SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2012; **00**:1–12
DOI: 10.1002/sec

JOURNAL ARTICLE

Fingerprint Recognition with Embedded Cameras on Mobile Phones

Mohammad Omar Derawi and Bian Yang and Christoph Busch

Norwegian Inoformation Security Laboratory, Gjøvik University College, Gjøvik, Norway

ABSTRACT

Mobile phones with a camera function are capable of capturing image and processing tasks. Fingerprint recognition has been used in many different applications where high security is required. A first step towards a novel biometric authentication approach applying cell phone cameras capturing fingerprint images as biometric traits is proposed. The proposed method is evaluated using 1320 fingerprint images from each embedded capturing device. Fingerprints are collected by a Nokia N95 and a HTC Desire. The overall results of this approach show a biometric performance with an Equal Error Rate (EER) of 4.5% by applying a commercial extractor/comparator and without any preproccesing on the images. Copyright © 2012 John Wiley & Sons, Ltd.

KEYWORDS
mobile devices, biometrics, fingerprint recognition, cameras

Received . . .

1. INTRODUCTION

Current mobile devices implement various new kinds of applications such as taking photos, and movie shooting by using embedded camera devices. This progress was made possible by the evolution of miniaturized embedded camera technology. Mobile devices – particularly mobile phones – are being found in almost everyone's hip pocket these days all over the world. Almost all newer cell phones now-a-days have embedded camera devices, and some of those have more than over 5 mega-pixel image cameras.

From a security point of view, the issues related to ever-present mobile devices are becoming critical, since the stored information in them (names, addresses, messages, pictures and future plans stored in a user calendar) has a significant personal value. Moreover, the services which can be accessed via mobile devices (e.g., m-banking and m-commerce, e-mails etc.) represent a major value. Therefore, the danger of a mobile device ending up in the wrong hands presents a serious threat to information security and user privacy. According to the latest research from Halifax Home Insurance claims, 390 million British pounds a year is lost in Britain due to the theft of mobile phones. With the average handset costing more than 100 British pounds, it is perhaps not surprising that there are more than 2 million stolen in the UK every year [1].

Authentication is an area which has grown over the last decades, and will continue to grow in the future. It is used in many places today and being authenticated has become a daily habit for most people. Examples of this are PIN code to your banking card, password to get access to a computer and passport used at border control. We identify friends and family by their face, voice, how they walk, etc. As we realize there are different ways in which a user can be authenticated, but all these methods can be categorized into one of three classes [2]. The first is *something you know* (e.g., a password), the second is *something you have* (e.g., a token) and the third is *something you are* (e.g., a biometric property).

Unlike passwords, PINs, tokens etc. biometric characteristics cannot be stolen or forgotten. The use of biometric was first known in the 14th century in China where "Chinese merchants were stamping children's palm- and foot prints on paper with ink in order to distinguish young children from one another". Approximately after 500 years has passed, the first fingerprinting was used for identification of persons. In 1892, the Argentineans developed an identification system when a woman was found guilty of a murder after the investigation police proved that the blood of the woman's finger on the crime scene was hers. The main advantage of biometric authentication is that it establishes an explicit link to the identity because biometrics use human *biological* and *behavioral* characteristics. The first mentioned are the biometrics derived directly from the part of a human body. The most used and prominent examples are the fingerprint, face, iris and hand recognition. The behavioral characteristics are the biometrics by persons behavioral characteristics, such as gait-recognition, keystroke recognition, speech/voice recognition and etc.

Many fingerprint recognition algorithms perform well on databases that had been collected with high-resolution cameras and in highly controlled situations [3]. Recent publications show that the performance of a baseline system deteriorates from Equal Error Rate (EER) around 0.02 % with very high quality images to EER = 25 % due to low qualities images [4]. Thus active research is still going on to improve the recognition performance. In applications such as fingerprint authentication using cameras in cell phones and PDAs, the cameras may introduce image distortions (e.g., because of fish-eye lenses), and fingerprint images may exhibit a wide range of illumination conditions, as well as scale and pose variations. An important question is which of the fingerprint authentication algorithms will work well with fingerprint images produced by cell phone cameras?

However, recent research [5, 6] have shown that by using low-cost webcam devices it is possible to extract fingerprint information when applying different pre-processing and image enhancements approaches. In this paper we present fingerprint recognition as means of verifying the identity of the user of a mobile phone. The main purpose of this paper is to study how it is possible to lower down the user effort while keeping the error rates in an acceptable and practical range. Therefore, this proposal is a realistic approach to be implemented in mobile devices for user authentication. To address this issue, we collected a fingerprint database at the Norwegian Information Security Laboratory using two different cell phone cameras, namely the Nokia N95 and HTC Desire where details mentioned later.

2. BACKGROUND - BIOMETRICS SYSTEMS

”Biometrics” come from the Greek words ”bio” (life) and ”metrics” (to measure). This interpretation is in well agreement with the following definition:

> Automated recognition of individuals based on their behavioral and biological characteristics

Automated recognition systems have only become available over the last few decades, due to significant advances in the field of computer processing. However, many of these new automated techniques are based on ideas that were originally conceived hundreds, even thousands of years ago. One of the oldest and most basic way to recognize humans from each other is by their faces. Since the beginning of civilization, humans have used faces to identify known and unknown individuals. This simple manual task, however, became more challenging as populations increased with time. More formal means of recognition were developed. One of the earliest use of fingerprints as a person’s mark, dates back to 500 B.C., where Babylonian business transactions were recorded in clay tablets that include fingerprints. In the 14th century it was recorded that Chinese merchants used fingerprints to settle business transactions. Further on Chinese parents also used fingerprints and footprints to differentiate children from one another. Proper biometric systems first began to emerge in the latter half of the twentieth century, coinciding with the emergence of computer systems.

