Dynamic QR Codes: A Solution for Secure Mobile Payments

Dr. Om Prakash YADAV, Ankit KUMAR, Kalash SHANDILYA, Shubhankar KUMAR
School of Computer science and Engineering, Lovely Professional University, Jalandhar India
om.26121@lpu.co.in, kumarankityadav88777@gmail.com, kalashshandilya@gmail.com, shubhankar.kr24@gmail.com

Abstract

Black and white barcodes have been employed recently to encode additional data inside of a designated area. A barcode is composed of gaps and bars that are ordered according to preset rules. However, as the demand for additional data storage increases, a new technology known as QR codes has been developed. However, security remains a major worry, so this is by no means the end. Mobile payment is necessary for mobile business. An easy-to-use mobile payment solution is needed to allow mobile users to execute transactions using their mobile devices in a reliable and safe manner. The purpose of this study is to give us dynamic QR code refreshes during financial payment. The paper's primary goal is to create and comprehend QR code technology in the context of today's global security environment.

Index terms: Barcode, QR Code, Dynamic QR, Payment, Scanner, SM2 and SM3

1. Introduction

Masahiro Hara created the two-dimensional QR Code i.e, quick response in Japan in 1994, during working in Denso Wave (the Japanese company). Compared to a conventional bar code, information can be stored up to several hundred times more efficiently because it is encoded in both the vertical and horizontal directions (Figure 1). To retrieve data, we can click picture of the code with a camera lens (like with the help of smartphone) and use a QR scanner to process the picture.

This is often caused by the fact that a QR code can include up to 7,089 characters, while a standard barcode can only contain 20 digits. This, together with the flexibility and diversity they provide, makes using QR Codes far more appealing than using barcodes. According to statistics, a QR code may hold the same amount of information as a standard bar code in about ten times less space.

One fantastic thing about QR Codes is that they can be read regardless of where they are, therefore scanning them from a specific angle is not necessary. Because there are three distinct squares in a QR code, scanners can identify the right way to decode the image. QR codes are being used for many different purposes, such as advertising, tickets for events, mobile payments, and product information. Because they facilitate contact tracing and provide access to immunization records, they are becoming an essential tool in the fight against COVID-19 [7].

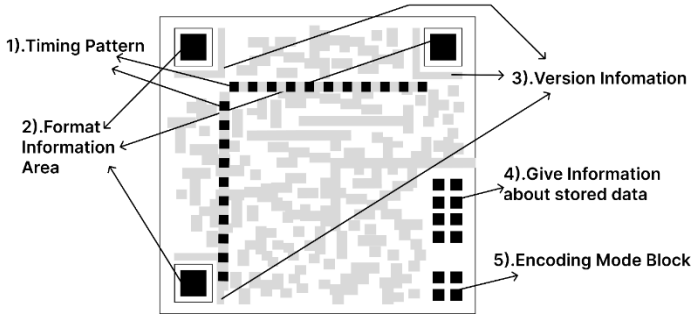

Fig. 1. QR Code Structure

Structure of QR Code:

1. Timing Pattern: The QR code is crossed both vertically and horizontally by these tiny black and white lines. They help the QR code's size and shape so that scanners can read it.

2. Format details: This section contains information about the data mask pattern and error correction level applied to the QR code. Two identical QR codes are present in the error correcting keys. It is also in charge of hiding patterns. Encrypting data can only happen here.

3. Version Information: This element, which is present in larger QR codes, describes the size of the QR code (number of modules on each side).

4. Provide details about the data that has been saved. The block up to which the data has been saved is mentioned.

5. Block for Encoding Mode: QR codes employ a variety of encoding schemes to effectively represent this data. Every style is appropriate for particular character sets. The kinds of data that are stored in that QR Code are identified by the scanner are:

a. Numerical (for 0-9 numbers)

b. Alphanumeric (for some symbols, numbers, and capital letters)

c. Binary (For any binary data)

d. Kanji (characters used in Japanese).

