

DESIGN AND IMPLEMENTATION OF A SECURE QR PAYMENT SYSTEM BASED ON VISUAL CRYPTOGRAPHY

SEMINAR REPORT

SUBMITTED

TO

**AWH ENGINEERING COLLEGE
KUTTIKKATTOOR, KOZHIKODE - 8**

**IN PARTIAL FULFILMENT
OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE
OF**

Master Of Computer Applications

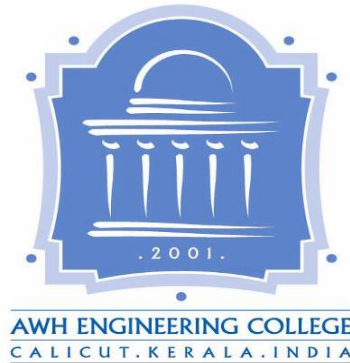
BY

AHAMMED HANI K



**DEPARTMENT OF COMPUTER APPLICATIONS
AWH ENGINEERING COLLEGE KUTTIKKATTOOR,
KOZHIKODE
MAY 2024**

DEPARTMENT OF COMPUTER APPLICATIONS



AWH ENGINEERING COLLEGE KOZHIKODE

CERTIFICATE

This is to certify that this seminar entitled “Design and Implementation of a Secure QR Payment System Based on Visual Cryptography” submitted herewith is an authentic record of the seminar work done by Ahammed Hani K (AWH22MCA-2003) under our guidance in partial fulfillment of the requirements for the award of Master of Computer Applications from APJ Abdul Kalam Technological University during the academic year 2024.

Head of the Department

Mrs. Sruti Sudevan

Assistant Professor

Dept. of Computer Applications

Seminar Co-ordinator

Ms. Prajina K

Assistant Professor

Dept. of Computer Applications

ACKNOWLEDGEMENT

I express my sincere gratitude to our beloved principal **Dr. Sabeena M V** for providing me an opportunity with the required facilities for doing this seminar. I express my hearty thanks to **Mrs. Sruti Sudevan**, Head of the Department of Computer Application and **Ms. Prajina K**, Assistant Professor Department of Computer Applications and seminar Co-ordinator for her guidance and advice. I am thankful to all other staff of the MCA department for their encouragement, timely guidance, valuable suggestions and inspiring ideas given throughout this seminar. I am grateful to my friends for the way they have cooperated, expected me to achieve success and have always stirred my ambition to do the best. Above all, I am grateful to the almighty, who has showered His blessings on me throughout my life and throughout the seminar.

AHAMMED HANI K

ABSTRACT

QR codes have been extensively used in recent years since they speed up the payment process and provide users with ultimate convenience. However, as convenient as they may sound, QR-based online payment systems are vulnerable to different types of attacks. Therefore, transaction processing needs to be secure enough to protect the integrity and confidentiality of every payment process. Moreover, the online payment system must provide authenticity for both the sender and receiver of each transaction. In this paper, the security of the proposed QR-based system is provided using visual cryptography. The proposed system consists of a mobile application and a payment gateway server that implements visual cryptography. The application provides a simple and user-friendly interface for users to carry out payment transactions in user-friendly secure environment.

CONTENTS

	Page No
1. INTRODUCTION	1
2. LITERATURE SURVEY	2
3. QR CODE	4
3.1 Design	4
3.2 Storage	4
3.3 Error Correction	5
3.4 Structure	6
3.4.1 Finder Pattern	7
3.4.2 Separators	7
3.4.3 Timing Patterns	7
3.4.4 Alignment Patterns	7
3.4.5 Encoding Region	8
3.4.6 Quiet Zone	8
3.5 Encoding	8
3.5.1 Data Analysis	9
3.5.2 Data Encoding	9
3.5.3 Error Correction Coding	9
3.5.4 Structure Final Message	9
3.5.5 Module Placement in Matrix	9
3.5.6 Data Masking	10
3.5.7 Format and Version Information	10
3.6 Decoding	10
3.6.1 Recognizing Module	11
3.6.2 Extract Format Information	11
3.6.3 Determine Version Information	11
3.6.4 Release Nasking	11

3.6.5	Restore Data and Error Correction Codewords	11
3.6.6	Error Detection and Correction	11
3.6.7	Decode Data Codewords	11
4.	VISUAL CRYPTOGRAPHY	12
4.1	Application of Visual Cryptography	13
4.1.1	Watermarking	13
4.1.2	Anti-Phishing System	13
4.1.3	Human Machine Identification	13
4.1.4	Secure Banking Communication	13
4.1.5	Defense System	13
4.1.6	CAPTCHA	13
4.1.7	Offline QR Code Authorization	14
4.2	VC Scheme	14
4.2.1	Types of Shares	14
4.2.2	Share Flexibility	16
4.2.3	Number of Secrets	18
5.	METHODOLOGY	19
6.	NEW SCHEME OF VISUAL CRYPTOGRAPHY ON THE QR CODE SECURITY	21
6.1	Collection of the C0 and C1 Encoding Matrix	21
6.2	Example Technique-Based XAI	21
6.3	Selecting the Basic Matrix	21
6.3.1	Rule for Creating Sharing Picture A	21
6.3.2	Rule for Creating Sharing Picture B	21
6.4	Hidden Picture Reconstructed	22
7.	PROPOSED SYSTEM DESIGN	24
7.1	Functional Description	24
7.2	Security Considerations	25
8.	SYSTEM IMPLEMENTATION	27

9. RESULT ANALYSIS	28
10. CONCLUSION	30
11. FUTURE SCOPE	31
12. BIBLIOGRAPHY	32

1. INTRODUCTION

The rapid expansion of online payment solutions has revolutionized transaction processes, leading to the emergence of innovative applications. From credit cards to NFC-based payments, the digitalization of payment systems has opened new possibilities. However, this progress comes with inherent security concerns, as evidenced by the potential threats of theft, fraud, and impersonation in online transactions. In response to these challenges, various secure QR-based online payment options have been developed, employing models like the Operator Centric Model and the Peer-to-Peer Model. These models utilize public and private keys in transactions, aiming to enhance security and ensure the confidentiality, integrity, and availability of the payment system.

This paper proposes a secure QR code-based online payment system, leveraging a comparative analysis between public key cryptography and visual cryptography as security measures. While public key cryptography presents challenges such as the need for third-party certificate validation and secure key storage, visual cryptography offers advantages such as enhanced secrecy, integrity, and authentication without the transmission of personal information. The proposed payment method focuses on transmitting data-carrying QR codes, emphasizing the protection of the QR code itself. With the integration of steganography and cryptographic algorithms, visual cryptography emerges as a robust technique to secure the visual data represented by the QR code, addressing the evolving security needs of the digital payment landscape.

2. LITERATURE SURVEY

The quick response (QR) code is a useful tool for mobile phone users. The code may be photographed using a smartphone camera and then decoded using a special reader software. The code specifically denotes brief text, contact details, or a web link. Its availability makes keypad typing on phones easier for consumers. This paper suggests a method for paying for on-street parking that is based on an E-QR bill's code. Consumers can think of the code as a bill to pay their parking charge, with the parking details being entered by the fee collectors into a distant server. The major goal of this technique is resource conservation, such as lowering paper usage. The suggested smartphone application offers a new method for Taiwanese on-street parking E-bill payment, according to simulation findings. Also, the aforementioned application acts as a role model for various parking payment methods. A rapid response (QR) code is a helpful tool for those who use mobile phones. The code may be captured using the smartphone camera and then decrypted using a specialized reader application.

Basheer, Amen, & Sawsan Kamal. (2016). A Novel Technique Using QR Codes to Decode a Message: Here. Another information-concealing computation that we've shown totally converts the message to OR code (Quick Response Code) and creates OR for cover (Key). Since OR Codes have greater or much larger capacity restrictions than other ordinary normal standard identifications, they are typically utilised to transmit or store communications. The authors of the current study have described an encryption method that involves first scrambling a message by XORing a section (series of parts) of a QR message with a related piece of OR veil Kev, and then inserting the Kev into the generated QR.

