Biometric Identification in Virtual Worlds using Biometric Fusion Techniques

Ahmed Al-Khazzar and Nick Savage
School of Engineering, University of Portsmouth, Portsmouth, U.K.

Keywords: Biometric Fusion, Biometric Recognition, Identification, Virtual Worlds, Games, Behavioural Biometric.

Abstract: The use of virtual worlds is becoming popular in many fields such as education, economy, space, and games. With the widespread use of virtual worlds, establishing the security of these systems becomes more important. In this paper a behavioural biometric system is implemented to identify users of a virtual environment. This research suggests the use of a score level fusion technique to improve the identification performance of the system. The identification is achieved by analysing user interactions within the virtual environments and comparing these interactions with the previously recorded interactions in the database. The results showed that using score level biometric fusion in behavioural biometric systems similar to the one presented in this research is a promising tool to improve the performance of these systems. The use of biometric fusion technique enhanced the performance of the implemented biometric system up to 7.5%. An average equal error rate of up to 22.7% was achieved in this work.

1 INTRODUCTION

A virtual world is an interactive 3D virtual environment that visually resembles complex physical spaces, and provides an online community through which the users can connect, shop, work, learn, establish emotional relations, and explore different virtual environments. Users of a virtual world can interact with the objects of the virtual environments through avatars. They can perform real world activities such as watching, hearing and touching the virtual objects through avatars.

Virtual worlds have become very popular in many fields such as E-learning (Dharmawansa et al., 2011); (Gonzalez-Pardo et al., 2010), economy (Harris and Novobilski, 2008); (Kim et al., 2002); (Peng and Xu, 2008), space (Noor, 2010); (Romann, 2007), and games (e.g. the World of Warcraft). USA National Aeronautics and Space Administration agency (NASA) use virtual worlds to test the design of equipment (Cline, 2005, p. 92). In the last few years a large number of virtual worlds have been developed, which share a number of characteristics (Noor, 2010):

1. Presence and real-time chat facilities in a shared space.
2. Persistent environment in which objects continue to exist in the absence of users and do not disappear when users are logged out.
3. Users are represented in the virtual world by avatars.
4. 3D graphical environments.

Cline (2005) argued potential impacts of virtual reality environments in human life and activity. He predicted that virtual reality will be integrated into a human's daily life and techniques will be developed to influence human behaviour, interpersonal communication and cognition. Cline (2005) also suggested that there will be a shift from the use of virtual reality from mainly communications to the use of virtual reality as an extension of the real world and a "migration to virtual space" will result in significant changes in economics, culture and other aspects of human life.

Therefore the future of the technology seems to be interconnected with the future of virtual reality as Cline (2005) predicts. With the expansion of virtual worlds there will be a demand for security of these newly created virtual reality environments. Similar to all types of systems and applications, virtual worlds require access control mechanisms to control the access of users to the resources of these environments. Authentication is the key component of any access control policy in any system. While

Al-Khazzar A. and Savage N..
Biometric Identification in Virtual Worlds using Biometric Fusion Techniques.
DOI: 10.5220/0004054602630269
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2012), pages 263-269
ISBN: 978-989-8565-24-2

almost all virtual worlds implement initial authentication through usernames and passwords, very few (if any) virtual worlds have mechanisms to verify the identity of the users after the initial log in.

The importance of subsequent verification results from the possibility of intruders seizing control from the genuine users initially logged in to the system. The difficulty with continuously identifying users inside virtual worlds is that it can be obtrusive and prevent users from easily interacting with the virtual world. However, continuous user identity verification can be achieved unobtrusively through analysing user interactions with the virtual environments. Identifying users in virtual worlds based on their interaction with these environments not only will be useful for continuous user recognition, but also for verifying the identity of the users claiming to be the genuine users of the system and possessing the genuine user password. Knowledge based authentication mechanisms such as passwords are currently used in virtual worlds; however the virtual worlds are not capable of distinguishing between genuine users and imposters who possess the knowledge needed to gain access to the virtual world. In addition current virtual worlds are not capable of determining if the current user is the continuing genuine user (who has been authenticated to access the system at the start of the session) or an imposter who has seized control of the virtual world.

