INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

CONTINUOUS VERIFICATION USING BIOMETRICS (2-FACTOR AUTHENTICATION)

Gadgi Sumangala
sumagadgi05@gmail.com
Department of Computer science and Engineering, Bheemanna Khandre institute of technology, Bhalki

Abstract-This project describes the theory, architecture, implementation, and performance of a bio-metric verification system that continually verifies the presence/participation of a logged-in user. To achieve robustness we have implemented the concept of 2-Factor Authentication, i.e. using the combination of biometrics (something we are) and text-password (something we know) for authenticating users. During the enrolment phase the user has to register with his name, password and finger-print. The finger-print and the text-password are stored against the user's name in the database. Continuous verification is achieved using a finger print scanner. The main thrust of work is to build a biometric feedback mechanism so that verification failure can implicitly/automatically log-off the computer. After every explicit log-off the user will be given a new, system generated 3 digit numeric passwords, which he will have to use in his next log-in. This project proposes a concept to make the system strong and secure by combining multiple suitably chosen modalities in a theoretical framework.

Keywords: Biometric, CLL, CLR, FAR, FRR, Minutiae Algorithm

1. INTRODUCTION

By 2-Factor Authentication we mean: User's fingerprint, His text password. By continuous verification we mean that the participation/presence of the user accessing the computer is continually verified. Verification is an operation in the normal usage of a computer system because we can assume that the user's identity has been already established by a preceding strong authentication scheme. We believe that Continuous verification, if realized efficiently with low false positives, can be vital in high risk environments where the cost of unauthorized use is high. This can be true for computer driven airline cockpit control, computers in banks, defense establishments, and other areas whose use directly affects the security and safety of human lives and proper-ties. Biometric verification is appealing because several of them are easy to implement in ordinary systems and eliminate the need to carry extra devices for authentication. How-ever, biometric verification can be interpreted as a matching problem and usually makes a probabilistic judgment in its classification. This makes it error prone. Building an effective reactive biometric verification system consists of many aspects. Not only must the verification results be integrated, it can be critical to balance several conflicting metrics: namely, accuracy of detection, system overhead incurred during the verification, and reaction time i.e., the vulnerability window within which the system must respond when it detects that the authorized user is no longer present. This relationship is especially important when all these aspects are performed in software on the same machine that is being protected from unauthorized use. As a secondary authentication mechanism we use the random password generation concept. We use this technique so that the user gets a new numeric password for every session.

In the rest of the paper we describe the theoretical aspects of our continuous biometric verification system, our implementation architecture and the performance impact of such a system on ordinary computer use. The goal is to render the computer system inoperable within a certain time period of verification failure.

1.1Aims and Objectives

To build, a user biometric verification mechanism based on the concept of 2-Factor Authentication, that continually verifies the presence or participation of a logged-in user.

1.To achieve a robust system by combining biometrics (fingerprint scanning) and text-passwords(randomly generated) as a form of authentication.

2. To build a safe and secure system by combining multiple suitably chosen modalities. To develop a strong security mechanism to authenticate and authorize the users.

1.2 Current System

Currently systems are fully implemented with different types of authentication schemes like smart cards, various biometrics and text passwords.

Figure 2.1: Current System

2.1 Loopholes in the Current System

Although these systems have many authentication schemes, all are used to authenticate the user only before the user logs in. The proposed system has a facility to continuously verify the participation/presence of the logged-in user, and hence we call it Continuous Verification Using Biometrics, a 2-Factor Authentication mechanism.

3. Proposed System

Our Proposed System eliminates the loopholes of the current system. This system uses the concept of Continuous Verification and continuously verifies the logged-in user and if the user is valid then the session is continued else the session terminates.

