IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, November 2022
Impact Factor: 6.252

Multilevel Authentication Employing Watermarking based on QR Codes, Mobile OTP, and Hadamard Transformation

Shubham Datir[1], Nikhil Padekar[2], Uddesh Devkar[3], Saurabh Shirsath[4], Prof. Dr. Khatal S. S[5], Prof. Mundhe B. B.[6]
Students, Department of Computer Engineering[1,2,3,4]
Professor, Department of Computer Engineering[5,6]
Sahyadri Valley College of Engineering & Technology, Rajuri, Junnar, Pune, Maharashtra, India[1,2,3,4,6]
Sharadchandra Pawar College of Engineering, Otur, Pune, Maharashtra, India[5]

Abstract: *High-speed internet technology has made it possible for users to transact with banks more quickly thanks to online banking services. The increased connectivity also creates numerous online security holes like phishing and pharming. By confirming the user's legitimacy, this mobile banking problem may be resolved. Here, we suggest a hybrid system that makes use of QR codes, One-Time Passwords (OTPs), and digital watermarking—a method of data concealment. The bank generates QR codes using OTP as the key to the watermark sequence. Here, OTP can be utilised for the initial authentication verification. The sequence for the second level of verification is concealed throughout the watermarking process using the Hadamard transformation. Online transactions may be made with maximum security thanks to the OTP and watermark combination. One benefit of this strategy is that the QR code may be created within a limited design window with a suitable real-time extraction method. Performance may be assessed by utilising an android application, including the real-time extraction using a mobile device.*

Keywords: In OTP, Hadamard transformation, QR code, digital watermarking, and Hamming distance

I. INTRODUCTION

Because it is so simple to use and saves time, more and more people are using the internet for financial services. Because banking information is available anytime, everywhere, the problem of crowded banks and long lines is resolved. Thanks to improvements in mobile technology, a variety of financial services are now available anywhere and may be fully customised.On the other hand, a significant security threat is raised by online banking services. The server will ask for a user ID and password when you log in to an account to verify your identity. There are several bad links, nevertheless, that might be used to spoof authentication in order to hijack communication. Web phishing is one of them, when the hacker tries to obtain private data such as usernames, passwords, credit card numbers, etc.Consequently, a reliable and secure authentication method is needed.In this research, we provide a technique that makes use of a watermarked authentication approach based on QR codes. Mobile OTP is advised to increase security. 2D barcodes, often known as quick response (QR) codes, may carry more data and are simpler to decode. The Hadamard matrix and OTP are utilised in this approach to extract the watermark, with the Hadamard matrix being employed to disguise the data and the OTP serving as the stego key. Because of its attributes and simplicity, mobile OTP is used in place of security cards. Double security is enabled via an OTP with a short duration that is also difficult to monitor. Therefore, only authorised users are permitted access to the amenities. Here, a hybrid approach using OTP, watermarking, and QR codes is suggested [1]. The following explains them.

1.1 One Time Password (OTP)

OTP is a special kind of password that may be used more than once and changes for each login. The basic function of OTP is to often change passwords, which increases security and makes it challenging to obtain unlawful information from online accounts. In other words, a hacker who records an OTP that has previously been used on a service won't be accepted. OTPs are therefore difficult to maintain.The categories for OTP generation are as follows:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, November 2022
Impact Factor: 6.252

(a) OTP that is time-based: OTP is changed often.
(b) Event-based OTP: An OTP token or device generates OTP.
In online banking, a time-based OTP with a 5-minute duration is utilised.

1.2 Digital Watermarking

Digital watermarking is one method of information blending into a cover signal. The use of watermarks to confirm authenticity. There are several watermarks accessible, including text, picture, audio, and video. The approach we suggest uses OTP as the key and text as the watermark, as seen in figure 1 below.Cover picture has a watermark sequence, such as a QR code and an OTP (as a secret key). The final picture will have a watermark on it.

