36

Haptics and the Biometric Authentication Challenge

Andrea Kanneh and Ziad Sakr
University of Trinidad and Tobago, O'Meara Campus
Trinidad and Tobago

1. Introduction

There has been an increasing demand for on-line activities such as e-banking, e-learning and e-commerce. However, these on-line activities continue to be marred by evolving security challenges. On-line verification is now central to security discussions.

The use of biometrics for individual authentication has always existed. Physiological biometrics, which is based on physical features, is a widespread practice. Behavioural biometrics, however, is based on what we do in our day-to-day activities such as walking or signing our names. Current research trends have been focusing on behavioural biometrics as this type of authentication is less intrusive.

Haptics has come a long way since the first glove or robot hand. Haptics has played an immense role in virtual reality and real-time interactions. Although gaming, medical training and miniaturisation continue to prove the enrichments created by haptics technology, as haptic devices become more obtainable, this technology will not only serve to enhance the human-computer interface but also to enhance cyber security in the form of on-line biometric security.

Limited research has been done on the combination of haptics and biometrics. To date, dynamic on-line verification has been widely investigated using devices which do not provide the user with force feedback. Haptics technology allows the use of force feedback as an additional dimension. This key behavioural biometric measure can be extracted by the haptics device during any course of action. This research has significant implications for all areas of on-line verification, from financial applications to gaming. Future challenges include incorporating this technology seamlessly into our day to day devices and operations.

This chapter starts with a brief overview of security. This is followed by an introduction to key concepts associated with biometrics. Current on-line dynamic signature verification is then reviewed before the concept of the integration of haptics and biometrics is introduced. The chapter then explores the current published work in this area. The chapter concludes

with a discussion on the current challenges of haptic and biometric authentication and predicts a possible path for the future.

2. Motivation

This chapter seeks to illustrate that the haptic force extracted from a user with a haptic device could be used for biometric authentication. It further shows that this form of authentication (using haptic forces) can potentially add to the accuracy of current on-line authentication.

3. The challenges of On-line Security

Security mechanisms exist to provide security services such as authentication, access control, data integrity, confidentiality and non repudiation and may include the mechanisms such as biometric authentication and/or security audit trails (Stallings, 2006).

On-line security is of particular importance especially for activities such as on-line banking or e-payments. Cyber attacks continue to increase and can take many forms. An example of this was the Banker Trojan which was created to copy passwords, credit card information and account numbers associated with on-line banking services from the user's PC.

In order for security mechanisms to work every link in the chain must work. This includes personal and/or resource passwords. People's habits or the security culture within organisations, such as sharing passwords or writing them down, or not logging off when they step away from the computer can break down most security systems. Often these habits are hard to monitor and prevent (Herath & Rao, 2009; Kraemera et al., 2009) yet in spite of this, text passwords remain popular as they are relatively easy to implement and still accepted by users. For the actual username–password method to be effective, it is essential that users generate and use (and remember) strong passwords that are resistant to guessing and cracking (Vu et al., 2007).

Biometric authentication cannot solve every problem with on-line security but it can be used to overcome some of these issues associated with passwords and system access. Biometric security can also provide a measure of continuous authentication when performing the actual transaction. The use of biometric security does not leave the user with something to remember or to write down. Dhamija and Dusseault (2008) suggest that users are more likely to accept a security system if it is simple to use.

4. Biometrics and Individual Authentication

4.1 Biometric Concepts

Biometrics is described as the science of recognizing an individual based on his or her physical or behavioural traits (Jain et al., 2006). Since a biometric is either a physical or behavioural characteristic of the user it is almost impossible to copy or steal. The use of biometrics as a security measure offers many benefits such as increasing individual user accountability or decreasing number of Personal Identification Numbers (PINs) and

passwords per user. This in turn allows stronger security measures for remaining PINs and passwords.

Biometric security has existed since the beginning of man – recognising someone by face or voice. Fingerprint biometrics dates back to ancient China. A formal approach for commercial use dates back to the 1960s and 1970s as is the case with fingerprint scanning, which has been around since the late 1960s (Dunstone, 2001).

Biometrics authentication refers to both verification and/or identification. In verification the subject claims to be a specific person and a one-to-one comparison is done. Whereas, with identification the applicant's data is matched against all the information stored or the entire database to determine his/her identity. This is a one-to-many task.

There are many applications of biometrics for both security and confidentiality. These include law enforcement and forensics, access control, and preventing/detecting fraud in organisations, educational institutions and electronic resources. Biometric Encryption also exists. This is the process of using a characteristic of the body as a method to code/encrypt/decrypt data. This can be used in asymmetric encryption to generate the private key.

Jain et al. (2004) outlined some characteristics of efficient biometric systems:
(i) Universality — every person should have the characteristics.
(ii) Distinctiveness — no two persons should have the exact biometric characteristics.
(iii) Permanence — characteristics should be invariant with time.
(iv) Collectability —characteristics must be measurable quantitatively.
(v) Performance — the biometric system accuracy, speed, consistency and robustness should be acceptable
(vi) Acceptability — users must be willing to accept and use the system.
(vii) Circumvention —fooling the system should be difficult.

4.2 Biometric Techniques

There are two types of biometric techniques – physiological and behavioural. Physiological techniques are based physical characteristics. Examples include fingerprint recognition, iris recognition, face recognition, hand geometry (finger lengths, finger widths, palm width, etc.), blood vessel pattern in the hand, DNA, palm print (apart from hand geometry), body odour, ear shape and fingernail bed (apart from fingerprints).

