

## Document verification using quick response code with modified secure hash algorithm-1 and modified blowfish algorithm

Rogel Ladia Quilala<sup>1</sup>, Theda Flare G. Quilala<sup>2</sup>

<sup>1</sup>Master in Information Technology Department, College of Computer Studies, Tarlac State University, Tarlac City, Philippines

<sup>2</sup>Information Technology Department, College of Computer Studies, Tarlac State University, Tarlac City, Philippines

---

### Article Info

#### Article history:

Received Mar 25, 2022

Revised Jul 5, 2022

Accepted Jul 27, 2022

---

#### Keywords:

Blowfish algorithm

Data integrity

Document verification

Encryption

SHA-1

---

### ABSTRACT

A previous study has been conducted integrating modification on secure hash algorithm 1 (SHA-1) to document integrity verification of printed documents using quick response (QR) codes. However, encryption is warranted as data is transmitted in plaintext directly to the server to prevent hacking and ensuring not only data integrity but data security as well. A more secured document integrity verification using QR code was designed and developed by successfully incorporating a better hashing algorithm—modified SHA-1 and integrating a modern encryption algorithm—modified blowfish algorithm. By integrating both, data integrity and data confidentiality is assured as compared to previous research. The developed software was checked against user requirements to check the acceptability of the software. Error rate and accuracy were also checked to see how the software performed. Based on the testing conducted, it has been found that the document integrity verification software using QR code with the integration of modified SHA-1 hash and Modified Blowfish encryption was acceptable, accurate, and more secure.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



---

### Corresponding Author:

Theda Flare G. Quilala

Information Technology Department, College of Computer Studies, Tarlac State University

Romulo Blvd. San Vicente, Tarlac City 2300, Philippines

Email: [tfgquilala@tsu.edu.ph](mailto:tfgquilala@tsu.edu.ph)

---

## 1. INTRODUCTION

Competency, skills, and qualifications for a certain craft are demonstrated by acquiring certifications. These documents act as your credentials and are considered by employers when hiring for personnel. But recently, people get involved in the creation of fraudulent academic credentials therefore its prevalence [1]. Verification of these documents is quite challenging because they cannot be traced as quickly and accurately [2]. Thus, a system is needed to inspect the authenticity and validity of such document certification rapidly and precisely [3].

Due to the rise in the usage of smartphones with cameras combined with the ease of scanning a quick response (QR) code using this device, studies have explored the use of QR codes as a cheap alternative to other tag-based systems [4]. QR codes have been used for authentication on printed documents for fraud identification. One study tried embedding watermark objects with QR codes to determine printed document validity but challenges were identified such as the preparation of validation links, watermark image (logo) configuration, and size restriction [5], [6] making the embedding of an image in QR unattractive. Others have embedded a blockchain technology pattern into a QR code for authentication [7] and encrypted lossless compression [8], but failed to incorporate hashing in their verification thus neglecting to consider the data integrity of the data being transmitted. One study analyzes the impact of blockchain on academic certificates

and has seen its advantage [9], [10] but on the other hand, others find it complicated, challenging, and costly therefore recommended to be better suited for financial and other sectors where mining is present [11].

Several studies successfully created verification apps using QR. One constructed a mobile app for securing issued degree documents which encrypts students' information from the database and saved it on a server, afterward creating a QR code to be printed on the document which is then used for validation purposes [12]. Another study combines QR codes, digital signatures, and hashing, in a smartphone application [13]. On the other hand, one study was able to integrate secured communication via transport layer security and hashing [14]. Another also developed an android application that used QR codes in the identification of objects along with hash [15]. However, for all studies the QR code can only be read using the created mobile application which is a hassle because it needs to be installed separately.

Hashing has been proven to ensure data integrity, so its wide usage has been evident. In one study, a hash function was used to create an efficient way to secure the personally identifiable information (PII) of a user in a QR code which is good because data integrity is assured but the disadvantage is that secure hash algorithm 1 (SHA-1) was used as the hashing algorithm and is already known to be weak [16]. Blockchain was successfully integrated with QR in one more study but failed to add additional security on transit [17]. Previous research applied QR code technology in verifying the authenticity of documents using a web application that doesn't require additional installation on the part of the user [18] but failed to consider data security by transmitting data in plaintext and thus is prone to hacking. To address this data security weakness, other studies make use of encryption schemes for security [19]–[21] against hacking.

