MINAR International Journal of Applied Sciences and Technology
ISSN: 2717-8234
Article type: Research Article

Received: 21/06/2022	**Accepted:**18/07/2022	**Published:** 01/09/2022

DOCUMENTS ISSUANCE VALIDATION USING 2D BARCODE

Mohammad A. TAHA ALDABBAGH[1]

University of Mosul, Iraq

Abstract

The daily procedures in both official and non-official organizations include the printing and archiving of thousands of paper-based documents, either as issued, incoming, or as attachment documents; as well as the verification of the authenticity of the issuance of such documents at the receiving party, this leads to the production of further papers that are referred to as "issuance validation", This procedure costs more time, effort, and money. Furthermore, the process of archiving and storing these documents electronically requires considerable effort and time in terms of manually entering the information or saving them as images, as well as the possibility of data entry mistakes. This paper proposes employing authenticated PDF417 barcodes in paper-based document publication procedures by adding an encrypted barcode (signature) to the issued document and making it simpler to authenticate the information. During the document verification process, neither internet access nor real-time interaction with the document issuer are required. Furthermore, the proposed system offers a way to digitally archive documents using a barcode scanner or smartphones, which enables accuracy and speed in entering the information of documents received or issued by the institution.

Keywords: PDF417, Issuance Validation, Encrypted 2D Barcode.

http://dx.doi.org/10.47832/2717-8234.12.2

[1] m.a.taha@uomosul.edu.iq, https://orcid.org/0000-0003-2240-9643

Introduction

Barcodes are widely used nowadays and it is a basic or supportive technique. barcodes have been used almost everywhere, including transportation (Taufik et al., 2021; Zubkov & Sirina, 2020), government(CHEN et al., 2021), manufacturing(Schuitemaker & Xu, 2020), marketing (Zhou et al., 2021), retail business, and automotive business(Rivera et al., 2021). Although the barcode provides speed to deal with data, it lacks confidentiality, so it is possible to increase confidentiality by adding some encryption algorithms to the texts encoded in the barcode. And through the use of encrypted barcodes, confidentiality, authentication and speed in dealing with documents will be provided.

BARCODES

barcode is a machine-readable representation of data attached to the item to which it is related. barcodes can be found in a different format 1D,2D and 3D formats(Morovia Corporation, 2009). Barcode can be read by scanners that read small images of lines and spaces and interpret these symbols into data and validate it. barcodes provides an easy and low-cost way of encoding data that is easily read using electronic readers. Barcodes are widely used nowadays because barcode technology provide a rapid and precise method for data entry without keyboard. Maintaining the Integrity of the Specifications

1D BARCODES

Calles also linear barcode "it is the first generation, 'one dimensional' barcode that is made up of lines and spaces of various widths that create specific patterns"(Morovia Corporation, 2009). there are several types of 1D barcodes like ISSN, MSI/Plessey, RSS, Code 39, Code 93, Code 128 ISBN and etc. Figure 1: 1D shows some examples of 1D barcodes.

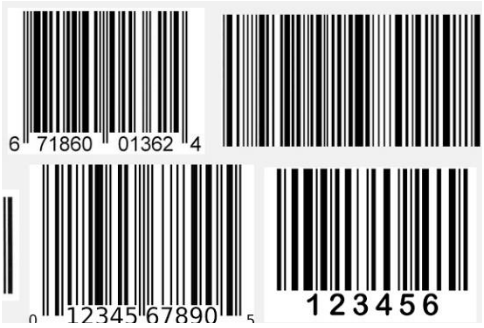

Figure 1: 1D barcodes (Morovia Corporation, 2009)

A. 2D BARCODES

2D barcode gives more information as it takes the form of a matrix and is mostly in the form of an image, and there are also different types of it - PDF417 - QR Code - Maxi Code - Data Matrix. Figure 2 shows a group of two-dimensional bar codes and their different types.

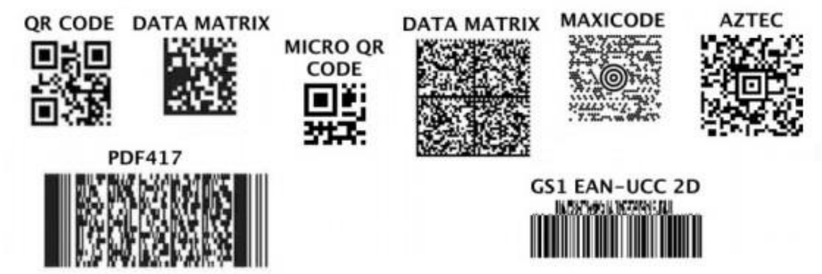

Figure 2 :2D barcode (Morovia Corporation, 2009)

B. *PDF417 2D Barcode*

The PDF417 barcode is a multi-row, variable-length barcode that has the ability to both store a huge amount of data and correct any possible errors. The PDF417 barcode is one of the most widely used barcodes since it has a number of characteristics that are exclusive to it. The PDF417 code can be read by a variety of different types of scanners, including laser scanners, linear scanners, and two-dimensional scanners. The fact that the PDF417 code can encode over 1100 bytes, 1800 text characters, or 2710 digits (Morovia Corporation, 2009)is another advantage of using this code. The feature is the main reason for choosing this type of barcode in this paper as the sender can encode and encode enough information about the sent document.

