is becoming apparent. Recent world events had lead to an increase interest in security that will impel biometrics into majority use. Areas of future use contain Internet transactions, workstation and network access, telephone transactions and in travel and tourism. There have different types of biometrics:
Some are old or others are latest technology. The most recognized biometric technologies are fingerprinting, retinal scanning, hand geometry, signature verification, voice recognition, iris scanning and facial recognition. A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

1) **Identification (1:n)** One-to-Many: Biometrics can be used to determine a person's identity even without his awareness or approval. Such as scanning a crowd with the help of a camera and using face recognition technology, one can verify matches that are already store in database.
2) **Verification (1:1)** One-to-One: Biometrics can also be used to verify a person's identity. Such as one can allow physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retina scan.

2. Biometric Characteristics

"Biometrics" means "life measurement" but the term is generally coupled with the use of unique physiological characteristics to identify a person, some other characteristics of biometrics are:
Universal: Every person must possess the characteristic. The trait must be one that is universal and seldom lost to accident or disease.

- **Invariance of properties:** They should be constant over a long time. The trait should not be focus to considerable differences based on age either episodic or chronic disease.
- **Measurability:** This should be suitable for capture without waiting time and must be easy to gather the attribute data passively.
- **Singularity:** Each expression of the element must be distinctive to the person. The characteristics should have adequate distinctive properties to distinguish one person from other. Height, weight, hair and eye color are all elements that are unique assuming a mostly accurate measure, but do not offer enough points of separation to be useful for more than categorizing.
- **Acceptance:** The capturing should be possible in a manner acceptable to a large fraction of the residents. Excluded are particularly persistent technologies, such technologies which is require a part of the human body to be taken or which (apparently) impair the human body.
- **Reducibility:** The captured data should be able of being reduced to a file which is easy to handle.
- **Reliability and tamper-resistance:** The attribute should be impractical to mask or modify. Process should make sure high reliability and reproducibility.

- **Privacy:** This process should not break the privacy of the individual.
- **Comparable:** They should be able to reduce the trait to a state that makes it is digitally comparable from others. It has less probabilistic for similarity and more dependable on the identification.
- **Inimitable:** The trait must be irreproducible by other way. The less reproducible the trait, the more likely it will be reliable.
- **Biometric technologies**: fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke dynamics, ear shape, odor and signature.

3. Fingerprint Recognition

The first thing to describe is the principle of fingerprint recognition, i.e. extracting the minutiae from the fingerprint. [8] It should be said that all fingerprints could be divided into 5 classes. ***Fingerprint classes:*** Arch, Left Loop, Right Loop, Tended Arch, Whorl.[3]. The whole process of fingerprint analysis (the method of minutiae comparison) consists of the following six steps .

1) Getting the input fingerprint image. The quality of acquired image is important for the performance of automatic identification. It is desirable to use finger print scanner of high quality that is capable to tolerate different skin types, finger injures and dryness or dampness of the finger surface.[4]
2) Performance of the algorithms for image quality improvement. Image quality improvement is used to recover the real furrow & ridge structures from a damaged image. At first the histogram of fingerprint image is obtained, then the histogram equalization is performed, the Gabor filters are used – they improve the clearness of ridge & furrow structures in recovered areas and so prepare image for minutiae extraction algorithm. Then the directional array is found in the image using filtering in frequency domain (FFT → Economopoulos filter → IFFT).
3) Performance of the image preprocessing. It is a preparatory step for minutiae extraction and classification. Thresholding by RAT scheme (Regional Average Thresholding) and thinning (by Emyroglu) is performed in this step.
4) Fingerprint classification. In this step the fingerprint is assigned to one of five classes. The classification is a difficult process for the machine as well as for the human, because for some fingerprints it is very complicated to unambiguously choose the particular class. At first the Karhunen- Loève transformation is applied on the directional array obtained from the step 2. Then the PNN classifier (Probabilistic Neural Network) is applied, which assigns the fingerprint into one of five classes.
5) Minutiae extraction. Here we use the Emyroglu extractor, which extracts only three types of minutia from the fingerprint skeleton – ridge ending, continuous line and bifurcation. In this step some improvements have been done. When the detection and extraction phase is finished, the minutiae are tested once more. If they lie on the edge of the fingerprint, they are deleted. The second test checks the papillary line continuity (partially done in step 3) – difference between line ending and bifurcation. And the last improvement includes more accurate scale for gradient of the minutia. Now it is possible to detect the degree of the bias of the papillary line more accurately and compute the gradient of this minutia.

