

Degree Certificate Authentication using QR Code and Smartphone

Ankit Singhal

M.Tech Computer Science
Faculty of Science, Dayalbagh Educational Institute,
Dayalbagh, Agra, U.P, India

R.S Pavithr

Assistant Professor
Faculty of Science, Dayalbagh Educational Institute,
Dayalbagh, Agra, U.P, India

ABSTRACT

An institution issued a degree certificate to those students who have successfully completed all studies included in the degree. The degree certificate awarded by the University is of prime importance in the person's life but the production and circulation of fake certificates is cheap because a paper document can easily be forged with the availability of advance printing and copying technologies. Hence, there is a need to adopt a process that can verify and ensure the authenticity of a document. In order to prevent the circulation of fake degree certificates a method is proposed where the integrity of the contents with in the certificate can be verified with the use of QR Code and Smart Phone Application. A QR Code will contain a digital signature over the data such as degree holder's name, enrollment number, roll number, total marks obtained etc. which will be signed by university authorities. In order to verify the digital signature a person need to use a specific smart phone application which will scan the QR Code and authenticate the certificate.

Keywords

QR Code, Digital Signature, Paper based Authentication, Smartphone Application, Degree Certificate Authentication.

1. INTRODUCTION

The incident of fraud and forgery of a degree certificate has increased with the advance technologies which are easily available at cheaper costs such as printing and copying the document which threat to the integrity of both the certificate holder and the educational institution that has awarded the certificate. The manual verification of these documents is a tedious task because it involves multiple level of human interaction and it also a time consuming task which imposes an extra burden to the university or colleges because they have to verify all the students who have passed from their college. Hence, it is necessary that the universities adopt a process that can ensure security of information and authenticity of the issued certificates.

The proposed method enables to combat this menace by embedding the QR Code on the degree certificate and by introducing the smart phone application which will read the digital data from the QR Code. It enables the verification of the certificate without depending on the certificate issuing institute. It brings in greater reliability and security in the existing process of issuing the degree certificates to the university students.

Digital signatures are widely used in networks to prove authenticity of electronic information. These signatures link the data to the identity of the signatory, ensuring that manipulations would be detected and forgery is prevented.

While providing authenticity and integrity of the information it also provide non-repudiation.

In order to print digital signature on paper documents, the documents need to be machine readable to start for which QR Code is used. The data and digital signature can be encoded in a QR Code at the bottom of every certificate and any anonymous person can scan that QR Code by using a specific smart phone application in order to authenticate the certificate. The advantage of this proposed method is that the certificates will not rely on the manual verification which is a tedious and cumbersome task. This method is also effective because it allows the authentication of a certificate at offline mode.

This paper is organized as follows: Section 2 describes the literature review relevant to the research work. It briefly discuss the existing work related to the authentication of a university degree certificate. In section 3 the theoretical background for QR Code, Android application and Digital Signature are discussed. In section 4 the procedure to prepare a degree certificate and the procedure to authenticate it using smart phone application is discussed. In section 5 analysis is performed and results are obtained at various error correction levels. Finally this papers concludes at section 6.

2. LITERATURE REVIEW

In 2007 TCS has successfully implemented Smart DEGREE at the University of Hyderabad, India, where Radio Frequency Identification (RFID based degree certificates were being issued. "RFID uses radio frequency waves to transfer data between a reader and a moveable item which is tagged" [8]. It neither require line of sight communication nor contact between reader/scanner and the tagged item. "The combination of the chip and antenna is called an RFID transponder, tag or inlet. When the RFID transponder is placed in the field of an RFID reader, information is transmitted to the reader and processed by a computer." [8]

Smart DEGREE uses an embedded passive 13.56 MHz RFID tag, complying with the ISO 14443A standard. "Each tag has 4-8 kilobytes of memory and is encoded with the certificate holder's name, date of graduation, type of degree and entire transcript, photograph and the biometrics (fingerprints), all digitally signed by the university authorities" [8]. They combined the fingerprint authentication with the digital encryption technology to authenticate the information in the degree certificate. By using RFID reader one can easily access the information from the RFID Tag when needed.

