VECIMS 2006 – IEEE International Conference on
Virtual Environments, Human-Computer Interfaces, and Measurement Systems
La Coruña - Spain, 10-12 July 2006

Using Haptic Interfaces for User Verification in Virtual Environments

Mauricio Orozco, Matthew Graydon, Shervin Shirmohammadi and Abdulmotaleb El Saddik
Multimedia Communications Research Laboratory
School of Information Technology and Engineering, University of Ottawa
morozco@mcrlab.uottawa.ca, mgray08@uottawa.ca, {shervin, abed}@discover.uottawa.ca

Abstract – *Haptics can characterize the complex sense of touch and kinesthetic stimuli through its technology of force or tactile feedback devices. Such technology is developing fast enough to become soon another human-machine interaction similar to computer keyboard or mice. However, currently commercial haptics interfaces are expensive and are typically applied to research projects or expensive systems. Fortunately the trend of the market is forcing haptic developers to release products that can be affordable in a similar fashion as some specialized computer peripherals. Haptics aim is to allow a user to touch, feel, manipulate, create, and/or alter simulated three-dimensional objects in a virtual environment. Most of the applications are dedicated to train physical skills such as medical procedure by using desktop haptic units. These human skills can be captured to model a particular human-behavioural pattern that can be used to build a biometric recognition system. The precision of such systems is reliant on the choice of biometric identifiers. For accurate identity recognition, identifiers must be chosen so that they are unique for each individual. Conventional choices of biometric identifiers include writing style, hand geometry, as well as iris, facial, and fingerprint features. In this paper, we are interested in identity recognition based on humans' manipulation of haptic devices such as PHANToM™ [15]. The purpose of our analysis is to evaluate the information content of this data source. Hence, we assess the uniqueness of each biometric identifier. Our analysis shows that the haptic data content of identifiers is more suitable in a verification mode rather than in identification mode.*

Keywords – *Haptics, Biometrics, Virtual Environments*

I. INTRODUCTION

Haptic based systems, which allow processing of the human sense of touch, have been subject to research and development for the past few years in various applications such as tele-robotics, tele-operation, medical training, remote instrumentation, education, arts, and computer games. Although not currently in place, one can imagine sensitive Haptic based virtual environments in the near future, such as remotely operating a robot in a hazardous environment, say a nuclear reactor, or tele-operating a shuttle in space. User authentication and verification is clearly necessary in such sensitive applications. Currently, Haptic-based virtual environments use traditional authentication methods such as passwords. Recently, however, Biometric systems, which identify users based on behavioral or physiological characteristics [20], have been gaining ground in terms of usage. The advantages of Biometric systems over traditional authentication methods such as passwords are well known. For example, there are systems already in place recognizing people based on their fingerprint, voice, iris, or face image. Applications for such systems are vast, and range from national security applications to access control and authentication. Following this trend, the idea of using Haptics as Biometrics instruments has recently been proposed [2] [10] [11]. The advantage of such a method is two-folds: first, because of the biometric characteristic of the method, one can expect advantages over traditional authentication methods. Second, since the haptic device is already part of the hapto-virtual environment, there is no additional hardware overhead. In fact, one can use the Haptic device in the application to continuously authenticate the user and not just at the beginning of a session - a feature that does not exist in other systems.

In this article, we present our verification system for such haptic virtual environment. A haptic maze application is built on an elastic membrane surface (see Fig. 3). The user is asked to navigate the stylus through the maze, which has sticky walls and an elastic floor. Such a task allows many different behavioral attributes of the user to be measured, such as reaction time to release from a sticky wall, the route, the velocity, and the pressure applied to the floor. This is not too unlike a handwriting recognition application [14] [16] [12], except there are more parameters available from a Haptic device. Using this application, we demonstrate that verification, which calculates the probability of a user being X given the user claims to be X, gives a much higher certainty percentage than authentication, which simply tries to match a user's profile to all existing profiles.