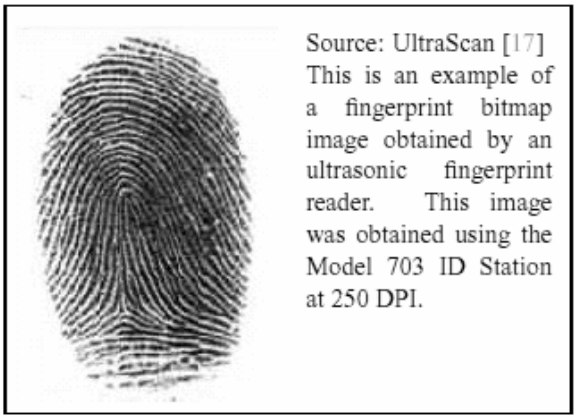
Source: UltraScan [17]
This is an example of a fingerprint bitmap image obtained by an ultrasonic fingerprint reader. This image was obtained using the Model 703 ID Station at 250 DPI.

Figure 2: Fingure print image

3.1 Hand Geometry

Hand geometry relies on measurements of the width, height, and length of the fingers, distances between joints, and the shape of knuckles. Using optical cameras and light-emitting diodes that have mirror sand reflectors, two orthogonal, two-dimension images of the back and the sides of the hand are taken. Based on these images, 96measurements are then calculated and a template created. Most hand readers have pins to help position the hand properly. These pin shelf with consistent hand placement and template repeatability, so there is a low false positive rate and a low failure to match rate.

Hand geometry readers usually cost between $2,000 and $4,000. Hand geometry is a mature technology primarily used for high-volume time-and-attendance and access control. For instance, both Krispy Kreme and McDonald's rely on hand geometry to record staff time and attendance. Hand geometry works well when many people need to be processed in a short period of time, so long as it is one-to-one matching. Although people's hands differ, they are not individually distinct. As a result, hand geometry technology cannot be used for one-to-many matching.

Hand geometry is perceived as very accurate and has been used in a variety of industries to regulate access control for more than 30years. It is useful in identifying who is permitted somewhere or to do something and who is not. It is very difficult to spoof someone's hand shadow without the person's cooperation. The necessary information is not left behind physically (as, by contrast, a fingerprint often is), so that it is quite difficult to create a fake hand that would work on the unit without the enrolled person's knowledge. The technology is relatively stable – units placed in the field in 1991 are still working. The main change over the years has been in cost reduction. A wide variety of places rely on hand geometry for access. The San Francisco airport uses it for access to the tarmac; the port of Rotterdam, Scott Air Force Base, and a sorority at the University of Oklahoma also rely on it.

Most people are comfortable using the technology. Since it

is an image of a hand as opposed to something more intrusive, most people consent to enrollment in the program. In addition, it is no less hygienic than touching a doorknob. (Indeed, acceptance of the technology by users has been made relatively easy by describing the hand geometry reader as a funny-looking doorknob) Furthermore, people's unwillingness to accept hand geometry technology can be overcome if the individuals can see that they will get something in return. For instance, Gold's Gym uses the units for access, which allows its members to avoid the hassle of carrying keys or cards; the University of Georgia employs the technology for tracking meal plans. In the near future, Sea World annual pass holders will use hand geometry to enter the park. It is also used in approximately 15,000 banking applications.

Figure 2: Hand Geometry

3.2 Iris

The iris is the colored ring of textured tissue that surrounds the pupil of the eye. Even twins have different iris patterns and everyone's left and right iris is different, too. Research shows that the matching accuracy of iris identification is greater than of the DNA testing.

The iris pattern is taken by a special gray-scale camera in the distance of 10–40 cm from the camera (earlier models of iris scanners required closer eye positioning). The camera is hidden behind a mirror, the user looks into the mirror so that he/she can see his/her own eye, then also the camera can "see" the eye. Once the eye is stable (not moving too fast) and the camera has focused properly, the image of the eye is captured (there exist also simpler versions without autofocus and with a capture button).[1]

