Design and Implementation of a Certificate Verification System using Quick Response (QR) Code

Oyediran Mayowa O
Bells University of Technology, Ota, Ogun State
mooyediran@bellsuniversity.edu.ng

Elegbede Adedayo W.
Bells University of Technology, Ota, Ogun State
bimpe24@rocketmail.com

Olusanya Olamide O.
Bells University of Technology, Ota, Ogun State
olamide4jc@yahoo.com

Awokola Jinmisayo A.
Precious Cornerstone University, Ibadan, Oyo State
rhgonline@gmail.com

Sodipo Queen B.
Bells University of Technology, Ota, Ogun State
queen.daisy1121@gmail.com

Corresponding Author's E-Mail: rhgonline@gmail.com

ABSTRACT
In the world today, individuals consistently fake their certificate to get a job or to present where and when required. The best way to single out those fake certificates is through verification. Notwithstanding, the paper verification sets aside a long process to handle certificate verification on the grounds that the certificates need to return to the issuing institutions which is tedious and time wasting. To this end, the certificates end up not getting verified or are delayed due to long process. Hence, in this paper, a certificate verification system utilizing QR code is created for simple check of the certificate authentications. This paper talks about the development of a certificate verification system, design a Quick Response code utilizing Advanced Encryption Standard method that will then be executed into the certificate of the students. The purpose behind the Advanced Encryption Standard Technique is on the terms that it is the most secure type of encryption technique in the world today. It is the most regular security protocol utilized for various wide applications. Overall, the implementation of Advanced Encryption Standard and Quick Response Code gives great execution, production, light, and fast responses in a certificate verification system.
Keywords: Quick Response code, certificate, verification, Advanced Encryption Standard

1. INTRODUCTION

A certificate is a statement or a document that is issued to a student or a person after the completion of a specific education either formal or informal (Singhal and Pavithr, 2015). Certificate verification is a system of application that is used by a school administration to make and manage certificates for students in a computerized manner where the certificates can be created, printed and verified. Certificate verification is rather tedious, with some institutions receiving the verification process from a third party. Attempts to use Information Technology have been questioned as universities' would not allow third party organizations access their verification database, as a result of which the verification process remains partially or entirely manual (Boukar, Isa and Salisu, 2017). In addition, fraud or plagiarism in the initial documents becomes a challenge in the academic community. The downside faced by such organizations in the process is that the validity of the documents cannot be completely checked. The tedious nature of the paper work influences the process of authentication of documents by the issuing institutions, contributing to an increase in the number of forged certificates in the world (Boukar, Isa and Salisu, 2017). Consequently, a new, safe and automated method is embedded into the system which is the use of Quick Response (QR) code and a smart-phone QR scanner that is used to read, authenticate and verify the QR code on the certificates. Quick Response code is a two-dimensional barcode that is usually used to encode bits of information represented as black square dots placed on a white square grid (Uzun and Bilgin, 2016). They are designed to decode the data quickly (Pons, 2011). It is the most popular type of verification system used in the world. It has a wide storage space and fast readability and it brings greater reliability and security in the existing process of issuing the degree certificates to the university students (Singhal and Pavithr, 2015). The online bank verification system (Mohadikar and Devade, 2013) and attendance system (Tresnani and Munir, 2011) are examples of the QR Code application system.

Therefore, this research studies the generation of a Quick Response Code and the implementation of the Quick Response code into a certificate for verification. A secure QR code will be designed based on the references to the student's records printed on certificates. Next, a mobile scanner will be developed that will be used on mobile devices with the help of AES algorithm which then decrypts the QR Code to validate the certificates. This system will be designed to enable only the scanner to be able to decrypt and translate the QR-code because of the securely embedded properties generated by the system. The QR code generated which contains the student's detail will be printed on the certificate. If the QR code is scanned using a mobile QR scanner and it doesn't provide any relevant information, then it shows that the certificate is fake (Singhal and Pavithr, 2015).

.

