Hindawi
Security and Communication Networks
Volume 2018, Article ID 3809462, 10 pages
https://doi.org/10.1155/2018/3809462

Research Article

Fake and Real Massaging at the Same Time with QR Code in Web Services for Different Users

Mirsat Yesiltepe and Muhammet Kurulay

Yildiz Technical University, Department of Mathematical Engineering, Istanbul, Turkey

Correspondence should be addressed to Mirsat Yesiltepe; mirsaty@yildiz.edu.tr

Received 10 July 2018; Accepted 11 November 2018; Published 19 November 2018

Academic Editor: Vincenzo Conti

At present, the notion of a cloud has expanded so much that there is no area of knowledge other than the concept of cloud. The most important reason for this is the ambiguity in the definition of this concept in the literature. Some have used the concept of a mobile cloud to create private cloud environments, while others have defined the cloud as a complex environment consisting of many different entities and layers, while others regard the cloud as parallel, discrete, and grid. In other words, the concept of cloud can sometimes be limited by the user devices and sometimes by the user devices. QR code, which is a precise and accurate way of communicating a text or symbol to the other side, is very broad, as is the concept of cloud use. The use of this technology is increasing with the availability of data encryption algorithms. As an abbreviation of the term "QR code," the QR phrase "Quick Response," which is the English language name, is used. In this study, when the same request is requested for different users (clients) in the web service, the response generated by the server at one time is sent to the different users at one time and the users get different messages. It is intended to reduce the load on the server and respond more efficiently to clients. Scrambled steganographic QR codes will be used for these operations. Some of the highlights of the paper are different message transmission with the same QR code to different users in web services and message verification with a hash value, using fake keys and advantage of changeable security mechanism.

1. Introduction

The QR code concept is a technology that allows two-dimensional data such as text and URL to be stored and read in a specific (standardized) format. The area of use is quite extensive. The most common use is to provide communication to the other party in full. For example, a dentist can communicate information to customers through the QR code, such as web addresses, addresses of workplaces, and services provided [1]. An educator can add resources to QR code by adding QR code to QR code [2]. Online navigation systems also started using QR code. In this case, instead of writing the address, the user must go to the code and read the code to determine the correct address to be forwarded [3]. A system in which the user uses his/her data to create a coded and hidden data QR using the system that the user uses when making a reservation for a hotel allows the user to use his/her room without having to contact the hotel with a special QR code reader located at the door of the communication room [4]. It is another area of application in which the information required for the robot to follow the trajectory of mobile robots is followed by the QR code [5].

When Figure 1 is examined, in recent years, the rate of increase of the publications related to QR code term has been slowed down. In particular, the rate of increase is the highest in 2009-2010. It is expected that the number of publications will increase in the following years but that the rate of increase will not increase much; that is, it approaches zero.

In the remainder of this section, the studies on QR code and web services, in general, have been reviewed and the difference between the previous studies and the previous ones is summarized. Topics of studies to be examined are as follows: QR code, QR code encryption, QR code steganography, QR code encryption and steganography use together, QR code encryption, and steganography use in web services.

Encryption is a way of changing data in plain text format so that it can only be understood by the user or system. General characteristics of publications made in QR code

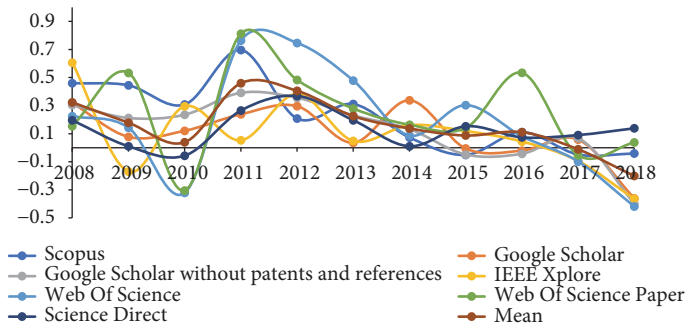


Figure 1: Relation with the database of publications related to the term "QR code" for years [37–40]. Access date: 7 November 2018.

and encryption field are as follows. QR codes are sometimes considered as an image and the image is encrypted [6]. Sometimes an image is converted into a sequence of numbers and stored in a QR code encoding. In this method, QR codes can be used in a certain way. In the encrypted QR codes, the working time was tested according to the classical encryption algorithm by working on the cellular automatic [7]. Sometimes QR allows certain images to be encrypted with users' social media information. These are the steps used in encryption. The URL of the user profile page is selected. This profile produces the appropriate QR code. The image or data to be uploaded from the profile is selected. The generated QR code is encrypted with the selected image [8]. Various encryption algorithms (AES, DES, and TripleDES) for accessing the original QR code and another application for making the decryption key requirement are used. Here the message is encrypted according to the algorithm that was originally set and the code creation and decompression processes have been tested [9].

Various methods are used to hide information in QR code. One method is to store the information to be stored on the keys determined according to the length of the error correction code specified in the QR code in specific regions in a piecewise manner [10]. Here it is desired to store information into the QR code. In another method, the main picture is compressed first, and the QR code to be stored is embedded in this picture. Here, it is desired to store the QR code picture in the main picture [11]. There are three methods for storing messages in the QR code. The first is to use the hash function. The second is to use a symmetric encryption algorithm for text encryption to be hidden. In the third method, the data to be hidden is embedded in the original QR code without distortion of the original contents. This method has been used [12]. Storing the encrypted message stored in QR code helps to prevent the message from being modified. If the content of the message in the stored code changes, the message will not be relevant to the original message [13]. In QR code, unlike the others, the concept of information storage on the code (region within) has emerged [14]. An approach similar to the algorithm used in water texture play in glazing is used [15]. In another concealment method, the information required to store is initially divided into three parts. Parts are translated to ASCII code. These parts are hidden on the color QR (digitally processed on the RGB bits) by associating each part with QR codes processed on different colors [16, 17].

