LAMK
Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

ELECTRONIC SIGNATURE FOR AUTHENTICATION

LAHTI UNIVERSITY OF APPLIED SCIENCES
Bachelor of Business Administration
Business Information Technology
Spring 2019
Bouljoub Abdelwakil

Abstract

Author(s)	Type of publication	Published
Bouljoub, Abdelwakil	Bachelor's thesis	Spring
	Number of pages	
	37	

Title of publication

Electronic signature for authentication

Name of Degree

Bachelor of Business Administration

Abstract

Authentication is a crucial aspect of IT systems. It is the process that protects personal data and prevents attempts of fraud that could lead to illegally overriding authentication. Many solutions are now based on biometrics such as fingerprints and facial recognition.

A signature is also one biometric trait that is different from person to person. In electronic format, it is one possible trait for authentication. Avenla Oy, a Lahti-based ICT company, is planning to create a web-based authentication system that uses an electronic signature for authentication instead of a password.

The thesis applies a design science method. It gathers information about authentication in general and discusses several related subtopics.

The thesis analyses and summarizes the topics and presents key findings. One of the main findings is that an electronic signature has certain advantages over other biometrics in electronic authentication.

Keywords

Authentication, electronic signature, biometrics

CONTENTS

LIST OF ABBREVIATIONS

PIN Personal Identification Number

DNA Deoxyribonucleic acid

VOC Volatile organic compound

FHE Forensic Handwriting Examiner

HMM Hidden Markov Model

DTW Dynamic Time Warping

ANN Artificial Neural Network

EER Equal Error Rate

FRR False Rejection Rate

FAR False Acceptance Rate

SDK Software Development Kit

DSV Dynamic Signature Verification

1 INTRODUCTION

1.1 Authentication

Proving the personal identity is an everyday act people do. Frequently, a person needs to prove who he claims to be. Consequently, a decision is taken to determine if that person is allowed to do what he wants to do, and this is what authentication is for. (Stephenson 2016, 38.)

There are several situations where authentication is used. For instance, the opening of a door with a key is a way to prove that a person has the privilege to access a building. However, the authentication concept is clearer in law enforcement and public service operations using plenty of policies and tools such showing an identity card or providing private information.

Traveling without a passport or identity document is a scenario that could become an option soon, not because authentication is not needed anymore but because of the use of biometric-based authentication in airports. (Moeller 2018)

1.2 Objective and method

The thesis aims to discuss the electronic signature as a biometric authentication method. The aim is to answer the following research questions:

- What are biometrics and how are they related to authentication?
- What makes a person's signature a suitable biometric authentication method?

The research questions are addressed following the design science guidelines:

- Gather data about the applicable knowledge related to authentication including theories, methods and key concepts
- Evaluate existing authentication methods that are based on biometrics
- Gather information about electronic signature and its application in authentication
- Assess the work by a simulation in the form of a web application demo created for the thesis commissioner.

The thesis was commissioned by Avenla Oy. Avenla is a Lahti-based ICT company planning to create an authentication method based on the user's signature.

1.3 Thesis structure

The structure of the thesis is illustrated in figure 1. The beginning starts with a discussion about authentication. Then, different types of biometrics are evaluated as authentication methods, which leads to the electronic signature verification.

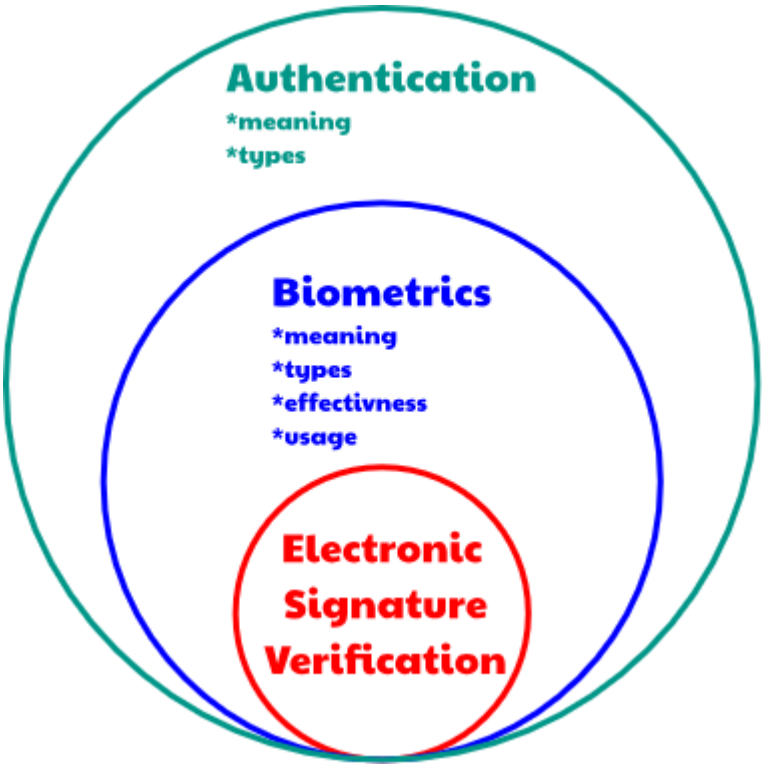

Figure 1 The thesis structure

2 ELECTRONIC AUTHENTICATION AND THE CHALLENGE

In the field of information technology, authentication is the act of verifying identity (ISO 16484-5:2017). This is the ability of a system or application to verify that a user is genuinely who that user claims to be. The authentication's result controls the user's access to a protected digital resource.

Generally, the methodology used to conduct an electronic authentication operation could be simplified into two types. The first one is looking at what a person or a thing possesses, and the second one is looking at what piece of information a person or a thing know or hold. However, the authentication credentials used in the operation should be unique for a user in that context, which means that some provided credentials are not enough even though they could be classified in one of the two types. In some cases, the two types are combined simultaneously, which create different categories of what is known as an authentication factor.

Margaret Rouse listed in her article (Rouse 2018) the authentication factors as the following:

- Knowledge factor: is an authentication credential that consists of information that the user possesses or know, including a PIN (personal identification number), a user name, a password or the answer to a secret question.
- Possession factor: is an authentication credential based on items that the user can own and carry with them, including hardware devices like a security token or a mobile phone used to accept a text message or to run an authentication app that can generate a one-time password or PIN.
- Biometric factor: sometimes referred to as inherence factor, is typically based on some form of biometric identification, including finger or thumbprints, facial recognition, retina scan or any other form of biometric data.
- Location factor: many peoples don't consider it as authentication factor as cannot usually stand on its own for authentication, but it could be sometimes used as an adjunct to the other factors "Where you are." While it may be less specific, the location factor is sometimes used as an adjunct to the other factors by providing a means of ruling out some requests. For example, it can prevent an attacker located in a remote geographical area from posing as a user who normally logs in only from home or office in the organization's home country.
- Time factor: similarly, to location factor, the time factor is not sufficient on its own, but it can be an additional mechanism for preventing attackers who attempt to access a resource at a time when that resource is not available to the authorized

user. For example, if the user was last authenticated at noon in America, an attempt to authenticate from Asia one hour later would be rejected based on the combination of time and location.

The crucial aspect of an authentication process is providing the authentication credentials, and regardless which authentication factor is used to create or generate those credentials, the risks and threats related to them are high.

In addition, because IT systems are essential in our lives, the need for an effective and efficient means of verifying an individual's identity has lead information technology experts to work in the development of mechanisms that enhance security. In addition to security, the challenge in IT is the difficulty to manage many credentials. A single user needs authentication to multiple accounts and systems. For instance, that could mean having multi-passwords or usernames. To avoid the burden coming with multi credentials, the development of a unique credential that could be used on all systems, seems to be a reasonable solution.

So far, several approaches have been implemented depending on the characteristics of the context where the authentication is used, and the development of new methods is ongoing with the focus to finding solutions for the challenges. However, one of the solutions proposed is the use of biometrics for authentication to meet existing challenges.

3 BIOMETRIC FACTORS

Biometric refer to the information about someone's body (Ngo, Teoh & Hu 2015, 3) such as the patterns of color in their eyes, that can be used to prove the person's identity. So, an authentication factor based on biometrics consists of a biological and behavioral characteristic of an individual. These can be used to extract repeatable biometric features for biometric recognition. (ISO/IEC 2382-37:2017.)

The Biometrics Institute, an independent non-profit organization, has categorized biometrics into the following types:

- Chemicals**:** They are characteristics extracted by a chemical operation like the analysis of segments from DNA.
- Visuals: They are characteristics based on sight that have been implemented in the following methods:
    - Iris Recognition: The use of the features found in the iris to identify an individual.
    - Retina Recognition: The use of patterns of veins in the back of the eye to accomplish recognition.
    - Face Recognition: The analysis of facial features or patterns for the authentication or recognition of an individual’s identity.
    - Fingerprint Recognition: The use of the ridges and valleys (minutiae) found on the surface tips of a human finger to identify an individual.
    - Ear: The identification of an individual using the shape of the ear.
- Visual/spatial: This type combines features based on visual and size, area and position of things, some example are
    - Hand Geometry Recognition: The use of the geometric features of the hand such as the lengths of fingers and the width of the hand.
    - Finger Geometry Recognition: The use of 3D geometry of the finger to determine identity.
- Auditory: They are characteristics depending on the hearing sense, like voice and speaker recognition
- Olfactory: They are characteristics depending on the smelling sense, like odor recognition where the use of an individual’s smell to determine identity.
- Behavioural: They are characteristics that define the particular way people act and behave, including:
    - Gait: The use of an individual’s walking style or gait to determine identity.

