LABORATORY ACCESS IMPLEMENTING QR CODE AUTHENTICATION USING OTP

Sghaier Chaabani, Abdulrahman Almuhaidib, Hussain Alsalem, Faisal Alotaibi, Mohsen Bamardouf, Ibrahim Abukhamseen, Hussain AlGallaf, Yosef Aljwaid, Abdulrahman Alharby and Hussain Alattas

srchabani@iau.edu.sa, asmalmuhaidib@iau.edu.sa, aalharby@iau.edu.sa, htalattas@iau.edu.sa

College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia.

ABSTRACT

Laboratories in colleges are used to give lectures to students, but what about after working hours? Students can get many benefits from these labs after working hours. For example, students can study and do their homework after working hours. In this project, we have proposed a new technique to control the access of these laboratories. Our idea is to use an encrypted QR code with an TOTP authentication that will be connected to LAN network to guarantee that each student enter can only use a single PC. Each student will have his own encrypted QR code that differs from other students. The TOTP code will be sent to student's university email. The encryption method used encrypted method used AES encryption to encrypt the data inside the QR code to guarantee the confidentiality, integrity, non-repudiation, and authenticity of the date.

KEYWORDS

Security, QR Code, Access control, embedded systems, image detection, OTP

1. INTRODUCTION

(Sumit Tiwari, 2016) & (Zhanna et al, 2022) stated that QR (Quick Response) code is a two-dimensional code that can store up to 4000 characters of data. It is designed to be read by phone cameras. This data is usually encoded in the form of white and black squares, it is encoded using specific programs. It decodes the data very quickly and that's why it's called Quick Response. In this paper we talked all about QR codes, how are they formed, what's the structure of it, and the history of the QR code.

The QR code is a very useful tool, and it gained its popularity over the years. However, it is not the best tool to use if you want to build a secure system. In order to fix that, we can add a new layer of security to it to be more secure. OTP (One Time Password) is a technique that's used to generate a password, only to be used one time, then it will be invalid. By complimenting QR code with OTP, we will have a reliable secure system.

Dhinaharan Nagamalai (Eds): EMVL, EDUT, SECURA, AIIoT, CSSE -2023
pp. 121-141, 2023. IJCI – 2023 DOI:10.5121/ijci.2023.120511

1.1. Problem Statement

Colleges have laboratories that used for teaching during working hours. To make more use of these laboratories after working hours, students can use these labs to study and do their homework. In order to control the access of these laboratories, we need a safe way to ensure that these laboratories are not used by unauthorized users.

1.2. Background

QR codes have grown in popularity in many different uses. Despite the many benefits they provide, QR codes have serious security concerns. For example, attackers can encrypt harmful links that take users to phishing websites. The attacker will than generate the malicious QR code and replace it with legitimate ones. The most common attack scenario to inject QR codes is by using social engineering. The skill of persuading others to expose sensitive information is referred to social engineering. There are two main approaches hackers use to attack QR codes. The attacker replaces the entire QR code with a new one that he made, or the attacker modifies part of the QR code, so the victim will be redirected to another link.

The uses of QR codes can be found in various of fields like advertising, mobile payments, access control, augmented reality, and navigation. One of the most common usability is in advertisement. Generating QR codes for URLs or contact details, geographic locations, and content to make them readily available to the user is the most frequent application in the field of advertising. QR codes are also used to conduct mobile payments and offer the ability to purchase a product or service by only scanning a QR code. After scanning the QR code the user will be redirected to the payment agent. Another filed is access control, QR codes are used in conjunction with other security improving measures for physical access control.

1.3. Justification

Many students want to study at the laboratories of the college after working hours, but the problem is that they need to register their fingers print to access the laboratories by their fingers print. The process of register each student fingerprint takes long time and cost a lot. Instead of depending on the fingers print, we can depend on the QR code of the student IDs and one time password to verify the student identity, after that the student will be allowed to use only a single PC.

2. RELATED WORKS

2.1. QR Code History

Before the technology of QR and barcode, it was hard for people to track and control their business. QR code history has a lot of difficulties like the beginning of using barcode with certain benefit limitation developing it to solve these limitations took 20 years. Inventing such technology helped people save time and resources using a simple code that hold a set of information.

2.1.1. QR Code Creation

In this paper (Pandey, 2008) proposed QR codes is unique invention it helped organization in marketing and advertisement, they can be used to help characterize and organize products, and it can be used to help customers to access the needed information they want by simply scanning QR

with their phone camera. Before QR codes they invented barcodes developed in Japan by Denso Wave and Masahiro Hara. They worked on it to help grow the Japanese supermarkets to keep track of their products, because of that cashier now move faster than before due to fast scanning product rather than writing them manually.

2.1.2. Barcodes Characteristics

In this paper (Gao, Prakash, & Jagatesan, 2007) shows that barcode technology is a parallel lines and numbers that represent data, first appearance of barcodes on June 26, 1974. First implemented in supermarkets to store products data then slowly other logistics companies started using it to tag their shipment and products. A linear barcode is a means to encode data so that it may be read, recovered, analysed, and authenticated by computer systems. It comprises a series of lines and gaps of different lengths.

The invention of barcodes, it can record a lot of information in a compact space to enhance dissemination of information without the need for querying a database, thought it has a great benefit, it also has disadvantages like it need special complex scanner tool, also it does not permit read and write, and it can hold only 20 alphanumeric. These issues raised the need for QR development to solve these problems.

2.1.3. QR Code Generations

In paper (Mary, 2022) QR code stand for quick response code, which as the name indicate it was high-speed reading technology, after the barcode succeeded in supermarkets a need for high speed, and capacity technology are needed. In 1994 Denso Corporation developed QR code to solve the issues that barcode faced. Auto companies implemented QR code in their electronic parts for transportation so they can track shipments and scan them fast without the need for low level technology scanners. Organizations form different sectors adopted this technology to control their products.

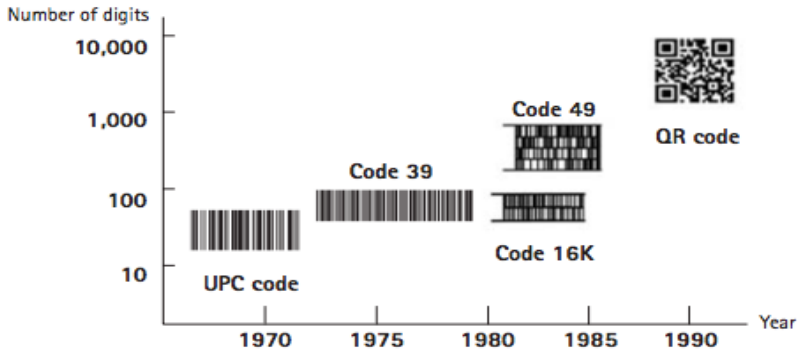

Figure 1. Evolution of Barcode to QR Code (Mary, 2022).