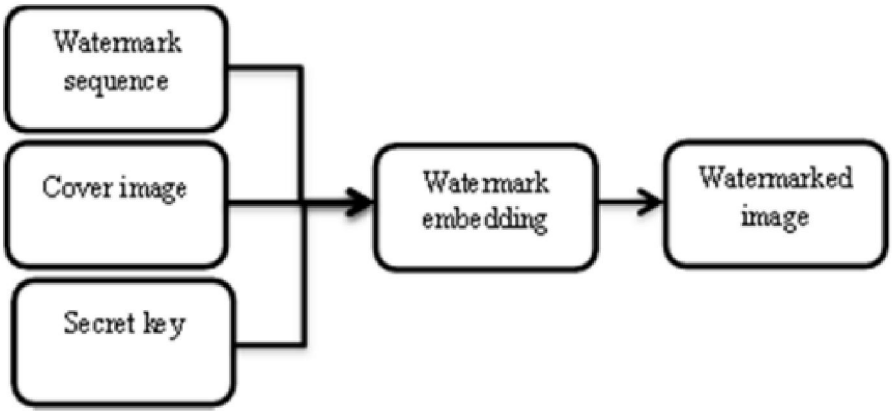

Fig 1: Watermark embedding at the bank

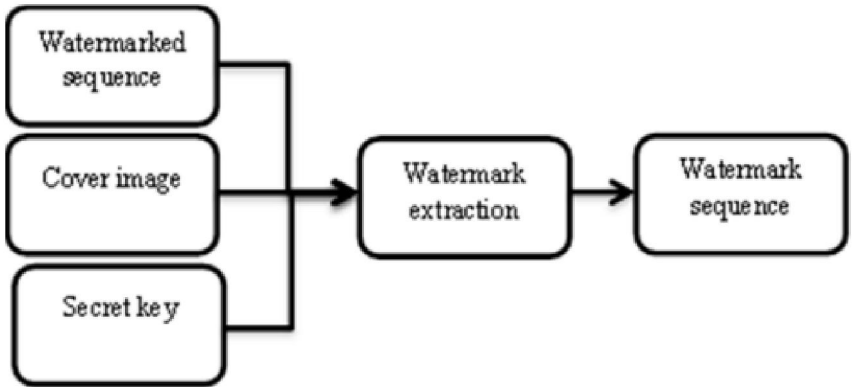

Fig 2: Watermark extraction by the use

Figure 2 above displays the watermarked sequence that was obtained during extraction together with the cover picture and secret key that was used for the decoding operation.

1.3 Hadamard Transformation

A signal is broken up into a collection of orthogonal nonsinusoidal signals using the Hadamard transform, an orthogonal transformation. Hadamard transform is mostly utilised in image processing for purposes involving compression. This transformation has several benefits, including a quick processing time, high resilience owing to the large energy content of the watermark, and simplicity of embedding and extracting invisible watermarks. Where V is the altered sequence, U is the original sequence, and Hn is the Hadamard matrix of dimension N*N, where N=2n, n=1, 2, 3, and so on, with element values that can be either +1 or -1.
Below is a hadamard matrix of order "n". Keep in mind that rows or columns are orthogonal to one another.

$$H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}$$

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, November 2022
Impact Factor: 6.252

1.4 QR code

Denso-wave, a Japanese business, created a 2D barcode with the ability to hold more data even in both vertical and horizontal orientations in 1994. Quick Response codes are referred to as QR. Its specialisation is high-speed data retrieval with greatest redundancy, as the name would imply. Figure 3 describes the QR code's construction.

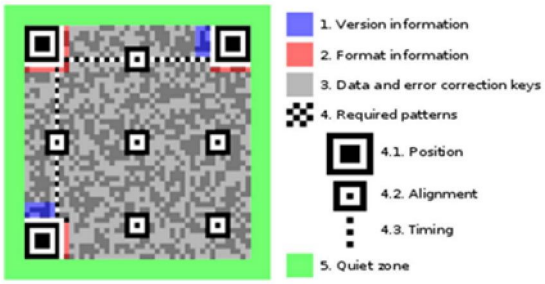

Fig 3: Structure of QR code

(1) Version details: QR code version
(2) Format Information: Describes the type of data mask and amount of error correction.
(3) Keys for data and error correction real data is saved as a data bit stream.
(4) Necessary patterns
(4.1)Position pattern: Provides information on how to align the code for printing.
(4.2) Alignment pattern: Aids in alignment and provides assistance in the event that there are any picture distortions.
(4.3) Timing Pattern: Matrix size is mentioned
(5) Quiet Zone: QR code's perimeter

There are now 1 to 40 version standards available, with V-40 having a 177*177 module size and the ability to store 2,953 bytes of binary data, 7089 numeric characters, and 4,296 alphanumerics. With the aid of coloured QR codes, it may be increased.

The following categories apply to this essay: The research's related work is listed in section2. The suggested plan is described in Section 3. Section 4 of the paper's conclusion also contains the paper's references.