Behavioural techniques are based on the things you do (a trained act or skill that the person unconsciously does as a behavioural pattern). Examples include voice recognition, keystroke recognition (distinctive rhythms in the timing between keystrokes for certain pairs of characters), signature recognition (handwriting or character shapes, timing and pressure of the signature process). Gait recognition or the pattern of walking or locomotion is also used as a biometric measure (Ortega-Garcia et al., 2004).

4.3 The Biometric Process

The Biometric Process has two stages – enrolment and authentication. Each user must first be enrolled in the system. Here the aim is to capture data from the biometric device which can identify the uniqueness of each subject as it is essential to establish a 'true' identity. The key features for each user are then extracted from this data and stored in a database. These features could be common for all users or customised, either by weights assigned to show the importance of the feature or by selecting different features, for each user. Usually before feature extraction/selection there is some form of pre-processing in which the data is made more manageable for extraction. Some form of normalisation or smoothing may be done at this stage. After the template is created for each user (during enrolment), a new sample is taken and compared to the template. This creates the genuine distance measure (Wayman, 2000). The average genuine distance for the whole sample population can be used as a common threshold or the threshold can be unique for each user.

During the authentication (identification and/or verification) process new samples taken from the subject are compared to the stored data and a match score is computed to determine the fit. The match score is compared to the threshold score and if it is greater that the threshold score this is not considered to be a fit. The general biometric process is shown in the figure below (Fig. 1.). This is them summarised in the table which follows (Table 1).

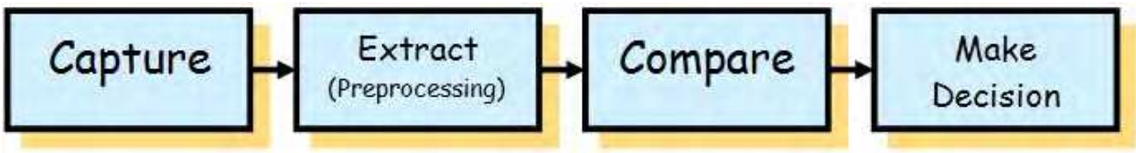


Fig. 1. The Biometric Process

Stage of Process	Activity
Capture	A physical or behavioural sample is captured by the system during enrolment. (Data Collection); this is influenced by the technical characteristics of the sensor, the actual measure and the way the measure is presented.
Extraction	Unique data is extracted from the sample and a template is created. Distinctive and repeatable features are selected. Feature templates are stored in the database.
Comparison/ Classification	The new sample is then compared with the existing templates. Distance Measures (DM) are calculated and compared to threshold(s). DM Never zero because of variability due to human, sensor, presentation , environment
Decision-making	The system then decides if the features extracted from the new sample are a match or a non-match based on the threshold match score.

Table 1. The Biometric Process explained

4.4 Some Challenges with Biometric Authentication

A biometric system cannot guarantee accuracy partly due to the variability in humans, the systems and the environment. Stress, general health, working and environmental conditions and time pressures all contribute to variable results (Roethenbaugh, 1997). Some of these factors are explained in Table. 2.

There are two main accuracy measures used: False Accept and False Reject. False Accept error occurs when an applicant, who should be rejected, is accepted. False Accept Rate (FAR) or Type II error rate is the percentage of applicants who should be rejected but are instead accepted. False Reject Rate (FRR) or Type I error rate is the percentage of legitimate users who are denied access or rejected. These two measures are also referred to as false match or false non-match rates respectively.

Since these are two different measures it is difficult to judge the performance of the system base on only one measure so both are usually plotted on a Receiving/Relative Operating Curve (ROC) (Martin et al., 2007; Wayman, 2000) which is a graph of FAR as a function of FRR (Gamboa and Fred, 2004). The equal error rate (EER) is defined as the value at which FAR and FRR are equal. This can be used as a single measure to evaluate the accuracy of the biometric system.

Factor affecting performance	Example
Environmental conditions	Extreme temperature and humidity can affect a system's performance
The age, gender, ethnic background and occupation of the user	Dirty hands from manual work can affect the performance of fingerprint systems
The beliefs, desires and intentions of the user	If a user does not wish to interact with the system, then performance will be affected. E.g. the user may deliberately control his/her typing speed
The physical make-up of the user	A user with no limbs cannot use hand or finger-based biometrics

Table 2. Factors affecting accuracy of biometric measurements

The UK Government Test Protocol for Biometric Devices (Mansfield et al., 2001) is a standard protocol which could be used for commercially available biometric devices. It suggests some time lapse between the collection of trials for template creation (to cater for the aging or learning process). Two common system errors are Failure to enrol and Failure to Acquire. Failure to enrol occurs when the system is unable to generate repeatable templates for a given user. This may be because the person is unable to present the required feature. Failure to acquire occurs when the system is unable to capture and/or extract quality information from an observation. This may be due to device/software malfunction, environmental concerns and human anomalies.

The following diagrams sums up some of the possible errors within each stage of the process.

