Open Peer Review on Qeios

A Security Framework for the Mobile Application Using Color Barcode

Rana Majumdar[1], Arijit Dutta[1], Anirban Mitra[1], Sangeeta Banik[1]

1 Sister Nivedita University (SNU)

Funding: No specific funding was received for this work.

Potential competing interests: No potential competing interests to declare.

Abstract

The thorough objective of this work is to establish a QR code framework for a secret key-secured concept. It is based on the asymmetric key verification context. SSH, server QR code is used for website login. The client-side stored RSA private key for encrypting information by implementing QR code verification, but presently QR codes are in the form of two-dimensional images for encryption purposes. The cell phones take the image of the QR code of the user and send a cryptographic reply to the server for broad verification. The upheld shading QR code inside the portable application for misusing the cyan (C), fuchsia (M), and yellow (Y) print the channels, and for the print shading by red (R), unpracticed (G), and blue channels, severally, apply the catch the shading picture. The hiding process embeds the quantized QR code so that it will not cause any visible distortion in the cover images and hides the QR code inside a color image. The results show the proposed method has high imperceptibility, integrity, and security.

Rana Majumdar*, **Arijit Dutta**, **Anirban Mitra**, and **Sangeeta Banik**

Dept. of Computer Science, Sister Nivedita University, Kolkata, India

Correspondence: rana.majumdarwb@gmail.com

Keywords: Barcode, color QR code, Security, Cryptographic.

I. Introduction

This work offers an authentication mechanism based on asymmetric key RSA encryption. One public key cryptosystem that is frequently used for safe data transmission is RSA. Installing the QR code software application is necessary; otherwise, passwords need to be remembered. The login process is quicker and less error-prone than with other frameworks. The application server is also not required to save the passwords of its clients. Additionally, it lets customers take advantage of how easy it is to filter QR codes. Because of their accuracy, readability, and practicality, scanner tags

have found widespread use in a variety of settings. For example, they are used by retail chains and anchors to identify customers, track items, and value products in addition to serving as a means of identifying them from participation postcards. in the development and delivery of the following items, such as courier services, rental cars, carrier equipment, quick delivery, enduring identifiable evidence in healthcare facilities, record management systems, silver screens, movie theaters, and transportation. The scanning label on the two measures is more opulent. The first, referred to as one-dimensional (1D) standardized tags, convey information by varying the gaps and thicknesses of corresponding ranks. The amount of electronic data stored in 1D scanning tags is limited, and these public spaces are allowed to have fewer errors. Expanding the number of scanner tag numbers or making alternative standardized tags available can effectively increase the amount of information.

QR CODE SOFTWARE APPLICATION: QR code provides a common technique to complete secure authentication while keeping the private key under the control of the users during the whole process.

QR CODE HARDWARE DEVICES: QR token hardware devices, which contain a unique serial number and provide a unique public and private key pair during the processing. Both public and private keys are generated by a thermal noise random number generator.

Figure 1. QR code authentication

These days, it's very common to use QR code scanning for authentication. In order to manage account accreditations, Snap2Pass and Snap2Pay [2] rely on QR codes rather than SSL to transmit the mutual secret between the phone and the PC program. In his work, researcher McCune has connected two-dimensional standardized identifications and phone cameras to transmit open keys, one device at a time. The user's data is encoded and sent as a QR token to facilitate the authentication process. A unique QR code is generated for each mobile device, PC, or laptop when the visitor first connects to the WI-FI network.

Some companies are using the QR code for the login process and identity verification. When the soft token interface

receives the user pin, the smartphone generates unique, single-use QR codes that can be scanned by a webcam or other mobile devices.

Figure 2. Web QR code

II. LIterature Survey

Against the framework, we characterize different possible outcomes and how they are approached. We all agree that, in order to prevent basic sessions, the login process and the subsequent PC session must be served over SSL. Each and every private key is kept on the code's chip. Passwords cracked using hardware is the only way to obtain the private key. An attacker cannot obtain additional private keys if one is leaked following their efforts. Another key does not correlate with the other.

