IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol-6, Special Issue-5, Jun 2018 E-ISSN: 2347-2693

Biometric Based on Fingerprint

Samiksha Suri

Lect. Computer Applications, Gdc (Boys) Udhampur, India

Available online at: www.ijcseonline.org

Abstract: Security has always been a major concern for authentication over networking. Fingerprints are one of the biometrics which plays an important role in identifying a person based on some minutiae features. This is one of the most commonly used algorithms for extracting features that characterizes a fingerprint. This biometrics has several applications like e-governance, commercial and forensic. The fingerprint biometric offers a higher degree of security and personal privacy. Emerging privacy concerns with the database acquisition and lack of availability of large scale fingerprint databases have posed challenges in exploring this technology for large scale applications. Fingerprint recognition looks for the unique patterns of ridges and valleys that are present in an individual's fingerprint. These patterns are unique to every individual and thus help to identify individuals from an entire population. Verification and identification are the two ways in which an individual's identity can be determined using biometric technology. This research also developed user-friendly software to synthesize fingerprint databases, which could help to advance further research in fingerprint biometrics.

Keywords: Biometric, Authentication System, Fingerprint recognition, Minutiae Based, Biometric security system, Identification access control.

I. Introduction To Fingerprint Biometric

Biometrics is derived from the Greek words ―bio (life) and ―metrics (to measure).Biometrics is a term that encompasses ―the application of modern statistical methods to the measurements of biological objects‖. However, by language misuse, the term biometrics usually refers to automatic technologies for measuring and analyzing biological and anthropological characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for identity prove. Biometrics refers to ―Identifying an individual based on his or her distinguishing characteristics. Ideally the biometric characteristics used should satisfy the following properties: Robustness Over time, the characteristic should not change (Permanence), and thus have low intra-class variability. Distinctiveness Over the population, a great variation of the characteristic should exist (Uniqueness), and thus have large inter-class variability [1]. Availability ideally, the whole population should possess the characteristic (Universality). Accessibility The characteristic should be easy to acquire (Collectability). The characteristics could be physiological or behavioral. Characteristics, which can be measured on a part of the body at some point in time (passive), are physiological biometrics. On the other hand, characteristics, which are learned or acquired over time (active), are called behavioral. For example, fingerprint, hand geometry and face are physiological biometrics, while dynamic signature, gait, keystroke dynamics and lip motion are behavioral once.

II. Concept Based On Fingerprint Biometric

Enrollment Refers to the entire process of capturing a fingerprint image, extracting relevant data, creating a record with user information, and storing the record to memory. Overall system performance will be increased by also evaluating the quality of enrollment before deciding to store the record. Verification (Authentication). This is the operation of comparing a live fingerprint against the corresponding record stored during enrollment. A result of pass or fail is returned based on whether the score was above a pre-defined threshold value. Scanning an Image When the reader properly reads a fingerprint; it looks for image quality and fingerprint content. When a raw image is collected from the sensor, the reader searches for the fingerprint core. Proper Finger Placement The basics for

successful operation of the fingerprint readers are simple but important. System performance improves dramatically with consistent finger placement. It is important to make sure that the position of the finger allows the reader to record the unique features of the print. Here are the steps to follow for trouble-free fingerprint recognition. Bioscrypt has designed the Ridge-Lock to create "simple user instruction" and "consistent" finger position. With the fingertip raised, slide the finger across the RidgeLock, until it "locks" into place within the first indentation of the finger. Next, lower the finger onto the sensor and apply moderate pressure. Common mistakes correct finger placement is a significant component for reliable fingerprint imaging. The following list some common mistakes to avoid. Sliding the fingertip into place instead of lowering it onto the sensor will cause distortion of the• fingerprint and will degrade image quality. Keep the fingertip raised while locating the Ridge-Lock, and then lower the fingertip. Rotating the finger into position also will cause distortion of the fingerprint, subsequently making• verification less reliable. Positioning the finger to one side and leaving a portion of the sensor exposed will degrade image• quality. Placing the finger at an angle to the finger guide is another common mistake. Rotation of the fingertip• will not provide a reliable image of the fingerprint. Image Quality The quality score is based on how well the ridge pattern is defined within the fingerprint image that was enrolled. In other words, quality measures how clearly the reader imaged the fingerprint. Poor quality enrollments can result in an elevated rate of false rejection making it difficult for the user to verify reliably. For best image quality, be sure that the sensor window is clear of dirt, residue, or other material that can block the reader's view of the fingerprint Dry skin is another factor that can contribute to an unreliable image of a fingerprint. A normal amount of moisture on the skin makes the ridges and valleys of the fingerprint stand out to the sensor. Too little moisture makes the image "noisy" and will cause the reader to reject the image during processing [4]. Lightly moisturizing the finger will enhance the contrast of the print and provide more reliable verification. The increased sensitivity of the silicon sensor is dramatically reducing problems in this area. Content The Content score is based upon the amount of usable information the reader sees in the fingerprint. Templates that are characterized by low content scores may result in elevated rates of false acceptance. The higher the content, the greater the degree of useful information. Image Consistency Once a user's fingerprint template has been enrolled, the best performance in the candidate matching process depends on consistency. Obviously, the user must use the same finger for ID verification as was used to form the original template. It also is important to position the finger correctly for each verification, as was done when the template was originally enrolled.

