Multi-Layered Security By Embedding Biometrics in Quick Response (QR) Codes

K. Lakshmanaswamy[1]
Dept. of Computer Science & Engineering
Saveetha School of Engineering, Saveetha University
Chennai, India

Debajit Das Gupta[2]
Dept. of Computer Science & Engineering
Saveetha School of Engineering, Saveetha University
Chennai, India

Sailesh Toppo N.[3]
Dept. of Computer Science & Engineering
Saveetha School of Engineering, Saveetha University
Chennai, India

Biswajit Senapati[4]
Dept. of Computer Science & Engineering
Saveetha School of Engineering, Saveetha University
Chennai, India

***Abstract*—Biometrics is now-a-days becoming more popular and prolific in highly secured areas where security is concerned with much priority. But with the advancement in technology, fingerprints can be easily duplicated & secured areas can be trespassed. QR code is another important innovation in the field of data storage which stores data in 2D format containing alphanumeric characters arranged in a matrix order. Moreover the disadvantage of misusing biometrics can be overcomed. Keeping in mind with the fact, the authors come up with the idea of transfusing Biometrics in QR codes which would not only provide much security to the prevailing system, but also reduce in many cost factors and complicacies. Such a kind of system can be used in highly authenticated areas where security is highly concerned. This system can also be implemented in MNC's where employees' need to shift to other branches or departments for a particular span of time.**

Index*—Authentication, Biometrics, QR codes, AES, Signal Processing

I. INTRODUCTION

In this present world of technology and highly advanced secured services, biometrics has been widely used in many national and international organizations, agencies and bureaus. The main purpose of this biometric system is manifold including data entry of the inflow and outflow of persons in the organization, entry of only authorized personals, also in some areas used for mode of attendance too. Despite the advantages of biometrics, the data is very sensitive in the sense that a person cannot change a biometric trait. Biometric recognition systems should preserve the users' privacy by storing data in a much procured way. Fingerprint is considered highly risky as it can be traced easily. It means that fingerprint data may be seized without knowledge or consent, and used for unrevealed purposes.

QR (Quick Response) Code is a type of 2-D bar code in the form of Matrix which was developed by Denso Wave. It is composed of black and white modules which became wildly known and used because of its reading speed, accuracy and functionality characteristic. It contains information in both vertical and horizontal direction. The maximum data capacity, within version 40 of the QR Code, is 7,089 numeric characters or 4,296 alphanumeric characters. QR Codes provides information for products in industry, data on a mailing label, or information on a business card. It is small in size and the pattern can be hidden or integrated into an aesthetically attractive image in any printed form such as newspapers, magazines, or clothing. Data can be converted into QR code by any means of QR generator which can be later electronically displayed or printed.

In this paper, the authors propose the idea of collaborating biometrics within a QR code so as to overcome the disadvantages of the former. In the proposed system, the security would be two fold, i.e. the fingerprint of user will be loaded into the database and the overall information of the user including his/her name, designation, department, and etc. along with the user's fingerprint will be embedded into a QR code. As a user try to access permission for an authenticated service, he/she would be asked for a fingerprint scan. As the scan goes through the database, it asks for the QR code which contains the overall information of the user.Then the system compares with the output of the data from the fingerprint scan in the database and the QR code data, if both the data matches 100%, the person is allowed to access the service.

Advantages of biometrics

Biometrics is a feature which identifies and authorizes an individual over information using physiological features such as iris scans, face recognition,

voice recognition, fingerprint scans and DNA tests. The main advantage of biometrics is that it uniquely identifies an individual even when there are variations in time. It minimizes ID fraud, buddy punching.
Biometrics eliminates the problems when an ID card is lost or the password is forgotten by the user.

Disadvantages of biometrics

The disadvantage in biometrics is that 2D recognition it affected when a person's hair colour is changed and when the persons age increases. Sometimes when a person's voice changes due to cold he/she cannot be recognized by the biometric system.

Advantages of QR codes

QR codes stores information's that appear in magazines, business cards or any product that the user needs to know about.

