BACHELOR INFORMATICA

UvA UNIVERSITEIT VAN AMSTERDAM

Biometric Authentication in MOOCs

Peter Bond

August 18, 2013

Supervisor(s): Toon Abcouwer (UvA)

Signed:

Contents

Abstract

Authentication of students' identity by Massive Open Online Courses (MOOCs) is a challenging task of which the answer might lie in the field of biometrics. This thesis reviews the potential application of various biometric methods to MOOCs in order to assist in user authentication (e.g. for granting credit points to students) as well as providing an introduction as to what MOOCs are. For this purpose, three biometric methods have been reviewed. Two of these are based on physiological features namely: fingerprint and face. The third method discussed is based on a behavioural feature, typing rhythm. These methods are assessed on a set of criteria and reviewed based on available literature which was acquired through a variety of queries using Google Scholar. Concluding, the biometric methods reviewed seem very interesting to apply to MOOCs, both on theoretical ground, as well as practical. Usage of all three reviewed biometric methods in conjunction is recommended, in which at least one method is to be used for continuous authorisation (fingerprint reading or typing rhythm). Future research could focus on the application of additional biometric or non-biometric (e.g. process monitoring) methods to MOOCs, either as a replacement or addition to the recommended biometric methods.

CHAPTER 1

Preface

This thesis will provide a literature overview of biometric methods which seem most appealing for application to Massive Open Online Courses (MOOCs). This overview then allows for recommendations for the application of biometrics to MOOCs based on characteristics as described in chapter *'Strength Weakness Assessment of Biometric Methods'*3. Finally, these recommendations are given at the end as well as conclusions.

Initially, a wide variety of biometrics was to be reviewed, this included: fingerprint, face, iris, retina, hand, palm, vein, thermal, typing rhythm, gait, voice and signature identification. However, this quickly proved to be an *extremely* optimistic task given the time constraints. Due to these time constraints, most were omitted. Eventually, after acquiring general knowledge on biometrics, the three which seemed most appealing were chosen to be reviewed and made it to the final version of this thesis. These three are: fingerprint, face and typing rhythm recognition.

Literature research was carried out by performing a variety of queries using Google Scholar. These queries mainly consisted out of a term being the biometric feature to be reviewed (e.g. fingerprint) coupled with the term 'biometric' and alike terms. Examples of queries are:

```
Fingerprint biometrics
Fingerprint biometric authentication
Fingerprint identification biometrics
Fingerprint reading biometrics
```

In addition, references of acquired literature were skimmed for additional relevant literature. Literature was found relevant if it provided information, criticism or experimental results on one or more of the biometric methods discussed.

Lastly, the author would like to express his gratitude to his supervisor drs. Toon Abcouwer for his valuable input during the entire process of authoring this thesis. Furthermore, the author would like to thank dr. Dick van Albada for providing constructive feedback on the final draft of this thesis.

CHAPTER 2

Massive Open Online Courses

1 Introduction

"An online phenomenon gathering momentum over the past two years or so, a MOOC integrates the connectivity of social networking, the facilitation of an acknowledged expert in a field of study, and a collection of freely accessible online resources. Perhaps most importantly, however, a MOOC builds on the active engagement of several hundred to several thousand 'students' who self-organize their participation according to learning goals, prior knowledge and skills, and common interests. Although it may share in some of the conventions of an ordinary course, such as a predefined timeline and weekly topics for consideration, a MOOC generally carries no fees, no prerequisites other than internet access and interest, no predefined expectations for participation, and no formal accreditation."[1]

The definition above broadly defines the basic principles behind Massive Open Online Courses (MOOCs). One can directly compare MOOCs with traditional courses as taughty by universities, since they are very much alike. However, three main distinctions should be made, which can be derived from the name itself:

1. *Open access:* students attending the course are not obligated to pay a fee, and literally anyone connected to the internet can participate, making it widely accessible.
2. *Massive attendance:* whereas a traditional course is taught to dozens, and sometimes hundreds of students, MOOCs' numbers are more often in the tens of thousands.
3. *Online education:* there is absolutely no physical interaction required between the students and the tutors, any information provided or exam taken, is done online. The student is taught at distance, making it a form of distance education.

The open access and online characteristics of MOOCs effectively remove most barriers from pursuing a course, which is the main cause for the massive attendance. Users can register freely for a MOOC and enroll in a course, which provides the user with all necessary course materials.

A welcome addition to MOOCs would be the granting of credit points to the students. For the credit points to be of any value, the student enrolled in the course and granted the credit points should be the same as the student completing the course exam(s). This problem of user authentication lies at the heart of this thesis: how can a MOOC authenticate the student taking the course as being the rightful student? A valuable tool for (digital) user authentication can be found in the field of biometrics, namely: biometric identification. Biometric identification refers to identifying an individual based on his or her distinguishing physiological and/or behavioral characteristics (biometric identifiers/biometric features) [33]. A typical example of biometric identification based on a physiological characteristic is facial recognition. An example based on a behavioural characteristic would be typing rhythm recognition.

2 History

A long pathway of technical evolution eventually led to the emergence of MOOCs. The first form of distance education can be traced back to 1840, in England. Isaac Pitman, whom was a teacher, provided course materials to aid in business administration [48]. This type of distance education is termed correspondence study, which refers to the non-concurrent nature of postal communication. In later years, correspondence study took off, and in the late 19th century was common among universities.

With the upswing of computer technology, multimedia devices were eventually used for distance learning. Education could be served on CD-ROMs to interact with on a computer, or be broadcast on television or radio with the use of a videocasette or audio cassette respectively. In 1999, the University of Tübingen, Germany, started the first so called 'OpenCourseWare' (OCW) [49]. OCW refers to course lessons created at universities which are published freely on the internet. However, although bidirectional communication was technically possible, it was not directly applied to distance education yet. The Massachusetts Institute of Technology (MIT) followed with their MIT OpenCourseWare in 2002. MIT being one of the worlds' top universities, this really lit the fire for OCW.

Not much later, MOOCs arose, also supporting bidirectional communication through discussion forums.

3 Existing MOOCs

Since the first MOOC originated somewhere around 2008, a variety of MOOCs popped up. A lot of universities started their own individual MOOCs. In March 2013, the University of Amsterdam also launched its own MOOC [56].

However, collaborative MOOCs, in which multiple universities cooperate to offer courses, are currently the leading MOOCs on the internet. With Coursera, edX and Udacity being among the biggest players.

Figure 2.1: The three major players in collaborative MOOCs: Coursera, edX and Udacity.

Coursera was founded in April 2012 by two computer science professors (Andrew Ng and Daphne Koller) from Stanford University. Coursera offers over 300 courses provided by over 50 universities world wide. Recently, the Dutch university of Leiden also offers a course on Coursera. According to Coursera's blog[5], they had over 3.2 million users as of April 2013.

edX was also launched in April 2012. The platform is an initiative of Massachusetts Institute of Technology and Harvard University. edX offers around 50 courses provided by 12 universities world wide, including the Dutch university Technische Universiteit Delft.

Udacity launched in February 2012, and evolved out of a Stanford University experiment offering an Artificial Intelligence course online which became highly popular.

Currently, only Coursera applies biometrics for user authentication in their so called 'Signature Tracks'. Coursera applies facial and typing rhythm recognition [6]. First, a user is required to enroll in the signature track. To enroll, the student needs to provide a photo of an ID document, as well as a headshot. Second, the student needs to type a short sentence, to create his or her 'signature profile typing pattern'. Coursera then verifies the students' identity. After verification the photo of the ID document will be deleted, and the headshot can then be used for verification, together with the typing rhythm. The combination of both these biometric features should allow for a reliable verification process.

CHAPTER 3

Strength Weakness Assessment of Biometric Methods

There is no silver bullet in the field of biometrics. Every biometric method has its own weaknesses as well as its strengths. In addition, the value one might attribute to their strengths and weaknesses is dependent on their application. For example, real-time processing might be an irrelevant strength of a biometric method when it is not required real-time and processing can be done at a later stage.

When we want to assess the relevance of a biometric method to its goal (the application), we can evaluate certain aspects of the biometric method to do so. By evaluating their accuracy, speed, ease of use (usability), storage and cost properties, we can come to an educated decision for their application to MOOCs.