The contribution of this paper is the improvement in the design and development of a document integrity verification using QR code by incorporating modified SHA-1, a better hashing algorithm than the weak SHA-1 to emphasize data integrity, and inclusion of modified blowfish encryption algorithm, a modern algorithm to encrypt the confidential data embedded as QR code in the document as the security measure. Both data integrity and data confidentiality are assured by incorporating both hashing and encryption. The software does not need to be installed separately unlike in previous studies and can be used on both Android and Apple smartphones to verify certificates. The app will make use of the phone's embedded camera. The specific objectives of this study are to: i) develop a more secured document integrity verification software using QR code with modified SHA-1 for hashing and integration of modified blowfish algorithm for encryption, ii) evaluate the acceptability of the developed software via use case tests, and iii) analyze the performance of the system in verifying documents by computing the error rate during the alpha testing.

## 2. METHOD

### 2.1. Research design

This study utilizes the design and development approach. The software was created in Visual Studio Community Edition in an Intel(R) Core (TM) i5-10210U processor with CPU @ 1.60GHz 2.11 GHz and 8.00 GB RAM running Windows 10 Pro. The web server must run on internet information services (IIS) version 10.0.19401.1. The developers applied the rapid application development (RAD) software development methodology. The process flow of the study is shown in Figure 1. The document integrity verification is subdivided into three sections: hashing, encryption and generation of QR code, certificate management, and certificate verification.

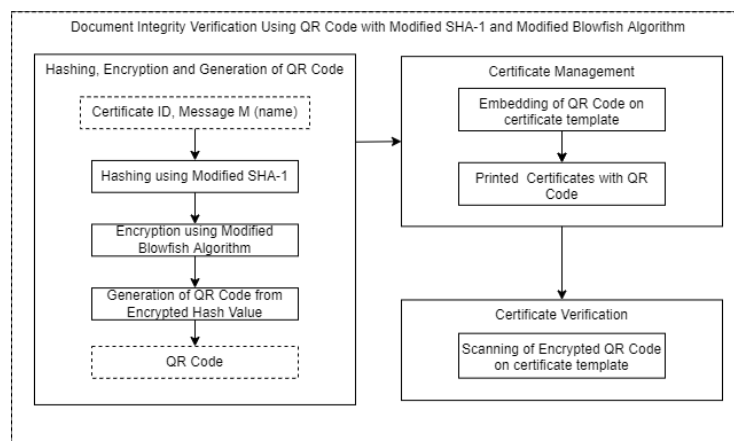


Figure 1. The process flow of the document integrity verification

In the hashing, encryption, and generation of QR Code section, first, the system administrator inputs the unique certificate identification (ID) of the document and message M which is equivalent to the name to which the document belongs. Then, the modified SHA-1 was applied to ID and message M to produce 192 bits hash value which is then saved to the database. Then, the modified blowfish algorithm (MBA) encryption will encrypt the hash and message M. After that, the QR code generator generates the QR code from the encrypted hash value. The QR code generated was to be printed on the documents.

In the certificate management section, the list of names, created QR codes, and images for the design of the document that will act as the certificate template, must be provided before the printing of the certificate commences. The documents were set using letter-size (8.5"×11") paper. The arrangement such as the draft of the background, location of the name, and QR code position in the certificate template is done on the developed windows application. Once done, the QR code is now embedded in the certificate template and can now be printed based on the list of names provided.

In the certificate verification section, after printing, anybody who wants to verify the document must use their smartphone with a camera to scan the QR. The operating system of the phone does not matter, it only requires a camera. However, the user's smartphone wireless fidelity (Wi-Fi) should be connected to the same network as that of the server. After capturing the QR code using the smartphone camera, the verify button needs to be clicked to let the web application send the encrypted hash value to the web server for data integrity verification. The server receives the information stored in the QR code, decrypts the code, and then it will search if the hash value exists in the database. If the hash value is found, the system retrieves the unique certificate ID of the document from the database. The system verifies if the generated encrypted hash value is the same as that saved on the server. If the values are equal, that means it is successfully verified, therefore the message is said to be authentic. If the hash does not exist in the server, the QR code message M was modified. The verification system prompts the message fetch from the server for visual assessment and compared the information from the printed document.

## 2.2. Use case testing

The study adopted alpha testing and will make use of sample documents (certifications) as the source of input. It will take note of message M (name on the document) and document ID to generate the hash value using modified SHA-1. Next, the generated hash will be encrypted using the modified blowfish algorithm, sent to the server, and decrypted when necessary.