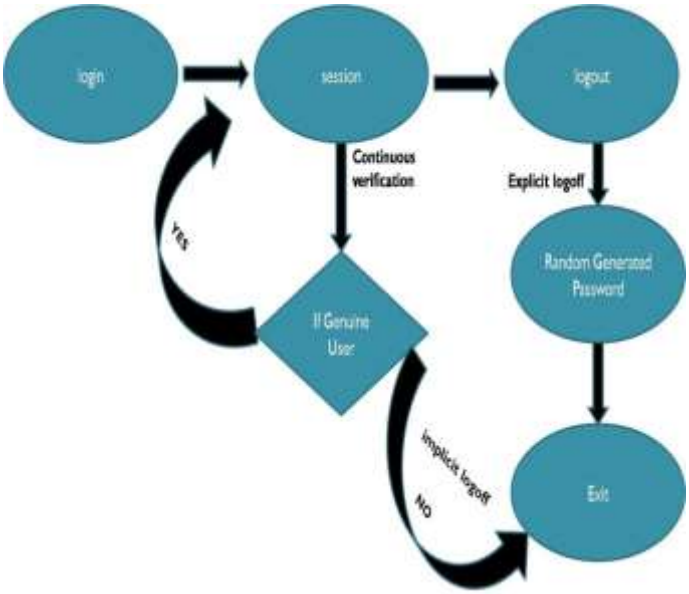


Figure 3: Proposed System

3.1 Technology for Proposed System

3.1.1Fingerprint: A Biometric

Presently, fingerprint biometrics are the most widely adopted biometric technologies in the industry. This is because the stability and uniqueness of the finger-print are well established. For instance upon careful examination, it is estimated that the chance of two people, including twins, having the same fingerprint is less than one in a billion people. In Digital Mainstream, many fingerprint scanners work by analyzing the position of minutiae which are small unique marks on the finger image. To further elaborate, minutiae are the points where two ridges on a fingertip meet.

FEATURES:

1. Fingerprints are unique.
2. They are a pattern of ridges and valleys.
3. Minutiae points are the characteristics that occur, either at a ridge ending or at a ridge bifurcation.
4. A ridge ending is the point where a ridge ends abruptly.
5. A ridge bifurcation is the point where ridge splits or unites.

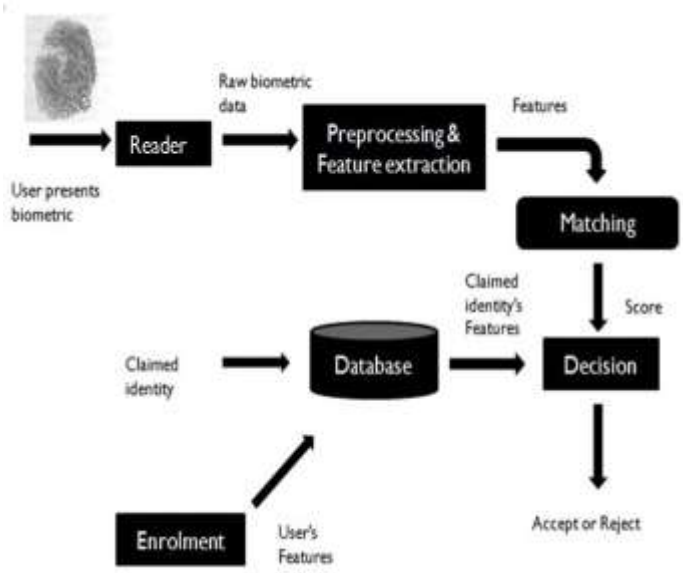


Figure 3.1: Working System

3.2 Fingerprint scanners use a procedure that consists of four Stages:

CAPTURE-This stage refers to the physical or behavioral sample that is captured during the enrolment process.

Figure 3.2: Fingerprint template

EXTRACTION-This stage refers to the extraction of unique data from the captured sample which is used in the creation of a template.

COMPARISON-In this stage comparison between the new sample and the enrolled sample, imprinted on the

template is carried out and a match-score is generated.

MATCHING-Finally, the matching stage uses the match-score to determine whether the new sample matches the enrolled sample or not.

