Journal of Computational Intelligence in Bioinformatics
ISSN: 0973-385X Volume 4 Number 1 (2011) pp. 19–27
© Research India Publications
http://www.ripublication.com/jcib.htm

A Biometric Authentication Via Fingerprint Recognition Instead of Password Protection

A. Venkata Subramaniam[1], D. Karthikeswaran[2]
S. Dinakar [3], C. Marikkani[4] and RamKumar[5]

[1]Asst. Professor, [2]Lecturer, [3,4&5]Final IT Students
Jayaram College of Engineering and Technology, Trichy, India
E-mail: [1]ma231@rediffmail.com [2]karthids@gmail.com .
[3]s.dinakar27@gmail.com [4] c.marikkani@gmail.com .[5]. ramkumar7888@gmail.com

Abstract

Owing to the recent advancements in technologies, Computer technology is great opportunity to modern life. Notably, however, the tool needs to be coupled with efficient and reliable security mechanisms to ensure the medium can be established as a dependable one. Authentication of user’s logging in is of prime importance so that security is given by fair means. A new approach has been proposed so as to ensure that no unauthorised individuals are permitted to give the passwords.

Keywords: computer technology, biometrics authentication, fingerprint, user’s login.

Overview

Due to advancement in technologies day-day life we have to depend on it to make our self comfortable and feel secure. Moreover the more we depend on these technologies there rises a question for security issues. Security which is at the high level gives the secured and reliable environment, based on the collected statistical data from various communities,

The advancement in computer technology had made the wonder that every person depends on this everyday right from age of 10 and a survey depicts that the out of 10 persons in a community at least 9 persons depends on these technologies.

Password

A password is a secret word or string of characters that is used for authentication to prove identity or gain access to a resource. Ex: An access code is a type of password.

The passwords should be kept secret from those unauthorised users. The use of passwords is known to be ancient sentries would challenge those wishing to enter an area or approaching it to supply a password. Sentries would allow a person or group to pass if they knew the password.

In modern times, user names and passwords are commonly used by people during login process that access control to the protected computer operating systems, mobile phones, cable TV decoders, Automatic teller machines, etc.,

A typical computer may require passwords for many purposes logging into a computer accounts, retrieving e-mails from servers accessing programs, database, network, websites and even reading the morning newspaper online.

A Recent Practice

Now-a-days it is a common practice for computer system to hide passwords as they are typed. The purpose is to avoid by standers by reading the passwords.

Role of an Intruder

Attempting to crack passwords by trying many possibilities as time and money permits is a brute force attack. A related method, rather more efficient in more cases, is a dictionary attack, wherein all words in one or more dictionaries are tested. List of common passwords are also typically tested.

Statistical Data

The statistical data shows clearly that about 22% of user passwords could be recovered, 55% of my space passwords could be crackable and 25.6% of passwords using password cracking kit.

Keystroke	Duration
4 character lower or uppercase letter	A few seconds
4 character lower and uppercase letter	A few seconds
4 character lower and uppercase and number	A few seconds
5 character lower or uppercase letters (Ex: passb)	Under 60 seconds
5 character lower and uppercase letter (Ex: passB)	Approx 6 minutes
5 character lower and upper case and number password	Approx 15 minutes
8 character lower or uppercase password	Approx 58 hours
8 character lower and uppercase password	Approx 21 months
8 character lower and uppercase and number password	Approx 7 years
10 character lower or uppercase password	Approx 5 years
10 character lower and uppercase password	Approx 4648 years
10 character lower and uppercase and number password	Approx 26984 years

Risk Analysis of Biometric System

In Password Protection

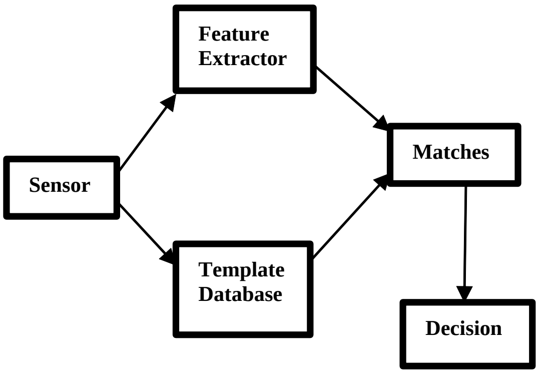


Figure 1: Biometric authentication system.