The general characteristics of publications made in the field of QR code and encryption/cousage: in a study, the encryption algorithm is determined for the message to be hidden and for encryption. Four images are determined, one of which is the image to be hidden and the other is the image of the outer surface. The result is color in the resulting QR code as it is imaged in color [18]. The QR code containing the message is stored in a selected image [19]. Another area of use for different users is to use different messages. On this basis, certain users can understand messages different from the same QR code as their decryption key [20, 21]. In another work, the QR code is concealed in a picture so that the user can see the secret message with the QR that the user has obtained with the decryption key. In practice, the QR code is hidden into the QR code without any distortion into the QR code [22].

Another area of use of QR codes is the watermarking. The concept of watermarking is often confused with stenography. The purpose of watermarking is to keep information about the object to be kept and to indicate the object belonging to whom it is working on, while the stenographer is to hide the information and make it understood only by the person concerned. Although the work done can also be used in watermarking hidden QR code, this has not been evaluated in the tests made. In a study conducted, the QR code was used in the marking of a medical image belonging to a company that belonged to that firm [23]. In another study on medical images, QR code and image were watermarking with various algorithms. The success of stigmatization was measured by taking certain parts of the images [24]. In the QR code, the watermarking was used to indicate that the relevant code belongs to a particular organization [25]. This image is usually identified as two images [26], because when the image is used in color, the duration of the process is extended [27].

The general characteristics of publications made in QR and web services are as follows: An example of use is the identification of authentication in web services by authenticating the QR code generated after the user has entered the authentication information with the mobile application through the mobile device [28]. The reason for using mobile devices here is that such devices are the most personal devices [29]. When you want authentication in web services to be

done with QR code, different ways are used to authenticate the client and server. But the code to be used for authentication is created (client) or verified (server) on the mobile device [30]. This two-dimensional verification can also be done using the QR code. At that time, the process first makes a request of the client, the server sends a QR code to the person, and this QR code of the client reads the mobile device, sends the request and device identifiers to the presentation, and ends with verifying the request of the server. The difference between the last two runs is that the QR code generated at the end is client specific and not client specific. In the first case, the code client was formed especially [31]. Another work is to authenticate with the QR code and to provide the response of the contents of the multiple services in one go [32]. The user has access to more than one application thanks to the single QR code. QR codes are also used for mobile authentication. In an operation, the user tries to enter the application with the password. The QR code is generated by checking the password. The user scans the generated code for execution. The application receives authentication information from the encrypted message. The application prompts the user to indicate this in the main application by displaying a descriptive code. This code is entered according to the correctness [33]. The difference here is the need to authenticate from the mobile application to access the difference.

Hash functions are algorithms that allow variable length data to be stored in the fixed length by converting it to data. Generally, the information to be used in comparison is stored in a fixed length format and used for comparison. They are not reversible. That is, the original value cannot be obtained from the obtained value. The aim is to generate an extract value from the user's intended data to be used in the study and to transmit the value to the server and to obtain the value of the extract and the comparison of these values with the data that the server will generate in the response service. This facilitates the detection of unwanted users. With the SHA512 algorithm used in the study, 384 bits with the SHA384 algorithm, 256 bits with the SHA256 algorithm, and 160 bits with the SHA1 and RIPEMD160 algorithms are produced. The large length of the output data produced reduces the possibility of generating the same output as another data set.

Hash functions can be used for various purposes with QR code. In product distribution, when a product is requested, product and user information are stored in the database and when the product reaches the customer, the product can be compared with the hash value of the QR code to be generated by the user's own mobile device when it is desired to be delivered to the user [34]. Sometimes the QR code contains a hash value and this value is used for signing [35]. When creating the hash value, it is important to determine the sequence in which the data is used to generate this value. A different combination refers to a different hash value. It is a different use area to use a particular message to be used in a stamp or to be encrypted and encrypted by a message [36].

By the end of the first half of 2018, it was observed that the studies conducted with the QR code were the most performed in the security field. In a study related to text reading for the handicapped, the text to be read was compressed, the QR code was generated with the obtained text, and then a sound file was obtained by analyzing. QR code and compression techniques [41]: in another work done, contents of other regions are embedded in different points of the QR code and the contents can be read without incomplete parts of the code. In other words, by default, the code was attempted to increase the percentage of missed readings [42]. In another similar study, color codes were proposed to increase the length of the text that can be stored in the QR code as the capacity [43]. More flexible access is another work of building glaze distribution schemes built with QR code for high-level security [44]. Normally, for client-side cloud storage cheats created from combinations of user's passwords, automatic authentication to new devices using QR code for authentication is not a new area for using QR codes as a security mechanism [45] but this work was attempted to develop this concept. In the last study examined, the QR codes on cardboard boxes containing liquids were exploited due to the deterioration of the sun or various factors. QR code and online and on-paper evaluation methods were compared in evaluation forms made with medical students in different regions. It has been seen that students prefer QR code the most and fill the form in less time thanks to it [46].

In a study close to the work done, this QR code was embedded in another picture [47] with the message being encrypted and the encrypted message stored in the QR code and stored in the QR code generated by the decryption information stencil. Another study is similar to the previous one, and the QR code generated is more likely [48]. In the work, the message is embedded in the QR code, the QR code is encrypted and embedded in the top QR code, and the concept of hash values, hash algorithm usage, pseudo key usage, and variable size are the differences of this work. Occasionally, QR can be corrupted as a result of code manipulation (e.g., stamping (Image Steganography Application C#, 26.05.2018) as well as the corruption of the value of the code. There is no such problem in working.

The literature should be understood as a collective examination of the subordinate subheadings of the publications mentioned in relation to the QR code, not merely related to the subject concerned. For example, in [49], it is aimed to perform code authentication with QR codes together with hash functions, encryption, and steganographic techniques. This is generally seen in the context of security mechanisms.

