6

Application of Contactless Fingerprinting

S. Mil'shtein, A. Pillai, V. Oliyil Kunnil, M. Baier and P. Bustos
Advanced Electronic Technology Center, ECE Dept., University of Massachusetts, Lowell USA

1. Introduction

There is an established belief that biometrics, specifically fingerprinting, was invented in 1900 by Sir Francis Galton. But in fact, the Chinese played a large role in biometrics' history. About 400 years B.C. the Chinese emperor was using his fingerprint as an official signature on the imperial documents (Onin.com). There were no cases on record identifying somebody attempting to falsify this unique signature or attempted to construct a decoy. It may well be that respectful handling of the emperor's signature is not an indication of strength of biometric technology rather a proof that copying and cheating were not acceptable in the culture of early Chinese civilization.

The major development of fingerprint technology in the form of wet-ink fingerprinting was initiated and improved for forensic applications by Scotland Yard about 100 years ago. However, the development of new fingerprinting methods has happened in recent years and continues to evolve. Fingerprint recognition technology is an integral part of criminal investigations. It is the basis for the design of numerous security systems in both private and public sector. It is also seen as an important tool for a variety of government organizations including Homeland Security, Immigration, Naturalization Services, and the Armed Forces, where fingerprinting procedures are used for recognition and verification of the identity for employees of federal departments and private contractors. In addition, the growth of the internet has made it necessary to verify the identity of individuals online. The simplest form of individual verification is the use of a password; however, this does not provide high levels of security. In the U.S., where the internet is widely used, an average citizen holds eleven passwords. Individuals tend to choose passwords that are easy to remember which makes them more vulnerable to online attacks. This is exacerbated by the fact that cybercrime is increasing. It is the recognition of this inherent security flaw which amplifies the need to use biometrics in securing network communications.

After the tragic events of September 11, 2001, the need for improved and reliable fingerprint recognition technology drastically increased. We witnessed the replacement of wet ink fingerprinting by digitized contact-based methods. (S. Mil'shtein and U. Doshi, 2004) did a study which emulated the fingerprinting procedure used with computer optical scanners, it was found that on average the distance between ridges decreases about 20% when a finger is positioned on an imaging surface. Using calibrated silicon pressure sensors, the distribution of pressure across a finger was scanned pixel by pixel, and a map of average pressure distribution on a finger during fingerprint acquisition was created. This demonstrated that it is impossible to replicate the same distribution of pressure across a finger during repeated fingerprinting procedures. Unfortunately, most fingerprints stored in current databases were acquired by contact-based methods using computer scanners and carry at least 20% distortion even if the finger is not pressed forcefully against the scanner. If a large force is applied, as in cases with non-cooperative individuals, the distortion is worse. In order to avoid pressure induced distortion we developed a line of unique contactless fingerprint scanners where rolled fingerprint equivalent images are recorded in less than one second. In (Yang and Park, 2008 as well as Nanni and Lumini, 2009), non-minutiae based methods have been proposed to overcome invariance.

Although fingerprinting is the most widely used biometric technique the common belief of law enforcement officials is that multi-modal biometrics is the future of this technology, i.e. the combination of fingerprinting with other types of biometric data such as face recognition or retina identification as mentioned by (Ross and Jain, 2004). This belief can explain the dynamics of the market's development, as illustrated in Figure 1. The global biometrics market experienced a growth from $1.95 billion in 2006 to around $2.7 billion at the start of 2008 (Techbiometric.com). Due to an annual growth rate of 21.3%, biometrics manufacturers are expected to achieve an impressive figure of $7.1 billion in revenue by 2012.

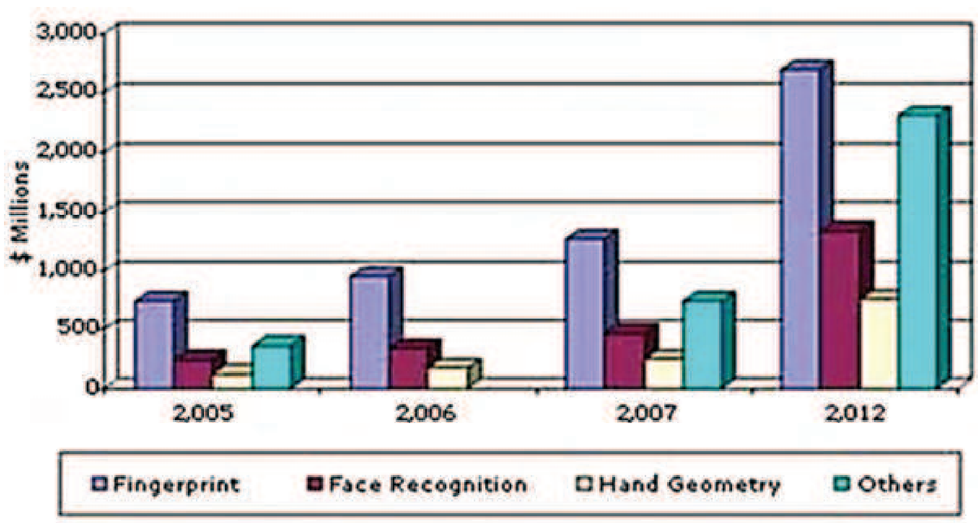


Fig. 1. Global Biometric Market Projections by Technology 2005-2012 ($ Millions)

Biometrics is starting to become a reality not only in the field of forensics, but in banking, internet services, medical services, food distribution, welfare, etc. The most integrated statewide approach to biometrics exists in Israel, where fingerprinting is mandatory and experimental passports with holographically imprinted fingerprints are expected to be issued in 2012.

Despite the known deficiencies and drawbacks of contact-based fingerprinting, this method is deployed in a variety of small mobile devices due to a relatively low cost of production. At the conference of Biometric Consortium held in Tampa, Florida on September 2010, about 17 companies demonstrated various forms of state-of-the-art contact-based hardware. Although contactless methods are known for producing distortion free fingerprints, this is a rather new technological development, and very few universities and companies are involved in their development. Figure 2 presents the major players involved in contactless fingerprinting.

Fig. 2. Contactless Fingerprinting Systems (Valencia, 2009)

Among these leaders of contactless fingerprinting only the Advanced Electronic Technology Center of UMass (AETC) has designed and tested systems where 180º contactless fingerprinting is combined with Infra-Red (IR) testing of blood vessels. Currently, the IR mapping of blood vessels is used to check whether a finger is alive and not a decoy; however, blood vessels can potentially be an additional biometric identifier. At the Advanced Electronic Technology Center, we designed and tested a novel, mobile, and contactless fingerprinting system based on line-scan technology. The system is capable of imaging the human palm, four fingers together, and nail-to-nail rolled-fingerprint equivalents, in a contactless fashion.

In the following sections, we discuss contactless fingerprinting technology, its benefits, its capabilities, and some of its applications in law enforcement, financial transactions, and network security.

2. Mobile contactless fingerprinting

In this section we describe alternative designs based on aerial and line scan cameras, compare different imaging and optical systems and the trade-offs involved with various design choices. There are two main imaging technologies used within current optical-based fingerprinting units. The first, and most widely used due to its simplicity, uses a two-dimensional array of imaging elements, much like the standard CCD found in most consumer cameras. A typical imaging setup involves a positioning system used to hold the finger steady, and a lens system used to form an image of the finger on the surface of the sensor. This technique allows for full fingerprint images to be taken in a single exposure using inexpensive camera systems. Images can be taken quickly and successively, but the sides of the fingerprint image will carry an unavoidable distortion due to the finger's edges being round.