Unlike other security measures such as keys, ID cards, passwords, pin-codes, tokens etc. biometrics have the advantage of recognizing an intrinsic property of an individual, thus besides being unique, it cannot be shared, forgotten, lost or copied (at least not in the same manner as an object). In general biometric systems provide a more secure and reliable user authentication method than traditional security measures. An user can relate the different authentication techniques as the following:

- *Something you know and/or have*, e.g. password, PIN code, key, or card. The issue is that many passwords are easy to guess and can also be easily forgotten. The key or card can be lost, stolen or even duplicated.
- Something you are, e.g. fingerprint, hand, iris, retina, voice etc. You cannot lose them, they are unique for each individual and very difficult to replicate, thus making a system always aware of your true identity.

Biometric traits which represent ”something you are” can be divided in two main classes:

- **Physiological** characteristics (also called biological characteristics) are related to the shape of the body/body parts. The most common used are the fingerprint, face, iris and hand recognition.
- **Behavioral** characteristics are related to the behavior of a person, such as gait recognition, keystroke recognition, speech/voice recognition and etc.

The biometric samples of physiological characteristics are said to be captured and specified in a point in time, whereas the biometric samples of behavioral characteristics are captured and specified during a short period of time. Biometric systems are either verification[*] or identification systems. In case of identification, the purpose is to determine a person’s identity, while the purpose of verification is to confirm a person’s claimed identity. Another way to interpret this is that for verification, the system’s comparison task will be one-to-one, whereas for identification systems, the comparison task will be one-to-n, where n represents the total number

[*] An alternative word for verification is authentication

Security Comm. Networks 2012; **00**:1–12 © 2012 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

of known persons to the system. Testings of fingerprint recognition will mainly deal with verification systems. A typical verification process is in a later in the evulation section.

Today one can find various types of biometric applications in both the public and private scene. For instance in the public scene it could be border control, banking, law enforcement, health care etc. A recent example concerns Sydney Airport expanding their biometric program, which is based on facial recognition technology. The expansion involved launching new kiosks and "SmartGate" to allow international travelers to more quickly establish their identities and pass through security. According to federal home affair minister, the average time to establish a commuter's identity using the technology is 38 seconds. Another example in the private scene, is the trend of using fingerprint scanners in laptops. For instance IBM ThinkPad notebooks features a fingerprint reader, placed on the wrist-rest, below the arrow keys, which will verify the identity of a user when he/she swipes a finger across a tiny sensor. Once identity is established, users are automatically logged on. The fingerprint reader works in tandem with an embedded security chip and software called Password Manager to protect vital security data, such as encryption keys, electronic credentials and passwords.

Despite of the many advantages biometric systems are not flawless. Inaccuracies in the captured biometric data could occur by various situation factors, such as wet fingers or worn out fingers in fingerprint recognition, poor lighting conditions in face recognition, exposure to loud background noise in voice recognition etc. Therefore biometrics systems are prone to error due to environmental and circumstantial uncertainties.

2.1. Basic System Errors

Biometric authentication systems typically require specifications in terms of maximum allowable degree of errors, usually expressed as error rates. It is important to understand the type of the errors before a solution is designed. Some of these errors can be directly related to the results deduced from a pattern recognition application, which is inherently similar to a biometric authentication system, while other errors are more specific related to the latter. What is certain is that any biometric authentication system will make mistakes, and that the true value of the various error rates cannot be computed or theoretically established; it is only possible to obtain statistical estimates of the errors using test databases of biometric samples. In other words, the development of a biometric authentication system will most likely include general trial and error methods. In this section the intuitive and theoretical meaning of different error types (found in biometric literature) will be introduced. The main focus will be on the errors made by the match engine of a verification system. As described earlier the match engine corresponds to the biometric comparator that makes a 1:1 match decision based on a score s. The match engine of an identification system makes 1 : n match decisions. The problem of matching biometric samples and the problem of checking the credentials of a subject for biometric authentication in terms of hypothesis testing will be defined.

2.1.1. Comparison

A comparison engine is a system that takes two samples of biometric data as input and returns a score that indicates their similarity as output. This score is used for determining whether the two biometric samples are from the same original "realworld" biometric. In order to deepen the meaning of a match engine, the following notations are introduced:

b **and** b': Two real-world biometrics (e.g., two fingers or two faces).

$B = f(b)$ and $B' = f(b')$: The associated machine representations of these biometrics. f represents the process of sampling the data with a sensor and, perhaps, applying some processing to extract the features B and B'.

Unfortunately, the real-world biometrics b and b' (of the actual subjects) are functions of time, and the sensing function f could also perhaps be a function depending on environmental factors. Therefore this variability must be introduced and is indicated by the denoted t in the following

$$B = B(t) = f(b(t)) \text{ and } B' = B'(t0) = f(b'(t'))$$

Biometric comparison engines make a decision by computing a measure of the likelihood that the two input samples from two persons (subject 1 and subject 2) are the same and hence that the subjects have the same real-world identity. This measure is typically an algorithmically defined similarity measure, which is highly dependent on the precision of the acquisition device and machine representation of the biometric samples. If the similarity measure is able to capture nuances in biometrics that differentiate one person from the next, this similarity should then successfully relate to the match probability. Nevertheless, the match engine takes b and b0 as input and computes a score:

$$s(B',B) = s(B'(t'),B(t)) = s(f(b'(t')), f(b(t)))$$

Typically one of the machine representations (for instance B) is the enrolled sample, which is rarely changed unless desired for specific reasons, and the other of the machine representations (for instance B') is the live query sample. However, this score $s(B',B)$ only expresses some sort of likelihooed that the true biometrics b' and b are the same. It can be assumed that for a higher similarity match score $s(B',B)$, the more likely that two biometrics come from the same b. An alternative way to compute match scores is to determine distances, or dissimilarities, *d(B',B)* between the samples *B'* and *B*. The assumption is then the opposite of a similarity match score, namely that a lower distance match score would result that the more likely two biometrics come from the same *b*.