2. Experimental Method

In the test environment, WCF, which is included in the editor of Visual Studio 2015 Professional, is used for web service. SOAP is used as the communication protocol, and communication is performed at the message level security layer. Because the web services are created in the environment client and server, the operations performed in the relevant sections are shown in the most basic form in Figure 2, and the client- and server-based operations in Figures 3 and 4 are listed.

Tests performed in the test environment are based on the lower value (the value contained in the QR code hidden

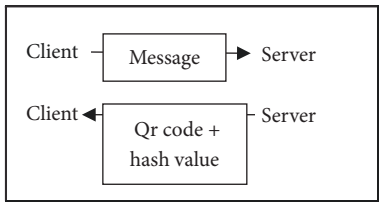


Figure 2: The general operation of the test environment processes (compose the hash value with the information to be obtained and compare it with the value sent to it).

in every visible QR code and decrypted as it appears in encrypted form), not over the transmitted value of the imager (the value contained in the QR code that appears everywhere).

Features of the computer used for testing are as follows: processor speed 2.3 GHz, 12 GB RAM, 1 TB memory, and 2 GB capacity display card. In the test environment, only the study period has been examined as an output variable and the size of the communication files resulting from the communication has not been examined. In the test process, up QR code contains "aaaaaaaaaa" string and hidden QR code contains "bbbbbbbbbb" string.

The test architecture will be examined separately as a server and a client. Here is the general outline of the process: converting a client request to the appropriate QR code format (hidden value is not tested in hidden or nonconfidential form), creating a hash value, accessing message content, and creating a hash value, hash values comparison, if the evaluation is positive.

Server-oriented operations include the following.

See Figure 3.

Client-oriented operations include the following.

See Figure 4.

The steps of the steganography algorithm used in creating and solving the image used in communication are as follows.

In order to convert the binary image into a binary image, the average of the R, G, B values of each pixel is taken as the value of the corresponding pixel of the grayscale image.

To obtain a bit sequence from the pixel array, the key value is first subjected to exponential processing with the pixel value, and the resulting value is converted into a bit sequence. Once the number of elements of this bit array is known, the array is converted to 1 and zero values. The index is reversed.

The elements of the bit array are summed, and the sum of the values is converted into a byte value to obtain the bit array. The converted value is subjected to exponential processing with key values and a new value is obtained.

Normal and QR code images to be stored are read and transferred to variables in the bitmap type. If the sizes of the two images are not the same, the size of the imager to be stored is equal to the size of the normal imager. The key value is read and the integer is stored in variable type. Message bits, Alpha-bits. Red bits, green bits, and blue bits. The new Alpha, the new red, the new green, and the new blue variables are initially created with a byte value of zero. The image is then passed to the encryption step.

In the image encryption step, the following operations are performed for each pixel in the image. The pixel value of the image to be hidden is read. The red component of the normal bit is read, and the message bits are transferred to the variable. The message bits are equal to the first and the first indexed elements of the variable are equal to the 6th and 7th indexed elements of the Alpha variable, and the second and third indexed elements are equal to the 6th and 7th indexed elements of the red bits variable. The 4th and 5th indexed elements are equal to the 6th and 7th indexed elements of the green bits' variable. The 6th and 7th indexed elements are equal to the 6th and 7th indexed elements of the blue bits' variable. Alpha bits, it's fried. Green and blue bits are equal to the image to be stored. In the decryption process, inverse operations are performed.

3. Results and Discussion of the Test

In this section tests made according to certain variables in the test environment will be examined on a variable basis. Variables were examined on a partition basis and at the end, the test environment was tried to be determined depending on the median of the variables. In Figures 5–12, the numbers in the x column and what they contain are reported in figure names.

When the subfigures of Figure 5 are examined, increasing the number of users for the same workload increases the working time. Therefore, it is advantageous for the users to communicate with the server that the user is not disconnected from the environment if the number of messages is likely to be large. But this advantage is fixed after a certain distance. This means that it is advantageous that clients who can receive services from the server more than a certain number of times are not disconnected from the environment. Because the strategy of disconnecting from the environment requires some security mechanisms at first to connect the user to the environment, the traffic in the environment is also increasing. For this reason, the transmission of the communication channel is falling.

When Figure 6 is examined, the number of messages for the variable client for the same workload is SHA512, the most appropriate hash algorithm in the client number combination. Although other algorithms are not considered similar in their runtime, nu has been chosen because the algorithm is the most secure (encryption key is longer). The algorithm can be used to develop a more secure hash algorithm that does not make a significant difference in the future work of the test.

Figure 7 shows that while size growth is a disadvantage in QR codes, communication over a single code is more advantageous than dividing the process if necessary.

When Figure 8 is examined, it is observed that the number of image layers is inversely related to the productivity in the test environment. However, the use of this feature in message communication at certain times does not affect the situation in which it can be used as a security mechanism.