1. Biometric Fingerprint Scanner

Nothing is completely secure. Locks can be picked, safes can be broken into, and online passwords can be guessed sooner or later. How, then, can we protect the things that we value? One way is to use **biometrics**—fingerprints, iris scans, retinal scans, face scans, and other personal information that is more difficult to forge. Not so long ago, if you'd had your fingerprints taken, chances are you were being accused of a crime; now, it's innocent people who are turning to fingerprints to protect themselves. And you can find fingerprint scanners on everything from high-security buildings to ATM machines and even laptop computers. Let's take a closer look at how they work!

III. How Does A Fingerprint Scanner Work

The fingerprint recognition involves snapping an image using a fingerprint scanner which is then digitally compared with a previously stored snapshot of your fingerprints. The scanner processor sees whether the loops, whorls and curves have any similarity. An important point to be noted is that the scanner doesn't keep the complete image of your fingerprint. It only stores information about specific points in the form of binary numbers.
Many fingerprint recognition technologies have been developed but only a few of them have seen a widespread implementation. Let's have a look at these:

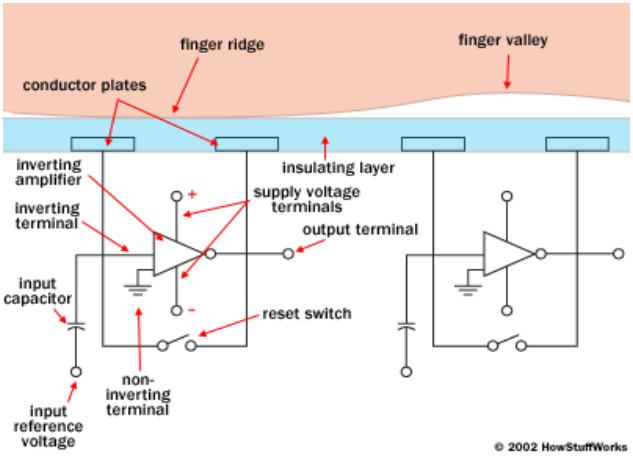
IV. Optical Fingerprint Scanners:

These type of scanners use visible light to take a photo of your fingerprints. In this, LEDs are used to illuminate a finger kept on a glass plate. The light reflected from the

finger falls onto a Charged-Coupled Device (CCD) present in the scanner. A CCD – also used in camcorders and digital cameras – is basically an array of pixels which respond to falling light over them and generate proportional electrical signals. These signals are then processed to create a digital imprint of your finger known as a "live scan".

The inverted image so created by the finger sensor represents the ridges – elevated regions – as dark coloured and valleys – depressed regions – as light coloured. You can think of it as a black and white image. One major issue that hampers the quality of the scan is that if the fingerprints are erased, lost due to burns or if the fingers are dirty. This would degrade the accuracy of the fingerprint scanner. Other types of sensors like Capacitive and Ultrasonic provide a solution for this problem. The final image generated should have appropriate darkness level and adequate sharpness to get qualified. If it fails to meet the standards, the image is discarded and sensors settings are adjusted to get the appropriate image in the next shot.

