IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013
ISSN: 2320 - 8791
www.ijreat.org

Enhancing Security in Identity Documents Using QR Code

RevathiM K[1], Annapandi P[2] and Ramya K P[3]

[1]**Information Technology, Dr.Sivanthi Aditanar College of Engineering, Tiruchendur, Tamilnadu628215, India**

[2]**Information Technology, Dr.Sivanthi Aditanar College of Engineering, Tiruchendur, Tamilnadu628215, India**

[3]**Information Technology, Dr.Sivanthi Aditanar College of Engineering, Tiruchendur, Tamilnadu628215, India**

Abstract

In earlier days we didn't have any certificate verification techniques, only the checking of marks is done by the person. Due to these verification methods so many mistakes are happened like duplication of marks in the mark sheet. Our system consists of QR reader and Biometrics finger print readers which are used to verify the certificate originality in order to eradicate fraudulent certificate. The procedure involved in this paper is getting the QR code the certificate and finger print of the person during the run time. Then the fingerprint is verified with that of the stored one, if it matches then the approved mark statement will be provided. As a result of completing the above procedure the security if identification document is increased. A running version of the system will have only one Administrator but it typically has multiple end users like educational institution, industries and etc. The administrator is responsible for managing user accounts, system resources and logs and for the health and safekeeping of the system. Educational institution, industries and other users have the responsibility of verifying the certificate as assigned by the administrator.

Keywords: *Fingerprint, QR Code*

1. Introduction

In today's world security for document is become more and more important. One area where security can be improved is in authentication. Biometrics is an automated method of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Physiological characteristics are derived from the measurement of the part of a person's anatomy. Examples of physiological characteristics are hand, finger images, facial characteristics, and iris recognition. Behavioral characteristics are traits which can be learned or acquired. Dynamic signatures verification, speaker verification, and keystroke dynamics are examples of behavioral characteristics. Biometrics system uses hardware to capture the biometric information, and software tomaintain and manage the system. In general, the system translates these measurements into a mathematical, computer readable format. We create a user biometric profile known as a template, that templates are stored in a database. Wherever the user access the system that compares the already stored template with new template created from the user. Biometrics adds a unique identifier to network authentication, which is extremely difficult to duplicate. Smart cards and tokens also provide a unique identifier, but biometrics has an advantage over these devices: a user cannot lose or forget his or her fingerprint, retina, or voice. The practical applications for biometrics are diverse and expanding, and ranges from healthcare to government, financial services, transportation and public safety and justice. The examples are on-line identification for E-commerce, access control of a certain building or restricted area, off-line personal identification, financial automated teller machine on-line tickets purchase and internet kiosk and military area access control and etc. Fingerprints are formed by friction ridges of the skin and thumbs. They have been used for identification because of their immutability and individuality. Immutability refers to the permanent and unchanging character of the pattern on each finger.

Individuality refers to the uniqueness of ridge details across individuals; the probability that two fingerprints are alike is about 1 in 1.9x1015. Fingerprints can be recorded on a standard fingerprint card or can be recorded digitally and transmitted electronically for comparison. By comparing fingerprints at the scene of a crime with the fingerprint record of suspected persons, officials can establish absolute proof of the presence of identity of a person.QR Code has high capacity encoding of data, its maximum symbol can encode 7089 characters; while PDF417 only encode 2710 characters. QR Code (2D Code) contains information in both the vertical and horizontal directions, whereas a barcode contains data in one direction only. QR Code holds a considerably greater volume of information than a bar code. While conventional bar codes are capable of storing a maximum of approximately 20 digits, QR Code is capable of handling several dozen to several hundred times more information. QR Code is capable of handling all types of data, such as numeric and alphabetic characters, symbols, binary, and control codes. Up to 7,089 characters can be encoded in one symbol. Development of this fingerprint verification method using QR Code can avoid the duplication of the certificate. This will prevent the certificate modification from the unauthorized persons.

