INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1803 - 1808
RECEIVED: 09-03-17 PUBLISHED: 24-03-17.
March 24, 2017

DOUBLE CHECKING: MULTIMODAL, INTEGRATIVE & CONTINUOUS VERIFICATION TECHNOLOGY OF SIGNATURE & FINGER PRINT IDENTIFICATION

[1]V.Rajesh, [2]V.Shyamsundar, [3]R.Naveenraj, [4]Mr.N.Karthik,
[1,2,3]UG Scholars, Sri Balaji Chockalingam Engineering college, Irumbedu, Arni,Tiruvannamalai.
[4]Asst Prof, Department of Computer Science and Engineering Sri Balaji Chockalingam Engineering college, Irumbedu, Arni, Tiruvannamalai.

Abstract

User Name & Password as well as Single Biometric Solutions are not useful in the Identification of a Personality. User is verified using Multimodal Verification System that too in the Continuous Process. Any of the User's Biometric is used for the Authentication process. In which user is verified on a random continuously. If user's verification failed the application is terminated immediately. Modification Part is we are building the Multimodal Authentication using Finger print & Signature Authentication. We are using Minutiae Algorithm & for Signature Verification Neural Network are used. A Secure protocol is defined for authentication through user verification. The protocol determines adaptive timeouts based on the quality, frequency and type biometric data transparently acquired from the user.

Index Terms: Identification and verification. Signature and Finger print. Registration and Authentication.

1. INTRODUCTION

Secure user authentication is fundamental in most of modern ICT systems. User authentication systems are traditionally based on pairs of username and password and verify the identity of the user only at login phase. No checks are performed during working sessions, which are terminated by an explicit logout or expire after an idle activity period of the user. Security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attacks; biometric techniques offer emerging solution for secure and trusted authentication, where username and password are replaced by biometric data. However, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially considering their possible application in the financial and banking sectors. Such observations lead to arguing that a single authentication point and a single biometric data cannot guarantee a sufficient degree of security. In fact, similarly to traditional authentication processes which rely on username and password, biometric user authentication is typically formulated as a "single shot", providing user verification only during login phase when one or more biometric traits may be required. Once the user's identity has been verified, the system resources are available for a fixed period of time or until explicit logout from the user. This approach assumes that a single verification (at the beginning of the session) is sufficient, and that the identity of the user is constant during the whole session. For instance, we consider this simple scenario: a user has already logged into a security- critical service, and then the user leaves the PC unattended trickier in the context

of mobile devices, often used in public and crowded environments, where the device itself can be lost or forcibly stolen while the user session is active, allowing impostors to impersonate the user and access strictly personal data.

In these scenarios, the services where the users are authenticated can be misused easily. A basic solution is to use very short session timeouts and periodically request the user to input his/her credentials over and over, but this is not a definitive solution and heavily penalizes the service usability and ultimately the satisfaction of users. To timely detect misuses of computer resources and prevent that an unauthorized user maliciously replaces an authorized one, solutions based on multi-modal biometric continuous authentication are proposed, turning user verification into a continuous process rather than a onetime occurrence. To avoid that a single biometric trait is forged, biometrics authentication can rely on multiple biometrics traits. Finally, the use of biometric authentication allows credentials to be acquired transparently, i.e., without explicitly notifying the user or requiring his/her interaction, which is essential to guarantee better service usability. We present some examples of transparent acquisition of biometric data. Face can be acquired while the user is located in front of the camera, but not purposely for the acquisition of the biometric data; e.g., the user may be reading a textual SMS or watching a movie on the mobile phone. Voice can be acquired when the user speaks on the phone, or with other people nearby if the microphone always captures background. Keystroke data can be acquired whenever the user types on the keyboard, for example, when writing an SMS, chatting, or browsing on the Internet. This approach differentiates from traditional authentication processes, where username/password are requested only once at login time or explicitly required at confirmation steps; such traditional authentication approaches impair usability for enhanced security, and offer no solutions against forgery or stealing of passwords.