3.3Methodology for Proposed System

3.3.1 Minutiae Algorithm

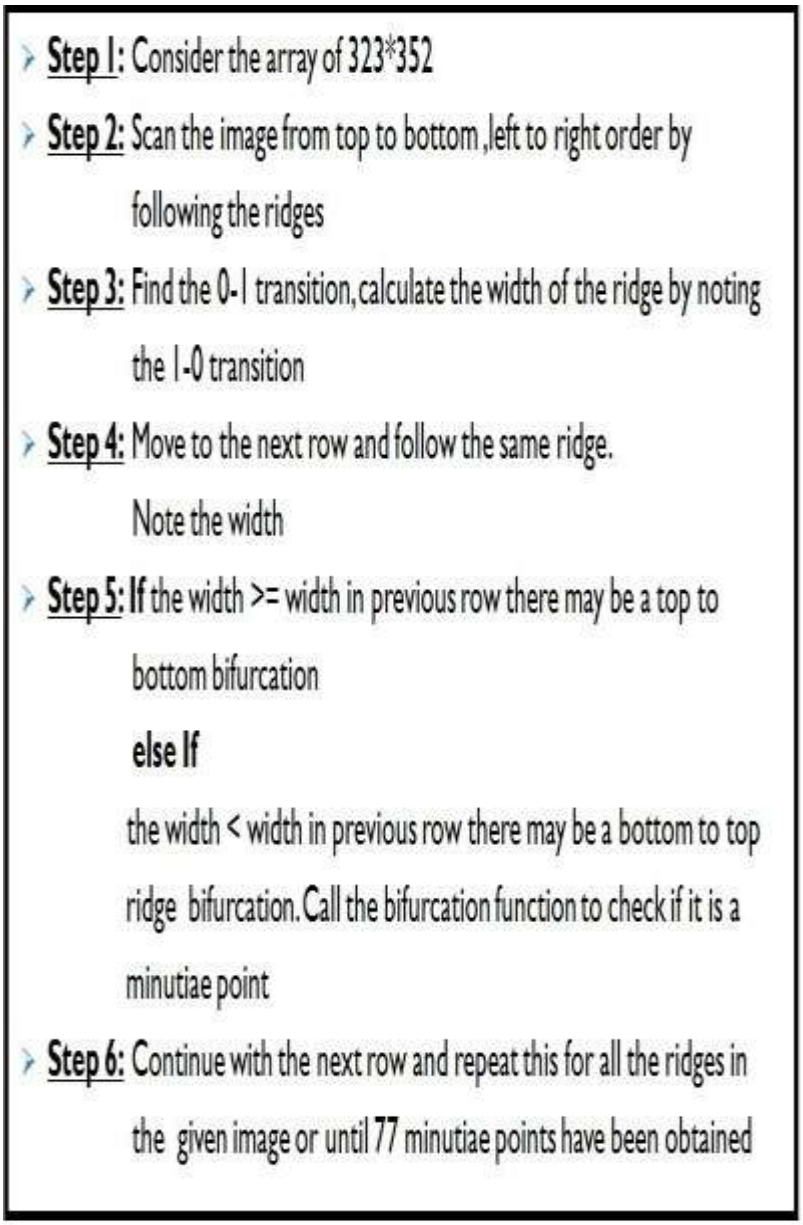
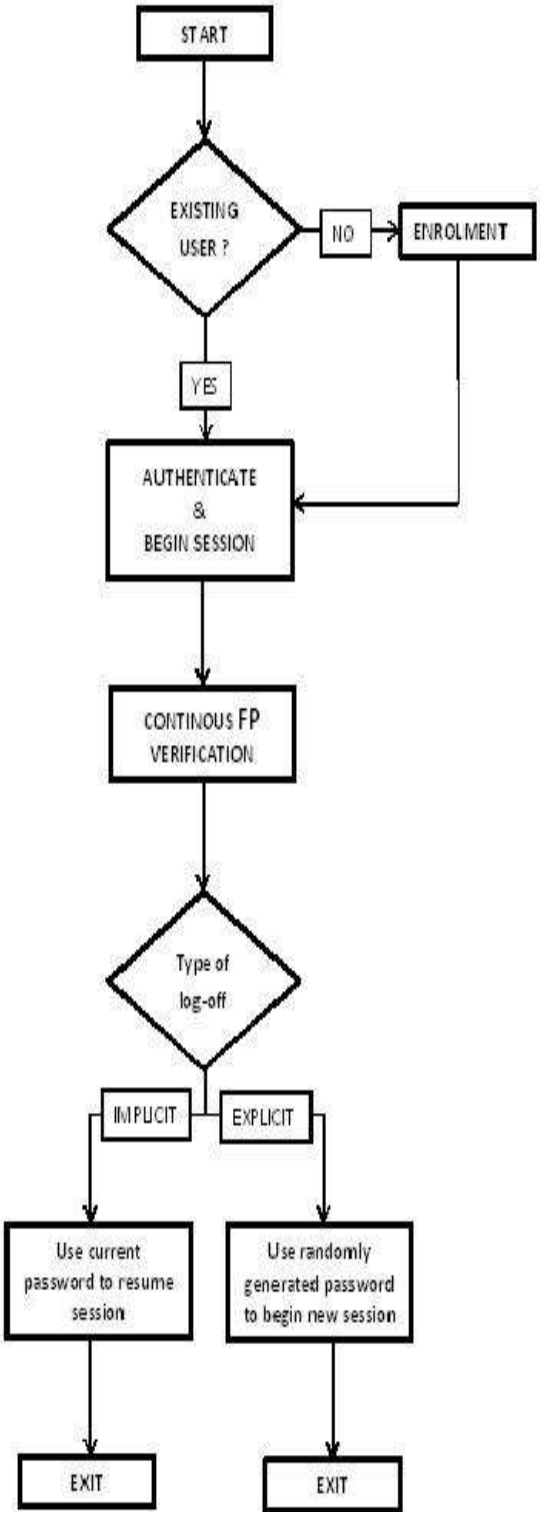