2 .Finger Print Recognition

Fingerprint recognition refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. There are two major classes of algorithms (minutia and pattern) and four sensor designs (optical, ultrasonic, passive capacitance, and active capacitance).

2.1. Enrollment

Fingerprint systems translate illuminated images of fingerprints into String template for further software such as enrollment (fingerprint registration) and verification (authentication of registered users).The algorithms extract minutiae data from the image, mapping the distinguishing characteristics of fingerprint ridge ends, bifurcations. This data is then converted into a String template, and stored in a database.

2.2. Verification

The actual fingerprint image is never stored, and cannot be constructed from templates. To identify or verify a fingerprint, a proprietary matching algorithm compares the new template made from the extracted minutiae points from the input fingerprint on the optical module to a previously stored sample. The entire matching process takes roughly one second. Authentication takes place either locally or on a server, depending on system

configuration.

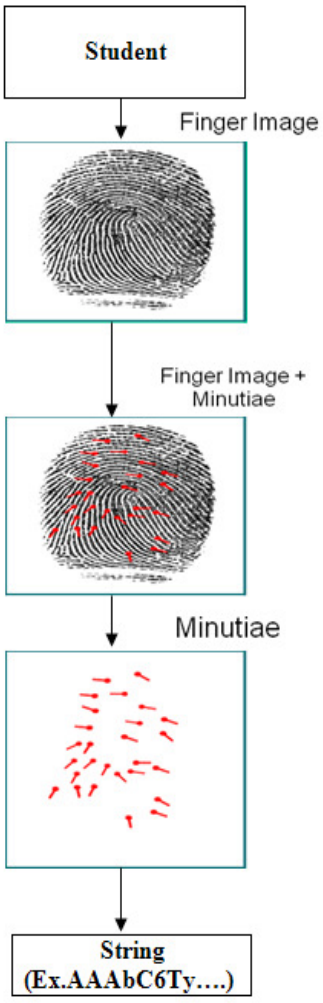

Figure 2.1. Fingerprint Recognition

3. QR Code

The QR code format was created in 1994 by Japanese company Wave. The standard is defined in ISO/IEC 18004:2006. The smallest QR codes are 21x21 pixels, and the largest are 177x177. The sizes are called versions. The 21x21 pixel size is version 1, 25x25 is version 2, and so on. The 177x177 size is version 40.QR codes include error correction: when you encode the QR code, you also create some redundant data that will help a QR reader accurately read the code even if part of it is unreadable. There are four levels of error correction that you can choose from. The lowest is L, which allows the code to be read even if 7% of it is unreadable. After that is M, which provides 15% error correction, then Q, which provides 25%, and finally H, which provides 30%.[1]

Figure 3.1. Example of QR Code symbol

3.1. Features of QR Code

1) High capacity encoding of data

QR Code has high capacity encoding of data, its maximum symbol can encode 7089 characters.

QR Code Data capacity	
Numeric only	Max. 7,089 characters
Alphanumeric	Max. 4,296 characters
Binary (8 bits)	Max. 2,953 bytes

2) Readable from any direction from 360 degree

QR Code is a matrix two-dimensional barcode; it can be readable from any direction from 360 degree. But the stack two-dimensional barcode, for example PDF417, is very difficult to realize the readable from 360 degree. [2]

3.2. Encoding of QR Code

Each QR Code symbol consists of an encoding region and function patterns, as shown in Figure 3. Finder, separator, timing patterns and alignment patterns comprised function patterns. Function patterns shall not be used for the encoding data. The finder patterns located at three corners of the symbol intended to assist in easy location of its position, size and inclination.

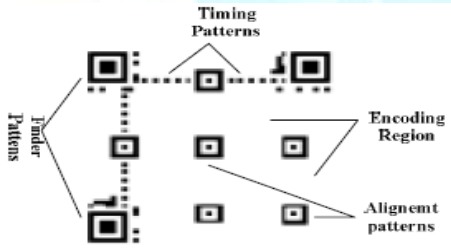

Figure 3.2. T he structure of QR Code

The encode procedure of QR Code including follows steps. Firstly input data is encoded in according to most efficient mode and formed bit stream. The bit streams are divided into code words. Then code words are divided into blocks, and add error correction code words to each block. All these code words are put into a matrix and are masked with mask pattern. Finally function patterns are added into the QR symbol. A QR Code symbol is formed.