A two-dimensional barcode, or 2D barcode, is a graphical representation that holds data vertically as well as horizontally, similar to one-dimensional barcodes. Because of this design, 2D codes have a storage capacity of up to 7,089 characters, which is substantially more than what a one-dimensional barcode's 20 character capacity can hold. Because 2D barcodes allow for quick data access, they are also known as quick response codes. Usually, smart phones are used in conjunction with 2D barcodes. All the user has to do is grab a screenshot and a picture with their phone.

The encoded URL is interpreted by a barcode reader, which then points the browser to the pertinent page on a website.

The encoded URL, which points the browser to the pertinent content on a website, is interpreted by a barcode reader. Because of this feature, 2D barcodes are helpful for mobile marketing. For users who have web access, certain 2D barcode systems also send information in a message.

Generally, 2D barcode are being used in such a field: -

1. *Some newspapers include 2D barcodes on stories that link mobile users to developing coverage.*

2. *2D barcodes on products in stores link to product reviews.*
3. *Some people post 2D barcodes that link to their blogs or Facebook pages.*

Data can be stored on both the horizontal and vertical axes with a 2D barcode. Printing, embedding on a computer screen and other presentations of this graphic image for scanning and analysis are all possible.

Another name for two-dimensional barcodes is a matrix barcode or matrix code.

Two-dimensional bar codes with square black modules on a white background are called quick response codes, or QR codes for short. Smartphones are intended to be able to read QR codes. They can offer a lot of information, including links, text, and other data because they can transport information both horizontally and vertically.

A QR code has a character limit of thousands, while a bar code has a limit of 20 alphanumeric characters. Consequently, multimedia content, like a whole e-book or website landing page, can be shared via a QR code.

Additionally, QR codes can instruct a phone to carry out specific tasks.

As an illustration: A theater company may offer a QR code that, in addition to taking the user to the website of the company for information on tickets and show times, also adds details about the dates, times, and locations of future performances to the mobile device's calendar.

To create a QR code from data, utilize a QR code generator. The QR code generator transforms data entered by users into an electronic symbol that can be printed or viewed. There are lots of free QR code generators online.

The boxes in a QR code that represent the buffers that can be removed can theoretically be determined mathematically, but this kind of computation is usually superfluous. Anyone can start applying their design techniques to a code and then test for scan ability by using a straightforward trial-and-error method.

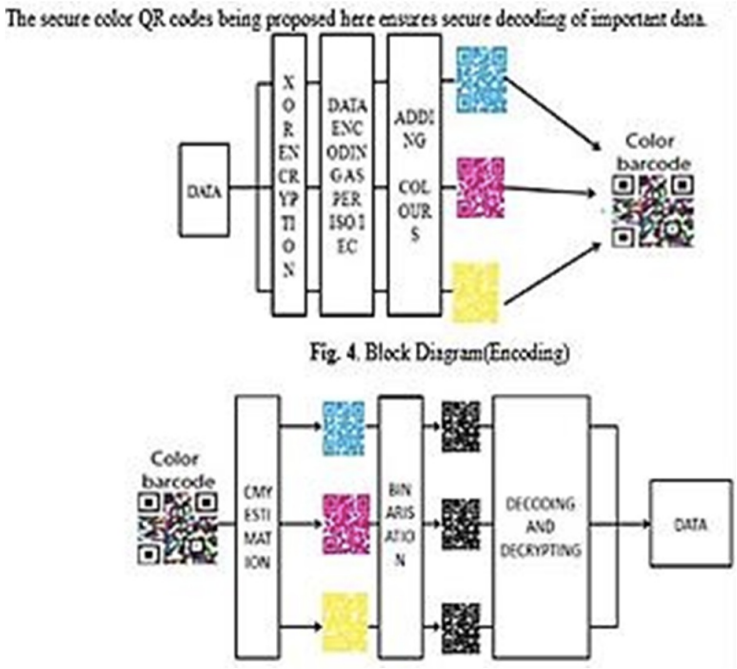

Figure 3. Secure color QR code

III. Proposed Methodology

The expected system can handle cases ranging from twenty-nine x twenty-nine modules to sixty-five x sixty-five modules. Similar to the information matrix system, the Finder style appears to be a 'L' shaped powerful line on the left, with sporadic lines constructed based on the best edge and benefit of the QR code.