2. RELATED WORK

This paper presents a new approach for on-line handwritten signature verification, which exploits the potential of multiple reference sets. Preliminarily, system performance is estimated using different sets of reference signatures for each writer. Successively, reference sets leading to diverse system behaviors are enrolled into the personal knowledge-base and used in a multi-stage verification process. The experimental results show the effectiveness of the proposed approach, compared to traditional techniques. Keywords: Biometry, Classification, Dynamic Signature, Signature Verification, Multi-expert system.

The Anoto technology uses a non-repetitive pattern printed on paper to enable a camera-equipped pen to locate its absolute position on that pattern. This technology is also used on projection screens to create large-sized interactive areas, but suffers from the drawbacks such as shadow casting or space requirements. Up to now, no implementation exists that enables a tracking on LC-displays using the Anoto technology. Thus, we introduce Digisketch, which uses special films that can be applied to LC-displays, to back and front projections, or to glass, allowing pattern recognition for the pen's camera.

After describing the technical development of a prototype, we compare this new possibility of using Anoto compatible surfaces with other traditional tracking systems for LC-screens.

Hand written signature verification is an important utility in real time applications. It is required to verify identify fake signatures. Many existing techniques are based on the storke pixels and the underlying gray level values. Local Binary Patterns are used to obtain good results in offline signature verification. The experiments were made using GPDS corpus containing offline signatures. The corpus signatures are with uniform white background in invoices or cheques. Ferrero et al. proposed a novel offline signature verification technique that makes use of gray level features. Their technique was tested with offline signatures of various kinds in invoices and checks. In this paper, we implement that technique. We build a prototype application that demonstrates the proof of concept. The empirical results revealed that the prototype is useful in real time applications. A novel robust technique for the off-line signature verification problem in practical real conditions is presented. The technique is based on the use of compression neural networks, and in the automatic generation of the training set from only one signature for each writer. Our proposal also incorporates a new kind of acceptance/rejection rule, which is based on the similarity between sub images or positional cuttings of a test signature and the corresponding representation stored in the class compression network. Experimental results showed that the proposed technique reduces significantly the False Acceptation Rate (FAR).

This paper presents a brief survey on Speech Recognition and discusses the major themes and advances made in the past few years of research, so as to provide a technological perspective and an appreciation of the fundamental progress that has been accomplished in this important area of speech communication. After years of research and development the accuracy of automatic speech recognition remains one of the important research challenges (e.g. variations of the context, speakers, and environment).The design of Speech Recognition system requires careful attentions to the following issues: Definition of various types of speech classes, speech representation, feature extraction techniques, speech classifiers, and database and performance evaluation. The problems that are existing in SR and the various techniques to solve these problems constructed by various research workers have been presented in a chronological order. The objective of this review paper is to summarize and compare some of the well known methods used in various stages of speech recognition system.

3. USER STUDY

1. User Registration

In this module we are implementing the Client interface by which the Client can interact with the Application. To access the Application, the Client want to the register their details with Application Server. They have to provide their information like Name, Password, Date Of birth, Mobile Number and etc. This information will store in the database of the Application Server. The User is allowed to the access the application only by their provided Interface.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1803 - 1808
RECEIVED: 09-03-17 PUBLISHED: 24-03-17.
March 24, 2017

2. Finger print registration

In this phase, the we'll train the system according to identify the User's Finger by using the finger print device, so the user have give the finger print to train the system to identify the correct finger print to valid the user.