"An Introduction to QR Code Technology," S. Tiwari:

A two-dimensional network code called "Quick Response" is set up by keeping two feasible focuses. As an example. When distinguished from ID-normalized differentiating pieces of proof, it has to hold enormous amounts of information (data), and any portable device, like a phone, should be able to swiftly decode it. The whole range of benefits offered by QR codes includes high information store capacity, rapid verification, omnidirectional clarity, error correction (so that a broken code may still be read correctly), and many

alternatives. Depending on their requirements, customers can select from a number of QR code image collections, including logo QR codes, scrambled QR codes, and iQR Code.

By X. Yan and Y. Lu, they applied the QR code to secure medical management:

Here, we'll show how a protected payment system with OR codes was planned and implemented. These OR codes are really very popular since they speed up the payment procedure and provide the customers a tonne of ease. Despite how beneficial it may appear, QR-based online payment systems are susceptible to a variety of attacks. This will ensure that exchange handling is sufficiently secure to protect each payment cycle's integrity and privacy. Also, the online payment system should provide authenticity to both the seller and the buyer in every transaction. Here, picture cryptography is used to demonstrate how secure the suggested QR based architecture is. The app provides customers with a clear and simple interface that is easy to use in a safe environment.

3. QR CODE

QR code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. Four standardized encoding modes (numeric, alphanumeric, and byte/binary) could be stored as QR for efficient data storage. The QR Code system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. Applications include product tracking, item identification, time tracking, document management, and general marketing.

A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera, scanner, etc.) and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns that are present in both horizontal and vertical components of the image.

3.1 Design

Unlike the older, one-dimensional barcodes that were designed to be mechanically scanned by a narrow beam of light, a QR code is detected by a 2-dimensional digital image sensor and then digitally analyzed by a programmed processor. The processor locates the three distinctive squares at the corners of the QR code image, using a smaller square (or multiple squares) near the fourth corner to normalize the image for size, orientation, and angle of viewing. The small dots throughout the QR code are then converted to binary numbers and validated with an error-correcting algorithm.

3.2 Storage

The amount of data that could be stored in the QR code symbol depends on the data type (mode, or input character set), version (1, ..., 40, indicating the overall dimensions of the symbol), and error correction level. The maximum storage capacities occur for 40-L symbols (version 40, error correction level L) as shown in table (1):

Input mode	max. characters	bits/char	possible characters, default encoding
Numeric only	7,089	3⅓	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Alphanumeric	4,296	5½	0–9, A–Z (upper-case only), space, \$, %, *, +, -, ., /, :
Binary/byte	2,953	8	ISO 8859-1

Table 1. Maximum character storage capacity (40-L)

3.3 Error Correction

Codewords are 8 bits long and use the Reed–Solomon error correction algorithm with four error correction levels. The higher the error correction level, the less storage capacity. The following table lists the approximate error correction capability at each of the four levels as declared in table (2):

Level L (Low)	7% of codewords can be restored.
Level M (Medium)	15% of codewords can be restored.
Level Q (Quartile)[7]	25% of codewords can be restored.
Level H (High)	30% of codewords can be restored.

Table 2. Errors correction levels & it's storage capacity

In larger QR symbols, the message is broken up into several Reed–Solomon code blocks. The block size is chosen so that at most 15 errors can be corrected in each block; this limits the complexity of the decoding algorithm. The code blocks are then interleaved together, making it less likely that localized damage to a QR symbol will overwhelm the capacity of any single block.

Due to error correction, it is possible to create artistic QR codes that still scan correctly, but contain intentional errors to make them more readable or attractive to the human eye, as well as to incorporate colors, logos, and other features into the QR code

block. It is also possible to design artistic QR codes without reducing the error correction capacity by manipulating the underlying mathematical constructs.

3.4 Structure

Each QR Code symbol shall be built of square modules arranged in a regular square array and shall consist of function patterns and encoding region. And the whole symbol shall be surrounded on all four sides by a quiet zone border.

Function patterns are the shapes that must be placed in specific areas of the QR code to ensure that QR code scanners can correctly identify and orient the code for decoding. There are 4 types of function patterns; they are finder pattern, separator, timing patterns, and alignment patterns.

Encoding region contains data, which represents version information, format information, data and error correction codewords. Fig 3.1 illustrates the structure of a QR Code symbol.

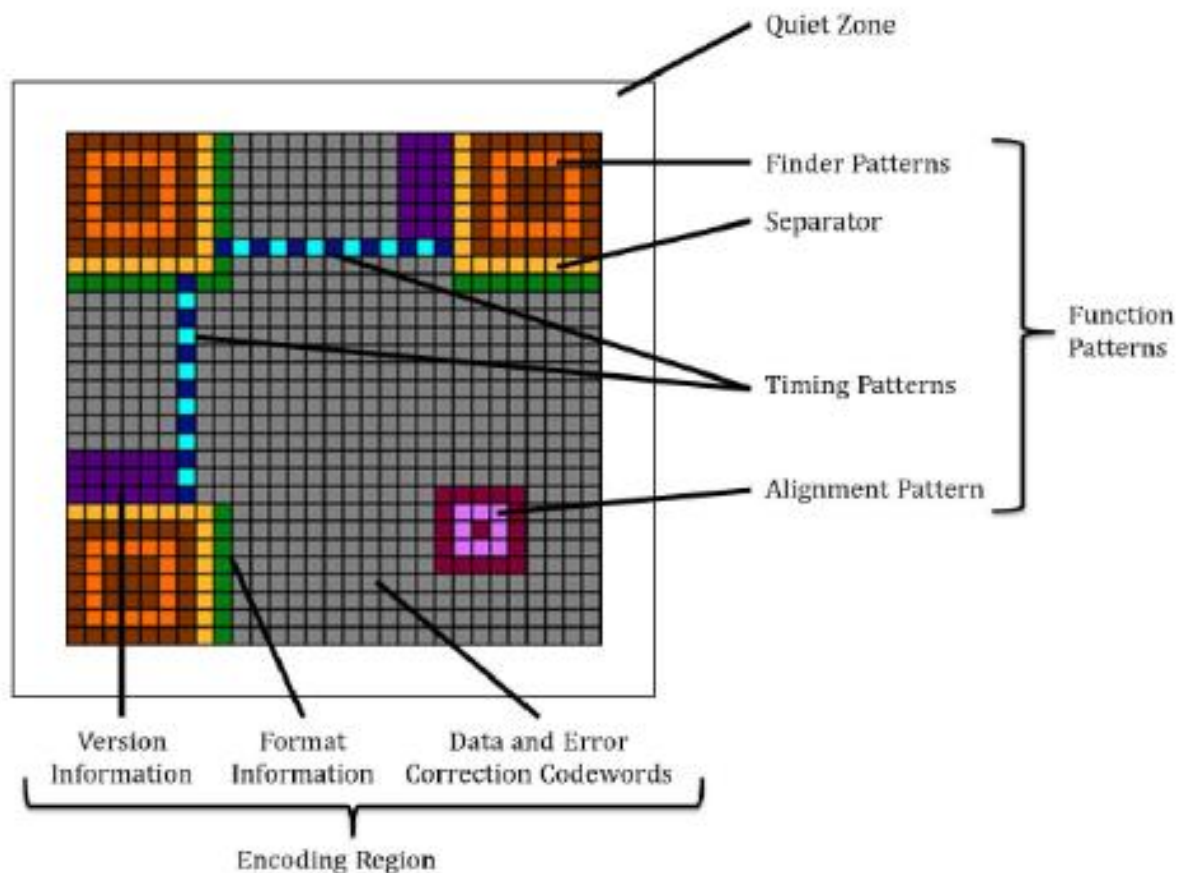


Fig 3.1. Structure of a QR Code symbol

3.4.1 Finder Pattern:

Finder patterns are the special position-detection patterns located in three corners (upper left, upper right, and lower left) of each symbol. It consists of an outer dark square that is 7×7 modules, an inner light square that is 5×5 modules, and a solid dark square in the center that is 3×3 modules. The ratio of module widths in each position detection pattern is 1:1:3:1:1, as shown in fig 3.2. The finder pattern is designed to be a pattern that is unlikely to appear within the other sections of the QR code so that QR code scanners can search for this ratio of light to dark modules to detect the finder patterns and correctly orient the QR code for decoding.