Figure 3.3: Minutiae Algorithm

3.4Activity Diagram and Flowchart

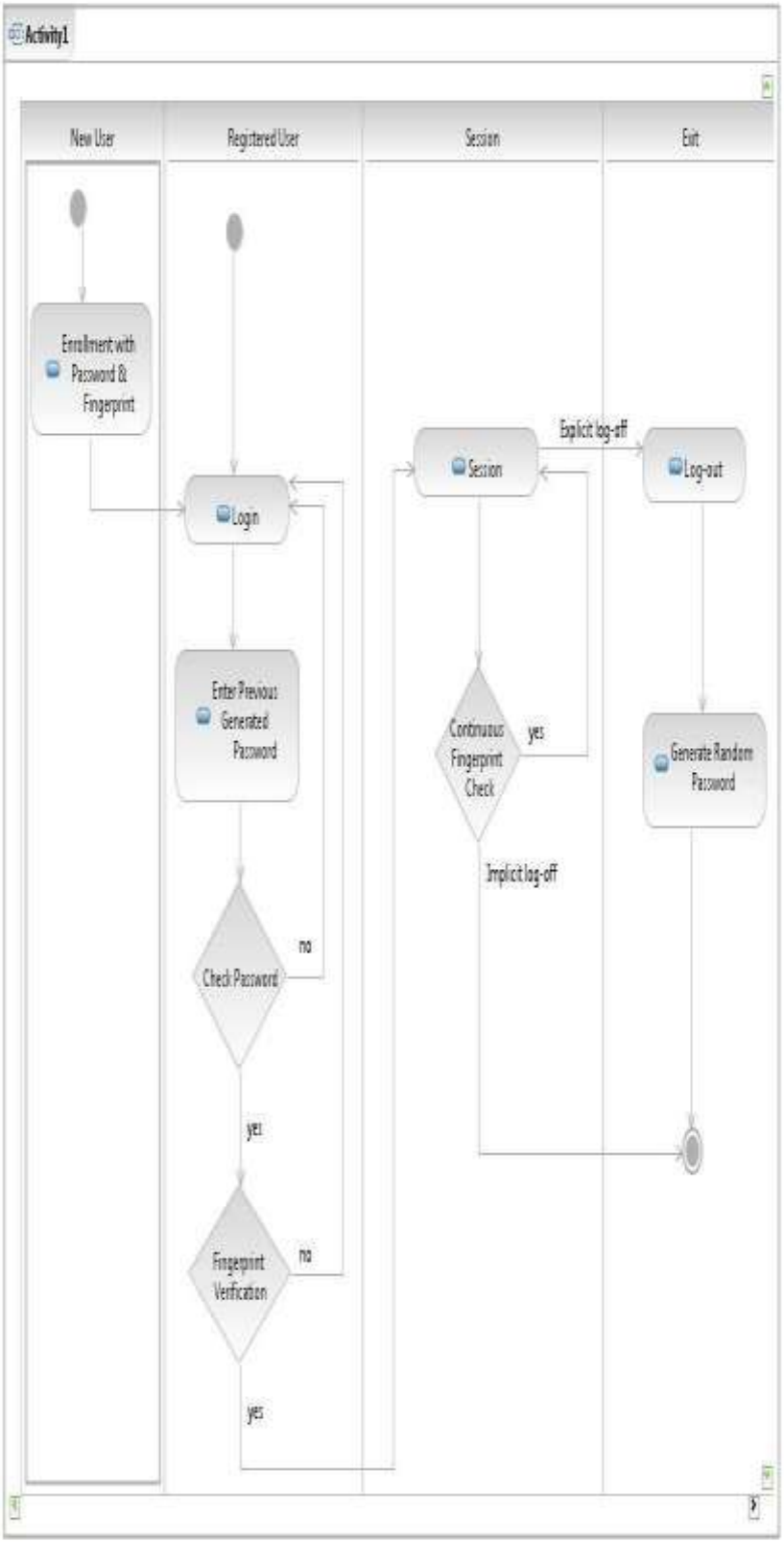
3.4.1 Activity diagram

Figure 3.4.1: Activity Diagram



3.4.2 Flow Chart

Figure 3.4.2 Flowchart



As we are designing a biometric application, we specify the requirements related to the system. In the two sections to follow, we list out the Hardware and Software specifications.

Figure 3.4.3: Hamster Finger Print Scanner

4. Implementation and Coding

The Microsoft.NET platform provides all the tools and technologies that you need to build web applications. It exposes a language independent, consistent programming model across all tiers of an application while providing seamless interoperability with easy migration from existing technologies. The .NET platform fully supports the Internet's platform neutral standard based technologies including HTTP, XML and SSL protocol, which is a language specially designed for building applications in the .NET environment. As a developer, you will find it useful to understand the Rationale and features that provide the foundation for the .NET platform before you start writing code.

4.1 Features of .NET

1. **Easy for developers to use** In the .NET Framework, code is organized into hierarchical namespaces and classes. The Framework provides a common type system, referred to as unified type system, that is used by any .NET language.

Common Language Runtime Engine The Common Language Runtime (CLR) is the execution

1. engine of the .NET Framework. All .NET programs execute under the supervision of the CLR, guaranteeing certain properties and behaviors in the areas of memory management, security, and exception handling.