Edges of the finger are not perpendicular to the image sensor, which causes their projection onto the flat surface of the sensing element to be a distorted representation of the actual finger. Figure 3 displays an image of a standardized test finger made of aluminium, taken with a traditional CCD. This test finger was made by US-National Institute of Standards and Technology. The dense grid pattern in the center of the image consists of circular dots regularly spaced 0.4mm apart. It can be seen that the pattern appears to be compressed towards the top and bottom edges of the image due the fact these edges on the test finger are "falling away" from the sensor as shown in the red boxes. Depending on the systems optics, this compression can be accompanied by image blur in these areas due to depth of field limitations within the specific lens system. These limitations tend to increase as the distance between the lens and the finger decreases, making it difficult to achieve desired image resolutions as fingerprinting machinery decreases in size. If higher quality images are desired, an alternative method of optical imaging must be used.

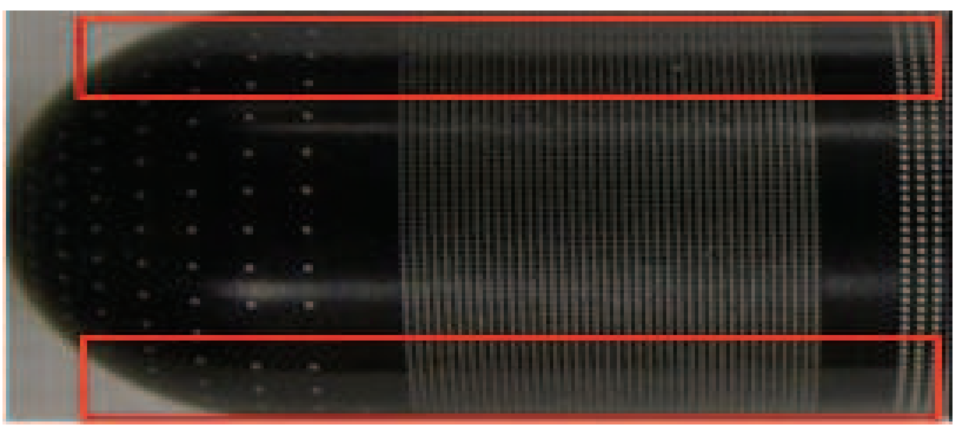


Fig. 3. Image of a test finger taken with a traditional CCD. Distortion in the form of compression and image blur in the top and bottom portions of the image can be seen

It is possible to record a high quality, two-dimensional image of a finger using an image sensor, as opposed to the standard two-dimensional pixel array, is one pixel wide by 512, 1024, 2048, or even 4096 pixels long. Such a sensor, known as a line-scan sensor, can capture an individual line of an image per exposure. By scanning an object across the sensing element, a two-dimensional picture can be built up from the individual image slices. When extended to fingerprinting, this technique can overcome the distortion issues encountered when using two-dimensional CCDs.

A two-dimensional image of a finger is built by orienting a line-scan sensor lengthwise to the finger and then rotating it around the main axis of the finger completing an 180º arc. The image captured represents an uncoiled view of the finger equivalent to a "rolled-ink" print. The line-scanner views each portion of the finger perpendicularly, removing the projection errors inherent in conventional two-dimensional scanning techniques. If this semicircular path is concentric with the finger, the path maintains a constant object-to-lens distance throughout the scan, eliminating any possible depth of field issues. Figure 4 displays an image of the same test finger shown in Figure 3 taken using the line-scanning technique. It can be seen that the irregularities present in Figure 3 are nonexistent, and the regular spacing of the grid pattern have been preserved.

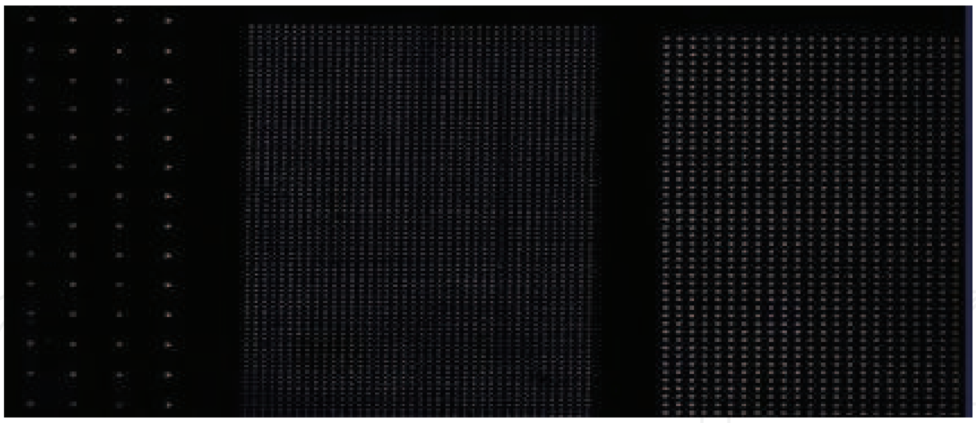


Fig. 4. Image of standardized test finger taken with the rotational line scanning approach

In such a setup, high quality fingerprint images at greater than 1000 ppi resolution have been obtained by various prototype units. This high precision enables the detection of fingerprint ridges as well as pores, facilitating the extraction of additional biometric data, such as the locations of the pores on a fingers surface.

2.1 Optical design

The raw image quality of any optical fingerprinting system is directly related to the system's optical design and configuration. Due to optical limitations which are deeply rooted in optical physics, designers of these systems are faced with design trade-offs which greatly affect the images produced by the system. For instance, a machine designed for imaging close objects will suffer from a smaller depth of field than the same machine if it were designed for imaging objects that are farther away. When viewed from a fingerprinting perspective, these optical limitations translate to practical considerations for a user or perspective buyer of fingerprinting hardware. For instance, the machine designed for up-close imaging will have less tolerance in the positions that a fingerprintee is allowed to place their finger, as deviations from this allowed position will result in a higher degree of image degradation than the more zoomed out model. The trade-off is that for the increased resolution associated with the up-close unit, the price of an increased number of re-prints, longer fingerprinting times, and higher operator training costs will most likely be paid.

2.2 Light control systems

In addition to a fingerprint reader's optical subsystem, the reader's final image quality is also dependent on the unit's lighting control system. Lighting control systems can be either *Active* or *Passive,* the distinctions, benefits, and drawbacks of each technique will be discussed in this section.

Passive lighting control is the simplest form a lighting control system can take. A passive system has the ability to *only* turn the lights on to a preset intensity value at the start of a scan, and turn the lights off at the completion of a scan. This type of system can be created with relatively cheap, easily accessible parts, and with minimal development time. This translates to a cheaper cost of fingerprinting units that employ this technology. However, because there is no feedback on whether the lighting intensity is at an optimal value, the resulting image can become over or under exposed in some operating conditions. This is because differences in skin tone, cleanliness, and moisture affect the amount of light that it will reflect back to the image sensor, having a direct effect on the exposure of the resulting image.

If over exposed, the image sensor becomes saturated, and all usable data from over exposed region is lost. In the case of under exposure, image enhancement techniques applied in post processing of the image can usually extract fingerprint ridge information, but in severe cases data can be lost. If optimal exposures are required across all fingerprintees and all operating conditions an active lighting control system should be used.

Active lighting control is a control system that utilizes feedback in real-time to adjust the light's output intensity. Active systems must use actual images from the camera to determine the correct lighting values for each use. This feedback requires the use of image processing, and relatively sophisticated control electronics. For this reason, active control systems can be more costly than passive control systems.

Active control systems can control one or many lighting zones over an image. Systems that have more than one lighting zone have the added benefit of being able to correctly control the exposure over different parts or "zones" of a finger, where systems with only one zone can only adjust the lighting intensity of the image as a whole. Multi-zoned lighting systems can be useful when fingers that are dirty over specific regions are trying to be imaged. For instance, a finger with grease only on its tip will have a high reflectivity on the dirty area, and a relatively low reflectivity on the areas not covered in grease. In a single lighting zone imaging system, the high dynamic range of the reflected lighting values can create exposure problems in the resulting image. In a multi-zoned lighting system, the lights illuminating the greasy portion of the finger can simply be turned down.