V. Capacitive Fingerprint Scanner



Like optical scanners, capacitive fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead of sensing the print using light, the capacitors use electrical current.

The diagram below shows a simple capacitive sensor. The sensor is made up of one or more semiconductor chips containing an array of tiny cells. Each cell includes two conductor plates, covered with an insulating layer. The cells are tiny -- smaller than the width of one ridge on a finger.

The sensor is connected to an integrator, an electrical circuit built around an inverting operational amplifier. The inverting amplifier is a complex semiconductor device, made up of a number of transistors, resistors and capacitors. The details of its operation would fill an entire article by itself, but here we can get a general sense of what it does in a capacitance scanner. (Check out this page on operational amplifiers for a technical overview.)

Like any amplifier, an inverting amplifier alters one current based on fluctuations in another current (see How Amplifiers Work for more information). Specifically, the inverting amplifier alters a supply voltage. The alteration is based on the relative voltage of two inputs, called the inverting terminal and the non-inverting terminal. In this case, the non-inverting terminal is connected to ground, and the inverting terminal is connected to a reference voltage supply and a feedback loop. The feedback loop, which is also connected to the amplifier output, includes the two conductor plates.

As you may have recognized, the two conductor plates form a basic capacitor, an electrical component that can store up charge (see How Capacitors Work for details). The surface of the finger acts as a third capacitor plate, separated by the insulating layers in the cell structure and, in the case of the fingerprint valleys, a pocket of air. Varying the distance between the capacitor plates (by moving the finger closer or farther away from the conducting plates) changes the total capacitance (ability to store charge) of the capacitor. Because of this quality, the capacitor in a cell under a ridge will have a greater capacitance than the capacitor in a cell under a valley.

To scan the finger, the processor first closes the reset switch for each cell, which shorts each amplifier's input and output to "balance" the integrator circuit. When the switch is opened again, and the processor applies a fixed charge to the integrator circuit, the capacitors charge up. The capacitance of the feedback loop's capacitor affects the voltage at the amplifier's input, which affects the amplifier's output. Since the distance to the finger alters capacitance, a finger ridge will result in a different voltage output than a finger valley.

The scanner processor reads this voltage output and determines whether it is characteristic of a ridge or a valley. By reading every cell in the sensor array, the processor can put together an overall picture of the fingerprint, similar to the image captured by an optical scanner.

The main advantage of a capacitive scanner is that it requires a real fingerprint-type shape, rather than the pattern of light and dark that makes up the visual impression of a fingerprint. This makes the system harder to trick. Additionally, since they use a semiconductor chip rather than a CCD unit, capacitive scanners tend to be more compact that optical devices.

VI. Ultrasonic Fingerprint Scanners

The latest fingerprint scanning technology to enter the smartphone space is an ultrasonic sensor, which was first announced to be inside the Le Max Pro smartphone. Qualcomm and its Sense ID technology are also a major part of the design in this particular phone.

To actually capture the details of a fingerprint, the hardware consists of both an ultrasonic transmitter and a receiver. An ultrasonic pulse is transmitted against the finger that is placed over the scanner. Some of this pulse is absorbed and some of it is bounced back to the sensor, depending upon the ridges, pores and other details that are unique to each fingerprint. There isn't a microphone listening out for these returning signals, instead a sensor that can detect mechanical stress is used to calculate the intensity of the returning ultrasonic pulse at different points on the scanner. Scanning for longer periods of time allows for additional depth data to be captured, resulting in a highly detailed 3D reproduction of the scanned fingerprint. The 3D nature of this capture technique makes it an even more secure alternative to capacitive scanners.

While this technology is still yet to appear in a commercial handset, Vivo has shown off a concept model that includes Qualcomm's ultrasonic in-display fingerprint scanner. Although not as snappy as other scanners yet, partly due to the reasons mentioned above, Vivo's prototype manages to hide the scanner under the smartphone's display, which could be a particularly useful feature as handsets move towards smaller and smaller bezels. Speaking of under the screen sensors, both Samsung and LG are working on their own in-house technologies too.

VII. Literature Review of Biometrics

The main objective of the present study is —

To develop multimodal biometrics using fingerprint and face recognition with neural network architecture. The researcher has studied a lot of related literature to understand the related work in this area. This study has cleared the idea of the work. Here is the brief of literature review.