2.0 LITERATURE REVIEW

Certificate verification has become an important task today. It is the process of ensuring that the certificate issued after the completion of an education phase presented by an individual is genuine and that the holder is the rightful owner (Singhal and Pavithr, 2015). Moreover, a certificate has to be verified to ensure that its content is true and also to ensure that the issued certificate comes from an accredited source. Certificates are written and printed using special paper and has become a very important document for job application and for pursuing to higher degrees. Counterfeit degrees have become very common with the development of forgery technology, however, and that is why verification is very necessary (Ghazali and Saleh, 2016). Several researchers has worked on this area to evade the idea of Certificate counterfeit, QR code and Smart phone were proposed as solution to attendance system for both employees and student, (Cho and Bae, 2014; Kumar and Kareemulla, 2017; Masalha and Hirzallah, 2014).

The attendance system proposed by these researchers was online system that requires lecturer to generate QR code that would be scanned by the students and sent via wired/wireless network for necessary automatic attendance checking, (Cho and Bae, 2014; Masalha and Hirzallah, 2014). The major extension offered by the work of (Kumar and Kareemulla, 2017) was the introduction of fingerprint and voice verification for authentication in order to avoid proxy of attendance. Also, in 2016, a new enhancing security in identifying documents using QR Code was developed (Revathi, Annapandi and Ramya, 2013). This system consists of QR reader and Biometrics finger print readers which are used to verify the certificate originality in order to eradicate fraudulent certificate. In this system, it focuses on using image of the certificate to generate into QR code and finger print of the person during the run time.

Dey, Nath and Agarwal (2013) developed a new Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System. In this system, the essential data of each student are saved in the QR Code, like the student's name, roll number, registration number, semester and year of study, marks obtained in different subjects and grades secured. But, all the data saved and embedded in the QR Code, are encrypted, and then the QR Codes are printed in the mark-sheet of the student. So, in future if the student or any other person wants to see the marks digitally or wants to send the academic information to any University or Organization in digital format, then the QR Code can be scanned and the embedded information can be decrypted and sent. This research proposed a new method, where the marks obtained by a candidate will also be encoded in QR Code in encrypted form, so that if an intruder tries to change the marks in the mark sheet then it will be impossible in the QR Code, because the encryption key is unknown.

Al-Khalifa (2008) also made it known that cell phones are becoming an important aspect of our lives. The comfort and convenience they provide certainly made our lives much easier than ever before. Two brilliant features found in modern cell phones are: the integration of digital cameras and the ability to access the Internet anytime and anywhere, thus, enabling us to seek information when we need it. The benefit of such a feature in modern mobile phones can be further extended to include blind and Visually Impaired (VI) people.

Also, with the introduction of speech technologies in cell phones such as the use of Nuance TA, which converts the displayed text on the mobile handset into speech, the blind and Visually Impaired (VI) person can easily interact with the mobile handset as a sighted person do. The idea of utilizing the capabilities of modern mobile phones with 2D barcodes to assist Visually Impaired (VI) and blind people identify objects in the environment is very promising. Thus, our proposed system uses mobile phones, which are inexpensive, portable and nearly a ubiquitous mainstream consumer product widely used by blind people, not like some expensive assistive technologies, to verbally identify objects tagged with 2D barcodes.

Schultz (2013) brought to the notice that libraries and museums are increasingly looking to mobile technologies, including quick response codes, to better serve their visitors and achieve their overall institutional goals; however, there is a lack of information regarding patrons' perceptions of quick response codes-information. This case study explored staff members' and patrons' perceptions of quick response quick response codes at Ryerson University Library and the museums.

3.0 METHODOLOGY

The research approach signifies a schematic view of the general solution to secure paper certificates with encryption algorithms and using mobile scanner for authenticity verification. A secure QR code will be generated based on the references to the student's records (Matric Number, Name, Class of Degree, Department etc.) printed on certificates.

Phase I: Generating the QR Code

The QR Code generation process entails the following steps:

Step 1: Data Analysis:

QR codes generally are of four types of data which are; alphanumeric, numeric, Kanji and byte. The data types can be encoded into string of bits 1's and 0's in different ways. However, in this stage, data to be encoded are analyzed to determine the data type and the proper encoding mode to be adopted. The matric number being considered here is of numeric data type therefor, the adopted encoding mode is numeric.

