ISSN: 2277-9655
Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ASSORTED DIRECTIONS OF AUTHENTICATION IN BIOMETRIC SYSTEMS

Shambhu Prasad Sah*, Purushottam Das, Himanshu Pant, Ankur Singh Bist
* Assistant Professor, Deptt. of CSE, Graphics Era Hill University, Nainital, Uttarkhand, India
Assistant Professor, Deptt. of CSE, Graphics Era Hill University, Nainital, Uttarkhand, India
Assistant Professor, Deptt. of CSE, Graphics Era Hill University, Nainital, Uttarkhand, India
Assistant Professor, Deptt. of CSE, KIET Ghaziabad

DOI: 10.5281/zenodo.51426

ABSTRACT

Biometrics refers to a way of authentication in the world of computer security using various metrics linked to human characteristics. It is used for access control and recognition of individuals. This paper provides the working of Biometrics System, description of its various features and various biometrics methods used in digital world of computer.

KEYWORDS: Biometrics, false acceptance rate, false rejection rate, Biometric Deception, Watchlist, fingerprint recognition, face recognition, iris recognition, voice recognition.

INTRODUCTION

We forget passwords. We lose access cards. Yet despite jokes about leaving our heads at home, we always take our bodies with us. This allows biometric authentication, which is based on biological (bio) measurements (metrics). Biometric authentication [1] is based on something you are (your fingerprint, iris pattern, face, hand geometry, etc.) or something you do (write, type, walk, etc.).

BIOMETRIC SYSTEMS

INITIAL ENROLLMENT

Figure 1 [1] shows a biometric authentication system. Each user must first be enrolled in the system. Enrollment has three steps:

- Step 1 The reader scans each person's biometric data. This enrollment scan creates far too much data to use. In addition, the scan data will be different each time the user is scanned.
- Step 2 The reader then processes the enrollment scan data to extract a few key features from the mass of scanned data. These few key features, not the entire set of scanned data, will be used to identify or verify the user in the future.
- Step 3 The reader finally sends the key feature data to the database, which stores the key feature data as the user's template.

Why not use entire scans instead of key features? The problem is that entire scans are not very useful in raw form. If a person swipes his or her finger at different angles, raw scan files will be very different, but key features such as the relative locations of loops, arches, and whorls in fingerprints will be the same or almost the same no matter how a finger is scanned.

ISSN: 2277-9655
Impact Factor: 3.785

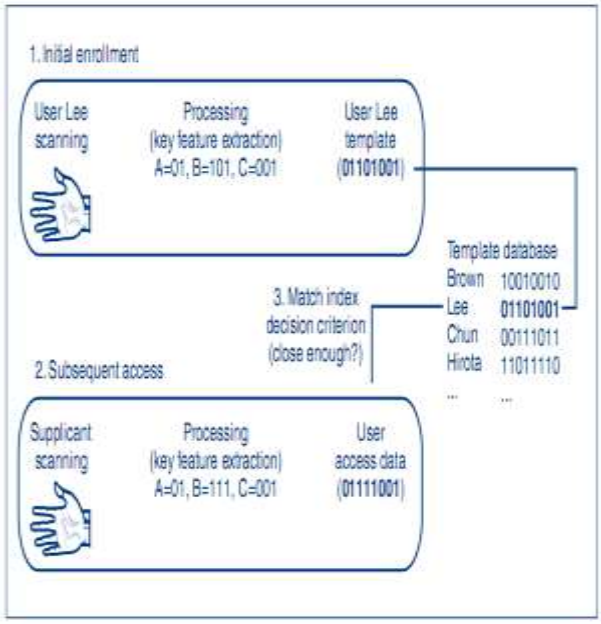

Fig. 1 Biometric Authentication System

Fig. 2: The enrollment process for a fingerprint reader

Figure 2 shows the enrollment process for a fingerprint reader on a Transcend JetFlash. The process is user-friendly and takes about three minutes. To complete the process, a user is required to swipe the same finger four times and enter a password.