The software is to be tested to validate as per compliance with customer requirements and will make use of the blackbox testing technique specifically the use case testing type [22]. This testing was selected to check if all parts of the system are working as intended and are acceptable to the user for quicker test case development, even without the knowledge or access to the code. The target of evaluation is categorized into login, hashing, encryption and decryption, QR code generation, certificate management, and certificate verification as reflected in Table 1. The test case objectives were also stated as well as the equivalent functional requirement. These test cases will be checked against their expected result and will be marked passed or failed depending on the behavior of the software.

Table 1. Test cases

Test case	Test case objective	Functional requirement
Login Module	Test the login functionality with different sets of data	Users shall be able to login into the system using the correct username and password credentials
Hashing Module	Test the hashing module using different certificate ID and message (name)	The system shall be able to generate a hash value using the Modified SHA-1 algorithm out of the certificate ID and message (name).
Encryption and Decryption Module	Test if a series of hash values can be encrypted and decrypted without errors	The system shall be able to encrypt the generated hash value using the Modified Blowfish algorithm before transmitting and decrypting upon saving on the server
QR Code Generation Module	Test if QR codes are correctly generated from sets of encrypted hash values	The system must be able to generate the QR code from the encrypted hash value
Certificate Management Module	Test that QR codes can be placed on certificate templates and can be printed	The user must be able to embed the QR code in the certificate template. The user must be able to print the certificates with the attached QR Code
Certificate Verification Module	Test if printed certificates display the correct message (name) on printed certificates	The user must be able to verify the authenticity of the certificate using the QR code

**2.3. Performance analysis**

After the test case evaluation of the use cases, the error rate will be analyzed and tested using thirty (30) documents with correct entries. Names were generated using a name test data generator tool [23]. The formula for error rate and accuracy will be computed as (1)-(2).

$$Error\ rate = \frac{|observed\ value - actual\ value|}{actual\ value} \times 100 \tag{1}$$

$$Accuracy = 100\% - Error\ rate \tag{2}$$

**3. RESULTS AND DISCUSSION**

In this section, it is explained the results of research and at the same time is given the comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily [24], [25]. The discussion can be made in several sub-sections.

**3.1. Development of the document integrity verification using QR code with modified SHA-1 and modified blowfish**

Before the user can access the system, a login form is created. To verify the authenticity of the user, only authorized username and password credentials are allowed. Figure 2 shows the login screen. Figure 3 demonstrates the creation of the hash value using the certificate ID and the message. The message to be embedded in the QR code is the name of the student to which the certificate belongs. A modified SHA-1 algorithm [26] was applied to create the hash value. After the hash value is created, the hash will be encrypted using modified blowfish algorithm [27] for added security during the transmission of data to the server. This will ensure the safe passage of data that will prevent hacking. After encryption, the QR code will now be generated as shown.



Figure 2. Login screen



Figure 3. Hashing, encryption, and QR code generation



Figure 4. Certificate template with encrypted QR code

Figure 4 shows a sample certificate template where the encrypted QR code was embedded. This certificate may be printed and contains different QR codes from the Certificate ID and names of all attendees of seminars or conferences. Figure 5 displays how the user will see the QR code when viewed on a cellphone camera. The IP address of the server will be displayed and will be directed to the certificate verification module.

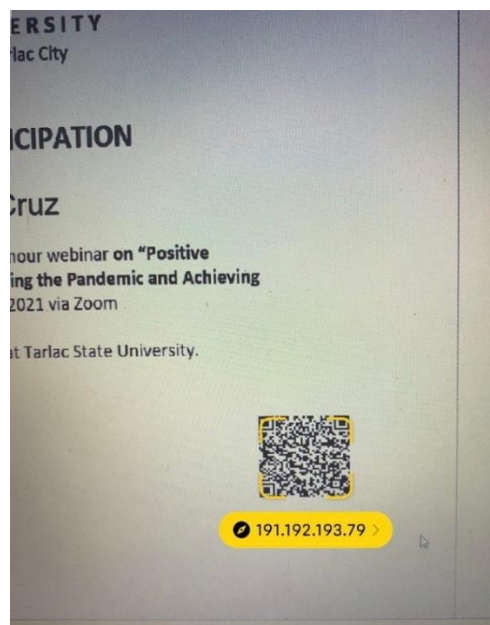


Figure 5. QR code as seen on cellphone camera

Figure 6 illustrates a sample verification message where the name of the holder of the certificate is displayed. This will then be counter-verified to the name listed on the printed certificate. If the names matched, the certificate is said to be untampered and valid.