The biometric match engine determines the accuracy of the error rates in terms of the trueness of two hypothesis. Given two biometric samples, Equation 1 is the null hyoptheisi while Equation 2 shows the alternate hypothesis and can be constructed:

$$H_0 \Rightarrow \textit{the two samples match}; \tag{1}$$

$$H_a \Rightarrow \textit{the two samples do not match}; \tag{2}$$

The definition of biometric applications can differ; as well as the decision making of that biometric application, which therefore gives different definitions of errors. There are many terminologies that express the accuracy of an application, such as False Match Rate (FMR), False Accept Rate (FAR), False Positive Rate (FPR) etc. The most common use of errors used are False Match Rate (FMR), False Accept Rate (FAR), False Non Match Rate (FNMR), False Rejection Rate (FRR) or the Equal Error Rate (EER).

One could wonder why FMR and FNMR are similar with FAR and FRR, and the simple answer would be that indeed they are almost the same. FAR and FRR are terminologies based on the more conventional pattern recognition; they are inherent effects of any recognition system, whereas FMR and FNMR arise from the effects of a specific recognition task. The only difference between the two pairs of error terminologies is that FAR against FRR (and/or FMR against FNMR) consider all failures. In other words, FMR and FNMR assumes that all captured samples are usable.

The tradeoff between FMR and FNMR can be shown by using the Decision Error Tradeoff (DET) or Receiver Operating Characteristic (ROC) curves. The difference between the DET and ROC curve is the change in the y-axis, where (1-FNMR) is substituted instead of FNMR for the DET-curve. Next it is to decide the threshold one should use. This depends heavily on the application. The extreme cases for the thresholds are when FMR=1 and FNMR = 0, and when FMR=0 and FNMR=1. The first extreme case implies that you are always able to authenticate you as yourself (for every and each authentication), but so does everyone else, and not only are they able to authenticate them as themselves, but also as anyone else. Another way to interpret this is that you will have full convenience, but no security at all. The other extreme case implies that you can never authenticate you as yourself, but this also accounts for everyone else, so they can never authenticate as you either. Therefore you will have full security, but no convenience. So high security applications would tend to have as low FMR (or FAR) value as possible, which could be the case in forensics. But most civilian applications are in somewhere in-between the two mentioned. The Equal Error Rate (EER), which is the intersection between the plotted DET curve and the dashed red line (with a slope of 45 degrees), expresses the threshold where you have FMR=FNMR. This threshold gives this joint error rate, which is very commonly used to compare different systems against each other, and thus it generally gives one an idea of how well the system has performed.

3. FINGERPRINT RECOGNITION

Fingerprint recognition is the most matured approach among all the biometric techniques ever discovered. With its success of use in different applications, it is today used in many access controls applications as each individual has an immutable, unique fingerprint. The hand skin or the finger skin consists of the so called friction ridges with pores. The ridges are already created in the ninth week of an individual's fetal development life [7], and remains the same all life long, only growing up to adult size, but if severe injuries occur the skin may be reconstructed the same as before. Researchers have found out that identical twins have fingerprints that are quite different and that in the forensic community it is believed that no two people have the same fingerprint [8].

Many capture device technologies have been developed over the last decades replacing the old ink imaging process. The old process was based on sensing ridges on an individual's finger with ink, where newer technologies uses a scanner placing the surface of the finger onto this device. Such technologies are referred to as live-scan and based on four techniques [9]:

Frustrated total internal reflection (FTR) and optical methods is a first live scan technology. Figure 5 illustrates, how the reflected signal is acquired by a camera from the underside of a prism when a finger touches the top of the prism. The typical image acquisition surface of 1 inch by 1 inch is converted to 500 dots per inch (DPI) using either charge coupled device (CCD) or complementary metal oxide semiconductor (CMOS) camera.

CMOS Capacitance. The ridges and valleys create different charge accumulations, when a finger hits a CMOS chip grid. This charge is converted to an intensity value of a pixel using various competing techniques such as alternating current (AC), direct current (DC) and radio frequency (RF). The typical image acquisition surface of 0.5 inch by 0.5 inch is converted to 500 dots per inch (DPI). The resultant images also have a propensity to be affected by the skin dryness and wetness.

Ultrasound Sensing. The thermal sensor is developed by using pyro-electric material, which measures temperature changes due to the ridge-valley structure as the finger is swiped over the scanner

Security Comm. Networks 2012; **00**:1–12 © 2012 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

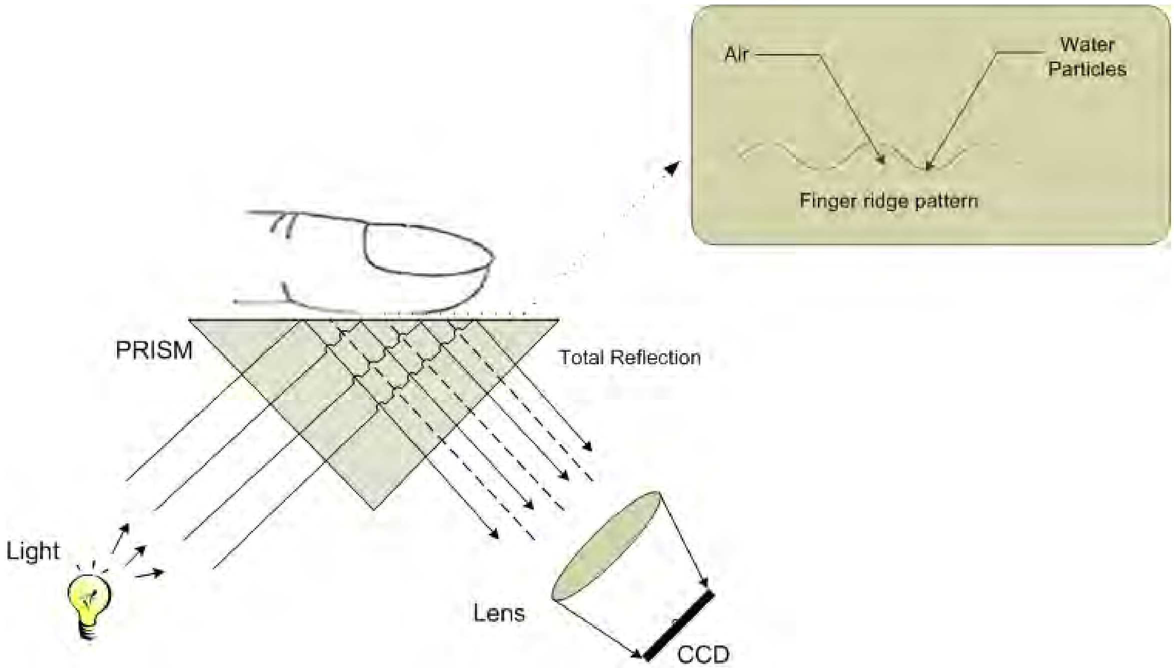

Figure 1. Optical fingerprint sensing by frustrated total internal reflection.

