American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

3D Password Enabling Using Gait Technology

M. BalaSai Charan[a]*, Prof. T.Venkat Narayana Rao[b], M.D.V.Saras Chandra[c]

[a]*JNTUK, Vizianagaram, A.P, India*
[b]*Sreenidhi Institute of Science and Technology, Hyderabad, India*
tvnrbobby@yahoo.com
mamidisaicharan@gmail.com

Abstract

Existing authentication systems is suffering with many weaknesses. In general, textual passwords are used to secure normal user accounts or data. However, these can be cracked by some techniques such as, if the number of characters is being fixed and there will be a finite number of possibilities as the length of the password is fixed (maximum allowed length). The current existing graphical password system uses less space than that of the textual passwords space. Firstly considering a 3D password, it is a combination of more than one authentication systems.. When the user intend to set a 3D password, it redirects into a 3D-virtual environment where in different types of objects navigates. User password will be set in the order in which he/ she selects/ interacts with those objects. Password key will be set based on intended 3D virtual environment and on the objects selected. Combining many systems of certification is an advantage of this 3D technique, providing higher security than the existing arrangement. Human gaits can also be combined with 3D password to provide more security to the users. Textual passwords may be easily ruptured because of fixed maximum possible length and harmfull as there is a chance of losing token based techniques/smart cards such as passports. Graphical passwords can be easily recorded as they take much time. In this paper, the usage of Human gaits face expressions, walk style, smile, etc. are taken into consideration and captured ultimately to attain better secured authenticated system than exiting scenario.

Keywords: Gait, password, attacks, motion, secured, graphical.

1. Introduction

With growth of utilization of computers in almost every area, we need to offer security for sensitive information as shown in the figure 1. Generally, human authentication techniques can be classified into knowledge based, token based and graphical passwords [6].

Knowledge based is again categorized into recall based and recognition based. Recall based is based on the sense to reproduce the password that the user created at the time of initialization. A recognition based is the

sense in which either the entire password or even a part of it may be recognized whenever the user wants to login.

The common known example of the recall based password scheme is Textual password. There is also a chance of misgiving the passwords set on token based systems, many reports are also have shown that tokens are vulnerable to fraud, loss or even theft by many simple schemes and techniques [2,5].

Graphical passwords are again separated into two characters. Recall based and recognition based. These types of password techniques have been introduced based on the view that the users can recall and recognize pictures rather than texts. Graphical password schemes take much longer time to perform. However, most of the graphical passwords can be easily observed or recorded while the user is performing the graphical password. Hence, it is vulnerable to attacks.

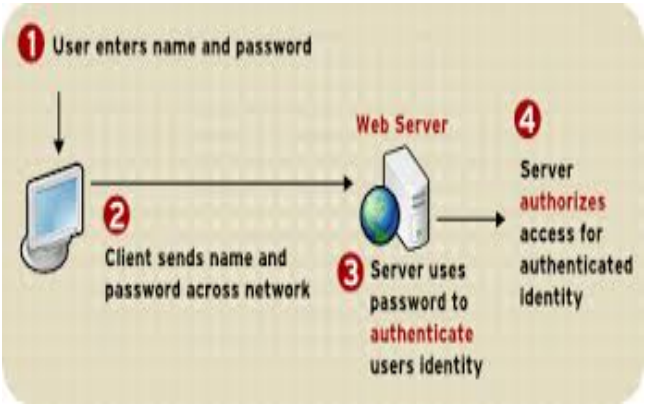

fig. 1: Pocess of authentication

Different biometric schemes such as fingerprints, palm prints, hand geometry, iris recognition, retina etc. have been artificial. Each biometric scheme has its own advantages and disadvantages based on the uniqueness, acceptability and consistency.

2. Usage of 3D PASSWORD Technique

Here, we discuss about the multi factor authentication scheme as shown in figure 2., which boost ups the benefits of various authentication schemes and techniques as it is the blend of various authentication schemes.

This 3D password technique may satisfy the following requirements:-

1) The scheme is not solely based on recall or recognition. It is a combination of recall, recognition, biometrics as well as token-based authentication schemes as shown in figure 2.

2) Users has flexibility to choose the specifications of the 3D password, whether it will be only recall,

recognition, or token-based, or a combination of two or more schemes. As the users are different and they have different needs and requirements, this flexibility of selection would be necessary. Some users do not like to carry cards. Some users do not like to provide biometrical data, and some users have poor memories.The user's freedom of selection is important which assures high acceptability.

3) The new scheme offers enough secrecy. This secrecy is flexible, so that the user must be allowed to change or remove them at his option.

4) This technique provide secrets that are easy to remember and very difficult for others to guess or suspect.