    - Typing Recognition or Keystroke dynamics is the pattern that an individual follow while typing in a keyboard or keypad for establishing identity.
- Vein recognition: can be used to identify individuals based on the vein patterns in a person's fingers or palms
- visual/behavioural characteristics related to the authentication of a person according to handwriting, particularly the signature. The visual part in the signature is its shape, and the behavioral part is the way an individual sign. (Biometrics Institute 2019.)

3.1 The uniqueness of biometrics

Biometrics characteristics are unique to an individual. Fingerprints are one example of this. Fingerprint patterns are formed around the 17th week of pregnancy as a lump of stem cell tissue, volar pads, grown under the skin of each finger, determining the main pattern. The American National Forensic Science Technology Centre categorizes the fingerprints patterns into 3 types:

- Arch
- Whorl
- loop. (American National Forensic Science Technology Centre 2013.)

DNA is responsible for the determination of the fingerprint pattern partially. But this pattern is affected chaotically by several physical conditions where the fetus grows, which give the fingerprint its uniqueness even between two twins. (Wertheim 2011, 19.)

In addition, the ridges inside each pattern cross each other which form either a fork, dead end or others shape in an unpredictable manner (Figure 2). Is not possible to compare each fingerprint of each human being or even predict the frequency of the pattern.

However, on average each finger has about 50 of at least two ridges types in different locations in the finger. Mathematically, end by ignoring their location for simplification, there are 2^{50} possibilities ($\approx 1126 * 10^{12}$), so, comparing to the 80 billion fingerprints (10 fingerprints per person) in the world now ($\approx 80 * 10^{9}$), and if we add the probability of the locations of each of those ridges, we can say that fingerprints patterns are unique. And that what explains the use of them in forensic science. Hence, the assumption is that biometrics is a reliable trait to distinguish between individuals.

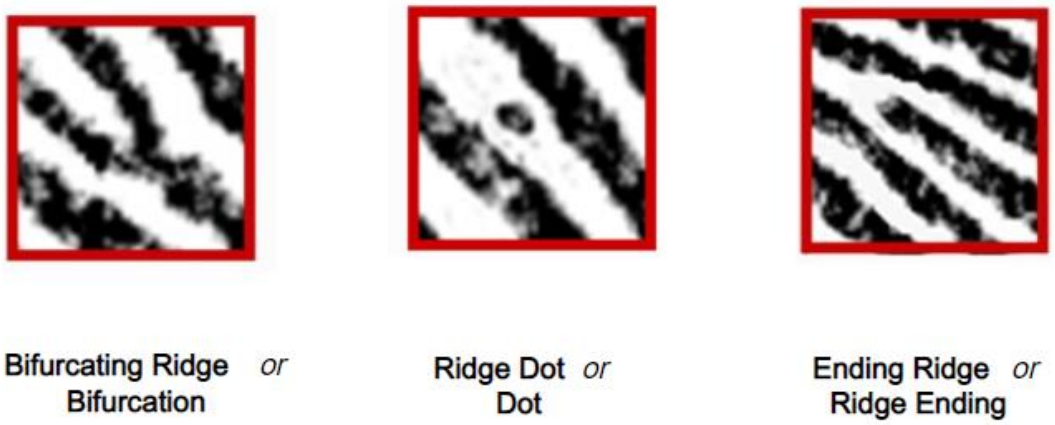

Figure 2 Three Basic Ridge types (Classroom forensicsTM and Scientific Inquiry Fingerprint Ridge Authorities Lab 2006)

3.2 The usage of biometrics

The first reference for the biometrics in the authentication context appeared in an article of the New York Times in 1981. However, the concept has been implemented several years ago, according to the National Biometric Security Project, the fingerprint, for example, represents the oldest method of biometric identification, with its history going back as far as at least 6000 B.C. The first recorded use of fingerprints was by the ancient Assyrians, Babylonians, Japanese, and Chinese for the signing of legal documents. (National Biometric Security Project 2008, section 2-1.)

Nevertheless, the popularity of biometrics has been attached strongly with technology. Especially during the last few decades, where the development of electronic devices has lead to narrow down the gap between the theoretical idea behind the use of biometrics and the possibility to implement them. For instance, it becomes easier to integrate sensors that capture data and algorithms that take advantage of that captured data, with devices and tools that are in use widely by people.

Statistics show that the biometrics market is growing rapidly. The cumulative worldwide revenue is forecast to reach nearly 70 billion USD during the period between 2016 and 2025, at a compound annual growth rate of 22.9%. The B2B market is the main target of the biometric solutions creators, to help companies manage their employees or improving public security in case of an authority or government party. (European Commission 2018.)

According to an analysis done by a French company called Yole Development, 65% of global biometrics revenues comes from the consumer market (Figure 3). Considering that

half of the world's population is mobile phone users, experts predict that biometrics will be used widely by normal people.

> *ubiquity of mobile devices capable of obtaining biometric samples would potentially represent a paradigm shift in which biometrics would become an every day, rather than an occasional, method of assuring identity (Guest, as cited in The House of Commons of the United Kingdom 2015, 9).*

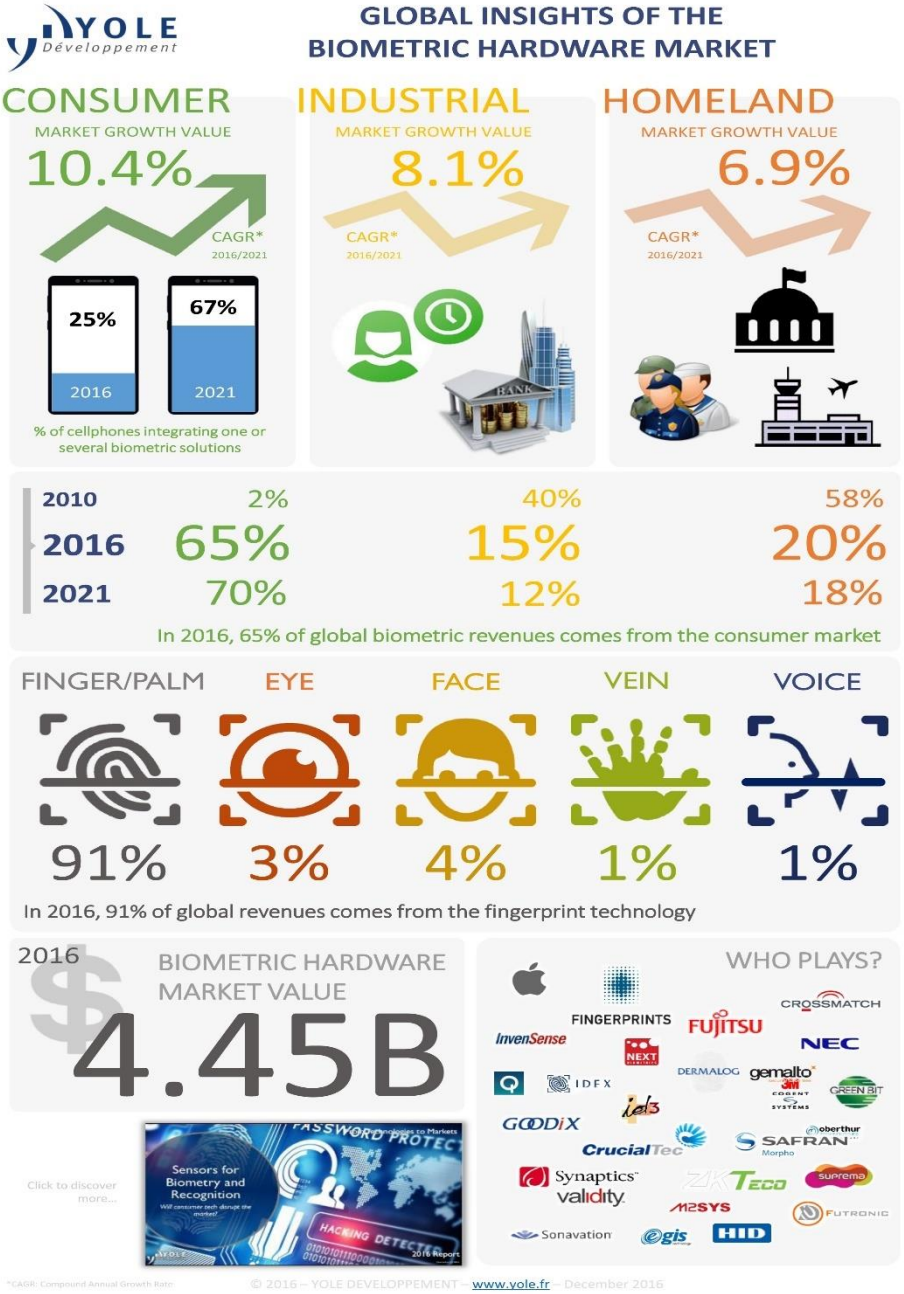

Figure 3 Global Insights of the biometric hardware market (Yole Développement 2016)

