RESEARCH ARTICLE OPEN ACCESS

Verification of University Degree Authenticity Using Encryption, Digital Signature, and QR Code Techniques

Fatima Al-Zahraa Mohamed Drrar Seyd
Maab Faisal Al-Haj Ibrahim
Department of Information Technology, Faculty of Computing Studies
Al-Ribat National University, Khartoum, Sudan

ABSTRACT

This study aims to enhance the reliability of university certificates and verify their authenticity using encryption techniques, digital signatures, and Quick Response (QR) codes, within the framework of applying the principles of information security: confidentiality, integrity, and availability. This study comes in response to the increasing cases of forgery and falsification faced by educational institutions, which weaken trust in the credibility of university certificates and affect the reliability of academic systems.

The study adopted the experimental methodology to design and implement an integrated electronic system aimed at protecting data and verifying its validity using advanced encryption algorithms, including RSA, SHA-256, and AES. An Android application was also developed to read QR codes embedded in university certificates, providing an immediate and secure verification mechanism for the correctness of the content and its source, without the need for manual intervention or official correspondence. The results of the study demonstrated the system's effectiveness in reducing manipulation of university certificates and facilitating their electronic verification. It also confirmed that integrating symmetric and asymmetric encryption with digital signatures provides high levels of security, confidentiality, and protection of sensitive data.

The study recommends several measures to ensure the sustainability of the proposed system's effectiveness, most notably developing standalone versions of the verification application compatible with various operating systems to ensure optimal performance, and adding a comprehensive scanning feature for the printed certificate to enable integrated visual and digital verification. It also recommends regular updates to encryption algorithms.

Keywords **:—** Information Security, Encryption, Digital Signature, QR Code, University Certificates, Digital Integrity

I. INTRODUCTION

The world is currently witnessing rapid development in the field of digital transformation, where modern technologies have become a fundamental pillar in various sectors of life, including higher education and the management of academic documents. Along with this development, new challenges related to information security have emerged, particularly the forgery and falsification of university certificates, which directly affect the credibility of educational institutions and the trust of the academic community and employers in their outputs. University certificates are highly important official documents, as they serve as proof of an individual's academic and professional qualifications; therefore, any tampering with them constitutes a serious violation of academic integrity.

Hence, there is a growing need to adopt technological solutions that ensure the protection of these documents from manipulation and enable reliable and rapid verification of their authenticity.

Encryption and digital signature technologies have contributed to a significant shift in the field of information security, as they provide the ability to protect sensitive data and ensure its integrity against any modification or forgery, in addition to verifying the identity of the issuing authority. Quick Response (QR) codes have also formed an important addition, as they allow quick access to data stored in secured databases and electronic verification of authenticity.

From this standpoint, this study aims to present an applied model that integrates encryption and digital signature techniques with QR codes to ensure the security and reliability of university certificates, thereby enhancing trust in educational institutions and contributing to reducing academic fraud.

II. STUDY PROBLEM

University certificates in the digital age face a serious issue related to the misuse of modern technologies in forgery and content manipulation. It has become possible to easily design fake copies of certificates using advanced image-editing software and professional

printing tools, making it difficult to distinguish between original and counterfeit certificates.

This situation has led to a decline in trust in academic documents issued by some educational institutions, negatively affecting their reputation and the credibility of their academic qualifications at both local and international levels.

In addition, traditional paper-based verification systems lack digital tools that enable stakeholders to validate certificates automatically and quickly. Manual verification methods require significant time and effort and open the door to human error and fraudulent attempts.

Accordingly, the main research problem lies in the absence of a unified and secure electronic system that allows direct digital verification of the authenticity of university certificates, thereby reducing forgery opportunities and enhancing document reliability.

III. SIGNIFICANCE OF THE STUDY

The significance of this study lies in supporting the information security framework within educational institutions by providing a secure and rapid electronic verification model for university certificates. It also contributes to strengthening trust in academic documents and supporting digital transformation in higher education, particularly within Arab universities.

IV. STUDY OBJECTIVES

This research aims to build an integrated electronic system for documenting and verifying university certificates using encryption techniques, digital signatures, and QR codes. The

objectives include implementing AES, RSA, and SHA-256 algorithms, integrating QR codes for instant verification, developing an Android verification application, and evaluating system performance in a real university environment.