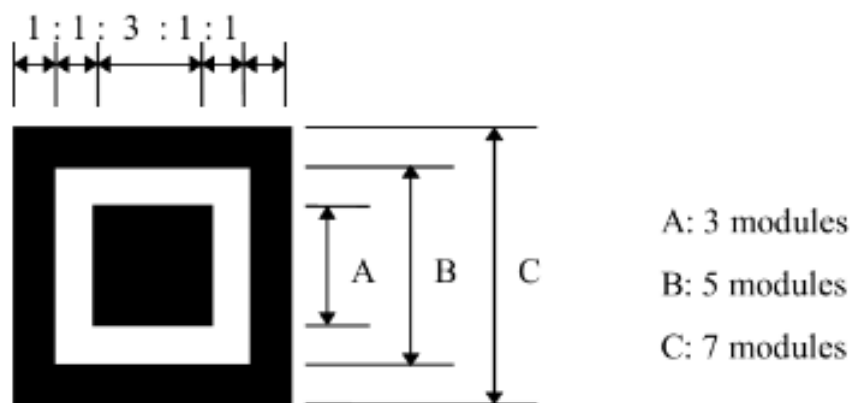


Fig 3.2. Finder Pattern

3.4.2 Separators:

Separators are the one-module wide areas of whitespace between each finder pattern and encoding region.

3.4.3 Timing Patterns:

There are 2 timing patterns, i.e. horizontal timing pattern and vertical timing pattern. They are consisting of alternating dark and light modules. The horizontal timing pattern is placed in the 6th row of the QR code between the separators. The vertical timing pattern is located in the 6th column of the QR code between the separators. These patterns are helpful in determining the symbol density, module coordinates and version information area.

3.4.4 Alignment Patterns:

An alignment pattern is constructed of 5×5 dark modules, 3×3 light modules and a single dark module in the center. QR codes that are version 2 and larger must have alignment

patterns and the number of alignment patterns depends on the symbol version.

3.4.5 Encoding Region:

Encoding region contains format information, version information, data and error correction codes. For format information, one-module array must be reserved near the top-left, top-right, bottom-left finder pattern and version information, an area of a 6×3 block above the bottom-left finder pattern and a 3×6 block to the left of the top-right finder pattern is reserved.

3.4.6 Quiet Zone:

It is a 4-module wide area containing no data, and it used to ensure that the surrounding text or markings should not misguide the QR code data.

3.5 Encoding

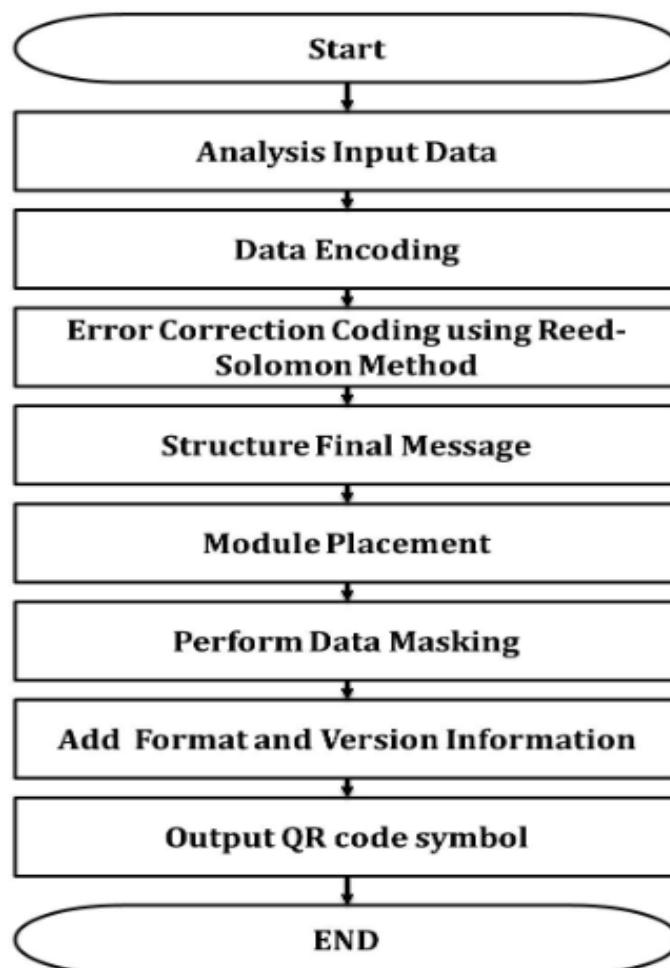


Fig 3.3. QR code encoding

3.5.1 Data Analysis:

A QR code encodes a string of text. The QR standard has four modes for encoding text: numeric, alphanumeric, byte, and Kanji. Each mode encodes the text as a string of bits (1s and 0s), but each mode uses a different method for converting the text into bits, and each encoding method is optimized to encode the data with the shortest possible string of bits. Therefore, first step should be to perform data analysis to determine whether text can be encoded in numeric, alphanumeric, byte, or Kanji mode, and then select the most optimal mode for your text.

3.5.2 Data Encoding:

Next step is to encode text. The result of this step is a string of bits that is split up into data codewords that are each 8 bits long. The mode used for encoding is identified by the Mode Indicator, which is a string of 4 bits. Encoded data must start with the appropriate mode indicator which is used for encoding. The number of characters that are being encoded is represented by the string of bits known as Character Count Indicator. Character Count Indicator is placed after the mode indicator and its length is version dependent.

3.5.3 Error Correction Coding:

QR codes use error correction. This means that the string of data bits that represent our text, we must then use those bits to generate error correction codewords using a process called Reed-Solomon error correction. QR scanners read both the data codewords and the error correction codewords. By comparing the two, the scanner can determine that it reads the data correctly or not, and if it did not read the data correctly it can correct errors.

3.5.4 Structure Final Message:

The data and error correction codewords generated in the previous steps must now be arranged in the proper order. For large QR codes, the data and error correction codewords are generated in blocks, and these blocks must be interleaved according to the QR code specification.

3.5.5 Module Placement in Matrix:

After generating the data codewords and error correction codewords and arranging them in the correct order, you must place the bits in the QR code matrix. The codewords are arranged in the matrix in a specific way.

3.5.6 Data Masking:

Certain patterns in the QR code matrix can make it difficult for QR code scanners to correctly read the code. To counteract this, the QR code specification defines eight mask patterns, each of which alters the QR code according to a particular pattern.

3.5.7 Format and Version Information:

The last step is to add format and (if necessary) version information to the QR code by adding pixels in particular areas of the code that were left blank in previous steps. The format pixels identify the error correction level and mask pattern being used in this QR code. The version pixels encode the size of the QR matrix and are only used in larger QR codes.

3.6 Decoding

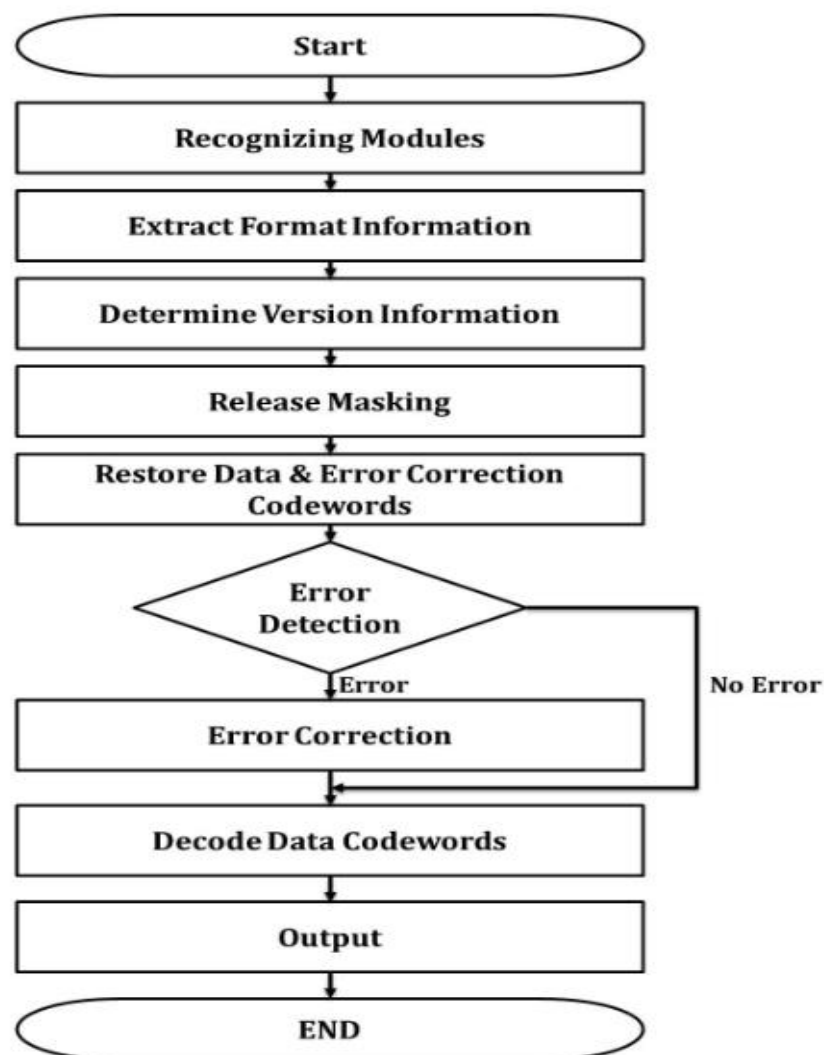


Fig 3.4. QR code decoding

3.6.1 Recognizing Modules:

Recognize dark and light modules as an array of “0” and “1” bits by locating and getting an image of the symbol.

