International Journal of Scientific & Engineering Research Volume 9, Issue 4, April-2018
ISSN 2229-5518

Speech Recognition Integrated with Graphical Password Authentication System using Sequence Image Click

[1]T.Nithya

Abstract— In this graphical password system with supportive speech recognition to increase the remembrance of the password is discussed. In proposed work a click-based graphical password scheme called Cued Click Point (CCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point per image in a Sequence Image Click (SIC). In addition user is asked to recognize their voice corresponding to each click point; this will be used to help the user in recalling the click point on an image. System showed very good performance in terms of security, accuracy, and ease of use.

Keywords—Speech recognition, Authentication, SIC.

1 INTRODUCTION

The main concept of this project is to design a voice recognition security system along with the graphical image click. The click point on the image is calculated based on the X and Y coordinate points. This project is mainly used for security purpose to identify the voice password spoken from the authorized person and the system opens when the graphical password along with the voice is correct. The voice recognition system is the capacity of a device or program to receive and understand dictation, or to understand a spoken instruction. When this voice security system is used with a computer, analog signal must be converted into digital using ADC. Text Based password suffers with security because the third person can easily guess the password related with his name, date of birth, phone number, etc…(dictionary attack, brute force search, guess, spyware, shoulder surfing) and also text passed suffers with usability problems. The human brain has very good remembrance in graphics rather than the text. And next the sequence of image click will leads to better security for the system. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click and if the voice not matches. If the match not found with both the click and voice the user is not allowed to enter into the system

2 KEY TECHNOLOGIES

2.1 Speech Recognition

The function of this speech recognition security system is to have a system that will only unlock upon recognizing a voice password spoken by the administrator or password holder. The first stage of the speech recognition process is preprocessing. In order for any speech recognition system to operate at a reasonable speed, the amount of data used as input must be kept to a minimum. Once preprocessing is completed, the input data moves to the recognition stage, where the primary work involved in speech recognition is accomplished.

Classification of Voice Recognition System

There are four classifications of voice recognition

- Isolated VRS
- Continuous VRS
- Speaker Dependent VRS
- Speaker Independent VRS

Type	Classification	Working
1	Isolated VRS	requires a brief pass b/n the spoken words
2	Continuous VRS	doesn't require a brief pass b/n the spoken words
3	Speaker Dependent VRS	identifies speech from only one speaker
4	Speaker Independent VRS	identifies anyone's speech.

Table 1: Classification of VRS

Voice recognition technique is to be integrated with the graphical password for the purpose of authentication of the System. The voice frequency is calculated based on the speech which you recorded at the time of registration.

• [1]*T.Nithyaa, Guest Lecture, Computer Science in Government Arts College for Women, Bargur. PH-9500654651. E-mail: nithya,tr02@gmail ,com*

,

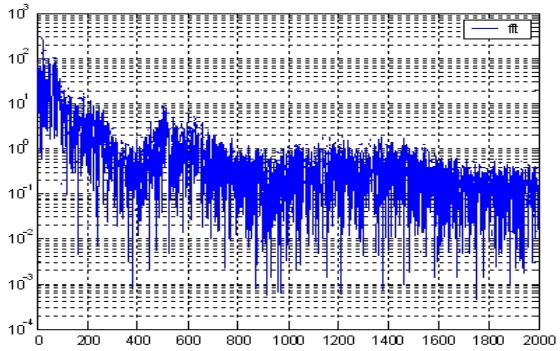

Figure1: The frequency spectrum of the word HELLO

2.2 graphical Representation

Graphical password can be used as an alternative to text based (alphanumeric) password in which users click on images to set their passwords. Text based password uses username and password. So recalling of password is necessary which may be a difficult one. Images are generally easier to be remembered than text and in Graphical password; user can set images as their password. Therefore graphical password has been proposed by many researchers as an alternative to text based password. In providing more security a sequence of images is to be used in which user can select a one click point on each image as a Sequence Image Click (SIC).

3 DESIGN

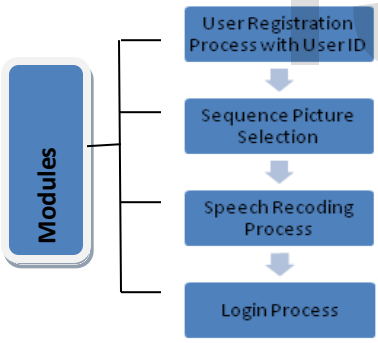

Figure 2: Procedure of Login Registration

4 PROCEDURES

4.1 login Registration

In this step the user has to enter the details for registration with their personal details such as Name, DOB, and gender, and so on along with the User ID which will be used while Login into the System.

4.2 sequence Image Selection

In this step, a sequence of images is presented on the user profile during registration. In that the user wants to click on the sequence of image. The coordinate points of the images are registered in the system based on the click made.

4.3 Speech Input Process

This module allows the end user to record the voice while registration. The file is converted to binary form and then it is associated with the graphical password.

4.4 login Process

This module allows the user to enter the user id and click on the image point and input the voice (speech) as same as registered at the time of registration. If all matches the same as registered, the system allows the user to login; if not the login fails.

5 RESULTS

Figure 3: Login for Graphical password with speech input

6 CONCLUSION

SIC increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images. In addition to that speech recognition integrated with this sequence image click

7 FUTURE WORKS

In future systems other patterns may be used for recalling purpose like touch of smells, and some other pattern recognition can be used, study shows that these patterns are very useful in recalling the associated objects like images or text. developed system used this approach. Furthermore, the system's flexibility to increase the overall number of images in the system allows us to arbitrarily increase this workload.

REFERENCES

[1] Markowitz, Judith A. Using Speech Recognition. Prentice-Hall, Inc, 1996.
[2] Keller, Eric. Fundamentals of Speech Synthesis and Speech Recognition. John Wiley & Sons, 1994.
[3] Wiedenbeck, S., J.C. Birget, A. Brodskiy, and N. Memon. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. ACM SOUPS, 2005.
[4] Graphical User Authentication (GUA): Graphical Password Algorithms and Analysis Paperback . Arash Habibi Lashkari , Farnaz Towhidi
[5].K. Golofit. Click passwords under investigation. In 12t h European Symposium On Research In Computer Security (ESORICS), Springer LNCS 4734, September 2007. 6.S. Chiasson, P.C. Van Oorschot, and R. Biddle, "Graphical password authentication using cued click-points, ".
[6].http://www.linfield.edu/~dbrewer/speech/spchi.html College student's informative summary paper on speech recognition
[7] http://www.speech.usyd.edu.au/comp.speech/FAQ6.html One of many speech recognition questions answered.
[8] https://www.ijser.org/researchpaper/integration-of-sound-signature-in-graphical-password-authentication-system.pdf
[9]https://www.cise.ufl.edu/~ddd/cap6635/Fall-97/Short-papers/4.html