Biometrics Security in a Virtual Environment

Andrea Kanneh, Ziad Sakr
School of Information and Communication Technology,
University of Trinidad and Tobago

Abstract

Security is a genuine concern with many applications. This paper reports a study of an intelligent haptics security system. The study evaluates the accuracy of user verification with the use of a haptics device on a virtual surface. A fuzzy logic controller is used for the decision making module. The system is simple and yet very effective. It can be used for access control applications such as access to data within organizations or incorporated within a virtual 3D game for access to a player's secrets.

1. Introduction

The study combines the use of three areas – haptics, biometrics and fuzzy logic.

1.1. Haptics

Haptics means pertaining to the sense of touch This area can be used to enhance virtual reality for the user as it adds another dimension to the user's experience – it provides touch access to virtual worlds. 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 [1]. Haptics also includes the study of movement and position (kinesthetics). This, together with tactation allows haptic applications to offer both spatial and temporal information.

Passwords, as a form of security, can be frustrating to remember and users tend to use the same or similar passwords for different accounts, thus lowering the effectiveness of the security system [2]. The use of Haptics instead of passwords makes it easier for the user and safer for the organization and makes the user interaction more seamless within a 3D scene.

Haptic interfaces enable manual interactions with virtual environment. The authors Salisbury and Srinivasan [3] highlight some desirable characteristics of haptics devices. They include minimal constraints on motion imposed by the device, low inertia and friction, and a balanced range of position sensing and force reflection.

The PHANToM (The Personal Haptic Interface Mechanism) http://www.reachin.se/ [4] device allows the user to literally feel virtual objects in a 3D space (see Figure 1). It is easy to manipulate with its stylus grip or a fingertip thimble. This device is able to extract data such as velocity, force, angular orientation of the stylus as well as the xyz coordinates all of which can fall under the heading of behavioral biometrics. The PHANToM is one of the components of the Reachin device/display (Figure 1) [5]. The Reachin API uses object oriented technologies in C++ and is based on the VRML programming.

Through the Reachin API velocity, force, torque and angular orientation of the haptic device are key biometrics that can be extracted. While, without a haptics device, it is possible to accurately copy the shape drawn by a user, it is difficult to mimic the differences in force applied around the shape. This makes the biometrics extracted with the haptics device very hard to accurately copy. Another advantage of using the Reachin device is that it can be incorporated into a 3D scene.

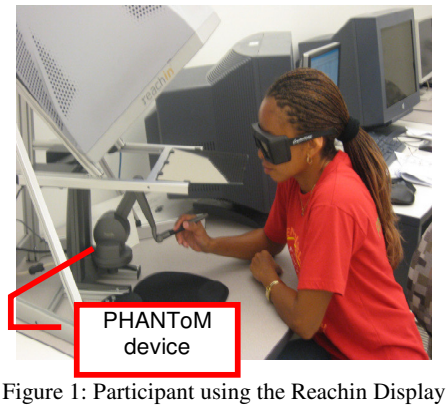


Figure 1: Participant using the Reachin Display
http://www.reachin.se/

1.2. Biometrics

Biometrics is a technique of authenticating individuals

based on their physiological or behavioral characteristics [6]. Physiological techniques are based on something you are. Examples include fingerprint recognition, iris recognition, face recognition and hand geometry (finger lengths, finger widths, palm width, etc.). Behavioral techniques are based on the things you do (a trained act or skill that the person unconsciously does as a behavioral pattern [7]). Examples include voice recognition, keystroke recognition (distinctive rhythms in the timing between keystrokes for certain pairs of characters), and signature recognition (handwriting or character shapes, timing and pressure of the signature process). Biometric systems aim to use measures that are both distinctive and repeatable [8].

Biometric security has existed since the beginning of man – recognizing 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; fingerprint scanning has been around since the late 1960s [9].

Biometrics authentication can be used for both verification and identification. For user verification, the subject claims to be a specific person and a one-to-one comparison is done. For identification, the applicant's data is matched against all the user templates stored in the entire database, to determine his/her identity. This is a one-to-many task. The system presented in this paper is used for verification.

Biometric systems present some variability which is partly due to human inconsistency. This inconsistency can be influenced by the many factors including user stress, fatigue, the time of day, the user's mood and environmental conditions [10].

Two key measures used for Biometric systems are False Accept Rate (FAR) and False Reject Rate (FRR). False Accept Rate (FAR) is the percentage of applicants who should be rejected but are instead accepted. False Reject Rate (FRR) is the percentage of legitimate users who are denied access or rejected.