In this paper we propose a behavioural biometric identification technique that utilises user interaction with virtual worlds. The virtual worlds are strategy-less 3D games that are implemented for the identification purpose in order to collect the user actions during the game play. While proposing a more secure biometric identification system is the main theme of this research, the study of the human behaviour in a virtual world can have several other applications. Examples of such applications are differentiating humans from machines (bots) in online games (Golle and Ducheneaut, 2005); (Thawonmas et al., 2008); (Yampolskiy and Govindaraju, 2007), and finding users operating multiple accounts in an online system (Ishikawa et al., 2010).

To the best knowledge of the authors, there is currently no research available which implements behaviour based user recognition inside virtual worlds. However there are a few studies that analyse the behaviour of users inside virtual worlds (Dharmawansa et al., 2011); (Gavrilova and Yampolskiy, 2010); (Gonzalez-Pardoe t al., 2010).

2 BIOMETRIC IDENTIFICATION

2.1 Introduction

Biometric identification as defined by ISO/IEC is the process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) matching the submitted biometric sample of a single individual (Standing document 2, 2007). Biometric identification systems are usually classified into two categories: physiological and behavioural biometric systems.

While there has been a significant surge in the use of physiological biometric systems for user identification and verification in recent years, they have not been a perfect solution. There are a large number of known attacks against these systems. A few security attacks have been reported in (Buthan and Hartel, 2005); (Ratha et al., 2001). Buthan and Hartel (2005) identified three types of spoofing attacks to biometric systems: coercive impersonation, replay attack, and impersonation attack. Although there are a number of counterattacks against spoofing by using liveness detection methods as described in (Toth, 2005), or using a (multi-sensor) multimodal biometric system (Schuckers, 2002), these methods add to the complexity and cost of the biometric system and they are not always successful.

To overcome some of these potential security threats, a behavioural biometric system can be used. Behavioural biometrics is a subset of biometrics which uses measurable properties of a person's actions for user recognition. The behavioural biometrics of a user are not physically accessible, in contradiction with the other physiological biometric methods where the user biometric is usually physically accessible (e.g. finger prints, iris, and face). Therefore behavioural biometrics are more resistant against the spoofing attacks mentioned earlier.

The proposed system of this paper is a behavioural biometric system, utilising algorithms used in previous systems for user identification inside virtual environments. However the feature extraction techniques proposed in the paper are novel and specifically designed to extract user interactions with the virtual worlds.

2.2 Multimodal Biometric and Score-level Fusion

A biometric recognition system is essentially a pattern recognition system which works by

acquiring biometric samples from an individual, extracting a biometric feature set from the acquired samples, and comparing the feature set with the previously recorded templates in a biometric enrolment database (Tran et al., 2011). The biometric feature sets extracted from the user behaviour inside a virtual world are of very different natures. Therefore, two or more of these biometric features can be combined to improve the efficiency of the system.

Different levels of biometric fusion may be defined based on the type of the available information. Score-level fusion is the most common fusion technique applied, due to the trade off between information availability and fusion complexity (Tran et al., 2011). Drosou et al. (2012) suggested a behavioural biometric system that uses score level fusion to combine two biometric features for user identification based on the spatiotemporal analysis of human activities. This paper uses a similar approach of score level fusion of two biometric features extracted from user interactions in virtual worlds.

In score-level fusion the match scores which are generated by multiple biometric comparison modules are combined to create a new match score. A match score is the outcome of comparing two feature sets extracted using the same feature extractor (Ross and Nandakumar, 2009). Match scores are typically categorised to two classes: similarity scores, and distance scores, which respectively reflect the similarity or distance of the compared biometric samples. These scores can be rescaled arbitrarily without affecting the performance of the biometric system, provided that the values are scaled in a monotonic manner (Hube, 2010).

Let X be the set of similarity scores from biometric features extracted from different feature extractors, and let $x \in X$. The normalised similarity score of x can be marked by x'. To normalise the set of similarity scores, the following method can be used to map the similarity scores to interval [0, 1). The original distribution and characteristics of the features will be retained as the result of the scaling process:

$$x' = \frac{x}{\sum_{i=1}^{N} x_i} \quad (1)$$

In this paper sum-rule-based score level (transformation based score level) fusion technique is used to combine the new normalised similarity scores x' and to create a new similarity score. This technique is generally easier than the other score-level fusion techniques. The procedure for sum-rule-based fusion is stated in (Horng et al., 2009): After computing the normalised scores (x_1, x_2, ..., x_m) from a single user (from different feature extractors), the fused score f_S can be calculated using the following formula:

$$f_S = w_1 x_1 + w_2 x_2 + \cdots + w_m x_m \quad (2)$$

The notation w_i represents the weight of each normalised score x_i, for i = 1, 2, ..., m. In the experiments of this research, equal weights are used. The newly generated fused score f_S can be used in the comparison process to determine the identity of the user.

