Mobile Wrist Vein Authentication Using SIFT Features

Pol Fernández Clotet

MASTERARBEIT

eingereicht am
Fachhochschul-Masterstudiengang

Mobile Computing

in Hagenberg

im Juni 2017

Declaration

I hereby declare and confirm that this thesis is entirely the result of my own original work. Where other sources of information have been used, they have been indicated as such and properly acknowledged. I further declare that this or similar work has not been submitted for credit elsewhere.

Hagenberg, June 12, 2017

Pol Fernández Clotet

Contents

Preface

I would like to thank Rainhard Dieter Findling at the University of Applied Sciences Upper Austria Hagenberg for the opportunity to do this master thesis under his supervision, which has been very interesting and rewarding. His helpful and instructive advices have been very useful and inspiring during the entire development of this work.

I would also like to thank my family for the support, motivation, and encouragement during the entire master. Finally, I would not like to forget to thank my friends and colleagues, who have always been there supporting and helping me.

Parts of this thesis have previously been published or are submitted for review in [10].

Pol Fernández Clotet,
Hagenberg, July 2017

Abstract

Mobile devices store sensitive and private data which has to be secured. To protect this data most of these devices implement authentication mechanisms like PIN, password, or unlock pattern. However, these approaches can be problematic in terms of usability and security. Users do not want to remember multiple and difficult authentication secrets, hence they tend to use easy and short secrets which are vulnerable to be captured and replayed by attackers. In recent years biometrics have become important for authentication on modern mobile devices. Thereby, different biometrics do not have to be remembered by users and are differently hard to observe by attackers. For example, veins used in vein pattern authentication remain hidden when not using specialized hardware. In this work we present a low cost mobile wrist vein authentication system based on Scale-Invariant Feature Transform (SIFT). We implement a low cost vein capturing sensor using near-infrared (NIR) illumination and a filter modified camera. For authentication we present an image preprocessing methodology and an image matching algorithm based on SIFT features. In parallel, using the proposed sensor we build up a self-recorded wrist vein database which contains 120 wrist vein images. Furthermore, we develop six different authentication decision models using 1 or 4 samples for enrollment and authentication. Then, we evaluate their performance using the self-recorded database and compare them with other existing vein authentication works. Concluding, our results indicate that the presented system using the proposed capturing sensor and SIFT features algorithm using 4 samples for enrollment is a viable approach for mobile wrist vein authentication.

Chapter 1

Introduction

1.1 Motivation

Nowadays modern mobile devices have access to, store, and process a lot of private information, including messaging (short message service (SMS), email), contacts, access to private networks (virtual privat network(VPN), WiFi), photos, or even mobile banking (eBanking, ePayment [1]). Thus, many devices provide local device access protection mechanisms, such as PIN, password, patterns. With those mechanisms the authentication secret could be easily forgotten and also observed by attackers using shoulder surfing and used in replay attacks. However, there are stronger mechanisms, like some biometrics, which are more difficult to observe by attackers, as they largely remain hidden without using special sensors. For example, observing biometric information is harder for vein than for face authentication as veins remain mostly hidden for human eye, whereas the face is easily captured with a normal camera. The idea behind this is that by combining multiple such biometrics, also including weak biometrics like gait, or voice [42], strong and reliable mobile authentication can be achieved [11]. Thus, we can protect our private information with stronger and more difficult to spoof security mechanisms.

One biometric authentication less explored with mobile devices is vein authentication, which has gained popularity outside the mobile environment for being contactless. Furthermore, as skin largely absorbs the visible spectrum of light, veins mostly remain hidden in normal conditions, which prevents vein from being reliably observed in this spectrum. Light in the NIR or far-infrared (FIR) spectrum has maximum depth of penetration of skin tissue with only hemoglobin absorbing it. This makes vein authentication harder to be spoofed by attackers as the secret can not be obtained without a special camera.

Hence, to obtain the secret veins are illuminated with NIR/IR light and captured using cameras with optical NIR/IR bandpass filters [34, 52]. Most vein authentication approaches use finger, hand dorsal, palm, or wrist vein patterns [59, 63], with vein capturing devices designed for medical and security fields of research [26]. Usually, this special sensors are very expensive and make vein biometric systems more costly than

[1] Electronic banking system that facilitates users of a financial institution in making financial operations, such as payments, through the Internet.

less secure, but more common systems like fingerprint authentication.

At the end, for mobile users wrist veins have the advantage of being relatively easy to access – which could be used e.g. with smart-watches, or smart-wristbands thereby not requiring any additional effort or changes in user behavior.

1.2 Goal

The goal of this thesis is to investigate wrist authentication using SIFT features and its application to the mobile environment. Our main contributions are:

- Development of a low cost wrist vein capturing device.
- Using and evaluating SIFT features for vein authentication.
- Evaluation of our approach using a self recorded wrist vein database.

1.3 Outline

This work is organized as follows: chapter 2, explains the existing authentication solutions for mobile devices. In chapter 3, we present the existing methods and technologies used in vein authentication systems. Thus, we summarize the principal vein capturing, vein preprocessing, and vein pattern matching techniques. Following, in chapter 4, we present vein authentication research projects and commercial products, hence we give an overview of the most common technologies and approaches used for vein authentication. Further, in chapter 5 we present our wrist vein authentication approach. With the methods and technologies learned from previous chapters, we present the main parts of the proposed vein authentication system, giving an overview and the explanation of the methods and technologies used in each block. In chapter 6 we evaluate our approach. Therefore, we explain in detail all parameters and methodologies used to build our capturing prototypes and models and measure their performance. Then, in chapter 8 we explain the characteristics of the system's application and evaluate its computational requirements using a mobile prototype. Finally, in chapter 9 we summarize and conclude lessons learned from this work. In addition, future work and suitable solutions to improve the system's results are presented in this last chapter.

Chapter 2

Authentication on Mobile Devices

Mobile devices store personal and important data which has to be protected from attackers. One way to protect this data from unauthorized access of third parties is by user authentication. Nowadays there are three types of security mechanisms to provide user authentication: a) knowledge based, b) biometrics, and c) token based. When using knowledge authentication users have to remember a secret, such as a password, to authenticate to the system. For biometrics authentication, the users possess the secret to authenticate, such as a fingerprint. And with token based authentication users possess a small hardware device such as a smart card, a key, a certificate, a token device. With this security tokens the system provides an extra level of assurance though a two-factor authentication method.

Nowadays, the most frequently used security mechanism is the one based on knowledge, although, biometrics are becoming very popular. Depending on the system requirements, there are authentication mechanisms that fit better than others. There are some systems, like mobile devices, where usability when authentication is very important. In this case, most users prefer to have an easy and fast authentication system rather than strong and difficult to use. Hence, when implementing a security system many measures have to be considered. The most influencing aspects on the usability of an authentication system are: time, user effort, cognitive load, and invasiveness.

2.1 Knowledge based

The most widely security mechanism in current mobile devices is the one based on user knowledge [5, 35]. The secret is provided by the user's knowledge through different inputs such as PINs, passwords, or graphical patterns. As the secret relays on the user's memory, every time the user wants to access the protected information has to remember the secret. This makes that many users tend to reuse the same secret for different systems, as using different ones can be difficult to remember. Another factor that influences the security of the knowledge based systems is the complexity of the secret. If we want to strongly protect the system, the secret should be as complex as possible. However, this leads to many users choosing an easy secret because of: 1) having an easy secret to be remembered, and 2) have a faster way to unlock the device – many complex secrets require time and attention from the user when being entered on

the mobile device. This lack of stability between the complexity of the secret and the usability of the knowledge based authentication into system makes that some users neglect the security of their devices.

2.1.1 PIN

PIN authentication in mobile devices is usually based on a secret of 4 digit numbers that the user enters to protect the device. In this case, the security secret is easy to remember and fast to input for the user, as it has 4 digits of length (see figure 2.1a). Despite, it generates a vulnerability as only $\left(\!\left(\begin{smallmatrix}4\\10\end{smallmatrix}\right)\!\right) = 10000$ possible secrets exist, resulting an entropy [1] of only $\frac{log(10000)}{log(2)} = 13.3$ bit. That makes brute force attacks [2] dangerous for this type of security mechanism.

2.1.2 Password

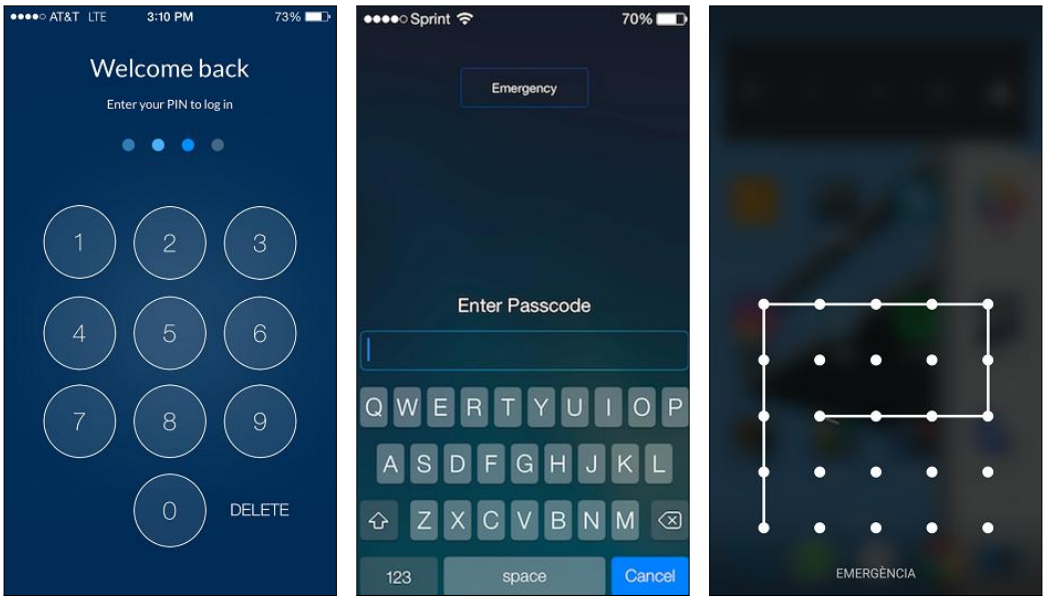
Password unlock mechanisms on mobile devices are basically the same as PIN based approaches but using a password (sequence of all existing characters with an arbitrary length) instead of only digit numbers. In contrast to PIN based authentication, passwords can be larger secrets. Thus, for the user is harder to remember and also more difficult and slower to enter. PIN keyboards are usually bigger than password keyboards as they only show 10 digits (see figure 2.1b). Passwords keyboards, instead, are smaller and combine multiple layouts for special characters or numbers. This layout can make the action of unlocking the device slower for the user [43]. On the other hand, this type of security is stronger, as the secret length and complexity is higher than PIN, which makes it harder to break using brute force attacks.

2.1.3 Graphical Pattern

With a graphical pattern based mobile authentication, the user enters the secret by connecting arbitrarily a sequence of fixed dots without repetition (see figure 2.1c). To unlock the device, the user has to input the same sequence in the same order into the fixed dots. To generate this secret, there are multiple fixed patterns, which can be composed of different number and geometrical formation of dots. In this case, the user needs to remember a sequence of dots instead of a PIN or password, and depending on the geometrical formation of dots the secret can be more or less complex.

[1] Measurement of the randomness, or unpredictability of a password.

[2] In cryptography, a brute-force attack consists of an attacker trying systematically many possible passwords until the correct one is found.

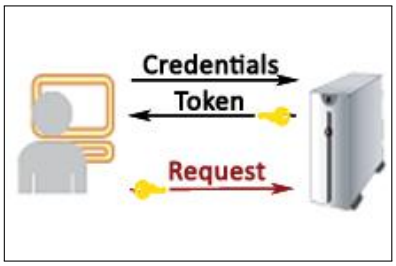


(a) (b) (c)

Figure 2.1: Mobile device locked screens: (a) PIN authentication [74], (b) password authentication [75], and (c) pattern authentication.

2.2 Token Based

A token based authentication systems provide authentication using a non-password scheme (see figure2.2a). In many cases tokens may store biometric data or passwords. There are two types of tokens: password tokens, and physical tokens. To prove identity in password tokens, the user needs to obtain the information contained inside the token. This mechanisms are frequently used in online banking. The user gets a code from the bank server, and by entering it into the token device obtains a password which allows him to access the banking information (see figure 2.2b). Using physical tokens, the user can prove the identity by using the secured information stored inside the physical token. The secret is usually stored into a chip which provides different authentication functionalities depending on the complexity of the system (see figure 2.2c). In recent years, mobile devices have been used as physical tokens for obtaining the secured information. This authentication is also known as two-factor authentication [85]. The user to have access to the secured information, receives a SMS with the authentication secret, or through an application protected with a PIN, generates a one time password and obtain the secret license for the user [76]. Because of this two-step authentication token based is not commonly used on mobile devices authentication. However, it is frequently used in e-banking, where strong security mechanisms are needed and the user does not worry about doing a two-step authentication, and mobile devices are frequently used in one of these two steps authentication.



(a)

(b)

(c)

Figure 2.2: Token based authentication: (a) token authentication adapted from [70], (b) password token based [85], and (c) mobile physical token based [76].

2.3 Biometrics

An alternative to knowledge and token based security mechanisms is using the user's biometric information for authentication. Biometrics are currently becoming very common in mobile devices' unlock systems as they can solve the two main problems with the previous security mechanisms: 1) then can provide a strong and complex secret which the user does not need to remember, and 2) in most cases the user does not need to make a big effort to authenticate [50]. There are a lot of projects and surveys about biometrics authentication [7, 25, 41]. Many measures can be taken to evaluate these comparison, an example is shown in table 2.1, where common biometrics are compared by grading different performance measures in high (+), medium (·), or low (-).

Moreover, for each individual we can obtain two types of biometrics: physical and behavioral. Making a differentiation between these two, in this section we present the most used and well known biometrics used for authentication.

Table 2.1: Comparison of multiple biometrics adapted from [7, 25].

Biometric characteristic	Universitality	Distinctiveness	Perfmanence	Collectabillity	Performance	Acceptability	Circumvention
Facial thermogram	+	+	-	+	·	+	-
Hand vein	·	·	·	·	·	·	-
Gait	·	-	-	+	-	+	·
Keystroke	-	-	-	·	-	·	·
Odor	+	+	+	-	-	·	-
Ear	·	·	+	·	·	+	·
Hand geometry	·	·	·	+	·	·	·
Fingerprint	·	+	+	·	+	·	·
Face	+	-	·	+	-	+	+
Retina	+	+	·	-	+	-	-
Iris	+	+	+	·	+	-	-
Palmprint	·	+	+	·	+	·	·
Voice	·	-	-	·	-	+	+
Signature	-	-	-	+	-	+	+
DNA	+	+	+	-	+	-	-

2.3.1 Physiological Biometrics

Physical biometrics are obtained from the individual's physical traits. Those are assumed to be relatively unchanging, and unique for each individual such as fingerprint, face, iris/retina, veins, and hand/palm [30]. We shortly highlighted some frequently used physiological biometrics including fingerprint, face, and vein.

Fingerprint Authentication

Humans fingertips contain patterns of valleys and ridges. These patterns are considered to be unique to individuals and not change over the years [23]. In fingerprint authentication, the system recognizes a user by capturing the fingerprint and represent its unique characteristics by extracting a set of features commonly by:

- Patterns: including arch, loop, and spiral of the fingertip skeleton.
- Minutia features: including ridge ending, and bifurcation of the fingertip skeleton.

This captured fingerprint is used as the secret to authenticate each individual. One of the main benefits of fingerprint authentication is that the fingertip is closely tied to the individual. However this sometimes requires users to touch a biometric scanner to authenticate. Thus, some users dislike the idea of touching these scanners. An example of this contact authentication system is Touch ID, a fingerprint recognition feature, designed and released by Apple Inc. They claim to use a capacitive touch to detect the

user's fingerprint [15]. To tackle this issue, touch-less fingerprint authentication has been developed [31]. As fingerprint is visible, some systems like ICE Unlock Pro Lockscreen simple use the phone's camera to capture the pattern and authenticate against the enrolled fingerprint for the device [72].

Face Authentication

One of the most widely used biometric for personal recognition is facial images. This biometric has the advantage of using non-intrusive methods and being contactless. Moreover, users are used to have their photo taken. The used authentication steps are similar to fingerprint authentication. A sample of the face is taken and transformed into a set of features which are used for matching different face images (see figure 2.3b). The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces [23]. The applications of facial recognition range from static to dynamic face identification. In static face identification, the individuals enroll to the system taking one or several images facing the camera. In these images the possible motion of the user and the different facial expression are not considered. This approach is mainly used in authentication for example in mobile devices or personal computers. In dynamic face identification the user enrolls to the system in a static way. However to perform identification or authentication a frame of images from the individual's face is recorded considering: motion, and facial expressions. This identification process can be harder as in most cases the user is not facing the camera, hence rotation and scaling variances have to be considered. This approach is mainly used for individuals identification for example in subways, airports, or casinos. There are some drawbacks in both face authentication methods. One is that some users might attempt to change the appearance, perhaps by wearing glasses or growing a beard. This fact can decrease the system's security, by accepting or rejecting the wrong user. Another drawback is that face like fingerprint, is well visible for attackers. They can thereby easily record a user's face by taking a picture and try to spoof our identity.

There are several existing commercial products based on mobile facial recognition, such as BioID, a mobile face regonition application that allows users to authenticate into applications and websites [68] using the mobile phone camera to capture face pictures.

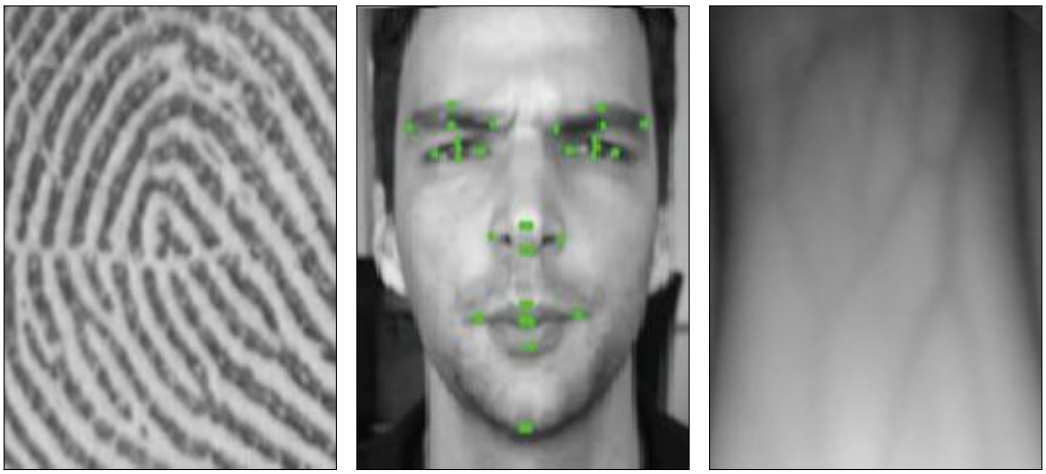
Vein Authentication

Vein recognition systems are one of the newest biometric technologies that have emerged in recent years. Vein authentication usually uses the vascular patterns of an individual's part of the body such as the palm, a finger, the wrist, or the palm of the hand as personal identification data.

Vein patterns are sufficiently different across individuals, and they are stable unaffected by aging (see figure 2.3c). Thus, the vein patterns are unique to each individual, even among twins [34].

The matching methodology for veins is similar to fingerprint and facial recognition. After capturing the vein pattern, it is uniquely represented by a set of features which is used to compare different vein patterns. In addition, compared to fingerprint and

face biometrics, veins are considered to be a highly secure biometric because of the sub-dermal nature of veins. On the other hand, as veins remain hidden for human eye, a special sensor is needed to capture the pattern. This requirement makes the vein authentication systems more secure but, at the same time, more expensive.



(a) (b) (c)

Figure 2.3: Physiological biometrics: (a) fingerprint [23], (b) face [14], and (c) wrist vein.

2.3.2 Behavioral Biometrics

Another type of biometrics known as behavioral biometrics can be obtained from human actions such speaking, walking or writing. This biometrics are obtained and learned by individuals over time. This biometric authentication continuously collects information about a user activity. Thus, behavioral biometrics can also be tracked at the same time as performing another activity, without the user's direct interaction. One drawback of behavioral biometrics is that the behavioral part of an individual can change over time due to age, medical conditions and emotional state. Hence, a human does not walk the same way when an ankle injury, or when being tired instead of full of energy. Behavioral biometrics for authentication must be trained to the individual's actions at enrollment time. Often, more than one enrollment session necessary. Then, behavioral recognition methods distinguishes individuals by matching particular activity samples against others. In this section we shortly highlighted some frequently used behavioral biometrics such as the voice, the gait, or the written signature.

Voice Authentication

Voice can be used to authenticate users when speaking. Humans frequently perform this recognition. They are able to recognize other humans only by their voice without seeing them. This is because each individual's voice sounds different depending on physical characteristics such as vocal tracts, mouth, nasal cavities, and lips. These characteristics of the human speech are invariant for an individual, but as mentioned before behavioral

biometrics can be affected by external factors. Thus, people do not necessarily sound the same when having a cold or being healthy. In voice authentication, the user's voice sample is trained and recorded, mainly with a microphone, in the enrollment session [42] (see figure 2.4a) and compared to other users samples.

Gait Authentication

Gait is the peculiar way that an individual walks. This authentication method is known for not being very distinctive among individuals but can be used in some low security applications. Due to change in body weight or other body factors this biometric's cycle may not remain the same over aging (see figure 2.4c). This biometric can be captured using a video sequence or a sensor. With video sequence different walking movements are captured with a camera on the training session. Hence, this method can be computationally quite expensive. Another alternative is by using a wearable sensor. Usually this sensor is placed on the shoe and records the pattern of acceleration (over the x, y, and z axes) during an entire walking cycle. This pattern has been demonstrated that can be proof of identity for authentication [55].

Written Signature Authentication

Written signature authentication it is a well known biometric mechanism to determine the authenticity of a document. It also can be used as a user authentication biometric [29]. There are two different ways to capture and identify an individual: statically or dynamically. In static signature authentication, the user writes the signature on a paper and digitizes it, or directly to a digital tablet (see figure 2.4b). Then the system analyzes the signatures shape and compares it to other signatures. In dynamic signature authentication, the user has to write the signature directly in a digital table, which captures the signature in real time. In this case, many information of the signature is analyzed by the system such as the shape, the pen's pressure, or the pen's inclination. All these information is then compared to others signatures characteristics for the further decision of authenticity.