1.3. Fuzzy Logic and Computational Intelligence

Computational Intelligence CI is an emerging concept of information processing aimed at the design of intelligent systems [11]. One area of computational intelligence is fuzzy logic.

Fuzzy logic is a form of soft computing. Unlike classical set theory where there are crisp boundaries, a fuzzy set is a set without crisp boundaries. This allows for imprecision and flexibility in a decision-making system. Fuzzy logic facilitates the variability inherent in biometric systems by the use of membership functions. This concept allows the user to totally or partially belong to a set.

A fuzzy set can be expressed with the following equation (Eq. (1)):

$$F= \{x, \mu F(x) \mid x \in X\} \quad (1)$$

Where X is the universe of discourse (all possible values for a specific feature within the system) and its elements are denoted by x. $\mu F(x)$ is called the membership function (or MF) of x in F (for example Very Fast, Fast, and Moderate shown in Figures 2, 3). μ can take the values $0 < \mu < 1$ when there is partial membership (Figure 2) or μ can take the value of 1 when there is total membership (Figure 3), or $\mu = 0$ when there is no membership [12,13,14].

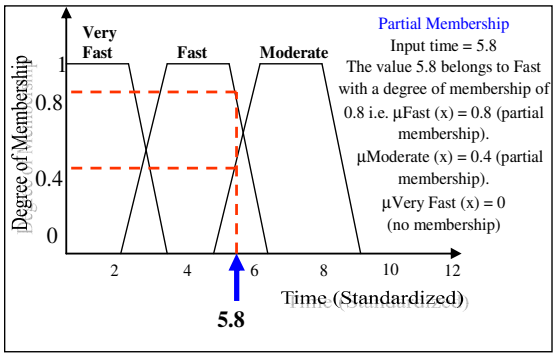


Figure 2: Partial Membership - Fuzzy logic membership functions

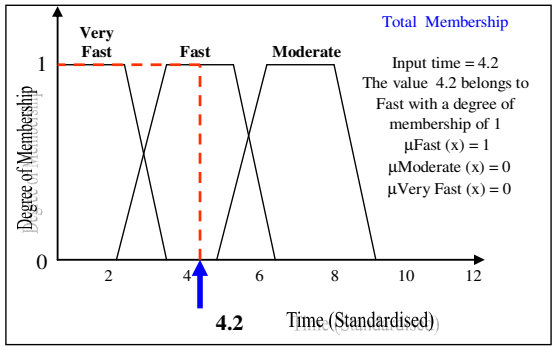


Figure 3: Total membership Fuzzy logic membership functions

2. Related Work

C Hook et. al. presented a study of a biometrical smart pen BiSP [15]. 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. In this study the user does not actually feel a virtual surface in a computer; it is the pen itself that

captures all the measurements.

The combination of haptics and biometrics is relatively new [16, 17, 18, 19, 20, 21]. In these papers Orozco et. al. presented several applications including studies with a virtual phone, maze and virtual check. Each application captured similar measurements such as force, time and momentum through the Reachin API and each proved to be very effective. Accuracy ranged from 80% [18] to 95.4% [20] with some initial findings showing the possibility of reaching accuracy as high as 98.4% [20].

As with Orozco et. al. [16, 17, 18, 19, 20, 21] this study presents a new algorithm for user verification. In this study a fuzzy logic controller is used to mimic human reasoning in decision making.

3. The haptics and biometrics verification system

A typical biometric system comprises two stages – user enrollment and authentication (user verification and/or identification) (Figure 4). In the enrollment stage key features, which can be used to distinguish each user, are captured and stored. In this system fuzzy membership functions are created and knowledge base templates are stored on each user. In the second stage – authentication – test data are compare to the stored templates and a decision is made to accept or reject the applicant.

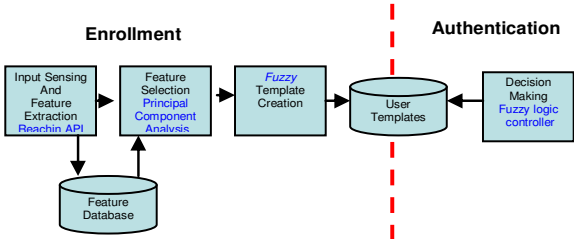


Figure 4: Typical biometric system

3.1. Input sensing and the virtual surface

The Reachin Display (http://www.reachin.se/) was used to capture key biometric features from each user (see Figure 1). The user used the PHANToM stylus to trace the circle shown in Figure 5. The system captured twenty three data features at a rate of 2200 measures per second. These features include data on force, angular momentum, average radius, time and xyz distances. This data was stored in a feature database.