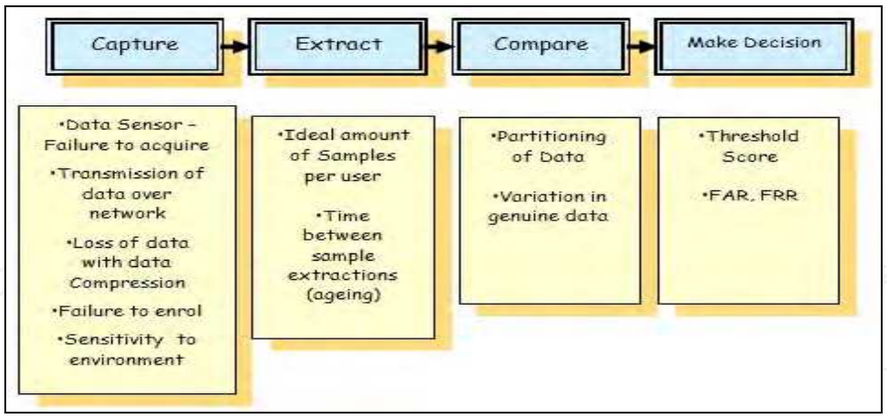


Fig. 2. Some possible errors within the Biometric Process

4.5. Multimodal Biometrics

A multimodal approach could be adopted to make a biometric system more secure. A layered or multimodal biometrics approach uses two or more independent systems or techniques to yield greater accuracy due to the statistical independence of the selected approaches. Therefore more than one identifier is used to compare the identity of the subject. This approach is also called multiple biometrics (Huang et al., 2008). Ortega-Garcia et al. (2004) refers to this as unimodal-fusion or monomodal-fusion.

5. Dynamic Signature Verification: a form of Biometric Authentication

Dynamic signature verification (DSV) can capture not only the shape of the image, as is done with static signature recognition, but also the space-time relationship created by the signature. Both static and dynamic signature verification are forms of biometric authentication.

Numerous studies have been done on dynamic signature verification – Plamondon (Plamondon & Srihari, 2000) and Jain (Jain et al., 2002) are just two of the popular names associated with these studies. Some of the work done on DSV follow.

In a study by Lee et al. (1996) individual feature sets as well as individual thresholds were used. The authors suggested that if time is an issue then a common feature set should be used. These features were captured using a graphics tablet (or digitising tablet, graphics pad, drawing tablet). Normalisation was done using factors such as total writing time (time-normalised features), total horizontal displacement, and total vertical displacement. Majority classifiers (implementing the majority decision rule) were used in the classification stage.

To decrease processing time a simple comparison was done before the classification stage - this took the form of 'prehard' and 'presoft' classifiers. This was done by comparing the absolute value of writing time of the signature being tested minus the average writing time. With the presoft classifier if this value was below a certain level (.2) the data did not need to

be normalised before extraction. For the prehard classifier if this value was too high the data was instantly rejected. They were able to achieve 0% FRR and 7%FAR.

Penagos et al (1996) also used customised feature selection – the weight assigned to each feature was adjusted for each feature of each user. The common features selected were the starting location, size, and total duration of the signature. As in Lee et al. (1996) the threshold was also customised for each user. The customised thresholds were adjusted, if needed, until either their signatures were accepted repeatedly, or the maximum threshold value was reached. The experiment was conducted with the use of a digitizing tablet to extract features such as shape of signature, pressure (measured with the stylus), speed and acceleration. Normalisation was done on the time, position and acceleration values. They were able to achieve an 8% FRR and 0%FAR.

Plamondon & Srihari (2000) presented a survey paper on on-line and off-line handwriting recognition and verification. It suggested that at the time of this article (2000), even if verification was being researched for about three decades, the level of accuracy was still not high enough for situations needing high level of accuracy such as banking. The survey listed several techniques used for user verification, they include neural networks, probabilistic classifiers, minimal distance classifiers, nearest neighbour, dynamic programming, time warping, and threshold based classifier. One point highlighted was that before recognition noise is removed by a smoothing algorithm, signal filtering.

Jain et al. (2002) used writer-dependent threshold scores for the classification stage. For their experiment, like the ones above, a digitising tablet was used. The features were separated into Global (properties of the whole signature e.g. total writing time) and Local (properties that refer to a position within the signature e.g. pressure at a point). Prior to the feature selection stage a Gaussian filter was used to smooth the signatures. Number of individual strokes and absolute speed normalized by the average signing speed were some of the features used. Dynamic Time Warping was used to compare strings. The experiment yielded a FRR of 2.8% and a FAR or 1.6%.

Some studies focus on the best selection of the features, for example Lei & Govindaraju, (2005). In this paper they compared the discriminative power of the biometric features. Here the position features were normalised by dividing by the maximum height or maximum width. The authors compared the mean or average consistency for each feature, the standard deviation over subjects, and EER of selected features. The authors highlighted the fact that a high standard deviation implies that this feature may not discriminate itself among users. Low mean consistency implies that this feature varies among one user. The results showed that some features such as the speed, the coordinate sequence, and the angle were consistent and reliable.

In most studies the features were first normalised to make them easier to select and compare. Dimauro et al. (2004) suggested that the data should be first filtered then normalised in time-duration and size domain. Faundez-Zanuy (2005) stated that length normalisation was used because different repetitions of signature from a given person could have different durations.

Feature such as 2D position and speed were common features selected. McCabe et al. (2008) used other features such as aspect ratio (This is the ratio of the writing length to the writing height). Number of "pen-ups" (This indicates the number of times the pen is lifted while signing after the first contact with the tablet and excluding the final pen-lift). Top Heaviness (This is a measure of the proportion of the signature that lies above the vertical midpoint i.e., the ratio of point density at the top half of the signature versus the density at the bottom half), and Area (This is the actual area of the handwritten word). They used a neural network for user verification. The FAR was as low as 1.1% with a 2.2% FRR.

