

Secure QR-Code Generation in Healthcare

Safa S. Abdul-Jabbar

Computer Science Department, College of Science for Women, University of Baghdad, Baghdad, Iraq; 1,2 Computer Science Department, University of Technology, Baghdad, Iraq, safa.s@csw.uobaghdad.edu.iq

Alaa k. Farhan

Computer Science Department, College of Science for Women, University of Baghdad, Baghdad, Iraq; 1,2 Computer Science Department, University of Technology, Baghdad, Iraq

Follow this and additional works at: <https://kijoms.uokerbala.edu.iq/home>

Recommended Citation

Abdul-Jabbar, Safa S. and Farhan, Alaa k. (2023) "Secure QR-Code Generation in Healthcare," *Karbala International Journal of Modern Science*: Vol. 9 : Iss. 2 , Article 14.

Available at: <https://doi.org/10.33640/2405-609X.3294>

This Research Paper is brought to you for free and open access by Karbala International Journal of Modern Science. It has been accepted for inclusion in Karbala International Journal of Modern Science by an authorized editor of Karbala International Journal of Modern Science. For more information, please contact abdulateef1962@gmail.com.



Secure QR-Code Generation in Healthcare

Abstract

QR codes have become ubiquitous across several industries, including e-commerce, education, and healthcare. In the healthcare sector, QR codes are increasingly used to relay essential information regarding medical products, patient history, and healthcare education. In addition, QR codes have proven to help secure and preserve patient records during transmissions. This paper aims to develop and analyze the implementation of QR code technology for healthcare applications. The proposed approach involves generating a unique QR code for each patient's information, facilitating data transmission between nodes such as hospitals. With its small size, the QR code provides a simple solution to transfer patient records, reducing internet capacity requirements and minimizing latency. The proposed system utilizes advanced techniques such as Diffie Hellman and logistic map for key generation and distribution, hash algorithm and Lorenz equation for key mask generation, the salting algorithm for data integrity, DNA encoding, and Huffman Algorithm for data coding. The proposed system's usability was tested with 366 patient records, and the results indicate that 99.76% of data was saved with a compression ratio of 416.8 for each patient record. Moreover, the comparative analysis demonstrated that the proposed strategy outperforms other data capacity, security, and integrity methods. Overall, the proposed system can revolutionize data transmission and security in the healthcare sector, ensuring the safety and confidentiality of patient records.

Keywords

QR-Codes; Huffman Coding; Quick Response Codes; Patient Records; DNA Coding; Chaos Systems

Creative Commons License



This work is licensed under a [Creative Commons Attribution-Noncommercial-No Derivative Works 4.0 License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

RESEARCH PAPER

Secure QR-Code Generation in Healthcare

Safa S. Abdul-Jabbar ^{a,b,*}, Alaa K. Farhan ^b

^a Computer Science Department, College of Science for Women, University of Baghdad, Baghdad, Iraq

^b Computer Science Department, University of Technology, Baghdad, Iraq

Abstract

QR codes have become ubiquitous across several industries, including e-commerce, education, and healthcare. In the healthcare sector, QR codes are increasingly used to relay essential information regarding medical products, patient history, and healthcare education. In addition, QR codes have proven to help secure and preserve patient records during transmissions. This paper aims to develop and analyze the implementation of QR code technology for healthcare applications. The proposed approach involves generating a unique QR code for each patient's information, facilitating data transmission between nodes such as hospitals. With its small size, the QR code provides a simple solution to transfer patient records, reducing internet capacity requirements and minimizing latency. The proposed system utilizes advanced techniques such as Diffie Hellman and logistic map for key generation and distribution, hash algorithm and Lorenz equation for key mask generation, the salting algorithm for data integrity, DNA encoding, and Huffman Algorithm for data coding. The proposed system's usability was tested with 366 patient records, and the results indicate that 99.76% of data was saved with a compression ratio of 416.8 for each patient record. Moreover, the comparative analysis demonstrated that the proposed strategy outperforms other data capacity, security, and integrity methods. Overall, the proposed system can revolutionize data transmission and security in the healthcare sector, ensuring the safety and confidentiality of patient records.

Keywords: QR-Codes, Huffman coding, Quick response codes, Patient records, DNA Coding, Chaos systems

1. Introduction

The Quick Response (QR) code is a 2D barcode allowing quick and easy access to encoded data [1]. QR Codes became widely used because they are simple to scan, provide robust error correction, and can be read from any direction [2]. Therefore, QR Codes are used in various fields, such as data transfer, product marketing, medical, transport ticketing, and attendance systems [3–5]. Additionally, QR Codes have several applications in many healthcare environments, such as storing case histories in facial imaging, safer medication administration, and assisting with patient instructions [6–8]. These applications can utilize several intelligent techniques used in smart design [9,10]. Although working with QR Codes has many benefits, one of the main drawbacks is that modern QR Codes still have a relatively limited data

capacity, which limits their widespread use [11]. QR Codes are matrix-based symbols with a square cell structure used to store information, and they contain functioning layouts for simple reading [12]. The main structure of the QR Code consists of five main components (Alignment Pattern, Timing Pattern, Quiet Zone, and QR Data) [13,14].