Step 2: Data Encoding:

The data encoding process includes the following:

i. Choosing the error correction level: There is probability of extracted character is damaged or disfigured in the attempt to extract character, therefore, Error correction are used to restore the extracted characters. To achieve this, the appropriate error correction level must be selected. The appropriate QR code for encoding matric number is level L.
ii. Determining the appropriate data version: QR code could be in different sizes called versions. The numeric mode and version 1 was adopted
iii. Determining the mode indicator: 0's and 1's in four-bit sequence are used to indicate the chosen encoding mode.
iv. Determining the character count indicator: character count indicator states the total number of characters to be encoded.
v. Encoding the input data: the chosen encoding mode will be used to encode the input data.
vi. Breaking up the intermediary bits into 8-bit code words: Since, version 1 QR code in numeric mode is being used, 19 total data code words will be needed. The total number of bits needed for the QR code generation now becomes 19 * 8 i.e. 152 bits.

Step 3: Error Correction

Errors occur due to inappropriate handling of QR code and which may challenge the integrity of the data encoded in the QR code; therefore, in the process of data encoding, code words needed to correct the errors are also generated. However, Reed-Solomon error correction technique was used for error correction. It is the most commonly used error correction techniques which make use of polynomial long division as well as Galois field arithmetic in computing the error correction code words.

Step 4: Developing the mobile application to scan the QR code

A mobile application was developed to decode, read and translate the encoded data information embedded in the QR code. Java software Development Kit versions 6 (JDK6) containing eclipse Integrated Development Environment (IDE) and Android Development Tools (ADT) eclipse plugin were used for the mobile application development.

4.0. Result and Discussion

The results obtained after the execution of the QR mobile scanner on the QR code embedded in the student certificate is stated and discussed in this session. The sample of the developed certificate embedded with the QR code is presented in Figure 3, which is then scanned using the developed mobile application for verification and was verified and it is presented in Figure 6. The performance evaluation was carried out on the system with an existing system (Revathi and Ramya, 2013) using Response time and also the authenticity of the certificate as metrics.

4.1 Testing of Result

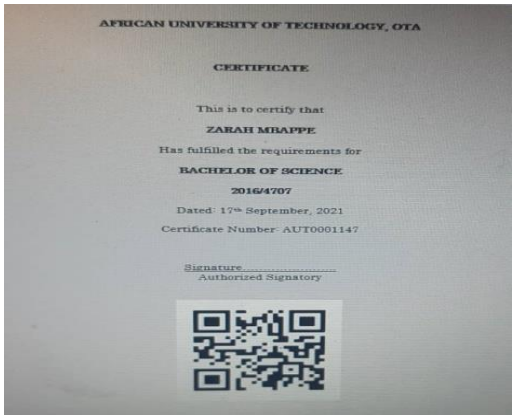

Figure 3: Student's certificate with QR code

Figure 4: Scanned QR code

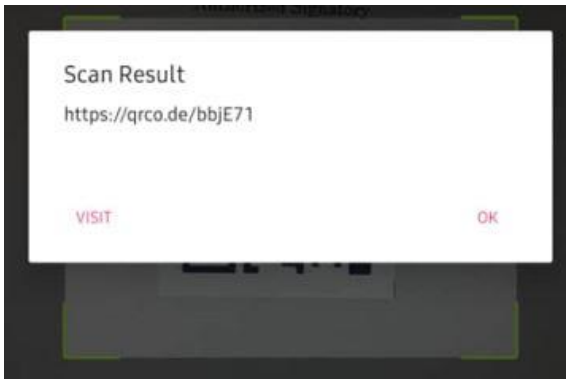

Figure 5: Link to certificate verification status

Figure 6: Student certificate verification status

4.2 Discussion of result

The student's details from the certificate are encrypted into a QR code. The QR code is then added to the student certificate. The already built mobile QR Barcode scanner is used to scan the QR code. When it scans, it shows the link to the URL where the QR code is saved. When the link shows up and it clicked, it redirects to show the details embedded in the QR code and the document can then be downloaded. The document that is downloaded is the Verification status of the student certificate. The research was tested based on its speed and the results were analyzed and discussed.