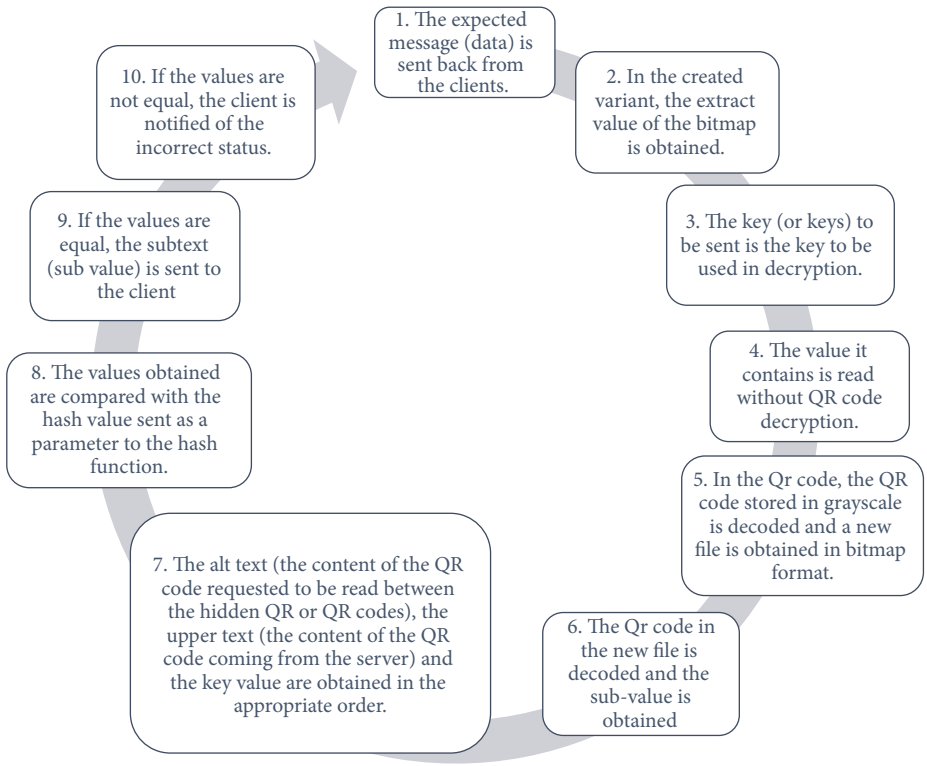


Figure 3: Server-side structured operations.

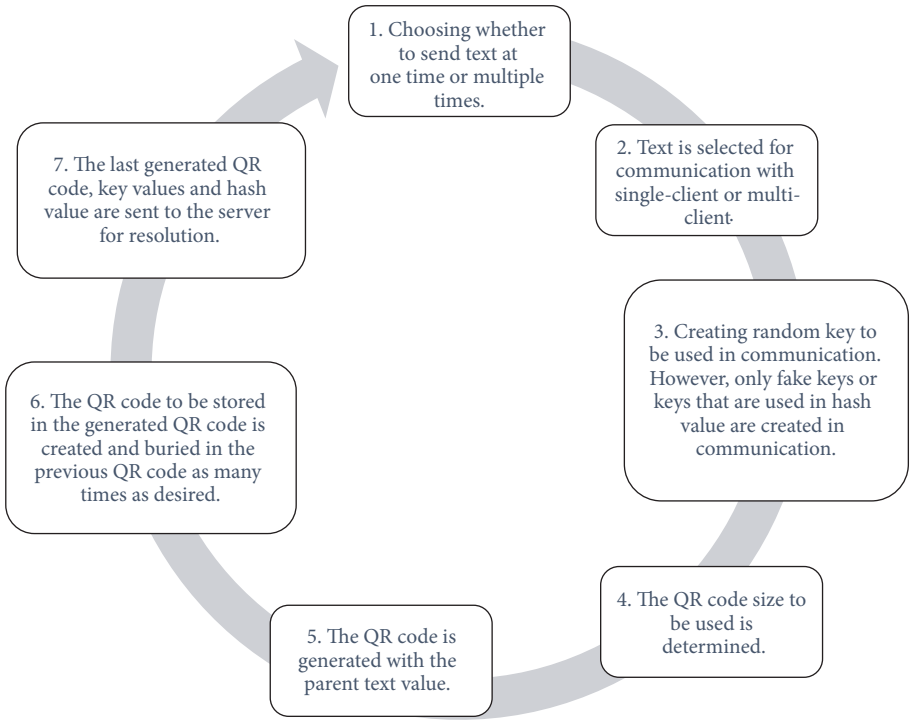
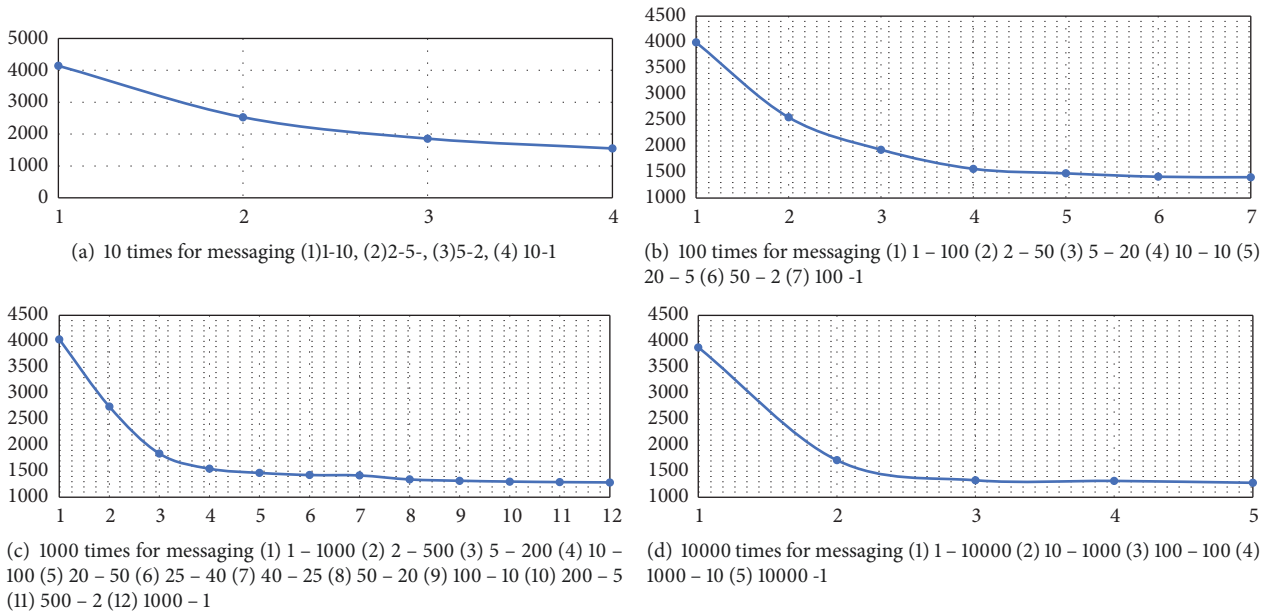


Figure 4: Client-side structured operations.