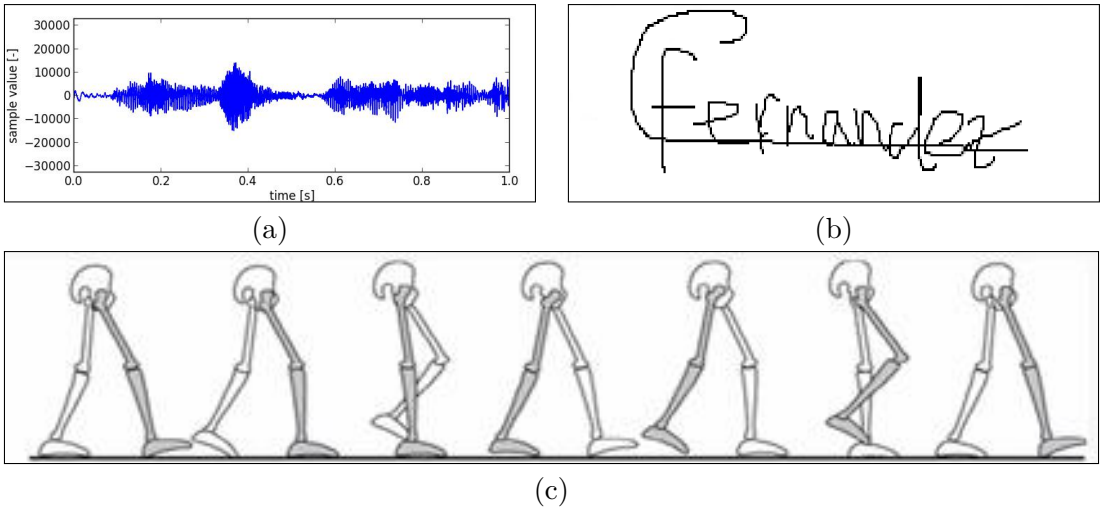


Figure 2.4: Behavioral biometrics: (a) voice sample [83], (b) digital hand wrote signature, and (c) gait cycle [21].

2.4 Multi-Modal Authentication

There are many approaches that can be used for authentication, such as the mentioned above: knowledge based, token based, and biometrics. There are multiple studies that measures the performance of different biometrics for authentication. For example, [57] explores time, effort, error, and task disruption that users experience when unlocking a mobile device when using three different biometric authentication modalities: voice, face and gesture. In addition [57] also compares them to a knowledge based modality: password authentication. [40, 41] make an overview and study of usability of existing physiological and behavioral biometrics. These works focus on the study of authentication techniques on mobile phones. In all of them there is a common conclusion: each biometric modality has unique strengths and weaknesses (see table 2.1), and has the potential to improve on the widely used PIN, or password approaches. On mobile devices, not only a strong authentication is important, mobile users require authentication systems with high speed, and usability. Hence, most of the research in multi-modal systems is focused on increasing these metrics when combining different of authentication systems. [20] is an example of usability in multi-modal authentication systems. It presents a risk-aware multi-modal authentication framework called CORMORANT. They claim that this framework offers a strong security authentication system for mobile devices. With CORMORANT different authentication approaches can be combined (including biometrics). By this combination a better usability and security can be achieved.

2.5 Summary

Many approaches can be used to authenticate on mobile devices. With the most commonly used authentication techniques being based on knowledge. However many users

lower security when setting simple authentication secrets to not forget them and also to speed up the authentication process. In recent years, biometrics such as fingerprint for authentication are rising and being integrated in many mobile devices. There are two types of biometrics: physiological and behavioral. The first ones store the secret in the physical biometric information of the user, e.g, the palm print. The second ones learn the behavior of the users action, such as gait. The advantage of using biometrics for authentication is that the users do not need to remember the secret as it is attached to them. In addition, they require little user interaction when authentication, as they can be recorded in parallel while doing other activities. An alternative to knowledge based and biometric authentication is token based authentication. In recent years it is being used more frequently with systems that require strong security such as banking, by providing a two step authentication. Despite the high security that token based authentication systems can offer, there is still a lot to improve in the usability of these systems. Some of these systems require an additional hardware, such as the mobile phones. However, two step authentication is not useful for many systems like unlocking a mobile device. These systems require easy and fast mechanisms for authentication.

Leaving aside all the strengths and weaknesses of these authentication approaches, studies showed that strong and reliable security mechanisms can be achieved using multimodal authentication [36, 43]. Thus, by combining different authentication mechanisms the weakness of one, can be overcome using with the strengths of others. This combination results in a strong authentication system. Hence, the study and improvement of one authentication approach can result in a strong authentication if it is combined with other authentication approaches.

Chapter 3

Vein Recognition and Authentication

In contribution to the idea of mobile multi-modal authentication systems, we study and implement a less explored biometric: wrist vein pattern authentication. In this chapter we provide an overview of different technologies and methods that are needed for vein authentication such as vein capturing, vein image preprocessing, and vein pattern matching. Furthermore, this chapter presents rules and metrics which are used to build and properly compare different decision models.

3.1 Vein Capturing Techniques

When using veins for authentication, the authentication secret is the pattern of the veins. Thus, to authenticate or enroll the user needs to capture a vein pattern. In visible light [1] veins mostly remain hidden under the skin, hence we need special sensors to capture them. There are many types of sensors that can be used for capturing veins, from expensive ones, mostly used for clinical purposes, to cheaper ones. In medicine expensive sensors with high image resolution and strong depth penetration are frequently used to capture veins. On the other hand, for authentication purposes there exist cheaper sensors which are able to capture vein patterns, despite providing low quality images. Nevertheless, with a good image preprocessing these low quality images can be enhanced and used for a proper authentication. Moreover, vein capturing sensors do not only differ on the cost. These sensors have different fields of applications, hence they have different hardware specifications and shape. There exist static (fix position of the hand) and mobile (freedom position of the hand) solutions. Furthermore, to penetrate the skin tissue, and obtain the vein pattern there are multiple illumination techniques. There different wavelengths that can be used to visualize veins. The most common and cheap ones use illumination inside the NIR bandwidth. Also, there exist more powerful solutions that provide deeper skin penetration that easy the capture of veins. These solutions use more complex techniques like Venography or stronger illumination bandwidth: IR, FIR. This chapter gives a brief overview of the most common vein capturing techniques, used in medical, and authentication fields.

[1] Visible light spectrum ranges from 400 nm to 700 nm [71].

3.1.1 Venography

Venography is an X-ray medical examination. X-ray is an electromagnetic radiation at the wavelength ranging from 0.01 nm to 10 nm [19]. This technique is used for medical purposes and uses an injection of contrast material to show how blood flows through the veins. In medicine it is used to find blood clots, identify a vein for use in a bypass procedure or dialysis access, or to assess varicose veins before surgery [19, 54].

This technique is not used without medical care as there is a very slight risk of an allergic reaction if contrast material is injected. In addition, X-ray are known to be non-invasive, but long term or repeatedly exposure to its radiation can be harmful. Hence, this technique is not used for capturing veins for authentication purposes where the exposure to X-ray or the injection of the contrast material would be required very often.

3.1.2 IR

Infrared radiation is used in industrial, scientific, and medical applications. This radiation is adjacent to the long wavelength of visible light spectrum in the electromagnetic wavelength diagram (see figure 3.1). It extends from the nominal red edge of the visible spectrum at 700 nm, to 1000000 nm [71]. IR thermal cameras are frequently used to detect heat loss in insulated systems, to observe blood flow under the skin, and to detect overheating of electrical machines. Inside the IR wide spectrum there are different regions, with different wavelength, which can be used for multiple purposes they are the NIR, the short-wavelength infrared (SWIR), the mid-wavelength infrared (MWIR), the long-wavelength infrared (LWIR), and the FIR. Long exposure to strong infrared radiation may be hazardous for human eyes, resulting in damage or blindness to the user. Since the radiation is invisible for the human eye, special IR proof goggles must be used when exposing the human eye directly to strong IR radiation. However, IR radiation it is frequently used for skin therapies such as photo-aging skin, and improvement in skin texture as it increases collagen and elasticity in the skin. In addition, it has been suggested that IR radiation at an ambient temperature is safe and does not cause harmful thermal injuries to the skin [32].

NIR

One frequently used IR bandwidth for capturing veins is the NIR window (also known as optical window or therapeutic window). It is defined in the range of wavelengths from 700 nm to 1350 nm [71] where light has its maximum depth of penetration in tissue. As blood flows through human veins, NIR can be used to detect the vein pattern. Oxygenated and deoxygenated hemoglobin contained in the blood absorb light at the NIR wavelength [39]. In medicine NIR spectroscopy it is used to detect and highlight deep structures on image-guided surgeries. However, NIR spectrum it is not only used for medical purposes. Some night-vision devices, also use active NIR illumination to detect people or object without the observer being detected. This illumination technique is frequently used for security cameras, such as the charged coupled (CCD) cameras which have an array of IR light-emitting diodes (LEDs) and a modified NIR filter. CCD cameras are very sensitive in the NIR spectrum. They have a modified filter that blocks

the visible light and only allows light emitted inside the NIR window go through it.

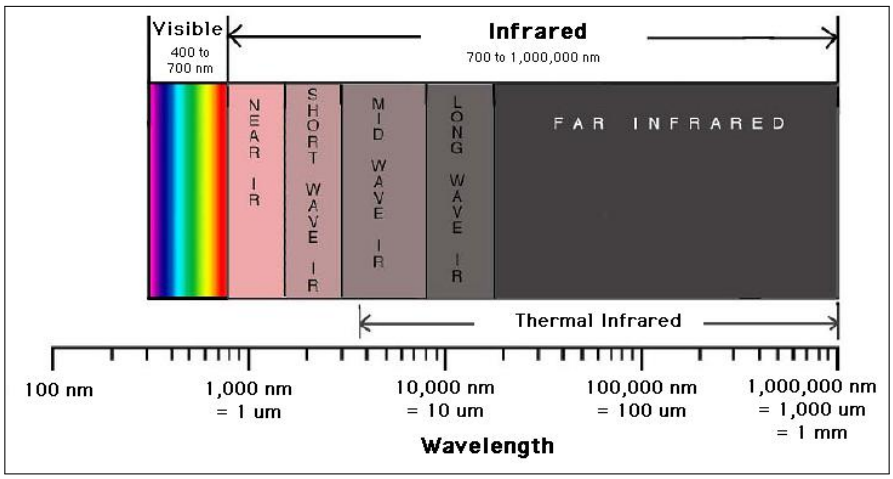


Figure 3.1: Visible light and IR spectrum [71].

3.2 Vein Image Preprocessing Techniques

As veins are under the skin, many vein images are blurred and require some preprocessing to properly enhance the vein pattern [62]. Usually, after capturing the vein pattern images contain noise because of low quality cameras, or illumination conditions. For authentication purposes, there are multiple preprocessing techniques as they vary depending on the captured vein images and the following matching algorithm used. Thus, in this section we present the most widely used techniques for vein images preprocessing. Hence, despite the individual differences that exist from work to work, most of them share the same preprocessing principles (see figure 3.2a) image enhancement for noise reduction and normalization, b) image segmentation to sharpen and differentiate veins from background, and c) points of interest (POI) extraction for further matching algorithms.

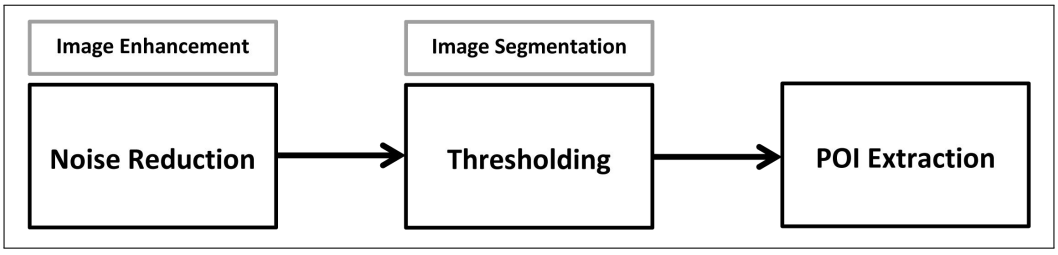


Figure 3.2: Preprocessing schema.

3.2.1 Noise

Many devices like cameras, or processing algorithms can introduce noise to the system, in form of distorted pixel values [65]. When capturing images with low quality cameras, they usually can introduce two types of noise: a) salt and pepper like noise, and b) Gaussian noise [16]. Independently to its type, this noise can be either correlated or, in many cases, uncorrelated at different pixels. As usually vein images for authentication are captured with low quality cameras in many cases the captured vein images contain these types of noise. In this section, we explain the most used techniques to overcome this unwanted effect on the captured images.

Salt and Pepper Like Noise

Salt and pepper like noise can be detected because color or intensity of some pixels are very different and uncorrelated from their surrounding pixels. Generally, this type of noise only affects a small number of pixels which are differentiated for being white and dark dots, hence the term salt and pepper noise. Typical the root of this noise are some flecks of dust inside the camera, or overheat or faulty of some CCD elements.

Gaussian Noise

Gaussian noise can be detected because all the pixels in the image differ a little bit from their original value. In this case, the noise is known to be correlated, thus when plotting an histogram of the noise distribution, a Gaussian distribution is observed. However, this is not the only distribution as other distributions can also occur. Gaussian distribution is known to be a good model due to the central limit theorem. This theorem usually applies to the distribution noise effect and tells that the sum of different noises tends to approach a Gaussian distribution [81].

Noise Removal

Noise reduction is the process of removing noise from a signal. In imaging, we can improve an image quality only by removing the contained noise. The most common technique to erase noise from an image is by applying a filter. By filtering an image we can smooth or erase some unwanted frequencies. The main filters used to overcome the effect of salt and pepper like noise and Gaussian noise are:

- **Linear smoothing filters:** convolving the original image with a mask that represents a low-pass filter or smoothing operation to remove noise. The output tends to be a blurred image, which is sometimes not wanted, as many image features can be lost.
- **Non-local means:** averaging by non-local measures all the pixels in an image. The value for a noisy pixel is based on the degree of similarity between a small window centered on that pixel and another small window centered on the weighted neighbor pixel.
- **Non-linear filters:** the output is not a linear function of its input. There are several types on non-linear filters depending on the input function used such as

the median [2] filter. This one is very good at preserving image detail and removing the salt and pepper like noise. It can also cause some blurring of edges, but is one of the most frequently used in computer vision applications.

3.2.2 Thresholding

Thresholding is the simplest method for image segmentation. It transforms a gray scale image into a binary (black and white) image [3] (see figure 3.3b). There are many thresholding methodologies. The simplest one is to replace all the pixels in an image with black pixels if their intensity is less than some fixed threshold, or with white pixels if their intensity is greater than that threshold. Moreover, there are more accurate and complex thresholding methodologies which consider different measures than a threshold:

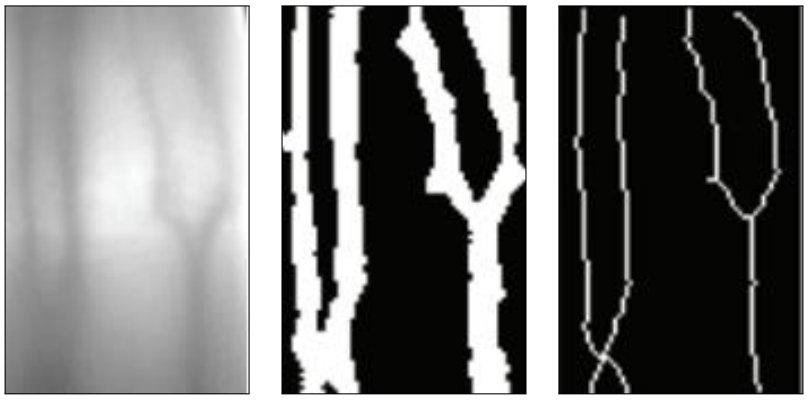
- **Histogram shape-based**: an analysis of the peaks, valleys and curvatures of the image's histogram are analyzed. With the obtained results, the values of the pixels are decided.
- **Clustering-based**: the gray-level samples are clustered in two parts as background and foreground (object), or alternatively are modeled as a mixture of two Gaussian.
- **Entropy-based**: uses the different entropies measures like: the foreground and background regions, or the cross-entropy between the original and binarized image.
- **Object Attribute-based**: searching a measure of similarity between the original (gray-level) and the binarized images, such as shape similarity, or edge coincidence.
- **Spatial**: this method uses higher-order probability distribution and/or correlation between pixels.
- **Local**: in this method the threshold to determine the pixel's value depends on the local image characteristics, so it is calculated differently for each pixel.

Thresholding is some times the last step in the preprocessing tool chain [27, 51]. Hence, after thresholding the obtained binary images are used in the matching algorithms to compare two images.

3.2.3 Skeletonization

Skeletonization is also known as thinning process. It is often applied to the binary images obtained after thresholding. This process obtains the binary images's skeleton by removing foreground (white) pixels from them. The output of the skeletonization process results in a binary image with a thinner foreground structure than the previous thresholded image (see figure 3.3c). This preprocessing technique is only used where the matching algorithm uses the properties of the image's skeleton such as: bifurcations [60], endpoints [59], breaches lengths [63].

[2] Statistical metric that computes the middle value of a data set. This value is obtained after separating the higher half of a data sample, a population, or a probability distribution, from the lower half.



(a) (b) (c)

Figure 3.3: Vein image preprocessing [63]: (a) vein image, (b) thresholded vein image, and (c) skeleton of vein image.

3.3 Vein Pattern Matching Techniques

Vein pattern matching, as well as preprocessing, highly depends on the obtained vein pattern after the capturing and preprocessing steps. In this case, depending on the techniques and steps followed, different matching techniques have been used to measure similarity between two vein patterns [8].

3.3.1 Cross Correlation

Cross Correlation (CC) is a measure of similarity between two series as a function of the displacement of one relative to the other. In this case we assume a comparison of discrete functions (f and g) which represent the image's pixels (see equation 3.1) [28, 51]. When comparing two images by CC usually the last preprocessing step is thresholding. Therefore, when using CC for vein pattern matching, two binary vein images are compared. Hence, all the information of the veins should be considered. By applying skeletonization, some relevant information from the veins would be erased like the veins width, thus the CC approach would be less optimal.

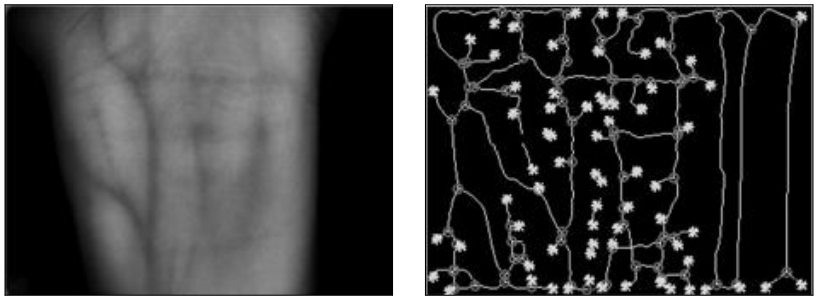
$$(f * g)_i = \sum_j f_j^* g_{i+j} \tag{3.1}$$

In [27] and [51] it is claimed that using CC as similarity measure to compare vein patterns works and it is a reliable measure for authentication. However, this algorithm is a rigid matching technique because provides translation as the only form of geometric transformation, and positioning is limited to whole pixel units. Thus, is not invariant to rotation, and scaling of images. One common solution to solve the rotation invariance problem is rotating each image a range from -30° to 30° with steps of 1° as proposed in [51]. Using this approach, for each two pairs of images instead performing a 1:1 comparison, the system has to compute a 1:60 comparison to obtain the final matching result. Hence, taking this solution the computational complexity of the system increases in a 60-comparing-effort.

3.3.2 Minutiae Feature Matching

Minutiae feature matching is a technique that obtains relevant key characteristics from the skeleton of a vein pattern. Therefore, skeletonization is needed in the preprocessing steps and consequently: number of branches, bifurcations, length of branches, and endpoints, can be used as features to compare two images (see figure 3.4).

Many measurements can be used for evaluation of similarity between minutiae points such as Hausdorff distance (HD), modified Hausdorff distance (MHD), similarity based mix-matching (SMM). [17, 18] present a method to compare hand and wrist vein patterns by representing a minutiae set of features as fixed-length feature vector, invariant to translation, rotation and scaling. [63] presents a method based on minutiae points and Hausdorff distance algorithm to evaluate the identification ability among all possible relative positions of the finger vein patterns shape.



(a) (b)

Figure 3.4: (a) Wrist vein image, and (b) skeleton of wrist vein pattern with extracted minutiae key points [17].

3.3.3 Non-Rigid Matching

Non-rigid matching, also known as elastic matching, is a technique capable of registering a reference image under (almost) arbitrary geometric transformations, such as changes in rotation, scale, and affine distortions.

One example of non-rigid matching is the Lucas-Kanade algorithm [61]. This algorithm differs from the rigid template matching that perform a global search over the entire image to find the best match such as CC. Instead, the Lucas-Kanade algorithm starts from an initial position in the reference image to find the best match on a search image. To start the comparison between two images it estimates the initial reference image position on the search image. Then, in the estimated region of the search image, it performs a randomly perturbation in $x-$ and $y-$ directions by Gaussian noise. This iterations are performed several times over the matching process. Finally, whenever one of these search image region perturbation converge with the reference image region, it is considered to be a match.

However, non-rigid matching are demonstrated to work better on textured images as they require to select a particular region or key point to compare two images [61]. Thus, this algorithm is not frequently used for comparing binary images. Binary images only contain white and black pixels, hence, there are many regions which result on a

high correlation after multiple perturbations.

3.3.4 SIFT Features

Scale invariant feature transform (SIFT) is a technique for local feature detection. It was first proposed by D. Lowe [38]. This technique is used in computer vision for object recognition and matching in multiple images [37, 61]. Moreover, SIFT features have been also demonstrated to work in biometric authentication systems for face [14] and finger veins [22] recognition. All these approaches are based on locating relevant local features of an image which can be robustly identified under different image variations and viewing conditions, such as scale invariance. To detect relevant features of an image, a SIFT detector works with subpixel positioning accuracy and a rotation invariant feature descriptor attached to the candidate points. This feature descriptor (typically 128-dimensional) is used as an image key point, which contains relevant information of its surrounding such as the distribution of its neighbors gradient directions [38]. Based on [61] approach, there are five main steps involved in the calculation of SIFT features for an image:

1. Extrema detection in a Laplacian of Gaussian (LoG) scale space.
2. Key point refinement.
3. Creating local descriptors.
4. Orientation assignment.
5. Formation of feature descriptor.