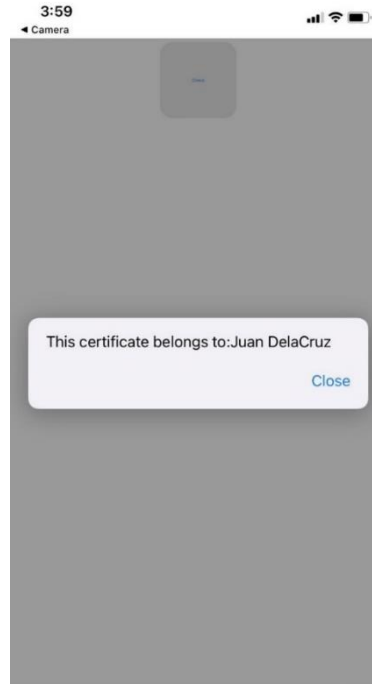


Figure 6. Certificate verification

**3.2. Use Case Testing**

Table 2 displays the test case created for the login module. Four (4) test data were used, and a sample screenshot was inserted to show the result of the test. The module behaves as expected therefore the login module passed the use case test. Table 3 shows the test case created for the Hashing Module. Three (3) sets of certificate ID and name combinations were used. Sample screenshots were attached to show the result of the hashing.

Table 2. Login module test case

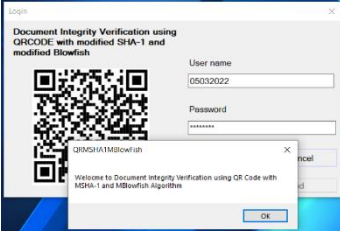
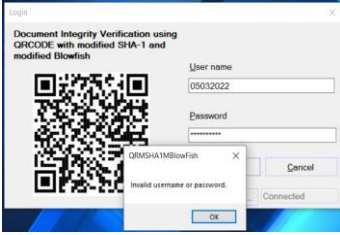
Test case objective	Test data	Expected result	Actual result	Sample screenshot	Remarks
Test the login functionality with different sets of data	1. Valid username and password	Users shall be able to login successfully	Same		Passed
	2. A valid username and invalid password	Users should not be able to log in	Same		Passed
	3. Invalid username and valid password	Users should not be able to log in	Same		Passed
	4. Invalid username and invalid password	Users should not be able to log in	Same		Passed

Table 3. Hashing module test case


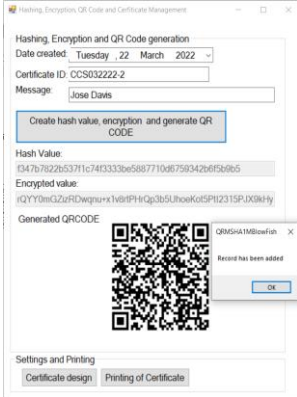
Test case objective	Test data	Expected result	Actual result	Sample screenshot	Remarks
Test the hashing module using different certificate ID and message (name)	CCS032222-1 Lina Upton	5c7a1db3bf 3c20214469 f04d4f43ca a40a11447df f742aa4	Same		Passed
	CCS032222-2 Jose Davis	f347b7822b 537f1c74f3 333be58877 10d6759342b 6f5b9b5	Same		Passed
	CCS032222-3 Giovani Cole	7d0b577323 382f701340 850a93466b ae696e7729b 4f88920	Same		Passed

Table 4 shows the test case created for the Encryption and Decryption Module, the QR Code Generation, and the Certificate Verification test cases. The three (3) names and ID combinations used in the hashing module were re-used here. From the encrypted hash, the QR code is generated and placed in the certificate template. To check the process of decryption, the generated QR from the name was scanned and the decrypted name was displayed. As shown in the table, the same name appears in the certificate and the displayed decrypted hash except for test data four (4). Test data for sample four (4) was intentionally modified to showcase where a copy-pasted QR code will still show the original hash value from the initial certificate ID and name combination. This only signifies that modification or editing of a name without updating the QR code will be detected and thus can be marked as a fraudulent certificate. Sample screenshots were attached to check the comparison. For all input data, the output data is the same indicating that the test case was a success. Table 5 displays the Certificate Management module for the three (3) sets of data. These certificates can be printed after the placement of QR codes on the certificate template.