Alphanumeric encoding mode stores a message more compactly than the byte mode, but cannot store lower-case letters and has only a limited selection of punctuation marks. Two characters are coded in an 11-bit value by this formula:

$$V = 45 \times C1 + C2$$

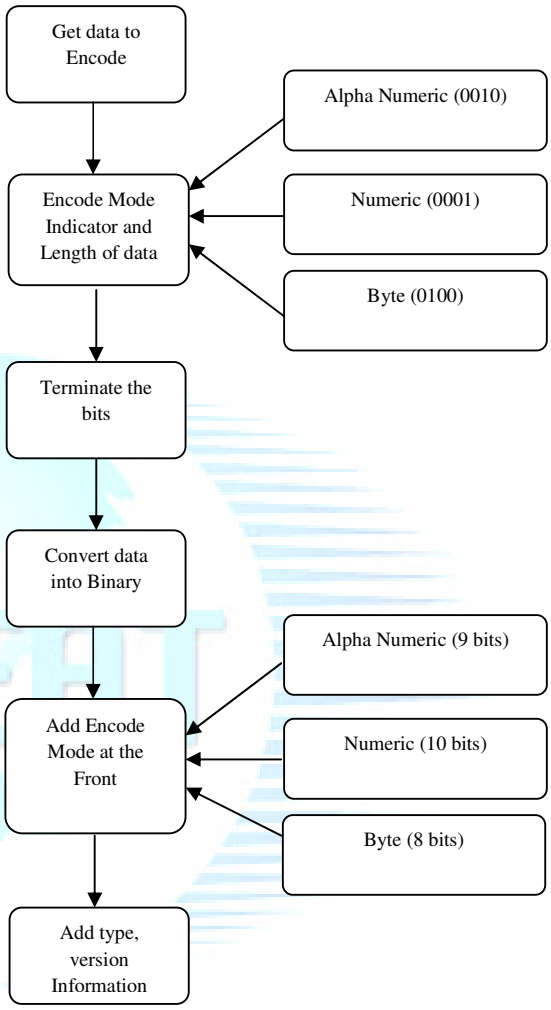

Figure 3.3. Algorithm to Create a QR Code

4. Modules Description

In this paper, we provide the **Secure Certificate Issuing System (SCIS).**

4.1. Certificate Creation

A certificate was created using ASP.NET. The certificate consists of all details of the student that are already stored in the database. At the runtime admin only has the responsibility to enter the

Indicator	Meaning
0001	Numeric encoding (10 bits per 3 digits)
0010	Alphanumeric encoding (11 bits per 2 characters)
0100	Byte encoding (8 bits per character)