5) As this scheme is based on the navigation of the objects, it is difficult to write down those secrets on paper, which disallow the secrets to be shared with others [1].

fig. 2: Multiple factor authentication

3. 3D PASSWORD System Implementation

The 3D password is a multi factor authentication scheme. The 3D password presents a 3D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3D password is simply the combination and the sequence of user interactions that occur in the 3D virtual environment. The 3D password can combine recognition, recall, token, and biometrics based systems into one authentication scheme [4,1]. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized and tokens to be presented, and biometric data to be verified as shown in the figure 3.

For example, the user can enter the virtual environment and type something on a computer that exists in (a, b, c) position, then enter a room that has a fingerprint recognition device that exists in a position (p, q, r) and provide his/her fingerprint. Then, the user can go to the virtual store, selects his most interested object. The combination and the sequence of the previous actions towards the specific objects construct the user's 3D password [3,2].

Virtual objects are in the sense any object that we encounter in real life. Any instantaneous actions and interactions toward the real life objects can be done in the virtual 3D environment toward the virtual objects.

We can have the following objects:

1) A computer with which the user can type.

2) A fingerprint reader that requires the user's fingerprint.

3) A biometric recognition device.

4) A paper or a white board that a user can write, sign, or draw on.

5) An automated teller machine that requests a token.

6) A light that can be switched on/off.

7) A television or radio where channels can be selected.

8) A staple that can be punched.

9) A car that can be driven.

10) A book that can be moved from one place to another.

11) Any set of images in which the user selects most liked one.

12) Any real life object.

13) A set of costumes, which the user selects/shops by his interest.

14) Any puzzle which is to be solved.

15) Treasure hunt can be implemented.

16) Any upcoming authentication scheme.

figure 3: A Virtual Room

The action towards an object (assume a fingerprint recognition device) that exists in location (a1, b1, c1) is different from the action towards a similar object (another fingerprint recognition device) that exists in location (a2, b2, c2). Therefore, to perform the authorized 3D password, the user must follow the same scenario performed by the authorized user. This means interacting with the same objects that reside at the exact locations and perform the exact actions in the proper sequence result in proper login.

4. 3-D PASSWORD Selection And Inputs:

Let the size of the 3-D virtual environment space is S×S×S. The 3-D environment space is represented by the coordinates (x, y, z). Each and every object located in the 3D Virtual environment poses unique coordinates. Let us assume that the user enters into the virtual environment where the user interact with different objects using any input device. Here, the sequence of actions performed with the help of input device can be treated as the user's 3D password [6,7].

For example, consider a user who navigates through the 3D virtual environment which consists of students study room. Now, let us consider that the user wants to use the computer then first of all user opens the door located in (20, 20, 20). Then, the user closes the door. Next the user recognizes the computer on the room existed in the position (20, 11, 10) and types "WELCOME" (without quotes). Then, the user moves to the rack where books are located, he/she selects a book located on (10, 20, 30), picks it and places it in some other location (20, 10, 20). The user now clicks on the login button. Initial representations of the user actions in the 3D virtual environment can be recorded as follows:

(20, 20, 20) Action = Open the student study room door

(20, 20, 20) Action = Close the student study room door

(20, 11, 10) Action = Typing, "W"

(20, 11, 10) Action = Typing, "E"

(20, 11, 10) Action = Typing, "L"

(20, 11, 10) Action = Typing, "C"

(20, 11, 10) Action = Typing, "O"

(20, 11, 10) Action = Typing, "M"

(20, 11, 10) Action = Typing, "E"

(10, 20, 30) Action = pick up the book

(20, 10, 20) Action = drop/place the book

This representation is just an example. The extensive real representation will not be discussed in this paper. If user wants to be get authenticated, the user has to follow the same sequence and perform the actions and interactions towards the object for the user's original 3-D password. 3D virtual environments can be designed in order to include any virtual objects.

5. Usage of Gait Technology

Gait analysis is the systematic study of animal locomotion, more specifically the study of human motion, using the eye and the brain of observers, augmented by instrumentation for measuring body movements, body mechanics, and the activity of the muscles. Gait analysis is used to plan, and treat individuals with conditions affecting their ability to walk as shown in figure 4.

Gait recognition is a developing biometric technology which involves people being identified purely through the analysis of the way they behave as shown in the figure IV. While research is still underway, it has attracted interest as a method of identification because it is non-invasive and does not require the subject's cooperation. Gait recognition could also be used from a distance, making it well-suited to identifying perpetrators at a crime scene. But gait recognition technology is not limited to security applications – researchers also envision medical applications for the technology.

For example, recognizing changes in walking patterns early on can help to identify conditions such as Parkinson's disease and multiple sclerosis in their earliest stages.