First, accuracy can be defined as a point at which, at a given relative operating characteristic (ROC), both the False Match Rate (FMR) and (FNR) are acceptable. I.e. there is a settable threshold at which the risk of an imposter being validated as legitimate, as well as the risk of a legitimate person being rejected, are found acceptable. The FMR describes the rate at which an imposter is mistakenly being recognized and accepted. The FNR describes the rate at which an individual is mistakenly being rejected. For application to MOOCs the aim should be to keep the FMR as low as possible, while maintaining a comfortable FNR.

Second, speed can be defined as the time required for the biometric method to return a result after the user has presented the requested biometric characteristic to the sensor. For certain applications real-time processing is irrelevant, however for the application to MOOCs it might be necessary for the biometric application to make a decision in near-real-time, e.g. when it is used for continuous evaluation. Furthermore, it should be taken into account that the biometric sensor and the biometric application are remote of each other, processing takes place on a remote site and is dependent on an internet connection. Big chunks of data can seriously delay the transfer time, and thus slow down the biometric application. Proper compression of the data, without significantly affecting the performance of the biometric application, is important.

Third, ease of use is quite self-explanatory. The biometric application should be easy to handle, and should be acceptable to use. For example, a student should not need to perform difficult tasks to authenticate himself during an exam in the case of continuous evaluation.

Fourth, storage can be defined as the format in which the biometric features are being stored, digital size, which compression is used, and where it is stored. In the case of MOOCs care should be taken to reduce the digital size, since transfer takes place through an internet connection between the client and a remote server. Compression directly affects speed: it takes time to compress, and the compressed result reduces size and thus transfer time. In any case compression should net result in a time reduction. However, with the enormous storage capacity and high-speed internet connections these days, storage hardly seems to be of any concern in general. Luckily, MOOCs are readily built to handle large amounts of internet traffic.

Fifth, cost can be viewed from the client perspective (does the client need to acquire an expensive biometric sensor?), and the provider (does the provider need to allocate a lot of resources to let the biometric application perform well? E.g. programmers, hardware requirements).

In general, these properties are not equally important. Accuracy is a highly important feature to minimize the FNR, however in a system in which multiple biometric methods are used, accuracy of complementary methods is of less relevance. Furthermore, when the biometric method is applied continuously and requires (near-)real-time decisions, speed is very important (in which case speed is also inherently linked to storage). Moreover, cost is of moderate importance, but mainly do the requirement of additional hardware per se, as most biometric sensors are affordable. Finally, these five properties allow for a systematic approach of reviewing biometrics methods.

CHAPTER 4

Biometrics

1 Introduction

Biometrics involve the utilization of automated methods to authenticate or recognize a person based on its physiological and/or behavioural traits. The inclusion of automated to this definition is necessary to distinguish it from other identification methods, e.g. a forensic specialist attempting to identify someone by his fingerprint with the use of a magnifying glass, which does not fall in the scope of biometrics. The term biometrics in this context should not be mistaken with biometrics as used in biology, which refers to utilization of statistical data in the field of biology. Luckily however, this is more often referred to as biostatistics, which circumvents any confusion. Application of a biometric method can be subdivided into two phases: enrollment phase and identification phase. The enrollment phase involves the creation of a biometric pattern of a person, which can then later be used to identify the person in the identification phase. This biometric pattern created in the enrollment phase is termed a biometric template. The identification phase is used to either identify a user with his template, or to determine that the person is not stored in the template database, and thus is unknown to the system. The system therefore tests one of two possibilities: the user is either known to the system (positive identification), and thus enrolled, or the user is not known to the system (negative identification), and thus not enrolled.

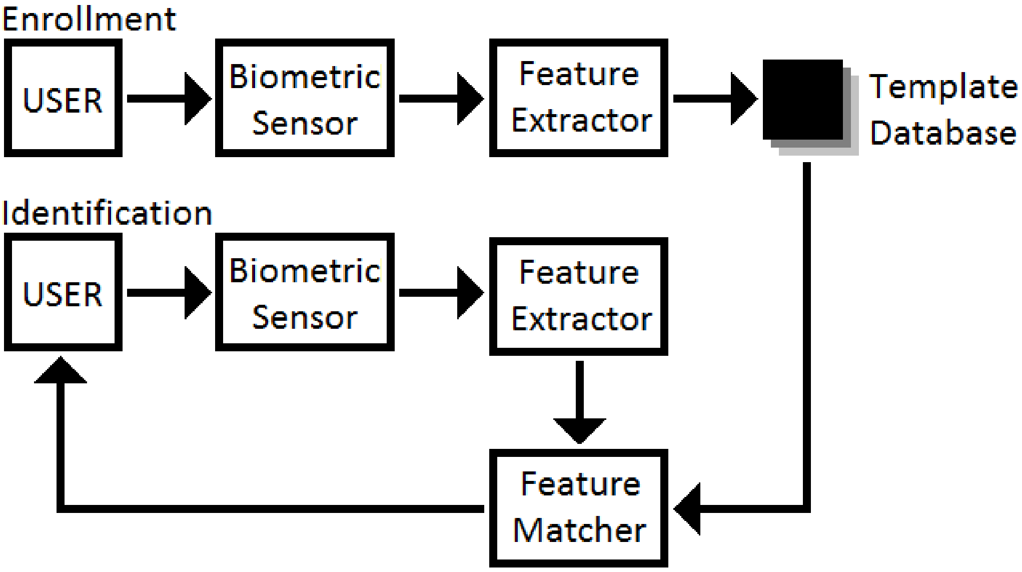

Figure 4.1: A generic biometric system. Figure based on Jain et al. [33].

In the context of MOOCs we are interested in a positive identification system, since we would like to authenticate an individual. A one-on-one comparison with a submitted sample and a stored template is made to achieve this. This process of identification can be subdivided into four stages: segmentation, feature extraction, quality control and pattern matching. Segmentation extracts the required biometric pattern from a given sample. E.g. it extracts the face from a picture for facial recognition (face localization), removing the background and anything not part of the face. This result is then used to extract features. The feature extractor removes any additional irrelevant features which can be the result of the biometric characteristic presentation, sensor and transmission. The distinctive qualities remain. The quality control then validates if these distinctive qualities make sense within the context of the biometric method used. If they are either of poor quality (or the amount of features is low), or totally unrelated to the biometric characteristic being verified, the sample is rejected. Some biometric systems apply quality control even before feature extraction is initiated, saving resources. When the sample has passed the quality control, it goes through pattern matching. It matches the distinctive qualities with a stored template, and calculates the quantitative distance between the two. Based on this quantitative distance, the system can either choose to reject, or accept the sample and can be set to a certain threshold. This threshold directly influences the FNR and FMR as they are dependently related.

Depending on the biometric method used, the techniques to walk through these steps can vary extensively, although in essence they do the same. E.g. the segmentation process of a facial sample (image) differs extremely from the segmentation of a voice sample (audio), but both strive to extract the required biometric pattern from a given sample. In addition, although the techniques used influence the reliability of the biometric method, in principle the biggest determinant of reliability remains the physiological or behavioural trait (the biometric characteristic) which is used.

If we would examine which biometric characteristic is 'best', we can look at five qualities: robustness, distinctiveness, availability, accessibility and acceptability [30]. Robustness refers to the change of the characteristic over time, ideally, the characteristic does not change at all. Indeed, if a characteristic were to change much, we can not verify it with the stored template. Distinctiveness refers to how 'unique' the characteristic is, i.e. no two people should share exactly the same characteristic. Availability refers to how many people actually express the characteristic. It would be rather impractical to utilize a biometric system based upon a characteristic which a significant amount of people do not have, thus making it impossible for them to enroll in the system. Accessible refers to how easy (or hard) it is to obtain the characteristic in a workable format. If a biometric system can not obtain the characteristic it, of course, can not function. The final characteristic, acceptability, refers to the objection people might have on 'sharing' the characteristic with the system.

2 History

Identifying a person based on physiological characteristics by quantitative measurements has long been identified. It was back in the late 19th century that Bertillon developed "Bertillonage", which identified an individual based on his or her body measurements [51]. Although fingerprints were being used before for identification, it lacked a classification system. It was only in 1892 until a classification system for fingerprint identification was developed [52]. However, it required the development of computative systems to automatize the process of identification, and thus give rise to biometrics. The development of digital signal processing techniques in the 1960s gave a push towards the automatization of person identification. Any potential of these methods was also rapidly recognized, leading to interest of governments.

