IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Biometrics Based Authentication Systems

[1]Dixita Dhobi,[2]Ajay Dhobi

[1]Lecturer,[2]Biomedical Service Engineer
[1]Biomedical Engineering Department,
[1]Parul University, Vadodara,India

Abstract: In this paper we outline the inherent strengths of biometrics-based authentication system, to identify the weak links in systems employing biometrics-based authentication also automated biometrics can provide the security advantages of long passwords while retaining the speed and characteristic simplicity of short passwords. Although, for illustration purposes, fingerprint authentication is used throughout, our analysis extends to other biometrics-based methods.

Index Terms **– Biometrics, password, accuracy, fingerprints.**

I. Introduction

Biometric readings, which can be anywhere from a few hundred bytes to over a megabyte in size, have the advantage of having a higher information content than a password or pass phrase. To get similar bit strength, just increasing the length of passwords causes severe usability issues. A 2K sentence is nearly impossible to memories, and typing such a phrase takes an excruciatingly long time (especially without errors). Fortunately, automated biometrics can combine the security benefits of long passwords with the speed and convenience of short passwords. Even though automated biometrics can help solve some of the challenges associated with current user authentication methods, hackers will still identify vulnerabilities in the system that can be exploited. Systems that required passwords for security purpose..

Even while automated biometrics can help solve some of the challenges associated with current user authentication methods, hackers will still identify flaws in the system that can be exploited. Brute force dictionary attacks are common in password systems. Biometric systems, on the other hand, necessitate a significant amount of work to launch such an assault. In the biometrics area, however, various new sorts of attacks are feasible. This may not apply if biometrics is used as a supervised authentication tool. But in remote, unattended applications, such as Web-based e-commerce applications, hackers may have the opportunity and enough time to make several attempts, or even physically violate the integrity of a remote client, before detection.

II. Biometric Accuracy

The accuracy of biometric technology is an important consideration when choosing the right one. The system's capacity to distinguish genuine matches from imposters is referred to as biometric accuracy. A matching score is used to authenticate or deny the user's identification when the live biometric template is compared to the saved biometric template. The False Acceptance Rate (FAR) and False Rejection Rate (FRR) are used by system designers to determine the acceptable level of accuracy for the system (FRR). The False Rejection Rate (FRR) is the statistical probability that a biometric system will be unable to validate an enrolled individual's lawful stated identification or would fail to identify an enrolled person. The statistical probability of False Acceptance or faulty verification is referred to as the False Acceptance Rate (FAR). Both False Rejection and False Acceptance provide a security risk in the most prevalent scenario.

A false acceptance occurs when a mismatching pair of fingerprints is accepted as a match. A mistaken reject, on the other hand, occurs when the system rejects a matching pair of fingerprints. The threshold determines the mistake rates. Plotting FAR against FRR with the decision threshold as the free variable is a common way to show the interplay between the two mistakes. The ROC (Receiver Operating Characteristic) curve is the name of this graph. The two errors are complementary in the sense that if one tries to reduce one of them by adjusting the threshold, the rate of the other error increases. The relative false accept and false reject rates of a biometric authentication system can be controlled by selecting a certain operational point (i.e., a detection threshold). It is impossible to achieve extremely low (near-zero) error rates for both FAR and FRR at the same time. The FAR error can be near to zero if the threshold is set high enough, while the FRR rate can be close to zero if the threshold is set low enough. The FAR versus FRR error rates at that operating point may be substantially different, depending on the application requirements. Instead of the frequently recommended equal error rate (EER), biometric systems function at a low FAR to give strong security.

III. Fingerprint Authentication

Fingerprints are a distinguishing trait that, with exception of scrapes and bruises, stay unchangeable throughout a person's lifetime. A fingerprint impression is taken as the initial stage in the authentication process, usually with an inkless scanner. There are several scanning technologies available. Figure 5A displays a fingerprint obtained using an optical sensor and a scanner. The fingerprint impression is digitized at 500 dots per inch (dpi) with 256 grey levels per pixel in a standard scanner. In terms of ridge bifurcations and ridge ends, the digital representation of the fingerprint has various distinct features known as minutiae.

IV. Components Of a Fingerprint System

A matching algorithm can be implemented in one of two ways: by employing identity matching or authentication matching. One fingerprint is compared to several fingerprints using an Automated Fingerprint Identification System (AFIS) that consists of several computers and a database storage system in identification matching. There needs to be only one fingerprint terminal and a token loaded with the fingerprint template in authentication matching, where there is a "one to one" fingerprint comparison. Matching could take place on the token, in the terminal, or in both the terminal and the token.

In which, Capacitive, optical, thermal, and pressure sensitive (resistive) technology are all used to make electronic fingerprint sensors. When the ridge is darker than the valley, these distinct types of sensors can provide an image of the fingerprint. Capacitive and optical sensors are the most prevalent sensors on the market today. Optical sensors provide the finest image quality, but they are also the most expensive and can be tricked by phoney fingers. Capacitive sensors provide a good blend of image quality and cost, yet certain fake fingers can deceive this technology as well. The most common silicon fake fingers, on the other hand, cannot trick a capacitive sensor because they lack electrical characteristics.

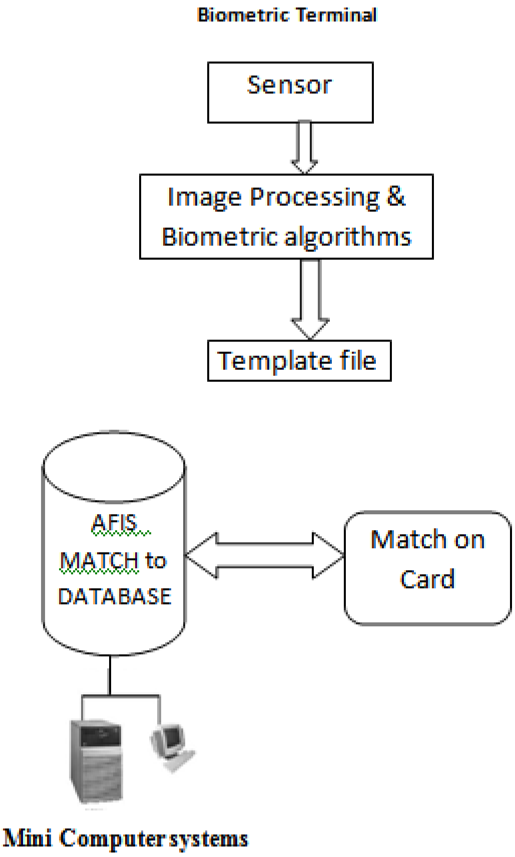

fig. Components Of a Fingerprint System

References

[1] A. Jain et al: BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, ISBN 0-7923-8345-1

[2] Anil K Jain, Arun Ross and Salil Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no.1, pp. 1-29, 2004.

[3] Choudhury B, Then P, Issac B, Raman V and Haldar M K, “A Survey on Biometrics and Cancelable Biometrics Systems”, International Journal of Image and Graphics, pp. 1-28, 2018.