and produces an image. In this case the skin is a better thermal conductor than air and thus contact with the ridges causes a noticeable temperature drop on a heated surface. This technology is claimed to overcome the dryness and wetness of the skin issues of optical scanners. But the resulting images are not affluent in gray value images. The thermal sensor is becoming more popular today, because they are small and of low cost. Swipe sensors based on optical and CMOS technology are also available as commercial products.

4. DATA COLLECTION

4.1. Rationale

Besides fingerprint recognition systems deployed for applications with high-security requirements such as border control [10, 11] and forensics [12], fingerprint recognition is supposed to be promising for consumer markets as well for many years [13, 14]. In the meanwhile, privacy concerns over fingerprint recognition technologies' deployment in non-high-security applications have been raised [15, 16] and thus leads to a refrained development of biometrics in consumer market in recent years compared with the rapid development in the public sectors such as border control, critical infrastructure's access control, and crime investigations.

We suppose there are at least two ways to alleviating these privacy concerns. Biometric template protection [17, 18] is one of the most promising solutions to provide a positive-sum of both performance and privacy for biometric systems' users. The European Research Project TURBINE [19] demonstrated a good result in both performance and privacy of the ISO fingerprint minutiae template based privacy-enhancement biometric solutions. On the other hand, for the consumer market, we think using customers' own biometric sensors will also help alleviate the customers' privacy concerns. That is the motivation of this paper to try using cell phone cameras as sensors for fingerprint sample collection.

Obviously, for applications requiring high security, subjects' own biometric sensors may not be suitable for data collection unless the cell phone can be authenticated as a registered and un-tampered device in both software and hardware aspects, which is difficult to realize for a normal consumer electronics that is out of the control of the inspection party. However for consumer market, cell phone can be deemed nowadays as a secure device accepted by many customers, e.g, many banking services send transaction password, TAN code or PIN code via SMS to customers' cell phone. So in this paper we assume biometric data collection by the customers' cell phone cameras will not raise more privacy and security concerns to the customers than the cell phone based banking services.

In the meanwhile we expect technical challenges in quality control to the cell phone camera captured samples, especially from the sample image processing aspects such as bias lighting conditions and unstable sample collection environment caused by hand-holding. In addition, most

Figure 2. Left: CMOS Sesnor (HTC Desire), Right: CMOS Sensor (Nokia N90) and a cropped/contrasted fingerprint image from each cell, at the same scale factor.

existing cell phone cameras are not designed for biometric use and accurate focusing will always be a challenge for fingerprint image capturing. We address these potential challenges in this paper in a simplified way to investigate whether cell phone camera can generate good quality samples and corresponding good biometric performance in a relative stable data collection environment.

4.2. Data Collection Steps

As there is no standard benchmark database available for fingerprint images captured by digital camera, we constructed an independent database. The image database is comprised of 22 subjects from which fingerprint images were taken with a cell phone camera. The fingerprint data used in this paper are captured by two commercial sensors as shown in Figure 2. The cell cameras used were Carl Zeiss Optics from Nokia N95 and HTC Desires' embedded camera. Further detailed information of the sensors is described in Table I.

Cell Phone	**Nokia N95**	**HTC Desire**
Lens Type	**CMOS, Tessar lens**	**CMOS**
Mega Pixel	5.0	5.0
Resolution	2592x1944	2592x1552
Flash	LED Flash	LED Flash
ISO Speed	100 - 800	52
Auto-Focus	Yes	Yes

Table I. Cell phone camera setting for fingerprint image acquisition.

The constructed independent database comprises of 1320 fingerprint images. These images stem from 220 finger instances, where each instance was captured 6 times.

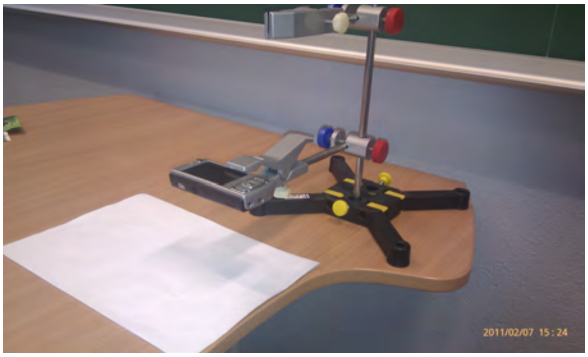

Figure 3. Setup for the Nokia N95 capture device.

The images are stored in the internal memory of the phones and all the images were collected in the camera's "Burst Mode". For evaluating the performance of various algorithms under different settings, the Nokia N95 was fixed placed on a hanger as illustrated in Figure 3 where images were taken by a human operator holding the phone and capturing images for the HTC Desire. The image capture was performed inside a laboratory with normal lighting conditions.