SUBSEQUENT ACCESS ATTEMPTS

When users later wish to be authenticated, they are scanned again. The reader processes this supplicant scanning information to create key features. These key features become the user access data. The central system matches the user access data against the person's template in the database.

ISSN: 2277-9655
Impact Factor: 3.785

Fig. 3: Subsequent Access Attempt

ACCEPTANCE OR REJECTION

When a system receives access data, it computes a match index, which is the difference between the scan's key features and the template. There is never a perfect match, because scanning never works exactly the same way twice. If the error is smaller than a value called the decision criterion, the supplicant is accepted as a match. If not, the supplicant is rejected as a match.

Biometric Errors

Access control requires high accuracy. Unfortunately, there are many questions about the reliability of various types of biometric authentication. One issue [3] is error rate, which refers to accuracy when the supplicant is not trying to deceive the system. The other accuracy issue is the deception rate, which is the likelihood that an impostor will be able to deceive the system if he or she tries. For now, we will focus on error rates.

FALSE ACCEPTANCE RATE

An acceptance means that the person is matched to a particular template. As we have just seen, a false acceptance is a match to a template that should not be made. The rate of false acceptances as a percentage of total access attempts is called the false acceptance rate (FAR).

False acceptances have different implications for different uses, for instance, in door or computer access versus terrorist watch lists.

For access to a computer or a door, a false acceptance means an impostor is matched with a legitimate template and thereby given access. As a consequence, an impostor can get in (even without attempting deception). This is a serious security violation

For terrorist watch list matching, in contrast, a false acceptance means incorrectly matching a person to the list—in other words, incorrectly labeling an innocent person as a terrorist. This will inconvenience the person falsely matched, but it is not a security breakdown. If there are too many false acceptances, however, complaints may force the system to be discontinued.

For watch list access to an equipment room, in turn, false acceptances are security problems, while false rejections are merely inconvenient.

FALSE REJECTION RATE

In a false rejection, in turn, the supplicant is incorrectly rejected as a match to a template when the applicant should be accepted as a match. The false rejection rate (FRR), [5] then, is the probability that the system will reject a person who should be matched to a template.

•For instance, in access to a computer, a false rejection means that a legitimate user is denied access. Although not necessarily bad from a security viewpoint, a high FRR for computer or door access can lead to a great deal of user dissatisfaction, and this can kill the system.

•For watch lists, false rejection means that a person who should be identified as being on a watch list is not. If this is a terrorist watch list, this means that a terrorist goes unidentified. This is a serious security violation. If it is a door access watch list for an equipment room, then it is merely an inconvenience.

WHICH IS WORSE?

Which is worse, then—a false acceptance or a false rejection? It depends on the context. In door or server access, a false acceptance allows an attacker in and is a serious violation. A false rejection is simply an inconvenience. For terrorist watch list matching, however, a false rejection (a failure to match an attacker to a watch list template) is a major security violation. A false acceptance, in turn, is only a nuisance.

VENDOR CLAIMS

Unfortunately, vendor claims for FARs and FRRs can be misleading. They usually are based on idealized situations that are not representative of real-world conditions. For instance, we have seen that the false acceptance rate increases as the number of templates increases because there is a small false acceptance probability for each template. To take advantage of this, vendors may base FAR estimates on databases with only a few templates. In addition, vendors enroll users under ideal circumstances and have ideal situations for the access attempt. For instance, in face recognition, their test subjects might be very well lit and looking straight forward for both enrollment and access attempts conditions that are not likely to occur in the real world. This can make a vendor's reported false rejection rate lower than it would be in practice.

FAILURE TO ENROLL

There is another type of error, failure to enroll (FTE).This occurs if the system will not enroll a user. For instance, in the case of fingerprint authentication, some people do not have well-defined fingerprints due to age, years of construction labor, long clerical paper handling, or other reasons. In some cases, this can make a fingerprint authentication system useless.

VERIFICATION, IDENTIFICATION, AND WATCH LISTS

1. VERIFICATION

Biometric authentication [1] has one of three possible goals. In verification, a supplicant claims to be a particular person, and the challenge is to measure the supplicant's biometric access data against the template of the person he or she claims to be. When you log into a server with a username and password, this is verification.