3.6.2 Extract Format Information:

Decode the format information and release the masking pattern and apply error correction on the format information modules as necessary. Also obtain a mask pattern reference.

3.6.3 Determine Version Information:

If version information is applicable then decode it from the version information area and then determine the version of the QR code symbol.

3.6.4 Release Masking:

In order to release the masking, XOR the encoding region bit pattern with the Mask Pattern whose reference has been extracted from the format information.

3.6.5 Restore Data and Error Correction Codewords:

Restore the data and error correction codewords of the message by reading the symbol characters (according to the placement rules for the model).

3.6.6 Error Detection and Correction:

By utilizing the error correction codewords, identify errors and if any error is detected, correct it.

3.6.7 Decode Data Codewords:

Divide the data codewords into segments according to the Mode Indicators and Character Count Indicators. And finally, decode the data characters according to the mode(s) in use and output the decoded text as result.

4. VISUAL CRYPTOGRAPHY

The concept of Visual cryptography firstly implemented by Naor & Shamir in 1994. They conceptualized a completely new and secure method for secret sharing. According to them a secret image can be split into n shares in encryption phase. And while decryption a person should have all n shares to reconstruct the secret image. The beauty of this method was that any $n-1$ shares are not capable to reveal the secret image. When all n shares were superposed, the initial image would seem. Image which will be thought of for Visual Cryptography may be Binary Image, Grayscale Image and Color Image. The technique given by Naor and Shamir for sharing a secret binary image was by mistreatment their own cryptography table. During this process the binary image is split into 2 shares, for the white component within the secret image, one in all the higher 2 rows of table 1 is chosen to create share1 and share2. Pixel expansion is the main feature in which each pixel of the secret image is extended to four pixels. So, regenerated image will be 4 times the original secret image as the pixels are extended to four pixels. By imposition of all shares together will generate a four times larger image than the original secret image. But the resolution quality will be degraded of reconstructed image than the original secret image due to decomposition of each white pixel. The decomposition process includes decomposition of each white pixel into two black and two white pixels.

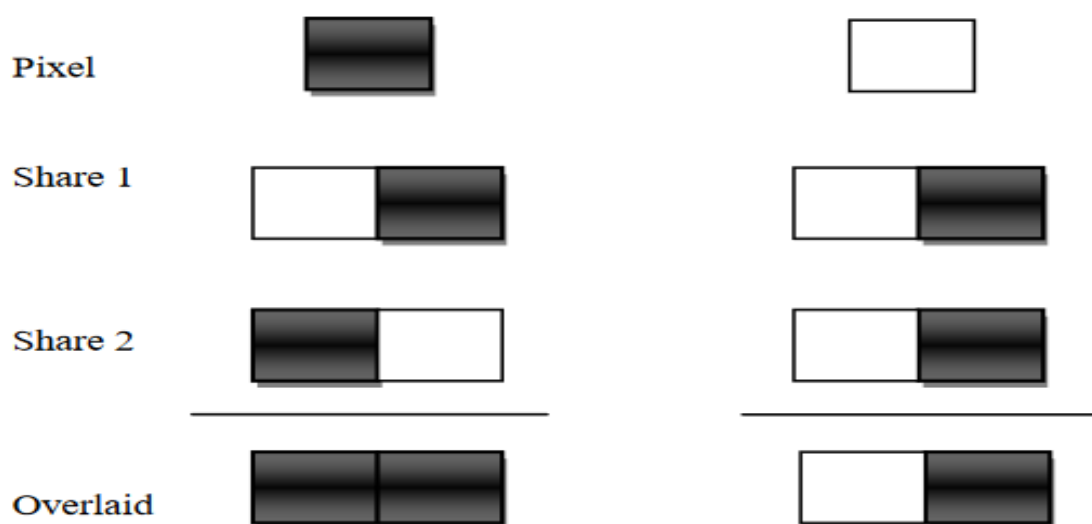


Fig 4.1. Encoding of pixels

4.1 Applications of Visual Cryptography

4.1.1 Watermarking:

Visual cryptography finds application in watermarking, involving two key steps: watermark embedding and retrieval. The watermark is split into shares using visual cryptography, with one share embedded with the host image based on the frequency domain. The owner retains the other share, and to claim the original image, both shares must be combined.

4.1.2 Anti-Phishing Systems:

Visual cryptography contributes to anti-phishing systems by enhancing the security of sensitive credentials. Users receive two shares, one from the server and the other owned. By combining these shares, users can confidently verify a website's authenticity, mitigating phishing risks.

4.1.3 Human Machine Identification:

A technique for human/terminal machine identification is proposed, building on Kim et al.'s work. This extends Katoh and Imai's scheme, showcasing the adaptability of visual cryptography in identification processes.

4.1.4 Secure Banking Communication:

Visual cryptography is applied to secure client information in the core banking industry, preventing forgery of passwords and enhancing security in web banking systems. Image processing within visual cryptography plays a pivotal role in securing sensitive data.

4.1.5 Defense System:

Visual cryptography serves as an encryption technique in defense systems, safeguarding highly sensitive information during data transfers. The scheme involves splitting secret data into shares, requiring collaboration among multiple partners to retrieve the hidden information, ensuring the security of the data.

4.1.6 CAPTCHA:

Visual cryptography contributes to CAPTCHA, offering authentication processes based on the creation of distinctive CAPTCHA images. The method involves share creation, hash code generation using MD5, and an authentication process, enhancing security and

distinguishing between computers and humans.

4.1.7 Offline QR Code Authorization:

An algorithm for offline QR code authentication is proposed, utilizing Visual Secret Sharing Scheme. This approach enhances the security of QR codes, offering resistance to dirt and damage, and enabling authentication from any direction.

4.2 VC Schemes

This subsection explores various schemes aimed at enhancing the flexibility of Visual Cryptography (VC) concerning the types and uses of shares, as well as the number of secrets. Share flexibility involves alternative methods of generating shares that contribute to the recovery of the secret image.

4.2.1 Type of Shares:

Extended Visual Cryptography (EVC) generates meaningful shares during the encryption process, addressing the issue of suspicion. Meaningful shares, as opposed to random noisy shares, eliminate concerns of adversaries detecting vital secret information. A flip-based EVC scheme, an improvement over prior schemes limited to meaningless shares, allows meaningful shares to be flipped to reveal different secret images. This technique enhances security and finds applications in copyright protection. Tagged Visual Cryptography (TVC) schemes address management problems of meaningless shares by embedding a tag image onto existing shares. Although TVC schemes may compromise image quality, probabilistic approaches have improved their performance. Natural Language Letter-based VC (NLLVC) replaces pixels with letters, alphabets, or numbers in share images. NLLVC shares the advantages and disadvantages of EVC, providing a method to indicate contrast differences through overlapping alphabets. Additionally, varying share importance is explored in a (t, s, k, n) VC scheme for binary images, allowing different levels of access to secret images.