QR codes are used in many real-world scenarios, including advertising, mobile payments, e-ticketing, warehousing and healthcare, business applications, mobile tagging, and commercial tracking [8], [9], [10]. Apart from these applications, URL encoding is another common use for QR codes [11]. Therefore, the most popular method of sending URLs from billboards to smartphones is now the QR code [12].

2. Literature Review

By utilizing cryptographic methods, we can implement a dynamic system for QR code payments as introduced by the authors in their work [4]. These methods play a crucial role in enabling instant generation of dynamic QR codes, ensuring enhanced security measures in the process.

The authors [5] introduced a new way to secure e-transaction technique using dynamic QR codes. Each order's QR code has two layers: the first layer includes payment information, while the second layer employs SET for encryption. This two-layer approach enhances security by reducing exposure to online threats.

The primary concerns are security and data privacy from attacker. Monitoring the data exchanged between the QR code reader app and its web service using HTTP(S) interception allows for better understanding of the communication process [1]. So, with the help of this we can only discovered that most of the apps seriously infringed users' privacy by sending private information to a malicious website and other parties, in addition to redirecting users to another page because they were unable to recognize malicious QR codes. Therefore, we can leverage the concept of a dynamic

QR code to protect user information and prevent other attackers from stealing money during a purchase. With the help of this user can be able to change the existing QR code by their own through refresh button on the same transaction page.

The authors [6] suggest that dynamic QR code payment systems offer improved security and address the limitations of static QR codes. This literature review highlights the use of cryptographic techniques to generate real-time dynamic QR codes that are both unique and random. When compared to other algorithms, this system excels in payment processing and meets expected security measures.

The main purpose of this study is to fill these gaps by exploring the integration of a dynamic QR code by user during payment with the help of user by clicking refresh button on the same payment page. This research seeks to address these deficiencies by investigating how users can incorporate a dynamic QR code during the payment process. Through a thorough examination of security and privacy vulnerabilities in smartphone apps, we put forward a series of design suggestions to enhance the encoding of QR codes, reader software, and website functionality. To test these suggestions, we developed a prototype app (Refer to Figure 2 & Figure 3) that prioritizes security, privacy, and user-friendliness. Our findings indicate that following our recommendations can lead to the creation of secure and user-friendly apps that are resistant to tampering during financial transactions.