2.3 An example of a mobile contactless fingerprint system

The Advanced Electronic Technology Center designed and fabricated a line of contactless fingerprinting systems. The design of these machines is based on the general principles described above. Figure 5 depicts a front view of one of these fingerprinting systems. The finger is positioned in the center of the optical system illuminated by blue LEDs, and then a line by line image is taken by a system of three mirrors, where one of the mirrors rotates clockwise around the finger. The nail-to-nail fingerprint image is a collection of multiple one pixel thick line-scan images and is acquired in less than one second. In anti-clockwise the map of blood vessels is taken by using IR LEDs.

Fig. 5. Front view of the contactless line scans fingerprinting system

The machine is provided with a touch screen interface, which is used to interact with an operator. The operator has the options to perform a contactless scan alone or with blood vessel imaging. Once the image acquisition is complete, it is transmitted over WLAN to a remote server which performs image processing and stores it. From this server the image may be send to law enforcement agencies for further processing.

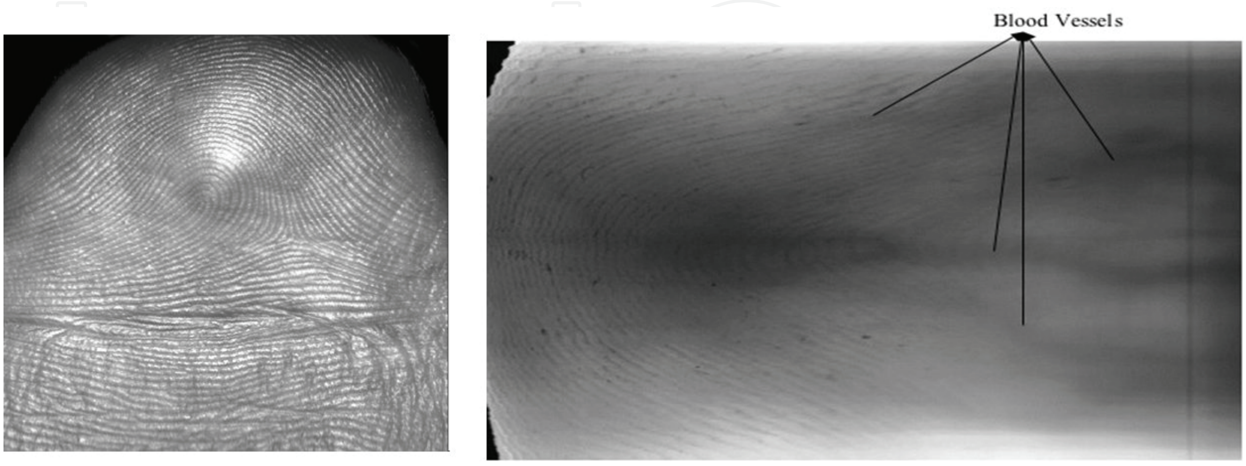


Fig. 6. a) presents an image of a fingerprint recorded in contact less fashion. b) presents an image of blood vessels taken by the contactless machine

Figure 6 has two sub-images, Figure 6a and Figure 6b. Figure 6a presents a fingerprint taken by line-scan camera where the mirror goes clockwise around the finger. The scan takes ¾ of a second. Figure 6b presents a map of blood vessels in the finger. The finger is seen in transmitted IR light where the anti-clockwise rotation of the mirror takes ¾ of a second.

3. Fingerprint processing algorithms

Different modes of fingerprint acquisition pose challenges in the form of format, size of images, non-linear distortions of fingerprint ridges, differences in orientation, and variation of gray scale values.
These challenges are mitigated by developing algorithms which pre-process raw images taken directly from acquisition devices, and facilitate reliable recognition of fingerprints.
We have developed a new binarization method that is used to eliminate variations in gray scale levels of each image, leaving the resulting images looking like a traditional wet-ink rolled fingerprint. In this study we tested 720 fingerprints generated by wet-ink, flat digital scanners, taken from FVC 2004 and by the novel contactless fingerprinting scanner described in (J. Palma et. all, 2006) and (S. Mil'shtein et. all, 2008). In following sections, we describe the binarization steps, and the fingerprint alignment process.

3.1 Binarization procedure

Most fingerprint recognition algorithms rely on the clarity and details of ridges. Hence, it is necessary to clearly differentiate the fingerprint ridges and valleys using only two distinct values; this process is called binarization. Regardless of the quality of any image recognition algorithm, a poorly binarized image can compromise its recognition statistics.

A good binarization algorithm would produce an image which would have very clear and uniform black ridges on a white background even if the image is overexposed to a certain degree. We used the following binarization techniques:

1. Region-Based thresholding as described below.
2. Filter-Based technique mentioned by (Meenen and Adhami, 2005).

The region based thresholding starts with division of the image into an N-by-N grid of smaller blocks. Identification of ridge regions within these smaller blocks is performed. This is implemented by taking the gradients in the x and y direction and then finding the co-variance data for the image gradients. Once this step is completed, the orientation of ridges is computed by finding the angle with respect to the coordinate axis. Then, estimation of ridge frequencies in these blocks is performed. This is done to find out which blocks have a higher and a lower density of ridges. The image block is then rotated to make the ridges vertical. and is cropped to remove invalid regions. A projection of the grayscale values, down the ridges, is obtained by summing along the columns. Peaks in projected grey values are found by performing dilation and finding where the dilation equals the original values. The spatial frequency of the ridges is determined by dividing the distance between the 1st and last peaks by the number of peaks. If no peaks are detected, or the frequency of ridge occurrence is outside the allowed bounds, the frequency is set to 0. The information about ridge regions, orientation and frequencies returns a mask of a fixed size which defines the actual area where the fingerprint exists. The ridges are then enhanced with the help of a median filter. The image obtained after this process is thresholded to obtain the binary fingerprint. The threshold for binarization depends on the resolution for the image. This process can also be called Adaptive Binarization.

This method works very well with the images that are obtained from the contactless fingerprinting system described in section 2.3. This binarization technique is not affected by varying brightness levels throughout the image, and results in a binary image that has consistent information throughout. The drawback of this process is that a relatively large number of calculations are needed, which adds to the time needed for the overall recognition algorithm to complete.

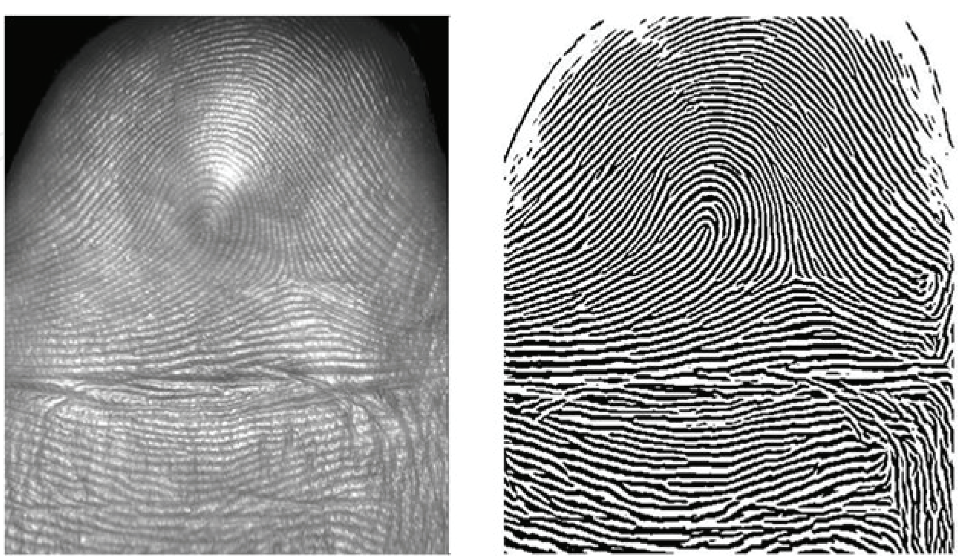


Fig. 7. Grayscale image of a selected fingerprint (Left) and the corresponding binarized image (Right)