Encoding: The information message is converted from stomach muscle to the supply channel for bit stream exploitation. There should be a guarantee that there will be fewer errors made in the flow of data transmission.

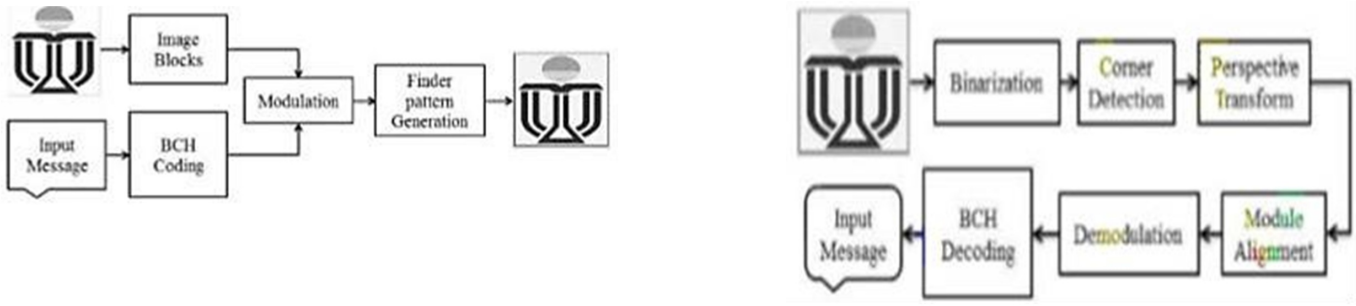

Figure 5. Decoding of QR code

Bose, Chaudhuri, and Hocquenghem developed the BCH Encoder-BCH Code to monitor and validate a variety of errors within the sent message. The coding framework is used to translate the encoded data into a QR code that can be retrieved.

The QR Code is first binarized, and four unusual corners are examined using historical data from the institutionalized ID structure. The corners are indicated by the bold lines inside the bottom right corners and the softer lines rising up the top-left corners. The gathering technique is a switch strategy of adjustment during which each module is examined to recover the message that has been encoded within.

To recover the encoded learning from every shading channel, we typically select the shading impedance cancelation algorithmic program that measures the C, M, and Y colorant layers from the R, G, and B channels of the captured standardized tag. After that, each evaluated colorant channel's encoded data is turned off. The implied that appeared in Fig are effectively addressed the following.

Password Cracking: Every single mystery is concealed within the token's chip. The most effective way to unravel each mystery is through the use of technology that primarily relies on word-breaking mystery. The most advanced examination Assurance Level for chip security is EAL5+, which is what we typically use. The chip would quickly be destroyed by any attempt to view the banner inside of it. Since the key match is made by warm uproar sporadic range generator, there is no chance that the attacker will ask for or predict elective individual keys, even if a single mystery is revealed through their immense labor. The different keys are unrelated to one another.