(a) 10 times for messaging (1)1-10, (2)2-5-, (3)5-2, (4) 10-1

(b) 100 times for messaging (1) 1 – 100 (2) 2 – 50 (3) 5 – 20 (4) 10 – 10 (5) 20 – 5 (6) 50 – 2 (7) 100 -1

(c) 1000 times for messaging (1) 1 – 1000 (2) 2 – 500 (3) 5 – 200 (4) 10 – 100 (5) 20 – 50 (6) 25 – 40 (7) 40 – 25 (8) 50 – 20 (9) 100 – 10 (10) 200 – 5 (11) 500 – 2 (12) 1000 – 1

(d) 10000 times for messaging (1) 1 – 10000 (2) 10 – 1000 (3) 100 – 100 (4) 1000 – 10 (5) 10000 -1

Figure 5: The number of clients for the test environment is related to the work size, the content of sample descriptions is the number of clients, in the form of messaging per client.

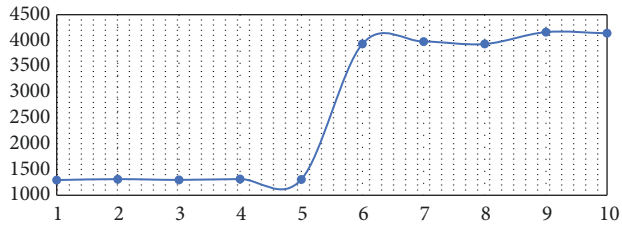


Figure 6: Sign algorithm efficiency study for the test environment, the number of messages for each client, the number of clients, the signing algorithm (1) 1000 - 1 - SHA512 (2) 1000 – 1 - SHA384 (3) 1000 – 1 – SHA256 (4) 1000 – 1 – SHA1 (5) 1000 – 1 - RIPEMD160 (6) 1– 1000 SHA512 (7) 1 – 1000 SHA384 (8) 1000 – 1 – SHA256 (9) 1000 – 1 – SHA1 (10) 1000 – 1 - RIPEMD160.

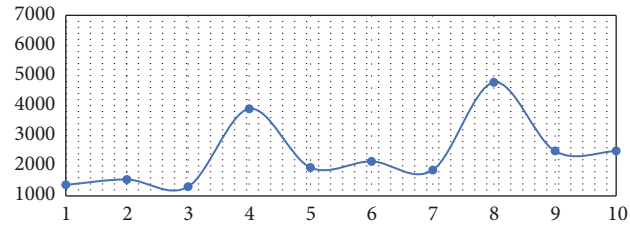


Figure 7: QR code size efficiency study for the test environment, the content of sample descriptions, the number of clients, the number of messages per client, the QR code size (1) 1000 – 1 – 10 (2) 10 – 100 – 10 (3) 100 – 10 - 10 (4) 1 – 1000 – 10 (5) 1000 – 1 – 12 (6) 10 – 100 – 12 (7) 100 – 10 - 12 (8) 1 – 1000 – 12 (9) 1000 – 1 – 14 (10) 10 – 100 – 14 (11) 100 – 10 - 14 (12) 1 – 1000 – 14 (13) 1000 – 1 – 16 (14) 10 – 100 – 16 (15) 100 – 10 - 16 (16) 1 – 1000 – 16.

Because of using the different number of image layers and using it as a parameter, the other party will be able to prevent attack by false QR codes sent as an attack by knowing the approximate value of the size of QR code to be formed with these parameters. It is more convenient to use this security acquisition as an auxiliary solution, not as a standalone solution.

In Figures 9 and 10, it can be underattended that if there is an image transmitted in the test environment and encrypted, the difference between unencrypted communications is not sufficient considering the advantages of the encrypted environment. So encrypted media should be preferred. It may be advantageous for clients that may be able to make another request for the same workload not to be disconnected from the media as much as possible.

When Figure 11 is examined, the running time of the encrypted environment is more variable. The minimum values are close to each other. The relationship between the

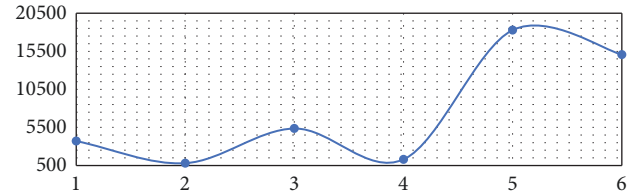


Figure 8: Image layer relationship for test environment, the number of layers included in the description of the sample, the number of clients, the number of messages per client (1) 1 – 1 – 1000 (2) 1 – 1000 -1 (3) 2 - 1 – 1000 (4) 2 – 1000 -1 (5) 32 - 1 – 1000 (6) 32 – 1000 -1.

values in the same test step is negligible. When all the load distribution in the system is examined, the encrypted communication for this test environment is not a disadvantage but it can be an advantage.

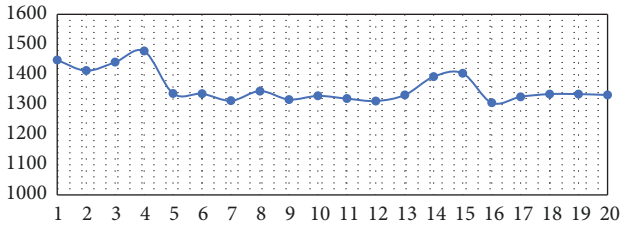


Figure 9: The text size for the unencrypted test environment is the length of the subtext of the content description, the width of the upper text, the average of the run time of the repetition numbers (1) 5 - 5- 10 (2) 5 – 10 - 10 (3) 10 - 5 - 10 (4) 10 – 10 - 10 (5) 5 – 5 - 100 (6) 5 – 10 – 100 (7) 10 – 5 – 100 (8) 10 - 10 – 100 (9) 5 – 5 – 1000 (10) 5 – 10 – 1000 (11) 10 – 5 – 1000 (12) 10 – 10 – 1000 (13) 5 – 5 – 2000 (14) 5 – 10 – 2000 (15) 10 – 5 – 2000 (16) 10 – 10 – 2000 (17) 5 – 5 – 4000 (18) 5 – 10 – 4000 (19) 10 – 5 - 4000 (20) 10 – 10- 4000.