3 METHODOLOGY

3.1 Data Collection

In order to have complete control on the virtual world and the avatar actions inside virtual world, we implemented our own virtual environment. 3D computer games were adopted as virtual worlds for user identification. These 3D games are considered as interactive 3D environments with the ability to collect user interactions with the environments for identification purposes. Virtual worlds can have very different environments and to investigate the user behaviour in diverse environments with different user avatars and movement capabilities, three different 3D games have been considered. These three identification environments (3D games) are different in two main perspectives, namely, world constraints, and character movement. Each game has a set of different actions that can be performed using the computer keyboard. The three implemented games in this research are:

- A maze game (2D Movement)
- A car game (2D Movement)
- A subracer game (3D Movement)

3.2 Design of Experiments

After developing the virtual worlds, the next step is to run experiments to collect data from users interacting with these virtual worlds. Each user should play the games for a specified amount of time, called the identification time.

In tests that were performed to identify the approximate length of time for identification inside the developed virtual worlds of this research, 4 minutes was found to be the maximum time before

the users lose their concentration inside the game. This time also provided enough data for user identification. Therefore each user should play a game for the period of 4 minutes for the system to collect one set of biometric samples from the user. The biometric sample represents a set of avatar interactions with the environment and other data collected from the user during a period of 4 minutes.

The experiments of this research have been repeated twice and at different times. In each experiment a separate group of users were asked to play the games four times within a one month period. There was a gap of one year between the two experiments. The users played each game once per week for a total of four weeks. The total sets of samples gathered from one user for all of the games were 12. In the first round a total of 40 users participated in the experiment. In the second round and a year later, a total of 50 different users participated in the experiment. For the first round of experiments each of the 160 sets of samples are compared against 159 profiles giving a total of 25,440 identification tests. Similarly for the second round each of 200 testing sets are compared against 199 profiles for a total of 39,800 identification tests.

The biometric comparison module uses a similarity measure algorithm to classify the extracted biometric features. The similarity measure algorithm allows the system to compare the newly submitted samples with the samples in the biometric enrolment database. Various similarity measure algorithms have been used in behavioural recognition systems. For the sake of analysis in this paper, the distance similarity measure is used (Bergadano et al., 2002).

The user set of this research were all final year male engineering students. The dominant age group was between 20-25 years old. There were no constraints on the time and place of the test. The only requirement was to supply one sample of each game per week.

3.3 Biometric Features

Biometric features are the information (in the form of numbers or labels) extracted from biometric samples which can be used for comparison with other biometric samples. During the experiments, many parameters have been collected from the users. The parameters are: the actions of the user inside the virtual world, the Euclidean coordinates of the game avatar at the time of the action, and the time duration and delay between actions. From these parameters different features can be extracted. For the analysis purposes of this paper, two biometric features have been extracted, namely actions, and time biometric features.

During the game play the user may perform different actions, either sequentially (one by one) or several actions at the same time (each action corresponds pressing one or more keys). The actions can occur in different sequences and different frequencies. The sequence and frequency of the actions can be used as a biometric feature to compare biometric samples together. Each action starts and ends at specific times, decided by the user. Also there could be a delay between the previous action and the next one. The time duration and delay between actions can be used as another biometric feature in biometric comparisons. Also, the time biometric feature can be extracted using two different methods. The first method is to calculate the time between two subsequent actions. This method is referred to as *digraph* method. The second method is to calculate the time between three subsequent actions and can be referred to as *trigraph* method. An illustration of these two methods is shown in Figure 1. Digraphs and trigraphs are used in keystroke biometric systems (Bergadano et al., 2002). Digraphs are defined as the latency between two consecutively types keys. Similarly, three consecutively typed keys are referred to as trigraphs in these systems.

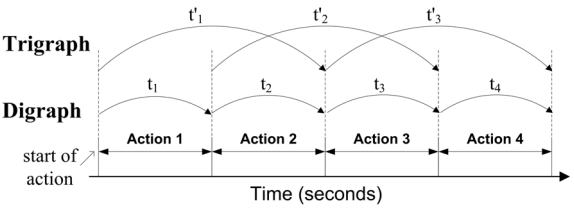

Figure 1: Time biometric feature calculation methods. Notations t1 to t4 (digraph) and t'1 to t'3 (trigraph) are time feature variables for actions 1 to 4.