The iris scanner does not need any special lighting conditions or any special kind of light (unlike the infrared light needed for the retina scanning). If the background is too dark any traditional lighting can be used. Some iris scanners also include a source of light that is automatically turned on when necessary. The iris scanning technology is not intrusive and thus is deemed acceptable by most users. The iris pattern remains stable over a person's life, being only affected by several diseases. 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 iris code, which characterizes the iris. When computing the iris code two influences have to be taken into account. First, the overall darkness of the image is influenced by the lighting conditions 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. And second, the size of the iris dynamically changes as the size of the pupil changes. Before computing the iris code, a proper transformation must be done. In the decision process the matching software given 2 iris codes computes the Hamming distance based on the number of different bits. The Hamming distance is a score (within the range 0 – 1, where 0 means the same iris codes), 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 in speed fact only counting the number of bits in the exclusive OR of the two iris codes). Modern computers are able to compare over 4000000 iris codes in one second. An iris scan produces a high data volume which implies a high discrimination (identification) rate. Indeed the iris systems are suitable for identification because they are very fast and accurate. Our experience confirms all that. The iris recognition was the fastest identification out of all the biometric systems we could work with. We have never encountered a false acceptance (the database was not very large, however) and the false rejection rate was reasonably low. The manufacturer quotes the equal error rate of 0.00008%, but so low false rejection rate is not achievable with normal (non-professional) users. It is said that artificial duplication of the iris is virtually impossible because of the unique properties. The iris is closely connected to the human brain and it is said to be one of the first parts of the body to decay after death. It should be therefore very difficult to create an artificial iris or to use a dead iris to fraudulently bypass the biometric system if the detection of the iris livens is working properly. We were testing an iris scanning system that did not have any countermeasures implemented. We fooled such a system with a very simple attack. The manufacturer provided us with a newer version of the system after several months. We did not succeed with our simple attacks then, but we wish to note that we did not have enough time to test more advanced versions of our attack. A single company (Iridian Technologies, Inc.) holds exclusively all the world-wide patents on the iris recognition concept. The technology was invented by J. Daugman of Cambridge University and the first iris scanning systems were launched in 1995.

3.3 Retina

Retina scan is based on the blood vessel pattern in the retina of the eye. Retina scan technology is older than the iris scan technology that also uses a part of the eye. The first retinal scanning systems were launched by Eye Dentify in 1985. 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. A skilled operator is required and the person being scanned has to follow his/her directions.[2]

A retina scan produces at least the same volume of data as a fingerprint image. Thus its discrimination rate is sufficient not only for verification, but also for identification. In the practice, however, the retina scanning is used mostly for verification. The size of the eye signature template is 96 bytes. The retinal scanning systems are said to be very accurate. For example the Eye Dentify's retinal scanning system has reputedly never falsely verified an unauthorized user so far. The false rejection rate, on the other side, is relatively high as it is not always easy to capture a perfect image of the retina. Retinal scanning is used only rarely today because it is not user friendly and still remains very expensive. [2]Retina scan is suitable for applications where the high security is required and the user's acceptance is not a major aspect. Retina scan systems are used in many U.S. prisons to verify the prisoners before they are released. The check of the eye liveness is usually not of a significant concern as the method of obtaining the retina blood vessel pattern is rather complicated and requires an operator.

Figure 3: Retina Scan

4. Conclusion

Biometrics is a rapidly evolving technology that is being widely used in forensics, security; prevent unauthorized access in bank or ATMs, in cellular phones, smart cards, PCs, in workplaces, and computer networks. There are numerous forms of biometrics now being built into technology platforms. It has been implemented in public for short time. There are lots of applications and solutions in biometrics technology used in security systems, which can improve our lives such as: improved security, it is reduced con and password administrator costs, easy to use and make life more secure and comfortable. But it is not possible to definitely state if a biometric technique are successful run, it is essential to locate factors that's help to reduce affect system performance. The international biometric group Strike System Strikes are: in Fingerprint Dry/oily finger, in Voice recognition Cold or illness that affects voice, in Facial recognition Lighting conditions, in Iris-scan Too much movement of head or eye, in Hand geometry Bandages, and in Signature-scan Different signing positions. Face recognition technology are more reliable, non-intrusive, inexpensive and extremely accurate. Currently Face recognition technology is the most challenging recognition technologies.

References

[1] K P Tripathi, International Journal of Computer Applications (0975 – 8887) Volume 14– No.5, January 2011
[2] Iridian Technologies, http://www. iriscan.com
[3] Eye Dentify, www. raycosecurity. com/biometrics/EyeDentify.html
[4] Zdeněk R íhaVáclav Matyáš "Biometric Authentication Systems"FI MU Report Series, November 2000.
[5] Hong, L.: Automatic Personal Identification Using Fingerprints, Michigan State University.
[6] Jain, L.C., Halici, U., Hayashi, I., Lee, S.B., Tsutsui, S.: Intelligent Biometric Techniques in Fingerprint
[7] Emyroglu, Y.: Fingerprint Image Enhancement & Recognition; Yldyz Technical University, Turkey, 1997
[8] Hong, L.: Automatic Personal Identification Using Fingerprints, Michigan State University,1998
[9] Nalini K. Ratha, Andrew Senior and Ruud M. Bolle," Automated Biometrics". IBM Thomas J. Watson Research Center, PP 1-10