3.3 Existing biometrics methods

3.3.1 DNA Matching

DNA stand for Deoxyribonucleic acid is a hereditary material consist of molecules that form a shape of twisted ladder that contains a sequence of four chemical bases: adenine (A), guanine (G), cytosine (C), and thymine (T). This determines the information available for building and maintaining an organism (U.S. National Library of Medicine 2018)

In 1984, Alec Jeffreys British genetics and his team at Leicester university developed a technique to extract a part of DNA that is unique for each person, this technique is knowns as DNA profiling or DNA fingerprint. (University of Leicester 2014)

The profile generated by that technique has been used in forensic studies and investigations, where the technique proved its effectiveness by solving critical cases. But the time, the process, and the tools required to use this technique make it nearly impossible to be implemented in other fields such IT authentication, where a quick and low-cost process is the only solution.

3.3.2 Body odor

The human body has a scent that gets affected by many factors like diet, environment, hygiene and genetic, which affect an organic chemical produced by the skin called Volatile organic compounds (VOC) that float in the air before it reaches our noise. Biologists believe that those VOCs could be collected and measured to produce a unique odor print for each person.

> *Gary Beauchamp, an active researcher in topics related to taste and olfaction said: "The findings using this animal model support the proposition that body odours provide a consistent 'odourprint' analogous to a fingerprint or DNA sample" as he commented a related experiment. (Beauchamp 2008, as cited in Thompson 2008)*

Research that has been conducted in the field of human body odour, show the usefulness of human scent in personal identity. This means that it could be used in the development of many fields as canine training for example. (Rajan, Hassan & Islam 2014, 33-34.)

But the usage of individual's odor in IT authentication is not something could be seen soon, regarding the process involved. Even though it could be applicable at least theoretically, especially with the progress made in the concept of what is called electronic nose, that can detect VOC and make it ready to be used in different applications. (Zheng, Li, Shen & Jian 2018.)

3.3.3 Vein recognition

As other biometrics, a vein pattern is considered unique for each individual. Bernard Birnbaum, senior vice president, vice dean and chief of hospital operations at NYU Langone, claims that Vein patterns are 100 times more unique than fingerprints. (Birnbaum 2011, as cited in Plasencia 2011.)

Contrary to previous types, the technology of vein recognition system is already existing. In Japan, many banks already use vein-scanning technology as an added security measure in their ATMs. The Bank of Tokyo-Mitsubishi UFJ was the first to deploy the system, in 2004. (Strickland 2019)

The vendors of vein recognition solutions encourage the adaptation of the technology because it provides a strong security level. Firstly, the vein pattern is hidden inside the body and it is far from the sight which makes it difficult to copy. Secondly, a recognizable pattern could be taken only from a living body. Finally, it ensures a friendly usage that doesn't ask from the user more than showing a hand to a scanning device. (Jones 2014.)

However, in 2014, the biometrics group at the Idiap Research Institute in Switzerland published a video on the internet where they perform a successful attack to a vein recognition device, by using some image processing technique and basic tools like paper and marker pen. (Idiap research institute 2014.)

3.3.4 Ear recognition

The outer section of the human ear forms a shape with geometrical features that it is used for identifying individuals. The outer ear may prove to be one of the most accurate and least intrusive ways to identify people (Abaza & Ross 2010). Especially its shape, that doesn't change dramatically by time or get affected by normal and daily human activities.

There is in the market a commercial surveillance and authentication systems based on ear recognition. This was developed by Descartes Biometrics a US-based tech company and demonstrated at CES (Consumer Electronics Show) in 2015.

But the explorable nature of the outer ear, make it susceptible to copying and hacking attempts, which bring many concerns while using a system that relies on ear recognition.

3.3.5 Eye recognition

Eye recognition is a well-known technique nowadays. It becomes popular as it been introduced in many recently released electronic devices like smartphones and devices used for surveillance.

In the past, eye recognition technique existed in science fiction movies and it appeared in the 1982 American film Star Trek II: The Wrath of Khan (Image 1) Kirk (movie's personage) uses a retina scan to access Project Genesis data.

Image 1 Kirk undergoing a retinal scan (Shatner 1982)

Before that movie, the French police officer and biometrics researcher Alphonse Bertillon, included with his book '*Identification anthropometrique: instructions signaletique'* a classification table of nuances human iris (Figure 4)

Figure 4 Table of different Human Iris (Bertillon 1893)

However, the implementation started only in 2001, when John Daugman a professor of computer vision and pattern recognition at the University of Cambridge developed the

algorithms to perform Iris recognition and created the first live demonstration (University of Cambridge 2019)

Eye recognition systems in general, including iris or retina scanning, raised plenty of concerns:

- privacy as it requires to capture the user face each time he needs to be identified to a system
- security expert claims that it could be possible to bypassed similar systems. (Brewster 2015.)

3.3.6 Voice recognition

Voice recognition means recognizing who is the speaker. Sometimes, it is confused with speech recognition which means recognizing what is being said. Patented following research in an Italian research center called CSELT *(Centro Studi e Laboratori Telecomunicazion*i) done by Michele Cavazza and Alberto Ciaramella in 1983 (Cavazza & Ciaramella 1988)

Nuance is the name of a multinational computer software technology corporation and one of the leaders in the field of voice technology. Especially after the acquirement of many companies over the world including the Italian Loquendo that have been emerged before with CSELT, it is also behind the famous Apple virtual assistance Siri. Nuance claims that surveys find that 90% of consumers would prefer voice biometrics for authentication over passwords and security questions. (Nuance 2013)

Voice recognition used to identify bank's customers over the phone as the case with the British institution Barclays (Barclays 2016). However, the BBC Click reporter Dan Simmons published a video where his non-identical twin, access an account made by Dan in a local bank that provides voiced identification service, via the telephone after he mimicked his brother's voice. (Simmons 2017)

3.3.7 Face recognition

In 2017, The multinational technology company Apple announced its new feature coming with a released new smartphone, called Face ID. A feature that uses a combination of integrated components like an infrared camera, a dot projector, and advanced algorithms to extract face features and make facial authentication. (Schiller 2017.)

So far, the technology shows its effectiveness regarding:

- Performance: as it is work under different circumstances and conditions with a high rate of accuracy.
- Security: Apple announced that their technology can't be hacked (Schiller 2017), However a journalist from Wall Street Journal tried the feature with identical twins and the system wasn't able to distinguish between them (Stern 2017)
- Health: infrared radiation level used in facial recognition is categorized as non-ionizing radiations (radiations that not causing cancer). (ICNIRP 2006)

However, the technique is one of the most arguable biometrics when it comes to user's privacy, especially as it could be overlapped with other implementation fields like law enforcement.

3.3.8 Signature recognition

Originally, the idea is derived from the ordinary and old method used by people to sign documents, and especially the legal ones. The aim of the signature is to show a person's consent of the document's content.

The signature is worldwide used and adopted by all nations. It evolved throughout history, starting from pictographs used 3000 BC, and ordinary signatures on paper during middle centuries, till the electronic signature become legally accepted at the beginning of 21st century.

And because it exists that long, it was mandatory to develop a verification system that approves genuine signatures and detect fraud attempts. The extraction of signature shape features was the main method used for a long period, till the first study was published in 1977 about computer system for the detection of freehand forgeries of signatures on bank checks (Nagel & Rosenfeld 1977). In parallel, a study was published in the IBM Journal of research about a verification system based not only on the signature shape but also parameter extracted from the process of signing. (Herbest & Liu 1977)

3.4 Similarities and disadvantages in biometrics

Almost all type of biometrics has been used in a way or another to perform authentication. Although they have a noticeable different taxonomy, they still have common issues when they are implemented in electronic authentication:

- Process: all electronic authentication system goes throughout a process that consists of at least two essentials steps:

1. Capture parameters of the biometric using sensors or other electronic devices, to create a credential or authentication claim.
2. Compare that credential with a captured reference credential that has been stored, using a matching algorithm or other type of algorithm.

- Imperfection: No type has passed all security test.
- Unchangeability: The usage of someone's biometrics could be useless if another person gets enough data about it. Unlike other authentication types, there is no possibility to change a credential obtained from biometrics.
- Unwillingness: biometrics could be used without the conscious or the intention of the owner.

Furthermore, some type of biometrics could be excluded from the list of the possible method used for the best electronic authentication system. Either regarding the insufficient scientific knowledge about them like odor recognition or regarding their inconvenient nature such as DNA recognition.