Several papers have been published to enhance and use QR Codes in various sectors. For example, Lin and Chen developed new QR barcodes that allowed them to create a secret hiding technique for QR barcodes, which allowed for a larger payload than previous versions. A regular scanner can only read formal information from a tagged QR Code, which a browser can disclose. Therefore, private information can be unmasked if a trusted party scans a tagged QR Tag [15]. Furthermore, they took advantage of built-in QR codes that can use pattern recognition and polynomial secret-sharing

Received 6 November 2022; revised 9 March 2023; accepted 15 March 2023.
Available online 10 May 2023

* Corresponding author.
E-mail address: safa.s@cs.w.uobaghdad.edu.iq (S.S. Abdul-Jabbar).

<https://doi.org/10.33640/2405-609X.3294>

2405-609X/© 2023 University of Kerbala. This is an open access article under the CC-BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

algorithms to provide a secure method of exchanging secret information between parties. Many achievements were presented, such as QR Codes can be viewed using any QR Reader and safely transmit confidential data over a public channel while storing it securely [1].

On the other hand, authentication information (i.e., encrypted message contents and signatures) can be embedded in the QR Code's design to create a secure authentication system. Therefore, the authorized user can check the QR Code's legitimacy without an internet connection. The suggested approach has been proven safe through evaluation against attacks that modify the barcode's data and offers a significantly larger embedding capacity than the existing data hiding scheme at the same error correction level [3]. Another scheme was presented using encrypted lossless compression technology as an innovative way to enhance the data storage of a QR Code. This scheme uses the Huffman algorithm and XOR operation to provide secure message transfer and authenticate documents [16]. Tikhonov also proposed a revolutionary method in 2019 for creating double-sided QR Codes, which might convey specific information, whether shown in a straight or mirrored orientation, using a brute-force method and an analytic solution [2]. Another method was suggested using a new QR Code with private and public clouds for storing confidential messages transmission [17]. Furthermore, several papers illustrate the challenges and issues faced when using QR Codes, such as [18,19]. Therefore, the main contributions of this paper can be summarized as follows.

1. Develop a suitable configuration for the key mask generation algorithm based on a Chaos Theorem to provide a good security level.
2. Using the salting algorithm to achieve data integrity.
3. Finally, we used the Huffman and DNA algorithms to compress the data size to address the capacity issue faced in QR Code-generating operations.

This paper is structured as follows: Section 2 introduces the research methodologies, while Section 3 presents compelling results and discussions that inform researchers of what they can learn from this research. Finally, Section 4 draws the conclusions that can be made from this research.

2. Research methodology

This section outlines the steps to implement the proposed system goals. First, we describe the overall system architecture, which includes the transmission

scenario and system components. Next, we provide a detailed explanation of the QR Code generating process. Finally, we apply various evaluation measures to test and analyze the validity of the proposed system.

2.1. System design strategies

The proposed QR Code systems can be used by healthcare providers, patients, and authorities across all nodes to speed up data processing and transfer while providing data security and integrity services. The patient's record can be transmitted using QR codes and adopting blockchain behaviour, ensuring its safety during transfer by including the location of QR creation and the hash value of all data. Additionally, all QR data is encrypted to ensure data security during transmission.

2.1.1. QR codes transmission scenario

A QR Code is generated for each patient record. As mentioned, this QR code contains patient data and a hash value encrypted with a value derived from the secret key. These keys are exchanged at the beginning of communication between two sites or when the secret key exchange is needed. Therefore, the scenario of generating and exchanging the QR Codes between two sides (e.g., A and B) can be described as follows:

Compute the shared public key using Diffie-Hellman as the other party's public key (PK) and return the computed shared secret key (K). K is a seed value for generating QR Code Key.

In node A:

1. Use the Salting algorithm to produce a unique hash value for the patient record data and link this data to the original data. (Note: using the Id Node Validation (K) and date as a salt value(s)).
2. Generate a key mask (KMSK) used for data encryption.
3. Use the proposed QR Code generation algorithm steps to construct the QR Code.
4. Node A sends the QR Codes for all patient records to node B.

In node B:

1. Receive the QR codes.
2. Use the Salting algorithm to produce a unique hash value for the patient record data. This step is done if the QR Code is used for data integrity, so the patient's data are sent with QR Codes (Note: using MAC and secret key as salt value(s)).

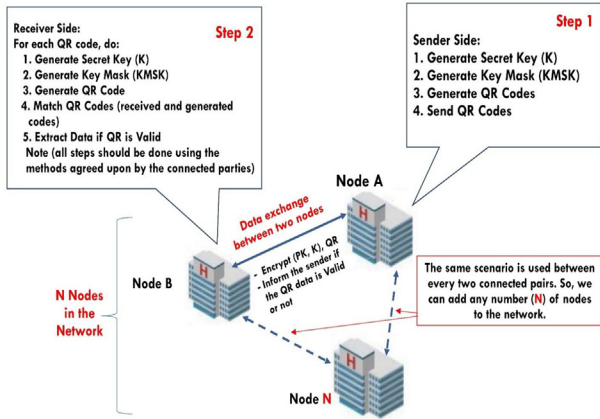


Fig. 1. The QR Code transmission scenario (using a local or global network).