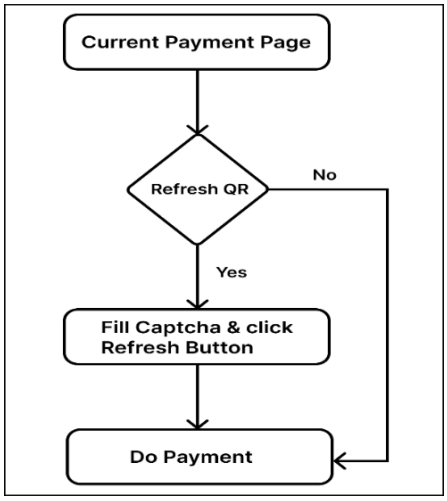

Fig. 2. Flow of payment page

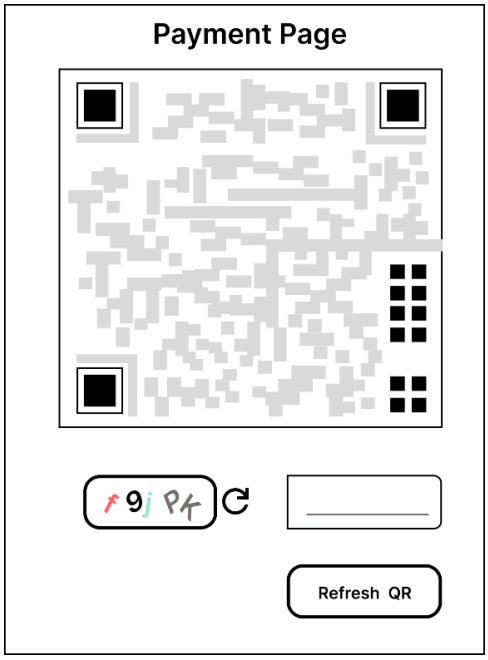

Fig. 3. Payment Page Interface

3. Methodology

As we all know, QR codes are extremely important in today's technologically advanced world for a variety of tasks. It could be a link to a profile, website, money transfer, Google registration form, photo sharing, etc. However, the primary issue throughout the content transmission process is security. Despite the numerous benefits QR codes offer, ensuring scanning security remains a significant issue. There is a large presence of static QR codes, often found in sticker or card format, which have been on the market for quite some time. These are primarily used for fund transfers or collections. However, criminals have exploited this functionality to manipulate, substitute, or obscure QR codes, resulting in the illicit appropriation of merchants' business revenue and the unauthorized access to users' personal information through clandestine methods.

So, in this research we are discuss about how we will enhance the security while generating dynamic QR code. Basically, we are going to talk about payment through QR code on the website. We do payment through QR code by scanning scanner on website. So, there can be attacker we can change the QR code. So, user is not aware about the attacker that someone change the code or not. Up until now, there has been a notion of updating the captcha code when completing forms, transferring money, etc. However, the payment page of the same website does not provide the option to refresh the QR code. Therefore, there will be a risk that an attacker will alter the QR code while the payment is being processed when we send money using a QR code. Therefore, the user won't know if the QR code has changed or not. Is the QR Code authentic or fake?

Therefore, the ability for the user to dynamically change the code after making a few small modifications on the same payment page should be provided in order to address this issue. To ensure that the QR code is updated correctly, the user can input the captcha code in the input box and then click the change button. After that, the user makes a payment so that the real recipient will be credited with the amount. Figure 3 shows an example of the steps a user would take to complete a payment. Additionally, figure 2 illustrates how the web payment interface will seem.

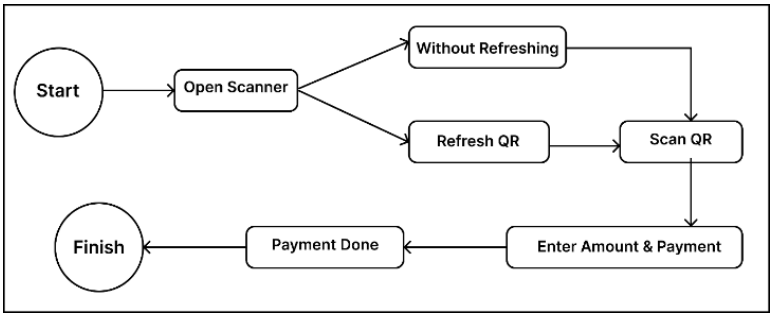

Fig. 4. Workflow of Refreshing Dynamic Code

Thus, we can utilize two-factor authentication (2FA) to update the captcha code: Although 2FA isn't a CAPTCHA in the strict sense, it does offer an extra degree of protection to the registration and payment process. Therefore, consumers receive a one-time code via SMS, email, or authenticator app after inputting their credentials or finishing a CAPTCHA challenge, which they need to enter to finish the registration/payment process. This greatly lowers the possibility of unwanted access, but it can make using the system more difficult.

A. Algorithm 1

According to the Chinese National Cryptography Standard, the SM2 method is a cryptographic technique that makes use of elliptic curve cryptography (ECC) for digital signature and asymmetric encryption.

SM2 public-private key pair generation algorithm

Creating SM2 Public-Private Key Pair Algorithm:

Input: Elliptic Curve Parameters (p, E(Fp), P, n)

Output: Public Key (Q) and Private Key (d)

- Step 1: Choose a private key (d) randomly within the range [1, n - 1].

- Step 2: Compute the public key (Q) using the formula Q=d×P, where P represents the base point on the elliptic curve.

- Step 3: Provide the generated public key (Q) and private key (d) pair.

SM2 signature verification algorithm

Input: Elliptic curve parameters (prime_mod, elliptic_curve, base_pt, order), public key (pub_key), message (msg), and signature (sig)

Output: True if signature (sig) is verified; False otherwise.