5. EVALUATION

As can be seen in Figure 4, the user initially presents its biometric characteristic (i.e., capturing the fingerprint) to the sensor equipment (i.e. camera in a mobile phone), which captures it as captured biometric sample. After preprocessing this captured sample, features will be extracted from the sample. In case of fingerprint biometrics, these features would typically be minutia points. The extracted features can then be used for comparison against corresponding features stored in a database, based on the claimed identity of the user. The result of the comparison is called the *similarity score* S, where a low value of S indicates little similarity, while a high value indicates high similarity. The last step is to compare the similarity score S to a predefined system *threshold* T, and output a decision based on both values. In case the similarity score is above the threshold ($S > T$) then the user is accepted as genuine, while a similarity score below the threshold ($S < T$) indicates an impostor who is rejected by the system. Obviously the biometric features of the user must initially be stored in the database before any comparison of a probe feature vector can take place. This is done during the *enrolment phase*. During the enrolment biometric samples are captured from the biometric characteristic, after which it is processed and features are extracted. The extracted data is now stored in a database and linked to the identity of the user who enrolled. The stored data in the database is referred to as the *reference template* of the user. In case of fingerprint biometrics it is a common approach to derive the features

Security Comm. Networks 2012; **00**:1–12 © 2012 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

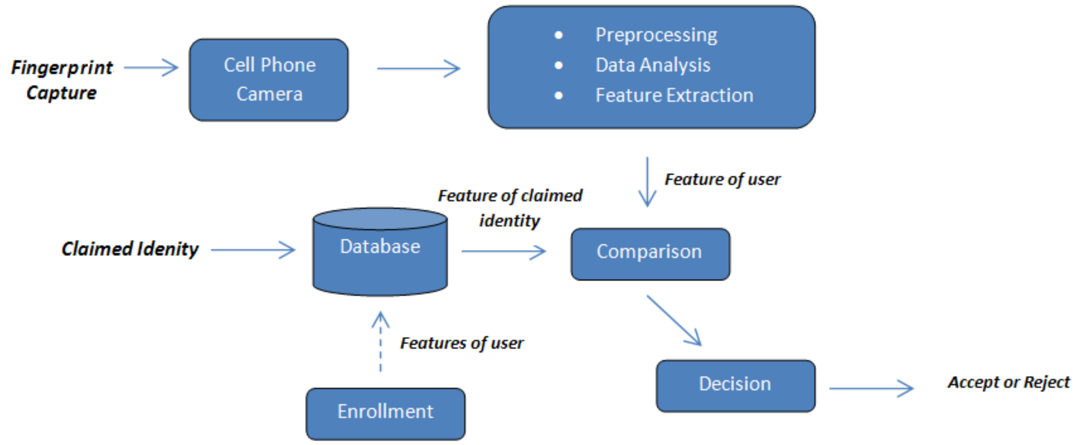

Figure 4. A traditional verification process.

from multiple captured samples and generate a single minutiae template.

5.1. Feature Extraction

In order to measure the sensor performance we have applied the Neurotechnology, Verifinger 6.0 Extended SDK commercial minutia extractor for the feature extraction. The SDK includes functionality to extract a set of minutiae data from an individual fingerprint image and to compute a comparison-score by comparing one set of minutiae data with another. Both SDKs support open and interoperable systems as the generated minutiae templates can be stored according to the ISO or ANSI interchange standard.

5.2. Feature Comparison

We compared the verification results of the Neurotechnology algorithm on the processed images. For each algorithm the error rates were determined based on a threshold separating genuine and impostor scores. The False Match Rate (FMR) and False None-Match Rate (FNMR) were calculated. The calculation of FMR and FNMR is done in the following way. We have collected N data samples from each of M participants, then we have calculated similarity scores between two samples, either stemming from one finger instance or from two different instances. A similarity score between two samples from the same source is called a genuine score, while an impostor score is the similarity score between two samples from different instances. Given our setting, we can have $N * M$ data samples from which we can calculate the total number of $N_{Gen} = \frac{M*N*(N-1)}{2}$ different genuine scores and $N_{Imp} = \frac{M*N*(M-1)*N}{2}$. Given these sets of genuine and impostor scores we can calculate FMR and FNMR for any given threshold T as follows:

$$FMR(T) = \frac{\#incorrectly\ accepted\ impostor\ images \geq T}{Total\ number\ of\ impostor\ images} \quad (3)$$

$$FNMR(T) = \frac{\#incorrectly\ rejected\ genuine\ images < T}{Total\ number\ of\ genuine\ images} \quad (4)$$

From this, we can find the point where FNMR equals FMR, or in other words the Equal Error Rate (EER). This rate is very common used value which is being used to compare different systems against each other, and it roughly gives an idea of how well a system performs.

The images that were generated with the mobile phones encode the finger position according to Table II and the equal error rates retrieved corresponding to the finger codes are overviewed in Table III

Finger Position	Code
Right thumb	1
Right index finger	2
Right middle finger	3
Right ring finger	4
Right little finger	5
Left thumb	6
Left index finger	7
Left middle finger	8
Left ring finger	9
Left little finger	10

Table II. Finger position codes according to ISO 19794-2.

In general we see that the left index finger (code 7) has performed best for both phones with EER of 0.0% and 8.47%. The overall performance (cross comparison of all