II. CONNECTED WORK

European banks created mobile banking/M-banking to provide clients with a unique platform for successful financial transaction. Prior to 2010, Mbanking services were delivered by SMS (short messaging service) or mobile web. The quick rise was due to the high level of acceptance of this, which gave other banks leap trust. Numerous possible hazards resulted from this. SMS/MMS problems such international roaming, delays, costs, and location constraints forced the development of OTP as a different authentication method [9]. Customers gained trust because of this. Strong authentication techniques are as necessary for authentication as are the customer's convenience. However, as the internet expands, additional problems have emerged [5][6]. The development of new authentication techniques began. With OTP, the potential of QR codes made them appear more secure [3][7][8]. The following discussion focuses on a few of the authentication techniques described in several articles that inspired the concept. Mobile banking in India: Issues & Challenges, Devadeven et al. [18]

The author discusses the development of mobile banking in India and how convenient it is for consumers to obtain services even from a distance. The fast expansion of mobile banking brought about by the development of 2G, 3G, and 4G technologies also brought about several difficulties and problems. Based on the author's study, a comparison is made between mobile banking in terms of its features and security concerns.

Comparing various banks, it is discovered that the best way to win over customers' trust is to leverage emerging technology to boost security, which will then reach every user [10]. The user will immediately embrace this technology if they feel comfortable using it.

"Secure bank transaction utilising data masking methods," Pranchi D et al.

In order to suggest a technique, the author first discusses the significance of authenticity in the online banking system before introducing steganography, a type of visual cryptography. The hidden key is portion of a picture that is divided

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, November 2022
Impact Factor: 6.252

into two pieces. While the second part will be held by the consumer, the first share will be kept in the bank's database. When logging in, this key is selected for authentication. The author makes it very clear that there are no password hacking problems with the suggested approach.

"Review on Quick Response Codes in the Field of Information Security (Analysis of Different Imperceptibility Characteristics on Grayscale and Binary QR Code)" by Ramya, V et al.

The author uses a QR code to suggest a novel security approach. It makes use of structure and cutting-edge technology to innovate data concealing. The peak signal-to-noise ratio (PSNR), mean square error (MSE), average and maximum difference, normalised absolute error, and other characteristics are used by the author to assess the performance of QR codes. It has been demonstrated that the QR code is one of the greatest options for information concealment.

Using a QR code for secure banking, Brindha G et al.

The author suggests a novel method for obtaining authentication without utilising any sophisticated features. The author of this paper discusses the QR code, which was chosen owing to its advantages on the internet. The IMEI of the phone and the client's login information are used to produce the QR code.

A revolutionary QR code-guided picture stenographic approach, by Md. Wahedul et al.

The author suggests a brand-new technique for employing picture steganography to conceal data in QR codes. Smart phones with high levels of mobility may readily utilise this for both commercial and consumer purposes. With a high PSNR ratio and the potential to self-correct, this approach is being evaluated for further security. In stegnography, the data is effectively hidden using the DWT-SWD approach, allowing for complete message recovery.

"Improving the Capacity of QR Code by Using Color Technique," by Prathibha et al.

Because of the benefits of QR codes, writers have thoroughly researched the performance traits to achieve optimum effectiveness. More than simply a QR code with two colours is discovered to exist (white and black pixels). Through memory, colour QR codes are more efficient. While it is tripled in colour coding, the maximum memory capacity of a two-color QR code is just 4296 characters. This is mostly because red, blue, and green are the primary hues in every image. As a result, the encoding may be carried out concurrently in all three pixels. Using the RS coding scheme can also improve error correction on QR codes.

"Online Banking System Using MobileOTP with QR-code," by Amandeep et al.

An OTP and QR code system was suggested by the author to increase the authenticity of the authentication technique [7]. Because of its adaptability, QR codes provide a platform for steganography. OTP can also be utilised in this operation as the concealed data. This newly created process provides security while also making it simple for any clients in faraway areas to access. Only authenticated users can view a QR code since it is created by an algorithm using the user's input as user details [17].

The bank generates an OTP and sends it to the client's cell phone. For authentication, each approach is independently evaluated. This suggested strategy makes advantage of two-factor authentication.

"Multilevel security feature for online transaction utilising QR code & digital watermarking," by Mishra et al. [2]

The author suggests a novel form of QR code authentication technique. The QR code has a digital watermark put to it to make it more secure. Only the authorised client will be able to remove the watermark and access the data that is buried in the QR code. OTP is a watermark that will regularly change. Therefore, the likelihood of hacking is quite low. Visible watermarks are applied to QR codes using the discrete cosine transform (DCT).