(1) Check if (r,s) is within the interval [1, order - 1]. If not, return False.

(2) Let msg=Z.

(3) Calculate H_{256}(msg).

(4) Calculate t=(r+S) mod n.

(5) Calculate (x1, y1) = s × G + t × pub_key.

(6) Calculate R=(e+x_1) mod n.

(7) If R=r, return True; otherwise, return False.

B. Algorithm 2

In real-time payment transactions, QR codes are not usually refreshed using the SM3 algorithm, a form of cryptographic hash function. On the other hand, it can support ensuring the legitimacy and security of the information that the QR code contains.

The SM3 algorithm creates a digest of data messages, verifies the authentication code of messages, and fulfills the security needs of multi-password applications. Here is the algorithm:

a: DEFINE VECTOR IV AND CONSTANT T_j AND INITIALIZE

IV = 7380166f 4914b2b9 172442d7 da8a0600 a96f30bc 163138aa e38dee4d b0fb0e4e

Q_i =

$$\begin{matrix} 79cc4519,\ 0 \le i \le 14 \\ 7a879d8a,\ 16 \le i \le 60 \end{matrix} \quad (1)$$

Boolean function definition:

DD_i (A,B,C) =

$$\begin{matrix} A \oplus B \oplus C,\ 0 \le i \le 14 \\ (A \wedge B) \vee (A \wedge C) \vee (B \wedge C),\ 15 \le i \le 60 \end{matrix} \quad (2)$$

EE_i (A,B,C) =

$$\begin{matrix} A \oplus B \oplus C,\ 0 \le i \le 15 \\ (A \wedge B) \vee (\neg A \wedge C),\ 15 \le i \le 61 \end{matrix} \quad (3)$$

Define replacement function P0, P1:

$$P0(A)=A \oplus (X<<<8) \oplus (A<<<16) \quad (4)$$

$$P1(A)=A \oplus (A<<<14) \oplus (A<<<22) \quad (5)$$

b:THE PROCESS OF ITERATIVE COMPRESSION

The completed message has been extended to form a group of 132 words W0～ W67,Wr0～ Wr63 for the compression function:

(1) Split the message group into 16 words W0～ W15.

(2) For $16 \leq j \leq 67$

$$Aj \leftarrow P1 (Aj\text{-}16 \oplus Wj\text{-}9 \oplus Aj\text{-}3 <<15)) \quad (6)$$

(3) For $0 \leq j \leq 63$

$$Aj' = Aj \oplus Aj+4 \quad (7)$$

c: DEFINE THE COMPRESSION FUNCTION

Let's say we have word registers A, B, C, D, E, F, G, and H, along with intermediate variables SS1, SS2, TT1, and TT2. The process of calculating the compression function can be broken down as follows: - Set the value of ABCDEFGH to V(i) - For every integer j from 0 to 63: - Update the value of V(i+1) to be the result of XOR operation between ABCDEFGH and V(i) - Update the value of ABCDEFGH to be V(n) Finally, the resulting 256-bit hash numerical value of ABCDEFGH is then outputted.

SM3 ALGORITHM HMAC CALCULATION PROCESS

In this document, once the terminal has been authenticated, a message is sent from the processing center confirming the completion of authentication. To ensure the message cannot be tampered with, it is secured using HMAC calculation. The MAC value of the input data text is determined through the following formula:

MAC(text) = HMAC(K, text) = Hash((K0 XOR 0pad) || Hash((K0 XOR ipad) || text))

For a more detailed explanation, please refer to Figure 5.