3. Signature registration

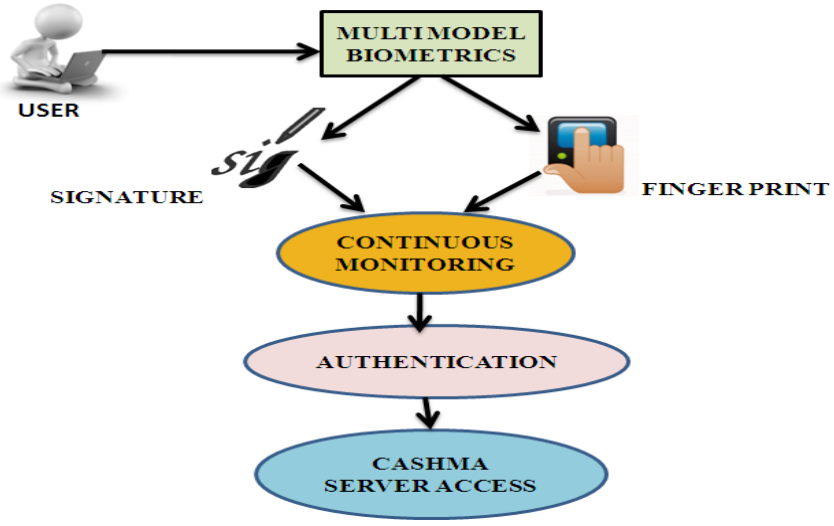
In this phase, the we'll train the system according to identify the User's Signature by using the mouse so the user have to gives 20 times of signature to train the system, here we are not using signature device which cost effective instead we use mouse signature to valid the user .

4. Finger print recognition

The Server will verify the finger print provided by the User while login with the Signature provided by the User when they provided during the Training Phase. If the finger print is not matched, then the Server will not allow the User to access their account.

5. Key stroke based signature recognition

The Server will verify the signature provided by the User while login with the Signature provided by the User when they provided during the Training Phase. If the signature is not matched, then the Server will not allow the User to access their account.



6. Banking authentication

Once the User provided both signature and finger print correctly, the Server will generate the Session Key using Secure Random Number generation algorithm and send it to the User Email id. Once

the User received their session key in their Email Once the Session key is verified by the Server, the User is allowed to access their account.

4. TECHNICAL APPROACH

There are many potential computer applications that are difficult to implement, for example applications that must perform some complex data translation, yet have no pre-defined mapping function that describes the mapping process, or those that must attempt to provide a 'best guess' as to the correct output when presented with noisy input data. One neural network that has been shown to be useful in addressing such problems is the feed-forward network

The input layer, where sets of data are presented to the network, is connected by bi-directional weighted connections to the hidden layer which is itself connected by bi-directional weighted connections to the output layer. all the weights in the network are modifiable, and the network learns to produce the correct input-output mapping by modifying these weights. the backpropagation network is an example of supervised learning, the network is repeatedly presented with sample inputs to the input layer, and the desired activation of the output layer for that sample input is compared with the actual activation of the output layer, and the network learns by adjusting its weights until it has found a set of weights that produce the correct output for every sample input.

CONCLUSION

We exploited the novel possibility introduced by biometrics to define a protocol for continuous authentication that improves security and usability of user session. The protocol computes adaptive timeouts on the basis of the trust posed in the user activity and in the quality and kind of biometric data acquired transparently through monitoring in background the user's actions. At present, our prototype only performs some checks on face recognition, where only one face (the biggest one rusting from the face detection phase directly on the client device) is considered for identity verification and the others deleted. While performing a client-side quality analysis of the data acquired would be a reasonable approach to reduce computational burden on the server, and it is compatible with our objective of designing a protocol independent from quality ratings of images (we just consider a sensor trust), this goes against the CASHMA requirement of having a light client.

REFERENCE

[1] CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.

[2] L. Hong, A. Jain, and S. Pankanti, "Can Multibiometrics Improve Performance?" Proc. Workshop on Automatic Identification Advances Technologies (AutoID '99) Summit, pp. 59-64, 1999.

[3] S. Ojala, J. Keinanen, and J. Skytta, "Wearable Authentication Device for Transparent Login in Nomadic Applications Environment," Proc. Second Int'l Conf. Signals, Circuits and Systems (SCS '08), pp. 1-6, Nov. 2008.

[4] BioID "Biometric Authentication as a Service (BaaS)," BioID Press Release, https://www.bioid.com, Mar. 2011.
[5] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr. 2007.
[6] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, "Quantitative Security Evaluation of a Multi-Biometric Authentication System," Proc. Int'l Conf. Computer Safety, Reliability and Security, pp. 209-221, 2012.
[7] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions," Proc. 21st Ann. Computer Security Applications Conf. (ACSAC '05), pp. 441-450, 2005.
[8] A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop Multimodal User Authentication, pp. 11-12, 2003.