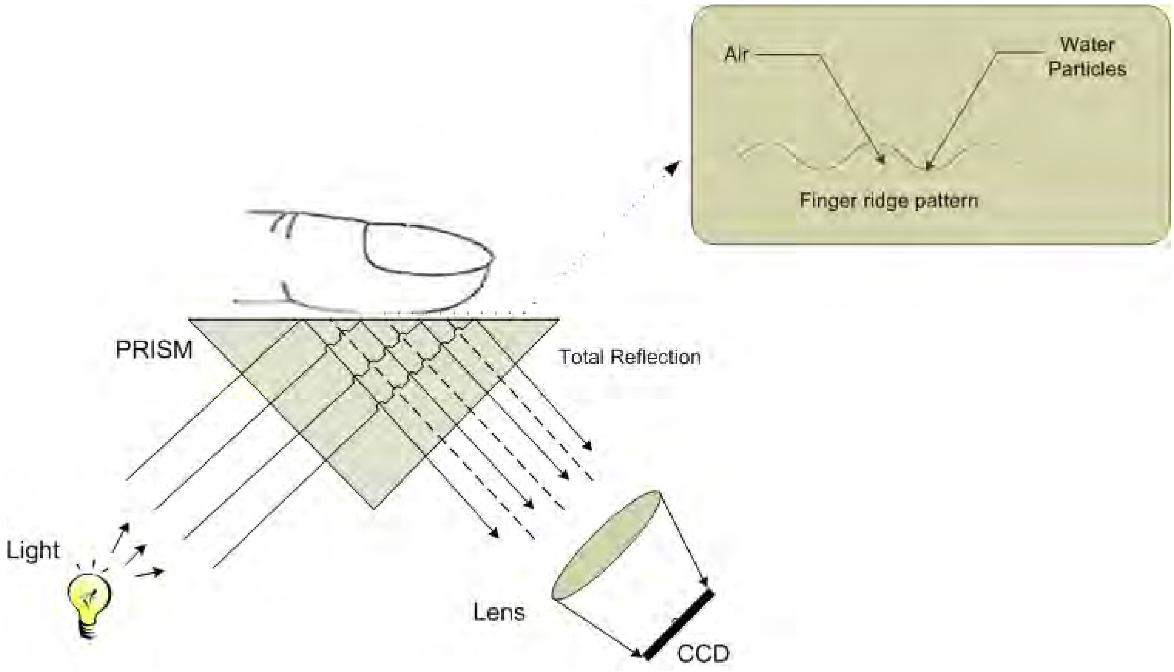

Figure 5. Optical fingerprint sensing by frustrated total internal reflection.

Cell Phone	1	2	3	4	5	6	7	8	9	10	all
Nokia N95:	5.77	5.92	5.11	7.36	5.43	2.98	0.0	0.43	6.26	5.45	4.66
HTC Desire:	11.73	11.43	23.62	21.17	16.01	10.98	8.47	15.37	16.11	15.96	14.65

Table III. EERs of cell phone fingerprint recognition. Numbers are in percentage.

ten fingers) which can be seen in column *all* for Nokia N95 performs significantly better than the Desire. This is so because of various reasons. The Nokia was placed in fixed way on the holder while capturing. Furthermore, the Nokia was set to an internal close-up mode setting. This mode is ideal for capturing details of small objects within a distance between 10 and 60 cm. Here we had to ensure that the auto-focus always resulted in better quality images at a small distance when capturing the fingerprints, whereas the HTC was manually adjusted by the human operator. Thus, this means that the Nokia N95's auto-focus was performing slightly better than the HTC Desire.

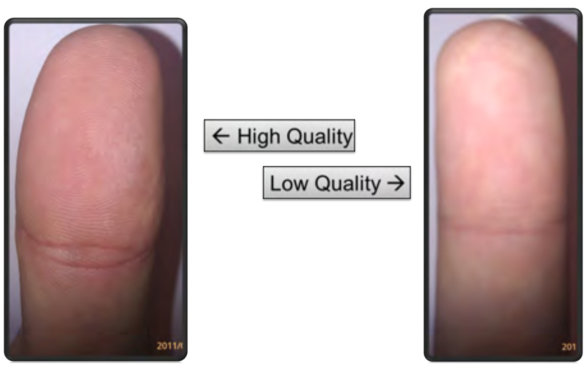

Figure 6. Left: High Quality Image, Right: Low Quality Image.

6. CHALLENGES

6.1. Image Quality Assesment

Fingerprint image quality is an important factor in the performance of fingerprint recognition in general including mobile devices. It is used to evaluate the system performance, enrollment acceptability, and evaluate fingerprint sensors. High quality images require less preprocessing and enhancement, while low-quality images the opposit. In Figure 6, fingerprint images of different qualities are taken from the same mobile phone - namely the HTC Desire. The left fingerprint in the figure shows the high quality fingerprint where the ridges and valleys are clear and have a good contrast. This means that the minutia are easily detectectable when processing. The right fingerprint is an example of an low-quality image. This pictures would be categorized as a totally corrupted picture, where ridges and valleys are not possible to see and minutia are not possible

Security Comm. Networks 2012; **00**:1–12 © 2012 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

to detect. In the following we will see the affect of quality when it comes to the (de)activation of flash om the phone.

6.2. Flash

Almost every mobile device has a built-in camera with flash. The flash is used used in photography creating an artificial light to help illuminate an object/scene. One purpose is to use the flash at night to ligthen a dark scene. And most mobile device cameras often activate flash units automatically. The advantage of camera phones flashes is that they are produces with LEDs over xeno. This means that they use less power and have a higher efficiency and extreme miniaturization.

When it comes to fingerprint capture, the flash has something to say, which is illustrated in Figure 7 Depending on the background, the flash can create either

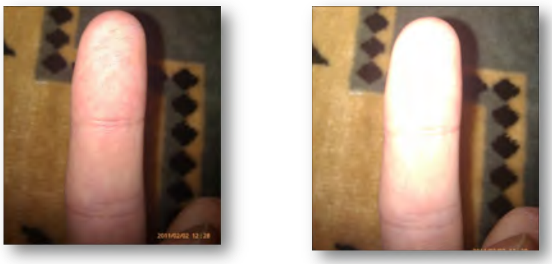

Figure 7. Left: Image with Flash, Right: Image Without Flash

and high quality image of the fingerprint, and in the same time a non-acceptable image. This in itself is a challenge. If an application is to be for fingerprint recognition, the mobile device application should know if the flash should be activated or not.

Since the flash is dependent on the background, we will in the next section go into some examples how fingerprint images are affected by background.

6.3. Background

In the following, we will observe the affect when the background is different. In Figure 8, a picture is taken with a plain white background with flash. What we observe is that the image is very clear and processing of the image could easily be performed.

Without flash, the image would be useful too, but not as clear as with flash. Thus we can conclude, that by having a plain white background with or without flash, the processing would be useful for the mobile device to perform fingerprint recognition.