II. HAPTIC-BIOMETRICS

The introduction of haptic technology to the security systems to authenticate individuals has received very little attention. Recently, it has been shown that identity recognition based on human-haptic interactions is feasible [10] [2]. The problem with the proposed methods so far is that they have a successful authentication rate of about 78% [10] and at the most 80% [11]. This is far from what is needed to have a practical and reliable authentication system. From the characteristics of the experimental set, these approaches have been mostly based on traditional behavioral biometric systems, such as keystroke dynamics, speaker recognition and dynamic signature verification. In the past two decades, keystroke analysis research has been studied and characterized by features that describe the writing and tipping dynamics actions [3]. The Main advantage of

keystroke dynamics in terms of biometric implementation is that it can be performed with the use of a non-specialized device, such as a keyboard, as a mechanism of input of behavioural information. Pioneering studies have been done in this domain by adopting different approaches in terms of analysis [4][19]. However they based their studies only on measurable quantities such as keystroke durations and latencies between pair of characters called *digraph* (two keys typed one after the other). In these systems, typing a long paragraph was required to capture the state of the system, making it an impractical application. Later improvements were suggested in terms of practicability and performance [5] [8] [9]. Joyce and Gutpa modified the experimental set based only on asking participants to type features such as username, surname, last name and password. In a similar fashion, Obaidat and Sadoun analyzed a login name input based on keystroke duration and latency features and claimed outstanding performance. However people tend to have difficulty remembering long passwords, for example. Therefore, this tendency makes people choose short passwords hence making the system more vulnerable according to security principles. In terms of dynamic signature verification, which is a subclass of handwriting recognition, plenty of research has been performed in the last three decades [16]. Commercial applications in this domain can be found in devices such as pen-based computers, PDAs, and digital tablets. An extensive spectrum of approaches has been tested with the aim to exploit the singular, exclusive, and personal character of the writing [16].There is however a well-established set of work that has been surveyed in [6] and [16]. Among the methods that can be applied to pattern recognition, dynamic time warping (DTW), spectral analysis (FFT), and analysis of temporal features such velocity, force, angle function and pressure systems have been studied [16]. Our study is based on such methodologies at the analysis level but it extends the concept by exploiting the use of using the programmable bi-directional interface for output information (haptics). The exchange of energy between user and computer through these haptic interfaces relies on a complex mechanism that delivers information in terms of haptic perception. In virtual environments, haptic perception provides the user with valuable perceptual information and allows performing diverse manipulation tasks in a very realistic scenario. In addition it can be a good candidate set for capturing more physical parameters than current systems such as computer mouse, digital tablets, pen-based computers and keyboards, which cannot handle obtaining a biometric template for each user. The proposed system captures parameters such as the user's force, exerted as a response to interaction with a synthetic modeled surface, the speed, and the pen's position at any time during the haptic training. Such features can be treated as hidden variables in the data registration process to produce a more robust system to avoid a great variety attacks.

III. SYSTEM OVERVIEW

The architecture that characterizes our proposed system follows the general authentication process for biometric systems. It is comprised of five core subsystems: *haptic based applications, behavioural data repository, feature generation, feature selection, and classifier design*. As we can see in Figure 1, in the haptic-based applications subsystem, there is a set of software applications. In other words, tasks are defined where haptics deliver an appropriate human-sensor system interface for capturing a person's behavioral characteristics (***f(B)***). This subsystem can be seen as an object oriented framework which is in charge of handling the graphical environment and its integration with haptic application interfaces from the haptic devices [15][17]. The behavioural data repository subsystem manages the recording, storing and updating about all haptic output information generated in the haptic-computer-human interaction in an unprocessed format. After acquisition, the data is handed to the feature generation subsystem (*FGS*). Here, a quantitative characterization of the state of the haptic system is formed (***B***). The system's state properties are described by an array of vectors, each corresponding to different features to be analyzed. In addition, within the *FGS,* a preprocessing task is required before data is ready to be processed in the feature selection processes. Outliner removal, data normalization, and missing data detection are accomplished via this preprocessing interface. The feature selection subsystem manages the next procedure, called feature selection, to receive a given number of features and select those of the greatest user-classificatory value. Using relative entropy, reduction of state vector dimensionality is achieved; and using chi-squared tests, features are extracted. For authentication, a set of biometric algorithms can be used in the classifier design procedure.