3.3.1 Fused Biometric Scores

To compute the fused biometric scores, Equation (1) and (2) can be used to fuse actions and time biometric scores. Since there are two methods to calculate the time scores, two fused scores can be generated. These scores can be compared to find the more efficient feature extraction method. The result of using digraph and trigraph feature extraction methods and fusion technique is two biometric scores: 1- digraph fusion score, and 2- trigraph fusion score.

4 RESULTS AND ANALYSIS

Table 1 illustrates the results of identification experiments in terms of EERs. Equal error rates are computed based on the extracted individual features of time and action and also the score fusion of these two biometric features. For each experiment, EERs from five different biometric features (scores) is reported: 1- actions, 2- digraph time, 3- trigraph time, 4- digraph fusion, and 5- trigraph fusion. The first three numbers represent the performance of system in the absence of fusion techniques. The last two numbers represent the performance of the system when applying digraph and trigraph fusion techniques respectively. The first round of experiments is identified with a 2010 label, and the second round of experiments is identified with a 2011 label. The results show EERs between 29%-46% for individual features and 26%-36% when applying fusion techniques.

Table 1: Average equal error rates based on individual biometric features and fusion scores.

Game	Actions	Digraph Time	Trigraph Time	Digraph Fusion	Trigraph Fusion
maze 2010	31.5	33.4	38.4	26.6	27.6
maze 2011	32.8	31.8	33.9	26.2	27.2
car 2010	36.0	34.6	40.0	33.7	33.6
car 2011	34.9	38.4	41.6	33.5	34.8
sub.2010	29.1	37.6	45.6	27.3	33.8
sub 2011	34.4	37.9	41.5	32.6	36.1

The results from Table 1 exhibits that the "actions feature" has a better identification performance than the "trigraph time feature". However this is not the case when considering "digraph time feature", where the EERs are comparable; though the "action feature" still performs better by a small margin. The similarity in the results of the actions and "digraph time" can be justified by the comparable discrimination power of the time and actions behavioural features. The slightly better results of the actions can be depicted by the way the time feature extractor works. The time feature value is essentially the durations of two or three consecutive actions. When these consecutive actions are repeated by the user in the same session, then there are two values for the same single feature variable. Further repeating the action results in multiple values for this feature variable. Since a unique value has to be assigned to each biometric feature variable, the possible solution will be to use the mean of these multiple values. This mean value might not perform well in classification tests.

It is also interesting to analyse the reason behind the different performances of digraph and trigraph time features. The reason behind the better performance of the "digraph time feature" is not instantly clear. It could be that the digraph features possess more behavioural attributes than trigraph features. Assuming that the user choice of the future actions is related to the previous actions of a user, these results could mean that in a sequence of three consecutive actions, the choice of the third action is less correlated to the first action and more to the second action.

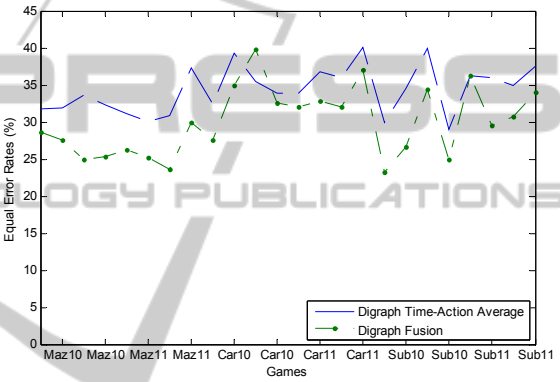

Figure 2: Performance gain in "digraph fusion".

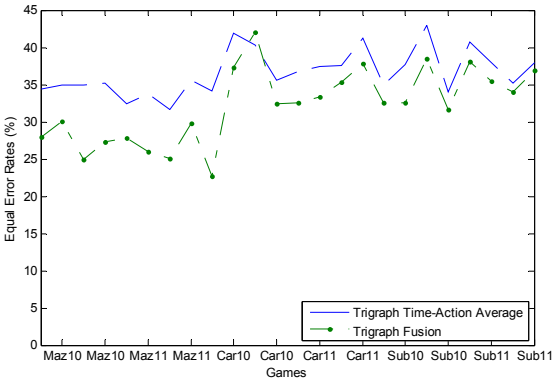

Figure 3: Performance gain in "trigraph fusion".