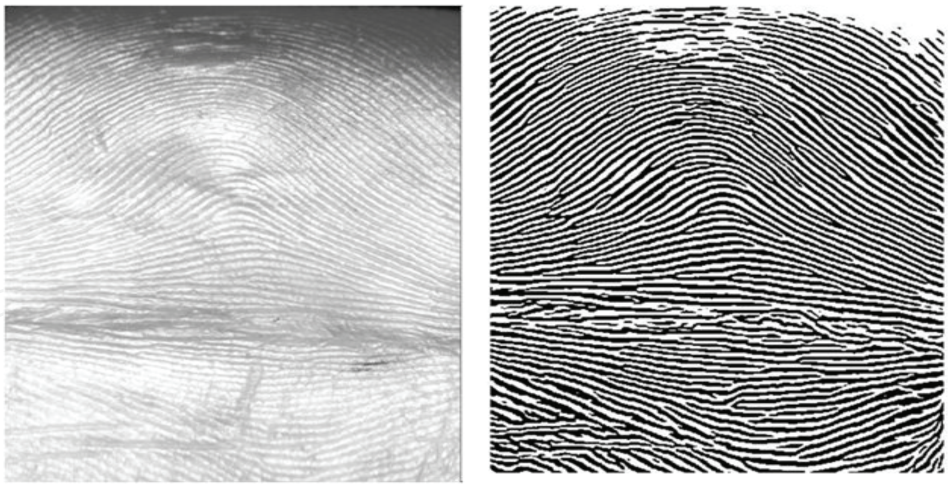


Fig. 8. Strength of binarization even if the image is seemingly overexposed

3.2 Fingerprint alignment

Fingerprint alignment is an important stage that is performed before fingerprint recognition. One must be sure that the regions being compared are the same. Fingerprint alignment using eight special types of ridges extracted from thinned fingerprint image is reported by (Hu et. all, 2008). Other alignment techniques based on phase correlation of minutiae points as described by (Chen and Gao, 2007), using line segments as pivots based on minutiae as mentioned by (Carvalho and Yehia, 2004) and using similarity histogram detailed by (Zhang et. all, 2004), have also been reported, creates a need for for a new novel alignment technique not based on minutiae. In this study, an alignment technique based on the Fourier Mellin Transform will be described.

The Fourier-Mellin Transform is a useful mathematical tool in image processing because its resulting spectrum is invariant in rotation, translation and scale. The Fourier Transform itself (FT) is translation invariant. By converting the resulting FT to log-polar coordinates, we can convert the scale and rotation differences to vertical and horizontal offsets that can be quantified. A second transform, called the Mellin Transform (MT), gives a transform-space image that is invariant to translation, rotation and scale. An application of the Fourier-Mellin Transform for image registration can be found in (Guo et. all, 2005).

The Mellin transform can be expressed as:

$$M(u,v) = \int_{\infty}^{\infty}\int_{\infty}^{\infty} f(x,y)\, x^{-ju-1} y^{-jv-1} dxdy;\ x,\ y>0 \tag{1}$$

Convert to polar coordinates using:

$$r = \sqrt{x^2 + y^2} \tag{2}$$

We now have:

$$M\{f(r)\} = \int_{\infty}^{\infty} f(r)\, r^{-ju-1}\, dr \tag{3}$$

Making $\boldsymbol{r = e^{\grave{y}}}$ and $\boldsymbol{dr = e^{\grave{y}}\, d\grave{y}}$ we have :

$$M\{f(e^{\grave{y}})\} = \int_{-\infty}^{\infty} f(e^{\grave{y}})\, e^{-ju\grave{y}}\, d\grave{y} \tag{4}$$

By changing coordinate systems from the Cartesian system to a Log-Polar system, we can directly perform a DFT over the image to obtain the scale and rotation invariant representation. The figures below show some of the results of the alignment using The Fourier-Mellin Transform. Figures 9 and 10 are the base image and the image in need of alignment. Figure 11 shows the two images aligned using Fourier-Mellin Transform.
The inverse Fourier transform of the Mellin Transformed images helps to see how well the image is aligned with respect to the base image. While this step is necessary to see the alignment results, the Fourier transforms; however are stored in as separate database as from here they are now the templates that will be used for comparison. This will eliminate the need to take again the FFT of the aligned image and the base image when it comes to comparing the fingerprints.

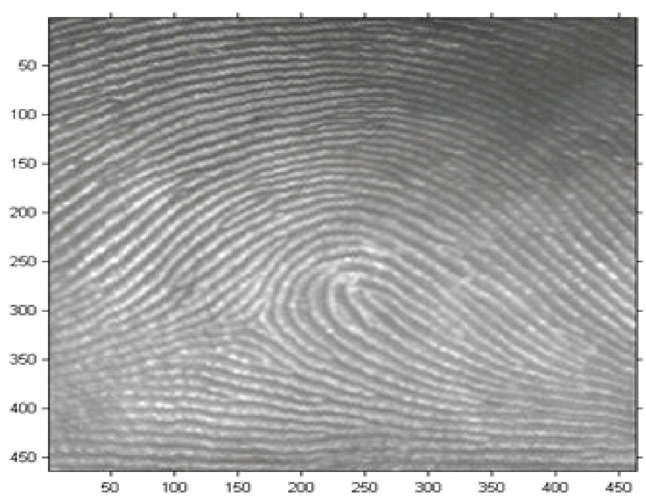


Fig. 9. Image of the 1st fingerprint

The Integrated Automated Fingerprint Identification System (IAFIS) of the FBI has fingerprints for more than 66 million people and more than 25 million civil prints (fbibiospecs.org). Most of these fingerprints have been taken with the ink and paper technique on FBI cards and then converted to a digital database using a high resolution scanner. But, it is well-known fact that most of these fingerprints are of poor quality due to smudging and smearing of the ink. In order to have improved quality of images and also improve the recognition rates, live-scan systems were used to obtain fingerprints. In these systems the image is acquired by sensing the tip of the finger using a sensor that is capable of digitizing the fingerprint on contact (Maltoni et. all, 2005). But recent studies (Mil'shtein and Doshi, 2004) have proven that fingerprints taken using the live-scan technique are also subject to pressure induced distortions. The distance between the ridges reduces depending on the pressure applied. Very recently, contactless fingerprinting techniques have been catching a lot interest due to their ability to produce almost distortion-free fingerprints. Also, because of their high resolution (Ross et. all, 2006), level 3 features can be used for identification. Figure 12 shows the fingerprint of the same finger taken using ink and paper, live-scan and touch-less technique.