Extrema Detection in a LoG Scale Space

This step is based on locating potential POI of an image. This locations are detected because they are image regions which are suitable to contain stable features. Hence, these stable features are used to uniquely represent the image, thus can be located under different scales and viewing conditions. To guarantee the scale invariance, the POI are located over multiple scales, by representing the image in a scale space. This scale space $L(x, y, k\sigma)$, is constructed by recursively convolving the original image $I(x, y)$ with a sequence of small Gaussian filters $G(x, y, k\sigma)$ at a certain scale level $k\sigma$ (see equation 3.2). The output of this sequence of filters results on a Difference of Gaussian (DoG) space, $D(x, y, \sigma)$ (see equation 3.3). Thus, the image's POI are taken as local maxima or minima of the DoG resulting space.

$$L(x, y, k\sigma) = G(x, y, k\sigma) * I(x, y) \tag{3.2}$$

$$D(x, y, \sigma) = L(x, y, k_i\sigma) - L(x, y, k_j, \sigma) \tag{3.3}$$

Key Point Refinement

Using the scale space extrema detection approach, we can obtain a lot of POI for an image. In this step, [61] proposes to remove the ones that are less stable by performing local interpolation and elimination of edge response. Thus, the POI with low contrast and poor location along the edges are rejected.

So, the three steps that SIFT performs to obtain the image's key points are: a) detection of extremal points int the DOG scale space, b) position refinement by local interpolation, and c) elimination of edge response.

Creating Local Descriptors

After detecting the image's key points the algorithm generates local SIFT descriptors. With the detected key point up to four local descriptors can be calculated. Only, more than four descriptors can be created if for a position the local orientation is not unique. In [61], they propose to generate the local descriptors by:

1. Finding the dominant orientation(s) of the key point k', contained on the distribution of the gradients at the corresponding Gaussian scale space level.
2. For each dominant orientation, create a separate SIFT descriptor at k'.

Orientation Assignment

For each key point SIFT assigns at least one dominant orientation. Thus, the key point descriptor is represented relatively to its orientation. Using this orientation information, SIFT descriptors are invariant to image rotation. To achieve invariance to rotation, the algorithm selects a square window around the key point center. With the local image gradient vectors within this window, it generates an histogram of the orientation angles (see figure 3.5). From this histogram, the dominant orientation $\theta(x, y)$ (sometimes more than one) is obtained and assigned to the key point. Thus the key point descriptor can by represented relatively to the key point's orientation and be invariant to image rotation. In [61] the dominant orientation $\theta(x, y)$, and its gradient magnitude $m(x, y)$, are obtained by pixel differences in the key point neighboring region for an image sample $L(x, y)$ at the space scale σ (see equation 3.4). To finally obtain the dominant orientation [61] proposes to form an orientation histogram formed by 36 bins, each covering 10 degrees. Searching the peaks in this histogram, the dominant orientations can be detected. Thus, the orientations with the highest peaks are assigned to the reference key points. An intermediate step, also proposed in [61],is to smooth the orientation histogram before locating the highest peaks(see figure 3.5). The smoothing process, which can be repeated several times, is done by applying a circular low pass filer, typically a simple 3-tap Gaussian or box-type filter [61].

$$\begin{aligned} m(x,y) &= \sqrt{(L(x+1,y) - L(x-1,y))^2 + (L(x,y+1) - L(x,y-1))^2} \\ \theta(x,y) &= atan2(L(x,y+1) - L(x,y-1), L(x+1,y) - L(x-1,y)) \end{aligned} \tag{3.4}$$

Formation of the Feature Descriptor

Previous steps covered how to find key point locations at particular scales and assigned orientations to them. This ensured SIFT features invariance to image location, scale and rotation. In this step for each key point $k' = (p, q, x, y)$ and each dominant orientation θ a corresponding SIFT descriptor is obtained by sapling the surrounding gradients at octave p and level q of the Gaussian scale space [61]. The final SIFT descriptor results

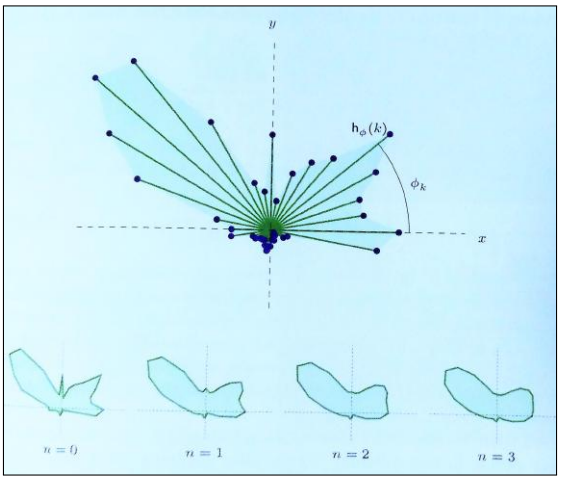


Figure 3.5: Orientation histogram example (above), and smoothing of the orientation histogram steps (below) [61].

in a vector f_{sift} of 128 elements. Thus, for a given key point k' the SIFT descriptor is a tuple s (see equation 3.5) which contains the key point's original image coordinates x', y', the absolute scale σ, the dominant orientation θ, and the corresponding gradient feature vector f_{sift}.

$$s = (x', y', \sigma, \theta, f_{sift}) \tag{3.5}$$

Matching SIFT Features

SIFT features are used in several applications for locating interesting points in two or more images, such as panorama stitching, feature tracking, self-location, or object recognition. Thus, all this approaches compare pairs of SIFT features in many different ways [14, 22, 37, 61].

[61] explains all the SIFT algorithm matching steps when comparing two sets SIFT features. Thus to compare two images (I_a, I_b), [61] proposes to obtain the features sets from both images $S_a = (s_{a1}, s_{a2}, ..., s_{an})$ and $S_b = (s_{b1}, s_{b2}, ..., s_{bm})$. Then the comparison between this two set of features is done by comparing pairs of SIFT descriptors. Thus, a metric proposed in [61] to measure the similarity between, $s_i = (x_i, y_i, \sigma_i, \theta_i, f_i)$ and $s_j = (x_j, y_j, \sigma_j, \theta_j, f_j)$ is the distance between the corresponding feature vectors f_i, f_j. This distance can be calculated using different metrics, however to most common one is the Euclidean norm denoted by $\| \cdots \|$ (see equation 3.6), as it is performed between individual points distributed in the 128 dimensional SIFT feature vector. With this similarity measure, two feature set can be matched. For each feature in the set there is always a best match (the one with the smallest distance) in the other feature set. However, matches may occur between unrelated features and this can be critical for comparing any correspondence between two images. Thus, this wrong matches have to be considered and preferably filtered, if not rotation and scale invariance of the algorithm can not be truly guaranteed.

$$dist(s_i, s_j) := \|f_i - f_j\| \tag{3.6}$$

3.3.5 SURF Features

For some approaches with several key points, SIFT features were slow and people needed a more speed-up version. In 2006 another algorithm for key point detection similar to SIFT was introduced [1]. Instead of using approximation of LoG with DoG for finding scale space, SURF uses the LoG approximation with Box Filters. Thus, this approximation can be done in parallel for different scales. Moreover, to assign orientations in a key point's neighborhood, SURF uses wavelets reposes in horizontal and vertical directions instead of the region gradient vectors. Simply following the same idea but improving the methodology SURF can faster extract features from an image [45]. Despite being a newer algorithm, it later has been shown that SURF has similar matching performance to SIFT, even, with SIFT being a more powerful algorithm (in terms of capability for extracting and matching features) than SURF [45] (see table 3.1). Thus, some studies conclude that when speed is not critical for image comparison, SIFT outperforms SURF [6, 44].

Table 3.1: Comparisons of SIFT and SURF features extraction and matching algorithms [45].

Algorithm	Detected Feature Points		Matching Feature Point	Feature Matching Time
	Image1	Image2		
SIFT	892	934	41	1.543 s
SURF	281	245	28	0.546 s

3.4 Performance Metrics

To measure the performance of biometric systems there are multiple statistical metrics that can be used [12, 46]. In this section we present the metrics and statistical concepts used in this work.

3.4.1 Equal Error Rate

Equal error rate (EER) indicates the probability of correctness in a biometric system [48, 56]. It predetermines the used threshold values for its false acceptance rate (FAR), or false positive rate (FPR) and its false rejection rate (FRR), or false negative rate (FNR). The FAR indicates the probability of the security system incorrectly accepts an access attempt by an unauthorized user. It can also be measured as the difference between 1 and the true rejection rate (TRR), or true negative rate (TNR) (see equation 3.7). The FRR measures the probability that the security system incorrectly rejects an access attempt by an authorized user. It can measured as the difference to one of the true acceptance rate (TAR), or true positive rate (TPR) (see equation 3.8).

$$FPR = 1 - TNR \tag{3.7}$$

$$FNR = 1 - TPR \tag{3.8}$$

When the FPR and FNR are equal, the common value is referred to as the EER. The value indicates that the proportion of false acceptances is equal to the proportion of

false rejections. The lower the equal error rate value, the higher the accuracy of the biometric system is.

3.4.2 Receiver Operating Characteristics and Area Under the ROC Curve

Receiver operating characteristics (ROC) curve is a graph that illustrates the representation of the TPR versus the FPR. This graph is used to measure the performance of a classifier model for all its possible thresholds [9].

Area under the ROC curve (AUC) is used in classification analysis in order to determine which of the used models predicts the classes better [2]. The measure is obtained by calculating the area under the ROC curve. The closer AUC for a model comes to 1, the better it is (see figure 3.6).

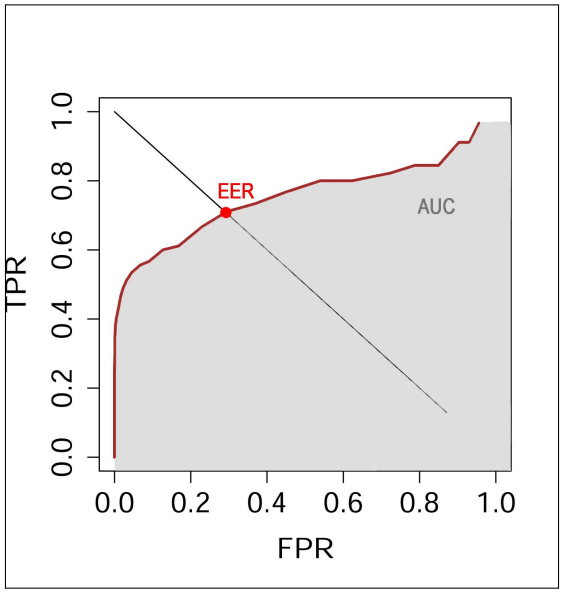


Figure 3.6: ROC curve example (brown), EER (red), and AUC (gray).

3.4.3 Overall Accuracy

Overall accuracy (Acc), or overall error captures the level of correctness of a model [13]. It counts the number of correct predicted samples: true positives (TP), and true negatives (TN), and weight them over all the measured samples, including the wrong predictions: false positives (FP), and false negatives (FN) (see equation 3.9). However this metric it is only used to evaluate the overall error. A drawback of this measure is that one can not state if the error comes from the samples wrongly classified as positives, or the ones wrongly classified as negatives.

$$Acc = \frac{TP + TN}{TP + FP + TN + FN} \tag{3.9}$$

3.5 Summary

Vein recognition and authentication can be complex as it involves several steps that can be solved using multiples solutions and techniques. Thus it is important to choose the ones that best support a given goal and approach.

The first reviewed set of techniques are the ones used to capture vein patterns. The most powerful vein capturing techniques are used in medicine. However, these techniques, like venography, result very expensive and can be harmful for the human body. Nonetheless, exists an alternative approach based on NIR illumination. This solution is cheaper and it has been proved to be non-harmful for the human body. After capturing vein images, to obtain the vein pattern it is necessary to apply preprocessing techniques to improve the visibility and segmentation of veins. In addition, some images contain noise which has to be removed to properly enhance and visualize the vein pattern. Thus, we reviewed the most useful preprocessing techniques to obtain an enhancement of the vein pattern for authentication purposes. One of the most used techniques is thresholding, an image segmentation technique. However, this preprocessing techniques have to be adjusted and tuned depending on the captured images. Along these lines, depending on the recorded images and the desired matching technique used for authentication the preprocessing steps can differ from work to work. There are works that differ only in little details such as some parameters, and others that change the entire methodology, or add additional steps such as skeletonization.

Furthermore, we explained multiple vein pattern matching techniques. Minutiae feature matching is one of the most expanded technique. However, this technique requires making an skeleton of the vein image to obtain relevant key points. This process can be very complex in noisy and low quality images, thus to obtain a reliable skeleton, the algorithm requires well preprocessed and high quality images. In addition, we have seen matching techniques for comparing binary images such as non-rigid matching, CC, and SIFT features. CC can result in a good matching technique but very sensible to image scaling and rotation, with computationally expensive solutions. Non-rigid techniques, can be used for matching binary images but may not be an optimal solution. These techniques perform better in greyscale or textured images, where pixels differ and have more than two intensity values. Finally, we have seen SIFT and SURF features. These two matching techniques can also be used to match two binary images. These techniques extract the images' key points which are invariant to scaling and rotation instead of directly comparing two images. Then, these algorithms use these key points to uniquely identify and compare multiple images.

Finally, we explained metrics and statistical concepts used to measure the performance and compare different decision models.

Chapter 4

Related Work

In this chapter we provide an overview of the current most important approaches related to vein visualization and authentication. Thus, we present an analysis of research papers, and commercial products explaining the used methods and technologies. At the end we summarize the most relevant points that we take for our authentication approach. Giving a first overview, we have already seen that there are two major areas when talking about capturing veins: medicine and security. Despite having different goals, in research works both areas use similar techniques when capturing veins [66]. In the case of medical research the focus is centered on capturing and visualization of vein patterns. Thus the obtained images are used for diagnosing of health problems [4, 49]. On the other hand, in the field of security the focus is wider. In this case capturing the vein pattern is just one box of the entire authentication system. This box mainly consist of: vein pattern preprocessing and vein pattern matching to finally perform authentication [33, 58].

4.1 Related Research

This section is focused on research projects for both medical and security fields. Both fields deal with measuring qualitative aspects of vein capturing, image preprocessing, or pattern matching. There exist much research regarding vein authentication, thus we make a summary of the ones we considered more relevant, in terms of technologies and methodologies for our work.

In [59] NIR (800 nm) and far infrared (FIR) light (1500 nm-1000000 nm) [71] are used to acquire vein pattern images of the wrist, back, and palm of the hand. The capturing device is mounted on a board with a CCD camera with IR filter and a NIR lamp. After the image acquisition, they use skeletonization to obtain the thinning of the vein pattern. Following the matching is performed measuring the Hausdorff distance (LHD) between minutiae points of the different patterns' skeletons. Using a similar setup, [51] presents a hand vein authentication system that uses fast spatial correlation for matching hand vein patterns instead. [53] explains how to capture wrist and hand veins images using a fixed prototype with mounted LEDs emmiting NIR illumination (880 nm) and a CCD camera.

In [47] wrist veins are captured using a physical structure and NIR illumination at the wavelength of 940 nm. They collect a database recording 5 samples from both

the left and the right hand of 50 subjects. Evaluation is done comparing nine different state-of-the-art vein matching techniques. Final founding show that the Log-Gabor and Sparse Representation Classifier (LG-SRC) models are the ones with the best performance. [27] use a local threshold for vein segmentation and 2D correlation coefficient for classification of obtained vein patterns. They evaluate on a self-recorded database of 1200 wrist images acquired from 50 volunteers for both left and right hands.

Finally [26] describes the design, development and initial evaluation of mVeinVision, a mobile medical application for assisting and improving venipuncture. This work uses NIR illumination at the wavelength of 740 nm and a HD USB camera. The application is implemented on a standard mobile device and intended to be a low-cost alternative to the commercial vein capturing devices. In contrast to our work, they only focus on vein detection and visualization as educational and clinical tool.

4.2 Related Commercial Projects

In recent years many commercial solutions using biometrics for authentication appeared to the market. These products propose an easy and usable authentication solution which can be used for e-banking, or unlocking mobile phones. In this section we present some commercial projects that use vein biometrics and use a principle or technique which can be useful for this work.

AccuVein

The first commercial project we present is AccuVein AV400 [67]. It is a clinical product which digitally displays a map of the vasculature on the surface of the skin in real time and contactless (see figure 4.1). They claim that can be used by clinicians for verifying the vein pattern and avoid valves or bifurcations. It uses IR light to detect veins under the skin, then it projecting the position of the veins on the skin surface. They claim to detect veins up to 10 mm deep, however it can vary depending on several factors such as vein depth, skin conditions (tattoos, eczema, etc.), body hair, or fatty tissue.

Figure 4.1: AccuVein AV400 vein visualization technology [67].

Hitachi Finger Vein Readers

Hitachi Finger Vein Reader [77] is used by a number of financial institutes in Japan as an authentication method. This product reads the individual's finger vein pattern

by illuminating the fingers with LEDs emitting NIR illumination. They use a physical structure which allows the individual to contactless authenticate (see figure 4.2a).

In addition Hitachi has another product: USB Finger Vein Biometric Authentication Unit [78] (see figure 4.2b). To capture vein patterns it uses the same principle (NIR illumination) as [77], however in this case using a closed structure. They claim that this product reduces the load on the host system or PC, thus it is compatible with many operating systems such as Linux, or Windows. Using this Hitachi USB Unit, users can authenticate to their personal devices using their fingers.

An example of an application of Hitachi's finger vein readers is the company FingoPay. They use Hitachi's units to build a vascular recognition-based payment system. They offer users a system to make money transactions, or payments, by simply scanning their finger's veins.

(a) (b)

Figure 4.2: Hitachi commercial products: (a) finger Vein Reader [77], (b) USB Finger Vein Biometric Authentication Unit [78].

Samsung Smartwatch Vein Authentication Patent

Samsung has a vein authentication patent for smartwatches. The patent [64] is titled "Wearable Device and Method of Operating the Same" and was filed on July 29, 2015. They claim to have a wearable device that using a sensor (including IR light and a camera) captures vein images from a user. These images are preprocessed and used to further authenticate users. In this patent, Samsung proposes to capture the user's back of the hand (see figure 4.3). Thus, emiting IR light on this area, the camera can capture the vein image, and authenticate the user on the smatwatch.

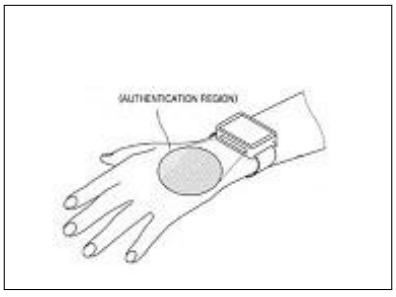


Figure 4.3: Sketch of Samsung's smartwatch authentication system using the user's veins from the back of the hand [64].

BioWatch

BioWatch is the closest commercial product to our work. BioWatch is a vein authentication buckle for smartwatches (see figure 4.4c). It requires direct user interaction as users have to scan their wrist for enrollment and identification. They claim that BioWatch module replaces badges, keys, cards, and passwords. Thus, using bluetooth users can, after identification, authenticate and unlock a car, access an office, login to the internet, sign contracts. BioWatch captures the user's vein pattern using a contactless system with IR light and an IR optic camera (see figure 4.4b).

(a) (b)

Figure 4.4: BioWatch product: (a) buckle module incorporation to smartwatch, and (b) vein scanning system [79].

4.3 Summary

Though, there exist much research on vein authentication, there is not much research focused on combining wrist vein authentication and mobile environments. For vein capturing most research is based on visualization of vein patterns using NIR light and modified filter cameras. However, in these works the proposed authentication prototypes use fixed structures and hand pegs. These setups facilitate the capture of a specific and uniform ROI of the vein pattern, thus it avoids scaling, rotation, and shifting problems. Only [26] presents a solution, which is very close to our work. In this work they present a clinical solution to visualize the body veins of any part of the human body using a mobile device. Most of these projects use the same capturing components and techniques: a mounted CCD camera, and LED illumination at the NIR bandwidth. Despite all using NIR illumination, they differ in the emitting frequency (see table 4.1). Thus, we can conclude that the illumination frequency depends on the setup and components used. The same happens with the preprocessing and matching techniques. Depending on the used capturing technique and the images obtained, each work present different preprocessing steps. Therefore at the end most of them use different image preprocessing and matching techniques for authentication (see table 4.1).

If we now look at the commercial solutions we see that they also use IR or NIR light for capturing veins. Some of the products, like Hitachi also use fixed, or closed structures to capture the vein pattern. Others like BioWatch, Samsung, or AccuVein use a mobile approach. As the main part of the authentication system is the matching technique non of the commercial products say which algorithms for preprocessing and matching do they use for authentication.

Table 4.1: Research and commercial projects review.

Project	Biometric	Capturing Technique	Vein Pattern	Matching Algorithm	Prototype
Research Projects					
IR imagining [59]	Hand veins	850 nm NIR + CCD	Skeleton	Minutiae points (LHD)	Fixed structure
Biometric authentication [51]	Hand veins	NIR + CCD	Thresholded	Spatial correlation	Fixed structure
Wrist sensor [47]	Hand/wrist veins	940 nm NIR + CMOS	CLAHE*	LG-SRC	Fixed structure
Vein database [27]	Hand/wrist veins	880 nm NIR + CCD	Thresholded	2D CC	Fixed structure
Vein authentication [53]	Hand/wrist veins	880 nm NIR + CCD	-	-	Fixed structure
mVeinVision [26]	Veins (clinical)	740 nm NIR + USB HD camera	DOG and Laplacian	-	Android mobile
Commercial Products					
AccuVein [67]	Veins (clinical)	IR + projection	-	-	Mobile unit
Hitachi [77, 78]	Finger veins	NIR + camera	-	-	Fixed structure
Samsung [64]	Hand veins	NIR + camera	-	-	Smartwatch
BioWatch [79]	Wrist veins	IR + camera	-	-	Mobile buckle

Chapter 5

Our Approach

In this chapter we explain the principles and methods used in this work to build a low cost wrist vein authentication system. All these principles and methods have been adopted from fundamentals 3 and related research 4 chapters and adapted to our work.

5.1 Overview

The system proposed on this work is adapted from the main structures shared in most of the systems from related research works. However, every work is highly dependent on the self captured images and the methods in its blocks. Hence, we adapted our blocks to obtain the best results for our system. Therefore, the proposed vein authentication system consist of the three main blocks that most of the related works deal with: 1) Wrist Veins Capturing, 2) Vein Pattern Extraction, and 3) Vein Authentication (see figure 5.1). Each of these blocks carries out different tasks, all necessary to finally obtain a good authentication. The first block is build in two parts: a) image capturing consisting on recording the images with a NIR sensor, and b) image preprocessing. The obtained are enhanced to properly visualize the vein pattern. Once the veins are clearly obtained, the second block performs the algorithm to obtain the relevant key points from that image. These key points are obtained to uniquely represent and identify the vein pattern. Finally, in the third block, implements the matching algorithm that allows to make the decision of authentication. Hence, the proposed matching algorithm is based on comparing two images by obtaining a similarity value when comparing their key points. Then the final decision of authentication is performed by a threshold decision model.