There are several problems and risks associated with the usage of biometrics in the authentication process. Some of them are:

Fake Input

One of the most common attacks on a fingerprint authentication system is of a fake input simply because this is the easiest mode of trying to gain access. It is a common practice for intruders to try to gain authentication by means of artificial fingers. Moreover researches are being conducted to overcome the artificial dummy finger prints to make the system reliable.

Low Quality Input

Fingerprint-matching techniques can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques first find minutiae points, and accordingly map their relative placement on the finger. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality.

Modification to the Biometric Database

The first step in any biometric recognition system is to store the template of an individual's feature so that it can be later used for authentication purposes. The place where these templates are stored is known as a database in most systems, and the process whereby the users will register their fingerprints for the first time is called ‘enrolment’.

Modifications to the Feature Extractor

The feature extractor may be attacked by intruders and modified, such that the legitimate fingerprint may be rejected and the unauthorized ones to be accepted.

Solutions

A new approach for authenticating individuals on the basis of their biometrics has gained name over the years. William et al for instance, explains that biometrics are unique physical features of an individual, such as fingerprints, iris, face, palm prints, etc. Fingerprint recognition systems are very common and popular due to their accuracy, ease, and proven track record . However, like any other biometric system, fingerprints also pose various threats and risks to the process of authentication .

Solution for low Quality Input

Proposed a method in which a pre-processing function is performed on the data to reduce the blur on the image. Subsequently, a pre-filtering operation is also performed so that the background can be reduced to a minimum. Along with these operations, segmentation of the fingerprint is also conducted by identifying the region of interest (ROI).

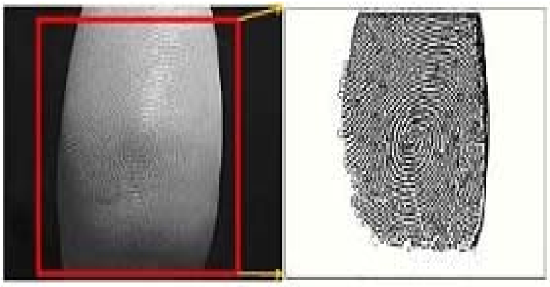


Figure 2: Fingerprint scan after pre-processing operation.

Here wherein, we propose that a webcam or a low-cost biometric sensor can also be used for the input, but the finger needs to be positioned only a few centimetres away from the objective lens, with the focal length of the lens needing to be tuned accordingly. Also propose a solution aimed at improving the quality of the image.

Solution to Overcome Fake Input

A method is proposed for handling the fake input for fingerprint recognition system— 'live-ness detection’. This term is also used by. Perspiration from the fingers is considered to be a sign of life which is obviously not present in the case of fake (dummy) fingers.

Solution to Overcome Modifications in the Database

To protect templates from fraudulent usage, which it involves using a distorted version of the biometric signal or the feature vector: if a specific representation of template is compromised, the distortion transform can be replaced with another one from a transform database. Data hiding and watermarking techniques have also been proposed as means of increasing the security of fingerprint images, by detecting modifications, and by hiding one biometric into another.

Disadvantage of using passwords

1. At odd times we tend to forget our passwords and it can be guessed, it should be as long as possible, not appear in the dictionary, and include symbols such as +, -, %, etc.,
2. A password should never be written down, never given to any other persons.
3. Should be changed at least every three months.
4. Any sedative technicians can break these passwords.
5. Proposed New Security System:

After a comprehensive study of the solutions that have been proposed so far, a new approach has been devised—fingerprint biometrics solution for password login in a public system with the use of intelligent security agent. The intelligent agent will use the following devices:

a. Mouse Applications

There are several fingerprint-scanning mice available, which will take the exam taker's fingerprints during the examination. For example, Digent offers a wide range of mouse including IZZIX FM 1000, IZZIX FD1000.