Using score level fusion has improved the performance across all games and in both experiments. Both digraph and trigraph fusion performed well in the identification tests. Figure 2 and Figure 3 show a graphical representation of the performance gain across the games and for digraph and trigraph fusion methods. Results show that the maze game benefit from fusion was the most notable with an average of 6- 7.5% increase in performance.

The car game performance gain was between 1.5-4.5% and the subracer game performance was between 2- 6%. These results suggest that more constrained environments (with restricted paths), such as the maze virtual environment, perform better than less constrained environments, such as car game environments.

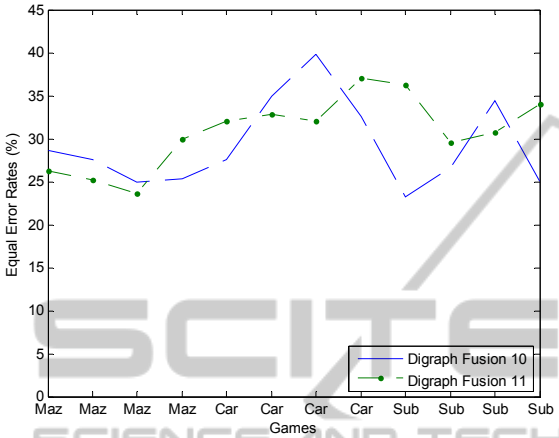

Figure 4: Performance comparison of "digraph fusion" between the two experiments.

4.1 Comparison of Experiments

The results of the two experiments showed that in general the performance of biometric fusion was consistent across both experiments. The number of users has not affected the results. Figure 4 shows a comparison of the fusion performances of the two experiments. The performance reported from the second experiment is comparable to the first experiment across different games. The importance of repeating experiments comes from the fact that the discrimination power of the behavioural traits is not easily provable. For example in the case of fingerprint biometric systems, it is well known that the fingerprints of humans possess a high discriminating potential. The same cannot be said about behavioural biometrics because of the lower performance of these systems. However since extensive work has been conducted on some behavioural systems, such as keystroke based systems, the discrimination property of these systems are known (e.g. (Bergadano et al., 2002)). In the case of this research, to the best knowledge of the authors, there is no similar system available at the time of writing and as a result repeating the experiments is necessary to prove the discrimination property.

5 CONCLUSIONS

This work proposed a behavioural biometric identification system for virtual worlds, which has the potential to identity users of virtual worlds using a new approach, based on their interactions with the virtual environments. In this paper three games were implemented to test the performance of the proposed system and biometric score level fusion technique has been used to improve the performance of the system. To test the performance of the system, two experiments have been conducted. In the first experiment 40 users, and in the second experiment, a year later, 50 different users participated in the experiment.

Two biometric features namely, time and action, are extracted using two different feature extractors (digraph and trigraph extractors). The resulting scores from these features are normalised and then fused using transformation based score level fusion method. The identification tests results showed that using this fusion technique in this particular biometric system improves the performance of the system significantly. The fusion technique boosted the equal error rates to up to 7.5%. It is recommended to use this technique to combine biometric scores with higher performances, since it is well known that the performance of biometric fusion is greatly affected by its biometric feature component with lower performance. The results also showed that the individual digraph features performed better than the trigraph features. This better performance also is reflected in the fused scores, so that the "digraph fusion" has a better performance than the "trigraph fusion".

The results from the two independent experiments were similar and consistent. This is especially vital since in behavioural recognition systems, it is usually difficult to find whether or not different behavioural biometric traits possess a discrimination power to distinguish between different users. The suggested biometric fusion technique in this research achieved an average equal error rate of up to 22.7%.

REFERENCES

Bergadano, F., Gunetti, D., and Picardi, C., (2002). User authentication through keystroke dynamics. *ACM Transactions on Information and System Security , 5* (4), 367-397.

Buthan, I. and Hartel, P., (2005). *The state of the art in abuse of biometrics.* Technical Report, Centre for

Telematics and Information Technology, Enschede.

Cline, M., (2005). *Power, Madness, and Immortality: the future of virtual reality.* University Village Press.

Dharmawansa, A., Nakahira, K., and Fukumura, Y., (2011). Develop a Monitoring Tool and Extract Facial Expression towards the Analyzing Student Behavior in Three Dimensional Virtual Environment. *Biometrics and Kansei Engineering (ICBAKE), 2011 International Conference on* (pp. 134 -139). Takamatsu, Japan: Abrasive Engineering Society.