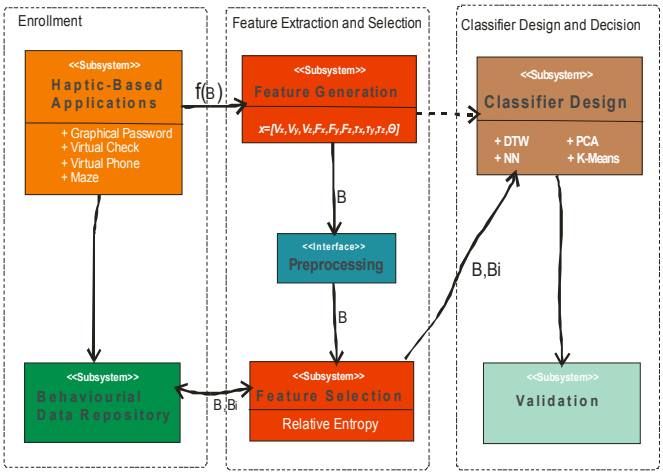

Figure 1: Overall architecture of verification system using haptics to identify human movements' patterns

From a great variety of pattern recognition methodologies, we have chosen the well-known Fast Fourier Transform (FFT) spectral analysis approach with definition of matching score as a metric to classify haptic user feature vectors extracted from raw data that characterize their psychomotor patterns. This final component of the system process results in an authentication decision based upon match score metrics between $\boldsymbol{B}$ and $\boldsymbol{B_i}$, where $\boldsymbol{B_i}$ is associated with the template that represents the credentials of an enrolled identity in the behavioural data repository.

A. Data Acquisition

The performance results reported here are based on a database of profiles collected over a period of 4 weeks. The collected data used complete time functions as parameters. The haptic-based application subsystem provided direct access to the tracking device through an application-programming interface registering events such as $\boldsymbol{xyz}$ position, stylus' orientation ($\boldsymbol{\Theta}$), time ($\boldsymbol{t}$), force ($\boldsymbol{F}$) and torque ($\boldsymbol{\tau}$). The haptic-based application involved the participant completing a flat 2D maze placed on one surface of a 3D cube. To eliminate the "training effect", participants were given the opportunity to practice with the maze before the trials were actually recorded. Since there is only one correct path through the maze and the ability to solve the maze was not being judged, it was important to ensure participants knew how to correctly solve the maze in advance. The final set of data was stored in Comma Separated Values (CSV) formatted text files with one file per participant, per trial. An example of three users' profile of representing the average angle of the pen's rotation is shown in the Figure 2.

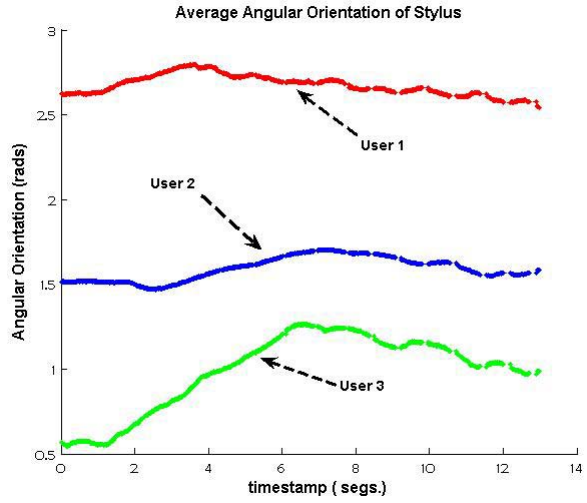

Figure 2. Profile of the angular rotation performed for three different users during the navigation process on a virtual maze.

An *essential assumption* in this study is that there is natural differences between the psychomotor patterns exhibited by individuals in virtual environments with haptic stimuli. As can be seen from figure 2, one can discriminate the particular way the haptic device is handled among a portion of the population (three users in this sample), characterized by angular rotation of the stylus. At first glance, it seems that using a primary-order statistic provides a valuable cue about the behaviour that characterizes each participant. But, it cannot guarantee the uniqueness of each biometric identifier if for example two users have similar mean value angular orientation. However, if the variance of user A's angular orientation is greater that that of user B, more information is contained in user B's angular orientation distribution. As we later will show using relative entropy [1] [7], user B is more unique that user A, and so we get more information from the behaviour of user B. In addition relative entropy is the best approach because it tells us how much information we get about someone's identity if we assume that they are all the same.

B. Haptic-Based Application

The haptic application was developed using the Reachin® system and its API [17], which captures raw data (see figure 3). The haptic software applications were developed in a combination of VRML-based scene and Python scripting programming language. The VRML-nodes create the 3D virtual environment, while the Python scripting programs provide the procedural method to handle and process events and provide data output to a file. The haptic stimulus is provided by accessing Reachin's special API, which handles the complex calculations for the touch simulation and its synchronization with the graphic rendering, all in the haptic loop process.