III. PROPOSED METHODOLOGY

Two layers of authentication are mostly employed in the suggested authentication approach. The initial stage of authentication will include sending an OTP to the customer's phone. By measuring the hamming distance between each of these 16 different types of sequences, a secret sequence will be employed as the second level of authentication where this 32-bit length watermark sequence is derived from another sequence of 4-bit length. There are basically two processes going on here.

Extraction and Embedding. Two different types of QR codes are developed, and embedding is done on the bank side. We refer to this QR code as the cover QR code image since it will be used as the cover picture for watermarking.

Each time a transaction is made, a new QR code with a customised watermark is created using the secret key, a configurable OTP number, and a cover QR code picture. 16 different types of watermark bit sequences, each with a size

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, November 2022
Impact Factor: 6.252

of 32 bits, are chosen during the embedding process and put into the 16 rows of the Hadamard matrix. The hamming distance between the selected bit sequence and every other bit sequence in the matrix is then calculated using one of the bit sequences that was picked among the others. The Hamming distance is useful for counting the differences between two matrices. The watermark sequence of 4-bit length is chosen as the smallest hamming distance between them.

Due to the Hadamard matrix's orthogonality, the hamming distance between these 16 watermark sequences is 16 for any combination other than the identical sequences. Using the cover QR code picture and the stego key, which is the OTP, this 4-bit sequence is utilised as the watermark sequence. At the bank, the OTP is delivered through SMS and the cover QR picture is supplied via email. The user's financial information is used to produce the QR code in the Zxing library. Figure 4 illustrates this embedding procedure in further detail.

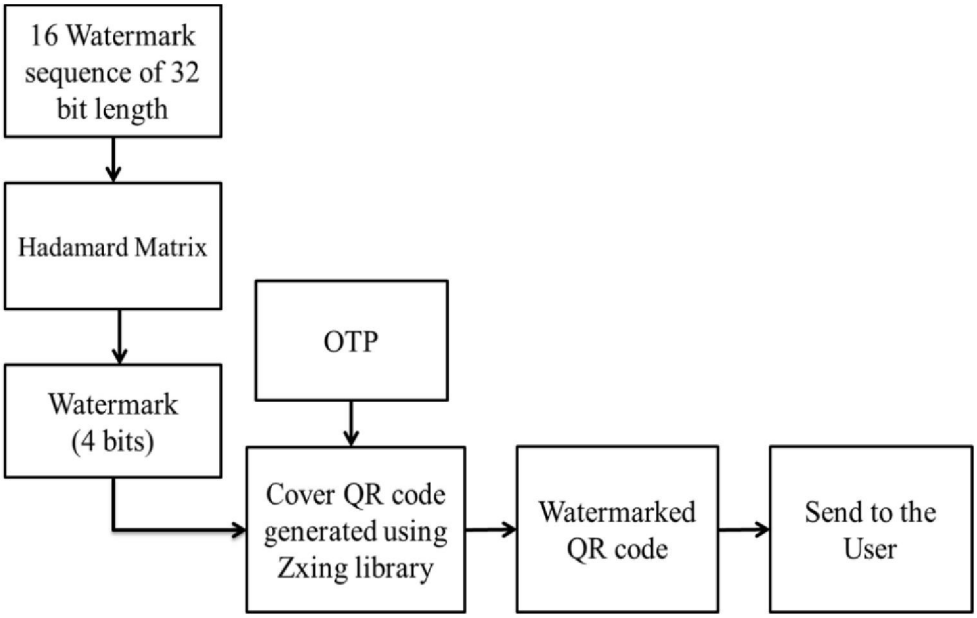

Fig 4: Watermark embedding

The method of phone-based user authentication is shown in figure 5 above. The two-level authentication will be done on a different web page that will be shown throughout the transaction. A 4-bit sequence may be accessed by scanning the QR code using the android application, together with the cover QR code picture that was downloaded during registration and the OTP that was received on the phone. Our watermark sequence, which is assessed using hamming distance on a threshold basis, T, has a low hamming distance. The sequence is deemed wrong if the hamming distance exceeds the threshold. Even if the mobile OTP was successfully received and the first level of authentication was successful, if the minimum hamming distance was not confirmed, the second level of authentication failed and was unable to proceed. The watermark may be recovered, disclosing the original 32-bit sequence, enabling effective authentication and high security if the sequence falls inside the threshold.