HP Labs also introduced a Document Authentication System at the University of IIT-Bangalore, where 2D barcode based degree certificates were issued. They created a centralized Document Authentication System which would accept information from

many document issuers and serve users on a network. Here the 2D barcode is in a machine readable format which can be easily read by either barcode scanner technology or smart phone with a camera and then it transmitted that data over the secure network and gets a response from the centralized system. Manual comparison of returned data with the document being verified would help to determine the authenticity of the document. [6]

3. THEORY BACKGROUND

3.1 QR Code

The Quick Response (QR) Code was designed as an improvement in comparison to its predecessor, the 1D barcode because it can contain more information. It was first designed for the automotive industry in Japan but later it become so popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC code.



Fig. 1 QR Code

The smallest QR Codes is of size 21x21 modules which is called version 1 QR Code and with each successive version the size of the QR Code gets increased by 4 modules so the largest QR Code is of size 177x177 modules which is version 40.

QR Codes also include some error correction information which is 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: L, M, Q, H. The lowest is level L which allows the code to be read even if 7% of it is unreadable. The another level is M which provides 15%, then level Q which provides 25% and then level H which provides 30% error correction. [5], [9]

The capacity of a QR Code depends on the version and error correction level as well as on the type of data that needs to be encoded. There are three data modes that a QR Code can encode: Numeric, Alphanumeric and Byte. If a QR Code is created that contain only numerical data then it can encode up to 7089 characters, with alphanumeric mode it can encode up to 4296 characters and with Byte mode it can encode up to 2953 characters.

“A QR Code consists of black modules arranged in a square grid on a white background, which can be read by an imaging device then the data can be extracted from patterns which are present in both horizontal and vertical components of the image.”[13]

There are certain factors which determine the readability of QR Code

3.1.1 Size/Distance

The size of the QR Code and the distance of scanning it determines whether it is readable or not.

3.1.2 Modules

The more information QR Code contains the denser it will be and that will make reading it more difficult.

3.1.3 Lens Quality of a Smartphone

The smartphone with macros (ability to focus up close) can read the small QR Codes whereas smartphone with poor camera quality finds difficult to read them.

3.1.4 Light

QR Code may be unreadable in low light or in a backlight surface.

3.1.5 Angle

“There is a tolerance of skewed catch the QR form 20-30° vertically or horizontally”. [15]

3.2 Digital Signature

“Just as handwritten signatures or physical thumbprints are commonly used to uniquely identify people for legal proceedings or transactions, so digital signatures ("digital thumbprints") are commonly used to identify electronic entities for online transactions. A digital signature uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption.”[10]

Some of the reasons for applying a digital signature are:

3.2.1 Authentication

Digital signature can also be used to authenticate the originator of a message. When a specific user is the owner of the digital signature secret key then a valid signature shows that the message was sent by that user. As no one else knows the user private key so any intruder cannot create a new valid signature.

3.2.2 Integrity

Digital signature also provide the integrity to the signed messages because any change in the message after signature invalidates the signature. It is still considered to be computationally infeasible to modify a message and its signature to produce a new message with a valid signature. Thus, it provides confidence to the sender and receiver that the message has not been altered during transmission.

3.2.3 Non Repudiation

Non Repudiation provides an important aspect of digital signatures, it ensures that an entity that has signed some information cannot at a later time deny having signed it. [11]

3.3 Android Platform

“With Android's breadth of capabilities, it would be easy to confuse it with a desktop operating system. Android is a layered environment built upon a foundation of the Linux kernel, and it includes rich functions”. [12]

Android provides wireless data over a cellular connection such as GPRS, EDGE, and 3G and it also provides a healthy array of connectivity options which includes Wi-Fi, Bluetooth etc. Android applications is also popular to link with Google Maps which display an address directly within an application. There is also a support for location-based services such as GPS and accelerometers in the Android software stack, but not all android devices are equipped with the required hardware.

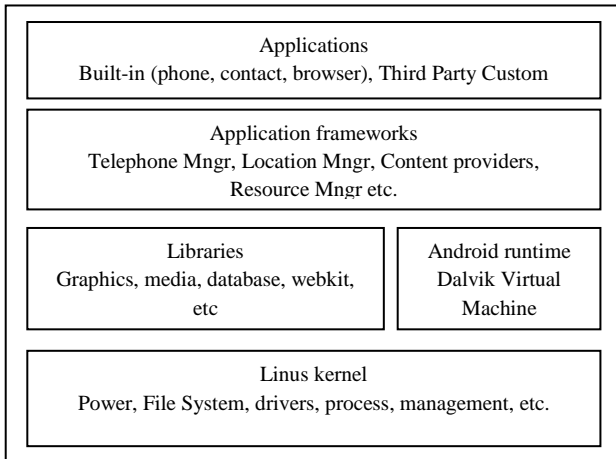


Fig. 2 Android Software Layers [12]