Similar to the work done by Orozco et al. [16] at the University of Ottawa, the users were first given some time to familiarize themselves with the Reachin apparatus and the application.

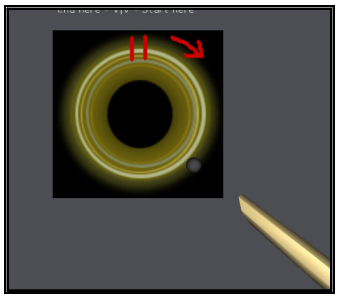


Figure 5 - Virtual surface for user verification

3.2. Feature selection

Feature selection aims to capture those features which could identify the uniqueness of each subject. Principal Component analysis (PCA) was used to select those features that showed the least correlation. From the twenty three features that were originally extracted seven were chosen. They included Force at different Positions, average radius (size), xyz distances and Time.

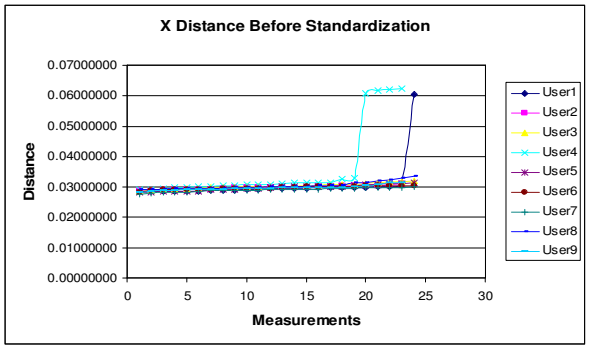


Figure 6: Measures viewed without standardization

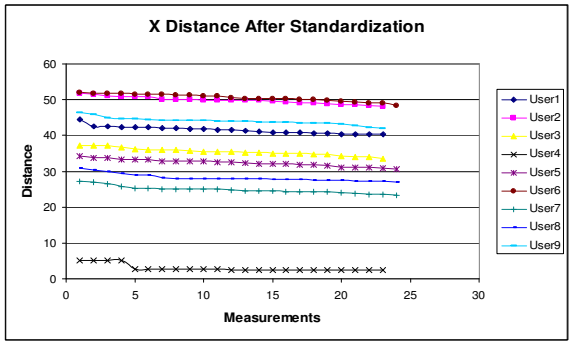


Figure 7: Measures viewed after standardization

The data was then standardized and sorted to be grouped and assigned to fuzzy membership functions. By standardization, the data was easier to separate for

classification (Figures 6, 7). Standardization was achieved by dividing each feature measurement by the standard deviation for that feature of each user.

3.3. Template creation and decision- making with fuzzy logic

The following diagram shows the typical fuzzy logic process (Figure 8).

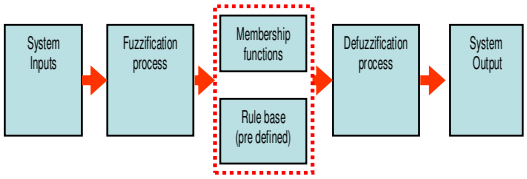


Figure 8: Fuzzy logic process

The input (user data) first goes through a Fuzzification process where each input is assigned to one or more predefined membership functions with a degree of membership (Figure 9; See also Figures 2,3).

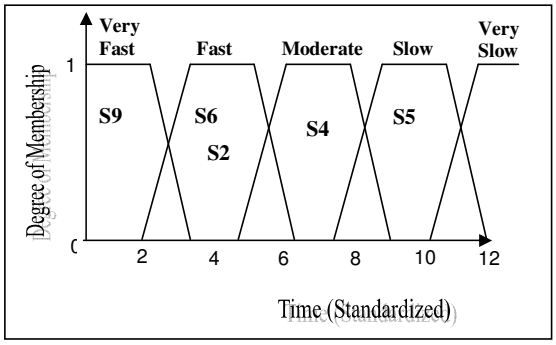


Figure 9: The overlapping membership functions with some users assigned

IF-THEN rules (the Rule Base) are then created to combine these degrees of membership for different features, to assign the output to a specific user. Each rule can be given a weight to show the strength or influence of that particular rule on the output of the system. The rules generally take the following form [12] (Eq. (2)). The default weight is 1.