3. Generate a key mask (KMSK) for decryption depending on a secret key.
4. Use the proposed algorithm steps shown in Fig. 5. Firstly, deconstruct the QR Code, then split the result (hash + patient data). Finally, decrypt the patient data part to produce the patient record data.
5. Match the resulting hash value from steps 2 & 4. If it's equal, then the data is valid. (Note: in this case, QR Codes are used to reduce required internet capacity, data security, and integrity purposes.)

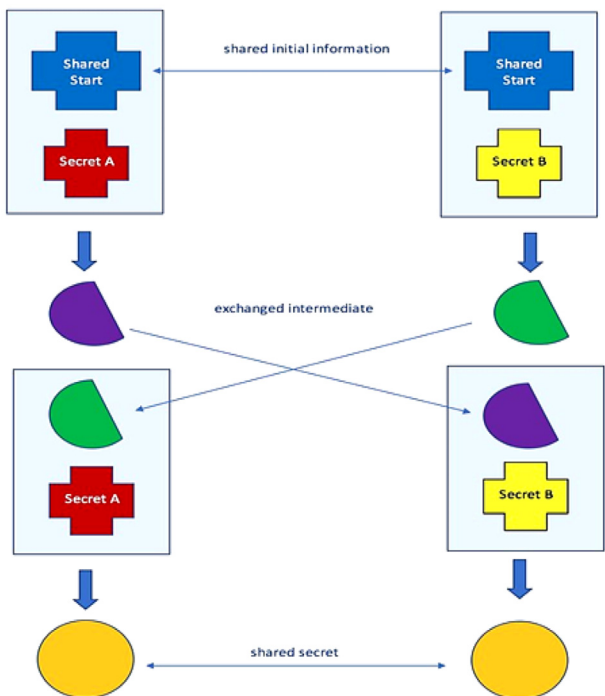


Fig. 2. The Diffie Hellman key exchange protocol [21].

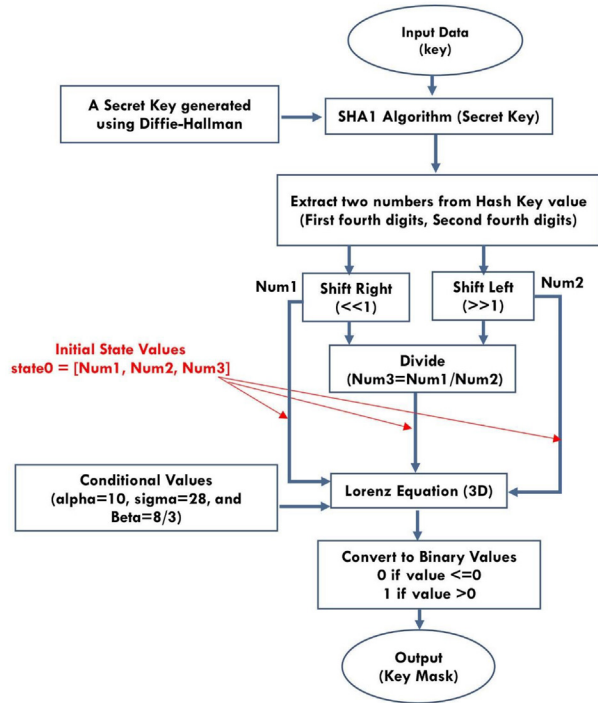


Fig. 3. Key mask generation based on Lorenz equation.

6. Check if the patient records data (if sent with QR) equals the data from step 4. The data is correct, and no transmission error has occurred. (Note: QR Codes are used for data transmission error correction and integrity.)

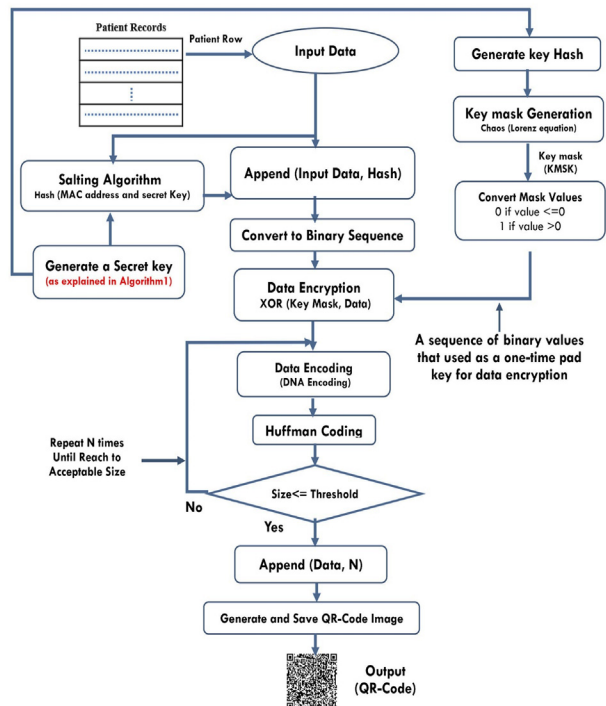


Fig. 4. QR-Code construction system.

As a summary of the transmission scenario, Fig. 1 illustrates the mechanism for sending and receiving QR Code data and required keys between nodes.

2.1.2. Key management protocol

When sharing data between two nodes via QR Codes, generating a secret key that can serve as a seed for key mask generation and an identifier for the two nodes in the salting algorithm is necessary.