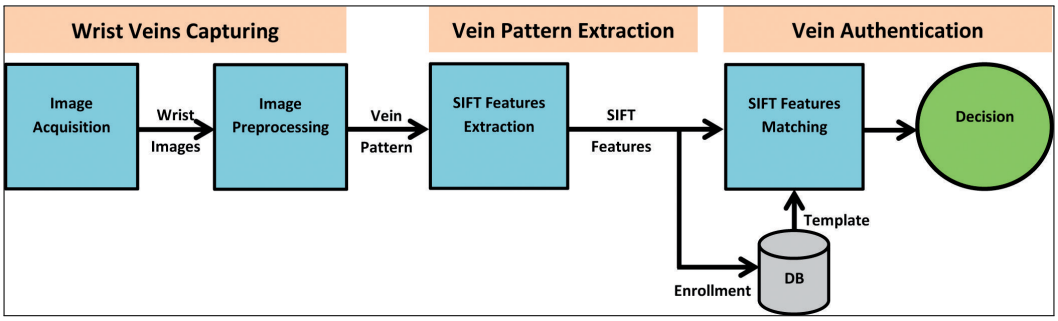


Figure 5.1: Constituent parts of our approach to mobile vein pattern authentication.

5.2 Wrist Vein Capturing

In this section, we explain which sensor technology we use to capture the wrist vein images. In addition, we present the preprocessing methodology and techniques used to properly enhance the vein images captured with the proposed sensor.

5.2.1 Image Acquisition

The first step of the system's tool chain is to capture the wrist vein images. In this work we present a low cost sensor to further capture a self-recorded wrist vein images dataset. Using the information from section 3.1, and chapter 4, we use the technologies that have been demonstrated to work adapting them to our requirements. Thus, we propose to build our sensor using LEDs emitting at the NIR bandwidth for illumination and a CCD camera to capture the veins. Many works already demonstrated how to build a low cost sensor using these technologies to capture vein patterns [26, 47, 53]. Thus, using this illumination technique we can penetrate the skin and illuminate the veins. Then using a low cost CCD camera with a modified NIR filter the vein pattern can be captured.

Challenges

Event though using NIR illumination and CCD camera for capturing veins worked in other works we have to demonstrate that this set up is valid for our mobile authentication system. In our work, wrists cannot be assumed to be placed in front of the sensor in a fixed or uniform position. This freedom of positioning implies three challenges that need to be addressed for successful vein authentication: image shifting, rotation, and scaling. One could use hand pegs (cf. [47]) to address shift and rotation. However this would make capturing images in a mobile environment overly cumbersome.

To solve the shifting invariance problem, we propose the following solution: instead of hand pegs, using a region of interest (ROI) window at the center of the camera's field of view (FOV).Thus, users have to position their wrist accordingly inside the ROI (see figure 5.2). Then, for proper identification, the image is cropped to only contain wrist information within the ROI.

In addition, to address rotation and scaling we propose to use SIFT features for the

matching algorithm. SIFT features have been shown to work for face, and finger vein authentication before [14, 22], therefore we evaluate the performance of SIFT features for wrist vein biometric. To our knowledge, this biometric and this technique have not been yet applied together. Thus we want to measure the performance of SIFT with wrist vein pattern, which is known to be less complex than finger or palm vein patterns [27]. Moreover, rotation invariance can be solved by (de) rotations of the images as proposed in [27], however this approach makes the system growth in computational complexity.

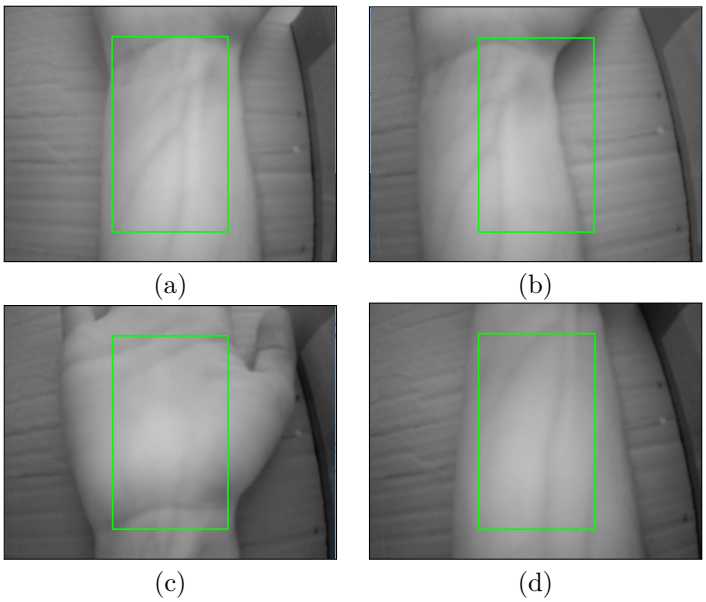


Figure 5.2: Wrist capturing position: (a) correct part of the body and position, (b) wrong position, (c)(d) wrong parts of the body.

Furthermore, the output images captured with the proposed low cost sensor result in low quality images. This implies that these images have to be preprocessed to increase the quality of the vein pattern. Also the possible noise and distortion introduced by the camera have to be reduced.

5.2.2 Vein Pattern Preprocessing

In this section we focus on the preprocessing steps used to properly enhance the vein pattern from the captured images. First, we need to determine what time of images we need at the output to fit with the matching algorithm. In this work, the proposed algorithm is based on SIFT features. This algorithm requires properly enhanced vein patterns in form of binary images to extract and compare their features. Thus, at the output of preprocessing veins have to be represented in white pixels, and background in black pixels. In addition, we also deal with the low quality images captured with the proposed sensor (see image 5.4a). As recorded images differ from work to work it is very difficult to adopt an existing preprocessing methodology in detail. In this work, after multiple attempts, we adopted the main preprocessing steps from the methodology presented in [27]: a) image filtering, b) veins segmentation, c) morphological closing,

and d) pixel inversion. Besides to better enhance our images we changed and fit most of the methodology's steps and parameters. The decision of adopting the preprocessing methodology from [27] is because the technologies used to build the capturing sensor are the same (NIR and CCD camera) as the ones used in our work. Furthermore the quality of the recorded images is very similar to the ones captured with our sensor. However both systems differ on the setup. [27] uses a closed structure without influence of external light. This setup ease the capturing of better vein patterns. Thus, we need to adapt the preprocessing parameters to overcome the differences in the setup and properly increase the quality and visibility of our recorded vein images.

Filtering

As the captured images have a low quality resolution these contain a lot of noise. Then, the first step in the preprocessing methodology is to filter the image to reduce this noise. We propose to use two filters to reduce noise: a Median, and a Gaussian Blur filter. The Median filter is a non linear filter that helps to remove the salt and pepper like noise introduced from the CCD camera. Additionally, the Gaussian Blur is a smoothing low pass filter which reduces the high-frequency components of the images (see figure 5.4b).

Thresholding

After the image enhancement, we apply a local thresholding technique to make the segmentation of the vein pattern. We first have compared six different thresholding measures to decide which one was the best for our images vein pattern segmentation: Bernsen, Otsu, Mean, Median, MidGrey, and Niblack (see figure 5.3). From this comparison, we decided that local mean thresholding was the one with the best performance. This measure is the one that maintains more information of the vein pattern, resulting in a good shape of the veins and not adding much noise and outliers. Hence, in our approach we apply a local thresholding method using as local image's characteristic threshold the pixel's mean value. This threshold is used to derive the pixel color value which is derived from the mean measure of the local greyscale distribution around the selected pixel (see equation 5.1).

$$pixel = \begin{cases} vein & \text{if } pixel > mean \\ background & \text{if } pixel < mean \end{cases} \tag{5.1}$$

To easy the next preprocessing step: morphology closing, when applying local thresholding we consider veins as black pixels and background as white pixels.

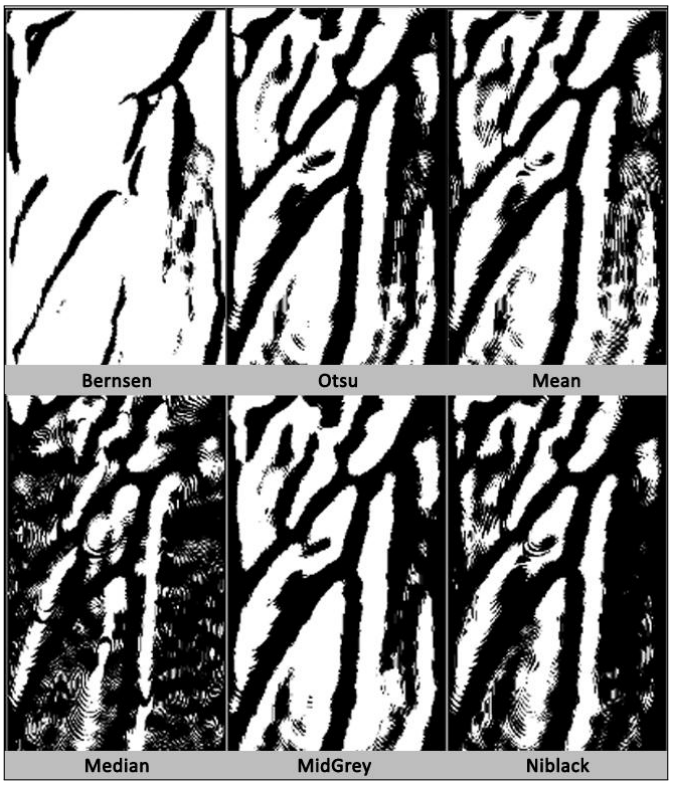


Figure 5.3: Local Thresholding output from different local characteristics.

Morphology Closing

To sharpen the veins and reduce outliers, we apply morphology closing to the mean local thresholded image (see figure 5.4d). Closing is an operator from the field of mathematical morphology and it is usually applied to binary images. It is derived from the fundamental operations of erosion [1] and dilatation [2] [61]. This method tends to enlarge the boundaries of the foreground (white pixels) and shrink background holes in the image. Applying this method, to the binarized image we sharpen the veins regions at the same time that removing outliers due to noise. In the presented approach after thresholding veins are represented as black pixels. Thus this morphological closing step makes a closing of the white pixels (background), and consequently sharpens the vein pixels (black).

Pixel Inversion

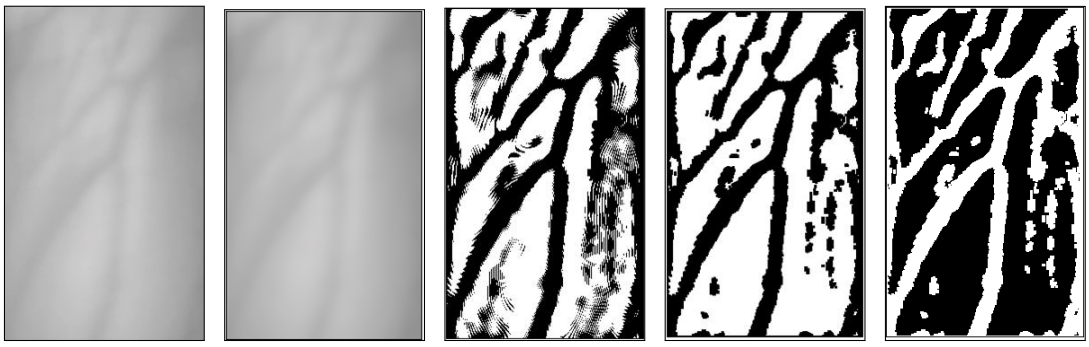
This is the last step of our proposed preprocessing methodology to enhance and segment the vein patterns. This action is also known as complement image. In binary images the white pixels are converted into black pixels and the other way around. Thus, as in previous steps we represented veins as black pixels, now we change the vein pattern

[1] By eroding, areas of foreground pixels shrink in size, and holes within those areas become larger.

[2] Dilatation expands the shapes contained in the input image, and holes within those regions become smaller.

values as desired: white pixels for veins, and black pixels for background (see figure 5.4e).

After this step we have the images properly enhanced and segmented. Thus the resulted binary images are suitable to fit with the proposed SIFT matching algorithm.



(a) (b) (c) (d) (e)

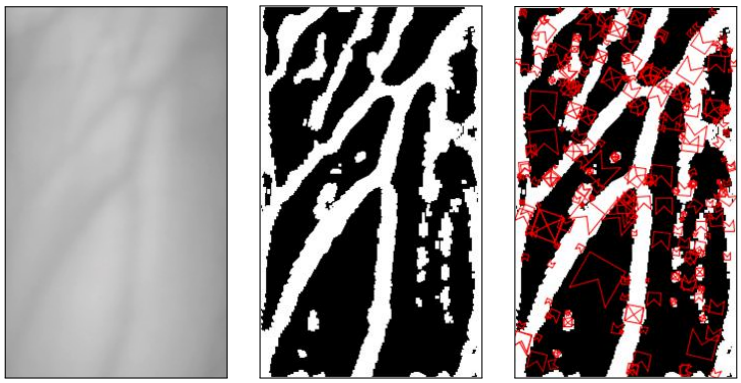
Figure 5.4: Vein image preprocessing: (a) sample after applying cropping, (b) filtering, (c) auto local threshold, (d) morphological closing, and (e) pixel inversion.

5.3 Vein Pattern Features Extraction

After the preprocessing of vein images, the next step is to derive features/key points to distinguish individuals' images based on their vein patterns. We propose to use SIFT features to represent the obtained vein patterns. Thus, using the similarity between SIFT features of two vein patterns we derive if those are actually from the same person or not. To extract the SIFT features from the vein preprocessed pattern we apply the theorem described in section 3.3.4. Figure 5.5, illustrates a representation of the extracted SIFT features from two different users. The red shapes represent the SIFT features descriptors which are modeled by their key point's original image coordinates x', y', the absolute scale σ, the dominant orientation θ, and the corresponding gradient feature vector f_{sift} (see equation 3.5).

5.4 Vein Pattern Matching Algorithm

Once the SIFT features for each image are extracted the following step is to make a matching algorithm to measure similarity between them, hence decide if they are from the same individual or not. For two samples I_A, I_B with corresponding SIFT features $S_a\{f_{A1}, f_{A2}, ..., f_{An}\}$ and $S_b\{f_{B1}, f_{B2}, ..., f_{Bm}\}$, our first step is to calculate a list of matching SIFT features L_{ab} between S_a and S_b e.g: $L_{ab} = \{f_{A1} - f_{B3}, f_{A3} - f_{A2}, ...f_{An} - f_{Bm}\}$. L_{ab} already contains suitable matches between SIFT features of the two samples – based on which we propose to enhance the accuracy of feature matching by going one step further. We propose to use the Euclidean distance of all possible pairs of SIFT features of S_a and S_b, to ensure matched features in L_{ab} actually have the minimum distance compared to all other possible matches using the same features. Using the obtained L_{ab}, for each proposed matched pair of features (p.e, $f_{Ai} - f_{Bj}$ with



(a) (b) (c)

Figure 5.5: SIFT features (red shapes) extraction process. (a) Captured vein sample, (b) preprocessed vein pattern, and (c) its extracted SIFT features.

i $\in$ [1,... n], and j $\in$ [1,... m]), we calculate the Euclidean distance of these features $D(f_{Ai} - f_{Bj})$ to all other features $D(f_{Ai} - f_{B1}), D(f_{Ai} - f_{B2}), \ldots, D(f_{Ai} - f_{Bm})$. If thereby $D(f_{An} - f_{Bm})$ is the minimum distance we say that $f_{An} - f_{Bm}$ are a feature match (Eq. 5.2):

$$\forall x : D(f_{Ai} - f_{Bj}) < D(f_{Ai} - f_{Bx}) \Rightarrow \text{feature match} \tag{5.2}$$

After obtaining all matching features between two vein patterns, the number of matches C_{ab} is used together with a predefined threshold τ as similarity between those patterns. If $C_{ab} \geq \tau$ we conclude that those patterns are originated by the same person, and by different people otherwise.

The presented SIFT matching algorithm is invariant to features rotation and scaling, as they are defined in different scale spaces and with an orientation vector. However, the SIFT matching algorithm can result to a wrong match between different SIFT features with high similarity. Thus, we can not assume a complete invariance of our approach. To overcome this uncertainty we propose to improve the matching accuracy of the presented SIFT. Thus, we propose to add an additional step to the SIFT matching algorithm: our proposed Euclidian minimum distance algorithm (see equation 5.2). Despite it improves the algorithm's accuracy when matching features, we can not guarantee that the proposed algorithm is totally invariant to rotation because Euclidean distance is not a rotation invariant metric.

5.5 Majority Voting

Majority voting is a decision rule to obtain a statistical value upon a group with different values. So far our approach acts in a 1:1 vein pattern comparison manner: it requires one sample to enroll users and one further sample to perform authentication. To improve authentication accuracy we propose to instead use majority voting with N vein pattern samples for both enrollment and authentication.

Thus, during authentication, comparisons between N enrollment samples $I_{A,n}$ and N authentication samples $I_{B,m}$ result in N^2 individual results $C_{ab,i}$. We apply a majority voting like approach over all $C_{ab,i}$ to obtain an overall authentication result C_{ab}. Such can be done using mean 5.3, median, standard deviation, or similar, based on individual results.

$$\overline{C_{ab}} = \frac{1}{N^2} \cdot \sum_{i=1}^{N^2} C_{ab,i} \tag{5.3}$$

The obtained similarity $\overline{C_{ab}}$ of two vein pattern samples is used with a threshold τ to decide if they were originated by the same person or not. If $\overline{C_{ab}} \geq \tau$ we say the samples are from the same person, respectively from different people otherwise.

$$if \begin{cases} \overline{C_{ab}} \geq \tau \implies \text{same person} \\ \overline{C_{ab}} < \tau \implies \text{different person} \end{cases} \tag{5.4}$$

Chapter 6

Evaluation

In this chapter we present different approaches and setups that we used to build a wrist vein capturing prototype to reproducible evaluate our wrist vein authentication approach. With the capturing prototype we have recorded our own wrist vein database. With this database's images we have adjusted and tested a preprocessing methodology to obtain vein patterns properly enhanced and segmented. With these patterns we have built the proposed matching algorithm based on the SIFT features matching algorithm. Thus, we built a SIFT matching algorithm that obtains a similarity value when comparing two images. Then with the resulted similarity value we have to decide if the compared images are from the same user or not. To achieve that we tuned a decision model based on a threshold τ. The model has been built using a partition of our self-recorded wrist vein database. Finally, with a new partition of the same database we evaluated the model's performance when making decision of similarity among users. In addition, following the same methodology but different configurations we built and evaluate nine different models using two different matching techniques: the proposed SIFT algorithm and CC algorithm for reasons of comparability.

6.1 Evaluation Setup

In the previous related research chapter 4 we have seen that there are multiple solutions and setups for capturing veins. In this section we explain in detail which steps we followed and which components and parameters we used to build our wrist vein authentication system. Furthermore we present the methodology followed to capture our self-recorded vein dataset. Finally we explain the process that we pursued to build and evaluate the proposed authentication decision models.

6.1.1 Capturing Prototype

The motivation of building a capturing sensor is to evaluate our proposed authentication algorithm in a self recorded dataset, for further reproduce the results in a working prototype. To be faster and to help during the repetitive capturing steps of the dataset we proceeded to build a capturing prototype. This process has not been easy, as many components and conditions influence in the way of capturing veins. Because of that we went through two prototype before obtaining the one that captured the desired vein

images. All the prototypes have been built accordingly to the mobile environment principles: open capturing structure and freedom of the wrist position. Using the proposed fundamentals in chapter 3: low cost prototype and NIR illumination. For each sensor prototype we tried out different components such as cameras, filters, LEDs illumination, and different positioning and distribution of those.

First Prototype

The first setup we designed to capture vein images was focused on trying to reproduce the capturing sensor proposed in [26]. The setup used in [26] claims to capture veins from different body parts in real time and using a mobile device. The specified capturing techniques are NIR illumination and a modified filter camera. Thus, to properly reproduce the same sensor we obtained the same hardware components:

- 4×LEDs OIS-330-740-X-T peak wavelength of 740 nm.
- HD Logitech USB webcam.
- NIR bandpass filter - 740 nm.

The required camera is a HD USB webcam used to capture images in the visible spectrum. Therefore we had to disassemble it and replace the optical filter for a NIR bandpass filter. To properly disassemble it we followed the specifications cited in [26](see figure 6.1a,b). Also, we ordered the same NIR badpass filter: a quite expensive square 10 mm×10 mm NIR bandpass filter with cut-off at 740 nm [82] (see figure 6.1c).

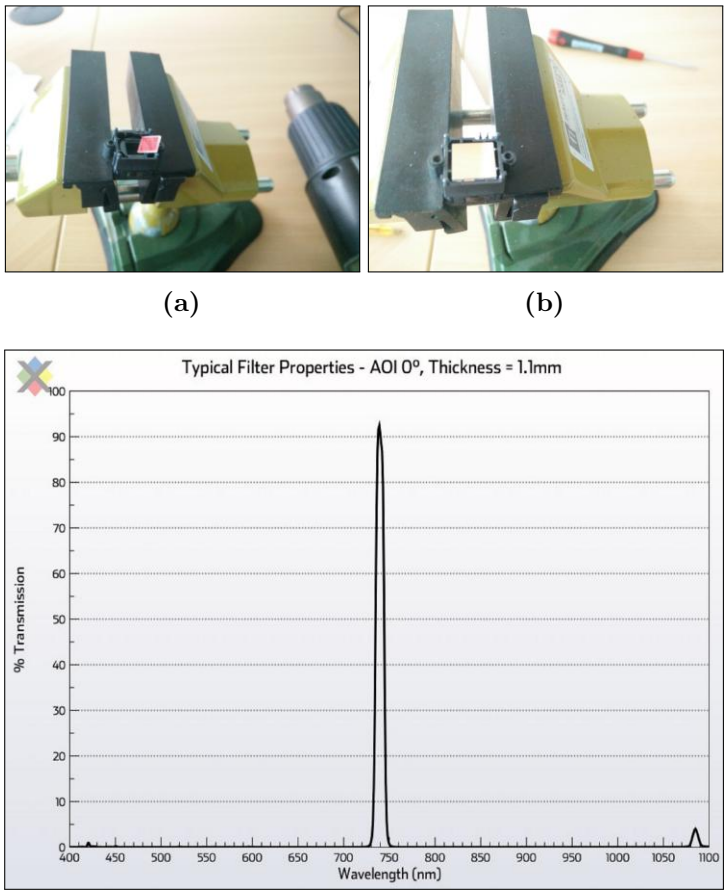


Figure 6.1: First prototype disassemble Web Cam process: (a) removing the optical filter, (b) replacing it with the NIR 740nm bandpass filter, and (c) NIR bandpass filter wavelength -– 740nm [82].