4 THE SOLUTION

This chapter explores different aspects of the signature. Alongside providing related studies, this section aims to explain the reason behind considering signature recognition as a good solution for biometrics authentication systems.

4.1 Signature definition

Signature is a personalized pattern recorded by a writing instrument (Styler & Steven 1995, 7). A human hand containing 27 bones controlled by more than 40 muscles, which give the hand the ability to move accurately according to a timing system under a neural control of movements of the arm, the hand, and the fingers. (Huber & Headrick 1999, 27)

In some cultures, people prefer to distinguish between a signature and an autograph. An autograph is similar to a signature but most likely have an artistic look and may consist of one symbol or more. For the purpose of this project, a signature refers to any kind of handwriting pattern (symbol, name, sentence, lines…etc) or combination of many paths using a pen.

4.2 Signature elements

A signature is a result of a behavioral process similar or part of the handwriting habit. The signing habit contains two elements:

- Form: the shape created as the pen leave a trace on a paper or other material
- Rhythm: aspects that define the behavior itself. For instance, the pen movement

Figure 5 illustrates several sub-elements of the two previous elements, which are integrated smoothly with each other in a manner that makes it sufficient to be considered as unique.

The value of those elements comes in the verification process. While judges and lawyers in most cases rely on the form element to compare two signatures, a document examiner or a specialist on signature verification should use all possible elements to extract as much as possible of parameters from a given signature in order to reduce the error rate.

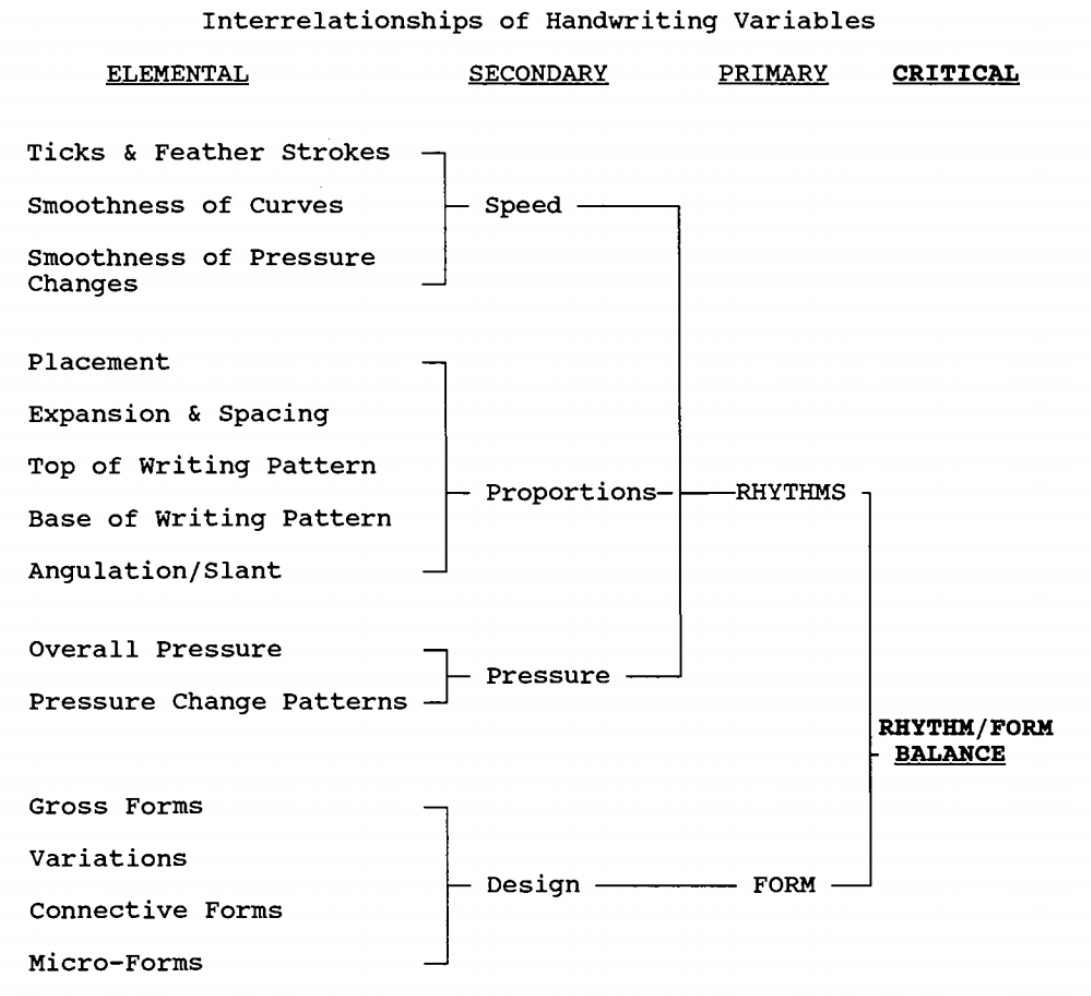

Figure 5 Signature elements (Styler et al. 1995, 11)

4.3 Electronic signature

The signature has been adapted to take its electronic form and it's known shortly by e-signature. It is used to secure personal authentication electronically, especially with applications that provide public services such as health, government, and justice. (Pirlo, Impedovo, Plamondon & O'Reilly 2014, 1-2)

E-signature is often used interchangeably with a digital signature, but they are two different concepts. A digital signature is as a term that mainly used to describe the encryption system that secure, prove the origin and integrity of the flow of documents electronically between a sender and recipient (Teletrust 2011, 59). On the other hand, the e-signature means the data aggregated from the capture of the signature.

4.3.1 Electronic signature hardware

Technically, an electronic signature is captured using a tablet (Image 2) and pen or often refer to as a stylus. The concept is similar to the drawing tablet, where the stylus used to send precise electrical signals from specific locations on the device screen.

Even though that all touchscreen devices could be used for capturing an electronic signature, in the market, there are some devices dedicated specially for e-signature usage. Those devices are in most cases using what is called Resistive Touchscreen technology because generally, this technology is more affordable and durable compared to other used touchscreens technologies. (Hill. 2002)

Thought the rest of this thesis, the word pad used to refer to the device used to capture the signature regardless of the type or the technology behind it as this is beyond the scope of this project.

Image 2 Signature pad duraSign Pad Brilliance (StepOver 2019)

4.3.2 Electronic signature and laws

In 2000, the USA Congress passed a regulation called the Electronic Signature in Global and National Commerce Act, that recognize the validity of the electronic signature on law enforcement. (Electronic Signatures in Global and National Commerce Act 106-229, 2000)

For the European Union, the Countries members regulate the electronic signature by a set of standards in 2014, those standards came in place to replace a relative directive made in 1999. (REGULATION (EU) No 910/2014)

In England and Wales, the Law Commission is on an advanced stage of working on a consultation report about the electronic signature. (Law Commission in England and Wales 2018)

In Finland, a related regulation issued in 2018. The regulation has many objectives like providing requirements for identification device creation process and identification method. (FICORA 72A/2018 M)

4.3.3 Electronic signature benefits

The electronic signature brings many benefits to governments, companies, and end users in general:

- Environmentally friendly: the usage of the electronic signature cut carbon footprint.
- Time-saving: the electronic signature reduces the time of exchanging documents between parties.
- Cost saving: it helps reducing operational costs. (Connecting Europe Facility 2019)

4.4 Advantages of signature in authentication

In addition to the biometrics' advantages, the signature is differentiated from other biometrics types on the following:

- Popularity: It is not difficult to ask people to give their signature. This is because the concept is familiar and acquired by people from different cultures across the world.
- Ensure privacy: even though the signature could be used to reveal the identity of the signer, it doesn’t gather any data about the signer that could be used as a selective factor, such as data about physiological features.

- Changeability: in contrast to other biometrics, the signature is the only biometric type that a person could change part of it easily. It could be hard and not recommended to change how a person signs, but it is easy to change how the signature looks like.
- Consciousness: Aligning with the main aim of the signature, the conscious of the person is the only way to get a signature. In contrast to other biometrics, the signature could be provided only with the user's intention.
- Effective complexity: the signing act is a complex operation that requires the intersection of brain, eye, muscle, fingers, and nerves. But this complexity is effective as it happens simultaneously and quickly.
- Security: when gathering all data about signature elements, it becomes a very strong and multilayer authentication credential that couldn't be forged easily. For example, the time factor tells exactly the time span that a given person needs to accomplish a signature. And the security is enhanced with the fact that most of the critical signature elements are hidden and couldn't be copied.

5 SIGNATURE VERIFICATION

A person’s signature can be slightly different each time. Hence, the signature verification is about developing a definition of the signature's range of normal variations and telling if a questioned signature is within that range. (Styler et al. 1995, 26)

The process of signature verification can have 4 results:

- Genuine: it means that the two signatures are identical and belong to the same person
- Random forgery: the two signatures have no or few similarities, which give the assumption that the forger has no access to the original signature.
- Casual forgery: in this case, the forger has access to the original signature and this reference might be used as a guide either by looking to it or trace over it.
- Skilled forgery: besides the access to the original signature, a skilled forger could have many references of the original signature and have time to practice the imitation of the original signature. (Nazakat, Khalid & Siddiqi 2014.)