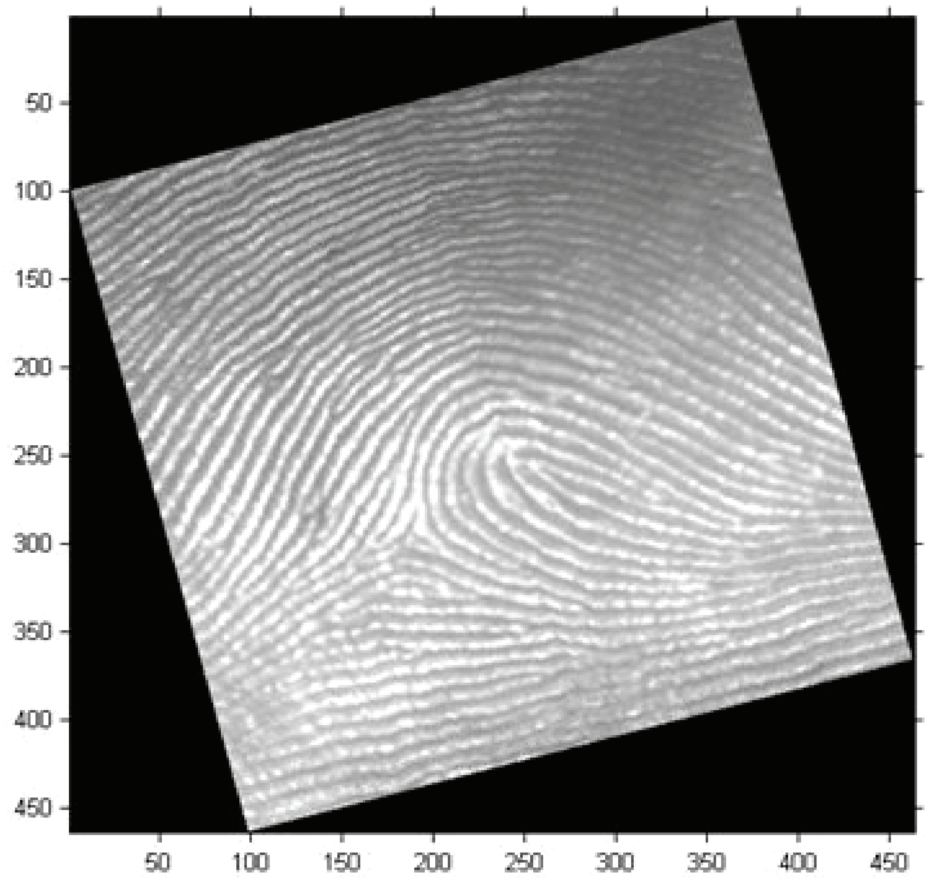


Fig. 10. Image of 2nd fingerprint (In need of alignment)

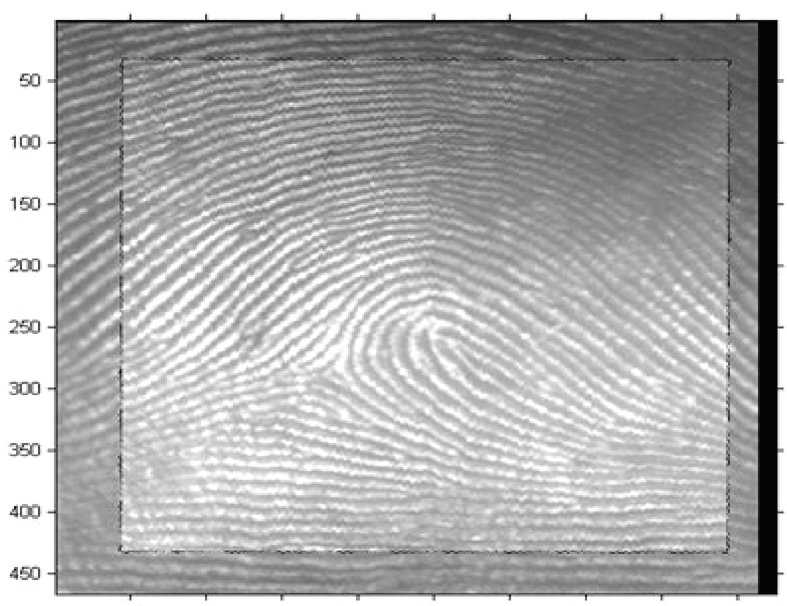


Fig. 11. Aligned 1st and 2nd images (Image 2 superimposed upon image 1)

Fig. 12. Fingerprints taken via wet-ink, live scan and contactless techniques

But the issue of conversion of existing database to a contactless database is now looming and large. Another issue is how wet-ink and live-scan fingerprints compare to their touch-less counterparts. Can law enforcement agencies compare a fingerprint taken by wet-ink / live-scan methods to the same fingerprint taken using contactless technique? How will minutiae algorithm perform when it comes to comparing these two types of fingerprints? Dominant presence of wet-ink / live-scan fingerprints requires that these questions be answered immediately. In the following sections, we attempt to highlight these issues for contactless fingerprints that will come in the way of comparison of the databases.

3.3 Problems

3.3.1 Grayscale variations

Figure 13 shows an image taken from (S. Mil'shtein et. all, 2008). Even though the resolution of the fingerprint is well above FBI requirements (fbi.gov), one can clearly see that the intensity is not consistent throughout the image. As a result, digitization leads to loss of information. Hence, the resulting image is rendered useless.

3.3.2 Aspect ratio differences

Figure 12 showed comparison between a fingerprint taken by conventional wet-ink method, live-scan, and contact-less method. The aspect ratios are nearly the same in the first two images but for the contactless fingerprint, the image looks stretched out and as a result the aspect ratio varies along with the location of the minutiae points.

3.3.3 Lack of optimum illumination

Very often, the illumination circuitry in contactless fingerprinting technologies are preset to certain values. As a result, when fingers with different skin tones are fingerprinted, the fingerprint images lack the optimum brightness which result in a completely under exposed or oversaturated image.

3.3.4 Inverted background and foreground

In Figure 14 and 15, the background and foreground in a fingerprint taken via wet-ink technique and contactless technique are switched. This creates significant problems for minutiae algorithms in locating and identifying the minutiae points.