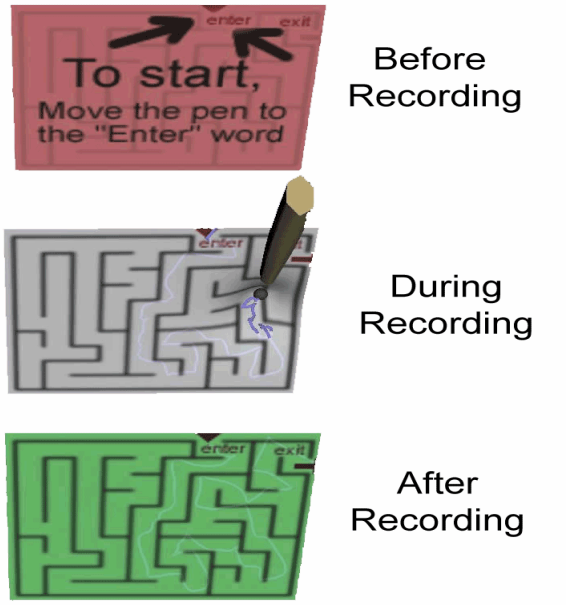

Figure 3: Screenshot of a virtual check application. The user is required to perform his/her hand written signature by using the haptic stylus in the area selected

C. Experiments

As part of this study, different participants were used to complete multiple trials of the same experiment with the haptics pen. The experiment involved the participant completing a flat 2D maze placed on one surface of a 3D cube. The raw values obtained from different participants completing the maze were then analyzed to look for similarities of characteristics between different trials of the same person and differences of characteristics across different people. In this haptic maze built on an elastic membrane surface, the user was asked to navigate the stylus through it (see Figure 3). The pen's position, force exerted, and velocity among other attributes were computed from the haptic-based application and provide the input to obtain the user's interaction patterns. The haptic-based application was used as a mean of testing individual's abilities and describing a psychomotor pattern through the selected task. A total of 39 different participants' movements were captured for the purposes of the analysis. The 39 participants were divided into two groups. Group one was comprised of 22 users where each person performed the exact same maze 10 times, one trial immediately after the other. The second group of users did the same test, except that this group was subjected to stress related to ask user to perform the maze trial like password during their last four trials. Again, it should be noted that the participants were given the opportunity to practice the maze before the trials were actually recorded.

IV. FEATURE EXTRACTION AND SELECTION ALGORITHM

Haptic systems can provide us with information about direction, pressure, force, angle, speed, and position of the user's interactions. In addition, all of the above features are provided in a 3D space covering width, height, and depth. This information can be used to verify a user. To maximize the precision of identity verification, we utilize features of optimal uniqueness; thus, permitting distinct characterization of an individual's interaction. Such features contain the most information pertaining to identity.

A. Haptic System State

To describe the state of a system, we first construct a vector $\boldsymbol{x}$ that provides a quantitative characterization of the system's features at some moment in time. For a dynamic system, there exists a set $\boldsymbol{X}$ of all state vectors with a finite, non-zero probability of measurement. The definition of X assumes the existence of a probability distribution function:

$$f : X \to (0,1] \tag{1}$$

Via the formulation of $\boldsymbol{f}$, we define the probability of measuring a system to be in some unique state $\boldsymbol{y}$, as:

$$f(x = y) \tag{2}$$

Therefore the state of the haptic system is represented by measurements of a set of physical attributes such as velocity ($\boldsymbol{v}$), force ($\boldsymbol{F}$), torque ($\boldsymbol{\tau}$), and angular orientation of the haptic end effector ($\boldsymbol{\theta}$). In our case the feature vector is:

$$x = [v_x, v_y, v_z, F_x, F_y, F_z, \tau_x, \tau_y, \tau_z, \theta]^T \tag{3}$$

where $\boldsymbol{T}$ denotes transposition. Each of the features vectors identifies exclusively an individual pattern movement.