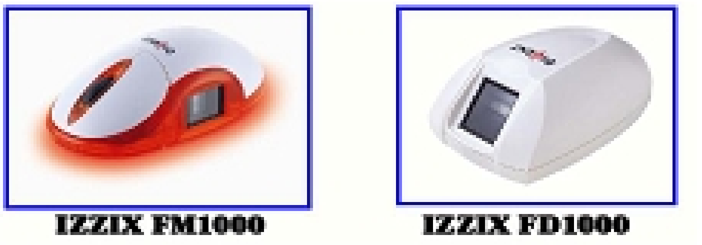


Figure 3: Fingerprint scan enabled mouse.

b. Keyboards

There are some keyboards also available in the market which can scan the fingerprint of the user whilst he is working, without any extra effort of getting his fingerprint scanned.

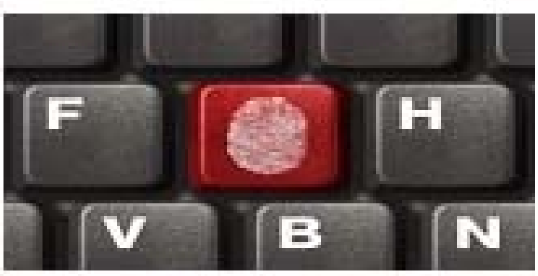


Figure 4: Fingerprint scan enabled keyboard.

Proposed Method

The first process in any biometric recognition system is 'enrolment', whereby all users who are supposed 'enrol' their fingerprints so that they are stored in the relevant login server database and biometric server database. All the fingerprint scans will be saved in an encrypted form to avoid any modifications.

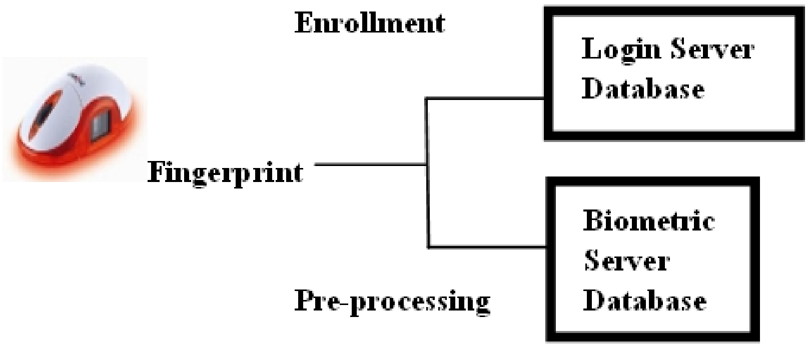


Figure 5: Enrolment.

When the client initiates the system, the intelligent agent assigns the user ID with an IP address so that the user cannot log-in from any other PC. The intelligent agent will then start extracting the fingerprint scans from the hardware devices mentioned above at every second, and the following steps will then be performed:

- Pre-processing operations shall be performed on these scans so as to ensure that there is minimal blur and noise present in the images.
- Test A: Additional live-ness detection tests will be performed by the intelligent agent to ensure that no dummy fingers are being used to pose as another user’s identity.
- Test B: After these initial operations, these scans will then be matched with the 'enrolled' scans which have been saved in the two server databases.
- If either Test A or B do not pass at any point of time, the access will then be immediately stopped for that specific user, and notification will be sent to the authorities for further action. This process will continue for the duration of the usage.

Idea behind the Proposal

The main grant of proposing this technique is to authenticate the users of a system while login in a public environment since there is a possibility that the bystanders may make note of your security passwords and intrude the contents by breaking the passwords at some costs by using third party programs.

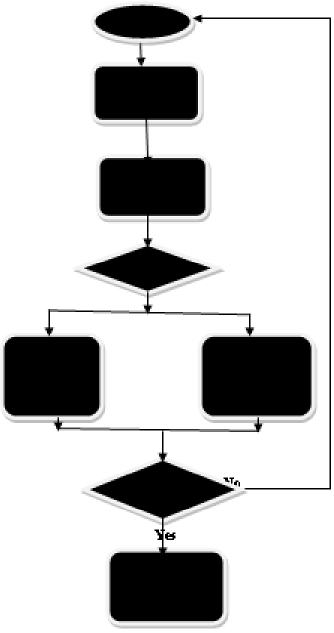
This system provides safer login to the remote users and the mechanisms flows as:

a. Mechanism

1. Sensors.

2. Feature Extractor.
3. Pre-Processor.
4. Matches with the database.
5. Decision.

b. Flow Chart



Advantages of the Proposed Solution

1. Since the fingerprints will be extracted whilst the user in working on the keyboard or the mouse, the pace of his work will not be affected.
2. The interval at which the fingerprints will be scanned is one second, which ensures that no other individual can take the exam on another student's behalf.
3. The scanned fingerprints will be saved in the two databases in an encrypted form to mitigate attacks from intruders.