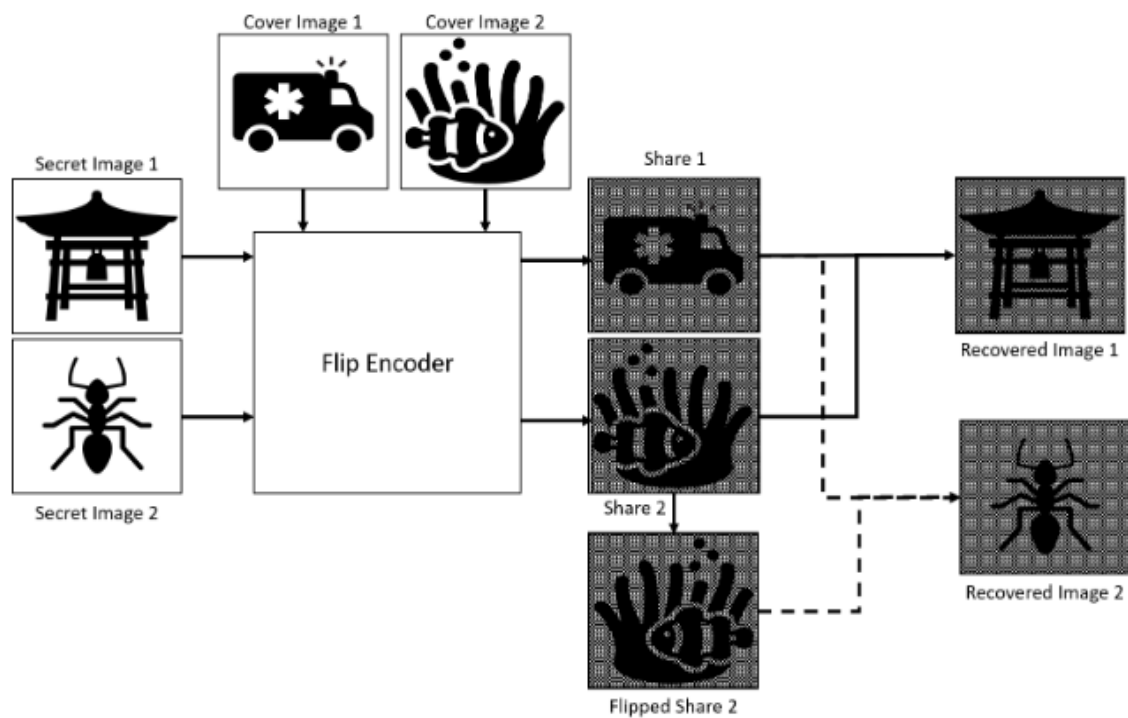


Fig 4.2. Flip-based extended visual cryptography

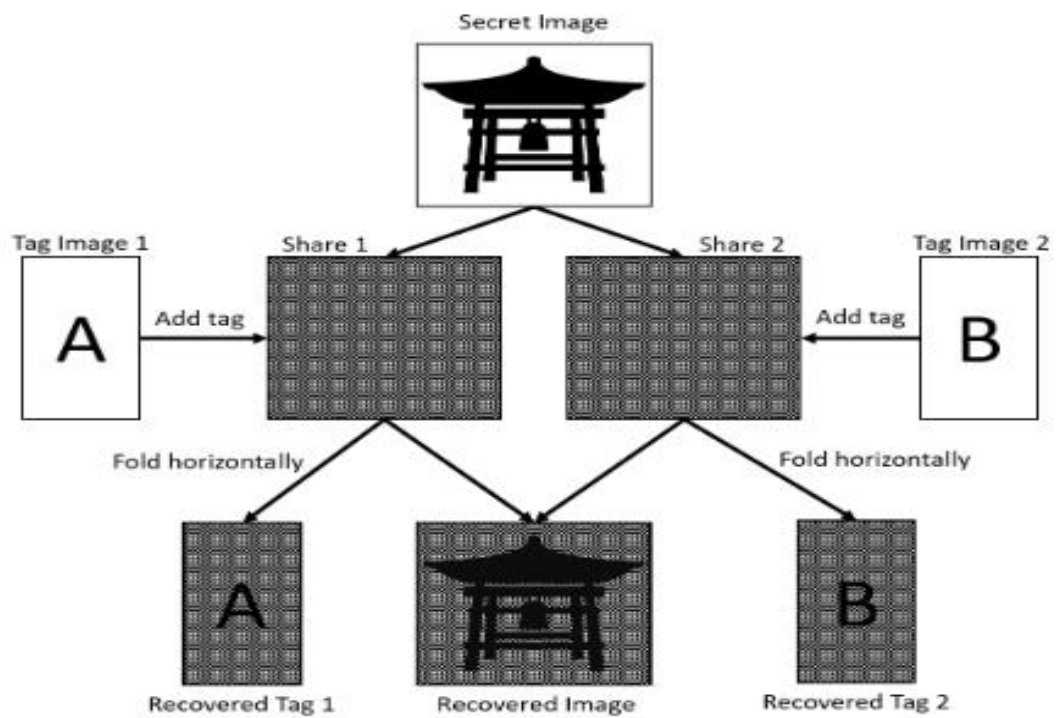


Fig 4.3. Tagged visual cryptography

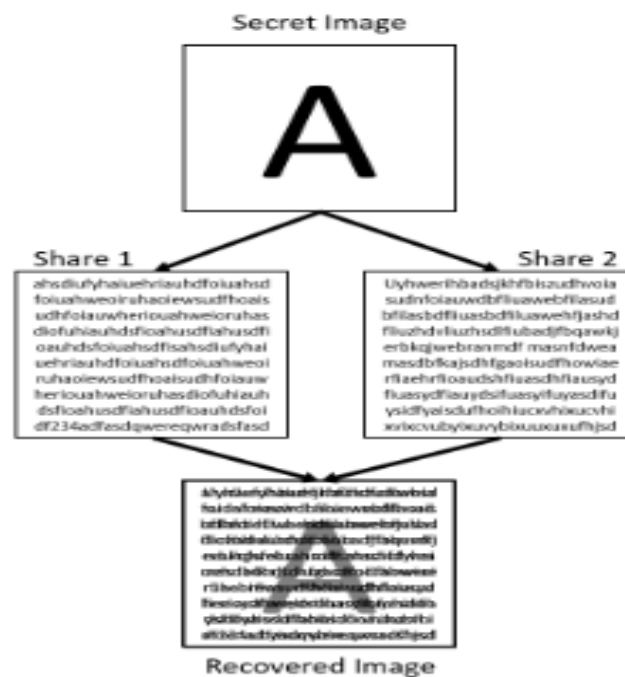


Fig 4.4. Natural language letter-based visual cryptography.

4.2.2 Share Flexibility:

Progressive VC (PVC) enhances recovered secret image quality with an increasing number of shares used for decryption. PVC schemes, whether extended or block-based, enable single encryption with multiple decryption possibilities. However, high memory complexity is a drawback. Hierarchical VC (HVC) encrypts a secret image in multiple levels, suitable for authentication systems but suffering from high memory complexity. VC for General Access (GAS) grants different levels of access to participants, ensuring varied recovery permissions. Although GAS provides flexibility, memory complexity remains a challenge. Dynamic VC (DVC) allows multiple secrets to be hidden within a set of shares, offering good image quality at the cost of high memory complexity. Flip-based Visual Cryptography (FVC) encodes two secret images into shares, supporting multiple secrets with optimal contrast and enhanced security but facing high memory complexity. Recursive Threshold VC (RTVC) hides smaller secrets within larger secrets, suitable for embedding watermarks or authentication information with high-quality recovered images. Extended hierarchical VC schemes and those proposed by support multiple secret images without increasing pixel expansion, achieving excellent visual quality.