B. Information Content: Relative Entropy

In order to evaluate the quality of the measurements in terms of providing valuable biometric information, we recurred to the information theory to select the Kullback-Leibler divergence as metric of evaluation. It has been applied mainly to formulate hypothesis tests or as metric for designing detectors [5]. In a discrete space, we assume $\boldsymbol{X}$ to be a discrete random variable with $\boldsymbol{p(x)}$, $\boldsymbol{x \in X}$ and $\boldsymbol{q(x)}$, $\boldsymbol{x \in X}$ to be two mass probability functions, therefore the Kullback-Leibler (KL) distance, also called relative entropy, can be defined as the expected value of the likelihood ratio between $\boldsymbol{p(x)}$ relative to $\boldsymbol{q(x)}$:

$$D(p \,\|\, q) = \sum_{x \in X} p(x) \log \frac{p(x)}{q(x)} dx \tag{4}$$

We can think of $\boldsymbol{D(p\|q)}$ as describing the "distance" of $\boldsymbol{q}$ from $\boldsymbol{p}$. The term "distance" is not intended to be taken in its most literal sense, since $\boldsymbol{D(p\|q)}$ is not a true metric. Indeed, $\boldsymbol{D(p\|q) \neq D(q\|p)}$ in the general case. From an information theory viewpoint, we interpret $\boldsymbol{D(p\|q)}$ as a measure of how much information is contained in the assumption of a distribution $\boldsymbol{p}$ on $\boldsymbol{X}$, when the distribution is actually $\boldsymbol{q}$ on $\boldsymbol{X}$ [1]. By definition, $\boldsymbol{D(p\|q): D(p\|q) = 0 \leftrightarrow p = q}$ [7]. This result indicates that no information is gained by correctly assuming that the distribution is $\boldsymbol{p}$.

The choice of a logarithmic base used in the integration of $\boldsymbol{p(x)\ log\ (p(x)/q(x))dx}$ corresponds to the units used to measure information [13]. In our study, we choose $\boldsymbol{\log_2}$, yielding information measurements in 'bits.' This choice suits the potential application of our findings to a system where information is also measured in bits.

The Kullback-Leibler distance, or relative entropy, gives us a mechanism to extract the most informative features from the observable feature space (OFS). Given probability

distributions ***p*** and ***q*** on various subspaces of the OFS, calculations of the relative entropy between ***p*** and ***q*** assess the uniqueness different observable features. We form ***p*** to model the general, intra-personal distribution; whereas, we construct a unique ***q*** distribution for each user. Indeed, the relative entropy between ***p*** and ***q*** is then interpreted as the amount of information contained in the assumption of a distribution ***p*** on the OFS, when the actual distribution is ***q*** [1].

The mean vector, **μ**, and covariance matrix, ***cov***, are used to characterize a Gaussian probability distribution ***f*** on **X**. For an arbitrary dimension ***'n'*** of all $x \in X$, $\mu = (E[x_1], E[x_2] \ldots E[x_n])$ and $cov_{ij} = cov(x_i,x_j) = cov(x_j,x_i)$. If we define two Gaussian distributions ***p*** and ***q*** on **X** then the relative entropy measured in bits is:

$$D(p \,\|\, q) = \frac{1}{2}\log_2\left(\left(\frac{\mathrm{cov}_p}{\mathrm{cov}_q\, e^{trace((\mathrm{cov}_p + (\mathrm{cov}_p - \mathrm{cov}_q)^t (\mathrm{cov}_p - \mathrm{cov}_q))}\, \mathrm{cov}^{-1}{}_q - I}\right)\right) \tag{5}$$

In (5), subscripts refer to the distributions ***p*** and ***q***, and ***I*** refers to the identity matrix of rank ***n***[1]. Via the selection of the observable features that maximize eq.5, we form the feature sets used for identity verification.

V. EXPERIMENTAL RESULTS: CLASSIFIER DESIGN AND DESCISION

The construction of biometric profiles is accomplished through the spectral analysis of the raw feature signals. The raw data sets consist of six-dimensional state vectors obtained by sampling the OFS at a rate of 70 samples/second. For each dimension of the state vectors, there is the associated biometric feature, e.g. 'force in the z direction'. To process the raw feature signals, we use windowed discrete time Fourier transforms. First, we apply a hamming window of length 256 with 128 non-overlap points. The given coefficients of the window allow us to optimize transition width with respect to maximum attenuation according to the following:

$$w(n) = 0.54 - 0.46\cos(\pi n / 128) \tag{6}$$

After the window is applied, the Fast Fourier Transform (FFT) of each signal is taken. As a result, the raw signals are transformed into a 256x6 matrix, whose 6 columns are associated with distinct biometric features. We refer to this matrix as the biometric profile. The relative entropy feature extraction mechanism and the spectral profile constructor permit the development of a generalized identity verification system. The decision policies of such systems vary with their application context. We are interested in high-security applications of haptic biometrics; hence, our test users' are first trained, and then given only a single authentication attempt. An attempt allows us to form a sample biometric profile. This sample is compared to pre-stored template profiles. Each template profile is associated with a specific identity. For each identity, we pre-store three templates taken from prior behavioural observation. Comparisons between the sample profile and the templates associated with the claimed identity produce a quantitative verification Match Score (MS) according to eq.7 below:

$$MS = \ln((\| d1_{i,j} \| - \| d2_{i,j} \|)^2) \tag{7}$$

In eq.7, '***ln***' denotes the natural logarithm and $\|d1_{i,j}\|$ denotes the complex norm of the ***(i,j)th*** element of biometric profile 1. The summation indices cover the number of features, 6, and the length of the windowed signals, 256. By definition, a low MS implies a small difference between two profiles, while a high MS implies a large difference. Essentially, the MS measures the separation between two biometric profiles. By establishing a threshold MS, we place an upper-bound on acceptable match scores. The threshold match score need not be common for each user. We study the effect of establishing user-dependent thresholds, and our results, presented next, indicate this approach is most favourable.

Using our relative entropy feature selection criteria, we choose 3D force and torque data for verification implementations. Samples from the 3D force and torque OFS subspaces contain, on average, 14.7 and 12.4 bits of information respectively. Our calculations indicate other features, such as velocity, contain much less information, with content measures on the order of 3 bits. To evaluate the performance of the verification system, we employ data gathered during 39 users' interactions with the maze application. The data gathered from their first six attempts is disregarded to diminish the training effect. The template profiles are formed based each user's seventh, eighth, and ninth trials. As sample profiles, we use data from each user's last maze completion. As previously mentioned the second set of data is submitted to a stress test.

The stress is induced by asking the participants to 'treat their behaviour like a password'. Each user in group 2 is given an explicit list of the features being captured to monitor their behaviour, and they are asked to consider these features in their attempt to 'solve the maze in the same way each time'. Remarkably, identity verification of users from group one is more accurate, as shown in figure 4 on the next page. The users subjected to stress exhibit a greater variance in their characteristics, and are falsely rejected nearly 66% of the time at 25% False Accept Rate (FAR). This result suggests the translation of identity into the virtual world need

not be a deliberate effort. Using a common threshold (CT) for acceptance does not provide the flexibility required to admit genuine users who demonstrate significant variance in their behaviour. So, we test verification system employing user-dependent thresholds (UDT). As shown in Figure 4, the choice of a user-dependent MS improves system performance, allowing for a significant increase of Probability of Verification PV for FAR > 0.15. Figure 4 also displays a receiver operating curve depicting the performance of an identification system. The test users of the identification system are not exposed to stress. Minimum intra-template match scores are determined using three biometric profiles of each user. On average, only 5% of imposter profiles produce these minimum match scores; however, such an analysis of system performance assumes the allowance of multiple authentication attempts. To explore the potential high-security continuous verification applications of haptic biometrics, we also evaluate scores generated in real-time. In this case, the probability of verification is at best 90.5% at 25% FAR using spectral analysis. If we also consider the global feature of total solving time, the results improve dramatically to 95.4% PV at only 16% FAR.

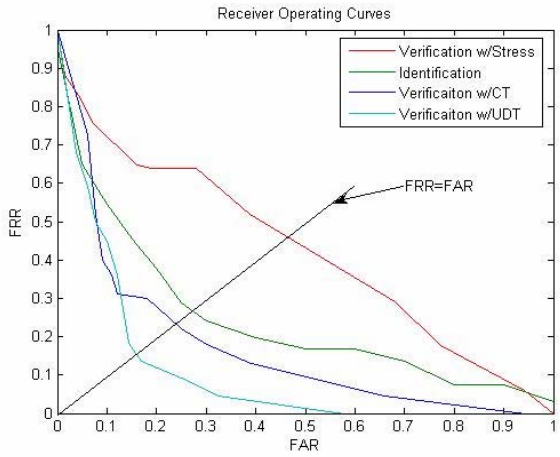

Figure 4 Performance of the majority classifier over the three different applications

VI. CONCLUSIONS AND FUTURE WORK

The biometric features chosen for our analysis all contain information about each user. The amount of information contained in an individual's features characterizes the uniqueness of that individual. Furthermore, via the analysis of a user's entropic signature, we answer the question 'in what way is this user unique?'. In addition, our findings suggest the design of a biometric recognition system based on the analysis of entropic signatures calculated from data collected from human-haptic interaction is feasible.