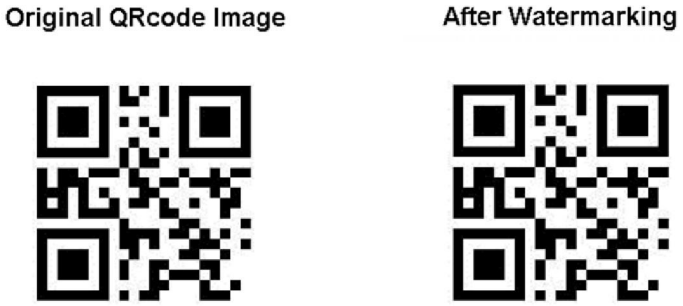

Fig. 6 Original QR code without watermarking and Watermarked QR code image.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, November 2022
Impact Factor: 6.252

The QR code picture is shown in Figure 6 both with and without watermarks. Our coverQR code picture is a watermark sequence without a watermark. It is obvious that the human eye is unable to distinguish between these two pictures. This strategy gains bonus points because the hacker won't know which way to use to obtain authentication.

IV. CONCLUSION

The internet already serves as the primary distribution route for mobile banking services, and this trend will only continue to grow. Therefore, security must be regarded seriously and protected by effective authentication and safeguards. Customers should find it easier to choose the degree of verification. With all of this in mind, we provide a solution for strong authentication, a watermarking approach that uses a QR code as the cover picture and an OTP for the stego key of the watermark. Hadamard matrix transformations can produce a watermark sequence. Using an android application, authenticity may be quickly verified on a mobile device. A second layer of security is enabled through OTP and watermarking. This strategy may be used to any financial services due to its simplicity and convenience of usage.

REFERENCES

[1]. Elliot Mbunge, Talent Rugube, "A Robust And Scalable Four Factor Authentication Architecture To Enhance Security For Mobile Online Transaction", International journal of scientific & technology research, ISSN 2277-8616, volume 7, issue 3, march 2018.

[2]. Mishra, A., & Mathuria, M. "Multilevel security feature for online transaction using QR code & digital watermarking". In Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of (Vol. 2, pp. 48- 51). IEEE, April, 2017.

[3]. Amandeep, Shweta, Akshata, Siddeshwar, Prof. F.S. Ghodichor5. "Online Banking System using Mobile-OTP with QR-code". International Journal of Advanced Research in Computer and Communication Engineering (IJARCE) Vol. 6, ISSN, 2278-1021, April 2017

[4]. Sudeep George, Reshma M, "Literature Survey on Mobile Banking Security", International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, Vol. 5, Issue 3, March 2017.

[5]. Student, Prachi D. Rathod, and Smita R. Kapse. "Secure bank transaction using data hiding mechanisms." In Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017 International Conference on, pp. 1- 6. IEEE, 2017.

[6]. Nosrati, Leili, and Amir Massoud Bidgoli. "A review of authentication assessment of Mobile-Banking." In Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016 IEEE 7th Annual, pp. 1-5. IEEE, 2016.

[7]. Sibi K, Suresh Kumar A, Ramya P, "Secured Online Banking System Using One Time Passwords Encrypted in QR-Code", International Journal of Digital Communication and Networks, march 2016.

[8]. Ms. Arati A. Gadgil, "Authentication Approaches for Online-Banking", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 4, Issue 11, November 2014.

[9]. Parvathavarthini, S., & Shanthakumari, R. "An Adaptive Watermarking Process in Hadamard Transform". International Journal of Advanced Information Technology, 4(2), 2014.

[10]. Ramya, V., & Gopinath, G. "Review on quick response codes in the field of information security (Analysis of various imperceptibility characteristics on grayscale and binary QR code". In Advances in Engineering and Technology (ICAET), 2014 International Conference on (pp. 1-5). IEEE, May, 2014.

[11]. Pakojwar, S., & Uke, N. J. "Security in Online Banking Services".A comparative Study. Published in: International Journal Of Innovative Research in Science, Engineering and Technology (IJIRSET) Volume, 3. 2014).

[12]. Murkute, J., Nagpure, H., Kute, H., Mohadikar, N., & Devade, C. (2013). "Online banking authentication system using qr-code and mobile OTP". International Journal of Engineering Research and Applications (IJERA) ISSN, 2248- 9622. 2014