- Secret Key Exchange

A secret key must be shared before any process in a symmetric cypher can occur, but the connection is made over insecure communication channels. The Diffie-Hellman algorithm [20] can solve this problem, as illustrated in Fig. 2.

Therefore, the secret key used for key distribution and QR-Key generation is based on the logistic map and Diffie Hellman secret key using the following steps (Algorithm 1):

The secret key serves as the seed for generating Q-Key, which produces a two-dimensional encryption key mask for encrypting the data in the QR. Chaos theory has opened up new and promising avenues for developing secure encryption solutions and is a widely researched area [22,23]. This paper proposes a high level of protection through a

mechanism that relies on 3D Chaos theory, specifically the Lorenz Equation, as outlined in the figure below [24,25]. The equation uses three conditional data values, alpha (10), sigma (28), and beta (8/3), documented in [26,27]. The resulting key mask is then converted into a one-dimensional array of binary values (0 or 1) to encrypt the data, following the same principle as a one-time pad. The most significant advantage of this technique is that a long key does not need to be shared each time data is exchanged since the key mask is quickly generated at each node and relies on a single seed. This feature makes breaking or guessing the key mask values difficult, ensuring the security and confidentiality of the encrypted data. Fig. 3 shows the general structure of the key mask generation algorithm.

2.2. QR code construction

This section provided a complete description of producing QR-Codes as the final result. This operation consists of several steps, including Data Selection (Extraction), the Salting Algorithm, Data Appending, Conversion to Binary, Data Encryption, Data Encoding (DNA algorithm), Data Compression (Huffman Algorithm), and Generating the QR image as shown in Fig. 4.

Step 1: Current and Next nodes get public numbers P, G

Step 2: Current node selected a private key (a), and the Next node selected a private key (b).

Step 3: Current and Next nodes compute shared values as follows:

$$\text{Current Node: } X = G^a \text{ mod } P$$

$$\text{Next Node: } Y = G^b \text{ mod } P$$

Step 4: Current and next nodes exchange public numbers

Step 5: Current node receives the public key (Y), and the Next node receives the public key (X)

Step 6: The current and Next nodes compute their symmetric keys as follows:

$$\text{Current Node: } Kc = Y^a \text{ mod } P$$

$$\text{Next Node: } Kn = X^b \text{ mod } P$$

Step 7: Determine the Shared Secret Key.

Step 8: In the Current Node, Do the Following

-Use the Secret Key as a seed for the Logistic Map

-Generate Key (each node must have the same Logistics)

- Generating Q-Key

Using a Chaos system (Logistic map equation) to produce a unique key (Q-Key) for the creation of the QR is derived from the secret key to achieve a high level of security instead of relying on the secret key directly [22]. Step7 and Step 8 in the previous algorithm.

- Key mask Generation based on the Chaos system and Q-Key

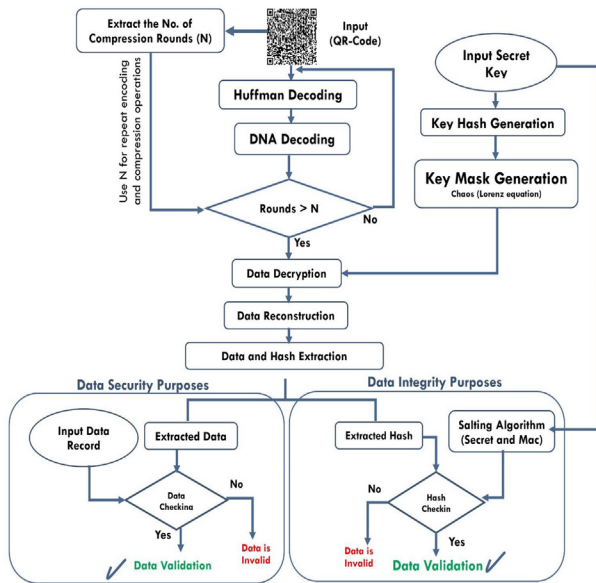


Fig. 5. QR-Code de-Construction system.

• Salting Algorithm

Hashing algorithms are commonly used to encrypt and generate a unique value for plaintext, thereby increasing the strength of the code by authenticating the hash code [28]. Salting the hash value is a technique that makes the resulting value more secure and unique. Therefore, this paper uses a secure salted hashing algorithm (SHA-256) to encrypt each patient record. The algorithm converts the input record data into a complex combination of 64 random numbers and letters, representing unique features for that record [29]. To leverage the benefits of Blockchain technology, the resulting value is attached to the data record and included in the QR Code, ensuring the integrity of the patient records. This method utilizes the secret key proposed in this paper and the current node's MAC number. By salting the hashing value and utilizing Blockchain, the security and confidentiality of the patient records are ensured.

• DNA Coding System

DNA is a coding technique commonly used for text and image coding inspired by DNA molecules [30,31]. This paper uses the DNA coding system consisting of 4 genes (A, G, C, T) for (00, 01, 10, 11), respectively. This step serves two purposes. The first purpose is to encrypt data to provide additional security for the patient's record. The second purpose is to reduce the data size to half its original size.

• Huffman Compression Algorithm

In the healthcare sector, patient data is precious, so any loss of it is usually unacceptable. Therefore, only lossless algorithms are acceptable in this step because this data contains essential medical information. In this paper, we used the Huffman coding algorithm to perform a statistical-based compression algorithm that can achieve high compression ratios [32,33]. The main steps of this algorithm can be described as follows.

