

Multilevel Authentication using OTP, QR-Code and Hadamard Transformation

M. Anusha¹, V. Kavitha^{2*}, S. P. Lekhana³, M. S. Sahana⁴, A. Sushma⁵

^{1,2,3,4}Student, Dept. of Information Science and Engineering, Sai Vidya Institute of Technology, Bengaluru, India

⁵Assistant Professor, Department of Information Science and Engineering, Sai Vidya Institute of Technology, Bengaluru, India

*Corresponding author: kavithav.16is@saividya.ac.in

Abstract: In this technical world everything becoming online because new technologies emerging day to day in the world. Banking is one of the important sector which have to provide more secure transactions. Everyday people converting to online due to less spending time and processes becoming fast. Providing the security is biggest challenge in the technical world. There are more number of malicious links which diverts the user and access the user sensitive information of users which is illegal. The main issue of the online banking is to verifying the authenticity of the user.

Here we proposed a mechanism with the use of One Time Password (OTP), QR Code i.e., Quick Response Code using Hadamard Transformation. OTP is used for first level of authentication. Hadamard Transformation and digital watermarking is used to hide the sequence which is secret key for second level of authentication. This mechanism will provide a high level security for authentication. Hence we used android application for performance evaluation.

Keywords: Digital watermarking, Hadamard Transformation, OTP, QR Code.

1. Introduction

In this era the internet banking is increasing gradually because of simple usage and saves more time in our daily lives. This internet banking allows the user to make electronic payments system this enables through the respective banking websites or softwares through the mobile. Another side the transactions can be done at anytime and anywhere this improves the flexibility of the transactions and eliminates the long queues in the bank.

SMS banking is also becoming popular in this technical world; which banks sends sms to respective users. This will also provide security which it gives notifications and alerts to user. Though the user may get the status of his/her account status periodically. Some banks services may also provide or enables the customers to perform some transactions using sms.

Online banking services arises the security problem which is an important treat. The traditional based authentication only involves the username and password which ensures the less security to the users. There is an enormous links which could create fake authentication to hack the communication which is also called web phishing, pharming etc. Therefore, requirement of the strong authentication scheme is needed.

To enhance the security, we introduced two levels of authentication, which is ease to customer usage and provides strong and secure authentication using OTP, quick response code (QR Code) based watermarking with hadamard transformation.

In this paper, we introduce a method where QR code based hadamard transformation authentication scheme is used. To enhance the security and privacy OTP is preferred. QR Code are also called 2D barcodes which holds the data digitally and can be extracted easily. Hadamard matrix is used to generate the secret sequence is called watermarked sequence. These techniques abused in watermarking by using hadamard matrix and OTP to enhance the security. Hence these methods are proposed.

A. One Time Password

One Time Password popularly called OTP, a unique password which is used to authenticate the user by generating a 4-bit random number and send to user through SMS of registered mobile number.

For Online banking the generation of OTP is categorized as follows:

1. Time based OTP: This type will frequently changes the OTP for every specified interval of given time by the developer.

The event based OTP for the online banking we used the span of five minutes.

B. Hadamard Transformation

The Hadamard matrix is one of the type of matrix which contains only -1's and 1's. This is an orthogonal transform. This transform is used in image processing. The hadamrd transform is highly robustness and takes less processing time. In this paper we used 8x8 matrix for the transformation.

C. QR Code

This is also called 2D barcode. Most of the internet banking and e-commerce websites uses QR Code for transactions purpose. Every user has a unique 2D barcode which improves the secure transactions. This becoming popular due its reputability and has high storage capacity.

This paper we generate two QR Codes for every user, one at registration time using user credentials and another at every transaction time using already generated QR Code we embed OTP and secret key from hadamard transformation.

We used zxing library to generate the QR code which provides a necessary objects and methods to create the QR Code and used hadamard transformation feature for secure the QR Code from hackers.



Fig. 1. QR Code generated at registration time and transaction time

2. Proposed Methodology

In the proposed method, mainly used two levels of authentication we also called multilevel authentication. The OTP sending to the customer's or user's phone is the first level of authentication. A secret sequence will be used as the second level of authentication where this 128-bit length watermark sequence is obtained from another sequence of 8-bit length from hadamard transformation. Two main processes are implement here. Embedding and Extraction. Embedding is done on the bank side server. Here two types of QR Code will be designed. At the time of registration, a QR code is generated according to the details given to the user like bank id, phone number etc. This QR code will be taken as the cover image for watermarking hence we call that as the *cover QR code*. During each transaction, another QR code a unique watermarked QR code will be generated from a variable OTP number, *cover QR code* and with the secret key. During embedding a two 8x8 matrix is created one is positive and another is negative and we concat both in such a way that the output must be hadamard matrix and 8x8 matrix is generated randomly. Using those two that is hadamard matrix and random generated matrix we do scalar multiplication and produce another matrix and this matrix is multiplied with 8-bit sequence which is done by transposing of 8-bit sequence, it produces 128-bit sequence.