Fig. 13. Grayscale variations within the image

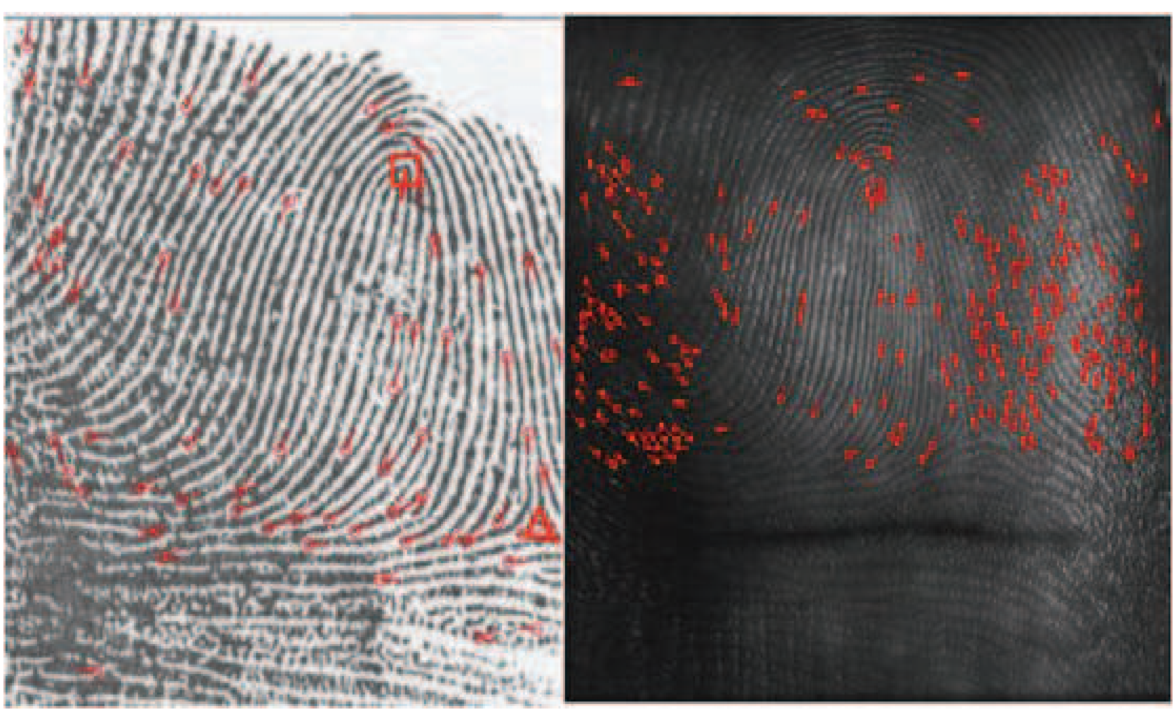


Fig. 14. Minutiae points on fingerprints taken via different techniques

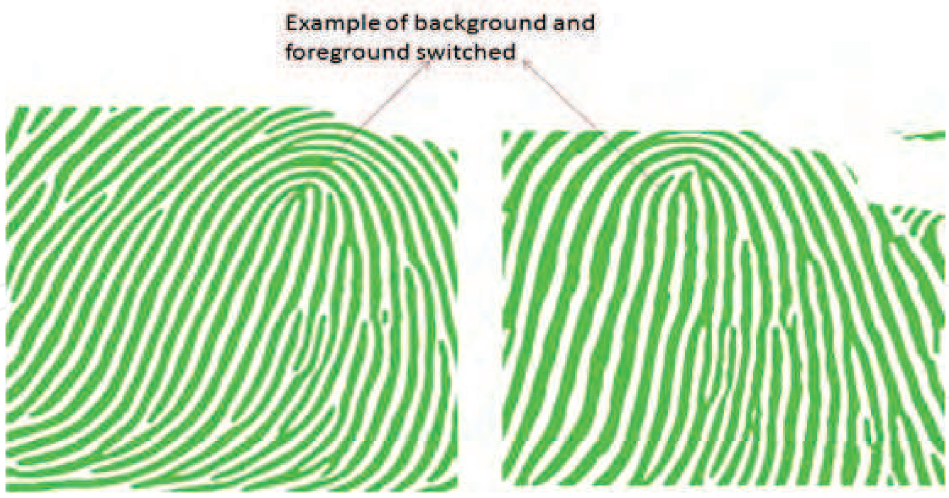


Fig. 15. Different foreground and background

3.4 Solutions

3.4.1 Adaptive binarization

One of the methods to solve the problem of grayscale variations is to binarize the image adaptively.

3.4.2 Solution to the aspect ratio problem

Since the fingerprint images are of different aspect ratios, there needs to be sensing mechanism that senses the size of the finger and then adjusts the resolution at which the camera is taking the image. Using software packages such as MATLAB or Adobe Photoshop to resize the images to equal sizes is also possible but it does not lead to a totally accurate result, and is not scalable to high throughput operations.

3.4.3 Adaptive histogram equalization

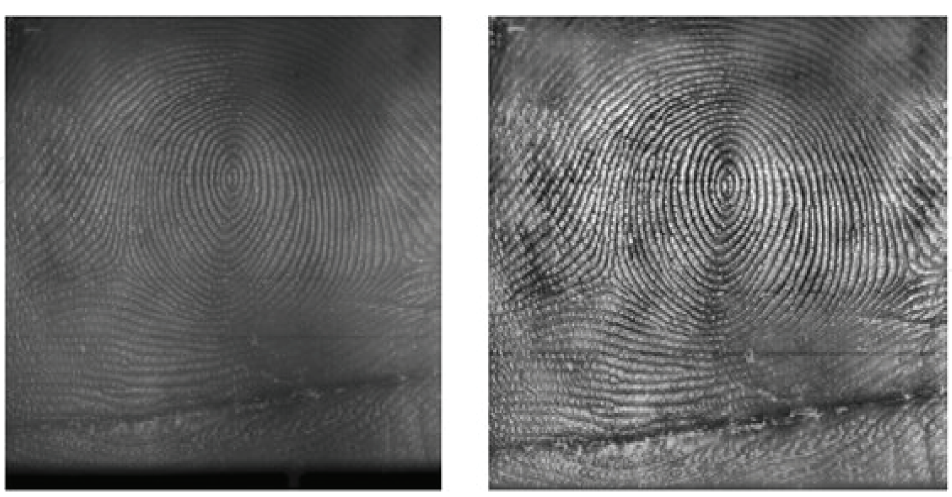


Fig. 16. Result of Histogram equalization

To make up for insufficient illumination, the contactless technology can be equipped with an adaptive histogram equalization algorithm (Pizer et. all, 1987). This ensures that fingerprint image has consistent in brightness and contrast which in turn results in good quality binarization. It could also be implemented at a hardware level by using the procedure described in (Jusoh et. all, 2001). Fig. 16 shows the result of this algorithm

3.4.4 Inverted background and foreground

There are two solutions to the problem described in the section 3.3.4. One can take the complement of the image at the machine level and then transfer it to a database where it is binarized and then compared. Or the image can be binarized first and then complemented again using MATLAB or Adobe Photoshop. In our comparisons we found that the later method gave better results for comparisons.

4. Applications of contactless fingerprint technology

Increased security threats with respect to terrorism and cyber-crime have recently necessitated the development of biometric systems to be used at commercial facilities, border crossings, airports, and government building access points. Additionally, fraud with credit card accounts, hacking of retail store websites, and most importantly, the critical interruption of governmental agencies such as the Department of Defense and the Department of Homeland Security, requires the development of systems capable of identifying individuals accurately to mitigate such attacks.

When automated fingerprinting systems were introduced in the late 1960s, digital contact-based fingerprinting replaced the old method of ink rolling. This facilitated a new range of fingerprinting applications. The increased accuracy of contactless fingerprinting will create new applications in fingerprinting as well. Specifically, applications will be found in the fields of information security, access control, and law enforcement. Below are some examples of how contactless fingerprint systems can be used in both the private and the public sector.

4.1 Law enforcement agencies

Every organization has unique requirements for stored fingerprints, depending on how these prints are utilized. For example, agencies that deal with crime scene fingerprints prefer to have nail-to-nail images, because crime scene images may be partial; and the more information available at registration stage helps in matching them with partial prints lifted from a crime scene. This specific need of individual organizations has resulted in different agencies having their own unique and often incompatible databases.

Recently, creation of a unified and accurate database across all agencies has been recognized as a necessary step in the evolution of law enforcement's capabilities. A standardized method which captures a nail-to-nail image will help these agencies migrate towards a single large database, from which a specific portion of the image may be extracted depending on individual requirements.

To make this step, a new standard of fingerprints and fingerprinting hardware will need to be developed and followed across all agencies. Implementation details of such project will not be discussed here; however applications of such a database will be explored.

Currently, it is impossible for law enforcement to identify an individual in real-time based on fingerprints only. This is partially due to a lack of computer processing power to sort through databases containing millions of images. Most important, the current databases contain fingerprints taken using contact-based methods, and thus have varying degrees of distortion.

A database system containing high quality images and a repeatable method for fingerprint capture would facilitate applications such as real time recognition of individuals. For example, police officers carrying mobile fingerprint capture units can successfully execute an arrest as soon as he verifies the identity of the individual.

4.2 Access control

Access control can also benefit from such devices. Current fingerprint based access control devices have a certain disadvantage in usability. Often a user may need to repeatedly scan their finger before they are granted access. The need to use a finger few times is caused by inconsistencies between the fingerprint data recorded by the capture device and the data stored within the system's database. This inconsistency increases the systems margin of error, translates to increased false rejections and a lower degree of confidence with every match.
In high security access control, an additional measure can be taken to further increase the degree of confidence with every match. Spoof detection is a technique that focuses on determining whether a finger is currently alive and attached to the body, and is in fact the person's real finger. Systems have been designed, such as the AETC's "Infrared Spoof Detection System", that satisfy such requirements (M. Baier, et. all, 2011).

4.3 Financial transaction

In the commercial sector, accurate biometric based authentication can be implemented in electronic commerce and confidential email exchange. Methods of authentication such as tokens, cards, badges, passwords and pins are widely being used today. These methods can be supplemented by accurate fingerprint based authentication to obtain a higher degree of user confidence, as well as decrease the presence of fraud in online spaces. At places of financial transactions, Automatic Teller Machines, and E-commerce are all areas that can potentially find solutions to long-standing security related problems through the use of commercialized contactless fingerprinting devices.