According to Chirillo and Blaul (2003, p. 3) "the term biometrics is derived from the Greek words bio (life) and metric (to measure)." China is among the first known to practice biometrics back in the fourteenth century as reported by the Portuguese historian Joao de Barros. It was called member-printing where the children's palms as well as the footprints were stamped on paper with ink to identify each baby. Alphonse Bertillon, a Paris based anthropologist and police desk clerk was trying to find a way of identifying convicts in the 1890s decided to research on biometrics. He came up with measuring body lengths and was relevant till it was proved to be prone to error as many people shared the same measurement. The police started using fingerprinting developed based on the Chinese methods used century before by Richard Edward Henry, who was working at the Scotland Yard.

Raina, Orlans and Woodward (2003, p. 25-26) stated references to biometrics as a concept could be traced back to over a thousand years in East Asia where potters placed their fingerprints on their wares as an early form of brand identity. They also pointed Egypt's Nile Valley where traders were formally identified based on physical characteristics such as eye color, complexion and also height. The information were used by merchant to identify trusted traders whom they had successfully transacted business with in the past. Kapil et al also made references to the Bible, first pointing to the faith Gileadites had in their biometric system as reported in The Book of Judges (12:5-6) that the men of Gilead identified enemy in their midst by making suspected Ephraimites say "Shibboleth" for they could not pronounce it right. The second reference is to The Book of Genesis (27:11-28) where Jacob pretended to be Esau by putting goat skins on his hands and back of his neck so his skin would feel hairy to his blind, aged father's touch. This illustrates a case of biometric spoofing and false acceptance. They finally wrote "Biometrics as a commercial, modern technology has been around since the early 1970's when the first commercially available device was brought to market" (p. 26).

VIII. Research Methodology

The research methodology designed for this dissertation is mainly the qualitative approach. A quantitative approach has been overlooked due to limited time as designing surveys, distribution take time and response time could not

be predicted. Therefore, my effort will be concentrated on critically reviewing previous literatures in order to acquire an overview of, and intakes on the topic. For more details, Journals, Books, Publications, Documentaries and previous dissertations related to the topic will be reviewed, compared and analyzed. The objectives will be achieved by purely reviewing literatures and previous researches and the literatures critically analyzed by comparing information obtained from different sources. Findings, recommendations and conclusions will be made from the analysis.

IX. Objectives of The Study

The main aim of this research focus on critically analysis of biometric security as an emerging and booming industry by examining the positives and negatives and providing ways of improving the method effectively and most importantly efficiently. Since biometrics applies to many applications, access control will be the main focus of this dissertation. Also, issues such as privacy, laws governing biometrics and standards will be examined.

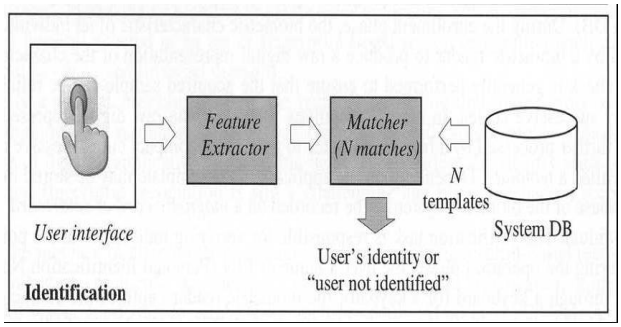
The main objectives of this research are;

1. To review biometric security and issues related to it.
2. To evaluate the threats, advantages and disadvantages of biometrics.
3. To propose ways of improving the effectiveness and efficiency of biometrics from previous researches.