In the 1960s the FBI pushed to automatize the process of fingerprint identification and in the 1970s the system was operational. Around the same period, the French Paris Police, the British Home Office and the Japanese National Police were also automatizing the process [53].

The first voice recognition system found its way in 1976, developed by Haberman and Fejfar [54]. In 1991 face recognition took off when an approach was proposed which significantly speeded up the process, making near-real-time face recognition possible [55]. Not much later, in 1993, the Face Recognition Technology (FERET) program was initiated, providing a large database, as well as a methodology to benchmark face recognition methods [45].

An extensive report, written by the NSTC Subcommittee on Biometrics, evaluating the history of biometrics by means of a timeline, can be found in reference [57].

3 Digital Authentication Problem

The biggest problem facing biometric methods in general, and especially in the case of applications wherein imposters can absolutely not be tolerated such as in high security systems, is the false match rate (FMR). The FMR describes the rate at which an imposter is mistakenly being accepted as valid. Since we would not want to have an imposter being accepted as valid with a MOOC, the goal is to reduce the FMR as much as possible. However, there is a trade-off between the FMR and the false non-match rate (FNR) as mentioned earlier, relying on the set threshold. The FNR describes the rate at which a valid individual is mistakenly being rejected as being invalid. Although a false non-match is not as bad as a false match, it does decrease comfortability of the system for the end-user. In fact, if the FNR is high enough, it is practically impossible for an individual to authenticate himself, thus the system fails its goal in the first place, namely authenticating a person. Therefore a biometric system should aspire a compromise between the FMR and the FNR, in which both are acceptable. Unfortunately, this is not always an easy task to accomplish.

Since the FMR and FNR are directly related depending on the threshold applied, researchers often report the equal error rate (EER) of a biometric system. The EER is the rate at which the FMR and FNR are equal, and thus providing a number to compare different biometric systems. The trade-off between the FMR and FNR is depicted in Figure 4.2.

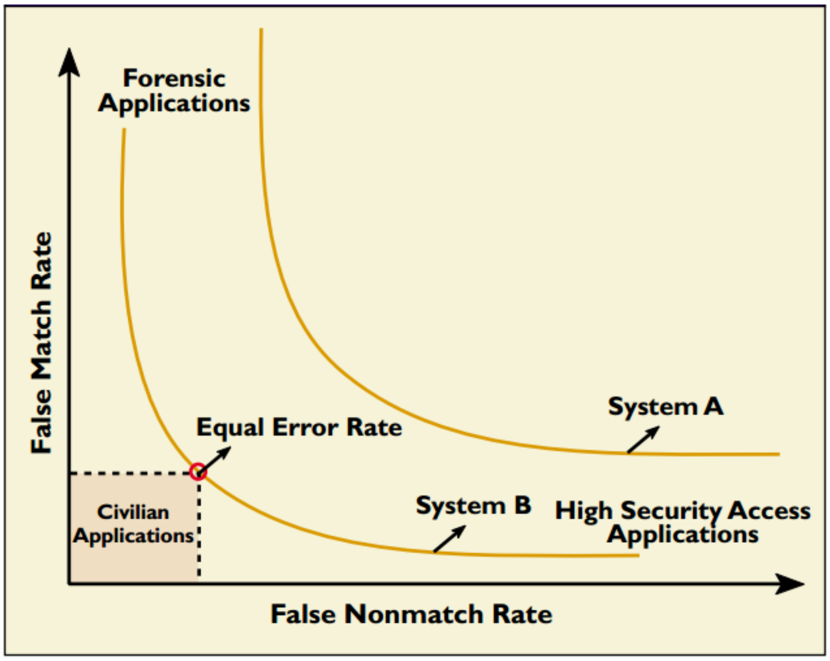

Figure 4.2: Illustration of the trade-off between the FMR and FNR. A smaller FNR usually leads to a higher FMR and vice versa. As can be seen, multiple Pareto optimal points exist. The EER is commonly the reported Pareto optimal point in literature. Figure adapted from Jain et al. [33].

4 Current Applications

Biometrics are widely employed as an addition, or full replacement, of traditional token authentication systems. Token authentication systems are based on something the individual either knows or has (e.g. a USB stick with a security token). However, these tokens are not inherent to an individual himself, it can in principal be freely exchanged to others (e.g. a USB stick can be given to someone else), thus distinguishing it from biometric traits which are inherent to an individual.

It is safe to assume that nearly all individuals (either forced or voluntarily) use a biometric system at least once in their lifes. They are employed by airports, e.g. Schiphol airport in the Netherlands which applies iris scans for checking-in rapidly [40]. Biometrics are also utilized by government agencies, e.g. the Dutch Dienst Justitiële Inrichtingen, which applies biometric systems to ensure that legal judgements are being fulfilled [4], such as a prison sentence.

Furthermore, the Unique Identification Authority of India (UIDAI) are collecting finger prints and iris scans of all Indian residents to create a database of biometric data, the AADHAAR program. The project had a resident enrollment database size of 84 million on the 31st of December 2011 [41]. The reported FMR and FNR are 0.057% and 0.035% respectively.

Forensics have applied biometrics for decades to identify suspects, most commonly by means of fingerprint identification. In fact, most of the advances in fingerprint identification originated in the field of forensics. Law agencies, such as the FBI, were struggling with an ever increasing archive of fingerprints and this sparked interest to automatize the process.

Even social media, most notably Facebook, are applying biometrics. Facebook first rolled out face detection, which suggests tags on photos, so a user can link names to it. However, not much later Facebook started suggesting names for these tags, hence utilizing actual face recognition to identify individuals based on photos which were already tagged with names by their users.

Moreover, something similar to Facebook's face recognition is being applied by Picasa Web Albums, an online web service provided by Google. The service allows users to share their photos with friends and family and now provides name suggestions, through appliance of face recognition algorithms, for faces displayed on photos.

5 Biometric Features and Their Methods

5.1 Fingerprint

Fingerprints are a unique physiological feature exhibited by all human beings with fingers (it is even common among mammals). The development of fingerprints starts during the 10th week of pregnancy and appears to be the result of a buckling instability in the basal cell layer (stratum basale) of the fetal epidermis as proposed by Kücken and Newell (2004) [2]. To elucidate this: The skin can be subdivided into two main layers: epidermis and dermis. The dermis lies underneath the epidermis and the two are separated by a basement membrane. Whereas the epidermis mainly serves as a protection against the external environment, the dermis mainly serves as a supportive structure and is primarily composed out of fibrous tissue. Furthermore, it is responsible for over 90% of the mass of the skin. The epidermis can be further subdivided into several layers, called strata. These strata are, in outermost to innermost order: stratum corneum, stratum granulosum, stratum spinosum, stratum basale. In addition, certain regions of skin also express the stratum lucidum, which can be found between the stratum corneum and stratum granulosum. The epidermal layers are depicted in Figure 4.3.

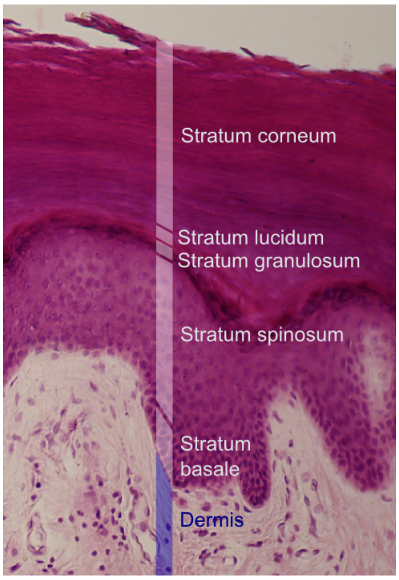

Figure 4.3: Histological image of human epidermal layers.

It is the innermost stratum (stratum basale) of the epidermis where fingerprints originate. Since all strata on top of the stratum basale also differentiate from the stratum basale, fingerprints are well conserved. Only damage to this innermost stratum of the epidermis would permanently alter a fingerprint (e.g. due to the formation of scar tissue).

When we look at our fingerprints we can detect certain repeating patterns. These basic patterns are used for biometric identification. The most common patterns are: whorl, loop and arch. These patterns are shown in Figure 4.4. One could name these three basic patterns the fundamentals of a fingerprint. In addition, there are certain details which heavily contribute to the uniqueness of fingerprints, these details are called minutiae. Minutiae are abnormalities among the ridges. Two commonly used minutiae in fingerprint recognition are the ridge endings (the abrupt end of a ridge) and the ridge bifurcation (a ridge which splits into two, resulting in a Y-shape).