Figure1 shows the timeline from barcode to QR code in 1994, barcode had evolved from 1970 till late 1985 containing UPC as the first invention of barcode due to capacity limit. New variations have been developed until barcode Code 49 which was the last barcode. It holds the capacity close to 900 alphanumeric. After Denso expansion of this technology using his final variation QR code quick reader and holds more than 7,000 characters. Denso Technology helped companies and government to control their assets from 1994 up until this day QR code is still used due to its easy usage and data storage.

2.2. QR Structure

QR structure constate of dark squares on lights squares. the squares modules are arranged in the function is used for. There is regular square array, function patterns and Data area. The whole module should be surrounded by quite zone (Sumit Tiwari,2016) (Mishra and Mathuria, 2017).

Figure 2. QR code of IAU website

2.2.1. Function Patterns

There are four function patterns in QR code. Their main function is to help the QR scanner to scan when there is problem in QR code. such as the missing part or disorder of the QR paper. There also more special area In QR which will explain next (Mishra and Mathuria, 2017).

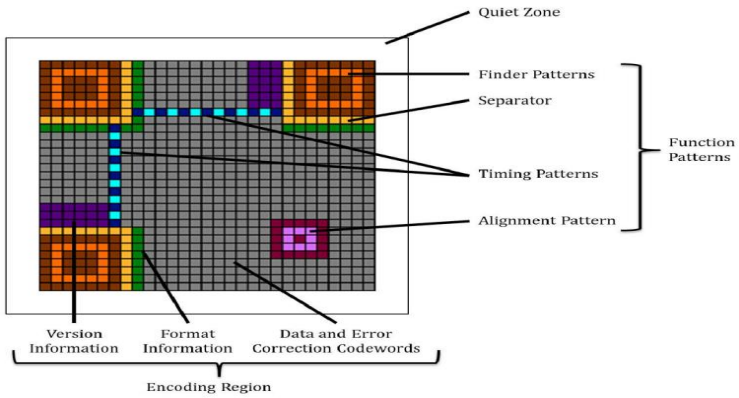

Figure 3. QR function patterns (Sumit Tiwari,2016).

Finder pattern: the finder pattern is design to help the QR scanner to accurately positioning the QR code for decoding. It is found in three corners (upper left, upper right, and lower left). It consists of two dark square in the centre and the outer area, and inner light square.

Separators: a light area separate the finder pattern and the code area.
Timing pattern: two patterns fixed in horizontal and vertical line between separators. It helps fixed the model coordination if the symbol is distorted.

Alignment patterns: it has similar shape to find pattern but with smaller size.it appear in QR code with larger size, and there can one alignment pattern or more deponed on the size of QR code. It helps in fixing the nonlinear distortion.

Encoding Region (Data Area): the QR information will sorted as binary numbers of 0 and 1.it will change to black and white cells. This will also have the reed-Solomon codes which helps QR scanner to correct error as missing part form QR code.

Quiet Zone: it makes sure the QR scanner does not include other text when scanning the QR code.

Format Information: it takes 15 bit of size and it store information of selected masking pattern and error correction level.

Version Information: store the QR code version that has been used.

2.2.2. QR code version and capacity

The QR code difference symbol version range from version1 to version40.there is difference module configuration for each version of QR code. The size of QR codes can be in the smallest is 21x21 pixels(version1), and the largest can be is 177x177 pixels(version40). It can store high amount of data in small size as shown in table1(Sumit Tiwari,2016).

Table 1. QR code Capacity(version40)

Data type	Data capacity (at maximum)
Numeric only	7,089
Alphanumeric	4,296
Binary (8 bits)	2,953
Kanji characters	1,817

2.2.3. QR code error correction

The QR code has high tolerance of damage as it uses Reed–Solomon error correction, which is code able to restore the damage happened to the QR code. It has four level restoration can be depended on the environment QR code use in it. For example, in environment where the QR code can be dirty or damaged it is recommended to use level Q (25%) or H (30%). Level L (7%) is selected when the code containing large amount of data and in save environment. In most case, the Level M (15%) is used.

Table 2. The Level of error restoration

Level	The Approx area restored
L	7%
M	15%
Q	25%
H	30%

2.3. QR Encryption

With the advancement of technology comes the easiness of use in all aspects. From authentication to authorization and more. QR code stores large amount of data vertically and horizontally for the user and organization. Thus, in our project well not just be implementing QR code for access but enhance its security with encryption. So that people's data are preserved and only the authorized people are allowed to enter. With that choosing the right algorithm is just as important for its security, fast performance, and uninterrupted experience for the user (S. R. M. Mary and E. K.Rosemary, 2016).

In this paper (Prerna Mahajan & Abhishek Sachdeva, 2013) presented the most known encryption algorithms which are the DES, AES, and RSA and compare between them. In DES (data encryption standard) the algorithm is moderate using a one key algorithm where the data is split and goes into permutation and Oxer for 16 rounds to be encrypted. AS for RSA (Rivest-Shamir-Adleman) algorithm it uses asymmetric key encryption being slower where it generates the private key using a large prime number to encrypt the data. On the receiving side the receiver

uses the public key to decrypt and get the received data. Finally, the AES is the fastest uses symmetric key encryption encrypting the data in blocks of 128 bits and up to 256 bits. After encrypting each block individually, it fuses them together after specified rounds getting the encrypted output desired.

2.3.1. Des Encrypted QR

(Hong, Y, 2020) argues that traditional access control systems are insecure as keys can be misplaced and lost. As well Magnetic cards demagnetized and getting an IC card with a CPU chip is expensive to get and maintain. Not forgetting biometric authentication which is costly and can have problems in the long run. That is why the author proposes an access control system using QR code encrypted with DES (Data Encryption Standard). Implementing an android application, server, and embedded control system.

The android application generates the encrypted QR code after the user enters his password he sets. The QR code can be sent to unauthorized users but is time limited to one minute to prevent misuse. The access control system identifies the QR code, records who enters and provide monitoring remotely. To read the code the QR need to be close for the infrared sensors to examine it. If it is validated the door will be open record the time the user accessed, it. For monitoring the camera is used and send suspicious findings and alarm to the web page. For the server it manages the records of information as well as that of multi doors and users. Electronic gates, user privileges can be added and deleted.

For monitoring, the pictures taken by the control system goes through the server. The QR code is stacked of two-dimension bar codes and matrix 2D with each width and length matters for the data. With the code system being code 49 for example for barcode and binary for matrix 1 for dots and 0 is empty. That is how it achieves high information capacity and reliability. Encrypting the code goes by using base64 encrypting every string of data using subkeys rotation of the string into blocks and repeated 16 times before the result of encrypted QR code.