In forensic science, Forensic handwriting examiners (FHEs) perform forensic analysis on several paper-based documents like contracts, and letters to be used in court cases (Tistarelli & Champod 2017, 329-330).

In the past, FHEs and documents examiners relied mostly on basic measurment tools such as metric ruler, angle meter and microscopes. In last century, new techniques and tools were invented to help FHEs like Electrostatic Detection Device that reveals some invisible elements (Griechisch 2018, 4). Curently, automated solution are used for the signature verification with two types, offline and online verification.

5.1 Offline verification

Offline or sometimes called static verification is the name of the verification type used when there is no available or no possibility to collect data about the signing process. In this situation, the design of the signature in question is the only available material which means the absence of the other signature’s elements. Therefore, the signature gets scanned, and the algorithms in this scenario are based on image processing techniques to extract the static feature of the given signature. (Azzopardi 2006, 4.)

5.2 Online verification

Online or sometimes called dynamic verification is applied to the signatures that are acquired using a pad. Some pads are capable to collect data about dynamic features of the signature including timestamp, x and y coordinates, velocity, pen pressure, and azimuth. (Griechisch 2018, 6.)

5.3 Verification steps

The following are the basic steps of verification:

- Data acquisition: is the enrolment of the signature in the system, like scanning the signature in case of offline verification or capturing the signature in online verification case.
- Pre-processing: Is the application of image processing technique on the signature image, to improve the quality of the image. Those techniques include noise reduction, size normalization, contrast, and line improvement...etc.
- Feature extraction: in this step, the characteristics of the signature are extracted and selected to be compared later. There are 3 categories of features that could be extracted:
    - Global features are the features that describe the signature like the height, the width, height/width ration, horizontal and vertical projection peaks...etc
    - Local features are similar to global features, but they describe a part of the signature. For example, the signature's image could be split by a grid and features are extracted from each cell of that grid.
    - Pseudo-dynamic features are individual characteristics like the pen pressure, stroke curvature, and stroke regularity and as the name said, those features attempt to recover the information about the missing signature's elements.
- Comparison process: or classification process, is about comparing two signature references if applicable or give a detailed description of the questioned signature. (Azzopardi 2006, 11-16.)

5.4 Verification techniques

In general, some techniques have been used for both online and offline verification. However, some techniques could be or have been used for a spesific one due to thier structure. (Impedovo & Pirlo 2008, 617.)

5.4.1 Template matching techniques

Template matching is a widly used techniques in digital image processing. For signature verification it is used to find small parts of a signature's image which match a template signature. (N.Purohit, S.Purohit & Satsangi 2014, 89.)

There are several approaches when template matching techniques are considered including DTW (Dynamic Time Wraping) which is a method used to measure the similarities between two sequences that represent measurements of a quantity over time (Elsworth 2017). For instance, to measure how much similar are two sequences that describe the pen speed over time of two signatures instances, the DTW calculate the distance between a point from the first sequence with the best possible point or points from the second one. (Shanker & Rajagopalan 2007.)

Simple distance is another approach. It means interpreting the signature features with variables. For example, coordinates of a point in the feature. A well-known system uses that method was proposed by Yoshiki Mizukami. The system is based on displacement features between the authentic signature and questionable signature (Figure 6). (Mizukami & Koga 1996.)

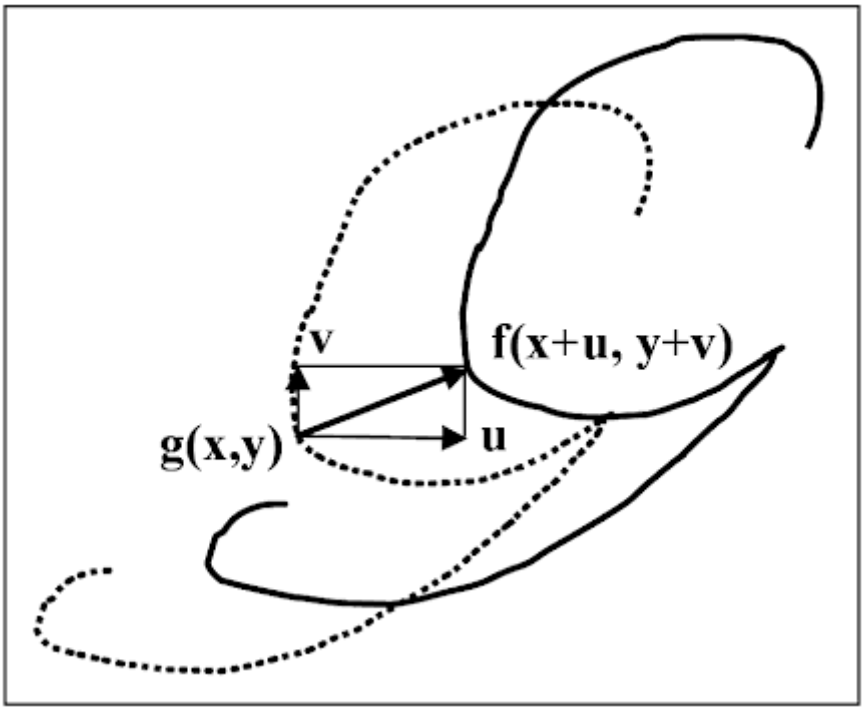

Figure 6 displacement function between g and f signatures (Azzopardi 2006, 17)

5.4.2 Statistical techniques

It is simply the use of the statistical methods to determine the similarities and deviations between two data items (Bhattacharyya, Bandyopadhyay, Das, Ganguly & Mukherjee 2008, 181). Some of the statistical techniques used for signature verification are:

HMM (Hidden Markov Models):

Markov model is a description of a random process (Tsitsiklis 2010). This process has a set of finite states, the transaction probability of an object from a state A to state B inside that process is presented with a matrix called Markov chains, which must meet certain conditions. The main one is that the next state depends only on the current one.

A hidden Markov model is an extension of Markov chains. The addition is a set of states that are emission of initial states that could not be observed. Hence, it is a Hidden Markov model. In that case, there is the possibility to calculate the probability of a state using the sequence of observed states. (Bobick 2015.)

In signature verification, A HMM is trained by extracting data from a reference signature, which means that the observation sequence used by the HMM is describing a given feature of the signature. A paper that describes the process of using HMM in signature verification is published by Rafal Doroz and Krzysztof Wrobel. (Doroz & Wrobel 2012, 75-84.)

ANN (Artificial Neural Networks)

In signature verification, a neural network applied to get advantages of the learning algorithm. By providing an extracted feature from a signature, the ANN learn the relationship between those features and a signature that make it able to classify a provided signature comparing to the one used in the training step. (McCabe, Trevathan & Read 2008, 9.)

There is also structural techniques. The simpliest are the ones that represent a signature using structres like graph and strings. Those techniques use structural analysis with matching algorithms such countour-following algorithm. Some of the well-know example including tree matching and structural description graph analysis. (Impedovo et al. 2008, 611.)

5.5 Signature verification evaluation

For an automatic signature verification, the process can generate the wrong results. Those wrong results are represented by two types, either FRR (false rejection rate) or

FAR (false acceptance rate). FRR is when a genuine verification is rejected, while FAR is when it accepte a forged signature. Those two measurments are used to determine the perfomance of a verification technique. However, the overall error of a system is measured the by EER (equal error rate) when FRR is equal to FAR. (Impedovo et al. 2008, 621.)

5.6 Signature verification competitions

Many surveys and competitions have been organized to test the performance of approaches and techniques used in handwriting verification in general and signature verification in specific. The competitions have been conducted using collected sets of signatures which were acquired with determined conditions. (Liwicki, Malik, Heuvel, Chen, Berger, Stol, Blumenstien & Found 2011, 1480.)

5.6.1 SVC2004

Stands for First International Signature Verification Competition has been held in conjunction with the first International Conference on Biometric Authentication with the participation of 27 teams from different countries.