Every time a match is attempted, there is a danger of a false match, meaning that the template data may match the applicant's access data when there should not be a match.

This danger usually is small, and because verification only matches the access data to a single template, there is only one chance of a false match.

To give an example, if the probability of a false acceptance is one in a thousand, then probability of a false acceptance is one in a thousand because only one match is attempted. There is a false acceptance rate (FAR) of 0.1 percent.

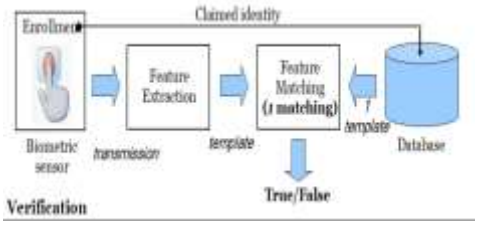

Fig. 4: Verification process

ISSN: 2277-9655
Impact Factor: 3.785

2. IDENTIFICATION

In identification, in contrast, the supplicant does not claim to be a particular person. It is [5] the job of the system to identify the supplicant, that is, to determine who he or she is.

In identification, the supplicant's biometric access data must be matched against the templates of everyone whose template is stored in the system. If the system finds no matches, it rejects the supplicant. In identification, the system makes many matches between the applicant's access data and the templates in the system. With each match, there is a small danger of a false match (false acceptance). Given the many matches required in identification compared with the single match required in verification, the chance of a false match is much higher in identification than it is in verification.

For example, suppose that the probability of a false match per template is 1/1,000. Suppose also that there are 500 templates in the database. Then there will be 500 match attempts, and the FAR will be 1/1,000 times 500, or 50 percent. This is 500 times the false acceptance rate for verification.

On the positive side, identification frees users from the need to type their names or account names. Identification is best for door access control and other situations in which identity claims cannot be made by the supplicant.

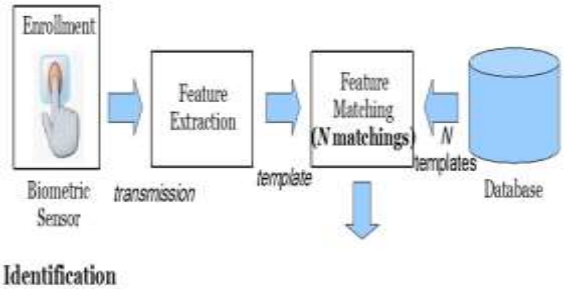

Fig. 5: Identification Process

3. WATCH LISTS

A limited but increasingly important form of identification is the watch list, which identifies a person as being a member of a group. For instance, the matches may be made against the templates of people on a terrorist watch list. Or, matches may be made against the members of a repair team who should be allowed to enter a room. Watch list matching makes more access data–template comparisons than verification and so is more prone to false acceptances. However, watch list matching makes fewer comparisons than full identification and so is less susceptible to false acceptances.

Biometric Deception

Although errors are a serious concern, deception is even more troublesome. A biometric system [5] with low error rates is useless if it can be deceived effectively with reasonable effort.

In deception, an attacker deliberately attempts to fool the system. For instance, many fingerprint scanners can be fooled if the adversary lifts a latent (present but not visible) fingerprint from a glass, puts it on a gelatin finger, and places the fake finger on the fingerprint scanner.

In watch list matching with a surveillance camera system at an airport, an attacker may walk into an airport and keep his or her head down and wear a brimmed hat to–deceive the matching algorithm. Real-world biometric deception rates are largely unknown, except for fingerprint scanners, for which deception frequently works using unsophisticated methods. Fortunately, for many assets, deception is not a critical issue. For instance, an ordinary person without sensitive information on a notebook computer is not likely to face a sophisticated attacker. In the case of notebooks without sensitive information, fingerprint readers mainly exist to eliminate passwords, which are too weak and are too frequently written down by users.