Drosou, A., Ioannidis, D., Moustakas, K., and Tzovaras, D., (2012). Spatiotemporal analysis of human activities for biometric authentication. *Computer Vision and Image Understanding* , 411 - 421.

Gavrilova, M. L., and Yampolskiy, R. V., (2010). Applying Biometric Principles to Avatar Recognition. *Proc. Int Cyberworlds (CW) Conf* (pp. 179-186). Singapore: IEEE Computer Society.

Golle, P., and Ducheneaut, N., (2005). Preventing bots from playing online games. *Computers in Entertainment (CIE) - Theoretical and Practical Computer Applications in Entertainment , 3* (3), 1-10.

Gonzalez-Pardo, A., Rodriguez, F. B., Pulido, E., and Camacho, D., (2010). Using virtual worlds for behaviour clustering-based analysis. *SMVC'10 - Proceedings of the 2010 ACM Workshop on Surreal Media and Virtual Cloning, Co-located with ACM Multimedia 2010*, (pp. 9-14). Firenze, Italy.

Harris, B., and Novobilski, A., (2008). Real currency economies: Using real money in virtual worlds. *2008 International Conference on Frontiers in Education: Computer Science and Computer Engineering, FECS 2008* (pp. 241 - 246). Las Vegas: CSREA Press.

Horng, S.-J., Chen, Y.-H., Run, R.-S., Chen, R.-J., Lai, J.-L., and Sentosal, K., (2009). An Improved Score Level Fusion in Multimodal Biometric Systems. *Parallel and Distributed Computing, Applications and Technologies, 2009 International Conference on* (pp. 239 -246). Higashi Hiroshima : IEEE.

Hube, J. (2010). Methods for estimating biometric score level fusion. *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on* (pp. 1 - 6). Washington, DC, USA: IEEE.

Ishikawa, N., Watanabe, Y., Nishimura, R., Umemoto, K., Okada, Y. and Murata, M., (2010). Detection of users suspected of using multiple user accounts and manipulating evaluations in a community site. *2010 International Conference on Natural Language Processing and Knowledge Engineering (NLP-KE 2010)*, (pp. 1-8). Beijing.

Kim, B., Barua, A., and Whinston, A., (2002). Virtual field experiments for a digital economy: a new research methodology for exploring an information economy. *Decision Support Systems* , 215 - 231.

Noor, A., (2010). Potential of virtual worlds for remote space exploration. *Advances in Engineering Software* , 666 - 673.

Peng, H., and Xu, X., (2008). The Analysis of Arbitrage Capital Flows between Online Virtual Game and Real Economy Based on Risk Premium. *Computational Intelligence for Modelling Control Automation, 2008 International Conference on* (pp. 1141 -1146). Vienna, Austria: IEEE.

Ratha, N. K., Connell, J. H., and Bolle, R. M., (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal , 40* (3), 614-34.

Romann, J., (2007). Projective virtual reality today and in the future: Application of virtual worlds in space, industry, and at the construction site with robotic know-how to improved virtual worlds. *VDI Berichte* , 55-67.

Ross, A., and Nandakumar, K., (2009). Score-Level Fusion. In S. Z. Li, and A. K. Jain, *Encyclopeida of Biometrics* (pp. 611 - 621). Springer Science+Business Media, LLC.

Schuckers, S. A., (2002). Spoofing and anti-spoofing measures. *Information security technical report , 7* (4), 56-62.

Standing document 2. (2007, 08 22). *Standing document 2, harmonized biometric vocabulary, version 8* . ISO/IEC JTC 1/SC 37 N 2263.

Thawonmas, R., Kashifuji, Y., and Chen, K.-T., (2008). Detection of MMORPG bots based on behavior analysis. *Proceedings of the 2008 International Conference on Advances in Computer Entertainment Technology, ACE 2008*, (pp. 91-94). Yokohama, Japan.

Toth, B., (2005). Biometric liveness detection. *Information Security Bulletin*, (pp. 291-297).

Tran, Q., Liatsis, P., Zhu, B., and He, C., (2011). An approach for multimodal biometric fusion under the missing data scenario. *Uncertainty Reasoning and Knowledge Engineering (URKE), 2011 International Conference on* (pp. 185 -188). Bali, Indonesia: IEEE.

Yampolskiy, R., and Govindaraju, V., (2007). Behavioral biometrics for recognition and verification of game bots. *8th International Conference on Intelligent Games and Simulation. GAME-ON 2007*, (pp. 108-114). Ghent-Zwijnaarde, Belgium.