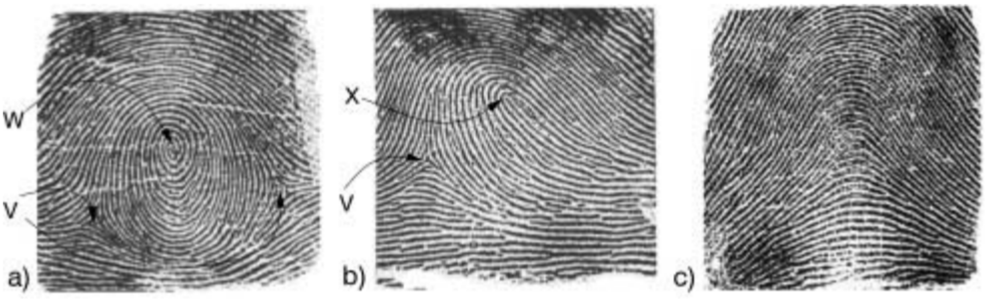

Figure 4.4: Common fingerprint patterns: a) whorl, b) loop, c) arch. A Whorl is characterizied by a target/spiral (v) and two triradii (v, v), loops by a Roman arch structure (x) and one triradius (v). Adapted from Kücken and Newell [2].

Since the ridge structure directly influences the performance of a biometric method employing it, it is of major importance that the ridge structure is as clear as possible. Therefore, a variety of algorithms have been developed to enhance the ridge structure. One such algorithm normalizes the intensity variation, this is called Local Area Contrast Enhancement (LACE). If one were to plot out a grayscale histogram of a raw fingerprint, a very heterogeneous distribution comes to light. By applying LACE, the distribution becomes homogeneous, making the ridges a lot clearer. One such method of LACE is provided by [3], in which first a global pixel mean ($GlobalMean$) is calculated for the image, after which a local mean and variance for a specified neighbourhood is calculated for each pixel. First we can calculate the $GlobalGain$ as follows:

$$GlobalGain = GlobalCorrection \cdot GlobalMean$$

Then we can calculate the $PixelGain$ as follows:

$$PixelGain = GlobalGain \frac{1}{\sqrt{LocalVariance}}$$

Now we can calculate a new intensity for every pixel as follows:

$$NewIntensity = PixelGain(RawPixel - LocalMean) + LocalMean$$

The result now is, when drawn a histogram showing the grayscale of the image, that the full grayscale spectrum of 0 to 255 is used. This is just one of the ways to enhance fingerprints, making their features more applicable to extract. In essence, these algorithms strive to maximally enhance the captured ridges, and suppress any abnormalities which are not part of ones fingerprint, and thus could lead to invalid features.

After enhancement, the features can be extracted and processed. The algorithms which process the features can be roughly divided into two categories: minutiae based and correlation based [31]. In general, minutiae based algorithms perform better than correlation based.

The accuracy of fingerprint recognition is extremely precise. Contrary to most biometric systems (in particular behavioural), zeroFMRs are often published. ZeroFMR is the point at which no false matches occur with the lowest FNR. A paper published in 2004 by Maio et al. on the third Fingerprint Verification Competition reports results of algorithms scoring an avarage zeroFMR as low as 6.21% [32]. A very acceptable score for authentication purposes. However, although fingerprint recognition is highly attractive from nearly all perspectives for the purpose of user authentication, one potential drawback is that it requires additional hardware, and thus costs for the student. Nevertheless, reliable commercially available fingerprint readers, such as used by Maio et al. (e.g. Digital Persona U.are.U 4000), are available for less than €100. The price of the additional hardware therefore does not seem to be a major drawback, but the requirement of additional hardware per se.

5.2 Face

Faces exhibit a wide variety of features which can be exploited to verify an individual's identity, thus face authentication is based on a physiological trait; utilizing an individuals' facial appearance for authentication purposes. While humans can identify other faces nearly without effort, automatizing the process has proven extremely difficult. Indeed, humans can identify faces with ease even when provided facial images with significant loss of quality as illustrated by Figure 4.5. However, it is reported that some face recognition algorithms are more accurate than humans in identifying faces using frontal images under different illuminations [42]. Note however, that this does not imply that face recognition algorithms have surpassed humans beings in practice. These results were obtained under specific conditions and therefore do not translate to practical situations. In addition, these results concerned identification (a one to many comparison), in which computers have a big advantage compared to humans, since humans can not accurately remember and identify an individual out of thousands of people. Nevertheless, these results are impressive.

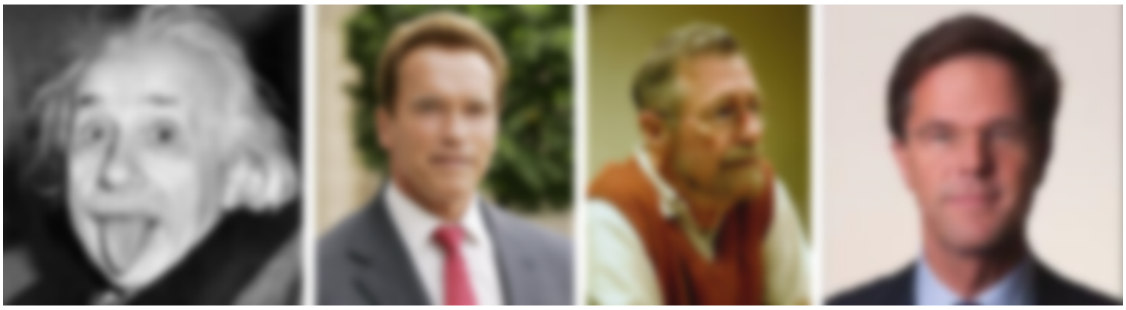

Figure 4.5: From left to right: Albert Einstein, Arnold Alois Schwarzenegger, Edsger Wybe Dijkstra and Mark Rutte. Inspired by Sinha et al. [34].

Considering the ease with which humans identify faces, it is important to understand how we do this, in order to apply it to computational algorithms. However, this will not be covered as it is beyond the scope of this thesis, the reader is therefore referred to a paper written by Sinha et al., which extensively evaluates this, named: 'Face Recognition by Humans: Nineteen Results All Computer Vision Researchers Should Know About' [34].

When a picture of a face is presented to a face recognition system, the initial step it performs is the extraction of the face from the background (face localization). This is commonly done by locating the eyes, after which the image is positioned, scaled and rotated so that the eyes match a certain position, in order to effectively compare two images, and hence recognition [35]. Beyond this geometric localization preprocessing, additional steps are usually taken to further enhance the face in the image, e.g. by removing pixels that are not in the oval shape of the face. Furthermore, the process of normalization is another important step in the process. For example illumination normalization, since (direction of) lighting can significantly alter pixel values, and thus ultimately impede the process of identification. Indeed, the FRVT 2002 reports that face recognition systems perform significantly better with indoor illumination as compared to outdoor illumination [36], emphasizing the influence of illumination on performance. A commonly applied technique for illumination normalization is Self Quotient Image (SQI) preprocessing [43], wherein the SQI is produced by calculating the ratio of the albedo of every pixel to a smoothed albedo value of local pixels, and thus resulting in a illumination invariant representation of a face [44].

Ultimately, these preprocessing steps are as important as the actual face recognition algorithm itself, and finds application to more fields than just identification and verification (e.g. facial expression analysis). Therefore face localization is important for many research fields and thus has attracted a tremendous amount of researchers from various disciplines. As a matter of fact, there have been literally hundreds of approaches to face localization [37]. Yang et al. categorizes the various approaches into four categories: knowledge-based methods, feature invariant approaches, template matching methods and appearance-based methods [38]. Of these four categories, appearance-based methods usually perform best. In particular one may note the Viola-Jones Face Detector [39], which was adopted and enhanced by many other researchers (as of writing this thesis, the original paper is cited nearly 8000 times) and had a tremendous impact on the field due to its very fast performance while still achieving high detection accuracy.

After face localization and normalization the features are extracted. These consists of both geometric as well as photometric features. Furthermore, these features can be categorized as being local (e.g. fiducial marker) or being inherent to a face (e.g. mouth). Methods to extract these features range from linear classifiers (e.g. principal component analysis) to kernel methods, generalized linear discriminants and SVMs [35].