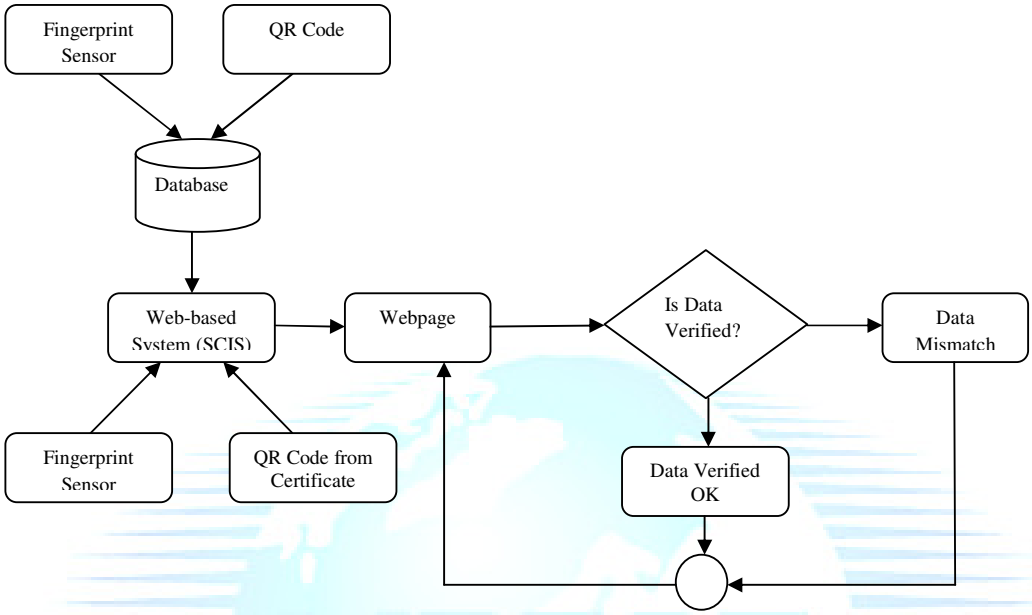

Figure 4.1 Overview of Proposed Algorithm

register number, certificate are displayed depends on the register number. The admin enters the wrong register number means redirected again to register number page.

4.2. QR Code Generation

The QR Code image consists of all the certificate details. The details embedded in the QR Code using the Alpha Numeric encoding techniques. Up to 7,089 characters can be encoded in one symbol. The name of the person, date of birth, register number, marks and fingerprint string are used for generate the QR Code.

4.3. Fingerprint Authentication

The fingerprints are enrolled from all the students and stored in the database. The fingerprint is differed from person to person. Fingerprint recognition refers to the automated method of verifying a match between two human fingerprints.

Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity.

4.4. Certificate Verification

The fingerprints are stored in the database. During the runtime the QR Code is read from the certificate. The decoded details are compared with database. If the details are matched means the certificate was displayed.

5. Experimental Results

The visual representation of our work example gives maximum accuracy and robust security in documents. Some of the visual representation of the output will be presented below.