The PDF417 code consists of several main elements (patterns), as shown in Figure (3), which are: (Morovia Corporation, 2009)

- module
- start pattern
- ciphertext codeword
- stop pattern
- row indicators
- row
- column

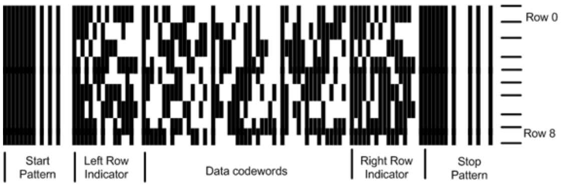

Figure 3: Anatomy of a PDF417 symbol (Morovia Corporation, 2009)

ENCRYPTION

Cryptography is the science of protecting data, by converting data into illegible form, so can be accessed by valid users at Destination. Cryptography using mathematics to encrypt and decrypt data. Data encryption is protecting information from eavesdropping. It converts data (plaintext) to another format (cipher text) using an encryption key(Calderbank, 2007).

Asymmetric cryptography is employed in digital signatures. In many applications, they serve as an additional layer of verification and assurance for messages that are sent through insecure channels. When used correctly, a digital signature gives the recipient reason to assume that the message was sent by the person or organization that was identified as the sender.

One of the best well-known asymmetric cryptography algorithms is RSA (Rivest et al., 1978) and it is a public-key cryptography algorithm. And it is convenient for signing and encryption. RSA used widely in e-commerce transactions, and adequately secure given sufficiently long keys(Calderbank, 2007).

The aim of RSA is to construct an algorithm that makes determining the private key impossible. The one-way function is used in this algorithm. The function is simply one-way, as the name implies, which means that it is quite simple to compute the result given certain input numbers. However, determining the input values given the result is exceedingly difficult, if not impossible. In mathematical terms, computing f (x) is reasonably straightforward given x, whereas computing x is exceedingly difficult given f (x). The multiplication of two very big prime numbers is the one-way function utilized by RSA. Multiplying them is rather simple, but factorizing them is highly complex, if not impossible, and time - intensive. It is typically used for message encryption, but it may also be used for digital signature over a message, which is what this paper proposes.

The RSA algorithm's step-by-step procedure is as follows:

- select two very large prime numbers **p** and **q**, each approximately 256 bits.
- Multiply **p** and **q** together to get **n**. $n = p \bullet q$
- **p** and **q** are kept secret, but **n** is made public. Even if **n** is known, factorizing a really high integer is computationally infeasible, therefore getting back **p** and **q** is not practicable.
- Generate a public key **<e, n>** where **e**: 1 < **e** < **φ (n)** is reasonably prime to the "totient" function $\varphi(n) = (p-1)(q-1)$
- Generate a private key <**d, n**> where **d** is the multiplicative inverse of **e** mod **φ(n)**.
- To Sign the message encrypt it with the private key <**d, n**> and decrypting it with the public key **<e, n>**.
- Generate the cipher text **c** by Encrypting the message **m** (< **n**), using:

$c = m^e \bmod n.$

or

$c = m^d \bmod n.$

- Regenerate the message **m** by Decrypting the cipher text **c**, using:

$m = c^d \bmod n.$

or

$m = c^e \bmod n.$

RSA employs a public and a private key pair. The public key is made available to the public and is used to encrypt the data. Data encrypted with the public key can only be decrypted with the private key, and vice versa (Calderbank, 2007).

LITERATURE REVIEW

Albar and Perdana (Albar & Perdana, 2021)used the Laravel framework in PT to develop a digital certificate printing system and use barcode technology to assist certificate authentication.

Shah and Parihar (Shah & Parihar, 2017)used QRcode with RSA to communicate and share files among android devices, they also use the MD5 algorithm to check the algorithm and its integrity.

Yicheng Zhan and others (Zhan, 2020)used QRcode to avoid customer purchase of counterfeit goods through interaction of QRcode data with customer and server. Also, RSA and DES were used to encrypt QRcode to ensure data security.