The field of face recognition has established several database of faces and testing procedures to benchmark algorithms, contrary to the field of typing rhythm as discussed later. This allows a quantitative comparison of performance of these algorithms in literature. One of these databases is the the Face Recognition Technology (FERET) database, which includes over 14.126 images from 1199 individuals, which is divided into development and sequestered portions [45]. However, this database only includes full-frontal images. Another commonly used database is the CMU-PIE database, in which photos are taken from 13 different angles as well as with 43 different illuminations and with four expressions [46]. The setup used for these photos can be seen in Figure 4.6.

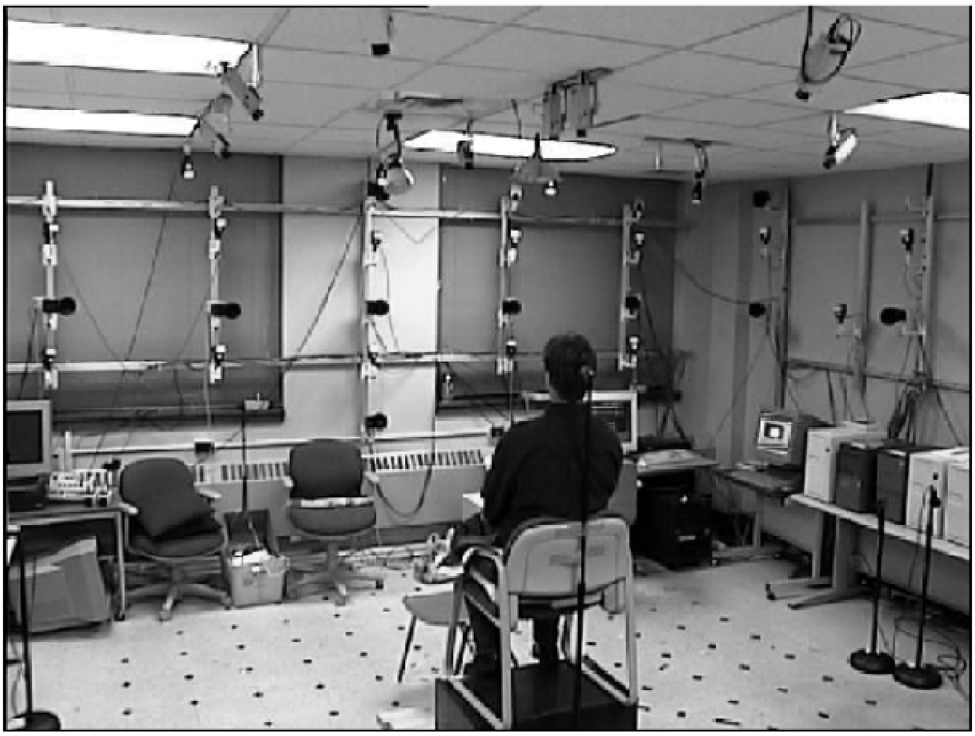

Figure 4.6: Setup of 13 cameras and 21 flashes used in the CMU 3D room [46].

Since so many researchers have approached face recognition from different perspectives as well as with different purposes, evaluating the accuracy of the different algorithms is a challenging task. Nevertheless, when we look at the chart provided by Introna and Nissenbaum in Figure 4.7 we can clearly see that face recognition has come a long way and one might interpret the figure as face recognition reaching maturity, and thus being a reliable biometric method [47]. In FRVT 2006, a FMR of 0,1% was reported with a FNR of 1%.

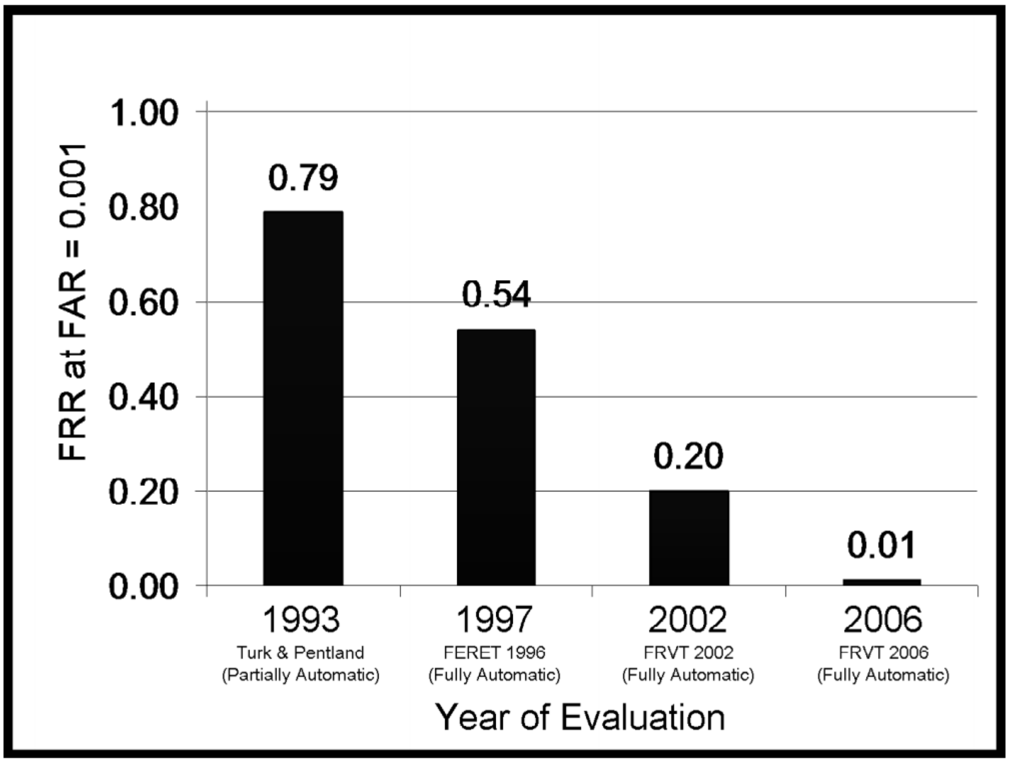

Figure 4.7: Comparative results of evaluations from 1993-2006 [47].

However, the figure should be interpreted with caution as the conditions were heterogeneous among these benchmarks, e.g. the database used in FRVT 2006 came with higher quality images than used in FRVT 2002. As FRT expert Jim Wayman justly notes, *"The test gives us little predictive information about the performance of current facial recognition algorithms in real-world immigration environments"*. Introna and Nissenbaum further review the results in great detail [47], and concluding it seems face recognition is not entirely ready yet to be solely used as a biometric authentication method. Nevertheless, it seems as a viable option as an addition to other biometric methods.

Although in principle it is right to state that additional hardware is required, in practice most laptops are already fitted with a proper webcam and a lot of users have standalone webcams. Therefore the requirement of additional hardware is limited to a subset of users. Moreover, webcams are readily affordable.

5.3 Typing Rhythm

Typing rhythm, also known as keystroke dynamics in literature, utilizes the typing behaviour of an individual as a biometric. This typing behaviour provides certain features to do so, the most common being the latencies which can be derived from keystrokes. In addition, pressure applied to keys as well as typing speed can be used as features. However, using the pressure applied to keys as a feature is not as practical as the others, since it requires special keyboards which can measure pressure applied.

In 1975, Spillane was the first to propose typing rhythm for user identification [21]. Not much later, in 1978, Shaffer demonstrated typing to be a motor programmed skill [8]. Typing characters at the beginning of a word was affected by both the previous words, as well as the continuation of that word. The effect could be explained by knowledge of the movement transitions required. This implies that the movement transitions are processed preceding actual physical movement. Being a motor programmed skill, typing rhythm undoubtedly is a behavioural biometric. In addition, the National Science Foundation and the National Bureau of Standards in the United States conducted studies establishing that typing patterns contain unique characteristics that can be identified [20]. Therefore, lending itself for biometric identification purposes.

Due to the nature of the biometric, the hardware necessary for a student to apply is readily available if pressure applied is excluded as a feature. Therefore, any typing rhythm biometric method applied in MOOCs should primarily be based on latencies, excluding the pressure data. Latencies commonly used for feature extraction are: press-to-press (PP)[1], release-to-release (RR)[2], release-to-press (RP), hold time[3], and trigraph. A visual representation of these latencies can be seen in Figure 4.8.