There were two sets of signatures, both of them containing genuine signatures and skilled forgeries. The first one was available for the teams before the competition and it was collected from 40 users. The other one released during the competition and it has been collected from 60 users. Each program was evaluated on 10 genuine signatures 20 skilled forgeries selected randomly. (Yeung, Chang, Xiong, George, Kashi, Matsumoto & Rigoll 2004, 2-3)

5.6.2 BSEC2009

Stands for BioSecure Signature Evaluation Campaign was an online signature competition with the aim to study how acquisition conditions and information contained in signatures could affect the system performance. In BSEC2009, there were two data sets used for tests, BioSecure Data Set 2 and BioSecure Data Set3, both containing data of the same 382 people, acquired respectively on a digitizing tablet and on a PDA (Personal Digital Assistant). (Houmani, Mayoue, Garcia-Salicetti, Dorizzi, Khalil, Moustafa, Abbas, Muramatsu, Yanikoglu, Kholmatov, Martinez-Diaz, Fierrez, Ortega-Garcia, Roure Alcobe, Fabregas, Faundez-Zanuy, Pascual-Gaspar, Carden˜oso-Payo & Vivaracho-Pascual 2012, 993-1003)

5.6.3 SigComp2009, 2011, 2013 and 2015

The signatures set used in this competition consisted of 1953 signature in an online and offline format of each signature. The aim was to test the ability of systems to detect skilled forgery. In SigComp2009, only one reference signature was used and compared with the questioned signatures. The systems gave a similarity score between 0 and 1, with zero means non-match and one means a complete match. (Blankers, van den Heuvel, Franke, & Vuurpijl)

The aim of SigComp2011 was to raise awareness among the community about the need to take into consideration FHEs' needs while developing a verification solution. For instance, participants were asked to produce a comparison score that represents the degree of similarity or difference. The signatures set used in that competition contained offline and online Dutch and Chinese signatures. (Liwicki et al. 2011, 1480-1484)

In addition to the signature, the 2013 competition also covered writer identification. The dataset used was taken from previous competitions with new offline handwritten text sample in English. The major emphasis of the competition was to keep encouraging the community to develop systems that are relevant for forensics' purposes. (Malik, Liwicki, Alewijnse, Ohyama, Blumenstein & Foundk 2015)

SigWiComp2015 is one of the recent competitions on signature verification. It kept the same goal which to make automated verification solution more suitable for FHEs. In many cases, a person could by purpose try to change his own writing style which makes the verification decision more challenging. The data set used was enhanced with more features. For instance, some signatures have been collected over a period of time that is between 3 and 5 years. (Malik, Ahmed, Marcelli, Pal, Blumenstein, Alewijns & Liwickik 2017)

5.6.4 Compitions winners

Table 1 summarises the result of the competitions as well as the criteria used for each one. However, the verification technique used by the winners is not always published.

Table 1 Methods that win the competitions (Griechisch 2018, 35)

NAME	FORGERIES	TASK	BEST SYSTEM (%)	BASED ON
SVC2004	skilled	1	2.84	DTW
	skilled	2	2.89	DTW
	random	1	2.04	N/A
	random	2	1.70	N/A
		TASK	EER IN % DS2/DS3	
BSEC'2009	skilled	1	2.20/4.97	DTW
	random	1	0.51/0.55	DTW
	high entropy	3	3.58	DTW
	low entropy	3	1.48	fusion of 4 systems
		TASK	EER IN % WITHOUT / WITH VARIABILITY	
	skilled	2	1.71/3.48	N/A
	random	2	0.42/1.37	N/A
	QUALITY		EER (%)	
ESRA'2011	bad	1 DS2	2.73	HMM
	good	1 DS2	2.85	HMM
	good&bad	1 DS3	6.05 /7.15	DTW
	bad	2A DS2	3.32	kernel
	good	2A DS2	4.31	kernel
	good&bad	2B DS2	1.67/2.43	HMM
SigComp2009	skilled	online	2.85	N/A
	skilled	offline	9.15	N/A
			FRR/FAR (%)	
SigComp2011	sk. Dutch	online	3.70/3.76	statistics
	sk. Dutch	offline	2.47/2.19	edge-based distribution
	sk. Chinese	online	6.40/6.94	statistics
	sk. Chinese	offline	21.01/19.62	polar coordinates SVM
SigWiComp2013	sk. Dutch	offline	23.1/23.7	HOG, LBP
	sk. Chinese	offline	9.72/9.74	+SVM
	sk. Japanese	online	27.36/27.56	DTW
SigWiComp2015	sk. German	online	9.87/9.67	N/A
	sk. Italian	offline	0.87/0.80	HOG, LBP and SVM
	sk. Bengali	offline	1.67/1.67	run-length features and K-NN, SVM

6 THE EXPERIMENT

This section describes aspects of signature authentication implementation on a web-based application.

6.1 Background

The implementation of the signature authentication created as an additional feature to a new resource management application, this new application intended to be used internally by Avenla Oy to manage employees related issues.

The idea came after the integration of electronic signature in that new application in order to sign agreements. For instance, an employee signs a non-disclosure agreement as a step of the enrollment process, and then, saving the electronic signature to be used for other purposes, like testing the usability of signature authentication in a practical environment.

6.2 Hardware component

The hardware used for the experiment is a signature acquisition device called Wacom STU-300. This pad is designed specifically for electronic signature acquisition. It has a 4 inches LCD screen protected against scratches with a glass. The pad comes with a pen that doesn't need a battery or wire and has 512 levels of pressure sensitivity.

During the capture process, the pad records the movement of the pen with time. Each point of the signature collected with its corresponding information, including x and y position, pen pressure and the amount of time the process takes.

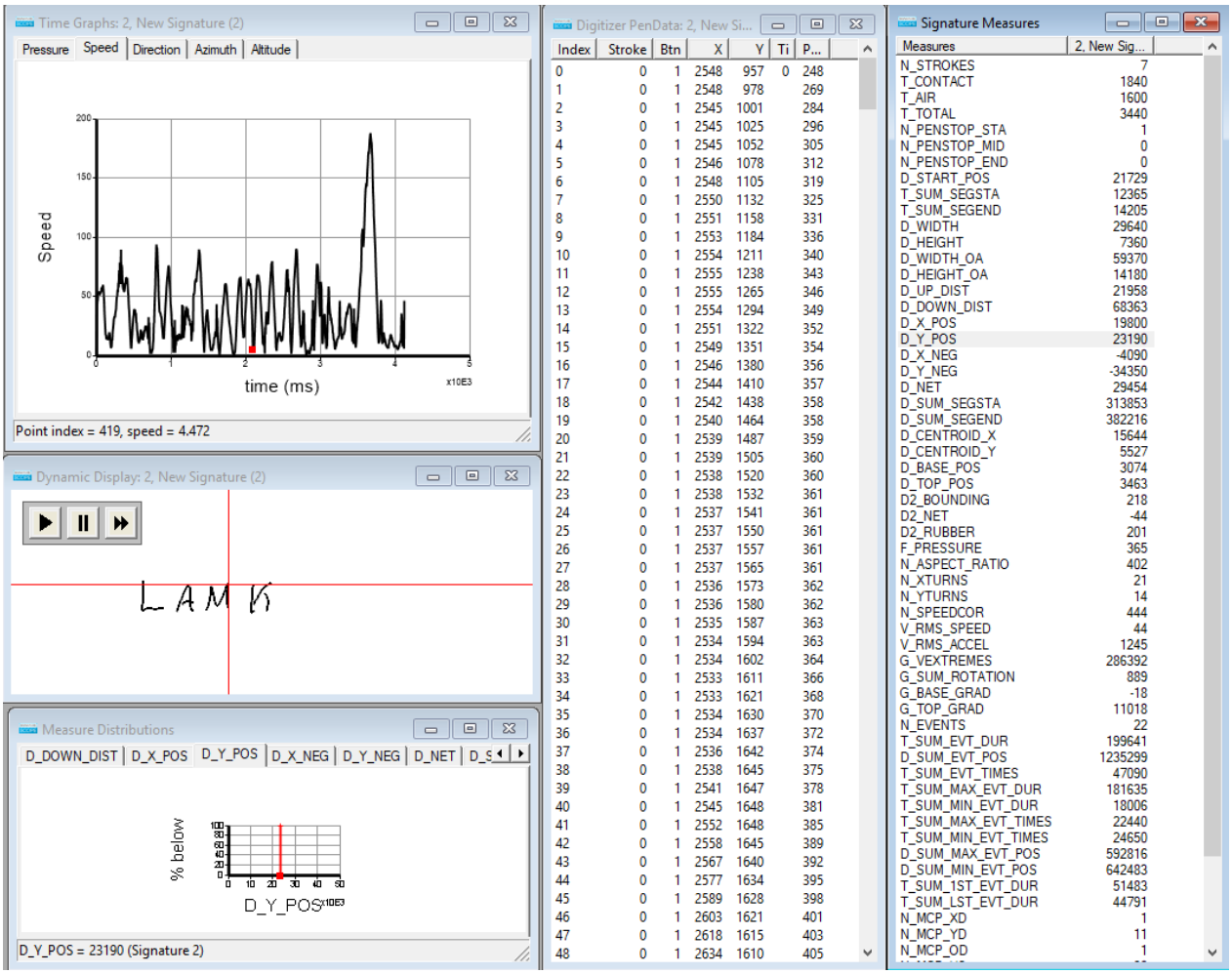

Image 3 A signature captured and examined on Wacom SingatureScop

6.3 Software component

The code needed for this experiment consist of two part.