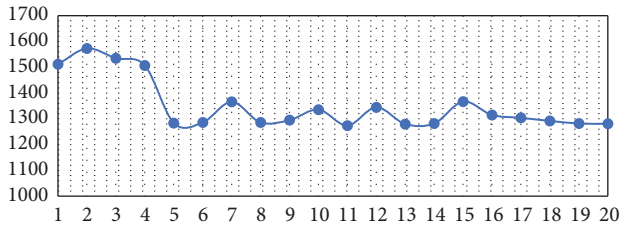


Figure 10: The text size for the unencrypted test environment is the length of the subtext of the content description, the width of the upper text, the average of the runtime of the repetition numbers.

When the test environment is repeated for the same business unit in the test environment, there will be an irregularity in the runtime. This is a case in the web service. When Figures 12(a) and 12(b) are examined, it is observed that there is no subtitle and upper text length for the test environment having the same conditions. The difference in working time is thought to be the irregularity of the working time of the system. This situation has been proven by Figure 12(b).

When all the conditions are examined, increasing the variables does not seem like a disadvantage, but it seems to be advantageous in situations where it is necessary or rather than dividing operations to increase the level of security. The disadvantage is that the incremental biased image layer greatly increases the working time of the test environment (according to the security level to be earned). This variable is suitable for testing clients at regular intervals when the requesting server communicates with a large number of clients.

4. Conclusion

The application strategies obtained when the test results are evaluated are as in Table 1.

The differences in the work from the other works can be as follows. It can be used with the encryption key of the desired length in the desired number. This key can be found in the non-QR information to be transmitted by adding the pseudo key (s), interleaved with various combinations. Hash messages can be obtained to be verified using the desired signing algorithm. It is usually advisable to hush extra messages in the work. Transmission can be done with the desired number of layered QR codes. The number of layers can be used as a parameter in an extra message. The desired size QR code is suitable for use. However, it is recommended to choose the smallest size that can accommodate the message to be sent. These features will allow applications to choose extra security features (which can be flexible depending on the features to be specified), specific to the group, specific to the user, or both.

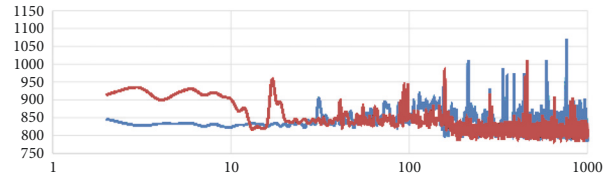
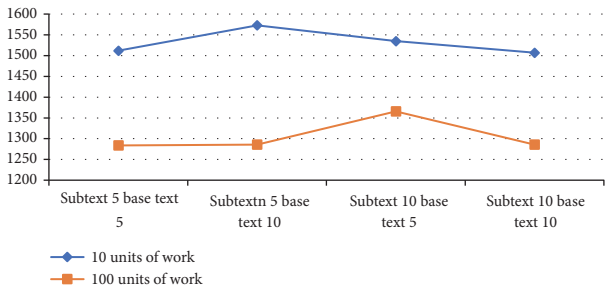


Figure 11: 100 times messaging for encrypted and unencrypted testing environment, working time, the processing sequence for other messaging except the first messaging, red encrypted media values, blue media-free media values, the horizontal axis is logarithmically ordered.

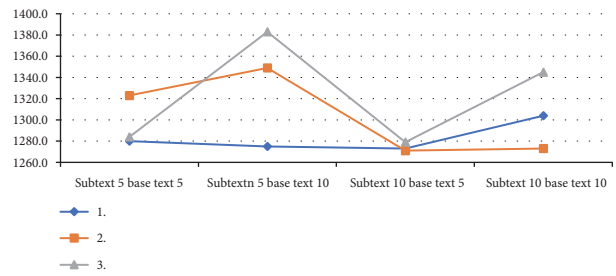
The biggest disadvantage of the work is that the QR code used must be created and used in a digital environment. That is, the desired features cannot be used with a printed QR code. As a further work, it is aimed to improve the conditions of security mechanisms in [50] and to work on printed QR codes.

Symbols

Ms:	Mile seconds
QR:	Quick Response
QR code:	Fact code (Quick Response code)
URL:	Uniform Resource Locator
SOA:	Service Oriented Architecture
SOAP:	Service Oriented Architecture Protocol
KB:	Kilobytes
HTTP:	Hypertext transfer protocol
RSA:	Public key cryptography
SHA:	Secure hashing algorithms
DES:	Data encryption standard
WCF:	Windows communication basics
XML:	Expandable mark-up language
RGB:	Red, green, blue
ASCII:	American Standard Coding System for Information Exchange
AES:	Advanced encryption standard
DES:	Data encryption standard
TripleDES:	Triple data encryption standard
GHz:	Gigahertz
RAM:	Random access memory
TB:	Terabyte
GB:	Gigabyte.



(a) 10 and 100 units of work (unit, how many times the number of messages is shown, the load per client is proportional to the unit work, and this ratio is fixed.



(b) Repetition of 1000 batches three times

Figure 12: Relationship between superscript and subtext lengths in an encrypted communication environment.

Table 1: Testing environment change and implementation strategy.