Recently Eoff and Hammond (2009) obtained accuracy of 97.5% and 83.5% for two and ten users respectively. The study was used to identify different user strokes on a shared (collaborative) surface. Here the authors used pen tilt, pressure and speed to classify users. A Tablet PC was used to capture the strokes of users.

Unlike the other studies discussed, C Hook et al. (2003) did not use the digitising tablet. They presented a study of a biometrical smart pen BiSP. In this study the pen itself was able to capture measures such as pressure and acceleration. This study took a multimodal approach - it also used fingerprint information as well as acoustic information for authentication. Results showed accuracy of up to 80% for user identification and 90% for user verification.

6. Haptic Devices and Biometrics

6.1 Haptics Force Feedback

Haptic, from the Greek αφή (Haphe) means pertaining to the sense of touch. Touch is different from sight and sound because with touch there is an exchange of energy between the user and the physical world: as the user pushes on an object, it pushes back on the user (Salisbury & Srinivasan, 1997).

Haptic interfaces allow a user to touch, feel, and manipulate three-dimensional objects in a virtual environment (Orozco et al., 2006).

Haptics not only refers to tactation (the distribution of pressure on the skin), it includes the study of movement and position, which is kinesthetics. Rendering techniques aim to provide reasonable feedback to users for instance the shape of the object, the texture of the surface and a sense of the force exerted by the user to achieve the task at hand (the mass of the object). Haptics applications can offer both spatial and temporal information.

The concept of the haptic force has been used in entertainment, training and education but, compared to these, haptics in security is relatively new. The haptic force can also be used to uniquely identify persons. The following diagram (Fig.3.) shows the force produced by two different subjects carrying out the same task. The individuals were provided with a surface which provided enough friction and softness to mimic a paper surface, and asked to write the same letter of the alphabet. As the number of users increase it is not as easy for the human eye to differentiate so this is why computer generated classification algorithms are applied.

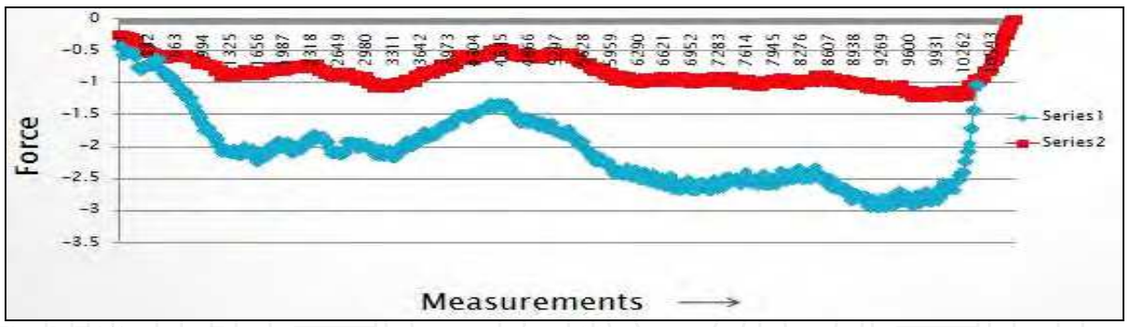


Fig. 3. Difference Force measurements produced by two users

While passwords and other access control provide some level of security, haptic devices can be used to supply behavioural biometrics such as force, position and angular orientation, which can provide ongoing/continuous security assessment while the user is using the system, thereby making haptics a good facilitator for (biometrics) signature recognition.

6.2 Haptics and Biometrics

A number of haptic devices exist, one of which is the PHANToM (The Personal Haptic Interface Mechanism) device (http://www.reachin.se/) which allows the user to feel virtual objects in a 3D space (Fig. 5).

(a) The Phantom Desktop

(b) The Reachin device form SensAble uses the Phantom Desktop as one of its components

Fig. 4. The Phantom Desktop and the Reachin Device

The PHANToM is part of the Reachin Desktop (Fig. 4b.). This device is able to extract and provide the same data as the digital tablets and more, such as force and torque, as well as the xyz (3D) coordinates all of which can fall under the heading of behavioural biometrics. Haptic devices can make biometric authentication (for access control) even more effective as the imposter using the device, to fool the system, can no longer just copy the visual output of the signature or activity, but now has to replicate the force produced by the user at a particular position, at the relative time (to the length of the signature) that that force was

produced. Unlike the digitising tablet, haptic devices act like an output as well as input device. Even though the stylus tip of the digital tablets may sense pressure, they do not provide the force feedback to the user.

The following papers present several applications with haptics and biometrics. The work was done at the Distributed & Collaborative Virtual Environments Research Laboratory, University of Ottawa, Canada. Each application captured similar measurements such as force, time and momentum. The Reachin device was used in these studies. The general aim of these experiments was to explore the use of the Reachin haptic device to gain continuous authentication of the user based on the behavioural biometrics obtained from the interaction with the on screen application. Accuracy ranged from 80% (Orozco et al., 2005b) to 95.4% (Orozco et al., 2006a) with some initial findings showing the possibility of reaching accuracy as high as 98.4% (Orozco et al., 2006a). Classification algorithms comprised nearest neighbour, k-means, artificial neural networks and spectral analysis. Relative Entropy was used for feature selection. For the studies which follow the participants were given some time to familiarise themselves with the application.