Moving from a white background to a more pattern based background like a desktop table, such as illustrated in Figure 9, we observe a smaller change in the quality. The picture was taken with flash but we did not loose much information. Still we are able to perform minutia detection, but first a contrast enhancement and some other preprocessing techniques to make the picture even more

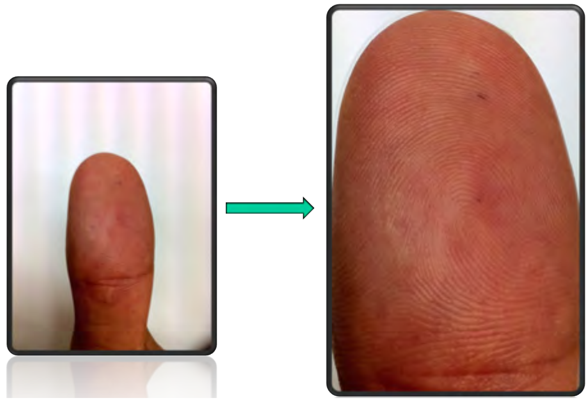

Figure 8. Fingerprint image taken with plain white background.

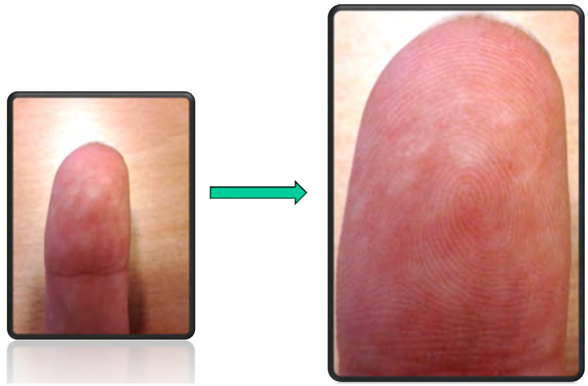

Figure 9. Fingerprint image taken with a pattern based (table) background.

bright should be performed. Without flash, the image would still be useful with sligth changes, but still clear and usable.

Figure 10. Fingerprint image taken with a complex background from an i-Phone 4.

The greatest challenge would be when the background is complex. A complex backgroun is defined by multiple objects in the background as illustrated in Figures 10 and 11. The difference here is that these two pictures are taken by two different cameras with 5 Mexapixel. The first image is taken with an Iphone 4 while the other image is taken with a Samsung S800 mobile phone. What

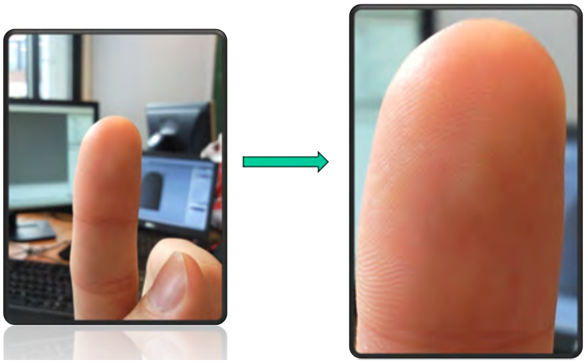

Figure 11. Fingerprint image taken with a complex background from a Samsung S800.

these two phones have not in common is the focus of the camera lens. And as explained earlier in this article, we see that some phones has options to focus on macro objects - meaning that the lenses can have a full focus on an object up to 7 cm - and in this case disregard the background. For a fingerprint recognition application it is thus important that the application developed takes this focus into consideration.

6.4. Geometric Distortions

Some general issues on fingerprint recognition is the rotation and translation of a fingerprint. Most of state of art minutiae comparators can well deal with the geometric distortions (affine transformation (translation, rotation, scaling) and other non-linear transformations) in the minutiae templates. It might be the case that a user has rotated his finger while capturing. In this case it usual to create some algorithms for that to ensure that all fingerprints taken has a standard when comparing. What happens if a fingerprint is taken from a distance of 5 cm, and later on taken from a distance of 7 cm. Normalization has to be performed. Figure 12 shows an example of a rotated finger. Even if the finger is rotated from a certain distance it is still possible to detect important features as illustrated. In this image, the fingerprint image has been rotated and enhanced with contract enhancement.

For a stable fingerprint recognition application to be performed in a mobile device we have in this section shown challenges that needs to be taken into consideration.

7. DISCUSSION

Since personal mobile devices at present time only offer means for explicit user authentication, this authentication usually takes place one time; only when the mobile device has been switched on. After that the device will function

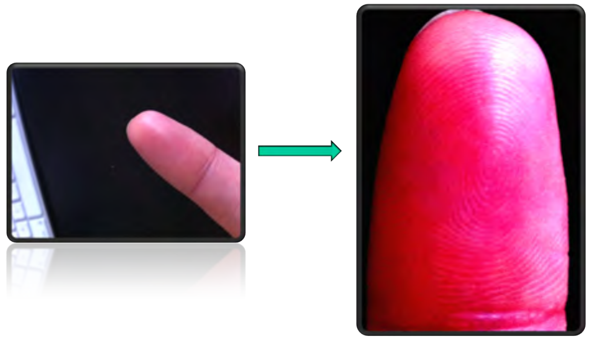

Figure 12. Left: Orignal fingerprint image taken, Right: Modified and Rotated Image

for a long time without shielding user privacy. As of today the majority of Internet users are expecting a transparent transition of services from the wired to the wireless mobile world. As personal mobile devices such as Apple's iPhone, T-Mobile's G1 or Nokia's S60 become more popular the ordinary user is expecting and using the full range of Internet services in the mobile Internet, since former limitations with regard to screen size and interaction capabilities (zooming, "copy and paste" functionality etc.) disappeared recently. In fact many users are even extending their expectations from their home and office environment, as they enjoy typical mobile features, such as location-based services, which are supported by widespread GPS-features.

On the contrary users tend to ignore the risks, which they accept while operating Internet services from their mobile device. Not only sensitive information is accessible from the mobile device but also transactions on the stock market and other critical services, which grant access to financial assets. At the same time mobile devices are more exposed to the public and thus there is likelihood that a mobile device is lost or stolen in an unattended moment. This threat is shown by the number of approx. 10.000 mobile phones, which were left in London taxis every month in 2008 [20].

It is obvious that a mobile Internet can only exist, if there is a strong link between the mobile device and the authorized user of that specific device. This requires that proper access control mechanisms are in place, to control that the registered user and only the registered user operates the mobile device. Unfortunately most mobile devices are operated today with knowledge-based access control only, which is widely deactivated due to the associated inconvenience.