Test Environment Variable	Application Strategy
The number of clients for the test environment is related to the job size	More work should be done for the same workload as possible per client.
Relationship of a hash algorithm for test environment	The SHA512 algorithm can be selected.
The hash algorithm for the test environment QR code size relation	The lowest QR code should be preferred whenever possible.
Image layer relationship for test environment	If the number of layers is selected a lot, the working time is very long, so it can be used as a choice between low numbers.
Text size for unencrypted test environment the content of the related descriptions includes the length of the subtext, the length of the upper text	The effect of the length of the top and bottom text on the duration of the study is insignificant. This feature can be used because variable length selection affects hash value.
The text size relationship for the encrypted test environment, the length of the contents of the description subtext	It has the same conditions as the free environment. As a difference, there is a period of irregular working which comes from the encrypted environment itself.

Data Availability

The data used to support the findings of this study have been deposited in https://mega.nz/#F!vmQxUaqD!m0yKto6y_-Tk1QgU78sJBA.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] D. Berkey, "QR Codes for Dentists," *Dental Abstracts*, vol. 58, no. 3, pp. 116-117, 2013.

[2] C. Aktas, B. Çaycı, and C. Aktaş, "Qr Kodun Mobil Eğitimde Yeni Eğitim Yöntemlerinin Geliştirilmesine Katkısı," *Global Media Journal: Turkish Edition*, vol. 4, no. 7, 2013.

[3] S.-Y. Yang and C.-L. Hsu, "A location-based services and Google maps-based information master system for tour guiding," *Computers and Electrical Engineering*, vol. 54, pp. 87–105, 2016.

[4] W. M. Lim, P.-L. Teh, P. K. Ahmed, S.-N. Cheong, H.-C. Ling, and W.-J. Yap, "Going keyless for a seamless experience: Insights from a unified hotel access control system," *International Journal of Hospitality Management*, vol. 75, pp. 105–115, 2018.

[5] P. Nazemzadeh, D. Fontanelli, D. Macii, and L. Palopoli, "Indoor localization of mobile robots through QR code detection and dead reckoning data fusion," *IEEE/ASME Transactions on Mechatronics*, vol. 22, no. 6, pp. 2588–2599, 2017.

[6] Y. Qin, Z. Wang, H. Wang, and Q. Gong, "Binary image encryption in a joint transform correlator scheme by aid of run-length encoding and QR code," *Optics & Laser Technology*, vol. 103, pp. 93–98, 2018.

[7] Y. Xiaoyang, S. Yang, Y. Shuchun, Y. Yang, C. Hao, and G. Yanxia, "Research and achievement of QR code encryption based on cellular automata," in *Proceedings of the 2013 2nd International Conference on Measurement, Information and Control, ICMIC 2013*, pp. 314–318, China, August 2013.

[8] Y. Amit, Y. Surendra, and B. Brahmdutt, "A secure approach of image encryption using QR code on social media," in *Proceedings of the 3rd International Conference on Computing for Sustainable Global Development, INDIACom 2016*, pp. 1126–1129, India, March 2016.

[9] N. Goel, A. Sharma, and S. Goswami, "A way to secure a QR code: SQR," in *Proceedings of the Computing, Communication and Automation (ICCCA), 2017 International Conference*, pp. 494–497, 2017.

[10] P.-Y. Lin and Y.-H. Chen, "High payload secret hiding technology for QR codes," *Eurasip Journal on Image and Video Processing*, vol. 2017, no. 1, 2017.

[11] P. Survase and P. Survase, "Qr code based image steganography with enhanced image quality and compression," *International*

Journal for Innovative Research in Science and Technology, vol. 2, no. 5, pp. 104–112, 2015.

[12] D. Davis, "A Survey on Secret Data Hiding in Quick Response Barcodes," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7, no. 1, pp. 234–237, 2017.

[13] S. Sharma and V. Sejwar, "QR code steganography for multiple image and text hiding using improved RSA-3DWT algorithm," *International Journal of Security and Its Applications*, vol. 10, no. 7, pp. 393–406, 2016.

[14] Y. W. Chow, W. Susilo, J. Tonien, E. Vlahu-Gjorgievska, and G. Yang, "Cooperative Secret Sharing Using QR Codes and Symmetric Keys," *Symmetry*, vol. 10, no. 4, p. 95, 2018.

[15] P.-C. Huang, C.-C. Chang, and Y.-H. Li, "Sudoku-based secret sharing approach with cheater prevention using QR code," *Multimedia Tools and Applications*, pp. 1–20, 2018.

[16] M. Ramya and M. J. Sheela, "VLSI implementation of hybrid QR code generation system," in *Proceedings of the Electronics and Communication Systems (ICECS), 2014 International Conference*, pp. 1–6, 2014.

[17] J. Yu and S. Zhao, *Color QR Code with Pseudo Quantum Steganography and M-band Wavelet and Patch Group Prior based Denoising*, 2016.

[18] S. Sharma and V. Sejwar, "Impementation of QR Code Based Secure System for Information Sharing Using Matlab," in *Proceedings of the 8th International Conference on Computational Intelligence and Communication Networks, CICN 2016*, pp. 294–297, India, 2016.

[19] M. M. Rani and K. RosemaryEuphrasia, "Data Security Through QR Code Encryption and Steganography," *Advanced Computing: An International Journal*, vol. 7, no. 1/2, pp. 1–7, 2016.

[20] D. J. Ohana and N. Shashidhar, "QR code steganography. In Proceedings of the International Conference on Security and Management (SAM)," *The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp)*, p. 1, 2013.

[21] A. Choche and H. R. Arabnia, "A methodology to conceal QR codes for security applications," in *Proceedings of the the International Conference on Information and Knowledge Engineering (IKE'11)*, 2011.

[22] A. Warang and A. Patankar, *QR Code Based Image Steganography*, 2017.