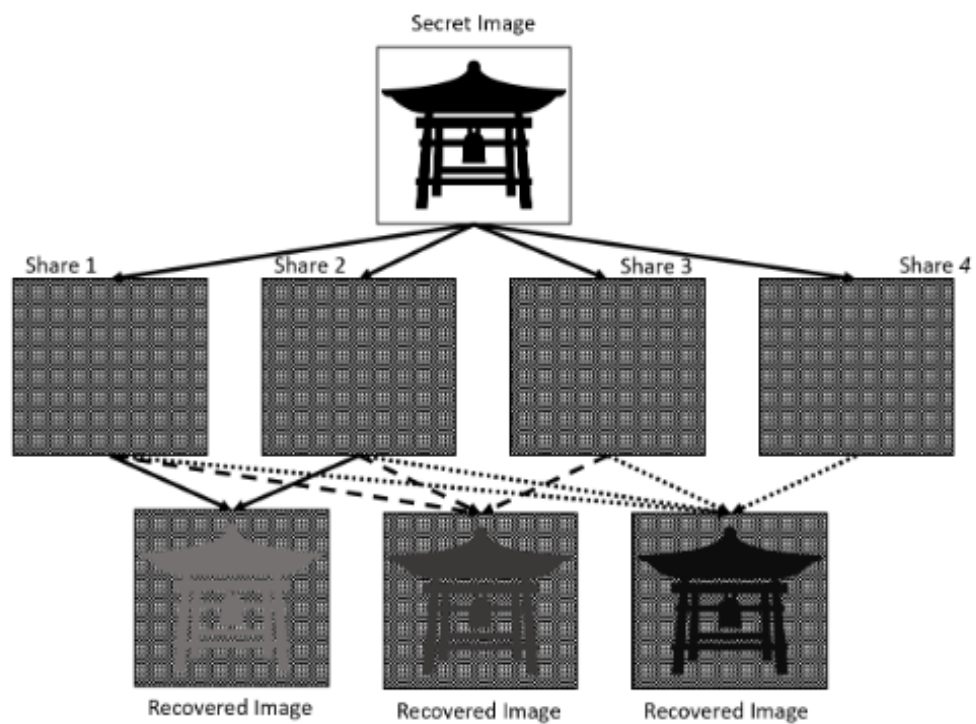


Fig 4.5. Progressive visual cryptography.

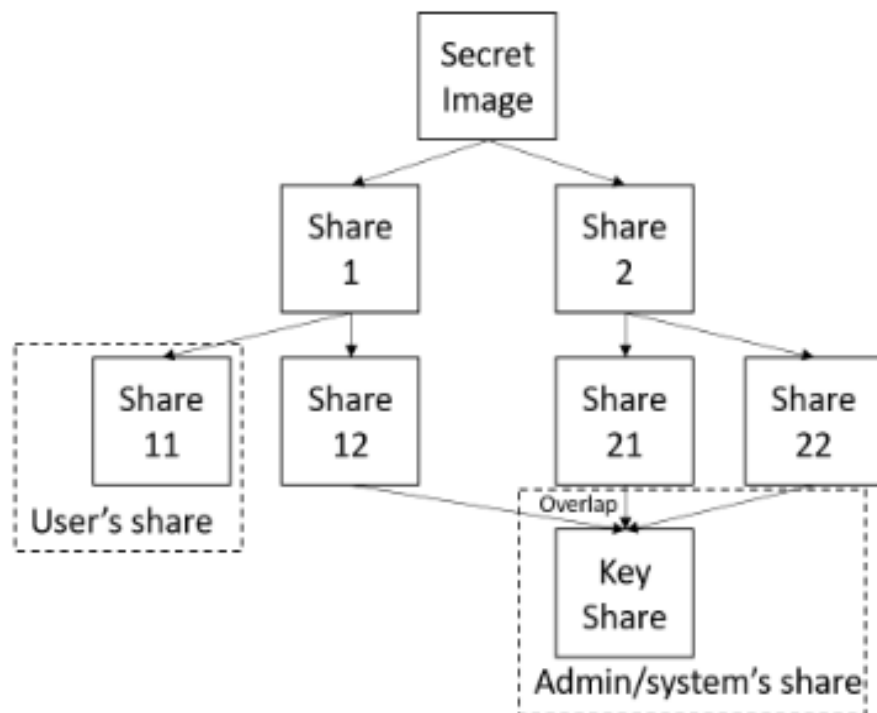


Fig 4.6. Hierarchical VC

4.2.3 Number of Secrets:

Dynamic VC (DVC) hides more than one piece of information within a set of shares, offering good performance but suffering from high memory complexity. Flip-based Visual Cryptography (FVC) encodes two secret images into share images, providing optimal contrast and enhanced security but sharing the same memory complexity issues as many VC schemes. Recursive Threshold VC (RTVC) hides smaller secrets within larger ones, offering high-quality recovered images but at the cost of higher memory complexity. Extended hierarchical VC schemes and those proposed by support multiple secret images without increasing pixel expansion, achieving excellent visual quality.

5. METHODOLOGY

The methodology employed in this study revolves around visual cryptography, a technique introduced by M. Naor and A. Shamir in 1994 as a solution to the general k out of n secret sharing problem. Visual cryptography enables human decryption without relying on computers, offering a unique approach to encrypting visual data such as pictures and text. The process involves encoding a secret image into a set of shared images, which can be deciphered to reveal the original image. Cryptographic procedures divide the secret image into shareable pictures, scattering pixels randomly in each image for sharing.

In the (t, n) -VCS (threshold visual cryptography system), the secret image is divided into several shareable images, and decoding is possible by stacking a sufficient number of shares. The human visual system (HVS) can then be used for decryption without the need for intricate cryptographic knowledge. If the accumulated shares fall below the threshold (t) , the concealed image remains inaccessible. The fundamental two-out-of-two visual threshold method is exemplified, where each image pixel is stored as a pair of subpixels in two shares. The selection of subpixels is determined randomly, simulating a fair coin toss for each decision. By allocating shares A and B based on the selected subpixels, the final step involves superposing the two shares, resulting in the reconstruction of the original image.

Pixel	White 	Black 
Probability	50% 50%	50% 50%
Share1	 	 
Share2	 	 
Stack Share 1&2	 	 

Fig 5.1. Construction of a two-out-of-two scheme: a secret pixel can be encoded into two subpixels in each of the two shares.

Figure 5.2 shows an example of the application of the 2-out-of-2 VSS scheme. Figure 5.2(a) shows a secret binary image SI to be encoded. According to the encoding rule shown in Figure 5.1, each pixel p of SI is split into two subpixels in each of the two shares, as shown in Figure 5.2(b) and Figure 5.2(c). Superimposing the two shares leads to the output secret image shown in figure 5.2(d). The decoded image is clearly identified, although some contrast loss occurs. The width of the reconstructed image is twice that of the original secret image since each pixel is expanded to two subpixels in each share.

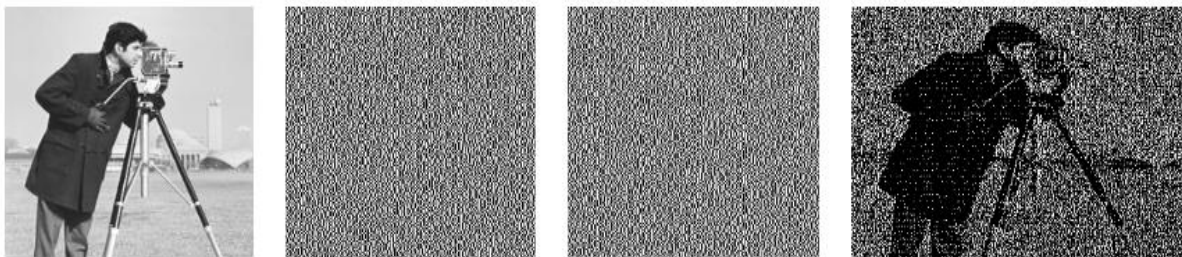


Fig 5.2. Example of 2-out-of-2 scheme.

This methodology provides a foundation for the proposed secure QR code-based online payment system, emphasizing the application of visual cryptography to enhance the security of the transmitted visual data in the form of QR codes. The approach ensures simplicity in both encryption and decryption processes, aligning with the broader goal of creating a secure and user-friendly online payment system.

6. NEW SCHEME OF VISUAL CRYPTOGRAPHY ON THE QR CODE SECURITY

The secure QR code technique we employ will be explained in this section. In order to hide the QR code pattern and the data it contains, we provided an improved visual encryption approach based on the most recent visual encryption technology. In order to more securely achieve the aim of the hidden information, this encryption method makes it more difficult for counterfeiters to obtain the information disguised in QR codes. The QR code is generated from the original secret image using a special encryption method that generates two identical images utilising a pseudo-random matrix and visual cryptography. These are the steps.

6.1 Collections of the C0 and C1 Encoding Matrix

The two sets of the Boolean encoding matrices C0 and C1, which, respectively, represent a white pixel and a black pixel of the original secret image

6.2 Example Technique-Based XAI

Make a pseudo-random matrix of size equal to the range of the original secret picture, between 0 and 3, and with values equal to the basic matrices C0 and C1, respectively. The fundamental matrices in C0 and C1 are XORed with the all-1 matrix.