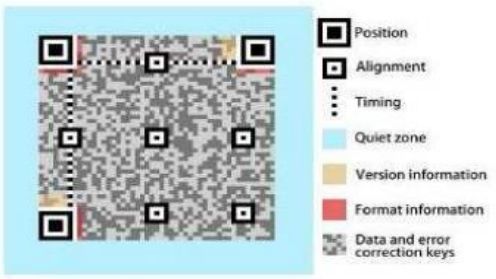


Fig.1: QR code architecture

Disadvantages of QR codes

The main disadvantage of QR code is sometimes it takes a lot of time to process identifying the data.

II. PROPOSED AUTHENTICATION SYSTEM

A. SYSTEM ARCHITECTURE

We are proposing a new system which will strengthen the privacy of the user. In our implementation, we are combining the biometrics with that of QR codes so that forgery may be reduced. Firstly we are going to process the user's biometric data for use by system in subsequent authentication operations. Then, we are going to extract the biometric features and store it in the database/repository. Then we are going to create a QR code based on the user's information and store it in the software so that it may be a two tier security system which will be easier to find the forgery done by people. Fig 1: The tier 1 architecture shows that the biometric of a person is collected and then it is sent to a transmission which contains compression, encryption, decryption and decompress. We are going to use an AES algorithm which is encrypted to each data block so that it can prevent attacks from the outside world. After the encryption and decryption the signal is processed and sent to a quality checker where it checks whether the quality of the biometric is good or not. If the quality is badthe biometric device asks the user to give the input again. If the quality is sufficient it generates a template and matches with that of user's data residing in the database. Fig 3: The tier 2 architecture shows that the data is encrypted in the form of QR codes using a QR code generator. Once the user wants to get authorization the QR code reader will scan the data through a QR code reader. If the data matches the user is authorized.

Advantages of proposed system

The system thus so proposed has many advantages over the conventional usage of biometrics.

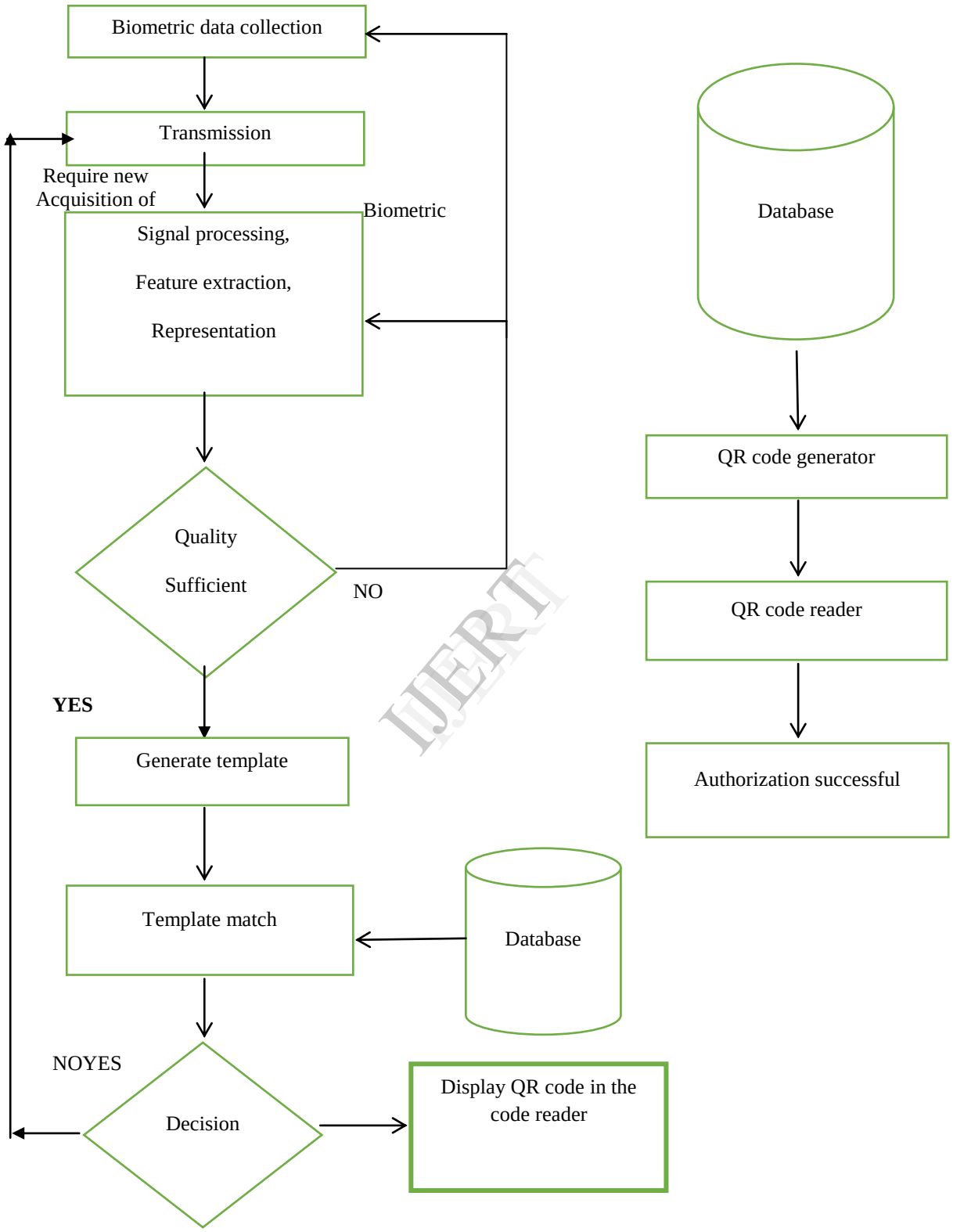
- Two tier authentication
- Enhanced security level
- Lower complicacies