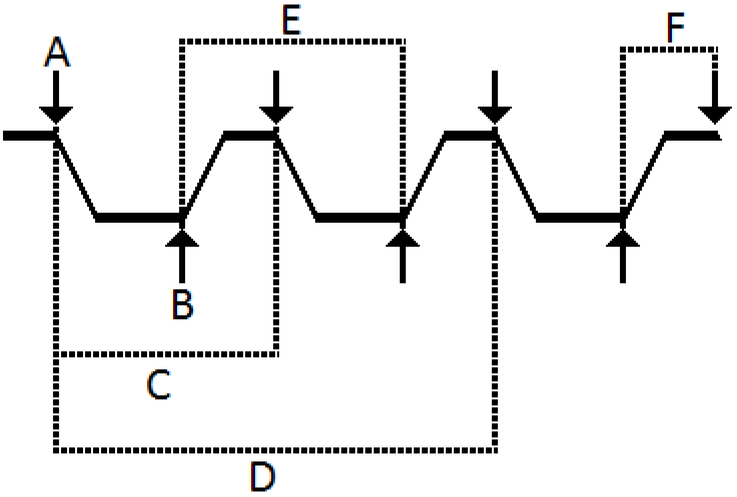

Figure 4.8: Key latencies: A) Key down, B) Key up, C) Press-to-press also known as digraph, D) trigraph, E) Release-to-release also known as flight time, F) Hold time also known as dwell time.

These latencies can then be used for analysis of ones typing rhythm, and thus authorisation or identification. In essence, there are two types of analysis possible to apply: static analysis and dynamic analysis. The former is based on typing samples of predetermined text, creating a template which will then be used for authentication. When the user attempts to authenticate, he will be requested to provide the same text, which can then be used to match with the template created in the enrollment phase. However, this poses a problem which all static methods have in

---

[1] Also commonly named digraph in literature.

[2] Also commonly named flight time in literature.

[3] Also commonly named dwell time in literature.

common. Bours and Barghouthi describe this problem as follows: *"They authenticate the user at the moment that the authentication mechanism is executed: any change of user after that will be unnoticeable to the system."* [7]. In the context of MOOCs this is a very important aspect, since a student could authenticate himself, after which someone else can pretend to be him. Since the system is static this would go undetected. However, this problem is not limited to typing rhythm methods, yet it is easy to apply continuous evaluation with it.

Dynamic typing rhythm analysis therefore seems to offer an attractive solution to this problem: it continuously evaluates if the user is legitimate. In addition to the check when a user logs in (as in static analysis), analysis continues during the entire operation. Furthermore, instead of looking at fixed texts and their corresponding individual latencies and keystrokes, it looks at timing information on specific keys and key combinations. Making it independent of any fixed text, hence making it dynamic. Since a keyboard is continuously used during the use of a computer, there is no extra burden on the user using such a method.

Ultimately, typing rhythm algorithms can be approached in different ways. The most commonly used techniques are either based on: statistical algorithms, neural networks, pattern recognition and learning based algorithms, or search heuristics.

Statistical algorithms apply, as their name suggests, statistical methods on the extracted features. These methods include: mean[11][9], variance[10], standard deviation[11][12], hypothesis tests (e.g. t-test[13]), distance measures (e.g. Euclidean distance[14], Manhattan distance[15], Mahalanobis distance[16][17]), and so on.

Neural networks are computing models inspired by biological nervous systems. Whereas biological nervous systems operate through an enormous amount of neurons, analogously neural networks apply interconnected nodes. These nodes are connected and have assigned weights, unlike statistical algorithms, these algorithms are adaptive. They can learn through either supervised or unsupervised learning. A variety of researchers have applied neural networks to typing rhythm with varying results. Brown and Rogers applied an ADALINE algorithm which scored an 17.4% error rate on FNR (0% FMR) [22], which is an unacceptable high FNR due to obvious reasons. As the techniques were set up to force an FMR of 0%, no EER was reported. Ahmed et al. however, managed an 0.0152% FMR (4.82% FNR)[23] applying a neural network, no EER was reported. Such results are encouraging and were obtained over a period of 9 weeks, collecting an average of 119979 digraphs per user, among 21 participants. The drawback of neural networks however, is that they tend to be slow, since they require a lot of iterations in their learning phase, to come to the desired output.

Pattern recognition classifies patterns into categories or classes which can be done by a variety of algorithms. These algorithms are roughly based on two types of classifiers: linear classifiers (e.g. Perceptron algorithm) and non-linear classifiers (e.g. Support Vector Machine [SVM]). Sang et al. applied a one-class SVM resulting in an FMR of 2% and a FNR of 10%, the two-class SVM yielded an FMR of 10% with equal FNR and thus having an EER of 10% [24]. Unfortunately, an EER was not provided for the one-class SVM and could not be derived from the given data. An approach by Zhong et al. resulted in an EER of 8.4%, unfortunately the authors did not report the FMR and FNR [18]. Zhong et al. used the nearest neighbour classifier with a newly proposed distance metric to achieve these results, in addition they removed outliers (EER 8.7% excl. outlier removal).

Search heuristics attempt to quickly find a good solution, which is not necessarily the most optimal. A great advantage of these algorithms is that they can handle large amounts of data relatively easy. However, this is mostly important for identification purposes and not for authentication purposes as potentially applied in MOOCs. Research in the field of search heuristics applied to typing rhythm is relatively scarce. Nevertheless, the results thus far at least seem promising. Revett reports an FMR of only 0.1% with equal FNR applying bioinformatics (utilizing genetic algorithm and global alignment algorithm) [25].

Unfortunately it is difficult to directly compare the various results as reported in the literature as there is no standard procedure of collecting results. There is a strong need for a standardized database to evaluate typing rhythm in the future. A small amount of researchers have already made some databases publicly available [26][27][28][29]. However, all databases contain only a small number of samples. Furthermore, only the database published by Jugurta et al. contains dynamic text [26]. Moreover, this database unfortunately is the smallest database to date with an extremely small sample size (150). Therefore, there is a high need for a large standardized database in the field of typing rhythm, providing both static and dynamic texts.

Concluding typing rhythm seems a very viable approach to authenticate users both in a static, as well as a dynamic (i.e. continuous) manner. However, although the EER provided by the best algorithms is relatively low, caution should be taken when applying these to MOOCs. Due to the massive attendance a MOOC might attract, it is nearly a statistical inevitability that false matches will occur. Combining with other biometric methods is recommended. In addition, it is unknown how the results of these trials translate to practical situations, as no standardized database is used, and trials usually occur under controlled conditions. Furthermore, long-term studies of the evolution of a persons typing rhythm characteristics over prolonged periods of time is lacking. Direct clinical data on robustness thus is unknown. Therefore it is unknown if this biometric can lead to inconvenience over time due to a higher FNR, as a result of potential changing of an individuals' typing rhythm over time. This might be circumvented by periodically updating the biometric typing rhythm template of the user automatically or manually by re-rolling.

CHAPTER 5

Findings and Recommendations

Three interesting biometric methods for application to MOOCs have been reviewed, of which two based on physiological traits (fingerprint and face), and one based on a behavioural trait (typing rhythm).

Fingerprint reading is very attractive as the biometric feature itself scores very well on nearly all points. Fingerprints are very robust as only damage to the innermost stratus of the epidermis would permanently alter a fingerprint. Furthermore, they are unique for every individual and are therefore extremely distinct, even identical twins have unique fingerprints which can be successfully distinguished by fingerprint reading [50]. And due to the nature of the biometric feature, it is readily available to anyone who still has at least one finger left, moreover the index of an individual's finger is highly accessible as well. However, in general fingerprints are experienced as being privacy sensitive, probably due to their ultimate uniqueness, therefore scoring fair on acceptability. When we look at the methods utilizing fingerprints for authentication purposes it further adds to the attractiveness the feature itself already has. The methods used are, as reviewed, highly accurate and very easy to use. Furthermore, in the past the automation process was heavily focused on a one-to-many comparison in which a fingerprint was matched against a database of millions: a one-on-one comparison is therefore extremely fast in terms of speed. Storage is for analogous reasons very applicable as well. The only drawback seems to be the requirement of additional hardware, not so much due to costs as reliable fingerprint readers are very affordable as reviewed, but due to the requirement of additional hardware per se. Next to the fair acceptability character as experienced by users, this makes it less attractive. However, due to the ease with which a fingerprint is read, this biometric lends itself for continuous authentication by requiring a fingerprint read e.g. randomly or repeatedly with a certain time interval.