ISSN: 2277-9655
Impact Factor: 3.785

BIOMETRIC METHODS

1. FINGERPRINT RECOGNITION

Thanks to crime movies, almost everyone is familiar with fingerprint recognition. Fingerprint recognition technology is well developed and inexpensive. Fingerprint [2] scanners are cheap enough to be added to computers and even small handheld devices. Due to their low cost, fingerprint scanners account for most of the total biometrics market. Unfortunately, fingerprint recognition technology often is easy to deceive. In 2002, researchers were able to defeat 80 percent of fingerprint recognition systems by creating a gelatin finger from a latent print (i.e., an invisible print left on a glass or other object).12 Fingerprint readers that can better detect deception use measures such as measuring skin capacitance and even pulse rates. However, these types of fingerprint readers are expensive and so are less widely used. Given that fingerprint scanners can be deceived, we have noted that they should only be used in applications for which there is little danger of serious deception. An example would be logging into a personal computer that does not hold sensitive information.

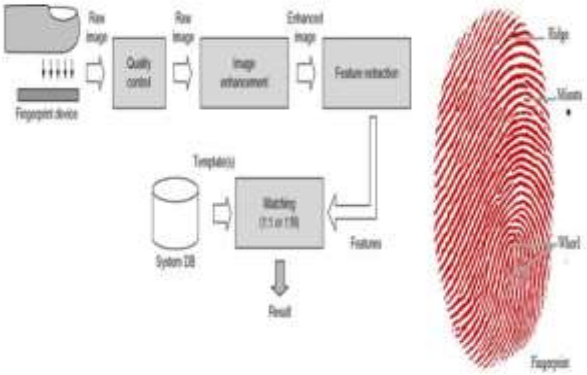

Fig. 6: Fingerprint recognition

2. IRIS RECOGNITION

The iris is the colored part of your eye. Irises are far more complex and individual than fingerprints. In fact, iris recognition is the most precise form of biometric authentication, with very low FARs. In general, iris scanning [4] is the gold standard in biometric authentication today. Unfortunately, like gold, it is expensive. Iris scanners can read iris patterns from several centimeters to a meter or so away. In movies, iris scanning typically is shown as a red laser beam shining into the supplicant's eye. This is complete nonsense. With iris scanners, people simply look into ordinary cameras. There is typically a small TV monitor to help the supplicant ensure that he or she is looking directly into the camera.

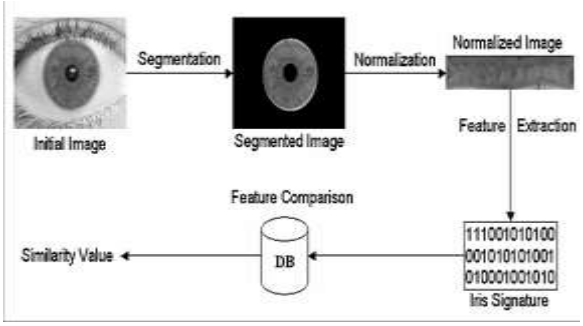

Fig. 7: Iris recognition

3. FACE RECOGNITION

Facial features can be read from several meters away. This makes face recognition useful for door access control. However, face recognition [2] is highly sensitive to lighting differences between the scanned image stored on the

ISSN: 2277-9655
Impact Factor: 3.785

computer and the situation in which the scan is taken. It also is moderately sensitive to changes in facial features such as facial hair, and it is often very sensitive to deception by people turning their faces away from the camera. The only major benefit of face recognition [4] is that it can be used surreptitiously, that is, without the subject's knowledge. This makes it seem to be good for surveillance cameras [11] searching for criminals and terrorists. However, its high error rates and the ease with which it can be deceived make its use for criminal and terrorist watch lists highly suspect.