1. Initiate a priority queue 'P' consisting of unique characters.
2. Sort the priority queue according to the ascending order of frequencies.
3. For all the unique characters inside the queue:
 - Initialize a new Node '0'.
 - Return the minimum value of P and assign it to the left child of '0'.
 - Return the next minimum value of P and assign it to the right child of '0'.
 - Find the sum of both returned values and assign it as the value of '0'.
 - Insert the value of '0' into the tree.
4. Repeat the same process until all unique characters of 'P' are visited.
5. Return the root node.

2.3. Generate QR-code image

Finally, the Python QR Code library "qrcode" can create QR Code images. This paper uses the Huffman result as input to the QR maker. This function adds the data in a specific structure that enables any QR Code reader to read the embedded data (encrypted and compressed data).

2.4. QR code deconstruction

In this section, the second node sent and received the QR code. Firstly, the number of compressions should be extracted from the QR code data when the node receives the QR code. Then, this node should use the secret key to generate the Q-Key to apply the salting algorithm. Next, using the Q-key, the key-Mask must be generated using the same method as on the sender node side. Finally, depending on the extracted compression rounds number, the data is decompressed using the same DNA coding technique and Huffman algorithm.

As a result, the patient data record and the hash value of this record were provided at this stage. Next, the validation of these data must be considered by comparing the result of the salting algorithm applied to the data record if it is available (in

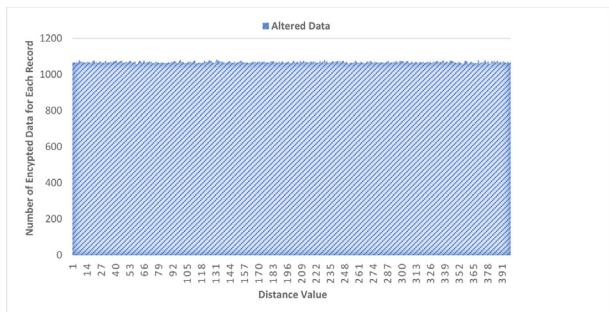


Fig. 6. Hamming distance between the original and encrypted data for each record.

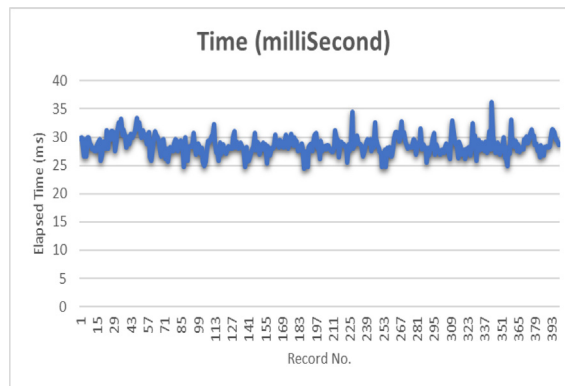


Fig. 7. The elapsed time for each record.

Table 1. The Compression ratio and space saving with and without using DNA for one round.

Compression Method	Compression Ratio	Space Saving
Huffman & DNA	11.85	91.56%
Only Huffman	8	87.5%

this case, the QR code used for data integrity purposes). All these steps are illustrated in Fig. 5.

3. Results and discussion

To test the efficiency of the encryption Key-Mask generated using the hash algorithm (SHA1) and Lorenz equation, the Hamming Distance metric was used to measure the distance between the original and encrypted data. Fig. 6 illustrates the number of altered bits for each patient data record. As we can see, the encrypted data for each record constitutes about 81–83% of the overall data for each record.

Next, compression ratios (CR) and space savings measurements were taken with and without DNA. It was determined that the proposed method provided better results when using DNA techniques in addition to the Huffman Algorithm (as shown in Table 1). This is because the data for each row and its hash value is around 10,368 bits when using only

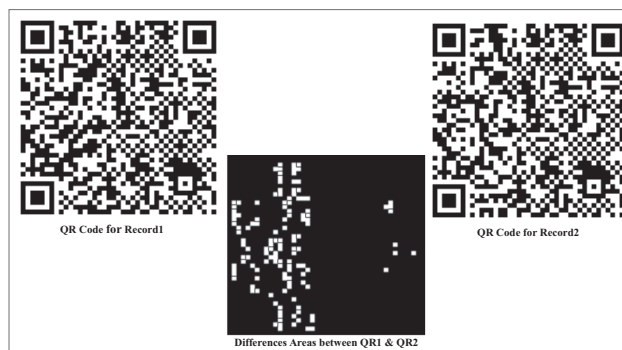


Fig. 8. The QR Codes of two consecutive records and their different areas.

Table 3. Different metrics are used to measure the differences between two different records.

Metric	Value
Root-Mean-Square Difference	79.90
Different percentage	5.48
Is_equal	False

the standard Huffman Algorithm. In comparison, the result when using the Huffman algorithm on DNA-coded data is equal to 6998 bits for one round

Table 2. One patient record details as an example of compression and DNA coding operations.