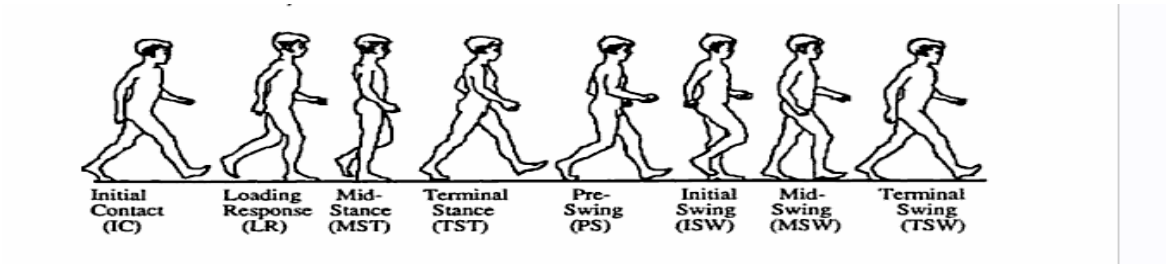

fig. 4: analyzing the movement of walk

Gait recognition technology is, however, still in its developing stages. No model has, as of yet, been developed that is sufficiently accurate and marketable. The technology is moving ahead at a rapid pace; however, with government-sponsored projects supporting research such as that going on at the Georgia Institute of Technology, MIT, the Lappeenranta University of Technology, and others academic institutions. There are two main types of gait recognition techniques currently in development. The first, gait recognition based on the automatic analysis of video imagery, is the more widely studied and attempted of the two. Video samples of the subject's walk are taken and the trajectories of the joints and angles over time are analyzed. A mathematical model of the motion is created, and is subsequently compared against any other samples in order to determine their identity.

The second method uses a radar system much like that used by police officers to identify speeding cars. The radar records the gait cycle that the various body parts of the subject create as he or she walks. This data is then compared to other samples to identify them. Efforts are being made to make gait recognition as accurate and usable as possible, and while it may never be as reliable as other biometrics such as fingerprint or iris recognition, it is predicted that gait recognition technology will be released in a functional state within the next five years, and will be used in conjunction with other biometrics as a method of identification and authentication.

6. Process And Implementation

A typical gait analysis laboratory has several cameras (video) placed around a walkway or a treadmill, which are linked to a computer. The user walks down the treadmill and the computer calculates the orbit path of each marker in three dimensions. A model is applied to calculate the movement of the underlying bones. This gives a complete breakdown of the movement of each joint.

CASE 1:

3D password with gaits can be implemented in banks to open the lockers or money chest. First of all the officer who wants to use the locker have to follow the following steps (I)Userneed to enter log in identity. (II) Now to access the user has to be authenticated first using gaits at the time of moving towards the chest/ locker the motion of the user gets monitored and this will be compared with the already authenticated one and if so match successful then it will be further proceeded to the next step. (III) In this tone, the user will be thrust out of the virtual room containing several objects. The order of the objects selected and the actions performed will be compared with the original authenticated password. (IV) If step (III) has been successfully passed, then the user log in details are considered as authenticated and the user will be allowed to access locker/ chest. An Exception in this instance: Unfortunately, if there is any scrutinizing by higher officials then the walking pattern of that particular officer will be recorded and added to the database. Or the respective officer is allowed directly without 3D password schemes as he/she has permission to access.

CASE 2:

3D password with gaits can be implemented in the malls in order to provide high security.

7. Conclusion

The 3-D password is not yet completely developed. Designing various kinds of 3-D virtual environments depending on the available password space and interpreting user feedback will result in more sophisticated 3-D password scheme.By combining this with gaits we acquire more secured authentication. In the days to come, this technology would bring about revolutionary advancement in the security domain.

References

[1] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annu. Comput. Security Appl. Conf., Dec. 5–9, 2005, pp. 463–472.

[2] D. V. Klein, "Foiling the cracker: A survey of, and improvement to passwords security," in Proc. USENIX Security Workshop, 1990, pp. 5–14.

[3] NBC news, ATM Fraud: Banking on Your Money, Dateline Hidden Cameras Show Criminals Owning ATMs, Dec. 11, 2003.

[4] T. Kitten, Keeping an Eye on the ATM. (2005, Jul. 11). [Online]. Available: ATMMarketPlace.com

[5] BBC news, Cash Machine Fraud up, Say Banks, Nov. 4, 2006.

[6] G. E. Blonder, "Graphical password," U.S. Patent 5 559 961, Sep. 24, 1996.

[7] R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in Proc. 9th USINEX Security Symp., Denver, CO, Aug. 2000, pp. 45–58.