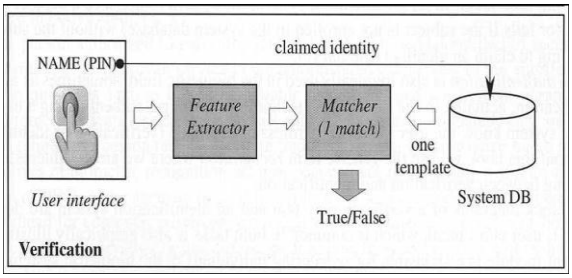
X. Use of Biometrics

A biometric system is essentially a pattern-recognition system. Such a system involves three aspects: data acquisition and preprocessing, data representation, and decision-making. It can thus compare a specific set of physiological or behavioral characteristics to the characteristics extracted beforehand from a person, and recognize this last one. The digital representation recorded in a database, which describes the characteristics or features of a physical trait, is defined as a template. It is obtained by a feature extraction algorithm. Biometric systems are traditionally used for three different applications: physical access control for the protection against unauthorized person to access to places or rooms, logical access control for the protection of networks and computers, and time and attendance control. An authentication procedure can be performed in two modes by a biometric system [3].

1. Identification: - This method consists in selecting the correct identity of an unknown person from a database of registered identities (Figure 1.1). It is called ―one to many‖ matching process, because the system is asked to complete a comparison between the person‘s biometrics and all the biometric templates stored in a database. The system can take either the ―best‖ match, or it can score the possible matches, and rank them in order of similarity. Two modes are
possible, positive and negative identification. The positive identification tends to determine if a given person is really in a specific database. Such a method is applied when the goal is to prevent multiple users of a single identity. A negative identification determines if a given person is not in a ―watch list‖ database. Such a method is applied for example when the goal is to identify persons registered under several identities.



2. VERIFICATION:- This method consists in verifying whether a person is who he or she claims to be (Figure 1.2). It is called a ―one to one‖ matching process, as the system has to complete a comparison between the person‘s biometric and only one chosen template stored in a centralized or a distributed database, e.g. directly on a chip for an identity document. Such a method is applied when the goal is to secure and restrict specific accesses with obviously cooperative users.



XI. Importance of The Study

Importance of the study can be identified as:

1. With the help of this multimodal biometric system, we can minimize the error rate present with unimodal biometric technologies like fingerprint and facial recognition.
2. This model will be cost effective, because it will need fingerprint scanner and webcam for registration. Page 9

3. Neural network model will help to maintain the weight of important trait for authentication.
4. Backpropagation in the neural network model will adjust the weights of traits based on false rejection. This will in turn minimize the FRR and FAR.
5. The same model will also be useful to create multimodal biometric systems with other traits like palmprint, hand geometry, voice and keystroke recognition.
6. This system will be useful for authentication in areas where it is hard to capture any single trait and perform authentication. It will be possible to identify the person even if any one trait is not clear.

XII. Fingerprint Recognition

Fingerprints it is known since a long time that fingerprints of humans are unique. They can be distinguished by the epidermal ridge and furrow structure of each finger, which is used to categorise fingerprints as shown in figure 2. Even identical twins don't have the same fingerprint. Fingerprints are therefore widely used to identify people since a long time. They are even accepted by law to prove evidence, which makes them a powerful tool for forensics. [JHPB97][2]. For electronically processing fingerprints using image recognition algorithms, a fingerprint has to be scanned first. There exist different fingerprint scanners, e.g. capacitive, optical and thermal, each using a different technology. An images gained by a scanner is further processed by a feature extractor which reduces the image to a set of minutiae points (e.g. end points or bifurcation ridges). The set of these points is a compact and expressive representation of the fingerprint which is saved and used for the authentication process. [OGBRGR04] Figure 2: The picture shows 3 different categories of fingerprints - left loop, whorl and twinloop[12].

A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching pattern; others use straight minutiae matching devices; and still others are a bit more unique, including things like moiré fringe patterns and ultrasonic characteristics. A greater variety of fingerprint devices is available than for any other biometric technology.

XIII. How It Works

Fingerprint systems translate illuminated images of fingerprints into digital code for further software such as enrolment (fingerprint registration) and verification (authentication or verification of registered users).