6.3.1 Software development kit

Software development kit (SDK) is a collection of tools that a developer uses to create an application for a certain platform or system. (Shamsee, Klebanov, Fayed, Afrose & Karakok 2015, 934)

Dynamic Signature Verification (DSV) is a Wacom's SDK to compare two signatures and produce a score between 0 and 1, which represent the level of similarity. Besides the score, the SDK reports the verification stage where a difference was found in case of a score of less than 1. There are 5 stages in the verification process:

- comparison between the signatures forms
- checking missing features in the questioned signature

- comparison of the average pen speed
- comparison of the velocity profile between the two signatures
- comparison of the pen pressure with time variations

6.3.2 Signature acquisition

Wacom’s SDKs are available for different development environment and platforms. For a web environment, a JavaScript SDK framework is used to establish and maintain the communication between the pad and the browser.

6.4 Application workflow

The flow of the process is as following:

- A user triggers the signature acquisition from the index page
- The application establishes a connection with the pad
- The user submits a signature
- The application makes the verification decision according to the following logic:
- Retrieve all employees stored in the database
    - Get employees' IDs and signature strings
    - Invoke the verification method written in the SDK
    - Get the verification result, if it equals 1 redirect the user to the profile page. If the result between 0.5 and 1, the application keeps verifying the retrieved signature strings and redirect the user to the profile that belongs to the employee with the higher matching score.
- Redirect the user to the appropriate page

7 CONCLUSIONS

In general, biometrics has many advantages. However, the signature has a set of unique features. Firstly, the signature is the only biometric that could be modified. Secondly, the intention of the signer is the only way to initiate the process. Finally, the signature is a complex process that consists of a lot of parameters that could be used to create a strong authentication system.

The signature verification is an active research field. Dozens of papers are published, and many approached the topic from different perspectives, but the evaluation part wasn't often effective. Because most of the systems were tested to identify a forgery signature without testing if that signature comes from the same person, in case that person give a signature with the purpose to hide or modify the personal identity.

Evaluating the concept, methods, techniques of signature verification found to be beyond the scope of this thesis. Furthermore, the sellers of signature verification solution are not revealing the methods behind their software. However, the SDK used in that demonstration is most likely based on DTW and HMM.

The risk management aspect is partially missing from the solution provided in the market, at least the one used in conjunction with this project. The problems that could appear with either the software or the hardware are not fully explored.

This thesis could serve as a good introduction to further development. One possible implementation is the integration of a fingerprint scanner with the pen so that the process uses two factors to make verification on a One-To-One basis. The fingerprint scanner should be installed exactly where the finger is placed to hold the pen so that a person gives a signature and fingerprint simultaneously.

LIST OF REFERENCES

Abaza, A & Ross, A. 2010. Towards understanding the symmetry of human ears: A biometric perspective. IEEE Xplore. [Accessed 18 March 2018]. Available at: https://www.researchgate.net/publication/224194515_Towards_understanding_the_symmetry_of_Human_ears_A_biometric_perspective

Azzopardi, G. 2006. How effective are radial Basis function neutral Network for offline handwritten signature verification. University of London

Barclays. 2016. Barclays launches voice security technology to all customers. Blog. [Accessed 18 March 2019]. Available at: https://newsroom.barclays.com/r/3383/barclays_launches_voice_security_technology_to_all_customers

Bertillon, A. 1893. Table of different Human Iris [acceesed 30 March 2019]. Available at https://wellcomecollection.org/works/z9pb2pzj?query=Orange

Bhattacharyya, D. Bandyopadhyay, S.K. Das, P. Ganguly, D. Mukherjee, S. 2008. Statistical Approach for Offline Handwritten Signature Verification. Journal of Computer Science 4. ISSN 1549-3636. [Accessed 9 April 2019]. Available at: https://pdfs.semanticscholar.org/ccd1/b90c0f9db8ba029b1e3b3b1d4f64fb287b92.pdf

Biometrics Institute. 2019. Types of Biometrics. [accessed 30 April 2019]. Available at: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

Blankers, V.L. van den Heuvel, C.E. Franke, K.Y & Vuurpijl, L.G. 2009. The ICDAR 2009 Signature Verification Competition. 10th International Conference on Document Analysis and Recognition. [Accessed 9 April 2019]. Available at: http://tc11.cvc.uab.es/index.php?com=upload&action=file_down&section=dataset&section_id=109&file=115

Bobick, A. 2015. Introduction to Computer Vision. Udacity. Video [accessed 30 April 2019]. Available at: https://www.youtube.com/watch?v=5araDjcBHMQ&t=32s

Brewster, T. 2015. Hacking Putin's Eyes: How To Bypass Biometrics The Cheap And Dirty Way With Google Images. Forbes. [Accessed 18 March 2019]. Available at: https://www.forbes.com/sites/thomasbrewster/2015/03/05/clone-putins-eyes-using-google-images/#4c89b68d214a

Cavazza, M & Ciaramella, A. 1988. Device for speaker's Verification. United states patent and trademark office [acceessed 30 March 2019]. Available at: https://patentimages.storage.googleapis.com/bb/a2/7a/b4f3f02fac4fff/US4752958.pdf

Connecting Europe Facility. 2019. What are the benefits?. [Accessed: 4 April 2019]. Available at: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773352

Doroz, R & Wrobel, K. 2012. Using Hidden Markov Models in signature recognition. Journal of Medical Informatics & Technologies. Vol 21/2012 ISSN 1642-6037. [accessed 30 April 2019]. Available at: http://jmit.us.edu.pl/cms/jmitjrn/21/10%20-%20Doroz.pdf

Electronic Signatures in Global and National Commerce Act 106-229/2000. USA Congress

Elsworth, S. 2017. Dynamic Time Wraping. University of Manchester. [accessed 15 March 2019]. Available at: http://www.maths.manchester.ac.uk/~mbbx2se2/Docs/Dynamic_time_warping(Steven_Elsworth).pdf

European Commission. 2018. Biometrics technology: a key anabler for future digital services. [accessed 15 March 2019]. Available at: https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Biometrics%20technologies_v2.pdf

FICORA 72A/2018 M. 14 May 2018. Regulation on Electronic Identification and Trust Services. Chapter 1, Section 1. The Finnish Communications Regulatory Authority

Griechisch, E. 2018. Online signature verification and handwriting classification. University of Szeged. [Accessed 26 March 2019]. Available at: http://doktori.bibl.u-szeged.hu/9823/3/GE_PHD_dissertation.pdf

Herbest, M & Liu, N. 1977. Automatic Signature Verification Based on Accelerometry. IBM Journal of Research and Development. Volume 21, Issue: 3

Hill, A. 2002. Touch screen technologies: Their advantages and disadvantages. Control Solutions, VOL 75. ISSN, 1074-2328

Houmani, N. Mayoue, A. S. Garcia-Salicetti, Dorizzi, B. Khalil, M.I. Moustafa, M.N. Abbas, H. Muramatsu, D. Yanikoglu, B. Kholmatov, A. Martinez-Diaz, M. Fierrez, J. Ortega-Garcia J. Roure Alcobé, J. Fabregas, J. Faundez-Zanuy, M. Pascual-Gaspar, J.M. Cardeñoso-Payo, V. C & Vivaracho, P. 2012. BioSecure signature evaluation campaign (BSEC'2009): Evaluating online signature algorithms depending on the quality of signatures. Pattern Recognition. Volume 45, Issue 3

Huber, R & Headrick, A. 1999. Handwriting Identification: Facts and Fundamentals. CRC Press LLC. Boca Raton. USA

ICNIRP. 2006. ICNIRP STATEMENT ON FAR INFRARED RADIATION EXPOSURE. [accessed 30 March 2019]. Available at: https://www.icnirp.org/cms/upload/publications/ICNIRPinfrared.pdf

Idiap research institute. 27 May 2014. Spoofing FingerVein Recognition. Video. [accessed 30 March 2019]. Available at: https://www.youtube.com/watch?v=zxb9xwaoeTU

Impedovo, D & Pirlo, G. 2008 Automatic signature verification: The state of the art. IEEE Transctions on systems, Man, and cybernetics, VOL 38, NO 5. [accessed 30 March 2019]. Available at: https://www.researchgate.net/publication/3421962_Automatic_Signature_Verification_The_State_of_the_Art

ISO 16484-5. 2017. Building automation and control systems (BACS) — Part 5: Data communication protocol 3.2.7. International Organization for Standardization.

ISO/IEC 2382-37. 2017. Information technology — Vocabulary — Part 37: Biometrics. International Organization for Standardization.