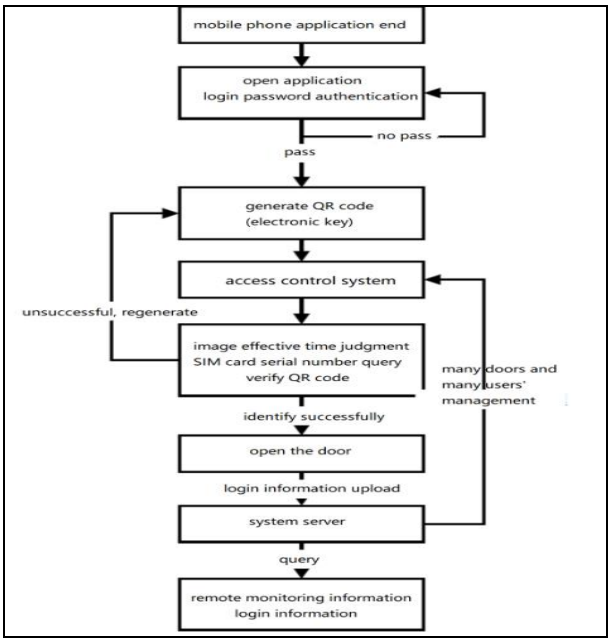

Figure 4. DES Encryption. (Hong, Y, 2020)

2.3.2. Rsa Encrypted QR otp

(Susukailo, V & Lakh, Y, 2018) States that QR technology have spread for its easiness and conveniency in sharing information everywhere. That is why QR code need to be secure through encryption and one time password to prevent the theft of sensitive information of users and organizations. Thus, the author proposes a system that encrypts the code with RSA and use OTP for extra security. The author used NetBeans 8.1 to implement the encryption of RSA with pseudorandom using the java function secure random. Furthermore, his solution made use of a mobile application, private server and QR scanner and reader for hardware.

As for software he used a computer application to generate the encrypted QR code. The code is only valid for half a minute and the system only accessible to security personnel. The solution works by authorizing the ID of the user to create the encrypted QR which is then stored on the server. Then authenticating the QR by the QR reader if it matches the one in the server then the user will get access.

The solution was compared in its performance against multiple operating systems from Linux to iOS and it turns out iOS has the fastest response time. The RSA QR is the best to use as it is highly dynamic in its access. With every QR encrypted differently which secures the access and prevent unauthorized attempts the most unlike biometric which can be copied or the plastic card that can be lost as well as the code panel. While the QR will be in the smartphone, so it is always in the hands of the intended person.

Table 3. Comparison of Different Access Control Systems (Susukailo, V & Lakh, Y, 2018)

Technology	**Characteristics**		
	Type of password	***Number of possible***	***Storage medium authorization***
Using QR-code encryption	Dynamic	10^{7098}	Mobile Gadgets
Biometric data reader	Static	–	Employee
Plastic card reader	Static	10^{30}	Plastic Card
Code panel	Static	2000	Employee

2.3.3. EQR with AES otp

(Cheong, S, et al, 2017) Indicates that hotel self-service technologies using barcodes is not enough to reduce a queue specially during the holiday season. Thus, he proposes a solution that extends the self-service with encrypted QR not only for a customer check in but for the room access as well. The scheme has two phases which are cryptography and the generation of the encrypted QR for check in and hotel room access that can be sent to customers beforehand after they booked the rooms. Allowing the encrypted QR (EQR) to act as digital keys in the process.

The solution implements a hotel management system for booking and room access control. A QR generator, a self-service kiosk, and a QR reader at the room door. Based on the user credential during booking the EQR will be generated specifically sent for him and saved in the system server. The person credentials will be used as an OTP which will be also encrypted using AES for maximum security during check in which is valid for one use. A key of 256 bits sizes along with a password chosen by the admin.

A simple SSK is implemented using a raspberry pi, a monitor, a CSMOS camera and a metal oxide semiconductor. The raspberry pi can be used to decode the EQR as its connected to the network and camera. If the EQR is genuine the OTP will be generated and after its inputted, it will be decrypted to allow access to the customer after it sent for verification to the management system. If its valid it will update the status and the customer will get his information on screen about his booking and his EQR will open his room when he scans it by the reader in front of his room. Then it sends to the management server the guest is authenticated and sends a signal for the door to unlock using the authentication module installed the door will be open. An experiment was conducted, and the resulting survey indicates ease of use, the requirement of little use and usefulness of the prototype solution with a mean above 6 which is satisfactory for the guests.

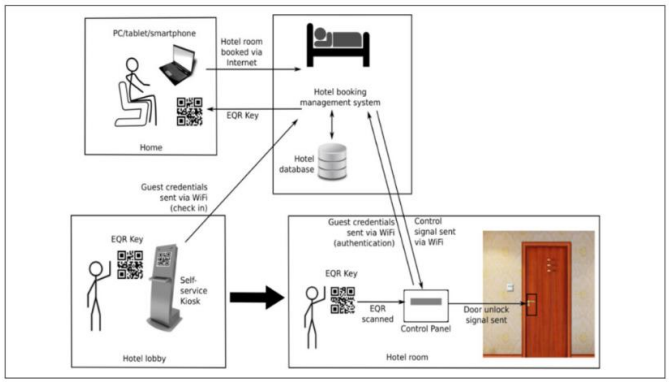

Figure 5. EQR with AES OTP (Cheong, S, et al, 2017).

2.4. OTP

A one-time password (OTP) provides a way to log into services with a unique password that can only be used once. This simple idea adds a new layer of security to your system. Having OTP in your system will prevent a lot of attacks by default, we will talk about some of the attacks in the coming sections. OTP has two methods of authentication. HOTP and TOTP, both methods are considered secure and reliable. However, TOTP priorities the security more while HOTP has more usability.

2.4.1. OTP Introduction

There exists a massive number of services and accounts on the internet and its rapidly growing. Trustworthy user authentication methods are necessary for security reasons. OTP systems provide the most efficient way to protect sensitive data. Even though OTP schemes increase the security of authentication through a variety of algorithmic extensions and customizations, some concessions need to be made, especially since systems that tolerate vulnerabilities too much often have large computational and storage requirements.

The OTP system's architecture can vary depending on the purpose and the vulnerabilities to known attacks. The most popular and effective OTP systems are discussed in this paper and assessed in terms of performance efficiency and resistance to security assaults. The findings demonstrated a correlation between an OTP system's security level, storage requirements and computational efficiency (Ioannis Tzemos, 2016).

The purpose of OTP is to prevent an unauthorized third-party who have credentials that has been stolen from another user. Using advanced authentication techniques to securely establish a client's identity is a possible solution to this problem. in the first decade of the twenty-first century, it was demonstrated that it is possible to hack an elementary OTP scheme such as single-DES. As a result, OTP schemes, such as HMAC-based OTP (HOTP), used A one-way hash function with collision-resistant properties for enhanced security.