[23] N. Singh and D. Sharma, *An Efficient Multiple Data Hiding Technique for Medical Images Using QR Code Authentication*, 2017, An Efficient Multiple Data Hiding Technique for Medical Images Using QR Code Authentication.

[24] C. Kavitha and S. Sakthivel, "An effective mechanism for medical images authentication using quick response code," *Cluster Computing*, pp. 1–8, 2018.

[25] P. P. Thulasidharan and M. S. Nair, "QR code based blind digital image watermarking with attack detection code," *AEÜ - International Journal of Electronics and Communications*, vol. 69, no. 7, pp. 1074–1084, 2015.

[26] J. Kim, N. Kim, D. Lee, S. Park, and S. Lee, "Watermarking two dimensional data object identifier for authenticated distribution of digital multimedia contents," *Signal Processing: Image Communication*, vol. 25, no. 8, pp. 559–576, 2010.

[27] C. Patvardhan, P. Kumar, and C. Vasantha Lakshmi, "Effective Color image watermarking scheme using YCbCr color space and QR code," *Multimedia Tools and Applications*, pp. 1–23, 2017.

[28] V. Malathi, B. Balamurugan, and S. Eshwar, "Achieving privacy and security using QR code by means of encryption technique in ATM," in *Proceedings of the 2nd International Conference on Recent Trends and Challenges in Computational Models, ICRTCCM 2017*, pp. 281–285, India, February 2017.

[29] W. M. Randall and N. S. Rickard, "Reasons for personal music listening: A mobile experience sampling study of emotional outcomes," *Psychology of Music*, vol. 45, no. 4, pp. 479–495, 2017.

[30] K. Navin, A. Shanthini, and M. M. Krishnan, "A mobile based smart attendance system framework for tracking field personals using a novel QR code based technique," in *Proceedings of Smart Technologies For Smart Nation (SmartTechCon), 2017 International Conference*, pp. 1540–1543, 2017.

[31] M. Zhang, Z. Ma, Y. Zhang, and Y. Wang, "An identity authentication scheme based on cloud computing environment," *Multimedia Tools and Applications*, vol. 77, no. 4, pp. 4283–4294, 2018.

[32] R. K. Sungkur, V. Neermul, and V. Tauckoor, "Exploring the educational potential of QR codes," in *Proceedings of the 3rd International Conference on Advances in Computing, Communication and Engineering, ICACCE 2016*, pp. 368–373, South Africa, 2016.

[33] B. Rodrigues, A. Chaudhari, and S. More, "Two factor verification using QR-code: A unique authentication system for Android smartphone users," in *Proceedings of the 2nd International Conference on Contemporary Computing and Informatics, IC3I 2016*, pp. 457–462, India, 2016.

[34] M. E. V. Melgar and L. A. Melgar Santander, "An alternative proposal of tracking products using digital signatures and QR codes," in *Proceedings of the 2014 IEEE Colombian Conference on Communications and Computing, COLCOM 2014*, Colombia, 2014.

[35] J. R. Mahajan and N. N. Patil, "Alpha channel for integrity verification using digital signature on reversible watermarking QR," in *Proceedings of the 1st International Conference on Computing, Communication, Control and Automation, ICCUBEA 2015*, pp. 602–606, India, February 2015.

[36] S.-J. Liu, J. Zhang, J.-S. Pan, and C.-J. Weng, "SVQR: A novel secure visual quick response code and its anti-counterfeiting solution," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 5, pp. 1132–1140, 2017.

[37] https://www.scopus.com/search/form.uri?display=basic.

[38] https://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=qr+code.

[39] https://scholar.google.com.tr/scholar?hl=tr&as_sdt=0%2C5&q=qr+code&btnG=.

[40] https://login.webofknowledge.com.

[41] J. H. Kim, M. Kim, T. Yang, I. Kim, J. Seo, and S. Kang, "Compressed QR code-based mobile voice guidance service for the visually disabled," in *Proceedings of the Advanced Communication Technology (ICACT), 2018 20th International Conference*, pp. 423–425, 2018.

[42] S. Li, J. Shang, Z. Duan, and J. Huang, "Fast detection method of quick response code based on run-length coding," *IET Image Processing*, vol. 12, no. 4, pp. 546–551, 2018.

[43] S. K. Chatterjee, S. Saha, Z. Khalid, H. N. Saha, P. Paul, and R. Karlose, "Space effective and encrypted QR code with sender authorized security levels," in *Proceedings of Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual*, pp. 439–443, 2018.

[44] Y. Cheng, Z. Fu, and B. Yu, "Improved Visual Secret Sharing Scheme for QR Code Applications," *IEEE Transactions on Information Forensics and Security*, 2018.

[45] A. Paverd, S. Tamrakar, H. L. Nguyen et al., "OmniShare: Encrypted Cloud Storage for the Multi-Device Era," *IEEE Internet Computing*, 2018.

[46] M. J. Snyder, D. R. Nguyen, J. J. Womack et al., "Testing quick response (QR) codes as an innovation to improve feedback among geographically- separated clerkship sites," *Journal of Family Medicine*, vol. 50, no. 3, pp. 188–194, 2018.

[47] B. Karthikeyan, A. C. Kosaraju, and S. Sudeep Gupta, "Enhanced security in steganography using encryption and Quick Response code," in *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016*, pp. 2308–2312, India, March 2016.

[48] S. Dey, K. Mondal, J. Nath, and A. Nath, "Advanced steganography algorithm using randomized intermediate QR KOD host embedded with any encrypted secret message: ASA_QR KOD algorithm," *International Journal of Modern Education and Computer Science*, vol. 4, no. 6, p. 59, 2012.

[49] C. Chen, "QR Code Authentication with Embedded Message Authentication Code," *Mobile Networks and Applications*, vol. 22, no. 3, pp. 383–394, 2017.

[50] G. K. Hong and S. Sinha, *Tracking Vulnerable People Using Body Worn QR Code*, 2018.