V. THEORETICAL FRAMEWORK

Information security focuses on protecting data from unauthorized access, modification, or misuse and is based on confidentiality, integrity, and availability. University certificates require high levels of protection due to their official nature.

A. Encryption Technologies

Encryption transforms readable data into an unreadable format. Symmetric encryption such as AES provides efficiency and speed, while asymmetric encryption such as RSA ensures secure key exchange and digital signature implementation.

B. Digital Signature

Digital signatures verify document authenticity and integrity and ensure non-repudiation, commonly implemented using RSA combined with SHA-256.

C. QR Code

QR codes enable fast electronic access to encrypted verification data and support instant validation of printed documents through scanning mechanisms.

VI. PREVIOUS STUDIES

Several recent studies have addressed securing academic and official documents using encryption, digital signatures, QR codes, and blockchain technologies.

Purwanto et al. (2025) proposed Certifichain, a blockchain-based platform that enables educational institutions to issue verifiable digital certificates using QR codes linked to blockchain records. The system achieved instant verification and reduced forgery risks while lowering operational costs. However, the study focused exclusively on digital certificates and depended on continuous blockchain connectivity, without addressing the protection of printed certificates. In contrast, the current study focuses on securing printed university certificates by embedding encrypted digital signatures within QR codes without full dependency on blockchain infrastructure.

Nuraeni et al. (2024) introduced a QR-code-based digital signature scheme using RSA and AES-128 super encryption. The study demonstrated improved security through double encryption but was limited to technical implementation without application in a specific academic context or evaluation of user experience. The current study extends this work by applying the same cryptographic principles within a complete university certificate verification system and measuring verification speed and usability in a real environment.

Suhardi (2024) proposed a document authentication system using QR codes and DSA-based digital signatures. While the system successfully verified document authenticity, it relied on a single cryptographic algorithm and did not evaluate printed document

verification after issuance. The current study enhances security by adopting RSA and SHA-256 and focusing on detecting tampering in printed certificates.

Sarfarz et al. (2024) developed a blockchain-based certificate issuance and verification system integrated with QR codes, achieving high security and fast verification. However, verification depended on a centralized digital platform. In contrast, the current study enables direct verification of printed certificates using a mobile application without requiring a centralized verification platform.

Walidaniy et al. (2023) utilized ECC-based digital signatures combined with QR codes to enhance document authenticity, achieving improved security and performance. The study did not address academic certificate contexts or provide comparative evaluation. The current study applies RSA and SHA-256 within an academic framework and evaluates verification speed and tamper detection accuracy.

Djajadi et al. (2023) proposed a blockchain-based automated e-certificate verification architecture that improved verification speed and reduced forgery. The approach focused on digital certificates, whereas the current study addresses the gap by securing and verifying printed university certificates in real usage scenarios.

VII. RESEARCH METHODOLOGY AND TOOLS

The study adopted the descriptive method to evaluate the effectiveness of the proposed system. Java, Android Studio, C#, Visual Studio, Firebase, and cryptographic libraries were used to implement and test the system. Performance, security, and usability tests were conducted using real certificates issued by Al-Ribat National University.

VIII. RESULTS AND DISCUSSION

The results confirmed the system's ability to detect certificate tampering instantly and verify authenticity within seconds. The integration of encryption, digital signatures, and QR codes achieved a balance between security and ease of use, reducing reliance on manual verification procedures.

IX. CONCLUSION AND RECOMMENDATIONS

The study demonstrated that integrating AES, RSA, SHA-256, and QR codes provides an effective solution to university certificate forgery. The proposed system enhances document reliability and supports digital transformation in higher education.

Future recommendations include expanding platform compatibility, enhancing visual verification features, and exploring integration with emerging technologies such as blockchain and artificial intelligence.

REFERENCES

[1] J. Horowitz, "Relative education and the advantage of a college degree," Pew Research Center, Washington, DC, USA, 2018.

[2] L. S. L. Carroll, "A comprehensive definition of technology from an ethological perspective," Social Sciences, vol. 6, no. 4, p. 126, 2017.

[3] D. Carrington, "Software engineering tools and methods knowledge area," in Guide to the Software Engineering Body of Knowledge (SWEBOK), ch. 10. Piscataway, NJ, USA: IEEE Computer Society, 2001.