5. Network security

Using fingerprinting for computer and network safety is another example of applications of contactless fingerprinting. The importance of network security motivated us to present a separate section on this subject.
Security of network transactions is a major concern today, as we move towards society that is increasingly dependent on the comfort of performing day to day activities like bill payment, shopping at home, etc. Use of a public network service requires some form of authentication, because it is easily accessible to anyone connected to the network; and is prone to unauthorized and potentially malicious usage (ICC, 2009). Majority of network based authentication is performed using knowledge based methods wherein a password is used for authentication. Contrary to appearance, this type of authentication is inherently (White paper, M86 Security, 2010) flawed. A compromised password may be repeatedly used by a malicious user. There are limited means by which a second authentication system may be added in to the current infrastructure.
Few options such as RSA SecureID, VeriSign token and eToken from Aladdin knowledge systems require the user to carry additional devices which generate one-time passwords. Although these systems are marginally effective, they have the disadvantage of the user having to carry these devices. This may be inconvenient, and also if users forget to carry the device or if the device fails, they may not be able to use the system. There is also the possibility of the devices being stolen and used for authentication by malicious users. Similar problems exist in systems which send one time passwords to user's registered mobile phones.

5.1 Biometrics for authentication

Shortcomings of the above mentioned systems may be easily overcome using systems which use biometric modes of authentication, in addition to conventional static passwords. Biometrics is the use of characteristic features of face, fingerprints, iris or retina scans, voice, signature etc for authentication. The merit of biometric systems is that its uniqueness, and users do not have to carry additional hardware. However these systems have a major deficiency when it comes to usability. Face recognition, fingerprints, voice and signature are not invasive and are convenient for users. But these often pose problems with data acquisition, resulting on high false recognition. Iris and retina scans are invasive, and often pose problems for people using eye-wear such as spectacles or contact lenses. Fingerprints by far are the least invasive and most secure in terms of individuality when compared to all other biometric modalities.

5.2 Fingerprint based authentication

Fingerprint acquisition devices are usually contact based and thus pose problems during recognition stage. Fingerprints differ if they are taken by contact methods due to contact based distortion. We propose using contactless fingerprinting for network based authentication. Using contactless acquisition technologies provide high resolution, undistorted and consistent images which may be used to generate high entropy keys. Such high resolution images provide better minutiae points if minutiae (Afsar et. all. 2004) based extractor is used.

A major drawback of fingerprinting is that once a digitized fingerprint is compromised, the attacker merely needs to duplicate (Ratha et. all, 2001) it for authentication. The possibility of entire fingerprints being compromised is increased in case of transactions requiring transmission of full prints. This problem can be addressed by using partial fingerprints for identification, which is obtained from high resolution fingerprints using contactless technologies (Mil'shtein et. all, 2009).

5.3 Network security using randomized partial fingerprint

We describe a randomized partial contactless fingerprint based security protocol which uses a portion of the user's fingerprint. Effective use of partial prints is enabled by the use of distortion-less high resolution images obtained from a contactless fingerprint reader. A simplified implementation of such a system is described below:

1. Once a fingerprint is registered, it is stored in the server.
2. Upon receiving an authentication request from the authentication device, the server calculates a random Co-ordinate information key (CIK) using the image stored in it. It also stores the transaction identifier (TID) and the CIK for verification. Figure 17 describes these portions of the image. The cross-point shows the co-ordinate axis used, the circle shows the core, and the rectangle signifies the partial region used for matching.
3. Server sends back CIK along with the TID to the acquisition device.
4. The device perform acquisition and depending on the CIK, and transmits the valid portion of the image along with transaction ID back to the server.
5. The CIK is recomputed and handshaking is repeated till the server can conclusively accept or reject the user's request.

Figure 18 describes the above steps. For additional security a trusted third party maybe added in between the communication entities, as described in figure.

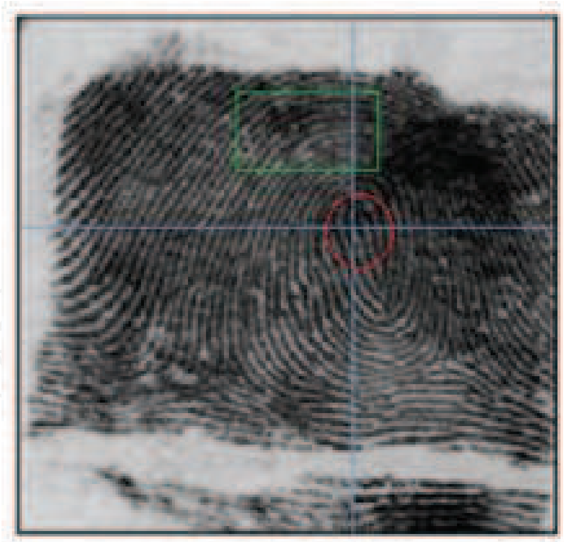


Fig. 17. A fingerprint showing CIK based region

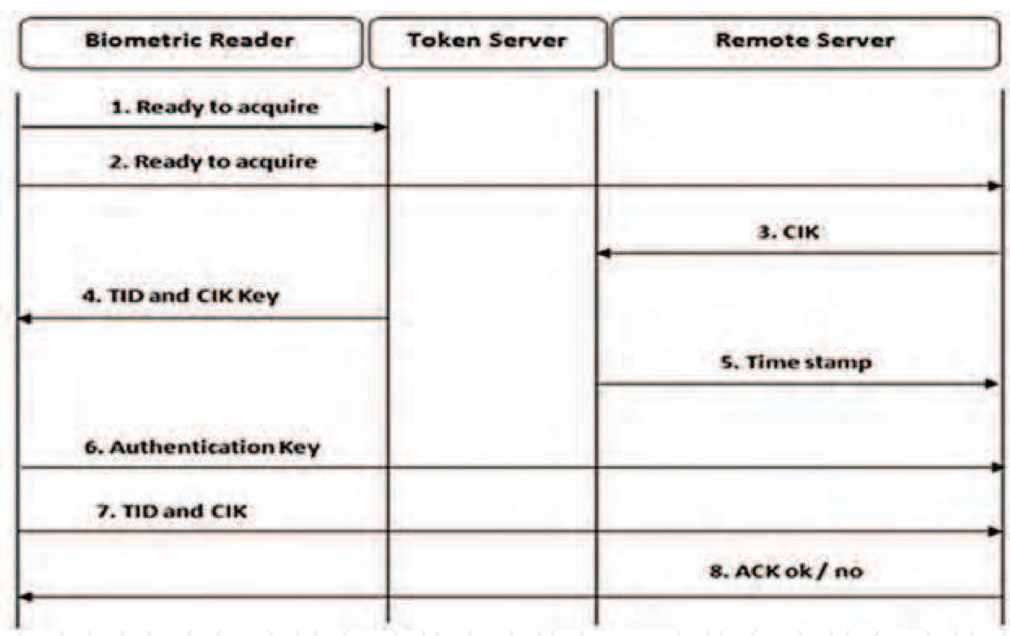


Fig. 18. A trusted third party based secure network transaction

The system described above has the following benefits:

1. The user does not have to remember multiple long passwords.
2. Once the acquisition devices are standardized, there is no need for additional hardware to be carried by the user.
3. An attacker who has access to multiple CIK will not be able to predict the next CIK, or infer which CIK will be used for a later transaction.
4. Since only a portion of the fingerprint is actually sent over the network, even if it were compromised, it would not be possible to bypass the system because of the inability to predict CIK, and thus the resulting image for any given transaction.
5. Since no complicated image processing is performed at the acquisition device, it keeps the device simple and thus economical, making it viable to be standardized.

6. Conclusions

In the last decade, both the hardware and the software of biometric technologies have been rapidly improving. The wet-ink procedures are being replaced by digitized fingerprinting, where a finger is pressed against a computer scanner. Simultaneously, novel contactless methods are being developed. Responding to the needs of forensic investigations and requirements of law enforcement new systems have been designed which made the examination of the entire palm, four -slap fingers, and nail to nail fingerprinting possible. Although, based on the old minutia algorithms current recognition software was modified to replace an operator by a computer to analyze and compare fingerprints. Fast network communication between police stations and database centers became a reality of the everyday operation of law enforcement. The Advanced Electronic Technology Center of UMass contributed to the recent modification of fingerprinting technology by combining contactless fingerprinting with blood vessel mapping in a line of newly designed hand-held systems which allow for examining of a palm and four fingers simultaneously, as well as each individual finger from nail-to-nail.