2. **Language Independence** The .NET Framework introduces a Common Type Sys-tem, or CTS. The CTS specification defines all possible data types and programming constructs supported by the CLR and how they may or may not interact with each other conforming to the Common Language Infrastructure (CLI) specification. Because of this feature, the .NET Framework supports the exchange of types and object instances between libraries and applications written using any conforming NET language.
3. **Simplified Deployment** The .NET Framework includes design features and tools which help manage the installation of computer software to ensure it does not interfere with previously installed software, and it conforms to security requirements.
4. **Security** The design is meant to address some of the vulnerabilities, such as buffer overflows, which have been exploited by malicious software. Additionally, .NET provides a common security model for all applications.

   Portability While Microsoft has never implemented the full framework on any system except Microsoft Windows, the framework is engineered to be platform agnostic, and cross-platform implementations are available for other operating systems. This makes it possible for third parties to create compatible implementations of the framework and its languages on other platforms.

5. GUI Explanation

Figure 5.1: Start page

Figure 5.2: Administrator Login Page

Figure 5.3: User Login Page

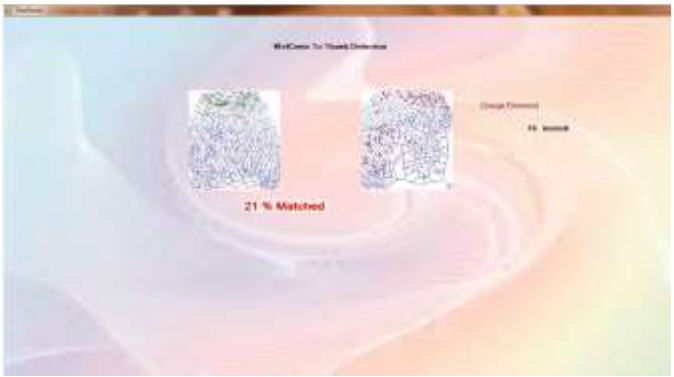


Figure 5.4: Fingerprint verification Page

dbo.info: Table(...CATION\MANU.MDF)