The Virtual Phone experiment (Orozco et al., 2005a, 2005b) was conducted to analyse the unique characteristics of individual behaviour while using an everyday device (a virtual phone). 20 subjects were asked to dial the same code 10 times (Orozco et al., 2005b). Specific measures obtainable from the experiment include hand-finger positions, force applied to the keypad as well as time interval between pressing each key. The results of the experiment revealed that features such as force, velocity and keystroke duration were not as distinguishable as those related to the pen position. In this experiment they were able to attain about 20% FRR (Orozco et al., 2005b).

The Virtual Maze experiment (Orozco et al., 2006a, 2006b; El Saddik et al., 2007) aimed to identify the unique psychomotor (combined physical and mental) patterns of individuals participants based on their manipulation of haptic devices. In this case a virtual 2D maze on a 3D space was used. Data collected included xyz position, velocity, 3D force and torque from 39 subjects (Orozco et al., 2006a). Relative entropy was used for feature extraction, and comparison was done using Hidden Markov Models, Fast Fourier Transform spectral analysis and Dynamic Time Warping (Orozco et al., 2006b).

User dependent thresholds were also tested which improved the verification accuracy produce with a common threshold (Orozco et al., 2006a). The study also looked at the effect of introducing stress (Orozco et al., 2006a). This resulted in more variability and hence lower accuracy (66% FRR). The results of the paper showed that the haptic devices were more successful at verification than identification. They were able to attain 4.6%FRR with 16% FAR for verification (Orozco et al., 2006a).

The Virtual Cheque experiment (El Saddik et al., 2007) was created with the aim of removing any mental interference that could affect performance. Pen position, force exerted and velocity were extracted from the 16 subjects used. Relative entropy was first used to analyse the information content and signal processing was used to form the biometric profile. In classifier design a quantitative match score was calculated and used for the

comparison and make decision stages. K-Means was used to cluster the features. It was found that Force data had the most information. The equal error rate fell between 6 % and 9% for the virtual cheque verification. Virtual signature verification was 8% FRR with 25% FAR. Some information was lost due to data compression which was used to reduce the storage requirement.

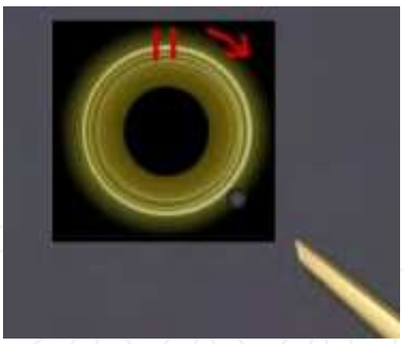
It is necessary to note that the authors concluded, based on their results, that these experiments (in this section) were more suitable for verification than identification (El Saddik et al., 2007). It was also observed that features such as speed became more consistent in the later trials than the initial ones as the participants became more comfortable with time (Orozco et al., 2005b; El Saddik et al., 2007).

Orozco et al. (2006c) also used a virtual grid. The user created a hapto-graphical password by navigating through the grid and selecting and connecting nodes on the grid, using a stylus. Features such as force, torque, angular orientation, and 3D position were selected. They also looked at pen-ups during the execution as was done in the study conducted by McCabe et al. (2008). Biometric classification was done with algorithms such as Nearest Neighbour and Artificial Neural Networks..

6.3 A Detailed description of a verification scheme

Our studies (Kanneh & Sakr., 2008a-d) presented a new algorithm for user verification. In our approach a fuzzy logic controller was used to mimic human reasoning in decision making. The user was instructed to trace a circle in particular direction. (Fig. 5.)

(a) User using the Reachin Device to trace the virtual circle



(b) The User Interface

Fig. 5. The Haptics and Biometrics Verification System

Limiting the direction was done to place some extra stress on the system to test just how effective the verification algorithm would be. In a real world application the user would be allowed to go in his/her preferred direction and this should improve the accuracy of verification even more. The Reachin Device and Application Programmer Interface (API) were used for this experiment. 9 participants were tested. These studies also introduced

normalisation or standardisation of features based on their standard deviations. This process made each subject's data more distinguishable.

Principal Component Analysis was then used for feature selection. Seven features were chosen – force values at different positions, average size of the radius drawn, XYZ Distances and time. It was found that the XYZ distances provided the most information for this system. Based on the unique method of normalisation, as well as the use of the fuzzy logic templates for classification, the experiment yielded a verification accuracy of up to 96.25% with a 3.75% FRR and an 8.9% FAR (Kanneh & Sakr., 2008d).

The Reachin Haptic system used for these experiments (sections 6.2 and 6.3) exhibited the properties of a good biometric system outlined by Jain et al. (2004). The experiments showed that while some features were not distinguishable for every application such as force data with the virtual phone (Orozco et al., 2006c) the force data was key for the virtual cheque (El Saddik et al., 2007). This shows that there is no one recipe (group of algorithms) that could be applied to all experiments – the target application dictated the key features that could be used for classification.

7. Current Challenges with Haptics and Biometrics

Based on the current work discussed in sections 6.2 and 6.3 the concept of biometrics based on haptics is reasonable. The experiments all show that there is greater potential to be explored. As haptic devices become cheaper and more commonplace user acceptance of a new method of authentication will be more probable. There are some variability issues due to the users, system and environment which affect most biometric systems. In addition to this variability within the trials, handwriting can also change with time. Using soft algorithms such as fuzzy logic and neural networks reduces the effects of variability. Both neural networks and dynamic fuzzy logic can cope with the gradual change in handwriting.