However, even with the best security measures in place, schemes can have limitations that compromise security, necessitating their replacement or replacement. By allowing different authentication channels, An OTP system can use its functionality to improve the security. there exist devices with advanced operating systems that are using less storage space than traditional devices. As a result, these devices can be great to use as OTP devices. (Ioannis Tzemos, 2016).

2.4.2. Attacks that can be prevented by OTP

Paper in (Lina et al., 2020) stated that because many users' requests access to services and protected data, users are being forced to set a complex password when registering, this results in a trade-off in usability (remembering complex passwords may be hard) that a lot of users will not do, especially older people. This leads users to bypass mechanisms because it is too complex for them. Due to that they are allowing their systems vulnerable to attacks resulting in flows in the security of the system. (loannis, 2016)

The One Time Password (OTP) approach is an effective technique to reduce the gap between usability and security while preventing known security attacks. We can divide the attacks that can be prevented into three categories, eavesdropping, denial of service and offline dictionary attacks target users with weak passwords. By default, these types of attacks present some risk that any simple password authentication solution should be able to handle. Also, dictionary attacks are the main reason for implementing password policies, an example of this attack is shown in figure 6. (loannis, 2016)

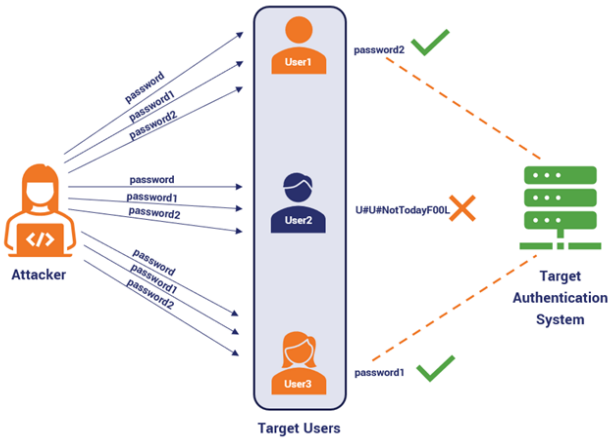

Figure 6. How a Dictionary attack work. (Crane, 2021)

Eavesdropping is another type of attack that increases the potential risk to your system. An example of eavesdropping is shown in Figure 7. If an attacker wants to capture (eavesdrop on) sensitive data, he must know how to read your network traffic. OTP strategies can mitigate eavesdropping attempts by adding cryptographic algorithms that generate private keys in a manner that is considered secure. (loannis, 2016)

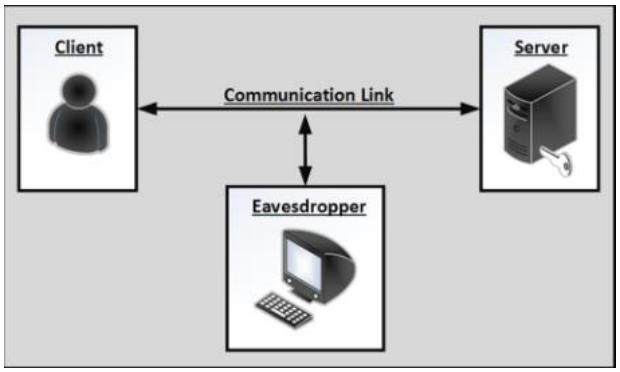

Figure 7. An example of Eavesdropping attack (Ioannis Tzemos, 2016).

Another attack is Denial of Service attacks it is an attempt to render the entire system so that the system becomes incapable of responding to queries. Such attacks target any existing system weakness, no matter how little or large it is. An example is shown in figure 8. (loannis, 2016)

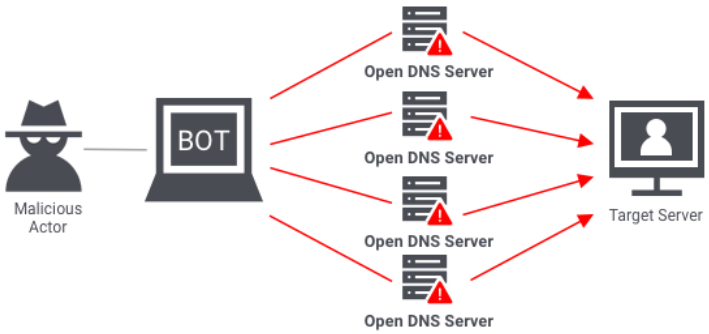

Figure 8. How DDOS attack work. (Thompson, 2020)

2.4.3. OTP Methods (HOTP and TOTP)

Before joining a network, it is essential to consider granting authorization, making resources available, and validating a user's identity. Authentication and authorization execute these actions. In this research, the focus is on one-time password methods HOTP (HMAC-Based One-Time Password) and TOTP (Time-Based One-Time Password) authentication techniques. One-time password is a unique set of characters that you will need to enter once only.

The generated password is only usable for a single login and cannot be used again. Password randomness is an important factor in security, and therefore passwords using this type of format are often used in authentication algorithms. The main difference between the HOTP and TOTP algorithms is that in HOTP only hash functions are used, while in TOTP method time is included at the beginning of the hash. Which algorithm to use can differ based in the situation and the environment. (Lina et al., 2021)

To access the network and its services, you must first authenticate yourself. Authentication involves recognizing an individual's identity. That is, determining whether someone or something is who they say they are. Usually a set of credentials (username, password) is used to verify this. The authentication procedure guarantees that the user has the appropriate permissions to access the required service.

Authentication and authorization are two procedures that always interact with one another and their always interdependent. Now let us focus on analysing the authentication process. Users often create easy to guess passwords so that they can remember it, because of that the password will be easy to guess. When accessing systems holding sensitive data, username and password authentication does not offer enough security. (Lina et al., 2021)

Systems that require more robust security should use authentication methods that require combinations of usernames, passwords, and other credentials. His two-factor authentication with username and password can also be used, which increases the security of the service. This authentication method adds a new layer of security that makes it more difficult for attackers to access your device online. Added. An attacker would also need to be aware of other parts of the authentication process. (Lina et al., 2021)

2.4.3.1. HOTP Algorithm

HOTP is an algorithm based on HMAC discovered in 2005 by David M'Raihi and his team. Hash functions are an essential component of current cryptography. These are functions that can transform a long message into a fixed-length sequence of bits. To encrypt and sign data, asymmetrical algorithms and hash functions are frequently employed in tandem. A modern hash function must be both trustworthy and efficient in terms of computation.

A one-way function is a type of function whose output is based on the input but cannot reverse the process. SHA families are one of the most common hash functions, and they are characterized by small changes in the message leading to large changes in the message leading to large changes in the density of the message. You can see how the algorithm works in Figure 9 (Lina et al., 2021).