Android applications are written in the Java programming language, and they run within a virtual machine (VM) which is known as Dalvik Virtual Machine and it is an open source technology. “Each Android application runs within an instance of the Dalvik VM, which in turn resides within a Linux-kernel managed process”. [12]

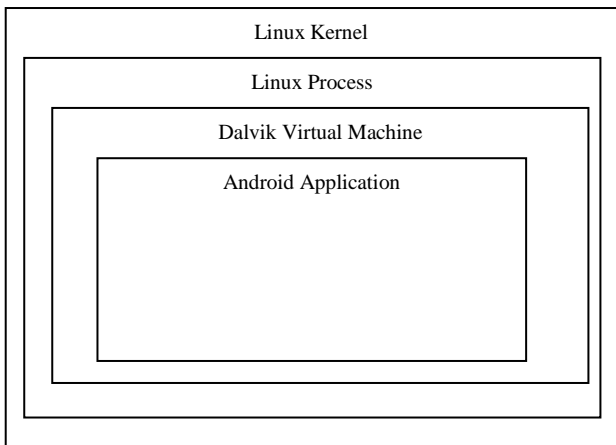


Fig. 3 Dalvik VM [12]

Every Android application contains a file called AndroidManifest.xml which along with an android application is deployed to the device. AndroidManifest.xml contains all the necessary configuration information which is required in order to properly install an android application to the device. It includes the required class names, permissions which an application needs to run and the types of events the application is able to process. Such declarative information helps to reduce the likelihood that a rogue application can cause damage to the device. [12]

4. DEGREE CERTIFICATE AUTHENTICATION

4.1 Preparation of a Paper Based Degree Certificate

The proposed scheme for the preparation of paper based certification is given in figure 4. The steps for the proposed method are as follows

- 1) Compose the message M from the details such as name of the student, father’s name, enrollment number etc.

- 2) Obtain the hash value (message digest) of the composed message M, using SHA-256.
- 3) Use the University Private Key to sign the obtained message digest which will result to a digital signature on message M.
- 4) Message M along with digital signature are combined together and fed into the QR Code generator. The system also makes an entry of message M in the university database.
- 5) The QR Code generator produces a QR Code which stores the message M and the digital signature.
- 6) Message M and QR Code at the bottom can be printed on the certificate.

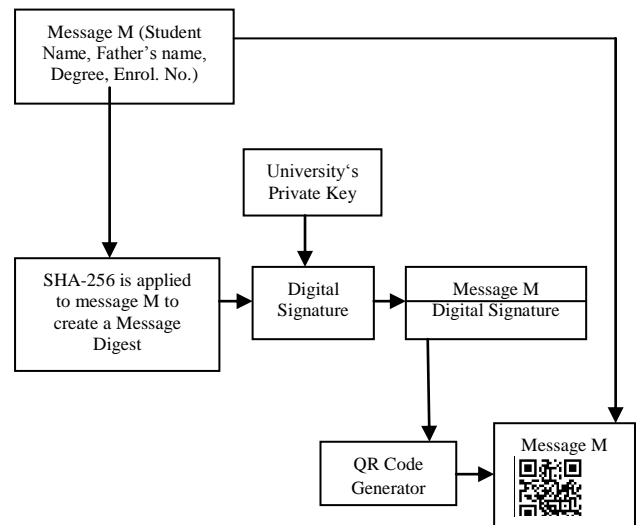


Fig. 4 Block Diagram for the Development of a Degree Certificate

4.2 Procedure to Authenticate the Degree Certificate by using Smartphone Application

The proposed scheme for the authentication of the certificate using smart phone application is given in figure 5. Following are the steps of proposed method

- 1) The information in the QR Code consists of the message M and the digital signature on the message M. The verification process starts by first scanning the QR Code and then decrypting the signature from the university’s public key in order to generate the hash value (M2).
- 2) A new hash value (M1) is generated using the message M and compare with the decrypted signature’s message digest (M2).
- 3) If both the values are identical then it can assure the integrity of the message. It also confirms the identity of the university because the public key can only decrypt data that has been encrypted with its corresponding private key.
- 4) However, if the hash values are different, then it can be concluded that the printed message has been modified.

- 5) Further human review must conduct to the message (M) obtained from the QR Code, which can be shown next to the printed message on the degree certificate and inspected visually.