Face recognition is somewhat less attractive compared to fingerprint reading when looking at the features of the biometric itself. It is moderately robust, as several factors can influence facial appearance, e.g. ageing, weight gain/loss, disease, illumination, expression and angle. However, most of these factors can be, at least partly, ruled out by properly instructing users when enrolling. E.g. requiring: neutral expression, full-front view and uniform lighting. In addition, the feature seems very distinct as witnessed by the low FMR reported earlier, nevertheless, identical twins share an extreme commonality among facial appearance. It should however be kept in mind that this very same problem applies to real life situations in which exams are taken. The feature is highly available and accessible. When we look at the methods utilizing face recognition for authentication purposes however, it is clear that it can not function as the sole biometric method in any system with many users. The accuracy varies in literature, an although some established big databases and methodologies are available for benchmarking, the translation to real-life situations seems not entirely predictable, due to the high variety compared to the controlled conditions in which these databases are created. Nevertheless the biometric method scores great on speed whilst maintaining high accuracy, as well as being very easy to use (an individual only has to look into a camera). Although scoring a relatively well FNR, continuous authentication can be found disturbing when the webcam is inappropriately placed, which could disturb an individual's concentration when authorisation is required (since the head needs to be positioned in a certain way). Storage should not be of any concern as photos are quite limited in size. In addition, although additional hardware is required (a camera), this would only apply to a subset of users as many already have (web)cameras attached to their desktop or laptop, in particular the latter is often equipped with a webcam. As known, webcams are available at very affordable prices.

On first instance, typing rhythm recognition seems highly attractive when considering no additional hardware is required. When we look at the biometric feature itself, one of the first things one might wonder about, is if the feature is robust. Unfortunately, no long-term trials have evaluated the robustness of typing rhythm. However, it is proven that is it a motor programmed skill, and in general motor programmed skills seem quite robust. For example, this can be witnessed in sports, wherein players often have a certain style of playing or performing which remains characteristic over their entire career. The neurological details hereof are not discussed as they are beyond the scope of this thesis. Furthermore, when reviewing the relatively low FMRs of recent algorithms it seems the feature is quite distinct as well. In addition the feature is highly available, accessible and acceptable, as users use their keyboards per definition in MOOCs anyway. When we look at the methods utilizing typing rhythm for authentication purposes, the recent algorithms seem to produce acceptable results in terms of accuracy. The speed of most of these algorithms is excellent as well (in particular search heuristics based), with the exception of neural networks. Furthermore, due to the nature of the biometric feature, the usability is extremely straightforward and hardly requires any storage. And the best of all is the fact that no additional hardware is required, being readily available to everyone. In addition, the biometric feature highly lends itself for continuous authorisation. For example, it could be required that a student retypes the questions asked during the exam before answering them, allowing this continuous authorisation.

Quality	Fingerprint	Face	Typing rhythm
Accuracy	***	**	**
Speed	***	***	***
Usability	***	**	***
Storage	***	***	***
Costs	*	**	***
Robustness	***	**	*
Distinctiveness	***	**	**
Availability	***	***	***
Accessibility	***	***	***
Acceptability	**	***	***

Table 5.1: Assessment of biometrics. One star represents the lowest and three stars represents the highest score for application to MOOCs.

As mentioned earlier, Coursera applies typing rhythm and face recognition in their signature tracks, which does seem as a viable combination. Furthermore, it should certainly be considered to add fingerprint reading to the figure, mainly due to its extremely high accuracy which the other two biometric methods are lacking to date. Although it requires additional hardware, it is affordable and arguable is worth purchasing when considering applying to MOOCs for acquiring credit points. As with typing rhythm, it might even be continuously used for authentication as it is highly accessible and is not dependant on environmental distortions, and thus does not require certain highly specific instructions such as is the case with face recognition. Usage of all three biometric methods in conjunction is therefore recommended, in which at least one of the two candidates is to be used for continuous evaluation (fingerprint reading or typing rhythm).

CHAPTER 6

Conclusions

Concluding the biometric methods reviewed seem very interesting to apply to MOOCs, both on theoretical ground, as well as practical. However, bypassing these biometric methods is both statistically possible (albeit highly unlikely), as well as intentionally due to frauding during the enrollment phase. Nevertheless, when frauding during the enrollment phase (e.g. by providing imposter's fingerprints), the student is stuck to this template making it less attractive. Furthermore, it should always be kept in mind that fraud even occurs in real life classes on a, most likely, regular base. Usage of biometric methods therefore should not be seen as a solution to eradicate this, but rather as means to discourage it to an acceptable level.

Moreover, this thesis has only covered biometric methods. MOOCs could also benefit from non-biometric methods to reduce the risk of frauding. Another fairly recent development is that of online proctor services, in which a third party can monitor students taking an exam through webcam and microphone by a human, thus serving as a real life remote authenticator. However, such services are costly and are not practical for MOOCs (yet), as sometimes thousands of students are taking the same exam during an interval of a few hours. Perhaps proctors could be useful during the enrollment phase as these are not clustered in a narrow time frame, as with exams. Either way, relying on automated methods, such as the biometric methods presented in this thesis, is a very attractive approach.

Further research could focus on the application of the remaining mentioned biometrics which were omitted during the process of writing this thesis as described in Section 1. Voice recognition seems particularly interesting, as it only requires hardware for a subset of users analogously to the requirement of webcams for face recognition. In addition, the biometric feature is expressed by -nearly- everyone and is hardly intrusive. Moreover, as shortly mentioned before, non-biometric methods could provide useful in conjunction with biometric methods. An example could be the use of process monitoring to reduce the chance of the individual running a program providing him an unfair advantage (e.g. remote desktop through which someone can 'look over his shoulder' and assist), as well as potentially querying the internet for answers (provided that it is prohibited). Such process monitoring is already successfully applied in online gaming, to prevent cheaters from using third party programs to provide them with an unfair advantage over other players.

Bibliography

[1] McAuley A, Stewar B, Siemens G, Cormier D, The MOOC Model for Digital Practice. 2010; http://www.elearnspace.org/Articles/MOOC_Final.pdf. Retrieved April 2013.

[2] Kücken M, Newell AC, A model for fingerprint formation. Europhys. Lett., 68 (1), pp. 141–146 (2004).

[3] Wayman JL, Jain A, Maltoni D, Dario M, Biometric Systems. ISBN 1852335963 (2004).

[4] Chocolaad PFG, Kritieke succesfactoren voor biometrie. Master Thesis (2011).

[5] Coursera, http://blog.coursera.org/post/48343453924/courseras-first-birthday. Retrieved May 2013.

[6] Coursera, https://www.coursera.org/signature/guidebook/profile-creation. Retrieved May 2013. 3, 2013.

[7] Bours P, Barghouthi H, Continuous Authentication using Biometric Keystroke Dynamics. The Norwegian Information Security Conference (NISK) 2009.

[8] Shaffer LH, Timing in the motor programming of typing. Quarterly Journal of Experimental Psychology, 30(2):333–345, 1978.

[9] Lin DT, Computer-access authentication with neural network based keystroke identity verification, in: Proceedings of the International Conference on Neural Networks, Houston, TX, USA, 1997, pp. 174–178.

[10] Shepherd SJ, Continuous Authentication by Analysis of Keyboard Typing Characteristics, European Convention on Security and Detection, Brighton, UK, Bradford University, 1995, pp. 111–114.

[11] Joyce R, Gupta G, Identity authentication based on keystroke latencies, Communications of the ACM 33 (2) (1990) 168–176.

[12] Monrose F, Reiter MK, Wetzel S, Password hardening based on keystroke dynamics, Proceedings of the 6th ACM Conference on Computer and Com-munications Security, Kent Ridge Digital Labs, Singapore, 1999, pp. 73–82, ISBN:1-58113-148-8.

[13] Gaines R, Lisowski W, Press S, Shpiro N, Authentication by Keystroke Timing: Some preliminary results, Rand Report R-256-NSF. Rand Corporation, 1980.

[14] Leberknight CS, Widmeyer GR, Recce ML, An investigation into the efficacy of keystroke analysis for perimeter defense and facility access, Proceedings of the IEEE International Conference on Technologies for Homeland Security, 2008, 345–350, ISBN: 978-1-4244-1977-7.