A promising way out of these pressing problems is to implement on mobile devices secure biometric access control mechanisms, which provide a non-reputable approach based on the observation of biological characteristics (i.e. the fingerprint) of the registered user. The aim of a biometric access control process is, to determine whether the biometric characteristic of the interacting subject and the previously recorded representation in the reference data match.

A possible application scenario of a the fingerprint biometric user verification system in a mobile device could be as follows; When a device such as a mobile phone, is first taken into use it would enter a "practicing" learning mode where the high quality fingerprints data are processed and stored. Password-based or PIN code user authentication would be used during the learning session. If the solidity fingerprint biometrics was sufficient enough, the system would go into a biometric authentication "state", a state that will need confirmation from the owner. In this state the system would asynchronously verify the owner's identity every time the owner wanted to authenticate.

8. CONCLUSION

The cell phone camera database has been used to study the performance of some fingerprint verification algorithms in a first step towards real-life situations. The database has scaled and posed distortions in addition to illumination. The camera lens' cause further distortion in the images with changes in orientation.

The novel biometric method for frequent authentication of users of mobile devices proposed in this paper was investigated in a technology test. It contained fingerprints data. The recognition resulted in different performances of using one minutia extractor and comparator. The best algorithm performance gained resulted in an EER of 4.66.% for the Nokia N95. Looking forward into which finger was performing best, then we observe an EER of 0.0% for the left index finger as well.

The shown results suggest the possibility of using the proposed method for protecting personal devices such as PDAs, smart suitcases, mobile phones etc. In a future of truly pervasive computing, when small and inexpensive hardware can be embedded in various objects, this method could also be used for protecting valuable personal items. Moreover, reliably authenticated mobile devices may also serve as an automated authentication in relation to other systems such as access control system or automated external system logon.

ACKNOWLEDGEMENT

We would like to thank Simon McCallum and Jayson David Mackie for using their cell phones for the experiment. Furthermore, we would like to thank all volunteers participating in the data collection.

REFERENCES

1. Mobile phone theft increasing across the uk. http://www.insure4u.info/home-insurance-mobile/mobile-phone-theft-increasing-across-the-uk.html. [Online; accessed 30-March-2011].
2. Shakir Ullah Shah, Fazl e Hadi, and Abid Ali Minhas. New factor of authentication: Something you process. *Future Computer and Communication, International Conference on*, pages 102–106, 2009.
3. Nist image group's fingerprint research. http://www.itl.nist.gov/iad/894.03/fing/ fing.html. [Online; accessed 13-February-2011].
4. Davrondzhon Gafurov, Patrick Bours, Bian Yang, and Christoph Busch. Guc100 multi-scanner fingerprint database for in-house (semi-public) performance and interoperability evaluation. *Computational Science and its Applications, International Conference*, pages 303–306, 2010.
5. Robert Mueller and Raul Sanchez-Reillo. An approach to biometric identity management using low cost equipment. *Intelligent Information Hiding and Multimedia Signal Processing, International Conference on*, pages 1096–1100, 2009.
6. Bee Yan Hiew, Andrew Beng Jin Teoh, and Ooi Shih Yin. A secure digital camera based fingerprint verification system. *J. Vis. Comun. Image Represent.*, 21:219–231, April 2010.
7. Fetal development. http://www.pregnancy.org/fetaldevelopment. [Online; accessed 13-February-2011].
8. Sharath Pankanti, Salil Prabhakar, and Anil K. Jain. On the individuality of fingerprints. *IEEE Trans. Pattern Anal. Mach. Intell.*, 24:1010–1025, August 2002.
9. Ruud Bolle, Jonathan Connell, Sharanthchandra Pankanti, Nalini Ratha, and Andrew Senior. *Guide to Biometrics*. SpringerVerlag, 2003.
10. Safety & security of u.s. borders: Biometrics. http://travel.state.gov/visa/immigrants/info/info_1336.html. [Online; accessed 13-February-2011].
11. 2004/512/ec: Council decision of 8 june 2004 establishing the visa information system (vis). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:32004D0512:EN:NOT. [Online; accessed 13-February-2011].
12. Method for fingerprint identification. http://www.interpol.int/public/Forensic/ fingerprints/WorkingParties/IEEGFI/ieegfi.asp. [Online; accessed 13-February-2011].
13. Fingerprint payment heads for the uk. http://www.talkingretail.com/news/industry-news/fingerprint-payment-heads-for-the-uk. [Online; accessed 13-February-2011].
14. Fingerprint biometric retail pos systems on show. http://www.prosecurityzone.com/News/Biometrics/ Fingerprint_recognition/Fingerprint_biometric_retail_pos_

systems_on_show_16250.asp #axzz1Dr8cNsOu. [Online; accessed 13-February-2011].

15. Retailers fingerprint plans prompt privacy concerns. http://www.computing.co.uk/ctg/news/1826631/retailers-fingerprint-plans-prompt-privacy-concerns. [Online; accessed 13-February-2011].
16. Europe tells britain to justify itself over fingerprinting children in schools. http://www.telegraph.co.uk/news/worldnews/europe/eu/8202076/Europe-tells-Britain-to-justify-itself-over-fingerprinting-children-in-schools.html. [Online; accessed 13-February-2011].
17. Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar. Biometric template security. *EURASIP J. Adv. Signal Process*, 2008:113:1–113:17, January 2008.
18. *ISO/IEC FDIS 24745 Information technology – Security techniques – Biometric information protection, FDIS, Feb. 2011.*
19. Eu fp7 integrated project - trusted revocable biometric identities. http://www.turbine-project.org/. [Online; accessed 13-February-2011].
20. Security park: 60,000 mobile phones left in london taxis in the last six months. http://www.securitypark.co.uk/security_article262056.html. [Online; accessed 13-February-2011].

Security Comm. Networks 2012; **00**:1–12
DOI: 10.1002/sec
Prepared using secauth.cls