This 8-bit sequence is used as the watermarked sequence and it is embedded in already generated QR Code using user details during registration using zxing library. This whole process of embedding is shown in figure 1 in a simpler manner.

During Extraction the 8-bit key will extract the 128-bit sequence using zxing library and verifies. If it verifies then this enables high security. This whole process of extraction is shown in figure 2 in a simpler manner.

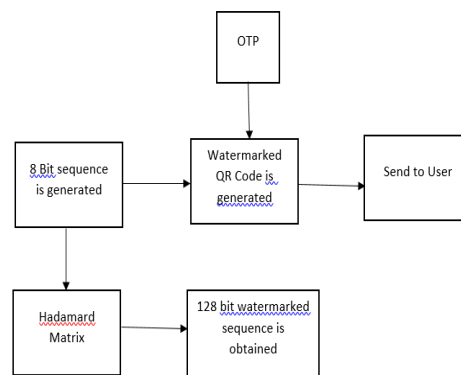


Fig. 2. Watermark embedding

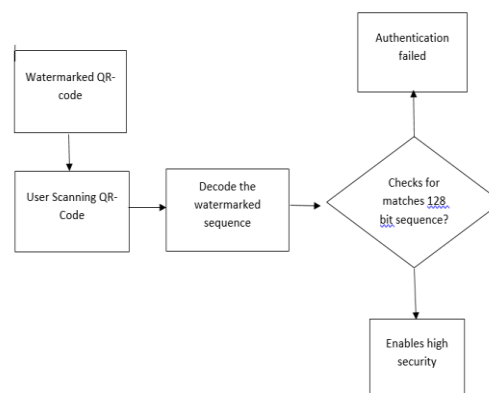


Fig. 3. Watermark extraction

3. Experiment and Results

The test for estimation experiments randomly using Android Studio software and java and xml programming languages for backend and frontend respectively. The PC for estimating the results is equipped with an Intel P4 2.4GHz Personal laptop and 2GB memory.

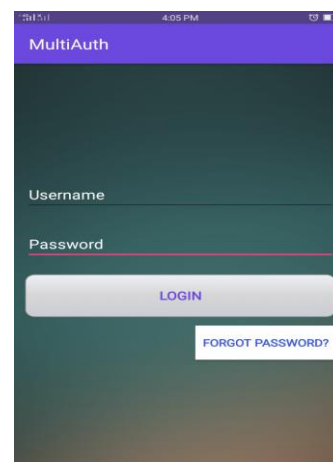


Fig. 4. Login Page

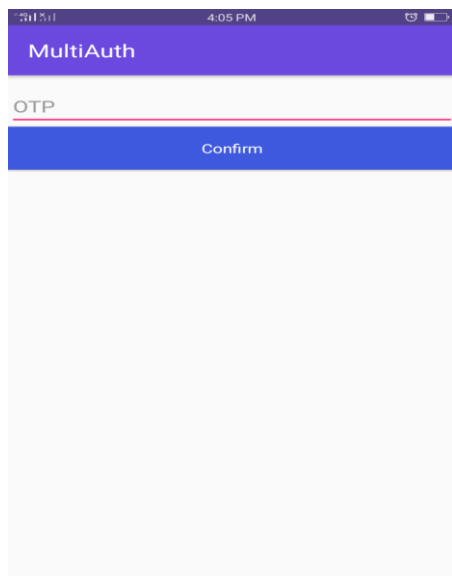


Fig. 5. OTP Generation



Fig. 6. Watermarked QR Code send to user

4. Conclusion

The internet is powerful carrier for online banking services and services using internet will gradually increase. Hence privacy and security must be taken austere and must provide strong authentication and safeguard measures. Selection of level of authentication as in more conducive manner to user or customer. By taking all these into scrutiny, we propose a method for strong and secure authentication, a digital watermarking technique by using QR code as cover image and OTP for secret key of the watermark. Watermark sequence can be obtained from Hadamard matrix transformations. By an android application, authenticity can be validated using a mobile phone within a short time period. OTP and watermark sequence enables double security. Simplicity and ease of use make this method able to adapt in any banking services.

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, volume 7, issue 3, march 2018.
- [2] 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.
- [3] 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.
- [4] Ms. Arati A. Gadgil, "Authentication Approaches for Online-Banking", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 11, November 2014.
- [5] Parvathavarthini, S., & Shanthakumari, R. "An Adaptive Watermarking Process in Hadamard Transform". International Journal of Advanced Information Technology, 4(2), 2014.
- [6] Ramya, V., & Gopinath, "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.
- [7] Pakojwar, S., & Uke, N. J. "Security in Online Banking Services - A Comparative Study," in International Journal of Innovative Research in Science, Engineering and Technology, Volume 3. 2014.