Symbols	Round Number	Probabilities	Space usage before compression (in bits)	Space usage after compression (in bits)
symbols: dict_keys(['A', 'T', 'G'])	Round 1	dict_values([3370, 1296, 518])	82,944	6998
	Round 2	dict_values([2291, 875, 333])	6998	4707
	Round 3	dict_values([1533, 589, 232])	4707	3175
	Round 4	dict_values([1036, 397, 155])	3175	2140
	Round 5	dict_values([697, 268, 105])	2140	1443
	Round 6	dict_values([471, 181, 70])	1443	973
	Round 7	dict_values([319, 122, 46])	973	655
	Round 8	dict_values([215, 82, 31])	655	441
	Round 9	dict_values([146, 55, 20])	441	296
	Round 10	dict_values([97, 37, 14])	296	199

without losing data. Therefore, the final result for our proposed algorithm is a compression ratio of 99.41% and a space-saving of 99.76%.

For example, the DNA data in the testing dataset illustrates the impact of applying the DNA algorithm each time the Huffman algorithm is used (note that in this example, the compression process was carried out ten times, or ten rounds), as shown in Table 2.

Each patient record waiting time (elapsed time) for all rounds was measured, as shown in Fig. 7. In this figure, the time was measured in milliseconds for each record, and the Minimum waiting time in the overall tested dataset was (24.424 ms) whereas the Maximum value was (36.125 ms).

To further evaluate the efficiency of the proposed system, we compared two consecutive QR Code images to measure the similarity of consecutive patient record data. An example was taken for the first and second records, and the results are shown in Fig. 8 and Table 3.

Space and time savings are measured and documented as CR. The CR is the proportion between the uncompressed and compressed file sizes [32], as shown in Equation (1). Therefore, a compression ratio value can be defined as follows: CR = 1 indicates no compression, CR > 1 is the desired value, and CR < 1 is a failure.

$$\text{Compression Ratio} = \frac{\text{Uncompressed Size}}{\text{Compressed Size}} \tag{1}$$

On the other hand, the amount of storage space saved after compression is the space savings [34], as shown in Equation (2).

$$\text{Space Saving} = 1 - \frac{\text{Compressed Size}}{\text{Uncompressed Size}} * 100\% \tag{2}$$

Because of the importance of healthcare data, it is worth mentioning that we combine Huffman with DNA coding to compress data in this research. This hybrid technique will provide a good compression ratio, and it is considered a lossless compression technique, so there is no data loss or errors in the data recovery process. Table 4 shows the result for the proposed method when applied to an ordinary text file (English language text data) compared with Shah's proposed method in 2019 [32].




For example.

- The origin data record before compression: [00-2208-2503-3640 null null 7.3 30.1 24.2 35.3 null null 10 43.2 6.7 50.1 4.3 0.7 5 2.77 87.7 26.3 11.4189 9.2 22.3]
- The original message after adding salt values: [00-2208-2503-3640 null null 7.3 30.1 24.2 35.3 null null null 10 43.2 6.7 50.1 4.3 0.7 5 2.77 87.7 26.3 11.4189 9.2 22.3,99bb826d861fab84edea58f07c739827058d114a]
- The compressed data: binary sequence consists of 4821 characters (0 or 1).

Table 4. The Compression ratio and space-saving between [31] and the proposed method.

Uncompressed Data (Bytes)	Method	compressed Data	Uncompressed Data (Bytes)	Method
3721	Improvised GZIP[9]	1888	1.970	49.26
	The Proposed Scheme	240	8569.6	99.9
11,150	Improvised GZIP[9]	5754.625	1.937	48.39
	The Proposed Scheme	208	25868.3	99.9

Table 5. Compare the QR Code results from the proposed system with [16].

Data Size in bits 83,846	Methods	Method1	Method2	Method3	Method4	Proposed Method
	CR	25	32	48	64	416
	Hash value	'0EFDD7C	Hash value	'0EFDD7C	Hash value	'0EFDD7C
	Hash length	23	32	46	64	40
	Average of execution time (second)	1.5719	1.5762	1.5725	1.6200	0.0297
	QR Code					

- The recovered data record after decompression and extracting the salting values: [00-2208-2503-3640 null null 7.3 30.1 24.2 35.3 null null null 10 43.2 6.7 50.1 4.3 0.7 5 2.77 87.7 26.3 11.4189 9.2 22.3]

Furthermore, we compared the results of our proposed system with the four different methods presented by Ali and Farhan [16], as shown in Table 5. It is important to note that the previously published paper only provided QR Codes for the hash value. In contrast, in our proposed system, the QR Codes are generated for the data and its corresponding hash value.

4. Conclusions

This paper presents and evaluates a novel method for generating QR codes. The results of the proposed system have demonstrated several advantages, including.

1. Ensuring the integrity of patient data by using a salting algorithm to provide the hash value that depends on the MAC and the secret key to work in behavioural blockchain technology.
2. The hash algorithm (SHA1) and 3D Lorenz equation provide a key with random values that depend on the secret key as a seed. This helps authorized nodes generate the same random numbers and use them to work as the one-time pad keys, overcoming the disadvantage of the one-time pad (key generation and distribution). However, this makes breaking or obtaining the key difficult or almost impossible due to the nature of Chaos Systems. As a result of using this key mask in each record data, about 81–83% of this data will be encrypted.
3. A simple modification is made to the Diffie-Hellman algorithm used to distribute the keys between nodes. This modification uses the logistic map equation to generate a value from each node's secret key, making it difficult for the hacker even if it somehow obtains the secret key because it was not used directly. However, it is used as a seed for the logistic map equation.
4. Using DNA coding to encode data improves results by 4% compared to the standard Huffman algorithm.
5. Applying the Huffman algorithm dynamically at both ends of compression and decompression with space saving equal to 99.97% for each record data. It is worth mentioning that the amount of data is not limited to a fixed number of bits

because the compression is dynamic until the data volume reaches a determined threshold.