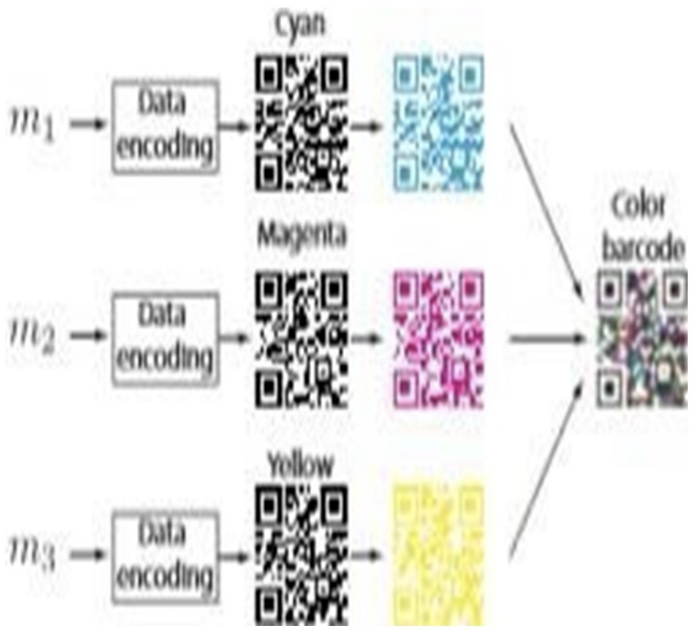

Figure 6. Encoding based on per-channel

Security Analysis: In our security analysis, we frequently show different possible attacks on the structure and how they might be carried out. We usually settle for using the domain for the login process, so in order to prevent basic session seizure, subsequent PC sessions are served over SSL. Our style is meant to set ourselves up for the opponents' eventual styles. The genuine and secure method for hiding colour QR codes is provided in this article. For abusing colour printing, the colour QR code has provided data rates of the colourless complements. Additionally, the perfect built mix has captured and withdrawn the space between the physical alternatives. The hacking team handled the revision of the

committal to create plausibility for the shading uniformed tag and QR code in the event that the mistake rate territory unit extends inside the third channel over the catch data zone unit.

References

- Thonky tutorial on QR Codes. Hiroko Kato, Keng T. Tan, DouglasChai,"Novelcolor selection scheme for 2D barcode",2009 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2009) December 7-9, 2009
- HenrykBlasinski, OrhanBulan, and GauravSharma;"Per-Colorant- ChannelColor Barcodesfor Mobile Applications: An Interference cancellation Framework"; IEEE TransactionsOn Image Processing, Vol. 22, No. 4, April 2013.
- O. Bulan and G. Sharma, “High capacity color barcodes: Per
- Arjun Puri, Sudesh Kumar, “Comparative Analysis of Reed Solomon Codes and BCH Codes in the Presence of AWGN Channel”, International Journal of Information and Computing Technology, vol.3 no.3, 2013
- H. Bagherinia and R. Manduchi, “A theory of color barcodes,” in Proc. IEEE Comput. Vis. Workshops, Nov. 2011, pp. 806–813.
- K. Nurwono and R. Kosala, “Color quick response code for mobilecontent distribution,” in Proc. 7th Int. Conf. Adv. Mob. Comput. Multimedia, Dec. 2009, pp. 267–271.
- H. Kato, K. T. Tan, and D. Chai, “Novel colour selection scheme for 2D barcode,” in Proc. Int. Symp. Intell. Signal Comm. Syst., Jan. 2009, pp. 529–532.
- H. Kato, K. Tan, and D. Chai, Barcodes for Mobile Devices. Cambridge Univ. Press, New York: NY, 2010.
- H. Gupta, S. Mondal, S. Ray, B. Giri, R. Majumdar and V. P. Mishra, "Impact of SQL Injection in Database Security," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2019, pp. 296-299, doi: 10.1109/ICCIKE47802.2019.9004430.
- H. Gupta, S. Mondal, B. Giri, R. Majumdar, N. S. Ghosh and V. P. Mishra, "An Authentication Model for Secure Electronic Transaction," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2019, pp. 283-286, doi: 10.1109/ICCIKE47802.2019.9004334.
- S. Som, R. Majumder and S. Dutta, "Elliptic curve cryptography: A dynamic paradigm," 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dubai, United Arab Emirates, 2017, pp. 427-431, doi: 10.1109/ICTUS.2017.8286045.
- P. Kaushik and R. Majumdar, "Timing attack analysis on AES on modern processors," 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2017, pp. 462-465, doi: 10.1109/ICRITO.2017.8342471.