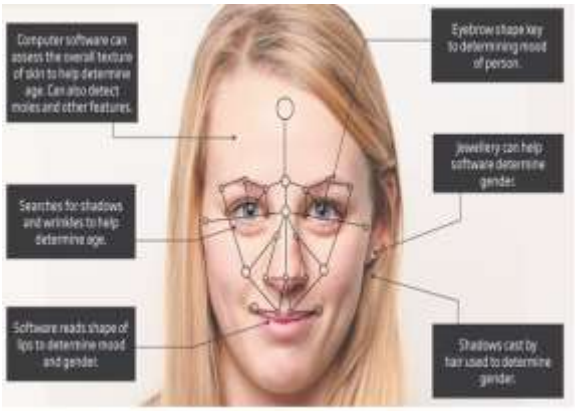

Fig. 8: Face recognition

4. HAND GEOMETRY

Human hand geometry, [4] including finger length, finger width, palm width, and other characteristics, is fairly easy to measure and is used mostly in door access control because of the size of hand geometry scanners. The user simply places his or her hand on a scanner that is the size of a textbook.

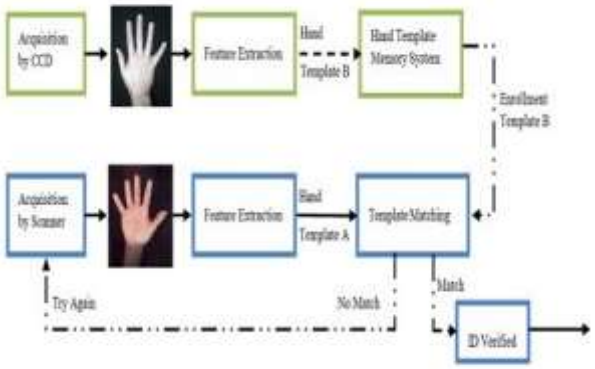

Fig. 9: Hand geometry

5. VOICE RECOGNITION

Fingerprint, iris, face, hand geometry, and vein recognition are examples of something you are. Voice recognition, in contrast, is based on something you do, namely speak.

Unfortunately, voice recognition is easily deceived by recordings. In addition, high false rejection rates make voice recognition frustrating to users.

ISSN: 2277-9655
Impact Factor: 3.785

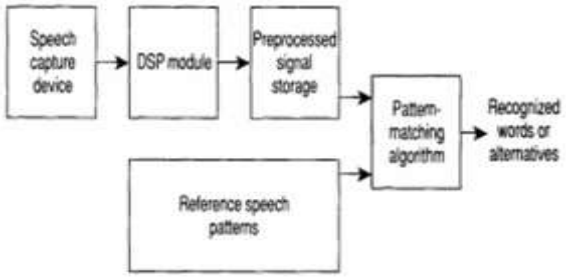

Fig. 10: Voice recognition

OTHER FORMS OF BIOMETRIC AUTHENTICATION

There are many other forms of biometric authentication the recognition of veins in the hand, keystroke recognition (typing pace between levels), written signature recognition, and the recognition of gait (way of walking), to name just a few. However, fingerprint, iris, face, and hand geometry are the most widely used types of biometric authentication today, and fingerprint recognition is dominant.

REFERENCES

[1] "Biometrics:Overview".*Biometrics.cse.msu.edu.*
[2] Bleicher, Paul (2005). "Biometrics comes of age: despite accuracy and security concerns, biometrics are gaining in popularity". *Applied Clinical Trials*..
[3] Technology Assessment Technology Assessment Using Biometrics for Border Security Using Biometrics for Border Security, November 2002
[4] Biometric Authentication Technology: From the Movies to Your Desktop by Fernando L. Podio and Jeffrey S. Dunn
[5] Zahid Akhtar, "Security of Multimodal Biometric Systems against Spoof Attacks", Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy, 6 March 2012
[6] Jain, A. K.; Bolle, R.; Pankanti, S., eds. (1999). *Biometrics: Personal Identification in Networked Society*
[7] *Bleicher, Paul (2005). "Biometrics comes of age: despite accuracy and security concerns, biometrics are gaining in popularity". Applied Clinical Trials..*
[8] Face Recognition 101: A Brief Primer by Duane M.
[9] Mordini E, Tzovaras D,(2012), *Second Generation Biometrics: the Ethical and Social Context*. Springer-Verlag: Berlin.
[10] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", *IBM Systems Journal*
[11] M. A. Dabbah, W. L. Woo, and S. S. Dlay, "Secure Authentication for Face Recognition", presented at Computational Intelligence in Image and Signal Processing