Jones, P. 7 August 2017. Ideas to Innovation: Finger Vein Technology. Hitachi. Video [accessed 30 March 2019]. Available at: https://www.youtube.com/watch?v=NCMM9sBUZyYLaw Commission. 2018. Electronic execution of documents consultation paper. [Accessed 20 March 2019]. Available at: https://www.lawcom.gov.uk/project/electronic-execution-of-documents/#related

Liwicki, M. Malik, M.I. Heuvel, C. Chen, X. Berger, C. Stoel, R. Blumenstein, M & Found, B. 2011. Signature Verification Competition for Online and Offline Skilled Forgeries. International Conference on Document Analysis and Recognition. [Accessed 9 April 2019]. Available at: http://www.iapr-tc11.org/archive/icdar2011/fileup/PDF/4520b480.pdf

Malik, M.I. Liwicki, M. Alewijnse, L. Ohyama, W. Blumenstein, M & Foundk, B. 2015. ICDAR2013 Competitions on Signature Verification and Writer Identification for On- and Offline Skilled Forgeries (SigWiComp2013). [Accessed 9 April 2019]. Available at: http://tc11.cvc.uab.es/index.php?com=upload&action=file_down&section=dataset&section_id=114&file=131

Malik, M.I. Ahmed, S. Marcelli, A. Pal, U. Blumenstein, M. Alewijns, L & Liwickik, M. 2017. ICDAR2015 Competition on Signature Verification and Writer Identification for On- and Off-line Skilled Forgeries (SigWIcomp2015). [Accessed 9 April 2019]. Available at: http://tc11.cvc.uab.es/index.php?com=upload&action=file_down&section=dataset&section_id=114&file=177

McCabe, A. Trevathan, J & Read, W. 2008. Neural Network-based Handwriting Signature Verification. Journal Of Computers. VOL 3 NO 8. [accessed 30 April 2019]. Available at: http://www.jcomputers.us/vol3/jcp0308-02.pdf

Mizukami, Y & Koga, K. 1996. A handwritten character recognition system using hierarchical displacement extraction algorithm. IEEE

Moeller, I. 2018. an interview with Isabelle Moeller, CEO Biometrics Institute. 1 March 2018.

National Biometric Security Project. 2008. Biometric Technology Application Manual. [Accessed 15 March 2019]. Available at: http://www.planetbiometrics.com/creo_files/upload/article-files/btamvol1update.pdf

National Forensic Science Technology Center. 2013. Principles of Fingerprint Analysis. [Accessed 15 March 2019] Available at: http://www.forensicsciencesimplified.org/prints/principles.html

Nagel, R & Rosenfeld, A. 1977. Computer Detection of Freehand Forgeries. IEEE Transactions on computers. VOL C-26, NO 2. [Accessed 18 March 2019]. Available at: https://www.academia.edu/22216240/Computer_Detection_of_Freehand_Forgeries

Nazkat, M. Khalid, S & Siddiqi, I. 2014. A review of offline Signature Verification Technique. Journal of Applied Envirnonmental and Biological Sciences. ISSN: 2090-4274. [Accessed 26 March 2019]. Available at: https://pdfs.semanticscholar.org/3bd6/a4a9712e4edb908e73b76b0417fb0adcca02.pdf

Nuance. 2013. Surveys Show: Consumers Ready to Say Goodbye to PINs, Passwords, and Probing. [Accessed 18 March 2019]. Available at: https://www.nuance.com/about-us/newsroom/press-releases/2013_05_08_voicebiosurvey_forweb.html

Ngo, D. Teoh, A & Hu, J. 2015. Biometric Security. Newcastle upon Tyne, England: Cambridge Scholars Publishing.

Pirlo, G. Impedovo, D. Plamondon, R & O'Reilly, C. 2014. Stability analysis of online signatures in the generation domain. Pirlo, G. Impedovo, D. Fairhurst, M. Advances In Digital Handwritten Signature Processing: A Human Artefact For E-society. Singapore. World Scientific, 1-12.

Plasencia, A. 2011. Hospital scans patient hands to pull medical info. NBC Newyork. Article [Accessed 18 March 2019]. Available at: https://www.nbcnewyork.com/news/local/Hospital-Scans-Patient-Hands-to-Pull-Medical-Info-126142628.html

Purohit, N. Purohit, S & Satsangi, C. 2014. Offline handwriting signature verification using template matching and clustering technique. International journal of soft computing and artificial intelligense. Volume 2. Issue 2. [accessed 9 April 2019]. Available at: http://www.iraj.in/journal/journal_file/journal_pdf/4-96-141544683288-91.pdf

Rajan, R. Hassan, N & Islam, M. Chemical Fingerprinting of Human Body Odor: An Overview of Previous Studies. 2014. Universiti Teknologi MARA. [Accessed 15 March 2019]. Available at: http://forensics.org.my/pdf/fssmVol.4No.1/Article6.pdf

Rouse, M. 2018. Authentication. WhatIs.com. Article [accessed 15 March 2019]. Available at: https://searchsecurity.techtarget.com/definition/authentication

REGULATION (EU) No 910/2014. 2014. The european parliament and the council of the european union

Schiller, P. 12 September 2017. Face ID on iPhone X. Video. [accessed 30 March 2019]. Available at: https://www.youtube.com/watch?v=z-t1h0Y8vuM

Simmons, D. 2017. BBC fools HSBC voice recognition security system. BBC. [Accessed 18 March 2019]. Available at: https://www.bbc.com/news/technology-39965545

Shanker, A & Rajagopalan, A. 2007. Off-line signature verification using DTW. Elsevier. [accessed 30 April 2019]. Available at: http://www.cin.ufpe.br/~in1129/projetos/Off-line%20signature%20verification%20using%20DTW.pdf

Shamsee, N. Klebenov, D. Fayed, H. Afrose, A & Karakok, O. 2015. CCNA Data Center DCICT 640-916: Official Cert Guide. Cisco

Shatner, W. 1982. Kirk undergoing a retinal scan.Star Trek II: The Wrath of Khan. [accessed 30 March 2019]. Available at: https://memory-alpha.fandom.com/wiki/Retinal_scan

Stephenson, P. 2016. Authentication. SC Magazine. 27(4). 38-39.

StepOver. 2019. signature pad duraSign Pad Brilliance. [accessed 30 March 2019]. Available at: https://www.stepover.com/fileadmin/_processed_/5/d/csm_Signature-pads-Signature-Pad-duraSign-Pad-Brilliance_790cfbaf59.png

Stern, J. 2017. iPhone X Review: Testing (and Tricking) FaceID. Wall Street Journal. Video. [accessed 30 March 2019]. Available at: https://www.youtube.com/watch?v=FhbMLmsCax0

Strickland, E. 2012. You're as Unique as the Veins in Your Hands. IEEE Spectrum. Video [Accessed 18 March 2018]. Available at:

https://spectrum.ieee.org/video/telecom/security/youre-as-unique-as-the-veins-in-your-hands

Slyter, S. 1995. Forensic Signature Examination. Springfield, Ill: Charles C Thomas. ILLinois. USA

The House of Commons of the United Kingdom. 2015. Current and future uses of biometric data and technologies. Sixth Report of Session 2014–15. [Accessed 15 March 2019]. Available at: https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf

Thompson, A. 2008. Your Odor: Unique as Fingerprint. Article [Accessed 15 March 2019]. Available at: https://www.livescience.com/5188-odor-unique-fingerprint.html

Three Basic Ridge Features. 2006. Classroom forensicsTM & Scientific Inquiry Fingerprint Ridge Authorities Lab. [Accessed 15 March 2019]. Available at: https://slideplayer.com/slide/10845114/

Tistarelli, M & Champod, C. 2017. Handbook of Biometrics for Forensic Science, Advances in Computer Vision and Pattren Recognition. Springer International Publishing. Cham, Switzerland

Tsitsiklis, J. 2010. Probabilistic Systems Analysis and Applied Probability. Massachusetts Institute of Technology. Video [accessed 30 April 2019]. Available at https://www.youtube.com/watch?v=IkbkEtOOC1Y

Types of biometrics. Biometrics Institute. [accessed 15 March 2019]. Available at https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

University of Cambridge. John Daugman. Blog [accessed 30 March 2019]. Available at: https://www.cl.cam.ac.uk/~jgd1000/history.html

University of Leicester. 9 September 2014. Interview with professor Sir Alec Jeffreys. Blog [Accessed 18 March 2019]. Available at: https://www2.le.ac.uk/news/blog/2014-archive-1/september/inventor-of-dna-fingerprinting-reflects-on-career-highlights-in-extensive-video-interview

U.S. National Library of Medicine. 12 March 2019. What is DNA?. Article [Accessed 15 March 2019]. available at: https://ghr.nlm.nih.gov/primer/basics/dna

Wertheim, K. 2011. Fingerprint Sourcebook-Chapter 3: Embryology, Physiology, and Morphology of Friction Ridge Skin. National Institute of Justice. [accessed 15 march 2019]. Available at: https://www.ncjrs.gov/pdffiles1/nij/225323.pdf

Yeung, D. Chang, H. Xiong, Y. George, S. Kashi, R. Matsumoto, T & Rigoll, G. 2004. SVC2004: First International Signature Verification Competition. The Hong Kong University of Science and Technology. [Accessed 9 April 2019]. Available at: https://www.cse.ust.hk/svc2004/icba2004paper.pdf

Yole Development. 2016. Global insights of the biometrics hardware market. [accessed 15 March 2019]. Available at: http://www.yole.fr/iso_album/illustration_biometrics_yole_dec_1.jpg

Zheng, Y. Li, H. Shen, W & Jian, J. 2018. Wearable electronic nose for human skin odor identification: A preliminary study. Elsevier. [accessed 30 March 2019]. Available at: https://www.sciencedirect.com/science/article/pii/S0924424718313827?via%3Dihub