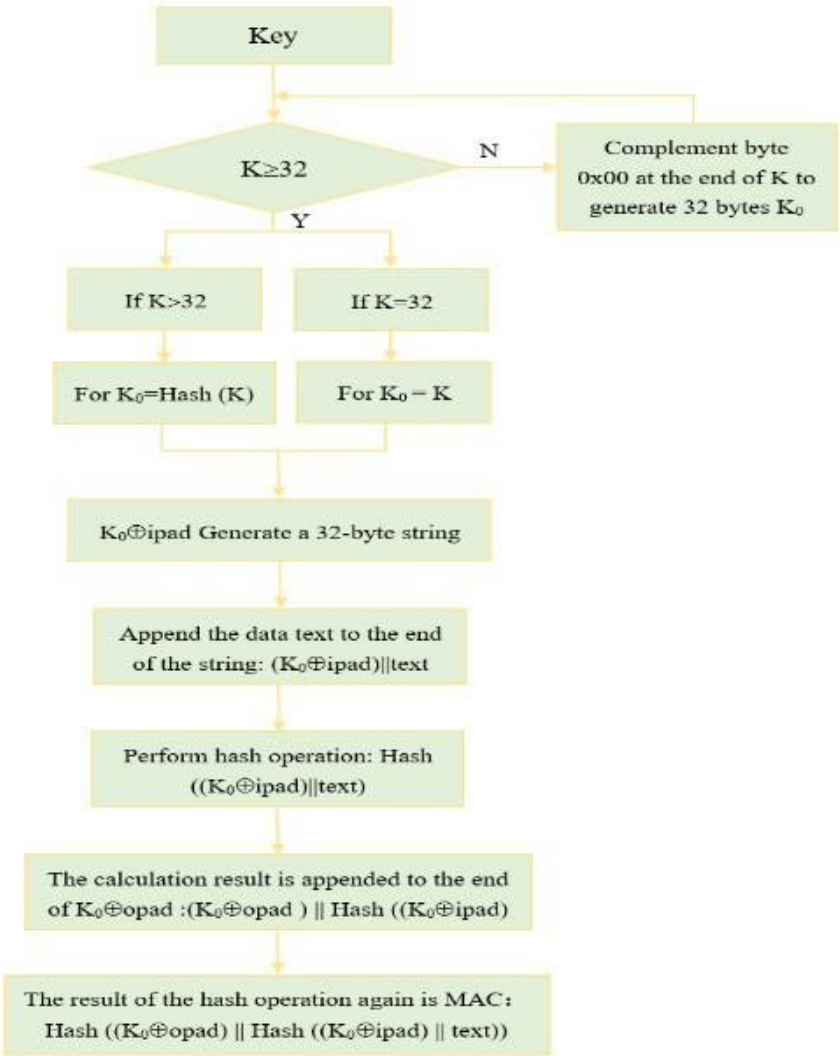

Fig. 5. HMAC calculation description

4. Conclusion

This study demonstrates how the transition from barcodes to QR codes represents a substantial advancement in data accessibility and storage. With the development of QR codes, new avenues for storing vast amounts of data in a compact, scannable manner have become possible. This has shown to be very helpful in the field of mobile payments, where security and usability are essential. A strong defence against potential dangers of malicious attack on financial transactions became necessary as digitalization and cashless transactions gained popularity. This led to the advancement of QR codes and the creative use of dynamic QR codes. With the assistance of the SM2 and SM3 algorithms, real-time dynamic QR code creation will play a potential role in addressing these security challenges and enhancing the safety and reliability of financial transaction.

This dynamic QR code that is generated in real-time, changes often, and can only be used once will protect banking applications from illegal attacks. Regardless of the particular payment systems and financial institutions involved, the system seeks to enable users to actively engage in seamless transactions through banking platforms with unparalleled ease, while also ensuring uniqueness and randomness. This is achieved by enabling real-time dynamic QR code generation.

References

[1]. ISO/IEC 18004: ISO Standard on QR Code 2005 Bar Code Symbology Specification.

[2]. Katharina Krombholz, Peter Fruhwirt “QR Code Security - How Secure and Usable Apps Can Protect Users Against Malicious QR Codes” 2015 10th International Conference on Availability, Reliability and Security.

[3]. Chahil Choudhary, Inam Ul Haq Utilizing, Adil Husain Rather, Dynamic QR Codes to Enhance Secure Payment Transactions: An Approach to Secure Computer based Transactions, 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI).

[4]. Y. Cheng, Z. Fu and B. Yu, ”Improved Visual Secret Sharing Scheme for QR Code Applications,” in IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2393-2403, Sept. 2018.