Users also pointed out some Human-Computer Interaction (HCI)/ergonomics issues such as the difficulty, on first contact, to sense the distance to touch the virtual surface and the discomfort caused by not being able to rest down the hand when using the Rechin device (Kanneh & Sakr, 2008d) (see figures 4b and 5a). As the technology becomes more available some of these HCI issues would be resolved.

Coping with problem signers is another issue with biometric security (Penagos, 1996). These signers have very variable signatures making template creation (to yield good FAR and FRR) almost impossible. There is always the possibility of the failure to enrol and failure to acquire errors (Mansfield et al., 2001) where the user is not able to perform the action required by the system or produces features with insufficient quality to register. Fàbregas & Faundez-Zanuy, (2009) proposed a system to guide the user through the process which reduces this error and also identifies those individuals who cannot be enrolled.

With respect to haptic devices there is a key issue which needs to be addressed, that is interoperability across different operating systems and different versions of a device and

device API. Haptic rendering is also still a work in progress as the haptic force sometimes becomes unstable under certain conditions.

Though biometrics presents a viable security measure there are some concerns specific to Biometrics. Standards are still being developed. Standards are essential for interoperability among vendors. Without standards biometrics is not cost beneficial to the potential user or the vendor. Another issue is that user data must be collected first to create the templates used for authentication. This becomes an issue for large-scale identification for example most terrorist are unknown. Security of the template database must also be addressed (Shan et al., 2008). When a typical password is compromised it can be changed. Unlike passwords, when a person's key feature (biometric) is copied, the template cannot be changed. This is referred to as the revocation problem (Panko, 2004).

According to Wayman (2000) and Mansfield et al. (2001) the sample size for biometric device evaluation should be large enough to represent the population and contain enough samples from each category of the population (from genuine individuals and impostors). In addition to this the test period should be close as possible to the actual period of the application's use. Both requirements increase the budget for testing and as a result, are usually not carried out.

There are other independent security issues which would not be solved with the use of a haptics device. Phishing and spam are just some of these issues. Shan et al. (2008) discuss various potential security threats to biometric systems, providing some food for thought when evaluating the storage and transfer of the unique biometric features in a biometric system. The authors seem to focus on this aspect as they appreciate the growing importance of e-commerce and the security of transactions.

8. Conclusion

The chapter shows that the potential for greater accuracy for on-line verification exists with the use of haptic devices by extracting data which is available from the digital tables in use as well as force data. Though experimental data using haptic devices are limited, the experiments covered showed that verification accuracy is very high- up to 96% (Kanneh & Sakr, 2008d). The potential exists for these results to be further improved with the use of customised threshold scores and customised feature selection (Lee et al., 1996; Penpgosl et al., 1996; Plamondon & Srihari, 2000).

Neural networks and other soft approaches can also be explored further with a view to increasing the authentication accuracy. There is a wealth of experiments with dynamic signature verification which could be altered by using a haptics device instead of the digital tablet.

It is worth noting that the haptics and biometrics experiments (sections 6.2 and 6.3) have been conducted in a controlled environment with engineering students as subjects. According to the target applications intended, the evaluation of the particular haptic device should again be done with the sample representative of the target population (Mansfield et al., 2001).

Haptics as a form of biometrics is a potential goldmine but it is still a work in progress. The accuracy of a biometric system can be further improved using a form of fusion with other independent biometric features or with the traditional password or smart card. These are multimodal approaches (discussed in section 4.5).

Haptics security need not only be applied to on-line activities. This concept of haptics and biometrics can be used within organisations for access to key areas. Both textual and graphical passwords could be supported with the use of haptic devices. Future research can explore the role of Haptics based biometric security in smart houses as ambient intelligence is gaining more and more interest.

Acknowledgements

Special thanks for the ongoing support of our families, as well as for the support of the staff and students of the University of Trinidad and Tobago and the Distributed & Collaborative Virtual Environments Research Laboratory, University of Ottawa.

9. References

Dhamija, R. & Dusseault, L. (2008) *The Seven Flaws of Identity Management: Usability and Security Challenges*. IEEE Security and Privacy, Vol. 6, No. 2, Mar./Apr. 2008, pp. 24-29, Institute of Electrical and Electronics Engineers (IEEE), USA

Dimauro, G., Impedovo, S., Lucchese, M.G., Modugno, R. & Pirlo, G. (2004). *Recent Advancements in Automatic Signature Verification*. Proceedings of the 9th International Workshop on Frontiers in Handwriting Recognition (IWFHR-9 2004), 0-7695-2187-8 Kokubunji, Tok, Oct. 2004, Institute of Electrical and Electronics Engineers (IEEE)

Dunstone, S. (2001). *Emerging Biometric Developments: Identifying The Missing Pieces For Industry*. Proceedings of Sixth International Symposium on Signal Processing and its Applications. vol.1. *pp*.351-354, 0-7803-6703-0, Kuala Lumpur, Malaysia, Institute of Electrical and Electronics Engineers (IEEE), USA

El Saddik, A., Orozco, M., Asfaw, Y., Shirmohammadi, S. & Adler, A (2007). A Novel Biometric System for Identification and Verification of Haptic Users. *IEEE Transactions on Instrumentation and Measurement*, Vol.56, No.3, (June 2007), (895-906), 0018-9456