After disassembling the camera and replacing the filter, we reproduced the components setup described in [26] (see figure 6.2a). We connected and placed the IR LEDs in a breadboard [1] (see figure 6.2b) and the modified filter HD USB webcam following the same distribution. Now, with this setup we were ready to start capturing images. Therefore we plugged the webcam in a Windows 10 desktop computer and used the Logitech webcam Software application to capture the images.

However, tying out this first prototype we did not achieve good wrist vein images resolution. Somehow, because of the specified distribution of LEDs the NIR illumination was not intense enough to illuminate and highlight properly the wrist veins. In addition, the veins were only (little) visible when there was no influence of external light (see figure 6.2c)d)). Thus, we though that even: a) the purchased bandpass filter was not as mentioned in the specifications, b) the filter bandpass wavelength was too narrow, or c) there was not enough illumination to penetrate the skin tissue.

[1] Construction base for prototyping of electronics.

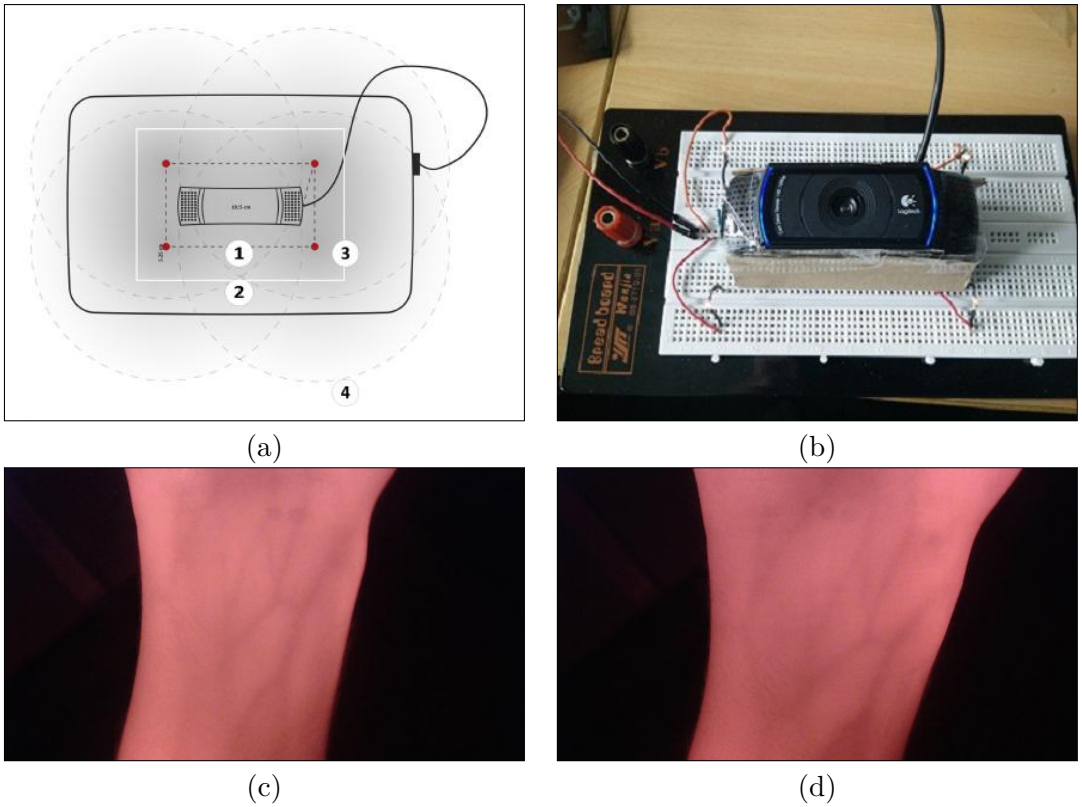


Figure 6.2: First prototype. (a) Schema presented in [26]: (1) USB filter modified camera, (2) Micro-B USB Host OTG Cable, (3) 4xIR LEDs of 740nm peak wavelength, and (4) radial NIR illumination distribution. First set up: (b) our implementation, (c)(d) resulting wrist vein images captured without external light influence.

Trying to improve this first attempt, we decided to change the NIR illumination intensity. Our idea was that only using four NIR LEDs the intensity was not enough to penetrate skin, hence veins were not properly visible. Thus, we decided to add more LEDs. In this second attempt, we plugged 10 LEDs around the camera and distributed them differently. Now, the LEDs were closer to the camera and were also illuminating more homogeneously the wrist area (see figure 6.3). The results that we achieved when using this setup were a little bit better. The visibility of veins improved even with external light influence. However, comparing the captured images with other works the way that we were capturing the veins was not good enough for further obtain a clear vein pattern (see figure 6.3c)d)).

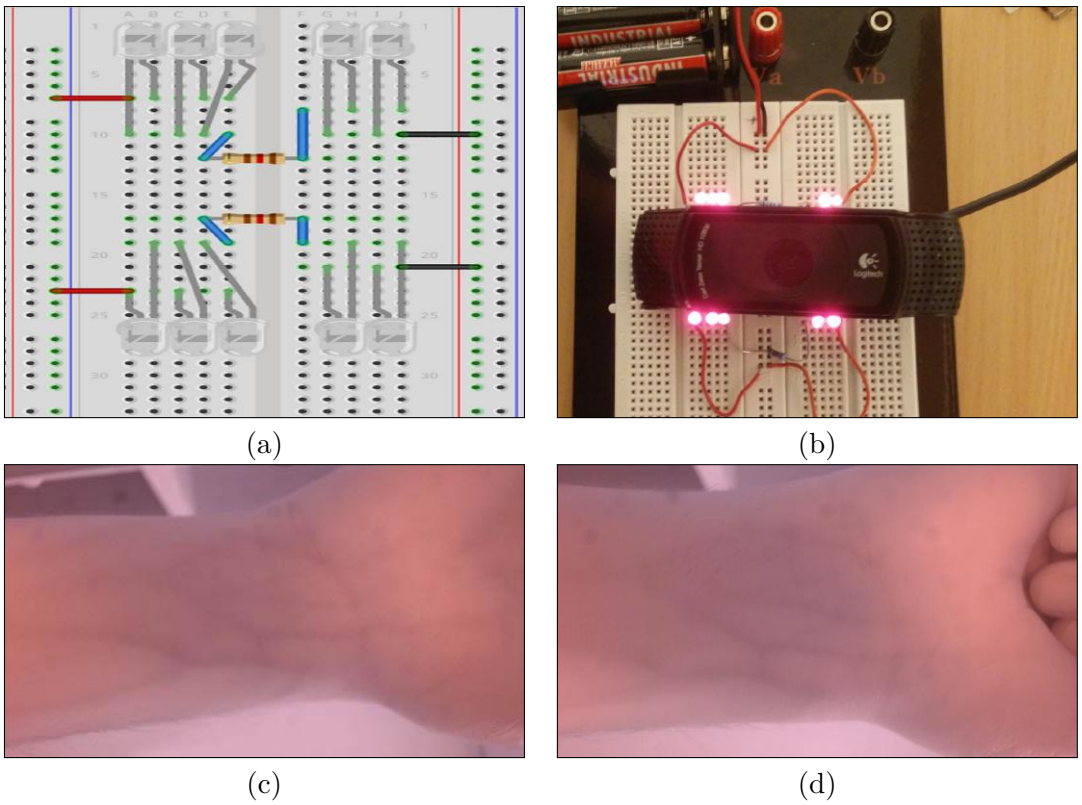


Figure 6.3: First prototype. Second set up: (a) digital components schema, (b) real implementation. (c)(d) Wrist vein images captured with external light influence.

Hence after testing this set up with the modified filter camera and after modifying the illumination to better capture the veins, we proved that the images where not good enough for our goal. The main reasons were: a) probably the filter bandpass was not accurate enough, and b) the NIR illumination at 740 nm was not intense enough to penetrate skin and highlight the veins. In addition, we also faced other problems because of disassembling the HD USB webcam. After replacing the filter the webcam's focus was altered and was not easy to set it back properly. Thus, sometimes images were not focused and very blurry.

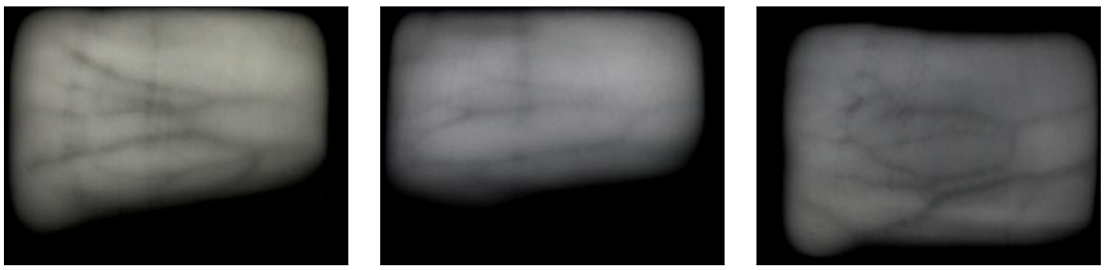
So, as the results were not the ones desired and the system was not stable we decided to change the strategy. From this first prototype we learned that: 1) using this setup the veins were not captured as desired, 2) the system was not stable because of illumination and focus problems, and 3) using the 740 nm filter with the HD USB camera was an expensive solution.

Second Prototype

With some lessons learned from the first prototype, we decided to use methodologies that proved to work in other projects [47, 59]. However, the proposed sensors from these works have not been proved to work in the mobile environment. This second time, the

first decision that we made was the filter bandwidth and the NIR illumination frequency. This decision was not easy as it is not stated clear which is the best wavelength in the NIR spectrum for capturing veins –that varies from 700 nm to 1000 nm. We have already seen one study working at 740 nm [26] and using a mobile device. Moreover, there are several works working in different wavelenght but using closed boxes structures using the NIR illumination principle at 880 nm [53] or 940 nm [47] (see table 4.1).

Thus, as there is nothing clear about which is the best wavelength for capturing veins, this time we decided to follow the setup used for capturing a public wrist vein dataset [69] (see figure 6.4). We tried out to preprocess and make a segmentation of the vein patterns from these images. The obtained results where good, hence we decided to reproduce the methodology stated in [27] to capture those images. The NIR wavelength used in this work is of 880 nm, and the only specification for the camera is that it is a CCD camera. Therefore we decided to build a new prototype using a low cost USB CCD camera with a NIR bandpass filter of 880 nm and IR light illumination.

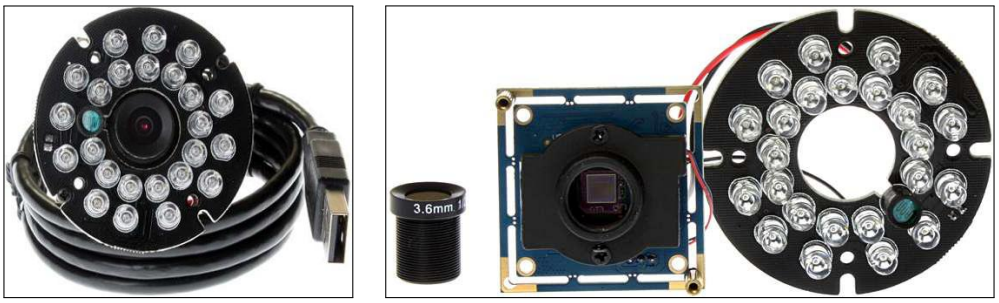


(a) (b) (c)

Figure 6.4: CIE Vein Dataset [69]: wrist vein samples from three different users.

For building this second capturing prototype, we purchased the ELP-USB30W04MT-RL36 camera, a low cost VGA USB camera module with a cluster of 24 IR LED and IR cut at 880 nm (see figure 6.5). These are the main specifications for the purchased camera module:

- OV7725 CMOS sensor with IR cut at 880 nm.
- Sensitivity: 3.8 V/lux-sec@550 nm.
- Resolution of 3 Megapixels.
- DC5V power supply.
- 24 IR LEDs.
- Optical bandpass filter at 880 nm.
- Compatible with WindowsXP or above, and Android 4.0 or above with UVC.



(a) (b)

Figure 6.5: CCD camera [73]: (a) camera block, and (b) disassembled camera.

This camera module depending on the environment sensed light provides two capturing options: (1) at the visible spectrum around 400 nm to 700 nm, and (2) night vision effect with IR light illumination at 880 nm. Hence, to set the camera always capturing at the NIR spectrum we isolate the light sensor from the external light covering it with tape obtaining a night vision effect (see figure 6.6).

(a) (b)

Figure 6.6: CCD camera views: (a) visible spectrum view, and (b) NIR spectrum view – night vision effect.

With this adapted camera module we finally obtained wrist vein images. In this case, the captured images resulted being very similar to the ones recorded in the public wrist vein dataset [69]. Then, with the camera properly working and capturing the desired images we build an open physical structure. The aim of this structure was to ease the recording steps when using the – for reasons of space and amount of parts – cumbersome NIR hardware. We designed an open physical structure for providing more realistic data in the mobile environment than e.g. frequently used closed box recording approaches with absolute darkness except for the intended NIR illumination.

Upon this structure we disassembled the camera and the LEDs array to better illuminate the wrist. The camera was placed about 15 cm above of the wrist and the LED array being about 8 cm away from the camera and about 17 cm from the capturing point – emitting light with an angle of about 62° to the wrist (see figure 6.7). Using this setup we obtained a reasonable illumination on the entire wrist. Therefore when

placing it on the camera field of view it shows a highlighting effect of the veins (see figure 6.7d). Finally, to capture and store images the camera was connected to a Windows 10 laptop using the Microsoft Corporation default camera software. To determine the wrist ROI, and properly crop these images, we used a rectangular ROI window of about 5.8 cm×9.7 cm size (see figure 6.7d).

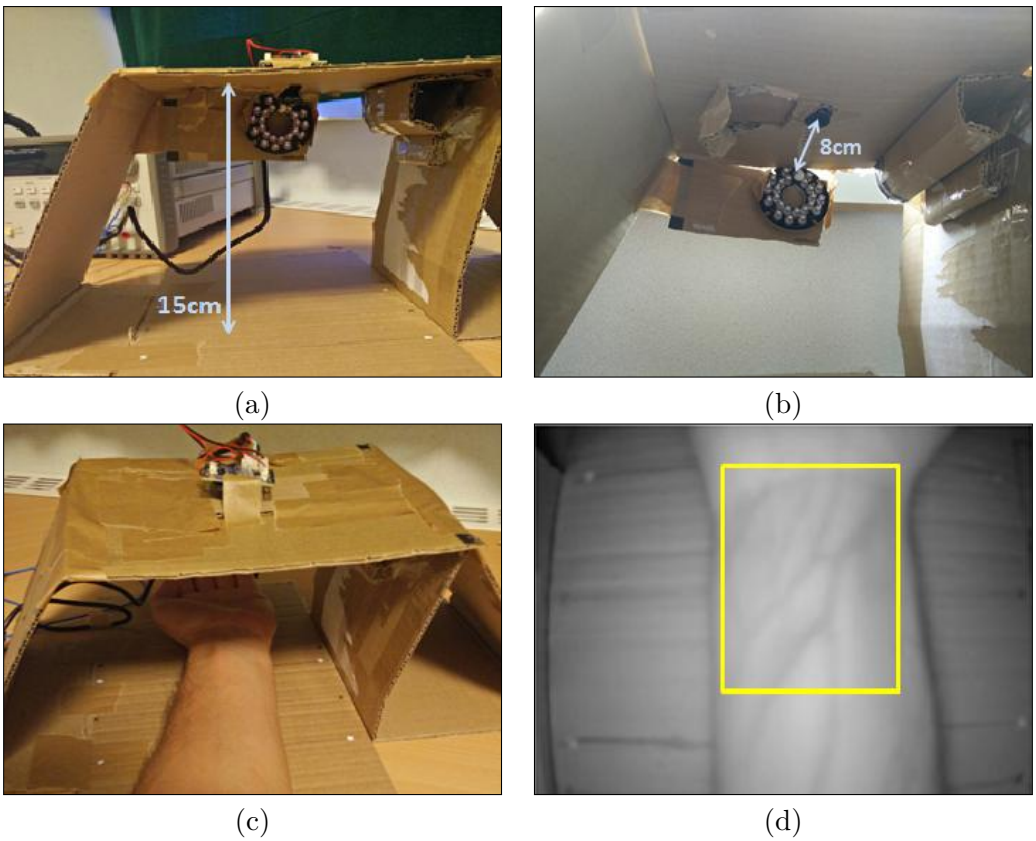
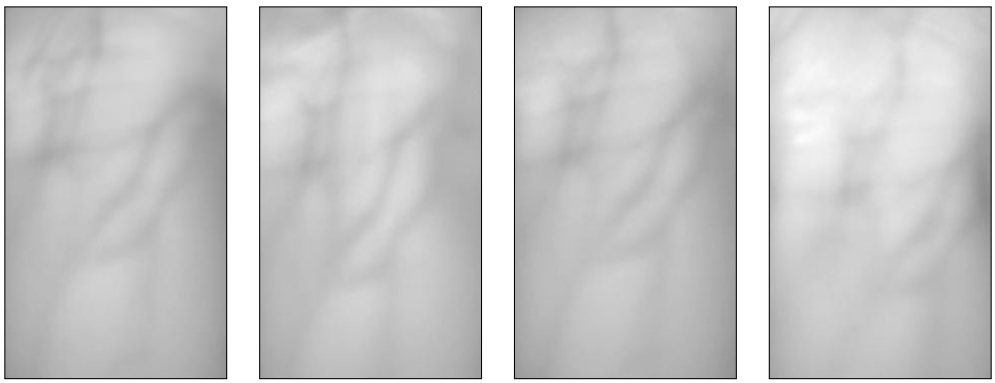


Figure 6.7: (a) Capturing device camera position, (b) NIR LEDs position, (c) hand position, and (d) camera view with ROI.

6.1.2 Dataset

With the final version of our capturing prototype we proceeded to capture our self recorded wrist vein dataset. Recording took place at the University of Applied Sciences Upper Austria, School of Informatics, Communication and Media in Hagenberg. The recording was done indoors using our second prototype with realistic indoor illumination conditions: the main source of light was artificial light from above and additionally there was influence of sunlight from outside shining from the glass to the wrist of the participants. To ease the capturing steps, the recording prototype was placed on a table and we simulated users placing their wrists in different conditions e.g. regular mobile devices: opening and closing the hand, and slightly rotating the arm, always maintaining the wrist ROI inside the camera's field of view frame. We thereby recorded 4 vein image

samples of the right wrist from 30 participants, which resulted in a total of 120 vein images (see figure 6.8).



(a) (b) (c) (d)

Figure 6.8: Database sample set: four unprocessed samples from the right wrist of a user.

6.2 Algorithm Evaluation

With the self-recorded dataset, we proceed to build and evaluate our authentication algorithm. In this section we explain all the preprocessing steps that we followed to obtain the vein patterns. Also, we present the authentication algorithm in detail, showing all the parameters, and steps that we used to compare and obtain a similarity value between two images. Finally this section explains how we built our decision models and how we evaluated their performance.

6.2.1 Image Preprocessing

Once we have captured the wrist vein images, the first step to finally make a reliable vein authentication system is to enhance the captured images' vein pattern. For that, we used the ImageJ an open source image processing program designed for scientific multidimensional images [80]. Using ImageJ we manually reproduced and validated all the needed steps to properly preprocess the vein images. Therefore, to enhance the captured vein images, and make the vein pattern segmentation we followed and applied with ImageJ the preprocessing methodology explained in section 5.2.2. However, as our images are self-recorded all the parameters used in all the steps have been tunned to finally obtain the desired binary images (see figure 5.4). Adapting the methodology and the steps explained in section 5.2.2 we used the following parameters to enhance and segment our captured vein images:

1. Image conversion to 8 bits.
2. Noise reduction:
   - 3×3 Median filter.
   - 3×3 Gaussian blur filter.

3. Veins segmentation:
   15×15 Local mean thresholding.
4. Morphological closing to sharpen the vein structures.
5. Pixel inversion to finally obtain veins as white pixels.

6.2.2 SIFT Features Extraction and Matching

Once we have the vein patterns properly segmented and represented as white pixels, the next step is to represent this pattern with unique values or characteristics for each user. Thus, we propose to extract unique key points from each pattern being as similar as possible between all the individual users' samples. Then, using these key points we can obtain a similarity value between samples, hence decide if the samples are from the same user or not.

From the segmented vein patterns, we use SIFT features to extract these relevant key points (see image 5.5). To automate the SIFT features extraction process we used ImageJ and the Imaging's book SIFT library [2]. The SIFT features extraction algorithm used is the one explained in section 5.3. However we adapted the algorithm's space scale parameters for our approach (see table 6.1).

To measure similarity between two samples we use the extracted SIFT features from each image. By comparing these list of features with a SIFT matching algorithm we can measure the similarity between these two samples' lists of SIFT features. Thus, to automate the SIFT features matching algorithm we also used the Imaging's book SIFT library. This algorithm is the one explained in section 5.4, but adapted to our work with the SIFT features matching parameters stated in table 6.2.

Table 6.1: Scale space parameters [61].

Symbol	Value	Description
Q	3	scale levels per octave
P	4	number of scale space octaves
σ_s	0.5	sampling scale
σ_0	1,6	base scale of level 0

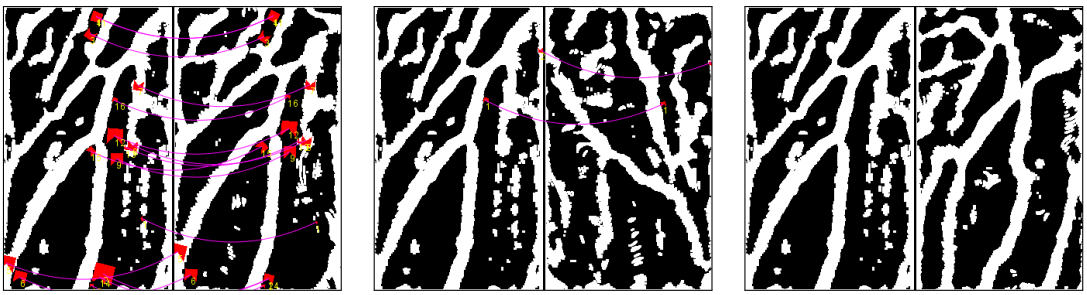
[2] Java open source code supplementing the digital image processing books by W. Burger & M. J. Burge [61]

Table 6.2: Key-point detection parameters [61].

Symbol	value	Description
n_{orient}	36	number of orientation bins (angular resolution) used for calculating the dominant key point orientation
n_{refine}	5	max. number of iterations for repositioning a key point
n_{smooth}	2	number of smoothing iterations applied to the orientation histogram
ρ_{max}	10	max. ratio of principal curvatures
t_{domor}	0.8	min. value in orientation histrogram for selecting dominant orientations
t_{extrm}	0.0	min. difference w.r.t any neighbor for extrema detection
t_{mag}	0.01	min. DoG magnitude for initial key point candidates
t_{peak}	0.01	min. DoG maginitude at interpolated peaks

Additional, to improve the certainty when matching SIFT features of the SIFT matching algorithm proposed in [61] we add another step. We propose to implement a minimum Euclidean distance algorithm (see equation 5.2). Hence if the matched SIFT features after applying the proposed algorithm in [61] are the ones with the minimum Euclidian distance we consider them as a true match, if not, the match is discarded.