If (condition or antecedent) then (action or consequence) weight w_i ***(optional)*** (2)

The following is an example of one of the many rules from our haptics and biometrics verification system.

If Force is Weak and YDistance is Large and Time is Fast and Size is Small then Output is User 2 weight 0.6

Note that Time is the time taken to complete the circle and Size is the average radius drawn.

The fuzzy output tends to overlap. The process of converting the fuzzy output to a scalar value is called defuzzification. Based on the strength of membership of each fuzzy output a crisp result can be derived. Defuzzification was done using a Weighted Average technique. The Sugeno inference method was used. In this method each user's output value is mapped to a constant (unlike the Mamdani method where the user output is assigned to a range of values). The output was calculated with the following equation (Eq. (3)).

$$Output = \frac{\sum_{i=1}^{n} \mu(O_i) c_i}{\sum \mu(O_i)} \quad (3)$$

Where c_i represents the predefined constant used to represent each user and $\mu(O_i)$ represents the degree of membership evaluated.

4. Results

Table 1 - Subject and Imposter verification accuracy

Subject	Subject Verification %	Imposter Verification %
1	90	100
2	100	100
3	90	98.07
4	90	84.61
5	100	100
6	100	96.15
7	100	75
8	100	92.3
9	90	82.69
Average	**96.25**	**91.10**
FRR	**3.75**	
FAR		**8.90**

This paper presented a user-friendly haptics and biometric security system. The results show that the system is very effective at user verification. The table

above (Table 1) shows a summary of the results for each of the 9 subjects.

The Sugeno fuzzy inference method resulted in 96.25% accuracy. Imposter verification for each user was calculated by comparing all imposters' data to the template of each particular user.

Imposter verification produced a success rate of 91.1%.

5. Discussion

Dhamija and Dusseault [22] suggest that users are more likely to accept a security system if it is simple to use. This proposed security system provides a simple virtual surface for the user to trace (Figures 1, 5). Key strengths of this security system include a simple interface, a systems that caters for human variability and a system capable of being integrated with an existing application.

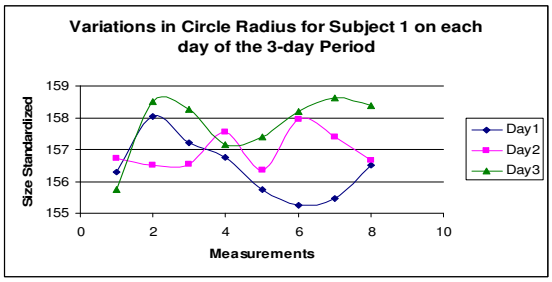
Ten computer engineering students were tested. All students were familiar with the Reachin Display (http://www.reachin.se/.) [4, 5]. Each student was asked to complete each set of trials on separate days. This process was carried out over a three day period to cater for the human variability [10] as well as the learning and aging process put forward by Mansfield et. al. [23]. One subject was unable to complete all three trials so nine subjects were used for the final process.

Apart from the variability due to the users and the system, some of the Human-Computer Interaction (HCI) issues that were identified by the users when using the device, could also account for some of the loss of accuracy:

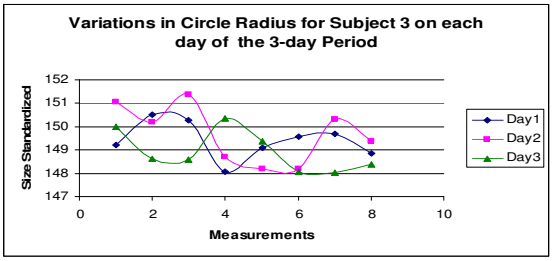
- When using the stylus of the Reachin device it was difficult to sense the distance to move for initial contact with the virtual surface. This affected some force measurements.
- The user was not able to see his/her hand and this created some discomfort (Figure 1).
- The user was not able to rest his/her palm on a solid surface while writing with the device (Figure 1).

The data captured varied for each user from trial-to-trial over the three days. Figures 10 (a) and (b) show how the measurements varied for a specific user, and Figure 10 (c) shows how the measurements varied across users over the 3-day period. There was no significant difference for each user over the three-day period. The measurements shown are standardized.