Eoff, B.D. & Hammond, T. (2009). *Who Dotted That 'i'? : Context Free User Differentiation through Pressure and Tilt Pen Data*. Proceedings of Graphics Interface 2009, Vol. 324 pp. 149-156, 978-1-56881-470-4, Kelowna, British Columbia, Canada, 2009, Canadian Information Processing Society Toronto, Ont., Canada, Canada

Fàbregas, J. & Faundez-Zanuy, M. (2009). On-line signature verification system with failure to enrol management. *Science Direct Pattern Recognition Elsevier Ltd,* Vol.42 No.8, (September 2009), (2117-2126), 0031-3203

Faundez-Zanuy, M. (2005). Signature Recognition – State of the art. IEEE Aerospace and Electronic Systems Magazine, Vol. 20, Issue: 7, July 2005, pp: 28- 32, 0885-8985

Gamboa, H. and Fred, A. (2004). *A Behavioural Biometric System Based on Human Computer Interaction*. Proceedings of SPIE Vol. 5404, pp. 381-392, 2004.

Herath, T. & Rao, H.R. (2009). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Science Direct Decision Support Systems Elsevier Ltd, Vol*. 47, No. 2, (February 2009) (154–165), 0167-9236

Hook, C., Kempf, J. & Scharfenberg, G. (2003) .*New Pen Device for Biometrical 3D Pressure Analysis of Handwritten Characters, Words and Signatures*. Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications , pp: 38– 44, 1-58113-779-6, Berkley, California, 2003, ACM New York, NY, USA

Huang, Y., Ao, X., Li, Y & Wang, C. (2008). *Multiple Biometrics System based on DavinCi Platform*. Proceedings of 2008 International Symposium on Information Science and Engieering, Vol. 2, pp.88-92, 978-1-4244-2727-4, Shanghai, China, December 2008, Institute of Electrical and Electronics Engineers (IEEE), USA

Jain, A.K., Griess, F., & Connell, S. (2002). On-line Signature Verification. *Science Direct Pattern Recognition Elsevier Ltd.* Vol.35 (2002) (2002) 2963 – 2972

Jain, A. K., Ross, A. & Prabhakar, S. (2004), An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, Vo1. 14, No. 1, (January 2004), (4–20), 1051-8215

Jain, A.K., Ross, A., & Pankanti, S. (2006) Biometrics: A Tool for Information Security. *IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 2. (June 2006), (125-143), 1556-6013

Kanneh, A. & Sakr, Z. (2008a). *Intelligent Haptics Sensing and Biometric Security*. Proceedings of ROSE 2008 – IEEE International Workshop on Robotic and Sensors Environments, pp.102-107, 978-1-4244-2594-5, Ottawa – Canada, October 2008, Institute of Electrical and Electronics Engineers (IEEE), USA

Kanneh, A. & Sakr, Z. (2008b). Biometric User Verification Using Haptics and Fuzzy Logic. Proceeding of the 16th ACM international conference on Multimedia, pp. 937-940, 978-1-60558-303-7, Vancouver, British Columbia, Canada, October 2008, ACM New York, NY, USA

Kanneh, A. & Sakr, Z. (2008c). *Biometrics Security in a Virtual Environment.* Proceedings of 18th International Conference on Artificial Reality and Telexistence 2008, pp. 203-209, Keio University, Yokohama, Japan, December 2008.

Kanneh, A. & Sakr, Z. (2008d). *A Haptic and Fuzzy Logic controller for Biometric User Verification*. Proceedings of CERMA 2008 Electronics, Robotics, and Automotive Mechanics Conference, pp. 62-67, 978-0-7695-3320-9 , Cuernavaca, Morelos, Mexico. Sept./ Oct. 2008, IEEE Computer Society Washington, DC, USA

Kraemera, S., Carayonb, P. & Clemc, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Science Direct Computers and Security Elsevier Ltd.*, (April 2009) (1 – 1 2), doi:10.1016/ j.cose.2009.04.006

Lee, L., Berger, T. & Aviczer, E. (1996). Reliable On-Line Human Signature Verification Systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 18, No. 6, (JUNE 1996), (643 - 647), 0162-8828

Lei, H. & Govindaraju, V. (2005). A comparative study on the consistency of features in on-line signature verification. *Pattern Recognition Letters Elsevier Science Inc.* Vol.26 No.15 (November 2005), (2483–2489), 0167-8655

Mansfield, T., Kelly, G., Chandler, D. & Kane, J. (2001). *Biometric Product Testing*. Final Report. Issue 1. Centre for Mathematics and Scientific Computing, National Physical Laboratory, March 2001, doi: http://www.cesg.gov.uk/policy_technologies/biometrics/media/biometrictestreportpt1.pdf

Martin, A., Doddington, G., Kamm, T., Ordowski, M. & Przybocki, M. (2007). *The DET Curve in Assessment of Detection Task Performance*. National Institute of Standards and Technology and Department of Defense, USA. doi: http://www.itl.nist.gov/iad/mig//publications/storage_paper/det.pdf.

McCabe,A., Trevathan, J. & Read, W. (2008). Neural Network-based Handwritten Signature Verification. *Journal of Computers,* Vol. 8, No. 3, (2008), (9-22)

Orozco, M. & El Saddik, A. (2005a). *Recognizing and Quantifying Human Movement Patterns through Haptic-based Applications*. Proceedings of IEEE International Conference on Virtual Environments, Human-Computer Interfaces and Measurement Systems, pp-, 0-7803-9041-5, July 2005.