Jau Ji Shen and Ken Tzu Liu (Shen & Liu, 2014)proposed a solution to the problem by considering the digital document as an image, allowing them to extract the digital document's authentication code from the text of the document itself, resulting in only the authentication code being encrypted in the image version of the initial document. The most significant advantage of this approach is that when the authentication code is encrypted, the document can be preserved at the same size.

Chak Man Li and others (Li et al., 2015) utilized the QR code to convey a huge amount of self-describing and, most importantly, verified data in a variety of formats, including text, images, and binary data. By embedding the certified 2D barcode as an integral part of the document, it is simple to check the validity of a paper-based document by comparing its content to the matching numbers.

RESEARCH PROBLEM AND CONTRIBUTION

It is possible to define the problem as the fact that there is no way to verify the authenticity of documents other than by using traditional methods, such as issuing another document, which takes a long time for the process and the arrival of the new document, or by using methods reviewed in the literature review, most of which require the availability of Internet service for both the sending and receiving parties.

The proposed tool enables the sender to encode the barcode, and it makes it possible for the receiver to decode the information and verify its validity in the absence of an internet service.

In addition, the tool that is being proposed would provide a mechanism for archiving documents and storing their information in a speedy, efficient, and error-free way, which is now impossible due to manual data entry.

METHODOLOGY

To simplify understanding of the proposed system's procedure, the design will be separated into two parts: the document issuer party and the document recipient party.

Issuer party:

Step 1: The user configures the encryption keys (both public and private keys) using the proposed system in a random fashion.

Step 2: The user then keeps the private key (which will be used to encrypt the barcode), submits the public key to the system, and the system declares it for all users.

After the issuance of the document is completed,

Step 3: The user chooses the fields that will be included in the barcode such as (the document number, the date of issue, the title of the document, the addressee, the issuer and parts of the document’s content) and it is the same information that is used in the archiving process**Step 4**: The system encodes the information (**signs the document**) using the private-key and converts it into a PDF417 code, and then this barcode is added to the document.

Figure (4) illustrated the proposed system steps in issuer party.

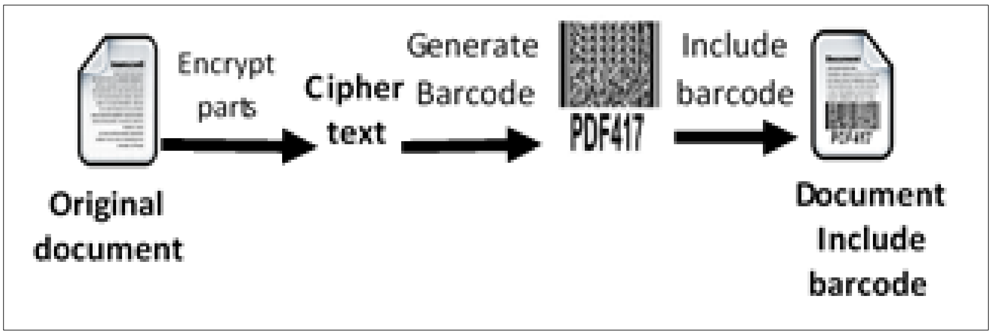

Figure 4:The document creation process for the issuer

Recipient party:

Step 1: The receiving party reads the PDF417 barcode using a barcode reader or phone camera.

Step 2: The system analyzes the barcode and converts it into text (the cipher text).

Step 3: The system decrypts the text using the public key.

Step 4: The user shows the information entered by the sender.

If the information in the received document matches, it means that the document is correct and has not been tampered with. Figure (5) illustrates the system steps in recipient party.

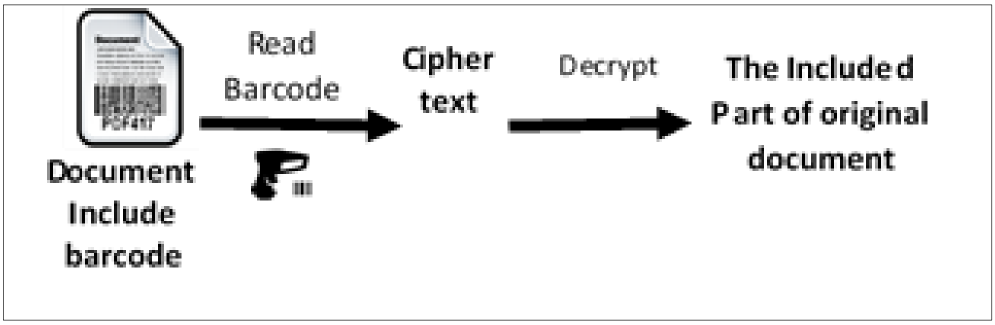

Figure 5:Read barcode and decrypt process by the recipient

Whereas encrypting the text with the private key is regarded the signature of the document's issuing party, decrypting it using the public key and retrieving parts of it will demonstrate that it has not been tampered with.