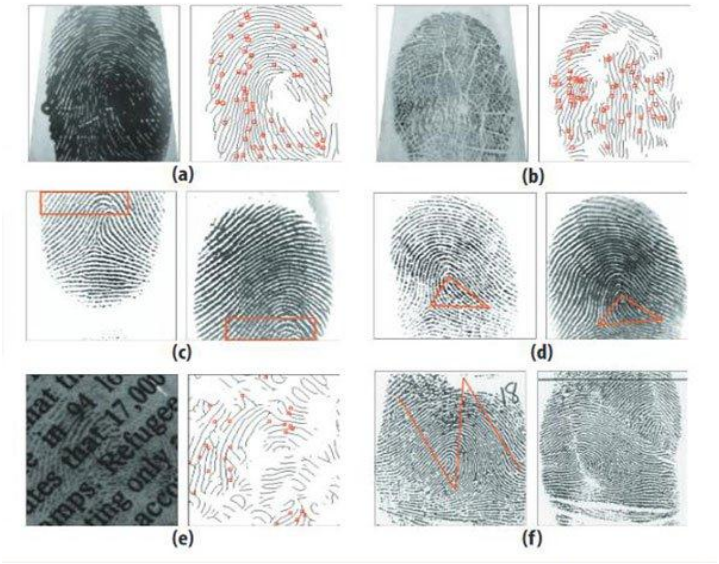
The scanner uses an advanced CMOS image sensor to capture high contrast, high resolution fingerprint images that are virtually distortion-free. A series of powerful algorithms extract data from the image, mapping the distinguishing characteristics of the fingerprint [24].

This data is then converted into an encoded binary string known as a digital template, and stored in a database. The actual fingerprint image is never stored. To identify or verify a fingerprint, a proprietary matching algorithm compares the new template made from the extracted characteristics from the input fingerprint on the optical module to a previously stored sample. The entire matching process takes roughly one second. Authentication takes place locally at the device or on a server, depending on system configuration.

XIV. Factors That Influence Fingerprint Image Quality

Fingerprint is the pattern formed by friction ridges on the surface of a fingertip. A good quality fingerprint image has distinguishable patterns and features that allow the extraction of features that are useful for subsequent matching of fingerprint pairs. Fingerprint image quality can be influenced by several factors like environmental, behavioral, quality of biometrics presented, system ability, etc. Some of the factors, affecting the fingerprint image quality and eventually the matching performance, can be addressed at user end, for example, subject might have wet fingers rendering biometric system unable to scan, so drying up fingers prior to sample collection will enhance quality of captured image[20]. Environmental factors like operating the equipment in extreme environmental conditions; scratched or smudged scanning surface, etc., can also be addressed at operator or user end. Factors like system's ability to resolve details, efficiency of biometric algorithm, worn off fingerprints due to disease or age, etc. cannot be intervened by a user hence there's nothing much that can be done at user end.

Image: Challenges in automated fingerprint processing: (a) wet fingerprint (left) and extracted features (right); (b) fingerprint with many cuts (left) and extracted features (right); (c) small overlapping area as marked by rectangles; (d) large nonlinear distortion in fingerprint patterns as indicated by the corresponding triangles; (e) latent fingerprint with overlapping letters (left) and the extracted



features (right); (f) altered fingerprint: a criminal made a Z-shaped incision into each of his fingers (left), switched two triangles, and stitched them back into the finger (right). Credit: Department of Computer Science and Engineering at Michigan State University

Maintaining high level of performance in verifying conditions for all population groups is a major challenge in fingerprint recognition[22]. There is one thing common in all the factors that influence fingerprint image quality is that they somehow affect the process of image capturing, let it be environmental, technical or the user behavior. Poor image capture further results in poor feature extractions and inadequately sampled biometric data. Even in manual capture of fingerprints, which has been a common application in law enforcement, a proper capture of fingerprints is an essential requirement. Captured digitally or manually, high quality image of fingerprint features can result in improved performance of automated biometric system as well as in manual matching [23].

Electronic capture of fingerprints is not only more efficient but also produces high quality images than the manual

process; however, image quality may still be hampered by certain conditions and factors.

For example:

- Operating the equipment in harsh environmental conditions like extreme heat, cold, light or humidity, beyond standard operating conditions.
- User behavior, like presenting moist, greasy or dirty fingers to scanner.
- The way fingertip is placed on the scanning surface and amount of pressure applied by the user can also affect the quality of scanned image.
- Equipment is not regularly maintained, dirty, smudged, or scratched scanning surface.
- If the user is suffering from disease affecting quality of friction ridges. Age is also a factor; fingerprint samples obtained from elderly population are mostly of inferior quality in comparison with a younger 18-25 year old population.
- Sensor type, technology and specifications of the acquisition device.
- Lack of training, users' unfamiliarity with sample acquisition process or a device that does not facilitate easy and correct user interaction may result in highly variable acquisitions.