Until now, using the proposed SIFT features extraction and matching algorithm it is useful to compare two samples. Thereby the similarity value to make a two samples comparison is based on the total number of SIFT features that they have in common, thus the number of features that satisfactorily matched. Figure 6.9 shows an example of the matching between different samples' SIFT features. Figure 6.9a), shows the comparison of two samples from the same user. In this case a total of 16 SIFT features matched, so we can say that these two samples have a similarity value of 16. Figure 6.9b), and figure 6.9c) show the comparison of two samples from different users. In the first case only 2 SIFT features matched so the samples have a similarity value of 2. On the second case there are no matches, thus they have a similarity value of 0. In following steps, we evaluate and decide which similarity values are considered as a positive match, hence the same user, and which ones are considered as a negative match, hence different users.



(a) (b) (c)

Figure 6.9: SIFT matching results: (a) different samples of the same user resulting 16 SIFT features matched, (b) different users samples resulting 2 SIFT features matched, and (c) different users samples resulting 0 SIFT features matched.

The algorithm explained until here is based on a 1:1 comparison between users' samples, hence only one sample it is necessary for the system to enroll and authenticate a user. Therefore, the decision of similarity between two users is made just by comparing two samples (one sample from user A vs one sample from user B).

As some times the proposed SIFT matching algorithm wrongly matches features of two different users the comparison might yield wrong result (see figure 6.9b). Thus, to improve the authentication algorithm accuracy to measure similarity between two users we also propose an approach based on a 4:4 sample comparison. In this case each user needs to enroll to the system by recording 4 samples, thus the classification of the singularity of the user is more accurate. Following this approach, when comparing two users' samples the similarity value is derived from the 16 similarity values. These values are obtained after matching both users' samples: 4 samples from user A $\times$ 4 samples from user B.

To obtain a reliable value from this comparison of 16 similarity values we apply the majority voting rule approach explained in section 5.5. In this work we evaluate this rule performance using two different statistical metrics: mean (see equation 5.4) and median. In the final evaluation we discuss which of these metrics performed best when used as similarity value.

With the similarity value between two users obtained using: a) 1:1 comparison, or b) 4:4 comparison with majority voting, the decision of authentication have to be done. Using the similarity value we propose to build a threshold τ decision model. With this model's threshold we perform the final authentication decision by comparing it with the similarity value between two users: if the similarity value is higher than the threshold τ we say that both users are the same, if not we say that they are different users.

To build the decision model, we first applied the algorithm to our dataset to obtain all the 1:1 and 4:4 similarity values of the 4 samples from the 30 users that we have stored in our self-recorded dataset. Figure 6.10, shows an example of a comparison between samples of the same user. This example only shows a comparison of 6 samples for simplicity and space reasons. Thus, this comparison results in an array of similarity values of $S =< 16, 17, 33, 10, 9, 31 >$. Using the 4:4 similarity approach we perform the majority voting rule. In this case, as only 6 comparisons are shown the final similarity

value based on mean would be: $(16+17+33+10+9+31)/6 = 19.3$. By using median as statistic metric for the same approach the similarity value would be the mean value of $< 9, 10, 16, 17, 31, 33 >= 16.5$. In the proposed 4:4 matching approach the comparison is made between 16 values instead of 6. On the other hand, in the proposed 1:1 matching approach each result S_i would be enough to decide if the compared individual samples are from the same user or not.

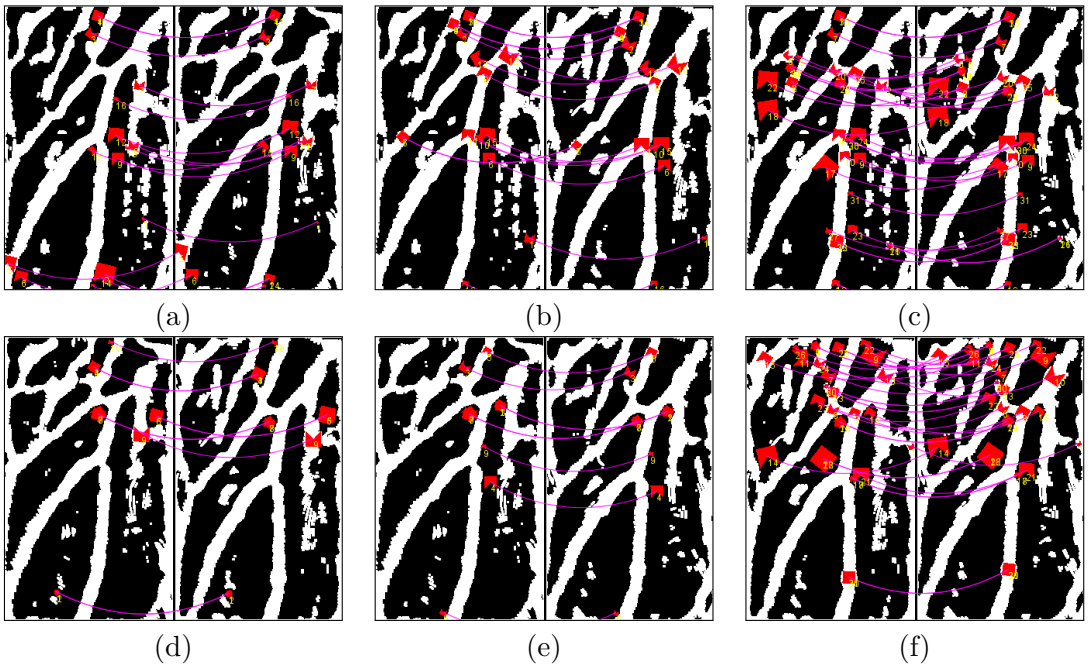


Figure 6.10: Count of SIFT features that matched after comparison of different samples from the same user: (a) 16, (b) 17, (c) 33, (d) 10, (e) 9, and (f) 31.

6.2.3 Decision Model

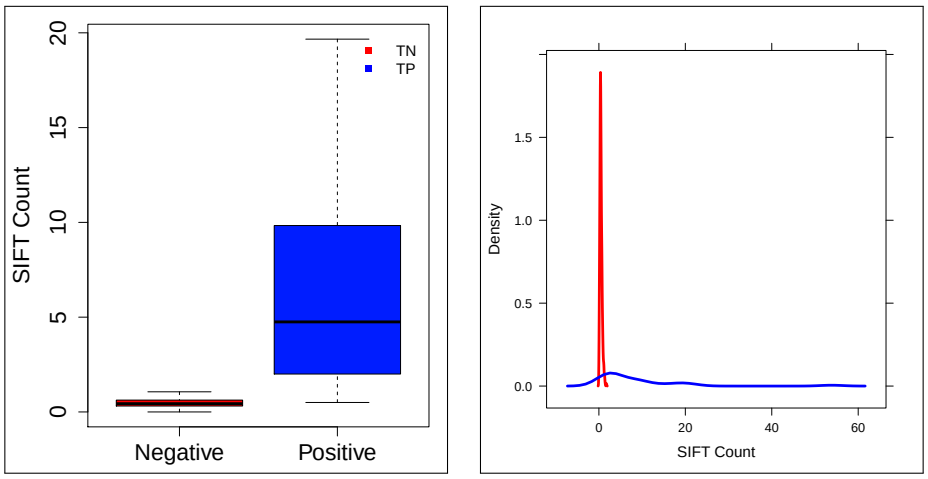
The final step to decide if a set of samples are from the same user or not is to build our decision model. In this section we explain how we build and evaluate the model's performance.

First, before building the model the first step is to analyze the distribution of the similarity values of our dataset users' samples. To visualize the classification of the obtained similarity values between users we used R [3] (see figure 6.11). With this statistical program we made a classification of our samples by dividing the ones from the same user: true matches (P), and the ones from different users: false matches (N). With this classification we can easily represent and observe the distribution of the similarity values. In the classification shown in figure 6.11b) we can already analyze the distribution of the classes from the 4:4 mean authentication approach. In addition we already observe that the P and N classes are imbalanced. Because the comparison of all the users

[3] A an open source programming language and software environment for statistical computing and graphics.

against all the others there are much more similarity values in the N class than in the P class.

After, analyzing the distribution of samples from P and N users, we propose to build a threshold τ based model. Thus, using this model the decision is made comparing the similarity value, obtained from the matching algorithm, with a pre-calculated threshold τ. As our model is build for authentication we want to minimize the error when making the decision. Therefore, we propose to build a threshold model based on EER (see section 3.4.1). The EER threshold model, is commonly used in biometrics systems [27, 47, 56]. It predetermines the threshold value for its FAR and its FRR. Hence when the error is the same in the P and in the N classes, the value is referred to as the EER. To build the prosed EER threshold model first we make a partition in our dataset. These partitions allow us to further evaluate the model's performance. Hence, in this work we used 50% of the data (15 users) for training the model and the remaining 50% of the data (15 users) for testing it. As our dataset is formed with data from different users this partition is called gallery independent [4]. Therefore, the partition used in the training set is used for building the model, and the partition of the testing set (composed from new users) is used for evaluating the model.



(a) (b)

Figure 6.11: SIFT 4:4 mean model classified in Positives (blue) and Negatives (red) classes. (a) Boxplot samples similarity values (SIFT Count) distribution, (b) densityplot samples similarity values distribution.

Decision Model Training

With the training partition (see figure 6.12a), we obtain a threshold τ when separating the P and N classes. As mentioned, during this training the obtained $\tau = 0.760$ that separates the training P and N classes is based on the model's EER (see figure 6.12): we thereby obtain the same separation error for the P and N class on new people.

[4] Training set contains data of different people than in the test set [24].

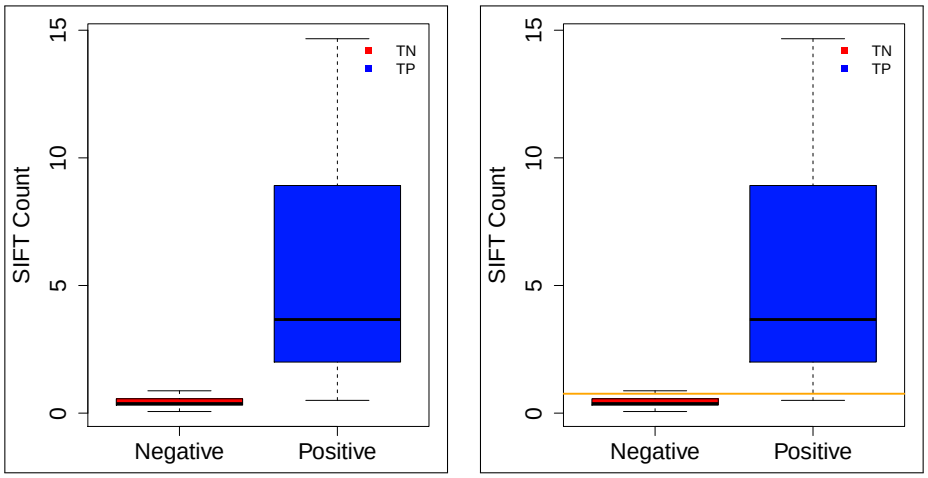


Figure 6.12: Training partition Positive (blue) and Negative (red) classes distribution: (a) distribution representation, and (b) same distribution with obtained EER threshold (orange).

Decision Model Testing

After training now we evaluate the performance of our model in the testing partition (see figure 6.13a). As both training and testing partitions are gallery independent, the results of applying the trained model on the testing partition gives us an overview of the performance of the trained model (see figure 6.13b).

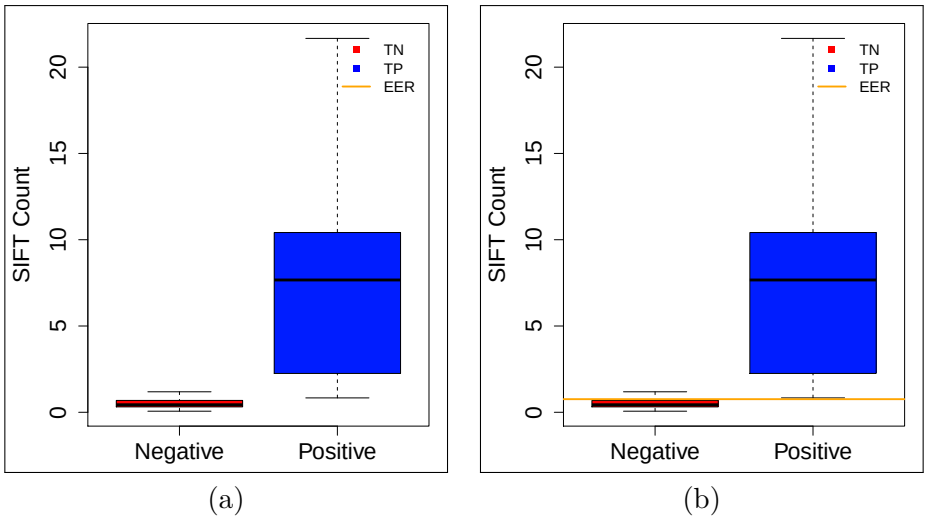


Figure 6.13: (a) Testing Positive (blue) and Negative (red) classes boxplot distribution, and (b) same distribution with evaluated EER $\tau = 0.760$ (orange).

Finally, we can evaluate how the trained $\tau = 0.760$, our model, performs on the testing partition. We measure its performance by analyzing the ROC curve (see figure 6.14), and the overall accuracy (see equation 3.9).

Using these evaluation metrics, in the next chapter we analyze and compare the different configurations and different models that we have built. Hence using these metrics we finally decide which is the best authentication model for our system.

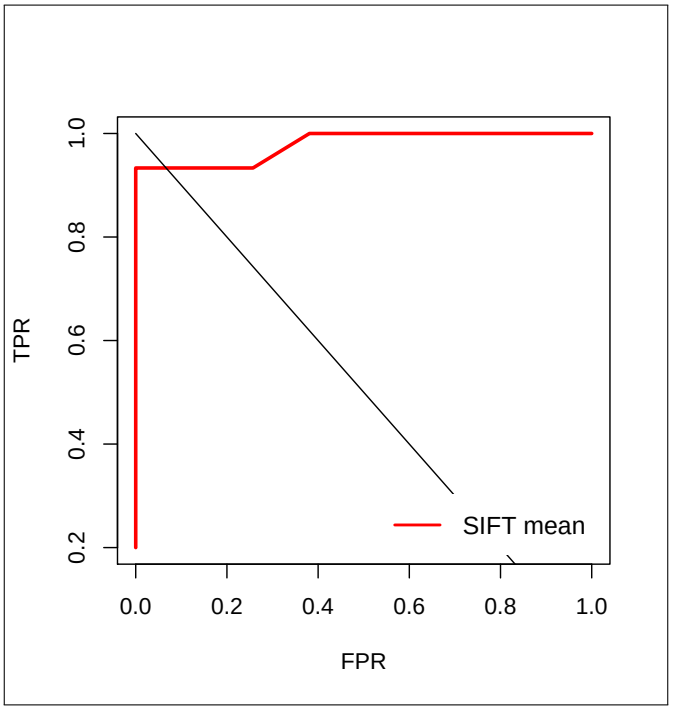


Figure 6.14: ROC curve of 4:4 SIFT mean model.

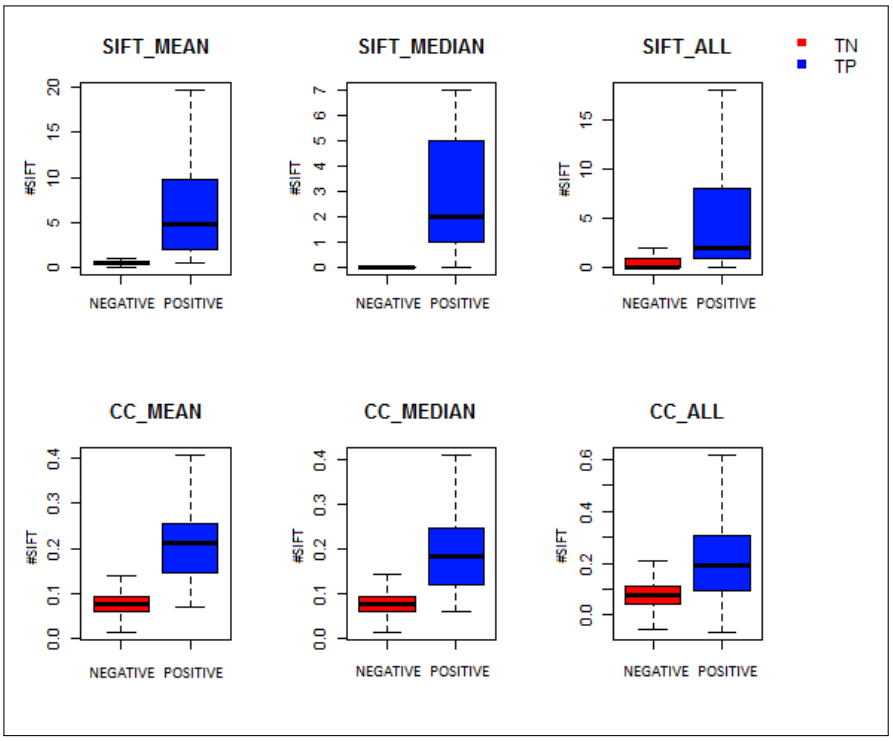
Chapter 7

Results and Models Comparison

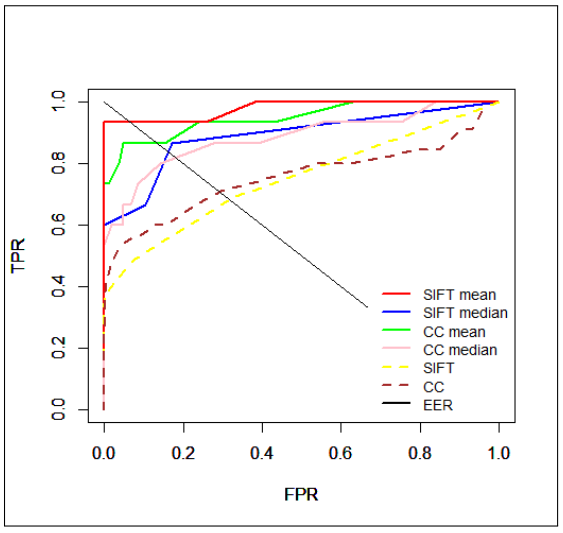
In this chapter we evaluate a number of differently configured versions of our model using our self-recorded dataset. Here we summarize all the performances, and results of these models, making a comparison between them. In addition we also compare our models' performance with the results of other works.

The first three models configured in our approach are based on SIFT features: SIFT, SIFT mean, SIFT median. The first uses 1 sample for enrollment/authentication, the others 4 samples – and either mean or median with majority voting (see figure 7.1). For further comparison with other works [27], we also configured and test three more models based on 2D cross correlation: CC, CC mean, CC median. The core difference of these three models with our SIFT based models is that instead of using matching SIFT features for similarity, these models use cross correlation similarity as underlying metric. The SIFT and CC models are based on the 1:1 sample comparison, thus they have been evaluated with only requiring one sample for enrolling and authentication. The SIFT mean, SIFT median, CC mean, and CC median models are based on 4:4 samples comparison, hence they require 4 samples for enrolling and authentication, using mean and median respectively as majority voting measures.

In these six different models the classification and distribution of the users similarity values of the samples are very different. Depending on the number of samples required for authentication and the majority voting measure used the classification varies significantly (see figure 7.1a). For the SIFT based models the negative class vary from 0 to 2, and the positive class from 1 to 10 approximately. Comparing these three SIFT models we can observe that the classification of P and N samples in the SIFT mean, and SIFT median models is stronger than the SIFT model. The mean of the positive samples for SIFT mean model is around 5 and the mean of the negative samples around 0. Also, in the SIFT meadian model are around 2 and 0 respectively. If we now compare it with the SIFT model the gap between the classes distribution is smaller and both classes mean values are also closer. On the other hand, comparing the CC models we can observe a similar behavior among them. In this case the distribution of samples is different than for the SIFT models as the CC similarity values range approximately from 0 to 0.6. However, if we observe these three models we see that also the gap between the P and N samples for the CC mean, and CC median models is bigger than the gap between these classes in the CC model (see also figure 7.1a).



(a)



(b)

Figure 7.1: Performance of our approach for different configurations: (a) models' P and N classification distribution, and (b) models' ROC curve representation.

In addition to the classification distribution for our models, we compare their performance using three metrics: 1) AUC, 2) Acc, and 3) EER. Comparing models by the AUC metric, the model with the best performance is the SIFT mean model ($AUC =$

0.980), followed by the CC mean ($AUC = 0.950$), the SIFT median, and the CC mean ($AUC = 0.890$) models. In addition, we also compared the models' Acc to measure their performance as in [13, 36] (see equation 3.9). In this case SIFT mean is the model with the best overall accuracy performance ($Acc = 0.858$) followed by the CC mean ($Acc = 0.775$), the CC median ($Acc = 0.758$), and the SIFT median ($Acc = 0.742$) models. However, this metric does not state the type of error, thus it does not show if a positive sample has been classified as negative, or vice versa. Finally, the last metric to measure performance used in this work is the EER. This measure shows which error does the separation of classes introduce to the model (resulting the same error in both classes). The model with less EER is also SIFT mean (EER = 0.072), followed as well for the CC mean (EER = 0.142), the SIFT median (EER = 0.153), and the CC median (EER = 0.175) models.

By doing this comparison we can see that the models using four samples for enrollment and authentication perform much better than the ones that only use one sample for it (SIFT and CC models). These two models have a significantly lower performance in all the stated metrics. The main reason of this lower performance is because these only use one sample for enrollment, hence there is a higher probability of wrong classification thus having a false match. Moreover, as the other models use four samples the users are identified and classified by their vein patterns' characteristics in much more detail. This performances comparisons can be also observed by plotting the models' ROC curves (see figure 7.1b).

Leaving appart the two models (SIFT and CC) with the lowest performance, between the other four ones we can determine that the model with better performance is the SIFT mean model. First, compared to SIFT median model we can observe that the resulting classes distribution is better for the mean model, being the mean of the P class much higher (around 5) than for the median model (around 2), with both N classes around 0. As both models use the same matching principle (SIFT) the only difference we can remark and assign the importance of making the model better or worse is the metric used for majority voting. In this case we can say that mean metric, makes a better average of the similarity value of the samples than the median. In addition, if we now look the CC mean, and CC median models we can also conclude that for the same reasons CC mean performs better than CC median. Thus between the mean and median metrics we can already state that the models using mean as majority voting rule perform better.