The best way to understand the future development of fingerprinting technology is to analyze the deficiencies of existing fingerprinting methods. In brief, these deficiencies could be classified into two groups.

1. General deficiencies related to biological conditions of human body are:
   a. The shape of fingerprint changes with age due to the appearance of wrinkles on human skin. Periodic recertification of individual fingerprints is a potential answer to this problem
   b. Medical conditions of the individual might modify the reflectivity of the skin and change the IR light absorption by blood vessels. Adjustable light intensity and contrast in a fingerprinting system is one of the potential solutions of this problem.
2. The deficiencies related to technical limitations of fingerprinting systems are:
   a. Low accuracy of recognition in some existing systems necessitates use of a second method of recognition of an individual. Often, computer scanners after taking fingerprint images need to scan an employee badge or a picture to confirm the identity of an individual. Non-distorted images generated by contactless fingerprinting systems and tight recognition algorithms are the answer to the problem.
   b. Fingerprinting based on a physical contact of a finger with a scanner generates pressure induced distortions of the fingerprint. Network security requires non-distorted, thus contactless images, for the computer (not an operator) to verify the identity of an individual.
   c. There are three libraries of fingerprints produced by wet-ink technology, digitized techniques and contactless methods. A compatibility study of these three libraries is urgently needed.

7. References

A. Ross, A. K. Jain, Multimodal Biometrics: An Overview, *Proc. of 12th European Signal Processing Conference*, pp:1221-1224, 2004.

C. Carvalho, H. Yehia, Fingerprint Alignment using Line Segments, *Biometric Authentication, Springer*, pp 1-10, 2004

C. Hu, J. Yin, E. Zhu, H. Chen, Y. Li, Fingerprint Alignment using Special Ridges, *Springer,* 2008

Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, Handbook of fingerprinting, *Springer* 2005

F.A. Afsar, M. Arif and M. Hussain, Fingerprint Identification and Verification System using Minutiae Matching, *National Conference on Emerging Technologies*, 2004

L. Nanni and A. Lumini, Descriptors for image-based fingerprint matchers, *Expert Systems With Applications*, vol.36, no.10, pp.12414-12422, December 2009

M. Baier, S. Foret, V. Oliyil Kunnil, M. Paradis, P. Bustos, S.Mil'shtein, Automatic Contactless Fingerprinting System, *To appear:Proc. of PECCS 2011*, Portugal.

Noor Ashedah Binti Jusoh et. all, Adaptive lightning system and method for machine vision apparatus, *patent # US 6,207,946 B1, 2001.*

N.K. Ratha, J.H. Connel, and R.M. Bolle, Enhancing security and privacy in biometrics-based authentication system, *IBM Systems Journal*, 2001

P. Meenen, R. Adhami, Approaches to image binarization in current automated fingerprint identification systems, *Proceedings of the Thirty-Seventh Southeastern Symposium on System Theory*, 2005, ISBN:0-7803-8808-9

Palma J, Liessner C, Mil'shtein S, Contactless Optical Scanning of Fingerprints with 180° View, *Scanning*, 28, 6, pp 301-304, 2006

Ross, Arun A., Nandakumar, Karthik, Jain, Anil K., Handbook of Multi-biometrics, *Springer*, 2006

S. Mil'shtein, M. Baier, C. Granz and P.Bustos, Mobile System for Fingerprinting and Mapping of Blood -Vessels across a Finger, *IEEE Intern. Conf. on Technologies for Homeland Security*, ISBN 978-1-4244-4179-2, p.30-34, 2009

S. Mil'shtein, J. Palma, C. Liessner, M. Baier, A. Pillai, and A.Shendye, Line Scanner for Biometric Applications, *IEEE Intern. Conf. on Technologies for Homeland Security*, ISBN 4244-1978-4 P 205-208, 2008.

S. Mil'shtein, U. Doshi, Scanning of the Pressure-Induced Distortion of Fingerprints, *Scanning,* 26, 4, 323-327, 2004.

S. M. Pizer, E. P. Amburn, John D. Austin, Robert Cromartie, Ari Geselowitz, Trey Greer, B. T. H. Romeny, John B. Zimmerman and Karel Zuiderveld, Adaptive histogram equalization and its variations, *Computer Vision, Graphics, and Image Processing,* Volume 39, Issue 3, September 1987, pp 355-368.

T. Zhang, J. Tian, Y. He, J. Cheng, X. Yang, Fingerprint alignment using similarity histogram, *International conference on audio and video-based biometric person authentication*, pp 854-861, 2003

V. Valencia, Intuitive Touchless Fingerprinting The Pressure's Off, *Biometric Consortium Conference*, Tampa Bay, Florida, 2009.

W. Chen, Y. Gao, Minutiae-based Fingerprint Alignment Using Phase Correlation, *Mechatronics and Machine Vision in Practice*, Springer Link, pp 193-198, 2007

Xiaoxin Guo, Zhiwen Xu, Yinan Lu, Yunjie Pang, An Application of Fourier-Mellin Transform in Image Registration, *The Fifth International Conference on Computer and Information Technology*, Sep 2005, pp 619-623.

Yang, J.C. ; Park, D. S., A fingerprint verification algorithm using tessellated invariant moment features, *Neurocomputing*, 71(10-12),1939-1946; 2008

http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis

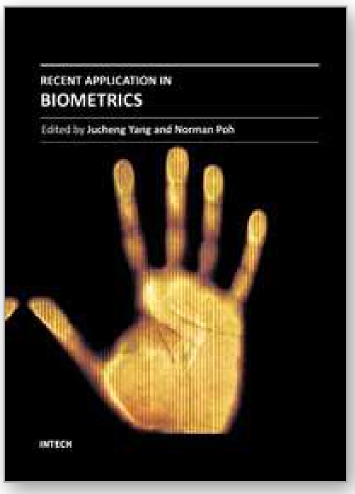
https://www.fbibiospecs.org/biometric_specs.html

http://techbiometric.com/biometric-market/global-market-overview/

http://www.onin.com/fp/fphistory.html

Internet Crime complaint Center, statistics for 2009 http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

Whitepaper M86 Security - August 2010, Cybercriminals Target Online Banking Customers - Use Trojan and Exploit Kits to Steal Funds from Major UK Financial Institution.



Recent Application in Biometrics

Edited by Dr. Jucheng Yang

ISBN 978-953-307-488-7
Hard cover, 302 pages
Publisher InTech
Published online 27, July, 2011
Published in print edition July, 2011

In the recent years, a number of recognition and authentication systems based on biometric measurements have been proposed. Algorithms and sensors have been developed to acquire and process many different biometric traits. Moreover, the biometric technology is being used in novel ways, with potential commercial and practical implications to our daily activities. The key objective of the book is to provide a collection of comprehensive references on some recent theoretical development as well as novel applications in biometrics. The topics covered in this book reflect well both aspects of development. They include biometric sample quality, privacy preserving and cancellable biometrics, contactless biometrics, novel and unconventional biometrics, and the technical challenges in implementing the technology in portable devices. The book consists of 15 chapters. It is divided into four sections, namely, biometric applications on mobile platforms, cancelable biometrics, biometric encryption, and other applications. The book was reviewed by editors Dr. Jucheng Yang and Dr. Norman Poh. We deeply appreciate the efforts of our guest editors: Dr. Girija Chetty, Dr. Loris Nanni, Dr. Jianjiang Feng, Dr. Dongsun Park and Dr. Sook Yoon, as well as a number of anonymous reviewers.