XV. Advantages and Disadvantages

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. Nataliya B. Sukhai for example writes in her article that there are many people who would hesitate using fingerprints for authentication because fingerprints are associated with criminals. Other people would never use an iris scanner, because they are afraid that the light used to scan the iris is harmful for the eyes. [Suk04] Another disadvantage is the high cost of biometric authentication technologies. The article [Hir05] 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. [Suk04] 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. [Hir05] One more disadvantage not yet mentioned, is the problem of integrating biometric authentication into corporate infrastructures. According to the article of Clare Hist [Hir05] 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 desireable 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 [Woo97]. In addition to that 10 people can't write them down ("25% of the people appear to write their PIN on their ATM card" [JHP00]) 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."[Hir05] In addition to that biometric authentication systems reduce costs because it is possible to eliminate overheads resulting from password management [Hir05]. 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.

XVI. Conclusion and Outlook

Fetching a fingerprint match is dependent on several factors, however, fingerprint image quality plays a pivotal role in successful matching. Other sub-systems of a biometric system depend on the quality of acquisition by the data capture sub-system. A poorly sampled fingerprint image not only hampers matching efficiency, but also results in poor performance by the overall system. Ensuring that sampled fingerprint image is of the highest possible quality is a crucial aspect, especially during the enrollment as subsequent matching operations post enrollment are compared against what is enrolled.

If fingerprint data presented for enrollment is of inferior quality, the system may not let it enroll at all, resulting in Failure to Enroll (FTE). Even if inferior quality fingerprint data is enrolled, there will be higher number of false non-match cases post enrollment, posing system as inefficient. If enrolled sample is of high quality and during the verification process, probe is also of high quality then it will give high comparison scores, but when high quality enrolled sample and a low quality probe is compared it is likely to yield a low comparison score, hence it is hard to assign high quality and low quality appropriately when it is not known beforehand which sample the comparison will be made with. Therefore high quality capture of fingerprints is important for both enrollment as well as verification process.

Fingerprint identification systems are very sensitive to the noise or to the quality degradation, since the algorithms' performance in terms of feature extraction and matching generally relies on the quality of fingerprint images. Technological advancement can always assist with keeping image quality at acceptable level. Early recognition system were more sensitive to environmental and other factors, however, new biometric fingerprint recognition systems come with improved fingerprint sensors, which have more tolerance against environmental and behavioral factors. Newer sensors are constructed in such a way that they are resistant to even high amounts of moisture on the sensing surface without compromising the fingerprint image quality.

References

[1] The Biometric Consortium, "Introduction to Biometrics", (http://www.biometrics.org), 2006.
[2] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition", Springer, London, 2009.
[3] Samir Nanavati, Michael Thieme, and Raj Nanavati, "Biometrics: Identity Verification in a Networked World", John Wiley & Sons, 2002.
[4] Julian Ashbourn, "Biometrics: Advanced Identity Verification", Springer-Verlag, London, 2002.
[5] Edmund Spinella, "Biometric Scanning Technologies: Finger, Facial and Retinal Scanning", SANS Institute, San Francisco, CA, 2003.
[6] Peatman, John B., "Design with PIC Microcontrollers", Pearson Education, India, 1998.
[7] "Biometrics Overview." National Science and Technology Council. http://www.biometricscatalog.org/ NSTCSubcommittee/Documents/Biometrics%20Overview.pdf.
[8] "Doubt cast on fingerprint security." BBC News, May 17, 2002. [3] Jain, Anil K. and Sharathchandra Pankanti. "A Touch of Money." IEEE Spectrum, July 2006. p. 22-27.
[9] "Biometrics Standards." National Science and Technology Council. http://www.biometricscatalog.org/ NSTCSubcommittee/Documents/biometrics%20standards.pdf.
[10] Prabhakar, S.; Pankanti, S.; Jain, A.K. "Biometric recognition: security and privacy concerns." Security & Privacy Magazine, IEEE Volume 1, Issue 2, Mar-Apr 2003, p. 33-42.
[11] F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "Quality measures in biometric systems," vol. 10, no. 6. IEEE, 2012, pp. 52–62.
[12] L. Coetzee and E. C. Botha, "Fingerprint recognition in low quality images," vol. 26, no. 10. Elsevier, 1993, pp. 1441–1460.
[13] K. Karu and A. K. Jain, "Fingerprint classification," vol. 29, no. 3. Elsevier, 1996, pp. 389–404.
[14] L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 20, no. 8, pp. 777–789, 1998.
[15] C. I. Watson, M. D. Garris, E. Tabassi, C. L. Wilson, R. M. Mccabe, S. Janet, and K. Ko, "User's guide to nist biometric image software (nbis)," 2007.
[16] P. Grother and E. Tabassi, "Performance of biometric quality measures," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 29, no. 4, pp. 531–543, 2007.