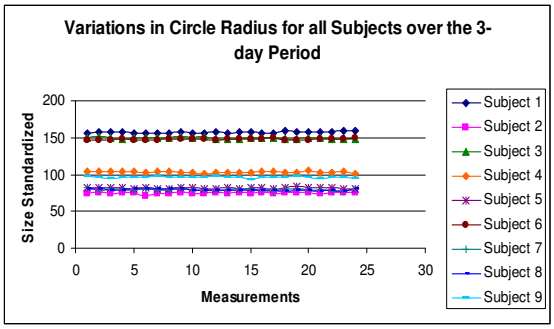
A matrix (Table 2) could be used to show the mappings defined by rules, as was demonstrated by Brubaker and Sheerer [24]. For systems with more than 2 features the dimensionality becomes difficult to represent. Table 2 shows only 2 of the 7 dimensions/features used. It is noted that Subjects 1 and 5 fall in the same category and were only distinguishable, for both subject and imposter verification, when more than 2 features were used.



(a) Variability in Radius size for Subject 1



(b) Variability in Radius size for Subject 3



(c) Variability in Radius size for all Subjects

Figure 10: Variations in size of radius drawn by users over the three-day period

Table 2 – User mappings defined by fuzzy rule base

	Size			
Force	Very Small	Small	Large	Very Large
Very Weak				Subject 1, Subject 5
Weak		Subject 2		
Strong			Subject 6	
Very Strong				

Tables 3 and 4 show how the accuracy percentage was improved for both Subject and Imposter verification as the features selected were increased. A high accuracy for subject verification was established with the use of three features whereas imposter verification needed seven

features to attain a sufficient level of accuracy.

Table 3 – Change in the Subject Verification accuracy as the number of features are increased

Subject	Number of Features					
	2	**3**	**4**	**5**	**6**	**7**
1	90	90	90	90	90	90
2	100	100	100	100	100	100
3	90	90	90	90	90	90
4	70	90	90	90	90	90
5	100	100	100	100	100	100
6	100	100	100	100	100	100
7	40	100	100	100	100	100
8	100	100	100	100	100	100
9	100	100	90	90	90	90
Average	**87.50**	**97.50**	**96.25**	**96.25**	**96.25**	**96.25**

Table 4 - Change in the Imposter Verification accuracy as the number of features are increased

Subject	Number of Features					
	2	**3**	**4**	**5**	**6**	**7**
1	88.46	88.46	88.46	90.38	100	100
2	78.8	78.8	82.7	98.07	100	100
3	67.3	67.3	67.3	78.84	94.2	98.1
4	15.38	17.3	30.8	38.46	44.2	84.6
5	61.5	65.4	67.3	94.23	98.1	100
6	73.1	73.1	71.2	88.46	88.5	96.2
7	69.2	61.5	61.5	73.07	75	75
8	61.5	65.4	65.4	90.38	90.4	92.3
9	67.3	67.3	71.2	71.15	73.1	82.7
Average	**61.76**	**62.01**	**64.68**	**79.08**	**82.93**	**91.10**

6. Conclusion

According to Base Rate Fallacy [25], to be of practical use, a security system should detect a substantial percentage of imposters while keeping the false rejection rate (FRR) at an acceptable level. This Haptics and Biometric Verification System shows great potential.

Further enhancements may be achieved in future research. These may include increasing both the number of users and the number of trials per user [26]. By increasing the number of users the results would provide a more adequate representation of the target population and this research may be also used to investigate a maximum number of users or tolerance of the system. By increasing the number of trials per user the effects of variations due to errors would be decreased A multimodal approach can also enhance the accuracy of the system [15].

In view of the fact that tracing the circle was able to yield 96.25% accuracy, a next step would be allowing the user to write freehand characters. This should allow for greater differentiation among the users.

7. References

[1] J. K. Salisbury, and M. Srinivasan. Phantom-Based Haptic Interaction with Virtual Objects. IEEE Computer Graphics and Applications, 17 (5): 6- 10, 1997.

[2] D. Florencio, C. Herley. A Large Scale Study of Web Password Habits. ACM International World Wide Web Conference, pp: 657 – 666, 2007.

[3] K. Salisbury, F. Conti, F. Barbagli. Haptic Rendering: Introductory Concepts. IEEE Computer Graphics and Applications, 24 (2): 24-32, 2004.

[4] SensAble Technologies – Reachin API. DOI = http://www.reachin.se/.

[5] Reachin API 4 Programmer's Guide. Reachin Technologies. 2005. DOI = http://www.reachin.se/.