6.3 Selecting the Basic Matrix

The pseudo-random matrix is involved while choosing the rule, and C0 or C1 is the basic matrix for the sharing picture.

6.3.1 Rule for Creating Sharing Picture A:

The position of each pixel (including white and black pixels) in the secret image is mapped to the corresponding position in the pseudo-random matrix, and the associated basic matrix is then chosen from C0 in accordance with the value in the pseudo-random matrix.

6.3.2 Rule for Creating Sharing Picture B:

The procedure is as follows in the event of a white pixel: the white pixel's location in the secret picture is mapped to its corresponding location in the pseudo-random matrix, and the associated basic matrix is then chosen from the C0 in accordance with the value in the

pseudo-random matrix. The following is the rule when dealing with a black pixel. The pseudo-random matrix is picked from C1 based on the value in the pseudorandom matrix, and the appropriate basic matrix is chosen according to the position of the black pixel in the hidden picture.

6.4 Hidden Picture Reconstructed

A white or black pixel from the original secret picture is represented by one sub-pixel in the reconstructed secret image.

$$C_0 = \left\{ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \right\}$$

Fig 6.1 The principle of pixel superposition based on AND in this scheme.



























Pixel	White				Black			
								
Probability	25%	25%	25%	25%	25%	25%	25%	25%
Share A								
Share B								
Stack Share A&B								

Fig 6.2. Construction of a two-out-of-two scheme of this paper: a secret pixel can be encoded into two subpixels in each of the two shares.

The secret sharing images A and B are produced using this method, which uses a visual cryptography system based on the AND operation. Due to the nature of the process and the basics of the visual cypher, the two sharing images A and B may be used to recover the secret image. The sharing photos generated by this method are linked to the pseudo-random matrix. The pixels of Share image A are generated at random from the basic matrix, and the pixels of Share image B are also generated in the same way from the basic matrix. The attacker is unable to decode the data or access the secret information, even if they succeed in obtaining the basic matrix.

The stacked secret image has a lower contrast compared to the original hidden image. The original image's pixel that caused this behaviour was converted to a square matrix. This is normal and what was anticipated from the experiment. The size of the shared photographs and the stacked hidden image were both four times larger than the original image. Moreover, replacing pixels is involved. Given that a pixel of the original image is replaced by a basic matrix of 4×4 , the sharing photographs and the QR image after overlay recovery would be four times as large as the original hidden image.

7. PROPOSED SYSTEM DESIGN

This section provides a description of the proposed QR-based online payment system. A functional description of the system, including detailed operation steps, will be given in the first sub-section. This is followed by discussing security considerations in the second sub-section.

7.1 Functional Description

The project has explored the opportunity of creating two different types of accounts; merchant and consumer. Consumer accounts have the feature of allowing both receiving and sending credit, while merchant accounts can only receive payment to further opt security. Fig 7.1 illustrates the architecture and the operational flow of the proposed QR-based online payment system. As shown in the figure, the system consists of three entities; merchant, consumer and the cloud server.

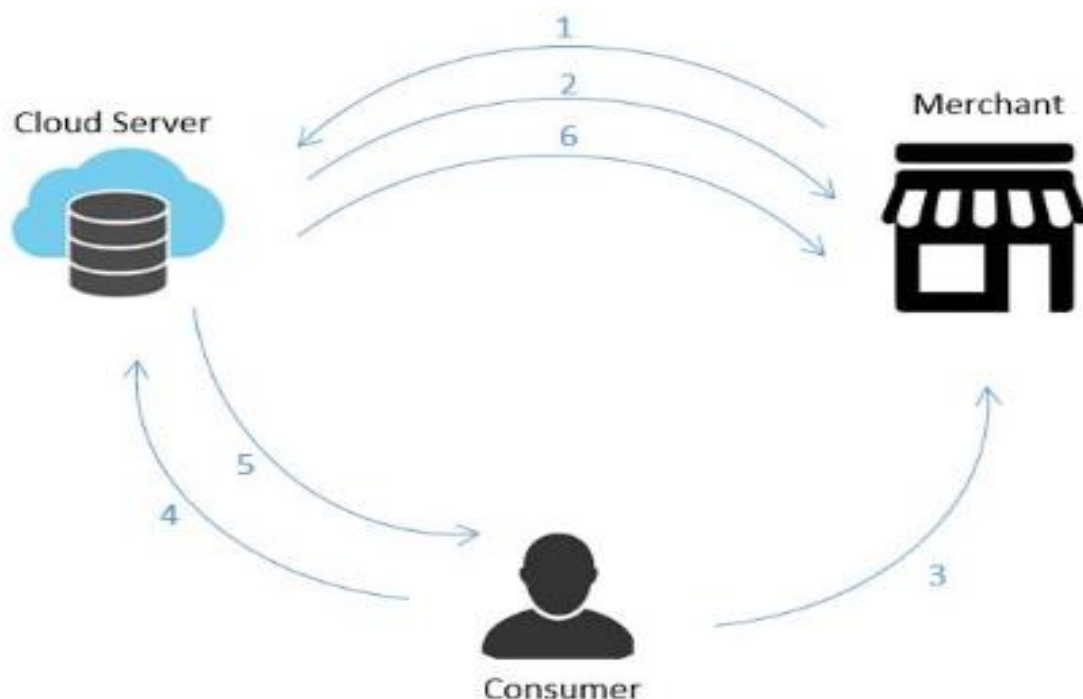


Fig 7.1. General workflow of the proposed QR payment system.

The following operational steps describe the interaction between the three entities during a payment transaction:

Step 1: is for the merchant to request a per-bill QR code from the cloud server.

Step 2: The cloud server sends a QR code with built-in sharing.

Step 3: To begin a transaction, the consumer scans the QR code.

Step 4: The payment request is sent to the cloud server's backend system.

Step 5: The cloud server completes the transaction and issues a confirmation number to the customer.

Step 6: The merchant is provided with the processing results for review Security Considerations.

7.2 Security Considerations

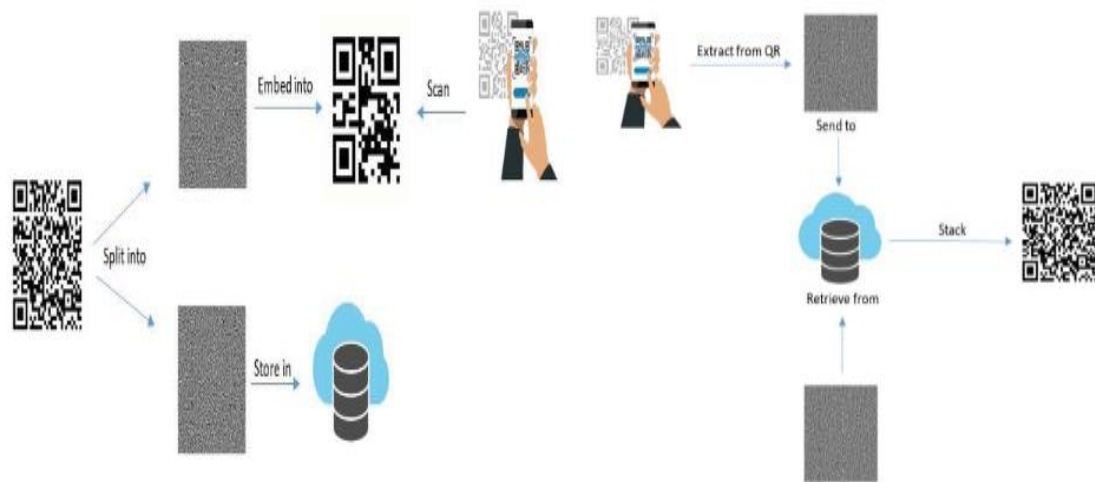


Fig 7.2. (left) Construction of (2, 2) VCS, and (right) Stacking of (2, 2) VCS

The design makes use of the visual cryptography scheme (VCS) algorithm, which is used to secure transactions between users. It is based on a (2,2) VCS, where two shares are generated and the two shares are required to be stacked to present the original image. The algorithm itself is bidirectional, such that the input can be encrypted at one end, then once again decrypted at the other. Both the encryption and decryption of images, the QR codes, are done at the server's side for increased security as to not allow any possibility of tampering at the client's side. The service starts with a merchant requesting a payment to be commenced providing a specific amount to be expected. The application creates the accustomed QR code with provided merchant information from the server itself, feeds it into

VCS, and transports one of the produced shares to the merchant in the form of a QR to be scanned. The other share will be kept in the server. Scanning the QR code will prompt the server to acquire the related twin share, combine both shares, and complete a successful transaction. The left side of fig 7.2 presents the process of generating two shadows from a QR code while the right side of the same figure shows the process of verifying a QR code upon scanning.