Column Name	Data Type	Allow Nulls
id	nchar(10)	☐
name	nvarchar(MAX)	☐
pass	nvarchar(MAX)	☐
phn	nchar(10)	☑
image1	nchar(10)	☑
		☐

Figure 5.5: Database Details

info: Query(abh...ATION\MANU.MDF)

id	name	pass	phn	image1
001	ab	412	9561708765	001.bmp
002	manish	770	9890790176	002.bmp
003	Kanchan	123	9890817474	003.bmp
004	anand	444	9004405585	004.bmp
005	rr patil	rr	9870583919	005.bmp
007	gs	116	1234657890	007.bmp
NULL	NULL	NULL	NULL	NULL

Figure 5.6: Content of Database: info

Figure 5.7: Session Page

Figure 5.8: Randomly Generated password after explicit shut down

6. Design Issues and Challenges

Biometric system deals with the physical characteristics of living body. So While designing a biometric system, there always be some designing issues and challenges regarding accuracy and uses. We have listed out some common designing challenges and their descriptions are as follows:

1. False Accept Rate (FAR)

This deals with the wrong accept rate i.e user is not the valid even though system is accepting it as a valid user. This rate must be as small as possible.

2. False Reject Rate(FRR)

This deals with the wrong rejection rate i.e user is valid but system is not allowing him to use it. This rate required to set very carefully. It neither be very high nor too small.

3. Failure to enroll

Since biometric system is not very well known to all. So there may a problem while enrolling with the biometric system. To avoid this suitable instruction must be provided to each and every users before using the system.

4. Failure to Capture

It is very common designing problem for the biometric system. So developer must have to pay attention regarding the device failure.

7. Future Scope and Application

- **Medical management-** Restricting access to patient data in hospitals. Managing access to individual computer systems and applications by medical staff. To improve security for prescription distribution.

- **Banks and financial organizations**-This biometric method also used in many banking and financial applications.

- **Commercial usage-such as electronic data security and e-commerce-**To combat the increasing fraud in online payments and financial transactions. It ensures the highest available security level to authenticate and authorize users. Minimizes the security breaches as in case of text-password. Enables highly personalized authentication schemes.

- **Airline traffic control, Defense sectors and intelligence department-**Minimizes the security breaches as in case of text-password Enables highly personalized authentication schemes. This technology has also used in research institutes.

8. Conclusion

We believe that the reactive system we have set out to build works reasonably well at this point. Biometric verification is the main bottleneck in the computation. Although our continuous verification technique is new, it is about how to integrate bio-metrics as a useful general abstraction so that all processes can gain from it, with the aim of enhancing the security of the system. Now that newer biometric devices are commonly appearing that can permit passive biometrics to be integrated into normal computer use, such abstractions can be useful to investigate at a lower layer so that computer response can be provided in a more general and encompassing manner. With a rapid growth in technology many factors such as security breaches, transaction frauds are also in the increase worldwide. Adopting biometrics helps to maintain security, surveillance and safety.

Hence in this paper, we present the design and implementation of a system which can be very promising and efficient in places where the security requirement level is very high.

8. References

[1]Device Information Retrieved from (2nd Feb 2012).http://fingerprintscanner.bioenabletech.com/products/usb-fingerprint-scanner.

[2]http://sourceforge.net/scm/type=cvs/groupid=146099.

[3]http://www.biometricsintegrated.com/KnowledgeCentre/Downloads/tabid/93/Default.aspx.

[4]http://fingerprintscanner.bioenabletech.com/applications/public/.

[5]http://www.griaulebiometrics.com/en-us/downloads/.

[6]http://stackoverow.com/questions/41107/how-to-generate-a-random-alpha-numeric/.