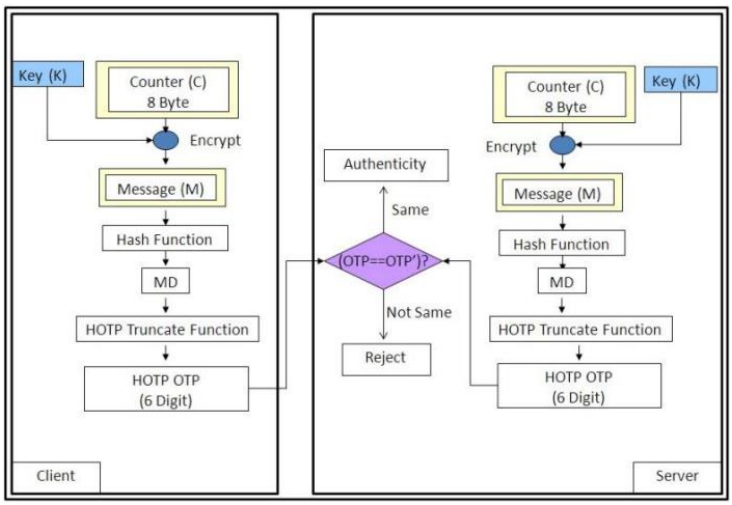

Figure 9. How HOTP works. (Lina et al., 2021)

Hash-based massage authentication code is a method of generating cryptography using a hash function. You can use MD5, SHA-1 or any other hash with your private key to generate a secure message authentication token. HMAC is similar to a digital signature. Both maintain integrity and authenticity. Both make use of cryptographic keys along with hash algorithms functions. The primary distinction of digital signature and HMAC is that HMAC employs a symmetric key whereas digital signature employs an asymmetric key. Hash-based MACs use two hash paths to create a measure of security. The private key is used to obtain two keys, the inner key and the outer key.

This algorithm generates a strong hash that comes from the message and the private key. The first pass rule generates a hash value based entirely on the message and its associated internal key. The second pass generates the latest HMAC code from the resulting internal and outer key hashes. (Lina et al., 2021)

$$\text{HMAC}(K, m) = H((Kj \oplus \text{opad}) \parallel H((Kj \oplus \text{ipad}) \parallel m)) \quad (1)$$

H stands for hash function, m stands for message to authenticate, K stands for private key, Kj stands for block length key generated from the private key, Opad stands for outer padding, and ipad stands for internal padding. (Lina et al., 2021)

HOTP is generated using an incrementing counter and a static symmetric key known only to the security device and validation server. HOTP values use HMAC-SHA-1. This is an algorithm that accepts a data set of any size and returns a value of 160 bits long. (Lina et al., 2021)

$$\text{HOTP}(K, \text{counter}) = \text{HMAC - SHA-1}(K, \text{counter})$$

Both server and purchaser proportion K as a mystery key. The counter is an 8-byte fee counter and the HOTP generator (purchaser) counter have to be synchronized with the HOTP validator (server). The ensuing truncated fee have to be dynamically truncated the usage of a unique truncate characteristic. HOTP values are one hundred sixty bits and 20 bytes long. Then use the DT characteristic to generate a 4-byte string. Examples of DT features:

$$\text{arSbits} = \text{DT}(\text{HMAC - SHA-1}(K, \text{counter}))$$

This will return a bit string of 31 we can recalculate the HOTP outcome by means of

$$\text{Snum} = \text{StToNum}(\text{Sbits})$$

Here we are converting a string to a number. Extract 4 bytes of dynamic binary from a 160-bit (20 bytes) HMAC SHA-1 result using offset dynamic truncation.

The server counter value only increments after a successful HOTP authentication. The token count increases each time the user makes a new her HOTP request. As a result, the server and token counter values may be out of sync. This means that the counter needs to be reset so that it is correct again. The only way to solve this problem is to set a parameter on the server. The server can recalculate the HOTP value for the next session and compare it with the received HOTP client. (Lina et al., 2021)

2.4.3.2. TOTP Algorithm

In an article (Lina et al., 2021), they defined TOTP as a one-time password set of rules that makes use of the contemporary time because the supply of uniqueness. The TOTP set of rules is a

model of the HOTP set of rules. Unlike his HOTP which makes use of a counter, OTP is time dependent. TOTP makes use of both HMAC-SHA-256 or HMAC-SHA-512. TOTP may be written as: TOTP = HOTP (K, T) T can be represented as:

$$T = (CurrentUNIXTime - T0)/X$$

X is the number of time steps in seconds (default is 30) and the UNIX time to start counting time steps is T0.

The authorization server cannot reliably determine when the OTP was generated. Network latency can cause the gap (number of time steps between OTP creation and receipt by validator) to be too large. Validation systems should have a policy regarding acceptable OTP transmission delay times. The greater the distance between two points, the greater the risk of attack. In general, it is recommended that the delay time be less than 1 step size. An example of TOTP is shown in Figure 10. (Lina et al., 2021)

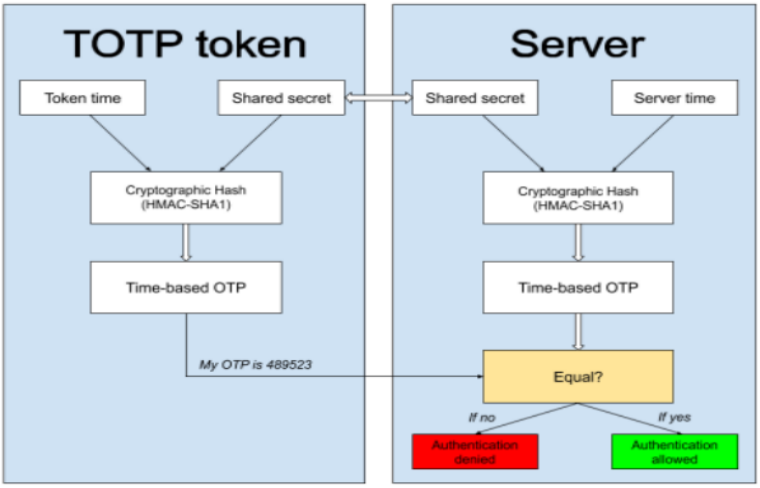

Figure 10. How TOTP works. (Lina et al., 2021)

The security of TOTP highly depends on the interval as mentioned, the larger the interval is the more it reduces the security of the system. Aim to keep the interval as small as possible. Also, TOTP algorithm is based on the HOTP algorithm, which means that its security depends on the HOTP parameters, and they both share a lot of rules together. (Lina et al., 2021)

2.4.3.3. Comparison between HOTP and TOTP

The study (Lina et al., 2021) argued that the HOTP method required two pieces in order to perform properly. First component is a secret key accessible to the token as well as the server only, which authenticates the provided OTP codes. The moving factor is the second piece of information. It is a counter in HOTP. Both tokens and servers store the counter. The token's counter which increases when the button is clicked differs from the server's counter which only increases when an OTP is authenticated successfully.