Disadvantages

1. The interval at which the fingerprints are being scanned can prove to be very small and can cause storage problems for such a huge amount of data.
2. This approach requires an initial investment of providing students with the fingerprint scanning enabled devices.

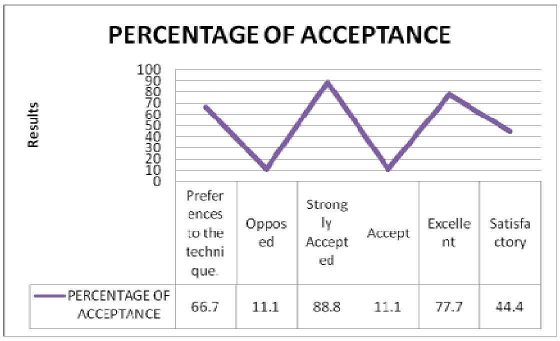
Steps to Handle Barriers

As soon as the e-exam is complete, the fingerprint scans should be completely analysed for the last time and then deleted so that the space can be available for the next exam. Another method of handling this can be to increase the time interval to at least three seconds so that the amount of data decreases to a reasonable degree.

Collected Facts

A survey conducted among students of Jayaram College of Engineering in Final Year Information Technology Department depicts the report which was plotted using MS-Excel as:

CATEGORY	PERCENTAGE OF ACCEPTANCE
Preferences to the technique.	66.70
Opposed	11.10
Strongly Accepted	88.80
Accept	11.10
Excellent	77.70
Satisfactory	44.40



Graph

Conclusion

A solution has been proposed to ensure a secure login environment in which user can be able to handle it in an ethical manner. It is very important to properly authenticate the remote loggers so that no unauthorised individuals are permitted access to the private contents of your system.

References

[1] C.G. King, R.W. Guyette, C. Piotrowski, 'Online exams and cheating: An empirical analysis of business students' views', The Journal of Educators Online, 6(1), 2009, http://www.thejeo.com/Archives/Volume6Number1/Kingetalpaper.pdf.

[2] M. Alavi, D. Leidner, ‘Research commentary: Technology mediated learning- a call for greater depth and breadth of research', Information Systems Research, 12(1), 1-10, 2001

[3] W. Huang, D. C. Yen, Z. X. Lin, J. H. Huang, 'How to compete in a global education market effectively: A conceptual framework for designing a next

generation eEducation system', Journal of Global Information Management, 12(2), 84-107, 2004

[4] K. M. Apampa, G. B. Wills, D. Argles, E. Marais, 'Electronic Integrity Issues in E-assessment Security', 2007

[5] E. Marais, D. Argles, 'Security issues specific to E-assessments', 8th Annual Conference on WWW Applications. Conference proceedings, Bloemfontein, South Africa, 2006.

[6] Vance, Ashlee (January 20, 2010). "If Your Password Is 123456, Just Make It HackMe". The New York Times.
http://www.nytimes.com/2010/01/21/technology/21password.html.

[7] The Memorability and Security of Passwords.

[8] Lyquix Blog: Do We Need to Hide Passwords?

[9] news.bbc.co.uk: Malaysia car thieves steal finger.\

[10] Top ten passwords used in the United Kingdom.

[11] Password Protection for Modern Operating Systems.

[12] http://support.microsoft.com/default.aspx?scid=KB;EN-US;q299656.

[13] "To Capitalize or Not to Capitalize?"

[14] Schneier, Real-World Passwords.

[15] http://www.cert.org/incident_notes/IN-98.03.html. Retrieved 2009-09-09.

[16] T Matsumoto. H Matsumotot, K Yamada, and S Hoshino, Impact of artificial 'Gummy' Fingers on Fingerprint Systems. Proc SPIE, vol 4677, Optical Security and Counterfeit Deterrence Techniques IV or itu.int/itudoc/itu-t/workshop/security/resent/s5p4.pdf pg 356

[17] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1001829,00.html