[17] A. J. Willis and L. Myers, "A cost-effective fingerprint recognition system for use with low-quality prints and damaged fingertips," vol. 34, no. 2. Elsevier, 2001, pp. 255–270.

[18] K. Ito, A. Morita, T. Aoki, T. Higuchi, H. Nakajima, and K. Kobayashi, "A fingerprint recognition algorithm using phase-based image matching for low-quality fingerprints," in Image Processing, 2005. ICIP 2005. IEEE International Conference on, vol. 2. IEEE, 2005, pp. II–33.

[19] D. Zhang, F. Liu, Q. Zhao, G. Lu, and N. Luo, "Selecting a reference high resolution for fingerprint recognition using minutiae and pores," vol. 60, no. 3. IEEE, 2011, pp. 863–871.

[20] Q. Zhao, F. Liu, and D. Zhang, "A comparative study on quality assessment of high resolution fingerprint images," in Image Processing (ICIP), 2010 17th IEEE International Conference on. IEEE, 2010, pp. 3089–3092.

[21] R. M. Bolle, S. U. Pankanti, and Y.-S. Yao, "System and method for determining the quality of fingerprint images," Oct. 5 1999, uS Patent 5,963,656.

[22] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, and J. Bigun, "Kernel-based multimodal biometric verification using quality signals," in Defense and Security. International Society for Optics and Photonics, 2004, pp. 544–554. ,29794-1:2009, "Information technology – biometric sample quality – part 1: Framework," October 2009.

[23] A. K. Jain and S. Z. Li, Encyclopedia of Biometrics: I-Z. Springer, 2009, vol. 1. [23] E. Tabassi, C. Wilson, and C. Watson, "Nist fingerprint image quality," NIST Res. Rep. NISTIR7151, 2004.

[24] G. Li, B. Yang, and C. Busch, "Autocorrelation and dct based quality metrics for fingerprint samples generated by smartphones," in Digital Signal Processing (DSP), 2013 18th International Conference on. IEEE, 2013, pp. 1–5.

[25] Z. YAO, C. Charrier, and C. Rosenberger, "Utility validation of a new fingerprint quality metric," in International Biometric Performance Conference 2014. National Insititure of Standard and Technology (NIST), April 2014.

[26] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Bigun, "A comparative study of fingerprint image-quality estimation methods," Information Forensics and Security, IEEE Transactions on, vol. 2, no. 4, pp. 734–743, 2007.

[27] L. Shen, A. Kot, and W. Koo, "Quality measures of fingerprint images," in IN: PROC. AVBPA, SPRINGER LNCS-2091, 2001, pp. 266–271.

[28] B. Lee, J. Moon, and H. Kim, "A novel measure of fingerprint image quality using the Fourier spectrum," in Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, ser. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, A. K. Jain and N. K. Ratha, Eds., vol. 5779, Mar. 2005, pp. 105–112.

[29] Z. Yao, J. Le Bars, C. Charrier, and C. Rosenberger, "Quality assessment of fingerprints with minutiae delaunay triangulation," in International Conference on Information Systems Security and Privacy (ICISSP), Feb 2015.

[30] N. K. Ratha and R. Bolle, Fingerprint image quality estimation. IBM TJ Watson Research Center, 1999.

[31] H. Fronthaler, K. Kollreider, and J. Bigun, "Automatic image quality assessment with application in biometrics," in Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on. IEEE, 2006, pp. 30–30.