Our results imply haptic biometrics are best suited for verification purposes; yet, a simple maze application does not provide optimal conditions for virtual identity authentication. We have begun an analysis of Observable Feature Space (OFS) data gathered while users where asked to sign a "virtual cheque". Our preliminary results show that with this application, the probability of verification is around 98.4%. This leads us to believe certain applications furnish better opportunities for an optimal pronunciation of one's virtual identity.

REFERENCES

[1] A. Adler, R. Youmaran, S. Loyka "Information Content of Biometric Features", Proc. Biometrics Consortium Conference 2005, Ottawa, ON, Canada, September 2005.

[2] Y. Asfaw, M. Orozco, S. Shirmohammadi, A. El Saddik, A. Adler, "Participant Identification in Haptic systems using Hidden Markov Model", Proc. IEEE Workshop on Haptic Audio Visual Environments and their Applications, Ottawa, ON, Canada, October 2005.

[3] F. Bergadano, D. Gunetti, and C. Picardi. "User authentication through keystroke dynamics". ACM Transactions on Information and System Security (TISSEC). Volume 5, Issue 4 (November 2002)

[4] R. Gaines, W. Lisowski., S. Press, and N. Shapiro, "Authentication by keystroke timing: Some preliminary results". Rand. Report R-256-NSF. Rand Corporation.1980

[5] R. Joyce and G. Gupta, G. 1990. "User authorization based on keystroke latencies". Commun. ACM 33, 2, 168–176.

[6] F. Leclerc and R. Plamondon, "Automatic Signature Verification: The State of the Art, 1989-1993", International Journal of Pattern Recognition and Artificial Intelligence, special issue signature verification, vol. 8, no. 3, pp. 643-660, 1994.

[7] M. Lexa, "Useful Facts about the Kullback-Leibler discrimination distance", Houston, Texas, 2004

[8] F. Monrose, A. Rubin," Authentication via Keystroke Dynamics". 4th ACM Conference on Computer and Communications Security, April 1997

[9] M.S. Obaidat and B. Sadoun, "Verification of computer users using keystroke dynamics". IEEE Trans. Syst. Man, and Cybernet. Part B: Cybernet. 27, 2, 261–269.1997

[10] M. Orozco, Y. Asfaw, A. Adler, S. Shimohammandi and A. El Saddik. Automatic Identification of Participants in Haptic Systems/ IMTC 2005-Instrumentation and Measurements Technology Conference, Ottawa, Ontario, Canada, 17-19 May 2005

[11] M. Orozco and A. El Saddik, "Haptic: The New Biometrics-embedded Media to Recognizing and Quantifying Human Patterns" In proceedings of 13th Annual ACM International Conference on Multimedia (ACM-MM 2005), Singapore, November 06-12, 2005.

[12] T. Qu. A, El Saddik, A. Adler, "Dynamic Signature Verification System Using Stroke Based Features", IEEE Int. Workshop on Haptic Virtual Environments and their Applications, Ottawa, Canada, Sept. 2003. pp. 83-88

[13] I.T.Nabney. "Algorithms for Pattern recognition". Advances in Pattern Recognition, Springer 2002. ISBN 1-85233-440-1.

[14] V. S. Nalwa, "Automatic on-line signature verification" Proc. IEEE, Vol. 85: Issue 2, Pages 215-240, Feb, 1997.

[15] PHAToM & GHOST : http:// www.sensable

[16] R. Plamondon, S.N. Srihari, "On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey" IEEE Trans. Pattern Analysis and Machine Intelligence, 22: 63-84, 2000

[17] Reachin Technologies, User's Programmers Guide and API http://www.reachin.se/

[18] C. E. Shannon, "A Mathematical Theory of Communication", 1994

[19] D. Umphress. and G. Williams, "Identity verification through keyboard characteristics". Internat. J. Man-Mach. Stud. 23, 263–273.1985

[20] J.L. Wayman, "Fundamentals of Biometric Authentication Technologies", Proc. Card Tech/Secure Tech, 1999. http://www.engr.sjsu.edu/biometrics/nbtccw.pdf