TOTP is developed based on HOTP, however the moving component in TOTP is time rather than a counter, which is the fundamental distinction between the two algorithms. TOTP uses timestamps which usually last somewhere between 30 to 60 seconds. If the timestamp time finish the OTP is no longer valid. Where in HOTP there is no time limit, the code is valid till you use it.

HOTP servers allow a wide variety of OTPs. The server will receive an OTP generated by a counter that is within a predetermined number of increments of the prior counter value. The validation is a rejected if the token counter is beyond the server domain, and the token must be resynchronized. Both TOTP and HOTP are consider secure, however TOTP is more secure. (Lina et al., 2021)

(Shushan Zhao & Wenhui Hu, 2018) Argued that while both HOTP and TOTP are more secure than not employing MFA, each has its own set of constraints and advantages. TOTP is simple to use and execute, but the time-based component includes the risk of time-drift (the delay between password creation and use). If the user does not input the TOTP quickly, it may expire before they do. So, the server must account for the user's prior activities and make it simple for them to retry the TOTP prosses again without kicking the user out.

HOTP is more user-friendly because it does not have a time-based restriction, but it is more vulnerable to brute force attack. HOTP code is valid for longer time and the probability of the password working increases with the length of the HOTP's validity, that is why it is vulnerable to brute force attack. It can be challenging to distinguish between these two kinds of OTP because certain HOTP vulnerabilities have been brought on by the addition of a time-based component to their code.

2.5. Text Detection

Nowadays, technology is evolving and entering data to the database manually is considered a tedious work we have decided in our project to use text detection to fill the database by feeding it the extracted names and IDs of students from an image. The concept of detecting a text inside an image is challenging due to many factors such as different type of text font and size, image clarity and varied in lighting situations. Text detection has been taken priority as in many studies have addressed different methods to handle these challenges. (Chen et al., 2011)

2.5.1. Stroke Width Transform

Paper (Epshtein et al, 2010) uses connected component (CC)-based approach, which uses Stroke Width Transform. the characteristic that distinguishes a text from other element in the environment that it has a constant stroke width with geometric reasoning a text detection can be achieved. Figure 14 shows that operator can be used to differentiate between a text as it has a constant stroke width and element with high frequency. Element with the same width can be grouped to form what probably to be a text.

Figure 14. operator output (Epshtein et al, 2010)

The method for how Stroke Width Transform (SWT) works illustrated in figure 15 it computes the pixel stroke that happens by calculating the distance between a to q resulting in w which the width. the next stage is to use the return of SWT which is an image containing the width of each pixel which probably a stroke grouping these to from a letter candidate. Grouping can be achieved if two contiguous pixels have the same width. Elements with the small size or too big will not detected.

The knowledge learned from training set, is that the size of the text from 10 to 300 will be detected. The next stage is to collect these letters candidate and group them as one letter will not usually be shown alone in image and this logic gives opportunity to eliminate random noise. Another logic is the space between letter are consider as when it written by a computer will have identical space and when written by human will have similar ratio space. The final stage is to use a heuristic the calculate ratio space between letters and if that ration has significant increase sperate it into new word.

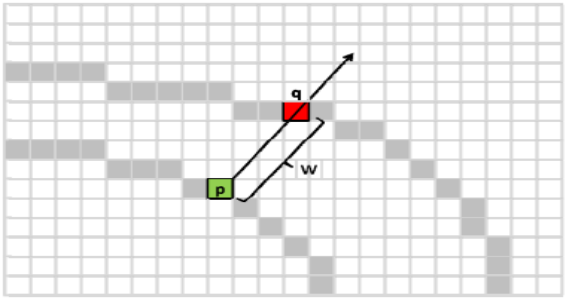

Figure 15. SWT calculassions (Epshtein et al, 2010)

2.5.2. Snooper Text

Paper (Minetto, et al, 2010) uses hybrid method approach proposed a hybrid scheme merging two strategies which are bottom-up and top-down. The scheme is provided in figure 16, the SnooperText method use data set generated by hypothesis and comparing them against complementary strategy. The Snooper Text algorithm is comprised of three stages: image segmentation, character classification and character grouping. The image segmentation stages use morphological work and toggle mapping. To enhance the contrast of the image toggle mapping takes place which performs mapping between functions and a set function.

A set of similar regions is produced as an output of image segmentation. To distinguish a text region from other regions classification strategy has been used. Descriptors are placed in different regions. Descriptors used: Fourier, polar and PZM. To distinguish text regions from non-text regions SVM classifier used at the first level there are three different descriptors classifiers produces three outputs the finals output is produced by margining these three outputs.

The last stage is grouping step which can be achieved by using text hypotheses. To obtain text region within image all identified letters are grouped together with their contiguous letters. Text region with no neighbours is removed this needed to identify words and eliminate the possibility of false positive. Finally, a box is generated and placed on the image which then passed to as input to the hypothesis validation.

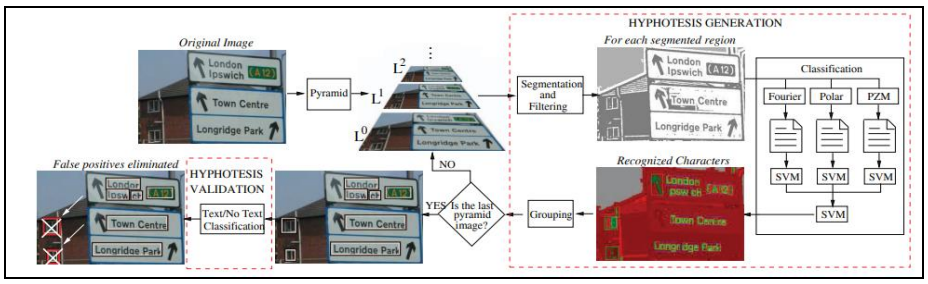

Figure 16. SnooperText scheme (Minetto et al, 2010)

Since false positive can occur as in the previous stages are just analysing the content of an image here where we use hypothesis validation to handle these issues. hypothesis validation depends on global descriptors to validate the box. Global descriptors introduced to be complementary to the descriptors of previous stages. Hypothesis validation recognize non-text boxes that falsely generated in the earlier stages and begin to remove them as shown in figure 17.

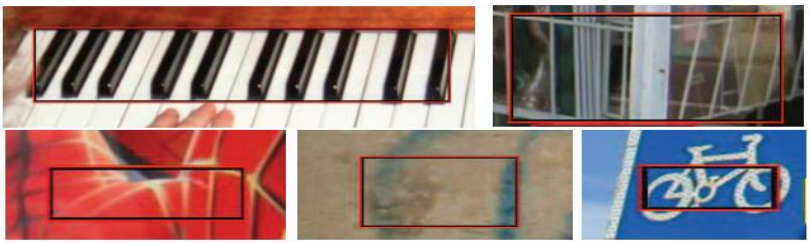

Figure 17. Hypothesis validation recognition of non-text box (Minetto et al, 2010)

2.5.3. Edge-Enhanced Maximally Stable External Regions (Edge-enhanced-MSER)

Paper (Chen, et al., 2011) uses connected component (CC)-based approach, which uses Maximally Stable External Regions (MSER). For more efficient and reliable result, it is necessary to build the stroke width image of these location using the distance transform. Both geometric and stroke width filters are applied to find a CC match. Additionally, examinations on clustered letters are performed to produce a reliable result and to remove false positive. These text detection steps used are shown in figure 18.