In this way a verifier can authenticate a university degree certificate without any need of an internet connection, the only requirement is an android platform based smart phone

with camera which will execute the developed mobile app. If the verifier wants to connect with the university website then he can connect with them from the developed mobile app where he will be able to see some more information regarding that student from university perspective. These additional information can give some insight details about the student which has not presented in his certificate.

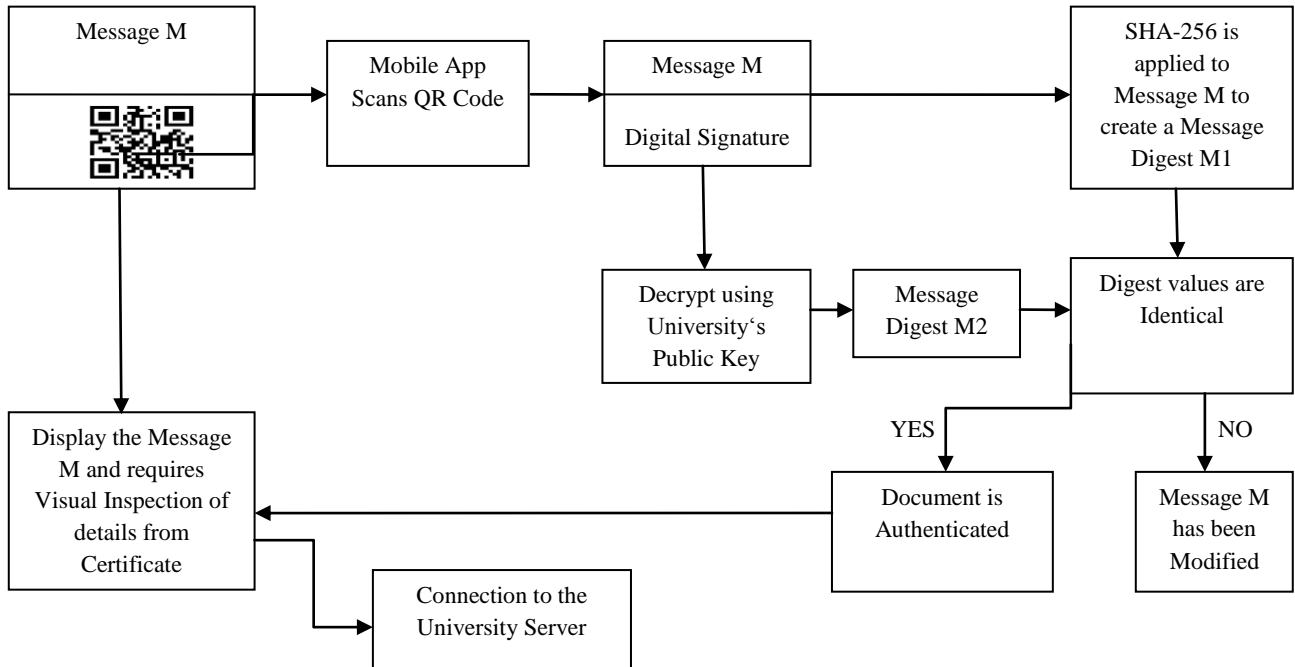


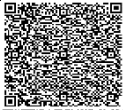
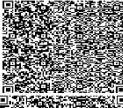

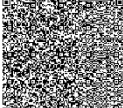
Fig. 5 Block Diagram for the Verification of a Degree Certificate using Smart Phone Application

5. EXPERIMENTAL RESULT AND ANALYSIS

This section presents the experimental results and their analysis. The SHA-256 algorithm is used to produce a fixed length message digest from arbitrary sized input data. The

input mode for the QR Code generator is Byte mode which can accommodate up to 2,953 characters where possible characters can be in ISO 8859-1 format.

Table 1. Generation of QR Code

Total Length (Message M + Digital Signature)	QR Code Version	Error Correction Level	QR Code
420	13(69x69)	L	
420	16(81x81)	M	
420	19(93x93)	Q	
420	22(105x105)	H	

The QR Codes at various correction levels with details are given in table 1. After creation of QR Code the optimal size for printing it on paper can be calculated using,

QR Code Size = (Scanning Distance / Distance Factor) * Data Density Factor [16]

Where, Distance Factor starts with 10 but can be reduce by 1 due to poor lightning or skewed position of scanning. Data Density Factor counts the individual module either in horizontal or vertical direction and then divides it by 25 to normalize it back to the equivalent of a Version 2 QR Code. [16]

Standard QR Code should be of size around 1 to 2 inches and the individual modules should not be less than 0.03 inches else it would be difficult for smartphone to read the QR Code. There should also be a white space (quiet zone) around the code which is approximately 4 times the size of the individual module.