Table 4. Encryption and decryption, QR code generation, and certificate verification module test case

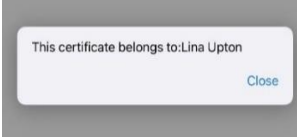

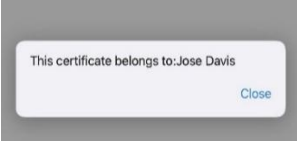

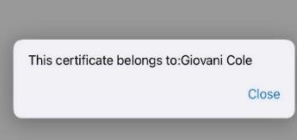

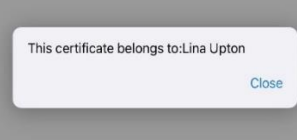

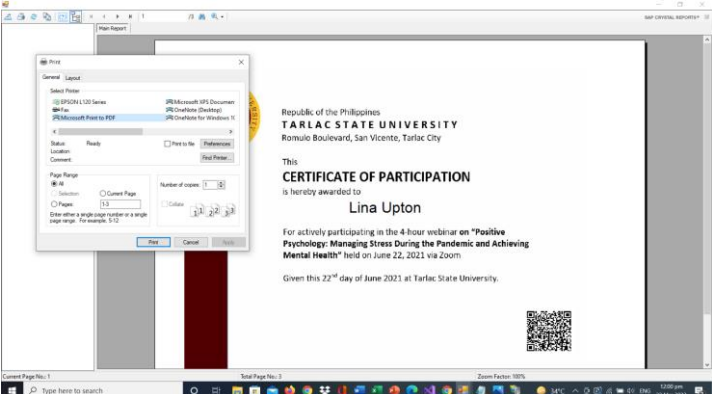
Test Case Objective	Test		Sample Screenshot		
	Data and Expected Result	Actual Result	Decrypted Name	QR Code	Remarks
Test if a series of hash values can be encrypted and decrypted without errors	1. Lina Upton	Same			Passed
	2. Jose Davis	Same			Passed
	3. Giovanni Cole	Same			Passed
	4. Test Data is John Doe, the decrypted value should be Lina Upton	Same			Passed

Table 5. Certificate management module test case module

Test Case Objective	Test Data and Expected Result	Actual Results	Sample Screenshot	Remarks
Test that QR codes can be placed on certificate templates and can be printed	Certificates for Lina Upton, Jose Davis, and Giovanni Cole	Same		Passed



### 3.3. Error rate computation

The observed value here is the number of correct certificates which is 29 and the actual value refers to the number of samples used, in this case, 30 certificates. Out of the 30 samples, one was found incorrect leading to an error rate of 3.33%. Computing for accuracy, the document verification system yields a 96.67% accuracy. The error was further investigated after a certificate does not exist prompted:

$$\text{Error rate} = \frac{|29-30|}{30} \times 100 \% = 3.33 \%$$

$$\text{Accuracy} = 100\% - 3.33\% = 96.67\%$$

Content of the QR CODE that should be generated:

<http://191.192.193.79/?dOFzzTED3yWTMI67YSH8rmX2u31KIfyaZib1B/od0wTIGoql7x2g9mtkhKwHOnSnW3IcttxBDN^/tt/YNMnyBTw==,Devyn Gleichner>

Content of the QR CODE after generation:

<http://191.192.193.79/?dOFzzTED3yWTMI67YSH8rmX2u31KIfyaZib1B/od0wTIGoql7x2g9mtkhKwHOnSnW3IcttxBD^/tt/YNMnyBTw==,Devyn Gleichner>

The capital letter N has been changed to the caret symbol ^.

## 4. CONCLUSION

A more secured document integrity verification using QR code was designed and developed by successfully incorporating a better hashing algorithm-modified SHA-1 and integrating a modern encryption algorithm-modified blowfish algorithm. By integrating both, data integrity and data confidentiality is assured as compared to previous research. The verification works even if no additional software is installed by using the smartphone's built-in camera making it better than other verification software. The developed software has been proven to satisfy all user requirements and is deemed to be acceptable based on the expected and actual results using the test data. The software is also deemed highly accurate with an error rate of 3.33%. However, to achieve 100% accuracy, the QR code generator dll needs to be further investigated and tested to much larger sample size. Exploration of the embedding of the simplest and most economical blockchain technology for an educational institution may also be further studied.

## ACKNOWLEDGEMENTS

The authors would like to express their sincerest thanks to Tarlac State University for their support during the conduct of this research.