[5]. S. Chandrasekaran, V. Dutt, N. Vyas and A. Anand, "Fuzzy KNN Implementation for Early Parkinson's Disease Prediction," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 896-901, doi: 10.1109/ICCMC56507.2023.10083522.

[6]. R. Bajaj, C. Chaudhary, H. Bhardwaj, L. Pawar, H. Gupta and D. Sharma, "A Robust Machine Learning Model for Prediction: The Electroencephalography," 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 2022, pp. 1270-1274, doi: 10.1109/SMART55829.2022.10047098.

[7]. A. Trivedi, E. K. Kaur, C. Choudhary, Kunal, and P. Barnwal, "Should AI Technologies Replace the Human Jobs?" 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/INOCON57975.2023.10101202.

[8]. V. S. Bhamidipati and R. S. Wvs, “A novel approach to ensure security and privacy while using qr code scanning in business applications,” in 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC). IEEE, 2022, pp. 198-203.

[9]. K. Saranya, R. Reminaa, and S. Subhitsha, "Modern applications of qr-code for security," in 2016 IEEE International Conference on Engineering and Technology (ICETECH). IEEE, 2016, pp. 173- 177.

[10]. H. A. M. Wahsheh, "Secure and usable qr codes," 2019.

[11]. K. Krombholz, P. Fruhwirt, P. Kieseberg, I. Kapsalis, M. Huber, and ¨ E. Weippl, "Qr code security: A survey of attacks and challenges for usable security," in Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22- 27, 2014. Proceedings 2. Springer, 2014, pp. 79-90.

[12]. A. Dabrowski, K. Krombholz, J. Ullrich, and E. R. Weippl, "Qr inception: Barcode-in-barcode attacks," in Proceedings of the 4th ACM workshop on security and privacy in smartphones & mobile devices, 2014, pp. 3-10.

[13]. Ohbuchi, E., Hanaizumi., H., Hock, L.A, "Barcode Readers using the Camera Device in Mobile Phones", in Proc. of 2004 International Conference on Cyberworlds, pp.260-265, 2004.

[14]. Subernarekha Ghoshal, Shalini chaturvedi, Akshay Taywade and N. Jaysankar,"Android Application for secure Mobile base payment systems" Indian Journal of Science and Technology, Vol 8(S2), 171-178, January 2015.

[15]. Purnomo, A. T., Gondokaryono, Y. S., & Kim, C.-S. (2016). Mutual authentication in securing mobile payment system using encrypted QR code based on Public Key Infrastructure. 2016 6th International Conference on System Engineering and Technology.

[16]. J. Steeman. QR code data capacity, 2004. available online http://blog.qr4.nl/page/QR-Code-Data-Capacity.aspx. last accessed on 02/07/2014.

[17]. Shao, Y.H., Wang, Y., Yang, Y. and Wang, X. (2022) Research on a Secure Communication Protocol Based on National Secret SM2 Algorithm. Journal of Computer and Communications, 10, 42- 56.

[18]. J.-C. Chuang, Y.-C. Hu and H.-J. Ko, "A novel secret sharing technique using QR code", Int. J. Image Process., vol. 4, no. 5, pp. 468-475, 2010.

[19]. Meruga, J. M., Fountain, C., Kellar, J., Crawford, G., Baride, A., May, P. S., … Hoover, R. (2015). Multi-layered covert QR codes for increased capacity and security. International Journal of Computers and Applications, 37(1), 17-27. doi:10.1080/1206212x.2015.1061254.

[20]. Zou Jian,Wu Wenling,Wu Shuang,Su Bozhan, Dong Le.Preimage Attacks on Step-Reduced SM3 Hash Function. LNCS,vol.7259:pp.375-390, 2011.

[21]. Limin Guo, Lihui Wang, Qing Li. Differential power analysis of dynamic password token based on SM3 algorithm,and conutermeasures.11th International Conference on Computational Intelligence and Security, Shenzhen, pp. 354-357, 2015.