4.3 Performance Evaluation of the system

In the implementation of the application to the system, there are some impacts that accompany it. To determine the impact that may occur as a result of the implementation of this system, it would require a prototype for the System. The performance of the system is evaluated using response time.

4.3.1 Response Time

It is the time takes for the mobile scanner to scan and decrypt the embedded message in the QR code. Comparing the response time for different data types embedded in a QR Code for the developed system and an already existing system,

Table 1: Response time between developed and existing systems.

Data	Developed software (seconds)	Existing system (seconds)
Numeric	1.45	1.57
Alphanumeric	0.59	0.65
Characters	0.63	0.78
Pictures	0.82	1.04

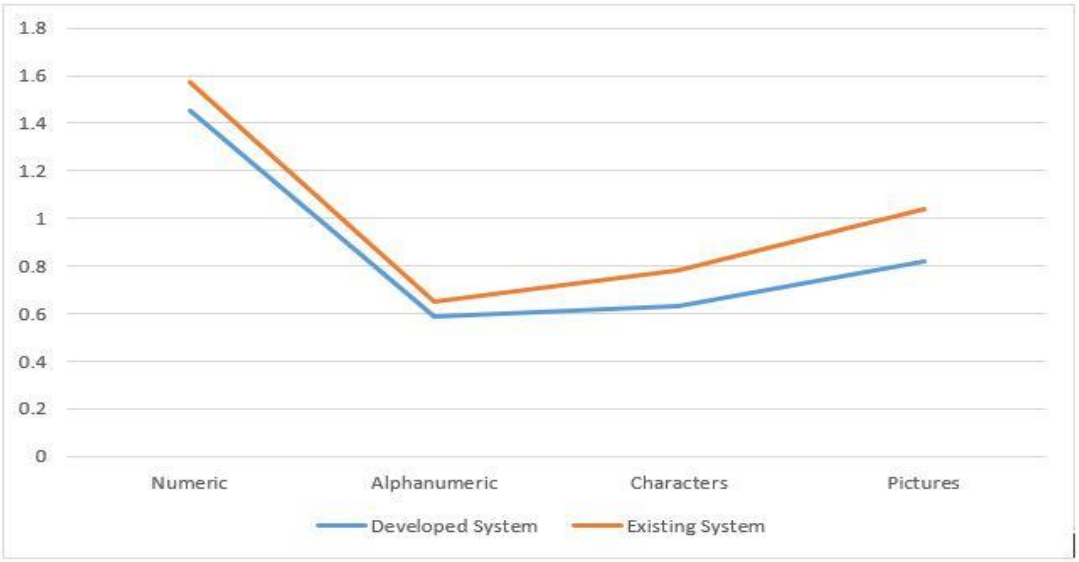

Figure 7: Graphical representation of the Response time between the developed System and the existing system.

5.0. Conclusion and Recommendation

This research is an attempt to eliminate fraudulent certificates from learning institutions. Verification of academic certificates is one of the significant research areas today, as discussed in the introduction chapter of this research. This work aims to address academic fraud issues. The proposed method enhances certificates verification process. It has resulted in a working prototype using the Advanced Encryption Standard, QR Code and Smartphone to authenticate a university degree certificate. This project allows the QR code embedded in a university certificate to be scanned in order to check the certificate's validity. Not only does this boost the validity of the certificate faster than manual verification, but it also prevents fake certificates from being created.

6.0 ACKNOWLEDGMENTS

Our thanks to all the authors that provided us support and funding that contributed towards success of this work.

7.0 References

Boukar, Moussa Muslu, Isa Yusuf and Salisu, "A Web Service Based Database access for Nigerian Universities' Certificate Verification System", *International Journal of Computer Techniques.*, 1-7, 2017.

Chernev b., 2019, Tech Jury [online] available at https://techjury.net/blog/what-is-aes/ [Acessed 06 April 2020].

Cho, D., & Bae, M. (2014). A Study on Development of OTIP System using QR Code based on Smartphone. International Journal of Multimedia and Ubiquitous Engineering, 9(10), 261–270.