## REFERENCES

- [1] J. G. Dongre, "Education Degree Fraud Detection and Student Certificate Verification using Blockchain," *Int. J. Eng. Res.*, vol. V9, no. 07, pp. 287–289, Jul. 2020, doi: 10.17577/IJERTV9IS070156.
- [2] N. Malsa, V. Vyas, J. Gautam, R. N. Shaw, and A. Ghosh, "Framework and smart contract for blockchain enabled certificate verification system using robotics," *Stud. Comput. Intell.*, vol. 960, no. July, pp. 125–138, 2021, doi: 10.1007/978-981-16-0598-7\_10.
- [3] H. Indriyawati, T. Winarti, and V. Vydia, "Web-based document certification system with advanced encryption standard digital signature," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 22, no. 1, pp. 516–521, 2021, doi: 10.11591/ijeecs.v22.i1.pp516-521.
- [4] M. Hasson, A. A. Yassin, A. J. Yassin, A. M. Rashid, A. A. Yaseen, and H. Alasadi, "Password authentication scheme based on smart card and QR code," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 23, no. 1, pp. 140–149, 2021, doi: 10.11591/ijeecs.v23.i1.pp140-149.
- [5] C. M. Li, P. Hu, and W. C. Lau, "AuthPaper: Protecting paper-based documents and credentials using Authenticated 2D barcodes," *IEEE Int. Conf. Commun.*, vol. 2015-Sept, no. January 2013, pp. 7400–7406, 2015, doi: 10.1109/ICC.2015.7249509.
- [6] T. Mantoro, D. D. Permadi, and A. Abubakar, "Stegano-image as a digital signature to improve security authentication system in mobile computing," in *2016 International Conference on Informatics and Computing (ICIC)*, 2016, no. Icic, pp. 158–163, doi: 10.1109/IAC.2016.7905708.
- [7] Q. Aini, U. Rahardja, M. R. Tangkaw, N. P. L. Santoso, and A. Khoirunisa, "Embedding a Blockchain Technology Pattern Into the QR Code for an Authentication Certificate," *J. Online Inform.*, vol. 5, no. 2, p. 239, 2020, doi: 10.15575/join.v5i2.583.
- [8] A. M. Ali and A. K. Farhan, "Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document," *IEEE Access*, vol. 8, pp. 27448–27458, 2020, doi: 10.1109/ACCESS.2020.2971779.
- [9] K. Kumutha and S. Jayalakshmi, "The Impact of the Blockchain on Academic Certificate Verification System-Review," *EAI Endorsed Trans. Energy Web*, vol. 8, no. 36, pp. 1–8, 2021, doi: 10.4108/eai.29-4-2021.169426.
- [10] K. Dhyani, J. Mishra, S. Paladhi, and I. S. Thaseen, "A Blockchain-Based Document Verification System for Employers," in *Algorithms for Intelligent Systems*, 2022, no. March, pp. 123–137, doi: 10.1007/978-981-16-7182-1\_11.