[15] Rybnik M, Tabedzki M, Saeed K, A keystroke dynamics based system for user identification, Proceedings of the 7th Computer Information Systems and Industrial Management Applications, 2008, pp. 225–230, ISBN: 978-0-7695-3184-7.

[16] Bleha S, Slivinsky C, Hussein B, Computer-Access Security Systems using Keystroke Dynamics, IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 12, no. 12, 1990, pp. 1217–1222.

[17] Cho S, Han C, Han DH, Kim H, Web-based keystroke dynamics identity verification using neural network, Journal of Organizational Computing and Electronic Commerce, 10(4):295–307, 2000.

[18] Zhong Y, Deng Y, Jain AK, Keystroke Dynamics for User Authentication, IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp. 117-123, 2012.

[19] Killourhy KS, Maxion RA, Comparing Anomaly-Detection Algorithms for Keystroke Dynamics, Proc. 39th Annual Int'l Conf. on Dependable Systems and Networks (DSN-2009), pp. 125-134, 2009.

[20] Coppenrath LF, Biometric Solutions by Classification. http://www.lfca.net/Reference%20Documents/Biometric%20Solutions/%20By%20Classification.pdf, 2001. Retrieved July 2013.

[21] Spillane RJ, Keyboard Apparatus for Personal Identification. Technical Disclosure Bulletin 17, 3346, IBM, 1975.

[22] Brown M, Rogers S, User Identification via keystroke characteristics of typed names using neural networks. International Journal of Man-Machine Studies, 39:999 – 1014, 1993.

[23] Ahmed A, Traore I, Almulhem A, Digital Fingerprinting based on Keystroke Dynamics. Proceedings of 2nd International Symposium on Human Aspects of Information Security and Assurance (HAISA), 2008.

[24] Sang Y, Shen H, Fan P, Novel Impostors Detection in Keystroke Dynamics by Support Vector Machine. Parallel and Distributed Computing: Applications and Technologies, Lecture Notes in Computer Science, Volume 3320, pp. 666-669, 2005.

[25] Revett K, A Bioinformatics Based Approach to Behavioural Biometrics, Frontiers in the Convergence of Bioscience and Information Technologies, pp. 665–670, Oct. 2007.

[26] Jugurta RMF, Freire OE, On the equalization of keystroke timing histograms, Pattern Recognition Letters, 27:1440–1446, October 2006.

[27] Killourhy KS, Maxion RA, Comparing Anomaly-Detection Algorithms for Keystroke Dynamics, IEEE/IFIP International Conference on Dependable Systems Networks, pp. 125–134, July 2009.

[28] Giot R, El-Abed M, Rosenberger C, GREYC keystroke: A benchmark for keystroke dynamics biometric systems, IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, pp. 1-6, Sept. 2009.

[29] Bello L, Bertacchini M, Benitez C, Pizzoni JC, Cipriano M, Collection and Publication of a Fixed Text Keystroke Dynamics Dataset, CACIC 2010, October 2010.

[30] Wayman J, Fundamentals of biometric authentication technologies, International Journal of Image and Graphics 01:01, 93-113, 2001.

[31] Tian J, He Y, Yang X, Li L, Chen X, Improving Fingerprint Recognition Performance Based on Feature Fusion and Adaptive Registration Pattern, Advances in Biometric Person Authentication, Lecture Notes in Computer Science Volume 3338, 2005, pp. 57-66

[32] Maio D, Maltoni D, Cappelli R, Wayman JL, Jain AK, FVC2004: Third Fingerprint Verification Competition, Biometric Authentication, Lecture Notes in Computer Science Volume 3072, pp. 1-7, 2004.

[33] Jain A, Hong L, Pankati S, Biometric Identification, Communications of the ACM, Volume 43, No. 2, February 2000.

[34] Sinha P, Balas B, Ostrovsky Y, Russell R, Face Recognition by Humans: Nineteen Results All Computer Vision Researchers Should Know About, Proceedings of the IEEE, Volume 94, No. 11, November 2006.

[35] Givens GH, Beveridge JR, Philips PJ, Draper B, Lui YM, Bolme D, Introduction to face recognition and evaluation of algorithm performance, Computational Statistics & Data Analysis, Volume 67, pp. 236-247, November 2013.

[36] Philips PJ, Grother P, Michaels R, Blackburn DM, Tabassi E, Bone M, Face recognition vendor test 2002, Analysis and Modeling of Faces and Gestures, 2003. AMFG 2003. IEEE International Workshop on. IEEE, pp. 44, 2003.

[37] Zhang C, Zhang Z, A Survey of Recent Advances in Face Detection, Tech. rep., Microsoft Research, 2010.

[38] Yang MH, Kriegman DJ, Ahuja N, Detecting faces in images: A Survey, Pattern Analysis and Machine Intelligence, IEEE Transactions on 24(1), 34-58, 2002.

[39] Viola P, Jones M, Rapid object detection using a boosted cascade of simple features, Computer Vision and Pattern Recognition, Proceedings of the 2001 IEEE Computer Society Conference, Volume 1, pp. I-511, 2001.

[40] Schiphol, Iris scans at Amsterdam Airport Schiphol, http://www.schiphol.nl/Travellers/AtSchiphol/Privium/Privium/IrisScans.htm. Retrieved August 2013.

[41] Unique Identification Authority of India, Role of Biometric Technology in Aadhaar Enrollment, http://uidai.gov.in/images/FrontPageUpdates/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf, 2012. Retrieved August 2013.

[42] Philips PJ, WT Scruggs, O'Toole AJ, Flynn PJ, Boywer KW, Schott CL, Sharpe M, FRVT 2006 and ICE 2006 large-scale results, Pattern Analysis and Machine Intelligence, IEEE Transactions, Volume 32, Issue 5, pp. 831-846, 2010.

[43] Wang H, Li SZ, Wang Y, Face Recognition under varying lighting conditions using self quotient image, Automatic Face and Gesture Recognition, Proceedings. Sixth IEEE International Conference, pp. 819-824, May 2004.

[44] Nishiyama M, Kozakaya T, Yamaguchi O, Illumination Normalization using Quotient Image-based Techniques, Recent Advances in Face Recognition, I-tech, Vienna, Austria, 97-108, 2008.

[45] Philips PJ, Moon H, Rizvi SA, Rauss PJ, The FERET evaluation methodology for face-recognition algorithms, Pattern Analysis and Machine Intelligence, IEEE Transactions, 22(1), 1090-1104, 2000.

[46] Sim T, Baker S, Bsat M, The CMU pose, illumination, and expression database, Pattern Analysis and Machine Intelligence, IEEE Transaction, 25(12), 1615-1618, 2003.

[47] Introna L, Nissenbaum H, Facial Recognition Technology: A Survey of Policy and Implementation Issues, Center for Catastrophe Preparedness and Response, New York University, 2009.

[48] Sumner J, Serving the system: A critical history of distance education. Open learning, 15(3), 267-285, 2000.

[49] Universität Tübingen, http://timms.uni-tuebingen.de/archive/sose99.aspx. Retrieved August 2013.

[50] Jain AK, Prabhakar S, Pankanti S, On the similarity of identical twin fingerprints, Pattern Recognition, 35(11), 2653-2663, 2002.

[51] Kaluszynski M, Alphonse Bertillon et l'anthropométrie, Maintien de l'ordre et polices en France et en Europe au XIXe siècle, 1987.

[52] Stigler SM, Galton and identification by fingerprints, Genetics, 140(3), 857, 1995.

[53] Moses KR, Automated Fingerpritn Identification System (AFIS), Scientific Working Group on Friction Ridge Analysis Study and Technology and National institute of Justice (eds.) SWGFAST-The fingerprint sourcebook, 1-33, 2011.

[54] Haberman W, Fejfar A, Automatic Identification of Personnel Through Speaker and Signature Verification-System Description and Testing, Carnahan Conference on Criminal Countermeasure Proceedings, 1976.

[55] Turk MA, Pentland AP, Face recognition using eigenfaces, Computer Vision and Pattern Recognition, Proceedings CVPR'91., IEEE Computer Society Conference, pp. 586-591, June 1991.

[56] University of Amsterdam Online Courses, http://mooc.uva.nl. Retrieved August 2013.

[57] NSTC Subcommittee on Biometrics, Biometrics History, http://www.biometrics.gov/documents/biohistory.pdf. Retrieved August 2013.