Further we can now compare the performance of the both matching algorithms SIFT and CC. Looking to the performance results of the two best models we can observe that the CC mean model has a lower performance than the SIFT mean. In this case the difference between these models is the matching algorithm used. Therefore with the evaluation on the self-recorded dataset matching the samples' features with the the SIFT algorithm is a better solution than matching the samples' binary vein patterns using the CC algorithm. One drawback of using CC algorithm is that the pattern of the used binary images is quite simple. Thus two different vein patterns can result in a high correlation coefficient even though being different samples. In addition, the SIFT algorithm is more powerful as detects key points of the pattern to represent the images more uniquely. Also, the proposed SIFT algorithm has the intention of being invariant to rotation and scale invariance. However, as mentioned before, we can not guarantee the totality of rotation and scale invariance as sometimes (as we can see in the model's

performance) false matches happen. Nonetheless, compared to the implemented CC method, the SIFT model is more sensible to the scaling and rotation variations which in the case of the CC algorithm are not considered at all.

After the comparison of the performance our approaches we further compare these models with other approaches. Therefore we look into detail the results from previous and related approaches which used different datasets and setups for the evaluation of wrist vein authentication models (see table 7.1).

In [47] after comparing nine different approaches the authors claim that the Log-Gabor and Sparse Representation Classifier (LG-SRC) is the one with the best performance resulting an EER = 0.0163. Moreover, in [27] using 2D CC they obtain a performance of EER = 0.038. The difference of the lower performance of our approach compared to those may be caused by a number of reasons. One difference is that the other approaches use a closed physical structure. Thus as our approach does not use this closed structure we can not prevent ambient illumination of non-NIR light sources. Further we only use 4 vein pattern samples for enrollment and authentication. The compared works use 5 and 12 samples for enrollment and authentication respectively.

Table 7.1: Performance or our approach and related work including the decision threshold τ used with the EER.

Model	**AUC**	**Acc**	**EER**	τ
SIFT Mean	0.980	0.858	0.072	0.760
SIFT Median	0.890	0.742	0.153	0.010
SIFT	0.705	0.636	0.319	0.010
CC Mean	0.950	0.775	0.142	0.100
CC Median	0.890	0.758	0.175	0.100
CC	0.710	0.631	0.292	0.100
LG-SRC [47]	–	–	0.016	–
Multiscale Match Filter [47]	–	–	0.134	–
2D Cross Correlation [27]	–	–	0.038	–

Chapter 8

Implementation

In this chapter we explain the final system implementation. The main idea of it is to automate all the steps involved in the proposed wrist vein authentication system (see figure 8.1. Thereby we explain in detail the software used to automate the steps for image capturing, system enrolling and authentication. Moreover we present the final version of the sensor used to capture the wrist vein images and how we store and label them into the system's database. Finally we state the libraries and software used to automate the decision block. In the explained implementation we have automated the decision model that resulted in a better performance: SIFT mean.

To achieve all the automation of the authentication steps we built a desktop application *WristAuthentication*. It consist on a tool that provides the user an intuitive user interface to enroll and authenticate to the system.

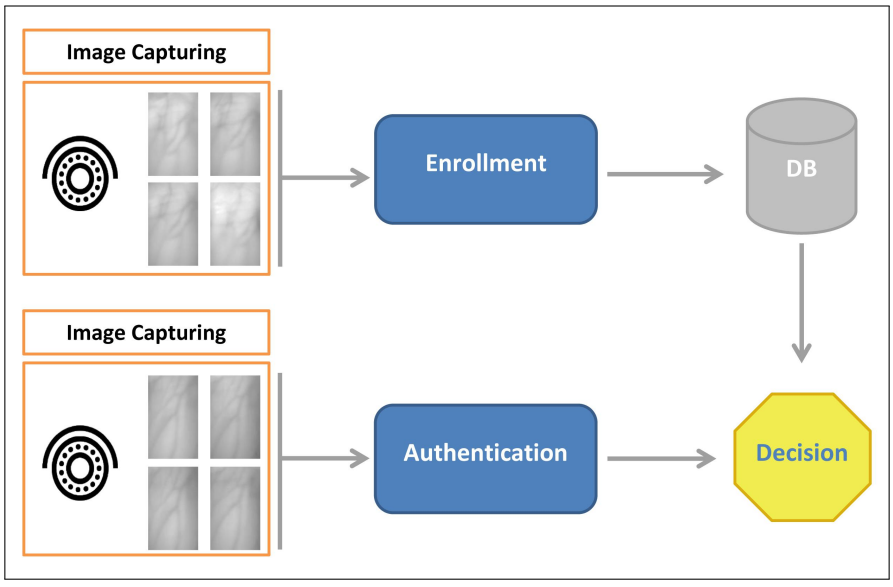


Figure 8.1: Summary of the authentication system's automated blocks.

8.1 WristAuthentication Application

WristAuthentication application is a JAVA desktop application to automates all the steps of a wrist vein authentication system using the presented capturing prototype, and SIFT mean decision model.

The goal of the application is to test the entire system's performance and usability in a mobile environment. The user interface of the *WristAuthentication* application has two modes: 1) enrollment, and 2) authentication (see figure 8.2a). When enrolling the user has to indicate a reference name, and capture four samples of the wrist (see figure 8.2b). These four captured samples are stored and labeled following this rule: W_o001_R_S1_Nri, where o001 indicates the enrolled user, and i $\in$ [1,...,4] the number of the recorded sample.

After the enrollment process the user can authenticate. For that it is also requested to capture four wrist samples. Likewise, these samples are also stored and labeled following the same rule as when enrolling: W_o002_R_S1_Nri, being o002 the label for the authenticated user. When these four samples are captured and stored the system performs the matching algorithm. The authentication decision is made with the implemented SIFT mean model with $\tau = 0.760$. Thus, after authentication the user interface shows if the process resulted as a valid authentication (see figure 8.2c), or invalid authentication (see figure 8.2d). In both cases, the user interface also shows the SIFT mean similarity value resulted between both users.

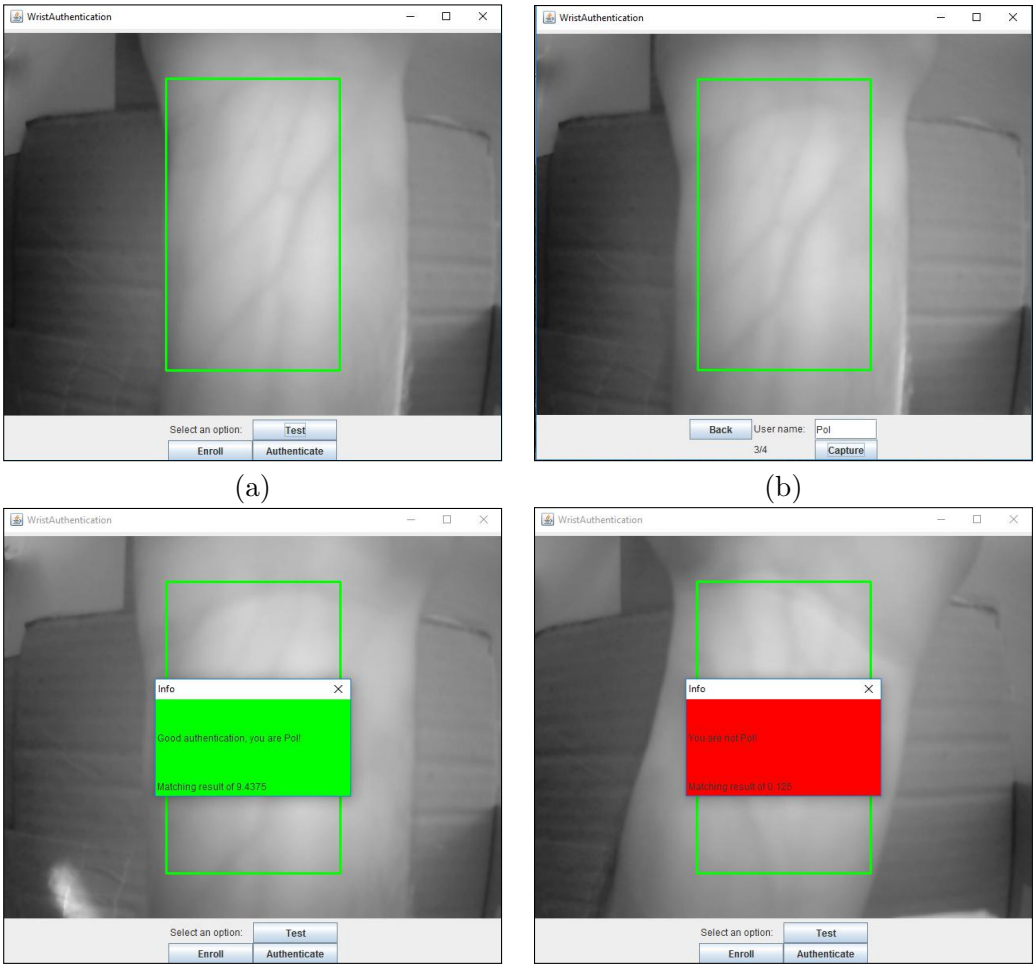


Figure 8.2: *WristAuthentication* app: (a) main dashboard, (b) enrollment dashboard, (c) good authentication, and (d) invalid authentication.

The *WristAuthentication* application has been built to test the compatibility of the proposed system with an Android mobile device. Thus, the software has been built using JAVA and two libraries: the Imagining Book common-1.0 [61], and the OpenCV 3.2 [1] [84] libraries, both also compatible for Android. Moreover, to better simulate the mobile environment we also adjusted the capturing prototype used to record the dataset (see figure 6.7). In this proposed version we present a sensor with total mobility of the camera. Hence we removed the structure that was holding the camera elements. Despite removing the holding structure we maintained the same distances and positions of the sensor's elements (see figure 8.3).

[1] Open source library for computer vision and machine learning software, compatible for JAVA, and Android.

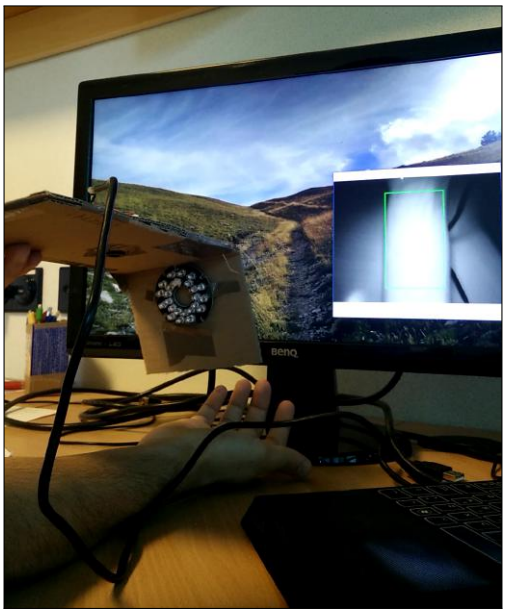


Figure 8.3: wristAuthentication app final capturing prototype.

With the proposed sensor and the software application we measured the entire system's time, and memory consumption when performing authentication. Therefore all these system's performances were tested under the following environment:

- Computer specifications:
  Model: Laptop Alienware M11x.
  Operating system: Windows 10 Home.
  Memory: 4 GB (RAM).
  Processor: Intel core i5-2467M at 1.60 GHz.
- Recording sensor: second prototype, without fixed structure (see figure 8.3).
- Recording conditions: indoor with external light influence.
- Participant's physical characteristics: white skin.
- Participant's physical status: rested.

With this testing environment we completed 10 authentication tests. We recorded samples from two users completely new for the system (see table 8.1). Then, we measured the time consumption and memory usage of the overall authentication process: arm positioning, images capturing, images preprocessing, and final authentication. The final results show that the system requires an average of 17.994 s and consumes 19.935 MB of CPU memory for authentication. Moreover, the experiment resulted in an accuracy of 90%. After the tests, 9 out of the 10 experiments produced a correct authentication result. Only 1 of these 10 experiments resulted in a false negative, hence the user was wrongly rejected for the authentication system.

Table 8.1: System's authentication tests results: time and memory usage.

#Experiment	τ	TP	TN	FP	FN	Time [s]	Memory [MB]
1	3.063	Y				16.020	24.435
2	7.375	Y				14.013	16.120
3	2.375	Y				17.277	11.681
4	0.750				Y	19.053	18.613
5	2.063	Y				20.069	19.304
6	0.250		Y			19.625	16.343
7	0.312		Y			18.228	23.506
8	0.000		Y			17.889	19.744
9	0.438		Y			17.955	25.668
10	0.500		Y			19.815	23.938
Average						**17.994**	**19.935**

8.2 Summary

In this chapter we presented the specifications of the developed desktop software application to automate the presented authentication algorithm. Using this application and the proposed capturing sensor we tested the usability of the entire authentication system on new users. The system has been totally automated, only requiring the users to position their wrists inside the field of view of the camera, decide between two modes: enrollment or authentication, and finally capture four images. The final results show that the proposed SIFT matching algorithm is quite slow when performing authentication. The entire authentication process takes an average of 18 s when performing authentication. The part that takes more time is the SIFT matching algorithm as the system has to compare 16 images when authenticating two users. This slowness can be a drawback for usability when speed is a requirement of the authentication system. One alternative to improve the system's speed could be the use of SURF features as matching algorithm instead of SIFT features. However, using these features can result in a worst authentication performance [45]. On the other hand, we also measured the performance of the application's memory consumption. In this case, when authenticating a user the application consumed an average of 20 MB. This rate of consumption can be supported for most of the new Android mobile devices, which currently have around 2 GB of memory. In addition most of the mobile applications already consume up to 400 MB of memory in a normal usage (see figure 8.4).

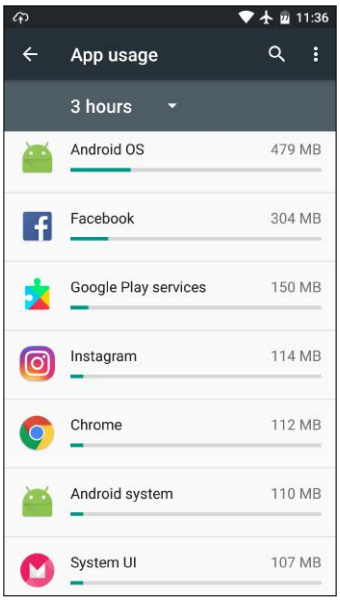


Figure 8.4: Average of memory consumption of Android applications during 3 h. Device model: OnePlus One. Android version: 6.0.1. RAM memory: 3 GB.

Chapter 9

Conclusion

Modern mobile devices store private information which has to be secured. Many authentication mechanisms rely on users to generate and remember an authentication secret. Users do not want to remember difficult or multiple secrets for different authentication systems. Thus, in many cases the security of the system is compromised due to usability of these mechanisms. Biometrics are promising security mechanisms because users do not have to remember their secret and its complexity relies on the biometric pattern, hence users cannot choose weak ones. Wrist vein authentication is promising for multiple fields of authentication applications, including mobile environments. In the future wrist vein authentication could be included in e.g. smart watches and wristbands and combined with other unobtrusive authentication approaches to obtain strong yet user friendly mobile authentication. Moreover, wrist vein authentication can be part of a multi-modal authentication system. Thus, by combining multiple authentication approaches the system can lead to a strong and reliable security mechanism.

In this thesis we present an authentication system for mobile devices. The proposed system uses wrist veins hidden under the skin, with the pattern only visible with a special sensor. Hence, it increases the system's security as without the special sensor the secret is hard to reveal. Moreover, as the secret is hidden and attached to the human body, users do not have to remember it. Therefore it speeds up and eases the way users authenticate to the system.

To achieve that, we propose a wrist vein authentication system based on a low cost capturing device which can be adapted to suit mobile environments. The proposed authentication system consists of a low cost capturing sensor to capture wrist veins and a decision algorithm for authentication. The presented capturing sensor has been built after testing two prototypes both using NIR illumination and an IR filter modified camera. The first prototype did not capture veins properly because of poor illumination conditions and a wrong selection of the camera filter's bandwidth (740 nm). In the second and final prototype, we improved the sensor's illumination by adding an array of 24 NIR LEDs. Also, we used a low cost CCD camera with a filter with a higher IR cutoff (880 nm). However, with this sensor the captured images result in low quality resolution. Thus, we propose a preprocessing methodology to improve the obtainment of the vein patterns and to reduce the images' noise. To properly enhance and segment the veins of these images, we adapted several preprocessing methodologies used in research works. Therefore, among others, we used noise reduction filters and local mean

thresholding techniques to properly segment the vein patterns. With the obtained vein pattern we then propose a matching algorithm based on SIFT features. This algorithm uses local scale invariant features to represent and match multiple patterns. However, the presented SIFT algorithm does not guarantee invariance to rotation, as under this variation some features can result in a wrong match. To improve this lack of invariance we propose to add another step when matching SIFT features. The proposed algorithm is based on the Euclidean distance between two matched features. Hence, these features are considered as a good match if their Euclidean distance is the minimum between all the other features. Finally, the similarity value between two vein images is obtained by counting the number of SIFT features that matched.

To properly evaluate the authentication system, we captured a self-recorded wrist vein dataset. Using the second prototype we captured 4 vein images of the right wrist of 30 participants, resulting in a dataset of 120 images. The recording was done in indoor conditions, with influence of external light. To facilitate the recording the capturing prototype was mounted in an open structure, simulating a mobile environment. Also, all the participants had white skin color and were rested.

Using the self-recorded dataset we then evaluated and compared six different models based on two different matching algorithms: the proposed SIFT algorithm, and the CC algorithm. For each model we configured three different approaches: using one, or four samples for enrolling and authentication, and mean or median as majority voting metrics. All these six models were evaluated using a threshold EER decision model. For each algorithm we trained and tested it basing on the data's gallery independence property. Thus, each model was first trained using 50% of the participants and then tested using the remaining 50%. The results after testing these six models show that the model using SIFT authentication, four vein images for enrollment and authentication and mean as majority voting metric (SIFT mean) is the one with more promising results (EER=0.072). Further, with the obtained results we can also conclude the models using four samples for authentication and enrolling have a better performance than the ones only using one sample. The models that use four samples can perform a more accurate classification of the users. Therefore, the final error when authentication is lower than the models using only one sample for the classification of the users.

In addition, we make a comparison of our approach to existing similar research works for vein authentication. The results show that our approach performs slightly worse than the compared ones. However, the other approaches work in different conditions than the ones in this work e.g, without external light influence, and using fixed structures, which ease the capturing of the vein images. We did not find any authentication system working in the same mobile conditions than us, thus it is difficult to compare the performance with others.

Regarding the SIFT and CC evaluated algorithms there is still room to improve. For both algorithms we can not guarantee invariance to rotation. Despite that the proposed SIFT algorithm considers features orientations when matching, we can not assure the totality of invariance to rotation. Sometimes wrong features match because of their high similarity. To improve the SIFT matching algorithm and reduce these wrong matches we propose another step based on the minimum Euclidean distance between features. Hence, if two features from different images match and the distance of their position inside the images is not the minimum one we can discard them. Nonetheless,

this Euclidean distance algorithm does not overcome the entire algorithm's variance to rotation.

On the other hand, the evaluated CC algorithm does not perform any step to overcome the rotation or scaling changes of the images. In this case, an alternative to improve the rotation invariance would be to (de)rotate the images. However this step is computationally very expensive.

Finally, using the proposed sensor to capture wrist veins, and SIFT authentication algorithm we built a software application to automatize all the capturing and authentication steps. Hence, we evaluate the performance and likelihood of the system working on an Android mobile device. The software is built on a laptop computer using JAVA and existing libraries compatible for both JAVA and Android environments. Also, we test the time and memory usage of the entire system. The results after this test show that the system requires an average of 18 s and uses an average of 20 MB for the authentication process. From these results we can conclude that the memory usage for the proposed system is valid to work in the Android mobile environment. Most of the Android modern mobile devices have at least 2 GB of memory. Besides, the slowness of the authentication system can be a drawback for systems that require speed authentication. After the time consumption experiments we observed that SIFT features are relatively slow for authentication. In addition, requiring four samples for enrolling and authentication makes the entire process time increase. The presented authentication system has to match and make a decision between 16 images.

Taking into consideration the slowness of the entire system a future step would be to increase the speed of the authentication algorithm. For this work speed was not in the initial scope, however we already presented a faster matching algorithms: SURF features. The matching for SURF features have been proved to be faster, but less powerful than the algorithm for SIFT features. Thus, an evaluation of this algorithm time and matching performance with the self-recorded dataset can be addressed in the future. Moreover, one point left open is the assurance of the totally invariance to rotation of the matching algorithm. Therefore, future research need to comprehensively evaluate the performance of approach under multiple rotation changes. Then different alternatives such as images (de)rotation, non-rigid matching algorithms –besides others– can be proposed and evaluated in the future. Likewise, future work will have to consider to reduce the number of samples required when enrolling or authenticating. The results show that using the proposed algorithm the use of only one sample for enrolling and authentication is not enough (EER= 0.319).

Further, one additional step to improve the system would be an evaluation of the matching algorithm under different lighting conditions. By now, the system has been evaluated indoors with the influence of external light and a capturing sensor with NIR illumination at 880 nm. Observing the related research works there are multiple solutions working at different NIR frequencies to capture veins (see table 4.1). In this work we implemented two different capturing sensors prototypes working at 740 nm and 880 nm resulting the vein images captured with the second one better than the ones recorded with the first one. Therefore, in the future one task can be the research and testing of the best NIR frequency to capture veins. Additionally, another challenge linked to the sensor's illumination would be evaluating the system under different human body conditions. Using the proposed sensor's illumination the surface-veins are

properly highlighted, although the deeper veins result difficult to be obtained. Thus, the light penetration in different skin tissues can be an open point to be considered in future work. Moreover, future research can investigate how veins behavior before and after doing sports. Hence, evaluate if this fact can compromise the final authentication decision. Also, all the participants recorded in the presented dataset have white skin color. So, one point left open in this work is to study the influence of the skin color when capturing veins using NIR light.

By now, our wrist vein capturing application does not detect if the recorded vein pattern is truly from the wrist. So the users can challenge the system by authenticating using p.e, the hand, or the finger veins. To improve the system's security and accuracy, a future work would be the detection of the human body part, in this case the wrist, before capturing any image for enrolling and authenticating.

The last point left open in this work is the development of the final Android mobile application. The presented software application has been theoretically demonstrated that can potentially work in an Android device. Also, all the resources used in the developed JAVA application, such as the libraries, are compatible with Android. Thus, in the future a mobile application will have to be developed and properly tested in an Android mobile device.