6. Reducing the time of QR generation by using simple operations that can be done faster. The maximum waiting time is about 36.125 ms.

As a result, this paper intends to provide a novel system that uses the behaviour of Blockchain technology to exchange patient history between various nodes by applying different algorithms and technologies.

This research is a valuable reference for future studies aiming to revolutionize how healthcare records are stored and processed. In particular, it suggests an initial step for converting traditional digital patient records, such as those saved in an Excel file, into QR codes. As a more advanced step, researchers could expand upon this idea by including all types of data, including images and signals.

To enhance the proposed approach, it is recommended to explore the integration of additional computational intelligence algorithms, such as Monarch Butterfly Optimization (MBO) [35], Slime Mould Algorithm (SMA) [36], and Elephant Herding Optimization (EHO) [37]. These algorithms have demonstrated their effectiveness in addressing complex optimization problems. Therefore, incorporating them into the proposed approach could produce a more robust system for processing and analyzing healthcare records.

Furthermore, all algorithms used in this study could be evaluated for their efficacy in handling different types of medical data and compared with the current performance. Additionally, it would be beneficial to investigate the use of other learning techniques, such as deep learning or reinforcement learning, in the proposed approach to improve its performance in dealing with more complex medical data.

A more sophisticated system could be developed by optimizing the proposed approach, which offers greater accuracy and efficiency in processing and analyzing healthcare records, ultimately leading to better healthcare outcomes. Overall, this research provides an important foundation for future work in this area and opens up exciting new possibilities for improving healthcare services.

Conflict of interest

The authors declare no conflict of interest.

Acknowledgements

We appreciate the University of Technology staff for providing the support necessary for us to finish this research.