[4] Elisava – Barcelona School of Design and Engineering, "What is a university degree?," 2024. [Online]. Available: Elisava official website.

[5] Association of Public and Land-grant Universities (APLU), "How does a college degree improve graduates' outcomes?," Washington, DC, USA, n.d.

[6] اليوم السابع، "تزوير الشهادات الدراسية: جريمة تهدد مصداقية التعليم والداخلية تتصدى لها"، اليوم السابع، 4 يوليو 2025.

[7] ع. بن محمد أبو عمّه، "الشهادات المزورة والوهمية والواهِنة والاعتمادات الصورية"، 2018.

[8] J. Hilton and Y. Cherdantseva, "A reference model of information assurance and security," 2015.

[9] Bakkah, "أمن المعلومات: أهميته، أنواعه، واستراتيجيات الحماية"، n.d.

[10] K. Somsuk and S. Phon-Amnuaisuk, "The development of signing and verification methods for electronic official documents," Cogent Engineering, 2024.

[11] Y. Xu, "Development of blockchain-based academic credential verification system," Open Access Library Journal, vol. 11, p. e12130, 2024.

[12] المؤسسة الوطنية للأمن السيبراني، "المعايير الوطنية للتشفير," يوليو 2020.

[13] OneFlow, "How to make a digital signature secure and safe?," June 2023.

[14] National Institute of Standards and Technology (NIST), SP 800-131A Rev. 2: Transitioning the Use of Cryptographic Algorithms and Key Lengths, Gaithersburg, MD, USA, 2019.

[15] National Institute of Standards and Technology (NIST), Announcing the Advanced Encryption Standard (AES) (FIPS PUB 197), U.S. Department of Commerce, 2001.

[16] National Institute of Standards and Technology (NIST), Secure Hash Standard (SHS) (FIPS PUB 180-4), U.S. Department of Commerce, 2015.

[17] Microsoft, "What is SQL Server?," Microsoft Documentation, 2023.

[18] Google Developers, "Android Studio overview," Google, 2024.

[19] Oracle, "What is the Java platform?," Oracle Documentation, 2024.

[20] PlantText, "PlantText UML editor – free online tool for drawing UML diagrams," 2024.

[21] Google Developers, "Firebase documentation," Google, 2024.

[22] Microsoft, "C# language documentation," Microsoft Learn, 2024.

[23] Microsoft, "Visual Studio documentation," Microsoft Learn, 2024.

[24] Balsamiq Studios, "Balsamiq wireframes documentation," 2024.

[25] أ. م. يسري، "رفع المستويات التأمينية للوثائق الحكومية بتضمين رموز الاستجابة السريعة ذات المعلومات البيومترية لحاملي الوثائق رقميًا," 2025.

[26] س. بن يوسف، "تكنولوجيا البلوك تشين وتطبيقاتها المحتملة في أرشفة الوثائق الجامعية," 2025.

[27] " تطبيق تقنية البلوك تشين في التحقق من الوثائق الأكاديمية بوزارة التعليم بالمملكة العربية السعودية," 2024.

[28] س. ص. ح. الدافع وج. أ. ح. قطب، "تطبيقات البلوك تشين في التعليم," 2024.

[29] Y. Purwanto et al., "Certifichain: Secure QR codes for blockchain-verified digital credentials," 2025.

[30] F. Nuraeni, D. Kurniadi, and D. N. Rahayu, "Implementation of RSA and AES-128 super encryption on QR-code based digital signature schemes," 2024.

[31] S. Suhardi, "Use of QR code and digital signature using the DSA method to authenticate student academic documents," 2024.

[32] M. Sarfarz, M. Raj, and V. Singhal, "Create certificate and verification system using blockchain technology and fast response," 2024.

[33] W. D. Walidaniy, M. Yuliana, and H. A. Darwito, "Enhancing document authenticity with QR codes and ECC-based digital signatures," 2023.

[34] A. Djajadi, K. S. Lestari, L. E. Englista, and A. Destaryana, "Blockchain-based e-certificate verification and validation automation architecture," 2023.

[35] TutorialsPoint, "Software design basics," 2023.

[36] TutorialsPoint, "UML – class diagrams," 2023.

[37] TutorialsPoint, "Software implementation phase," 2023.