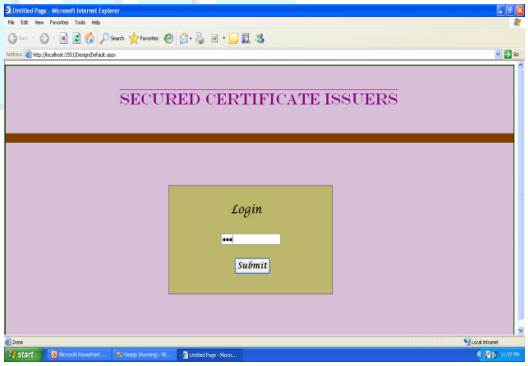

Figure 5.1 Login Page

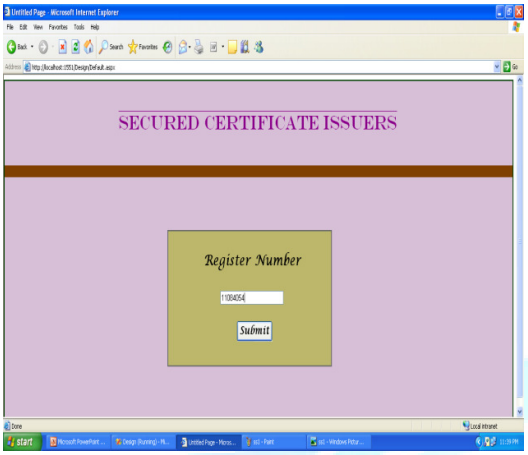

Figure 5.2 Page with Register number

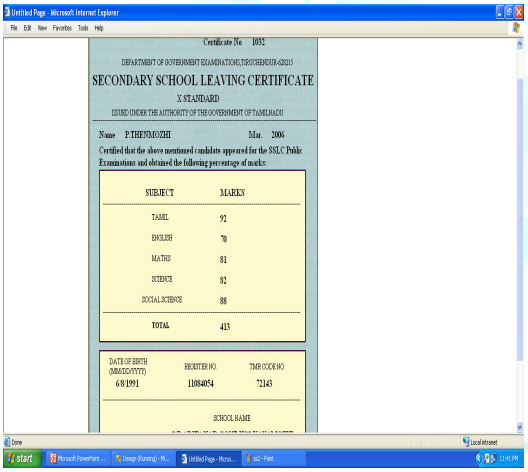

Figure 5.3 Page with Certificate details

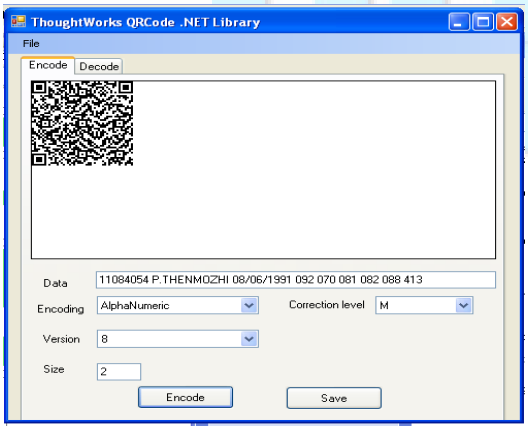

Figure 5.4 QR Code Creation

Figure 5.5 Verification Phase

Figure 5.6 Choose the Verification type

Figure 5.7 QR Code decoding using web camera

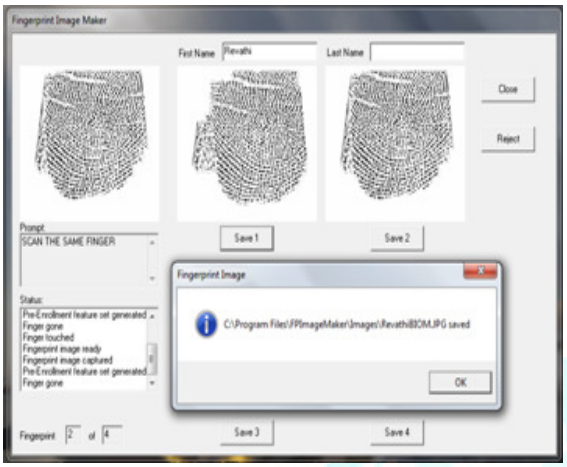

Figure 5.8 Fingerprint capture at the time of verification

Figure 5.9 Page of Verification Result

6. Conclusion

The concept of this project increases the security of identity documents. Because of this technique, there is no cheating on the mark sheets are possible. So this verification method is more effective than the earlier method, and we are identifying the person using the biometric techniques. Because of this technique the correct person also identified. This solution must be recovering the problem of mark sheet duplication. This research has thrown up many questions in need of further investigation. Further work needs to be done to establish the methods of verification based on the future technology development.

7. References

[1] L. Hong, Y. Wan, and A. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no.8, 1998, pp.777-789.

[2] D.C. Huang, "Enhancement and Feature Purification of Fingerprint Images," Pattern Recognition, vol. 26, no. 11, 1993, pp. 1,661-1,671.

[3] A. Jain, L. Hong and R. Bolle, "On-Line Fingerprint Verification," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 4, 1997, pp. 302-314.

[4] M. Kawagoe and A. Tojo, "Fingerprint Pattern Classification," Pattern Recognition, vol. 17, no. 3, 1984, pp. 295-303.

[5] L. O'Gorman. "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, Vol. 91, No. 12, 2003, pp. 2019-2040.

[6] Lin Hong. "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.

[7] D.Maio and D. Maltoni. "Direct gray-scale minutiae detection in fingerprints". IEEE Trans. Pattern Anal. And Machine Intell., 19(1), 1997:27-40.

[8] Jain, A.K., Hong, L., and Bolle, R, "On-Line Fingerprint Verification," IEEE Trans. On Pattern Anal and Machine Intell, 1997,19(4), pp. 302-314.