By assuming scanning distance of 6 inches and distance factor of 10, the optimal printing size of QR Code for the different versions obtained in table 1 are present in table 2.

Table 2. QR Code Printing Size

QR Code Version	13	16	19	22
QR Code Size(inches)	1.65	2	2.28	2.52

By damaging the printed QR Code obtained in table 2, scan is performed on it by smartphones whose results are in table 3.

Table 3. Scanning Results of Damaged QR Code

Damaged QR Code	Size & Location of Damage	Error correction Levels				Smartphones
		L(69x69)	M(81x81)	Q(93x93)	H(105x105)	
	0.5 inch at the Centre	1	1	1	1	HTC Desire (8MP camera)
		1	1	1	1	Moto G (5MP camera)
	0.4 inch at the Bottom	1	1	1	1	HTC Desire (8MP camera)
		1	1	1	1	Moto G (5MP camera)

In the table 3, if QR Code readable it is denoted by 1 and if it is unreadable then it is denoted by 0.

Although everyone takes care of their degree certificate but the additional error correction codes in QR Code will help to read it even if the certificate is damaged.

6. CONCLUSION

The proposed method facilitates the verification process of a degree certificate at offline mode. It has resulted into a working prototype which authenticate a university degree certificate by using Digital Signature, QR Code and Smartphone. An option of connecting to the university database also provides a convenient way to get the insight details of the student from the university perspective.

The proposed method is not only cheap and cost effective but it also helps university to issue a degree certificate to their student without any hassle of verifying it later. This not only improves the authenticity mechanism of the degree certificate at much faster rate than manual verification but it also prevents the creation of fake degree certificates. The successful verification of the digital signature ensures the integrity of the message and also confirms the identity of the university.

In order to use the digital signature a University does not have to necessarily register itself to Certificate Authorities for publishing its public key because the degree certificate and

the mobile app itself contain the public key which can be verified by visual inspection.

In the future the combination of digital encryption over the data and fingerprint or digital image can be used for authentication.

7. REFERENCES

- [1] K.M. Revathi, P. Annapandi, P.K.Ramya “Enhancing Security in Identity Documents Using QR Code” in International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013.
- [2] R.L. Renesse, “Paper-based document security–A Review,” in European Conf. on Security and Detection, 1997.
- [3] M. Singh and D. Garg, “Choosing best hashing strategies and hash functions,” in International Advance Computing Conference, 2009, pp. 50 – 55.
- [4] J. Z. Gao, “Understanding 2D-barcode technology and applications in M-commerce – design and implementation of a 2D barcode processing solution,” in International Conference on Computer Software and Application, 2007, pp. 49 – 56.
- [5] How UPC Barcode Work, <http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/upc.htm>

- [6] Document Authentication System Preventing and Detecting fraud of Paper Documents, <http://www.hpl.hp.com/india>
- [7] High Capacity Color Barcode, http://en.wikipedia.org/wiki/High_Capacity_Color_Barcode
- [8] SmartDEGREE from TCS to combat Certificate Malpractices, http://www.tcs.com/SiteCollectionDocuments/White%20Papers/TCS_Innovation_Whitepaper_TCS_Smart_Degree_11_09.pdf
- [9] QR Code Tutorial, <http://www.thonky.com/qr-code-tutorial>
- [10] Digital Signatures, <http://technet.microsoft.com/en-us/library/cc962021.aspx>.
- [11] Digital Signature, http://en.wikipedia.org/wiki/Digital_signature
- [12] Introduction to Android Development, <http://www.ibm.com/developerworks/library/os-android-devel>
- [13] What are 2D Barcodes, <http://tag.microsoft.com/what-is-tag/2d-barcodes.aspx>
- [14] International Organization for Standardization ISO/IEC 18004 Information technology - Automatic identification and data capture techniques - Bar code symbology - QR Code, http://raidenii.net/files/datasheets/misc/qr_code.pdf
- [15] QR Codes, <http://www.qrcode.es/en/2013/12/%C2%BFcual-es-el-tamano-minimo-de-un-qr-code/>
- [16] QRStuff, <http://www.qrstuff.com/blog/2011/01/18/what-size-should-a-qr-code-be>