References

Literature

[1] Herbert Bay, Tinne Tuytelaars, and Luc Van Gool. "SURF: Speeded Up Robust Features". In: *Computer Vision – ECCV 2006: 9th European Conference on Computer Vision, Graz, Austria, May 7-13, 2006. Proceedings, Part I*. Ed. by Ales Leonardis, Horst Bischof, and Axel Pinz. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 404–417 (cit. on p. 23).

[2] Andrew P. Bradley. "The use of the area under the ROC curve in the evaluation of machine learning algorithms". *Pattern Recognition* 30.7 (1997), pp. 1145–1159. URL: http://www.sciencedirect.com/science/article/pii/S0031320396001422 (cit. on p. 24).

[3] L. Chen et al. "Near-Infrared Dorsal Hand Vein Image Segmentation by Local Thresholding Using Grayscale Morphology". In: *2007 1st International Conference on Bioinformatics and Biomedical Engineering*. July 2007, pp. 868–871 (cit. on p. 17).

[4] F. B. Chiao et al. "Vein visualization: patient characteristic factors and efficacy of a new infrared vein finder technology". *BJA: British Journal of Anaesthesia* 110.6 (2013), p. 966. eprint: /oup/backfile/content_public/journal/bja/110/6/10.1093/bja/aet003/2/aet003.pdf (cit. on p. 26).

[5] S. Chiasson et al. "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism". *IEEE Transactions on Dependable and Secure Computing* 9.2 (Mar. 2012), pp. 222–235 (cit. on p. 3).

[6] Andrea Maricela Plaza Cordero and Jorge Luis Zambrano Martínez. "Estudio y Selección de las Técnicas SIFT, SURF y ASIFT de Reconocimiento de Imágenes para el Diseño de un Prototipo en Dispositivos Móviles." MA thesis. Universidad Politécnica Salesiana, 2012. URL: http://41jaiio.sadio.org.ar/sites/default/files/6_EST_2012.pdf (cit. on p. 23).

[7] K. Delac and M. Grgic. "A survey of biometric recognition methods". In: *Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine*. June 2004, pp. 184–193. URL: https://pdfs.semanticscholar.org/0846/33597b4186530867efe9b91f346bbdfe1756.pdf (cit. on pp. 6, 7).

[8] Yuhang Ding, Dayan Zhuang, and Kejun Wang. "A study of hand vein recognition method". In: *IEEE International Conference Mechatronics and Automation, 2005.* Vol. 4. July 2005, 2106–2110Vol. 4 (cit. on p. 18).

[9] Tom Fawcett. "An introduction to ROC analysis". *Pattern Recognition Letters* 27.8 (2006). {ROC} Analysis in Pattern Recognition, pp. 861–874. URL: http://www.sciencedirect.com/science/article/pii/S016786550500303X (cit. on p. 24).

[10] Pol Fernández-Clotet and Rainhard Dieter Findling. "Mobile Wrist Vein Authentication Using SIFT Features". In: *Computer Aided Systems Theory - EUROCAST 2017.* Ed. by Roberto Moreno-Díaz, Franz R. Pichler, and Alexis Quesada-Arencibia. 2017 (cit. on p. vi).

[11] Ramadan Gad et al. "Multi-Biometric Systems: A State of the Art Survey and Research Directions". *(IJACSA) International Journal of Advanced Computer Science and Applications Vol. 6* (2015). URL: https://thesai.org/Downloads/Volume6No6/Paper_18-Multi_Biometric_Systems_A_State.pdf (cit. on p. 1).

[12] M. Gamassi et al. "Accuracy and performance of biometric systems". In: *Proceedings of the 21st IEEE Instrumentation and Measurement Technology Conference (IEEE Cat. No.04CH37510).* Vol. 1. May 2004, 510–515Vol.1 (cit. on p. 23).

[13] M. Gamassi et al. "Quality assessment of biometric systems: a comprehensive perspective based on accuracy and performance measurement". *IEEE Transactions on Instrumentation and Measurement* 54.4 (Aug. 2005), pp. 1489–1496 (cit. on pp. 24, 57).

[14] Cong Geng and X. Jiang. "Face recognition using sift features". In: *2009 16th IEEE International Conference on Image Processing (ICIP).* Nov. 2009, pp. 3313–3316. URL: http://bayanbox.ir/view/4119301154021935385/Face-Recognition-using-SIFT-Features.pdf (cit. on pp. 9, 20, 22, 33).

[15] Alan Goode. "Bring your own finger - how mobile is bringing biometrics to consumers". *Biometric Technology Today* 2014.5 (2014), pp. 5–9. URL: http://www.sciencedirect.com/science/article/pii/S0969476514700888 (cit. on p. 8).

[16] A. A. Green et al. "A transformation for ordering multispectral data in terms of image quality with implications for noise removal". *IEEE Transactions on Geoscience and Remote Sensing* 26.1 (Jan. 1988), pp. 65–74 (cit. on p. 16).

[17] D. Hartung et al. "Comprehensive analysis of spectral minutiae for vein pattern recognition". *Biometrics, IET* 1.1 (Mar. 2012), pp. 25–36 (cit. on p. 19).

[18] D. Hartung et al. "Spectral minutiae for vein pattern recognition". In: *Biometrics (IJCB), 2011 International Joint Conference on.* Oct. 2011, pp. 1–7 (cit. on p. 19).

[19] Sam Heye, Geert Maleux, and Guy J. Marchal. "Upper-Extremity Venography: CO2 versus Iodinated Contrast Material". *Radiology* 241.1 (2006). PMID: 16928973, pp. 291–297. eprint: http://dx.doi.org/10.1148/radiol.2411050714. URL: http://dx.doi.org/10.1148/radiol.2411050714 (cit. on p. 14).

[20] Daniel Hintze et al. "Confidence and Risk Estimation Plugins for Multi-Modal Authentication on Mobile Devices using CORMORANT". In: *13th International Conference on Advances in Mobile Computing and Multimedia (MoMM 2015).* ACM. Brussels, Belgium: ACM, Dec. 2015, pp. 384–388 (cit. on p. 11).

[21] Thang Hoang, Deokjai Choi, and Thuc Nguyen. “Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme”. *International Journal of Information Security* 14.6 (2015), pp. 549–560 (cit. on p. 11).

[22] Qin Huafeng et al. “Finger-Vein Verification Based on Multi-Features Fusion”. *Sensors* 13 (Nov. 2013). URL: http://www.mdpi.com/1424-8220/13/11/15048 (cit. on pp. 20, 22, 33).

[23] A. K. Jain, A. Ross, and S. Prabhakar. “An introduction to biometric recognition”. *IEEE Transactions on Circuits and Systems for Video Technology* 14.1 (Jan. 2004), pp. 4–20 (cit. on pp. 7–9).

[24] A. Jain, B. Klare, and A. Ross. “Guidelines for best practices in biometrics research”. In: *2015 International Conference on Biometrics (ICB)*. May 2015, pp. 541–545 (cit. on p. 52).

[25] Anil Jain, Lin Hong, and Sharath Pankanti. “Biometric Identification”. *Commun. ACM* 43.2 (Feb. 2000), pp. 90–98 (cit. on pp. 6, 7).

[26] Simon Juric and Borut Zalik. “An innovative approach to near-infrared spectroscopy using a standard mobile device and its clinical application in the real-time visualization of peripheral veins”. *BMC Medical Informatics and Decision Making* 14.1 (2014), p. 100 (cit. on pp. 1, 27, 29, 30, 32, 40–42, 44).

[27] Mateusz Kabaciński Rafal nd Kowalski. “Vein pattern database and benchmark results”. *Electronics Letters* 47.20 (2011), pp. 1127–1128 (cit. on pp. 17, 18, 27, 30, 33, 34, 44, 52, 55, 58).

[28] D. K. Karna, S. Agarwal, and S. Nikam. “Normalized Cross-Correlation Based Fingerprint Matching”. In: *2008 Fifth International Conference on Computer Graphics, Imaging and Visualisation*. Aug. 2008, pp. 229–232 (cit. on p. 18).

[29] P. Kartik, S. R. Mahadeva Prasanna, and R. V. S. S. Vara Prasad. “Multimodal biometric person authentication system using speech and signature features”. In: *TENCON 2008 - 2008 IEEE Region 10 Conference*. Nov. 2008, pp. 1–6 (cit. on p. 10).

[30] Chorng-Shiuh Koong, Tzu-I Yang, and Chien-Chao Tseng. “A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices”. *The Scientific World Journal* 2014 (2014), p. 12 (cit. on p. 7).

[31] Chulhan Lee, Sanghoon Lee, and Jaihie Kim. “A Study of Touchless Fingerprint Recognition System”. In: *Structural, Syntactic, and Statistical Pattern Recognition: Joint IAPR International Workshops, SSPR 2006 and SPR 2006, Hong Kong, China, August 17-19, 2006. Proceedings*. Ed. by Dit-Yan Yeung et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 358–365 (cit. on p. 8).

[32] Ju Hee Lee, Mi Ryung Roh, and Kwang Hoon Lee. “Effects of Infrared Radiation on Skin Photo-Aging and Pigmentation”. *Yonsei Medical Journal* 47.4 (Jan. 2006), pp. 485–490. URL: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2687728/ (cit. on p. 14).

[33] Y.J. Lee. “User authentication based on a wrist vein pattern”. US Patent App. 13/844,344. July 2014. URL: https://www.google.com/patents/US20140196131 (cit. on p. 26).

[34] Guo Shuxu Li Xueyan. *Chapter 23 - The Fourth Biometric - Vein Recognition.* Ed. by Peng-Yeng Yin. 2008. URL: http://www.intechopen.com/books/pattern_recognition_techniques_technology_and_applications/the_fourth_biometric_-_vein_recognition (cit. on pp. 1, 8).

[35] Hsiu-Fen Lin. "An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust". *International Journal of Information Management* 31.3 (2011), pp. 252–260. URL: http://www.sciencedirect.com/science/article/pii/S026840121000099X (cit. on p. 3).

[36] S. Liu and M. Silverman. "A practical guide to biometric security technology". *IT Professional* 3.1 (Jan. 2001), pp. 27–32 (cit. on pp. 12, 57).

[37] David G. Lowe. "Distinctive Image Features from Scale-Invariant Keypoints". *International Journal of Computer Vision* 60.2 (2004), pp. 91–110 (cit. on pp. 20, 22).

[38] David G. Lowe. "Object Recognition from Local Scale-Invariant Features". In: *Proceedings of the International Conference on Computer Vision-Volume 2 - Volume 2*. ICCV '99. Washington, DC, USA: IEEE Computer Society, 1999, pp. 1150–. URL: http://dl.acm.org/citation.cfm?id=850924.851523 (cit. on p. 20).

[39] D. M. Mancini et al. "Validation of near-infrared spectroscopy in humans". *Journal of Applied Physiology* 77.6 (1994), pp. 2740–2747. eprint: http://jap.physiology.org/content/77/6/2740.full.pdf. URL: http://jap.physiology.org/content/77/6/2740 (cit. on p. 14).

[40] L. M. Mayron. "Biometric Authentication on Mobile Devices". *IEEE Security Privacy* 13.3 (May 2015), pp. 70–73. URL: http://ieeexplore.ieee.org/document/7118088/ (cit. on p. 11).

[41] W. Meng et al. "Surveying the Development of Biometric User Authentication on Mobile Phones". *IEEE Communications Surveys Tutorials* 17.3 (2015), pp. 1268–1293. URL: http://ieeexplore.ieee.org/document/7000543/ (cit. on pp. 6, 11).

[42] Lisa Myers. "An Exploration of Voice Biometrics". *SANS Institute Reading Room* (2004). URL: https://www.sans.org/reading-room/whitepapers/authentication/exploration-voice-biometrics-1436 (cit. on pp. 1, 10).

[43] L. O'Gorman. "Comparing passwords, tokens, and biometrics for user authentication". *Proceedings of the IEEE* 91.12 (Dec. 2003), pp. 2021–2040 (cit. on pp. 4, 12).

[44] Edouard Oyallon and Julien Rabin. "An Analysis of the SURF Method". *Image Processing On Line* 5 (2015), pp. 176–218 (cit. on p. 23).

[45] P M Panchal, S R Panchal, and S K Shah. "A Comparison of SIFT and SURF". *International Journal of Innovative Research in Computer and Communication Engineering* 1.2 (Apr. 2013), p. 5. URL: https://www.ijircce.com/upload/2013/april/21_V1204057_A%20Comparison_H.pdf (cit. on pp. 23, 63).

[46] P. J. Phillips et al. "An introduction evaluating biometric systems". *Computer* 33.2 (Feb. 2000), pp. 56–63 (cit. on p. 23).

[47] R. Raghavendra. “A low cost wrist vein sensor for biometric authentication”. In: 2016 (cit. on pp. 26, 30, 32, 43, 44, 52, 58).

[48] N. K. Ratha, J. H. Connell, and R. M. Bolle. “Enhancing security and privacy in biometrics-based authentication systems”. *IBM Systems Journal* 40.3 (2001), pp. 614–634 (cit. on p. 23).

[49] Catalin Curta Septimiu Crisan Titus E. Crisan. “Near infrared vein pattern recognition for medical applications. Qualitative aspects and implementations”. *International Conference on Advancements of Medicine and Health Care through Technology* (Sept. 2007). URL: https://ie.utcluj.ro/files/acta/2007/Number4/Papers/P30304.pdf (cit. on p. 26).

[50] H. A. Shabeer and P. Suganthi. “Mobile Phones Security Using Biometrics”. In: *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*. Vol. 4. Dec. 2007, pp. 270–274 (cit. on p. 6).

[51] Mohamed Shahin, Ahmed Badawi, and Mohamed Kamel. “Biometric authentication using fast correlation of near infrared hand vein patterns”. *International journal of Biomedical Sciences* 2.3 (2007), pp. 141–148 (cit. on pp. 17, 18, 26, 30).

[52] A. Shrotri et al. “IR-webcam imaging and vascular pattern analysis towards hand vein authentication”. In: 2010. URL: http://ieeexplore.ieee.org/document/5451897/ (cit. on p. 1).

[53] J.E. Suarez Pascual et al. “Capturing Hand or Wrist Vein Images for Biometric Authentication Using Low-Cost Devices”. In: *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP) 2010*. Oct. 2010, pp. 318–322 (cit. on pp. 26, 30, 32, 44).

[54] Kevin L. Sullivan et al. “Venography with carbon dioxide as a contrast agent”. *CardioVascular and Interventional Radiology* 18.3 (1995), pp. 141–145 (cit. on p. 14).

[55] S. Terada et al. “Gait Authentication using a wearable sensor”. In: *2011 Defense Science Research Conference and Expo (DSR)*. Aug. 2011, pp. 1–3 (cit. on p. 10).

[56] Kar-Ann Toh, Jaihie Kim, and Sangyoun Lee. “Biometric scores fusion based on total error rate minimization”. *Pattern Recognition* 41.3 (2008). Part Special issue: Feature Generation and Machine Learning for Robust Multimodal Biometrics, pp. 1066–1082. URL: http://www.sciencedirect.com/science/article/pii/S0031320307003627 (cit. on pp. 23, 52).

[57] Shari Trewin et al. “Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption”. In: *Proceedings of the 28th Annual Computer Security Applications Conference*. ACSAC ’12. Orlando, Florida, USA: ACM, 2012, pp. 159–168 (cit. on p. 11).

[58] L. Wang and G. Leedham. “Near- and Far- Infrared Imaging for Vein Pattern Biometrics”. In: *2006 IEEE International Conference on Video and Signal Based Surveillance*. Nov. 2006, pp. 52–52 (cit. on p. 26).

[59] L. Wang, G. Leedham, and S.-Y. Cho. “Infrared imaging of hand vein patterns for biometric purposes”. English. *IET Computer Vision* 1 (3 Dec. 2007), 113–122(9) (cit. on pp. 1, 17, 26, 30, 43).

[60] Lingyu Wang and Graham Leedham. “A Thermal Hand Vein Pattern Verification System”. In: *Pattern Recognition and Image Analysis: Third International Conference on Advances in Pattern Recognition, ICAPR 2005, Bath, UK, August 22-25, 2005, Proceedings, Part II*. Ed. by Sameer Singh et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 58–65 (cit. on p. 17).

[61] Mark J. Burge Wilhelm Burger. *Digital image processing : an algorithmic introduction using Java*. Ed. by Second edition. Second edition. London, Springer, 2016 (cit. on pp. 19–22, 35, 48, 49, 61).

[62] J. Yang and M. Yan. “An improved method for finger-vein image enhancement”. In: *IEEE 10th INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING PROCEEDINGS*. Oct. 2010, pp. 1706–1709 (cit. on p. 15).

[63] Cheng-Bo Yu et al. “Finger-vein image recognition combining modified hausdorff distance with minutiae feature matching” (2009). URL: http://www.scirp.org/journal/PaperInformation.aspx?PaperID=574 (cit. on pp. 1, 17–19).

[64] YUN et al. “Wereable Device and Methods of Operating the Same”. 14/812436. Feb. 2015. URL: https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2017010819 (cit. on pp. 28, 30).

[65] S. Zhao, Y. Wang, and Y. Wang. “Extracting Hand Vein Patterns from Low-Quality Images: A New Biometric Technique Using Low-Cost Devices”. In: *Fourth International Conference on Image and Graphics (ICIG 2007)*. Aug. 2007, pp. 667–671 (cit. on p. 16).

[66] Vladimir P. Zharov et al. “Infrared imaging of subcutaneous veins”. *Lasers in Surgery and Medicine* 34.1 (2004), pp. 56–61 (cit. on p. 26).

Online sources

[67] AccuVein. *AV400 Vein Viewing System*. English. AccuVein Inc. 2015. URL: http://www.accuvein.com/products/catalog/av400-vein-viewing-system/ (cit. on pp. 27, 30).

[68] BioID. *BioID Facial Recognition App with face login*. BioID Mobile. Apr. 2017. URL: https://mobile.bioid.com/ (cit. on p. 8).

[69] CIE Biometrics. *Vein Pattern Dataset (VPD)*. CIE Biometrics. Nov. 2016. URL: http://biometrics.put.poznan.pl/vein-dataset/ (cit. on pp. 44, 45).

[70] Hamdi Ceylan. *Asp.Net Web API Token Based Authentication*. Dec. 2015. URL: http://hamdiceylan.com/asp-net-web-api-token-based-authentication/ (cit. on p. 6).

[71] DEW. *Near Infrared and the Electromagnetic Spectrum*. Digital Earth Watch. 2016. URL: http://dew.globalsystemsscience.org/key-messages/near-infrared-and-the-electromagnetic-spectrum (cit. on pp. 13–15, 26).

[72] Inc. Diamond Fortress Technologies. *ICE Unlock Pro Lockscreen*. Diamond Fortress Technologies, Inc. Nov. 2015. URL: https://play.google.com/store/apps/details?id=com.dft.iceunlockpro&hl=es_419 (cit. on p. 8).

[73] Elpcctv. *USB2.0 VGA USB CAMERA MODULE WITH IR LED AND IR CUT 3.6MM LENS*. Elpcctv. Jan. 2017. URL: http://www.elpcctv.com/usb20-vga-usb-camera-module-with-ir-led-and-ir-cut-36mm-lens-p-192.html (cit. on p. 45).

[74] Nick Gavronsky. *Mobile PIN Login Now Available*. Betterment. Apr. 2014. URL: https://www.betterment.com/resources/inside-betterment/product-news/mobile-pin/ (cit. on p. 5).

[75] Yoni Heisler. *How to set up a complex passcode on your iOS device*. engadget. May 2014. URL: https://www.engadget.com/2014/03/05/how-to-set-up-a-complex-passcode-on-your-ios-device/ (cit. on p. 5).

[76] HID. *Soft Tokens ActivID*. Spanish. HID. Apr. 2017. URL: https://www.hidglobal.mx/products/cards-and-credentials/activid/soft-tokens (cit. on pp. 5, 6).

[77] Hitachi. *Finger vein reader*. Hitachi. Nov. 2016. URL: http://www.hitachi.co.jp/products/it/veinid/global/products/embedded_devices_r.html (cit. on pp. 27, 28, 30).

[78] Hitachi. *USB Finger Vein Biometric Authentication Unit*. Hitachi. Nov. 2016. URL: http://www.hitachi.co.jp/products/it/veinid/global/products/embedded_devices_u.html (cit. on pp. 28, 30).

[79] Laura De Kock. *Biowatch awarded first prize at the Swiss Fintech Convention 2017*. Biowatch. Feb. 2017. URL: http://www.biowatch.ch/web/ (cit. on pp. 29, 30).

[80] LOCI. *ImageJ - An open platform for scientific image analysis*. ImageJ. Sept. 2016. URL: https://imagej.net/Welcome (cit. on p. 47).

[81] Mathuranathan. *Central Limit Theorem*. Gaussianwaves. Jan. 2010. URL: http://www.gaussianwaves.com/2010/01/central-limit-theorem-2/ (cit. on p. 16).

[82] PixelTQ. *Near Infrared Bandpass Filter - 740nm FWHM 10nm*. Optical Filter Shop. Nov. 2016. URL: http://opticalfiltershop.com/shop/bandpass-filter/near-infrared-bandpass-filter-740nm-fwhm-10nm/ (cit. on pp. 40, 41).

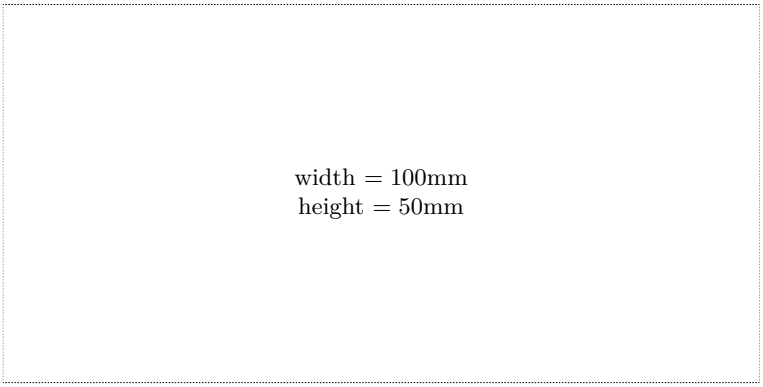
[83] Roland Smith. *Filtering a sound recording*. Roland Smith. May 2013. URL: https://rsmith.home.xs4all.nl/miscellaneous/filtering-a-sound-recording.html (cit. on p. 11).

[84] opencv dev team. *Using OpenCV Java with Eclipse*. OpenCV. Jan. 2017. URL: http://docs.opencv.org/2.4/doc/tutorials/introduction/java_eclipse/java_eclipse.html (cit. on p. 61).

[85] Chris W6oodford. *Two-factor authentication*. explainthatstuff. Sept. 2016. URL: http://www.explainthatstuff.com/how-security-tokens-work.html (cit. on pp. 5, 6).

Check Final Print Size

— Check final print size! —



— Remove this page after printing! —