RESULTS DISCUSSION

While encrypting the text with the private key is considered the issuing party's signature, decrypting it with the public key and retrieving it proves that it has not been tampered with. The processes that are being proposed for the new system produce two key benefits:

1- **Document authenticity verification**:

The current procedures in organizations require a submission of an additional document to verify the authenticity of the issue for the original document, which can take anywhere from one to eight weeks. On the other hand, the proposed system eliminates this delay by employing the barcode that is embedded on the original document that was received.

2- **Document auto archiving**:

By reading and decrypting the barcode at the recipient party, the barcode will be automatically converted into a set of information that is used in archiving and indexing paper documents into digital datasets that can be exported later in the form of datasheets; this will reduce the amount of time that the recipient must manually enter this information by the data entry employee, as well as eliminate data entry errors.

Table 1 presents a brief summary of the effectiveness study results.

Aspect	**Present procedure**	**Proposed System**
Time for Authenticity	1-8 weeks	0
Document information data entry	3 / min	20 / min
Data entry errors percentage	1-4%	0%

Table 1: Comparison summary

CONCLUSION

The proposed system can guarantee the authenticity of issued documents because of the encoding process included into the PDF417 barcode. Since the barcode and its contents were encrypted using RSA public key cryptography, forgery is next to impossible.

Additionally, the system that is being proposed provides a method of electronically archiving documents through the utilization of a barcode scanner. This offers both precision and speed in the process of entering the information of documents that have been received or issued by the institution.

Finally, all documents can be recognized by the proposed system even if they were printed or copied poorly, due to the PDF417 coding's error-correction features.

References

Albar, D., & Perdana, B. F. F. (2021). Designing Digital Certificate Issuance Information System. *IOP Conference Series: Materials Science and Engineering*, *1158*(1), 012018. https://doi.org/10.1088/1757-899X/1158/1/012018

Calderbank, M. (2007). *The RSA Cryptosystem: History, Algorithm, Primes*.

CHEN, T., DING, K., YU, Z., LI, G., & DONG, Y. (2021). Smart Supervision for Food Safety in Food Service Establishments in China: Challenges and Solutions. *Journal of Food Protection*, *84*(6), 938–945. https://doi.org/10.4315/JFP-20-370

Li, C. M., Hu, P., & Lau, W. C. (2015). AuthPaper: Protecting paper-based documents and credentials using Authenticated 2D barcodes. *2015 IEEE International Conference on Communications (ICC)*, 7400–7406. https://doi.org/10.1109/ICC.2015.7249509

Morovia Corporation. (2009). *PDF417 Fontware & Writer SDK 4.1 User Manual*. http://www.morovia.com.

Rivera, R., Amorim, M., & Reis, J. (2021). Technological Evolution in Grocery Retail: A Systematic Literature Review. *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–8. https://doi.org/10.23919/CISTI52073.2021.9476598

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

Schuitemaker, R., & Xu, X. (2020). Product traceability in manufacturing: A technical review. *Procedia CIRP*, *93*, 700–705. https://doi.org/10.1016/j.procir.2020.04.078

Shah, A. T., & Parihar, V. R. (2017). Overview and an approach for QR-code based messaging and file sharing on android platform in view of security. *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, 371–373. https://doi.org/10.1109/ICCMC.2017.8282711

Shen, J. J., & Liu, K. T. (2014). A Novel Approach by Applying Image Authentication Technique on a Digital Document. *2014 International Symposium on Computer, Consumer and Control*, 119–122. https://doi.org/10.1109/IS3C.2014.42

Taufik, M., Hudiono, H., Rakhmania, A. E., Perdana, R. H. Y., & Sari, A. S. (2021). An Internet of Things Based Intercity Bus Management System for Smart City. *International Journal of Computing and Digital Systems*, *10*(1), 1219–1226. https://doi.org/10.12785/ijcds/1001109

Zhan, Y. (2020). Anti-Fake Technology of Commodity by Using QR Code. *2020 International Conference on E-Commerce and Internet Technology (ECIT)*, 1–4. https://doi.org/10.1109/ECIT50008.2020.00008

Zhou, Y., Hu, B., Zhang, Y., & Cai, W. (2021). Implementation of Cryptographic Algorithm in Dynamic QR Code Payment System and Its Performance. *IEEE Access*, *9*, 122362–122372. https://doi.org/10.1109/ACCESS.2021.3108189

Zubkov, V. v., & Sirina, N. F. (2020). Advanced technologies of international cargo correspondence in railway transport. *IOP Conference Series: Materials Science and Engineering*, *760*(1). https://doi.org/10.1088/1757-899X/760/1/012056