[6] T. Song Ong and A. Beng Jin Teoh. Fuzzy Key Extraction from Fingerprint Biometrics based on Dynamic Quantization Mechanism. IEEE International Symposium on Information Assurance and Security, pp: 71 – 76, 2007.

[7] J. Ortega-Garcia, J. Bigun, D. Reynolds, J. Gonzalez-Rodriguez. Authentication gets Personal with Biometrics. IEEE Signal Processing Magazine, 21 (2): 50-62, 2004.

[8] J.L. Wayman, "Technical Testing and Evaluation of Biometric Identification Devices". National Biometric Test Center San Jose State University, 1998. DOI = http://www.cse.msu.edu/~cse891/Sect601/textbook/17.pdf

[9] E.S. Dunstone. Emerging Biometric Developments: Identifying the Missing Pieces for Industry. IEEE Symposium on Signal Processing and its Applications, 1: 351-354, 2001.

[10] G. Roethenbaugh, "Biometrics Explained", NCSA Biometrics Editor, 1997. DOI = http://www.incits.org/tc_home/m1htm/docs/m1050687.pdf.

[11] W. Pedrycz. Computational Intelligence as an Emerging Paradigm of Software Engineering. ACM international conference on Software engineering and knowledge engineering, 27:7-14, 2002

[12] G. Viot. Fuzzy Logic in C- Creating a fuzzy-based inference engine. Dr. Dobb's Journal, pp:. 40-49,1993.

[13] L.A. Zadeh. Commonsense Reasoning based on Fuzzy Logic. ACM Winter Simulation Conference, pp: 445 – 447, 1986.

[14] J.S.R. Jang, C.T. Sun, and E. Mizutani. Neuro-Fuzzy and Soft Computing – A Computational Approach to Learning and Machine Intelligence. Prentice- Hall Inc. Matlab Curriculum Series. 1997.

[15] C. Hook, J. Kempf, G. Scharfenberg. New Pen Device for Biometrical 3D Pressure Analysis of Handwritten Characters, Words and Signatures. ACM SIGMM

workshop on Biometrics methods and applications. pp: 38 – 44, 2003.

[16] M. Orozco, Y. Asfaw, A. Adler, S. Shirmohammadi, A., El Saddik. Automatic Identification of Participants in Haptic Systems. IEEE Instrument and Measurement Technology Conference, 2: 888-892, 2005.

[17] M. Orozco, A. El Saddik. Recognizing and Quantifying Human Movement Patterns through Haptic-based Applications. IEEE International Conference on Virtual Environments, Human-Computer Interfaces and Measurement Systems, 2005.

[18] M. Orozco, I. Shakra, A. El Saddik. Haptic: The New Biometrics-embedded Media to Recognizing and Quantifying Human Patterns. ACM International conference on Multimedia, pp: 387 – 390, 2005.

[19] M. Orozco, Y. Asfaw, S. Shirmohammadi, A. Adler, A. El Saddik. Haptic-Based Biometrics: A Feasibility Study. IEEE Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems, pp:265- 271, 2006.

[20] M. Orozco, M. Graydon, S. Shirmohammadi, A. El Saddik. Using Haptic Interfaces for User Verification in Virtual Environments. IEEE International Conference on Virtual Environments, Human-Computer Interfaces and Measurement Systems, pp: 25 – 30, 2006.

[21] M. Orozco, M. Graydon, S. Shirmohammadi, and A. El Saddik. Experiments in Haptic-Based Authentication of Humans. Springer Journal of Multimedia Tools and Applications, 37 (1): 71-72, 2008.

[22] R. Dhamija, L. Dusseault. The Seven Flaws of Identity Management: Usability and Security Challenges. IEEE Security and Privacy, 6(2): 24-29, 2008.

[23] T. Mansfield, G. Kelly, D. Chandler and J. Kane. Biometric Product Testing. Final Report. Centre for Mathematics and Scientific Computing, National Physical Laboratory, March 2001.

[24] D. Brubaker, and C. Sheerer, “Fuzzy Logic System Solves Control Problem," EDN, June 1992, pp 121

[25] W. Stallings. Cryptography and Network Security, 4/E, Prentice Hall. 2006.

[26] M. Schuckers. Some Statistical Aspects of Biometric Identification Device Performance. Stats Magazine. Department of Statistics West Virginia University. September 2001. DOI = http://www2.citer.wvu.edu/members/publications/files/11-Schuckers-STATSMag01.pdf.