Orozco, M., Shakra, I. & El Saddik, A. (2005b). *Haptic: The New Biometrics-embedded Media to Recognizing and Quantifying Human Patterns*. Proceedings of the 13th annual ACM international conference on Multimedia, pp. 387 – 390, 1-59593-044-2, Hilton, Singapore, 2005, ACM New York, NY, USA

Orozco, M. Graydon, S. Shirmohammadi & A. El Saddik. (2006a). *Using Haptic Interfaces for User Verification in Virtual Environments*. Proceedings of IEEE International Conference on Virtual Environments, Human-Computer Interfaces and Measurement Systems, pp. 25 – 30, La Coruña - Spain, July 2006. Institute of Electrical and Electronics Engineers (IEEE), USA

Orozco, M., Asfaw, Y., Shirmohammadi, S., Adler, A.& El Saddik, A. (2006b) *Haptic-Based Biometrics: A Feasibility Study*. Proceedings of the Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems, pp. 38, 1-4244-0226-3, 2006, IEEE Computer Society Washington, DC, USA

Orozco, M., Malek, B., Eid, M. & El Saddik, A. (2006c) *Haptic-Based Sensible Graphical Password*. Proceedings of Virtual Concept 2006, Playa Del Carmen, Mexico, Nov. / Dec. 2006, doi: http://www.discover.uottawa.ca/publications/files/VC2006Mauritz_V6.pdf

Orozco, M., Graydon, M., Shirmohammadi, S. & El Saddik, A. (2008). Experiments in Haptic-Based Authentication of Humans. *Springer Journal of Multimedia Tools and Applications*, Vol. 37, No. 1, (2008), (71-72), 1380-7501

Ortega-Garcia, J., Bigun, J., Reynolds, D & Gonzalez-Rodriguez. J. (2004). *Authentication gets Personal with Biometrics*. IEEE Signal Processing Magazine, Vol. 21, No. 2, pp. 50- 62, 1053-5888, March 2004.

Panko, R. (2004). *Corporate Computer and Network Security*. Pearson Higher Education. 0130384712, USA

Penagos, J.D., Prabhakaran, N. & Wunnava, S.V. (1996) *An Efficient Scheme for Dynamic Signature Verification*. Proceedings of the IEEE Southeastcon '96. 'Bringing Together Education, Science and Technology Department of Electrical & Computer Engineering, pp. 451-457, 0-7803-3088-9, Tampa, FL, USA, Apr 1996

Plamondon, R. & Srihari, S. N. (2000). On-line and off-line handwriting recognition: a comprehensive survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 22, No. 1, (January 2000), (63–84), 0162-8828

Roethenbaugh, G. (1997) *Biometrics Explained*. NCSA. Biometrics Editor 1997. Doi:http://www.incits.org/tc_home/m1htm/docs/m1050687.pdf

Salisbury, J.K. and Srinivasan, M. A. (1997). Phantom-Based Haptic Interaction with Virtual Objects. *IEEE Computer Graphics and Applications*, Vol.17, No. 5, (September 1997), (6 – 10), 0272-1716

Shan, A., Weiyin, R. & Shoulian, T. (2008). *Analysis and Reflection on the Security of Biometrics System*. Proceedings of IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08, pp. 1-5, 978-1-4244-2107-7, Dalian, Oct. 2008, Institute of Electrical and Electronics Engineers (IEEE), USA

Stallings, W. (2006) *Cryptography and Network Security*, Prentice Hall. 4/E . ISBN-10: 0-13-187316-4; ISBN-13: 978-0-13-187316-2, USA.

Vu, K-P. L., Proctorb, R., Bhargav-Spantzelb, A., Bik-Lam, T. , Cook, J, & Schultz,E. (2007). Improving Password Security and Memorability to Protect Personal and Organizational Information. *Science Direct International Journal of Human and Computer Studies Elsevier Ltd*, Vol. 65, No. 8, (April 2007), (744–757), 1071-5819

Wayman, J. 2000. *Technical Testing and Evaluation of Biometric Identification Devices*. Collected Works 1997-2000, August 2000 Version 1.2 National Biometric Test Centre, San Jose State University. doi: http://www.cse.msu.edu/~cse891/Sect601/textbook/17.pdf

Advances in Haptics

Edited by Mehrdad Hosseini Zadeh

ISBN 978-953-307-093-3
Hard cover, 722 pages
Publisher InTech
Published online 01, April, 2010
Published in print edition April, 2010

Haptic interfaces are divided into two main categories: force feedback and tactile. Force feedback interfaces are used to explore and modify remote/virtual objects in three physical dimensions in applications including computer-aided design, computer-assisted surgery, and computer-aided assembly. Tactile interfaces deal with surface properties such as roughness, smoothness, and temperature. Haptic research is intrinsically multi-disciplinary, incorporating computer science/engineering, control, robotics, psychophysics, and human motor control. By extending the scope of research in haptics, advances can be achieved in existing applications such as computer-aided design (CAD), tele-surgery, rehabilitation, scientific visualization, robot-assisted surgery, authentication, and graphical user interfaces (GUI), to name a few. Advances in Haptics presents a number of recent contributions to the field of haptics. Authors from around the world present the results of their research on various issues in the field of haptics.

IntechOpen