III. APPLICATIONS

The proposed system has many applications in the daily life:
E.g.: an employee of a company is requested to offer service for another branch or department of the same organization for a limited period of time till the project or the service work sustains. For this, the company has to provide the employee with a new set of ID card & also has to amend changes in the authenticated entrance in respective branch or department to authorize the employee. According to the conventional method, the organization just needs to change in the biometric system so as to allow the employee which can be misused. But the proposed system manages change in the biometric system database for the specific period of time providing a unique key in the QR code which would enhance the authentication of entrance. The system would also create a session timing of the entry and exit of the new alien employee which can be viewed by the database administrator. The key in the QR code would expire for the specific newly assigned location after a stipulated period of time, which would prevent further entry of that employee into the said location. If the service or the project

Fig 2. System architecture – tier 1

Fig 3. System architecture – tier 2



work's designated time needs to be extended, both the departments, or the branches need to agree for the extension of the expiry of the key in the QR code.

This system can also be used in many highly secured, authenticated and authorized areas where security is highly mattered like in defence and research areas.

IV. CONCLUSION

The conventional mode of authentication is pretty unsecure where security systems can be bypassed and misused. By providing such an updated and highly secured two tier system, would not only bring a change in the security service but also provide the ease in many areas. The proposed system would be helpful in many of key security prioritized areas and also in many of organizations.

V. REFERENCES

1. AglikaGyaourova&Arun Ross, *A Coding Scheme for Indexing Multimodal Biometric Databases*
2. Mauricio Ramalho, Paulo Correia, LuísDuclaSoares, *Distributed source coding for securing a hand-based biometric recognition system*
3. Ji-Hong Chen, Wen-Yuan Chen and Chin-Hsing Chen, *Identification Recovery Scheme using Quick Response (QR) Code and Watermarking Technique***Appl. Math. Inf. Sci. 8, No. 2, 585-596**
4. KalpeshAdhatrao, Aditya Gaykar, RohitJha, VipulHonrao, *A secure method for signing in using quick response codes with mobile authentication*
5. SartidVongpradhip, *Use Multiplexing to Increase Information in QR Code*
6. Rima Belguechi, Estelle Cherrier, Christophe Rosenberger, Samy Ait-Aoudia, *Operational bio-hash to preserve privacy of fingerprint minutiae template*s **ISSN 2047-4938**
7. Jonathan Blackledge, Eugene Coyle, *Authentication of Biometric Features using Texture Coding for ID Cards*
8. MukundSarma, *Second Level Authentication Using QR Codes***ISSN 0974-2247**
9. David PintorMaestre, *QRP: An improved secure authentication method using QR codes*
10. NituMujumdar, PoojaShinde, KarishmaThigale, Sanjay Agrawal *Application Of Smart Phone QR Code And Fingerprint For Anti-Counterfeiting***ISSN: 2278-0181**
11. Namita Chandra, AshwiniTaksal, DhanshriShinde, Prof.ArchanaLomte, *Sensitive Data Protection Using Bio-Metrics***ISSN: 2277 128X**
12. http://en.wikipedia.org/wiki/QR_code