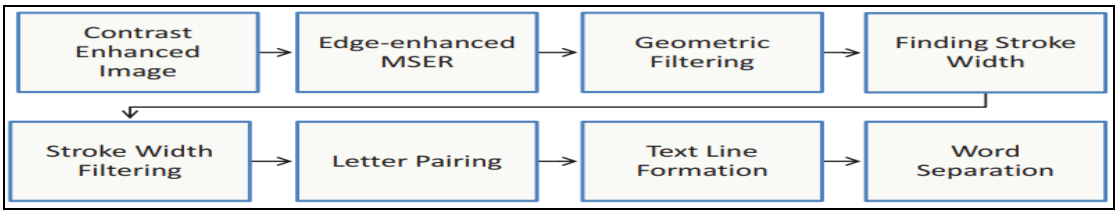

Figure 18. Text detection flowchart (Chen et al., 2011)

Given that the intensity contrast between text and its backdrop is often strong and that it is reasonable to presume that each letter has a consistent intensity or colour, MSER is good choice to detect a text. The negative side about MSER is that it is sensitive to image blur as shown in figure 19 various letters are considered as the same letter due to blur image. To handle the issue of blur images Canny edges proposed to complement MSER producing Edge-enhanced MSER. It enhances the outline of external regions and eliminate MSER pixels that is out of the scope. Edge-enhanced MSER is shown in figure 20 has individual representation of letters.

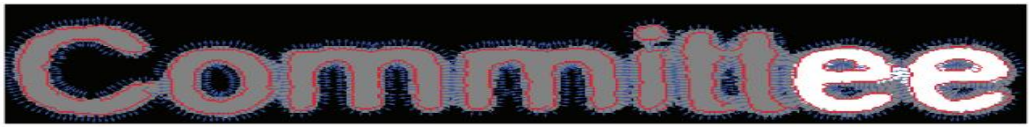

Figure 19. MSER representation (Chen et al., 2011)

Figure 20. Edge-enhanced MSER representation (Chen et al., 2011)

2.5.4. OpenCV (Open-Source Computer Vision) and Tesseract

Paper (Palekar et al., 2017) introduce the implementation of image processing using OpenCV and Tesseract. Tesseract used to convert image to a text. Using this software directly could lead to false reading, particularly if the content of the image is not clear. OpenCV (Open-Source Computer Vision) software were introduced to solve this issue. It offers a set of function that help in processing an image then processed image is fed to Tesseract software.

Testing the algorithm in real world action as shown in figure 21 were an image of license plate taken from camera. In figure 21 shows the look of an image after thresholding was applied. In this image most of the character are clearly visible however when Tesseract used alone the extracted characters were “MHo’2cz 5712” the inverted comma was taken by mistake as there is a single stray above letter “o” in the plate and some characters were recognized as small letters while they are capital.

Figure 21. Image taken from a camera before and after applying threshold (Palekar et al., 2017)

When OpenCV is used to process the image and then the result is fed to Tesseract. it produces successful result as shown in figure 21. The inverted comma that was falsely identified has been filtered out and the characters were recognized as small letters while they are capital are converted to uppercase. Text detection using OpenCV, and Tesseract has gotten 88.3% precision rating and 76.8% recall rating (Goel et al., 2019).

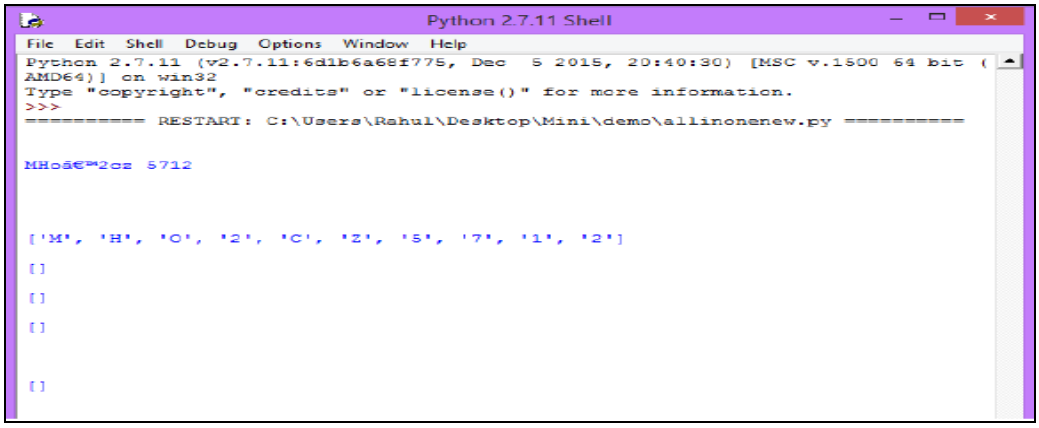

Figure 22. result of OpenCV and Tesseract (Palekar et al., 2017)

3. COMPARISON AND GAP ANALYSIS

Table 4. Encryption methods comparison.

Reference	Technique	Level of Security	Speed	Encryption	Key Size	Rounds
(Hong, Y, 2020)	DES	Adequate	Moderate	Weak	56 bits	16
(Susukailo, V & Lakh, Y, 2018)	RSA	Least secure	Slow	High	N/A	N/A
(Cheong, S, et al, 2017)	AES	Excellent	Faster	Excellent	128,192,256 bits	N/A
(Prerna Mahajan & Abhishek Sachdeva, 2013)	DES	Not Secure	Fast	Moderate	56 bits	16
	RSA	Least Secure	Fast	Slow	>1024 bits	1
	AES	Excellent Secured	Fast	Fast	192,128,256 bits	10,12,14

Based on (Susukailo, V & Lakh, Y, 2018) and the comparison between RSA, DES, and AES methods, although RSA method is easy to implement, AES is faster and more secure than RSA and DES. Thus, using AES algorithm to encrypt data, will enhanced the secrecy of data without any noticed delay.

AES encryptions have a variety of implementations as it can be used with different key sizes. The keys ranging from 128,192 and 256 bits and depending on these sizes, the number of rounds is adjusted. Being 10, 2, or 14 rounds to accommodate the best security for the key size. Where the round consists of a byte substitution of the data, which is changing of the data transforming it, shifting its rows, multiplying it by a matrix and finally adding the round key which is the key split to the number of rounds needed.

Table 5. HOTP and TOTP comparison.