References

- [1] S. Liu, Z. Fu, B. Yu, A two-level QR code scheme based on polynomial secret sharing, *Multimed. Tool. Appl.* 78 (2019) 21291–21308, <https://doi.org/10.1007/s11042-019-7455-1>.
- [2] A. Tikhonov, On double-sided QR-codes, arXiv preprint arXiv, 2019, 1902.05722, <http://arxiv.org/abs/1902.05722>.
- [3] C. Chen, QR code authentication with embedded message authentication code, *Mobile Network. Appl.* 22 (2017) 383–394, <https://doi.org/10.1007/s11036-016-0772-y>.
- [4] M. Baban, Attendance Checking system using quick Response code for students at the University of Sulaimaniyah, *J. Math. Comput. Sci.* 10 (2014) 189–198.
- [5] D. Sharma, A review of QR code structure for encryption and decryption process, *Int. J. Innova. Sci. Resea. Technol.* 2 (2017) 13–18.
- [6] C.T. Karia, A. Hughes, S. Carr, Uses of quick response codes in healthcare education: a scoping review, *BMC Med. Educ.* 19 (2019) 1–14, <https://doi.org/10.1186/s12909-019-1876-4>.
- [7] M. Shakil, D. Karteek, K. Spoorti, M. Jose, Quick response code in oral and maxillofacial radiology, *J. Oral Maxillofac. Rad.* 2 (2014) 95, <https://doi.org/10.4103/2321-3841.144696>.
- [8] J. Mira, M. Guilbert, I. Carrillo, C. Fernández, M.A. Vicente, D. Orozco-Beltrán, V.F. Gil-Guillen, Use of QR and EAN-13 codes by older patients taking multiple medications for a safer use of medication, *Int. J. Med. Inf.* 84 (2015) 406–412, <https://doi.org/10.1016/j.ijmedinf.2015.02.001>.
- [9] A.T. Gough, G. Fieraru, P.A.V. Gaffney, M. Butler, R.J. Kincaid, R.G. Middleton, A novel use of QR code stickers after orthopaedic cast application, *Ann. R. Coll. Surg. Engl.* 99 (2017) 476–478, <https://doi.org/10.1308/rcsann.2017.0070>.
- [10] S.K. Das, Smart Design and its Applications: Challenges and Techniques, Part of the Springer Tracts in Nature-Inspired Computing Book Series (STNIC), 2021.
- [11] C. Li, P. Hu, W. Lau, AuthPaper: protecting paper-based documents and credentials using Authenticated 2D barcodes, in: 2015 IEEE International Conference on Communications (ICC), 2015, pp. 7400–7406, <https://doi.org/10.1109/ICC.2015.7249509>.
- [12] V. Uzun, B. Sami, Evaluation and implementation of QR code identity Tag system for healthcare in Turkey, *Springer Plus* 5 (2016) 1–24.
- [13] I. Jelic, D. Vrkic, QR codes in library - does anyone use them?, 6th international convention on information and communication technology, electronics and microelectronics (MIPRO), IEEE (2013) 695–699.
- [14] O. Hugues, P. Fuchs, O. Nannipieri, New augmented reality taxonomy: technologies and features of augmented environment, in: *Handbook of Augmented Reality*, Springer, New York, 2011.
- [15] P.Y. Lin, Y.H. Chen, High payload secret hiding technology for QR codes 1, *EURASIP Journal on Image and Video Processing*, 2017, pp. 1–8, <https://doi.org/10.1186/s13640-016-0155-0>.
- [16] A. Ali, A.K. Farhan, Enhancement of QR code Capacity by encrypted lossless compression technology for verification of secure E-Document, *IEEE Access* 8 (2020) 27448–27458, <https://doi.org/10.1109/ACCESS.2020.2971779>.
- [17] U.K. Jannat, M.M. Kumar, S.A. Islam, Cloud based QR code for confidential message, *Int. J. Eng. Technol. Manag. Sci.* 6 (2022) 55–58, <https://doi.org/10.46647/ijetms.2022.v06i03.010>.
- [18] G. Amoah, J. Hayfron-Acquah, QR Code security: mitigating the issue of quishing (QR Code Phishing), *Int. J. Comput. Appl.* 975 (2022) 8887.
- [19] V. Kulkarni, R. Banegaon, Interactive QR code based online shopping system, *I. J. Innov. Eng. Res. Technol.* 7 (2021) 31–37.
- [20] N. Li, Research on diffie-hellman key exchange protocol 4, 2010 2nd International Conference on Computer Engineering and Technology, 2010, pp. V4–V634, <https://doi.org/10.1109/ICCET.2010.5485276>.
- [21] C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, J. Johnson, Cyber security primer for DER vendors aggregators and grid operators, *Tech. Rep.* 12 (2017) 3–62.
- [22] V.V. Tarasova, V.E. Tarasov, Logistic map with memory from economic model, *Chaos, Solit. Fractals* 95 (2017) 84–91, <https://doi.org/10.1016/j.chaos.2016.12.012>.
- [23] S.A. Fadhil, A.K. Farhan, Color visual cryptography based on three dimensional chaotic map 22, *Iraqi Journal of Computers, Communications, Control and Systems Engineering*, 2022, pp. 1–12.
- [24] É. Ghys, The Lorenz Attractor, a Paradigm for Chaos. Part of the Progress in Mathematical Physics Book Series vol. 66, 2013, pp. 1–54. Birkhäuser, Basel.
- [25] N.A. Ali, A.M.S. Rahma, S.H. Shaker, 3D textured model encryption using 2D logistic and 3D Lorenz chaotic map, *Iraqi Journal of Computers, Communications, Control and Systems Engineering* 21 (2021) 90–103.
- [26] S. Abid, S. Saad, A. Yaseen, Proposed neural network with FFT transfer function to estimate Loran Dynamical Map, *Adv. Comput.* 9 (2019) 1–20.
- [27] N.A. Ali, A.M.S. Rahma, S.H. Shaker, Multi-level encryption for 3D mesh model based on 3D Lorenz chaotic map and random number generator, *Int. J. Electr. Comput. Eng.* 12 (2022) 2088–8708, <https://doi.org/10.11591/ijece.v12i6.pp6486-6495>.
- [28] S.H. Shaker, HMAC modification using new random key generator 14, *Iraqi Journal of Computers, Communications, Control and Systems Engineering*, 2014, pp. 72–82.
- [29] A. Al Farawn, H.D. Rjeib, N.S. Ali, B. Al-Sadawi, Secured e-payment system based on automated authentication data and iterated salted hash algorithm 18, *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 2020, pp. 538–544, <https://doi.org/10.12928/TELKOMNIKA.V18i1.15623>.
- [30] X. Wang, Y. Su, An Audio encryption algorithm based on DNA coding and chaotic system, *IEEE Access* 8 (2020) 9260–9270, <https://doi.org/10.1109/ACCESS.2019.2963329>.
- [31] X. Xue, Z. Dongsheng, Z. Changjun, New insights into the existing image encryption algorithms based on DNA coding, *PLoS One* 15 (2020) 1–31.
- [32] A. Shah, M. Sethi, The improvised gzip, A technique for real time lossless data compression 6, *EAI Endorsed Transactions on Context-Aware Systems and Applications*, 2019, <https://doi.org/10.4108/eai.1-10-2019.160599>.
- [33] S. Zhang, S. Jichen, C. Shengkang, Constrained Optimal Querying: Huffman Coding and beyond, 2022, pp. 1–18, arXiv preprint arXiv:2210.04013.
- [34] S. Kodituwakku, U. Amarasinghe, Comparison Study of lossless data compression algorithms for text data, *IOSR J. Comput. Eng.* 11 (2013) 15–19, <https://doi.org/10.9790/0661-1161519>.
- [35] N. Bacanin, T. Bezdan, E. Tuba, I. Strumberger, M. Tuba, Monarch butterfly optimization based convolutional neural network design, *Mathematics* 8 (2020) 936.
- [36] Y. Wei, Z. Othman, K.M. Daud, S. Yin, Q. Luo, Y. Zhou, Equilibrium optimizer and Slime Mould algorithm with variable neighborhood search for job shop scheduling problem, *Mathematics* 10 (2022) 4063.
- [37] J. Li, H. Lei, A.H. Alavi, G.G. Wang, Elephant herding optimization: variants, hybrids, and applications, *Mathematics* 8 (2020) 1415.