D. L. Tresnani and R. Munir, "Implementation of Employee Attendance System Using QR Code on Android-Based Smartphones," Informatics Techniques, Bandung Institute of Technology, Bandung, 2011.

Erasmus University Rotterdam, 2015. [Online] Available: https://www.eur.nl/sites/corporate/files/201711/webbrochure2015_Cheating-plagiarism_EN.pdf, [Accessed 2020].

F. F. Rochman and I. K. Raharjana, "Implementation of QR Code and Digital Signature to Determine the Validity of KRS and KHS Documents," *Scientific Journal of Informatics*, vol. 4, no. 1, pp. 8-19, 2017.

Hend S. Al-Khalifa (2008). Utilizing QR Code and Mobile Phones for Blinds and Visually Impaired People. ICCHP 2008, LNCS 5105, pp. 1065–1069.

Indrayani, E, "The Effectiveness and the Efficiency of the Use of Biometric Systems in Supporting National Database Based on Single ID Card Number (The Implementation of Electronic ID Card in Bandung)", *J inform tech software engineering 4:129*, doi:10.4172/2165-7866.1000129, 2014

Kumar, B. D., & Kareemulla, S. (2017). Smart Mobile Attendance System for Employees Using QR Scanner. Asian Journal of Applied Science and Technology (AJAST), 1(5), 35–39.

Masalha, F., & Hirzallah, N. (2014). A Students Attendance System Using QR Code. International Journal of Advanced Computer Science and Applications (IJACSA), 5(3), 75–79.

Michelle Schultz (2013). A case study on the appropriateness of using quick response (QR) codes in libraries and museums. Library and Information Science Research. Vol 35, Num 3, pp 207-215.

N. Mohadikar and C. Devade, "Online Banking Authentication System Using QR-Code and Mobile OTP," *International Journal of Engineering Research and Applications (IJERA)*, pp. 1810-1815, 2013.

Nechvatal J, Barker E, Bassham L, Burr W, Dworkin M, et al. (2000) Report on the development of the Advanced Encryption Standard (AES). Computer security division information technology laboratory national institute of standards and technology administration, U.S. Department of Commerce, USA.

Nti IK, Gymfi E, Nyarko O, "Implementation of Advanced Encryption Standard Algorithm with Key Length of 256 Bits for Preventing Data Loss in an Organization". *International Journal of Advanced Technology* 8: 183. doi:10.4172/0976-4860.1000183, 2017,

Okfalisa, Novi Yanti, Wahyu Aidil Dita Surya, Amany Akhyar, Frica A Ambarwati, "Implementation of Advanced Encryption Standard (AES) and QR Code Algorithm on Digital Legalization System", Web of Conferences 73, *International Conference on Energy, Environment, Epidemiology and Information System (ICENIS)*, 13009, https://doi.org/10.1051/e3sconf/201873 2018.

Osman Ghazali and Omar Saleh, Proceedings of Academics World 54th International Conference, Malacca, Malaysia, 2nd-3rd December 2016, ISBN: 978-93-86291-48-6.

Pitchaiah M, Philemon D, Praveen (2012) Implementation of advanced encryption standard algorithm. *Int J Sci & Engg Res 3*: 1-6.

Pons, D, "QR code in use: the experience at the UOV library", Serials-24 (3), 47-56, 2011.

Revathi M K, Annapandi P, Ramya K P. (2013). Enhancing Security in Identity Documents Using QR Code. *International Journal of Research in Engineering & Advanced Technology*.

Singhal and Pavithr, "Degree certificate authentication using QR code and smartphone", *international journal of computer applications*, Volume 120 – No.16, 1-6, 2015.

Somdip Dey, Asoke Nath, Shalabh Agarwal. (2013). Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System. *IEEE International Conference on Communication Systems and Network Technologies (CSNT)*.

Uzun, V., & Bilgin, S, "Evaluation and implementation of QR Code Identity Tag system for Healthcare in Turkey". *SpringerPlus*. https://doi.org/10.1186/s40064-01630209, 2016.