Reference	Method	Level of Security	Technique speed	OTP duration	Average server response time
(Amna & Tawfiq, 2014)	HOTP	Secure	Low	Long	1.75 second
	TOTP	More Secure	High	Short	1.25 second
(Lina et al., 2021)	HOTP	Secure	N/A	Long	N/A
	TOTP	More Secure	N/A	Short	N/A

In paper (Amna & Tawfiq, 2014) they executed an experiment to check for the server response time. Ten alternative examples are suggested in order to test server response time. These examples demonstrate how rapidly the server answers to each system user's request. The average response time for each approach was calculated by the authors. According to the data in the table, HOTP's average response time is 1.75 seconds, whereas TOTP's average response time is 1.25 seconds. We concluded that TOTP's average response time is lower than HOTP's.

Based on (Lina et al., 2021), (Amna & Tawfiq, 2014) research and their comparison between HOTP and TOTP both papers concluded that TOTP is more secure than HOTP and is faster in the authentication prosses. The server response time is also less in TOTP which makes it more efficient based on (Amna & Tawfiq, 2014) experiment. Therefore, we are going to implement TOTP in our project as an authentication algorithm.

3.1. Recommendations for Future Works

As a future work, we can enhance the performance of our application by providing a full automated system, that can verify the student ID card then generate a QR code without any action from the admin.

4. CONCLUSION

In this project, we have proposed a technique to control the access of these laboratories. The idea is to use an encrypted QR code with an OTP authentication that will be connected to LAN network to guarantee that each student enter can only use a single PC. The system of generated QR code would be automated, so when a student requests the QR code through our website, the QR code would be sent it to his or her email. After that they can use it easily to enter the lab and do the verification steps to enter the lab.

REFERENCES

[1] D. Pandey, "Three QR Code," Academia, 2008. [Online]. Available: https://www.academia.edu/31427962/Three_QR_Code. [Accessed 30 September 2022].

[2] J. Z. Gao, L. Prakash and R. Jagatesan, "Understanding 2D-BarCode Technology and Applications in M-Commerce - Design and Implementation of A 2D Barcode Processing Solution," IEEE Xplore, 27 July 2007. [Online]. Available: https://ieeexplore.ieee.org/document/4291101. [Accessed 30 September 2022].

[3] G. Mary, "The Use of Quick Response (QR) Codes and Its Benefits to the Online Selling: An Action Research," Zenodo, 18 July 2022. [Online]. Available: https://zenodo.org/record/6853623. [Accessed 30 September 2022].

[4] Tiwri, S., 2016. An Introduction to QR Code Technology. [online] ResearchGate. Available at: <https://www.researchgate.net/publication/318125149_An_Introduction_to_QR_Code_Technology> [Accessed 4 April 2016].

[5] Mishra, A. and Mathuria, M., 2017. A Review on QR Code. International Journal of Computer Applications, 164(9), pp.17-19.
[6] Hong, Y., 2020. Design of Intelligent Access Control System Based on DES Encrypted QR Code. 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA).
[7] Susukailo, V. and Lakh, Y., 2018. Access Control System Based on Encryption in QR-Code Technology. 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS).
[8] Cheong, S., Ling, H., Teh, P., Ahmed, P. and Yap, W., 2017. Encrypted quick response scheme for hotel check-in and access control system. International Journal of Engineering Business Management, 9, p.184797901772003.
[9] S. R. M. Mary and E. K.Rosemary, "Data Security Through Qr Code Encryption And Steganography," Advanced Computing: An International Journal, vol. 7, no. 1/2, pp. 1–7, Mar. 2016. Accessed: Oct. 8, 2022. [Online]. Available: https://doi.org/10.5121/acij.2016.7201
[10] A. P. F. N. S. Ioannis Tzemos, "Security and Efficiency Analysis of One Time Password," Greece, 2016.
[11] J. D. S. A. H. M. T. V. D. Lina Lumburovska, "A Comparative Analysis of HOTP and TOTP Authentication Algorithms. Which one to choose?," Scientific Technical Union of Mechanical Engineering" Industry 4.0", 2021.
[12] C. Crane, "A Brute Force Attack Definition & Look at How Brute Force Works," 18 June 2021. [Online].
[13] A. Thompson, "What Is a DDoS Attack?," 2 November 2020. [Online].
[14] H. Chen, S. Tsai, G. Schroth, D. Chen, R. Grzeszczuk and B. Girod, "Robust text detection in natural images with edge-enhanced Maximally Stable Extremal Regions", 2011 18th IEEE International Conference on Image Processing, 2011. Available: 10.1109/icip.2011.6116200 [Accessed 27 September 2022].
[15] B. Epshtein, E. Ofek and Y. Wexler, "Detecting text in natural scenes with stroke width transform", 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2010. Available: 10.1109/cvpr.2010.5540041 [Accessed 27 September 2022].
[16] R. Minetto, N. Thome, M. Cord, J. Fabrizio and B. Marcotegui, "Snoopertext: A multiresolution system for text detection in complex visual scenes", 2010 IEEE International Conference on Image Processing, 2010. Available: 10.1109/icip.2010.5651761 [Accessed 27 September 2022].
[17] R. Palekar, S. Parab, D. Parikh and V. Kamble, "Real time license plate detection using openCV and tesseract", 2017 International Conference on Communication and Signal Processing (ICCSP), 2017. Available: 10.1109/iccsp.2017.8286778 [Accessed 6 October 2022].
[18] V. Goel, V. Kumar, A. Jaggi and P. Nagrath, "Text Extraction from Natural Scene Images using OpenCV and CNN", International Journal of Information Technology and Computer Science, vol. 11, no. 9, pp. 48-54, 2019. Available: 10.5815/ijitcs.2019.09.06 [Accessed 6 October 2022].
[19] N. K. V. L. Zhanna Deineko, "QR Code as an Element of Educational Activity," 2022.
[20] C. Chen, “QR code authentication with embedded message authentication code,” Mobile Networks and Applications, vol. 22, no. 3, pp. 383–394, 2016.
[21] S. Dey, A. Nath and S. Agarwal, "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System," IEEE Xplore, 10 June 2013. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6524449. [Accessed 27 October 2022].
[22] M. Warasart and P. Kuacharoen, “aper-Based Document Authentication Using Digital Signature and QR Code,” 2012 4 th International Conference on Computer Engineering and Technology (ICCET 2012), vol. 40, pp. 1–5, 2012.
[23] T. S. B. Amna S.M Abukeshipa, "Implementation and Comparison of OTP Techniques (TOTP,HOTP,CROTP) to Prevent Replay Attack in RADIUS Protocol," 1 June 2014. [Online]. [Accessed 1 November 2022].
[24] W. H. Shushan Zhao, "Improvement on OTP authentication and a possession-based authentication framework," 2 November 2018. [Online]. [Accessed 2 November 2022].