- [11] C. Shaik, "Preventing forged and fabricated academic credentials using cryptography," *Int. J. Comput. Sci. Eng. Appl.*, vol. 11, no. 1, pp. 11–20, 2021, doi: 10.5121/ijcsea.2021.11102.
- [12] Z. Yahya *et al.*, "A New Academic Certificate Authentication Using Leading Edge Technology," in *Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government - ICEEG 2017*, 2017, pp. 82–85, doi: 10.1145/3108421.3108428.
- [13] A. Singhal and R. S. Pavithr, "Degree Certificate Authentication using QR Code and Smartphone," *Int. J. Comput. Appl.*, vol. 120, no. 16, pp. 38–43, Jun. 2015, doi: 10.5120/21315-4303.
- [14] A. Wibiyanto and I. Afrianto, "QR code and transport layer security for licensing documents verification," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 407, no. 1, 2018, doi: 10.1088/1757-899X/407/1/012069.
- [15] D. Jagodic, D. Vujicic, and S. Randic, "Android system for identification of objects based on QR code," *2015 23rd Telecommun. Forum, TELFOR 2015*, vol. 7, pp. 922–925, 2016, doi: 10.1109/TELFOR.2015.7377616.
- [16] G. K. Hong and S. Sinha, "Tracking Vulnerable People Using Body Worn QR Code," 2018.
- [17] M. U. Abdullahi, G. I. O. Aimufua, and A. Aminu, "Certificate Generation and Verification System Using Blockchain Technology and Quick Response Code," *IOSR J. Comput. Eng.*, vol. 24, no. May, pp. 37–47, 2022, doi: 10.9790/0661-2401023747.
- [18] R. L. Quilala, A. M. Sison, and R. P. Medina, "QR Code Integrity Verification Based on Modified SHA-1 Algorithm," *Indones. J. Electr. Eng. Informatics*, vol. 6, no. 4, pp. 385–392, 2018, doi: 10.11591/ijeii.v6i1.494.
- [19] D. Agnihotri, S. Ahmed, D. Darekar, C. Gadkari, S. Jaikar, and M. Pawar, "A Secure Document Archive Implemented using Multiple Encryption," *Proc. - Int. Conf. Smart Electron. Commun. ICOSEC 2020*, no. Icosec, pp. 765–770, 2020, doi: 10.1109/ICOSEC49089.2020.9215302.
- [20] F. Ahmad and L.-M. Cheng, "Paper Document Authentication Using Print-Scan Resistant Image Hashing and Public-Key Cryptography," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, vol. 11611 LNCS, pp. 157–165, doi: 10.1007/978-3-030-24907-6\_13.
- [21] M. S. Ahamed and H. A. Mustafa, "A Secure QR Code System for Sharing Personal Confidential Information," *5th Int. Conf. Comput. Commun. Chem. Mater. Electron. Eng. IC4ME2 2019*, no. November, 2019, doi: 10.1109/IC4ME247184.2019.9036521.
- [22] M. A. Umar, "Comprehensive study of software testing: Categories, levels, techniques, and types," *Int. J. Adv. Res. Ideas Innov. Technol.*, vol. 5, no. 6, pp. 32–40, 2019, doi: 10.36227/techrxiv.12578714.
- [23] Coders Tool, "Name Test Data Generator Tool," 2022. [Online]. Available: [https://www.coderstool.com/fake-test-identity-data?fbclid=IwAR1ppNxa8iIKq5Hx6pygbl\\_2vzndCvkrZjEELsuvPATz4nx76wKS3vi7M](https://www.coderstool.com/fake-test-identity-data?fbclid=IwAR1ppNxa8iIKq5Hx6pygbl_2vzndCvkrZjEELsuvPATz4nx76wKS3vi7M). [Accessed: 03-Mar.-2022].
- [24] J. Sadowski, "When data is capital: Datafication, accumulation, and extraction," *Big Data Soc.*, vol. 6, no. 1, pp. 1–12, 2019, doi: 10.1177/2053951718820549.
- [25] J. R. Saura, B. R. Herraiez, and A. R. Menendez, "Comparing a traditional approach for financial brand communication analysis with a big data analytics technique," *IEEE Access*, vol. 7, pp. 37100–37108, 2019, doi: 10.1109/ACCESS.2019.2905301.
- [26] R. L. Quilala, A. M. Sison, and R. P. Medina, "Modified SHA-1 Algorithm," vol. 11, no. 3, pp. 1027–1034, 2018, doi: 10.11591/ijeecs.v11.i3.pp1027-1034.
- [27] T. F. G. Quilala, A. M. Sison, and R. P. Medina, "Modified Blowfish Algorithm," vol. 12, no. 1, pp. 38–45, 2018, doi: 10.11591/ijeecs.v12.i1.pp38-45.

## BIOGRAPHIES OF AUTHORS



**Dr. Rogel Ladia Quilala**     is an Assistant Professor of ICT at the Tarlac State University-College of Computer Studies Tarlac City Philippines. He received his Doctor in Information Technology (DIT) degree from Technological Institute of the Philippines (TIP), Cubao Quezon City Philippines. His research areas are security and data mining. He is the Chairperson of the Master in Information Technology Department. He has 18 years of academic experience teaching ICT courses at the tertiary level. During this time, he had a stint as an exchange professor in IT at YeungJin College in South Korea. He can be contacted at email: rlquilala@tsu.edu.ph.



**Dr. Theda Flare G. Quilala**     is currently an Associate Professor in the College of Computer Studies at Tarlac State University, Tarlac City, Philippines. A Doctor of Information Technology graduate at Technological Institute of the Philippines and a CHED K-12 scholar. Research interest includes security, data mining, and algorithms. She is currently the Director of the Admission and Registration Office. She can be reached via email at tfgquilala@tsu.edu.ph.