8. SYSTEM IMPLEMENTATION

This system is a software-based system. No hardware components, other than the user's mobile device, were required to accomplish the requirements and tasks assigned. An android application is launched as an interface between the users and the server that will provide the authentication and process the transactions. The application is written in Java using Android Studio which is an integrated development environment for Google's Android operating system. The server, which is written in Python, is a host machine found on the local network that acts as a payment gateway server for the mobile payment application. The server manages data in databases stored in a designated memory space and handles requests and responses from and to the mobile application. Fig 8.1 demonstrates the overall high-level functional implementation of the system.

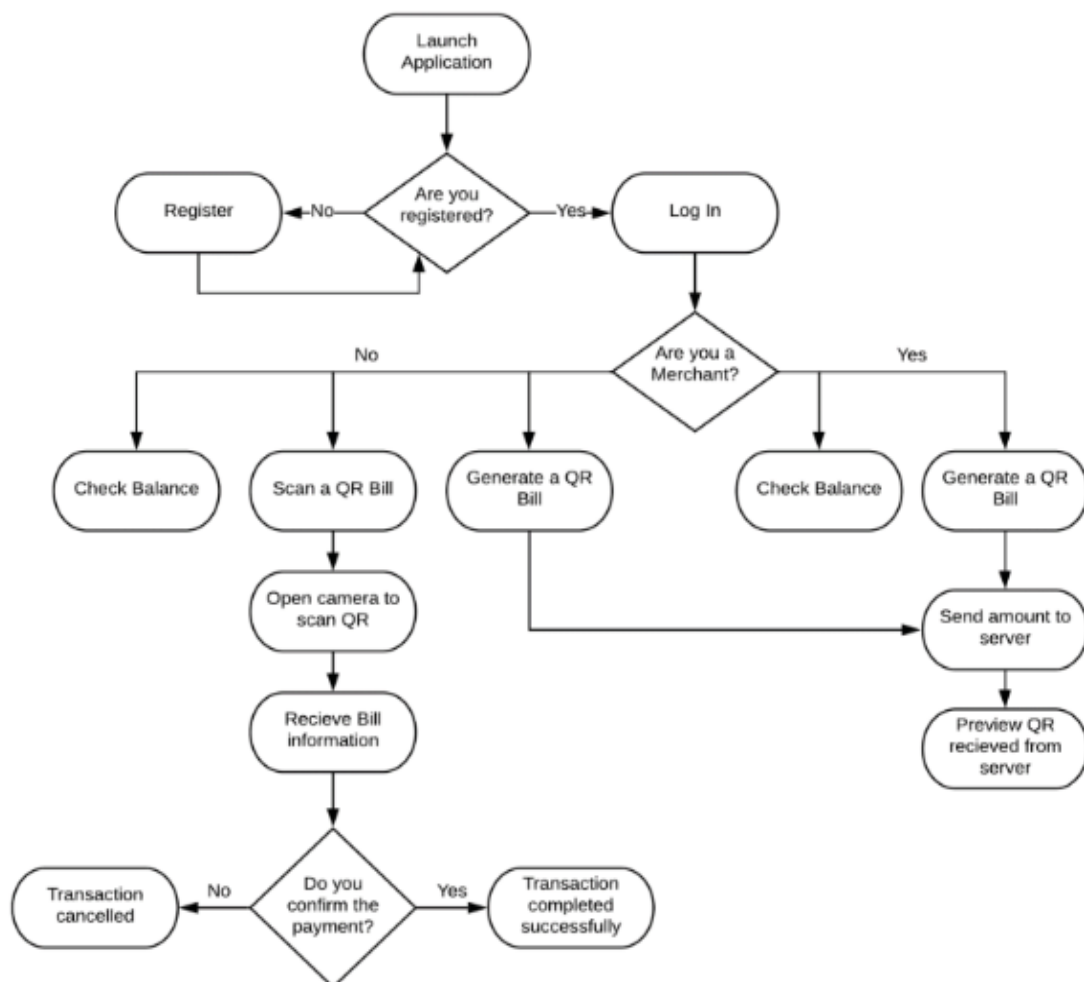


Fig 8.1. High-level functional implementation of the proposed payment system.

9. RESULT ANALYSIS

Users of the payment system can swiftly and simply navigate the mobile application. It only acts as a communication channel between users and the payment gateway server. Users are classified as consumers or merchants throughout the registration process, which entails providing personal information that will be hashed and uploaded to the server. A user can make a QR code after logging in or scan and create a QR code depending on whether they are a customer or a merchant. A new user must provide personal information such as name, email, password, phone number, and whether they are a consumer or a merchant on the registration screen, which is seen in Fig 9.1. Depending on the sort of user they are, options like Create QR, Scan QR, and Check Balance are displayed on the home page when the user logs in. A consumer user's home page and a merchant user's home page are both displayed in Fig 9.1. Once the user has chosen the Create QR Code option, the programmer directs them to Fig 9.2, where they must input the desired bill amount to start the payment process. A QR code containing the share is then sent back by the programmer after making an attempt to contact the server. There is no user specific information stored in the returned QR code.

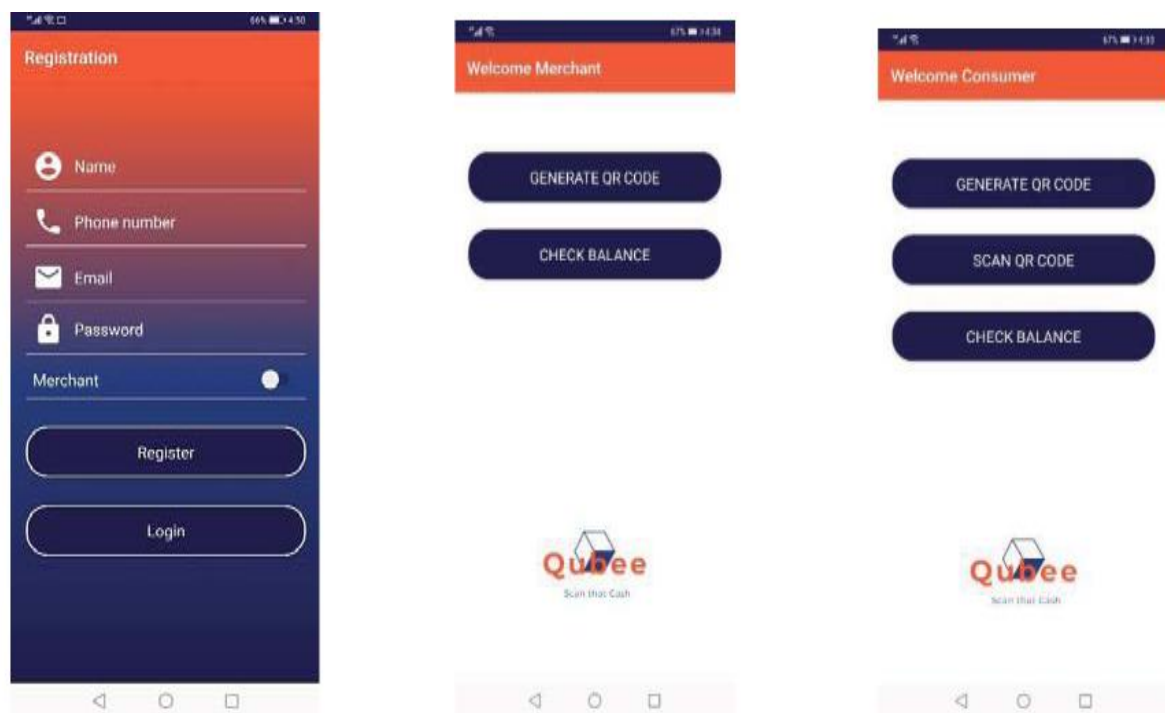


Fig 9.1. Registration page, Home page for merchant, and Home page for customer.

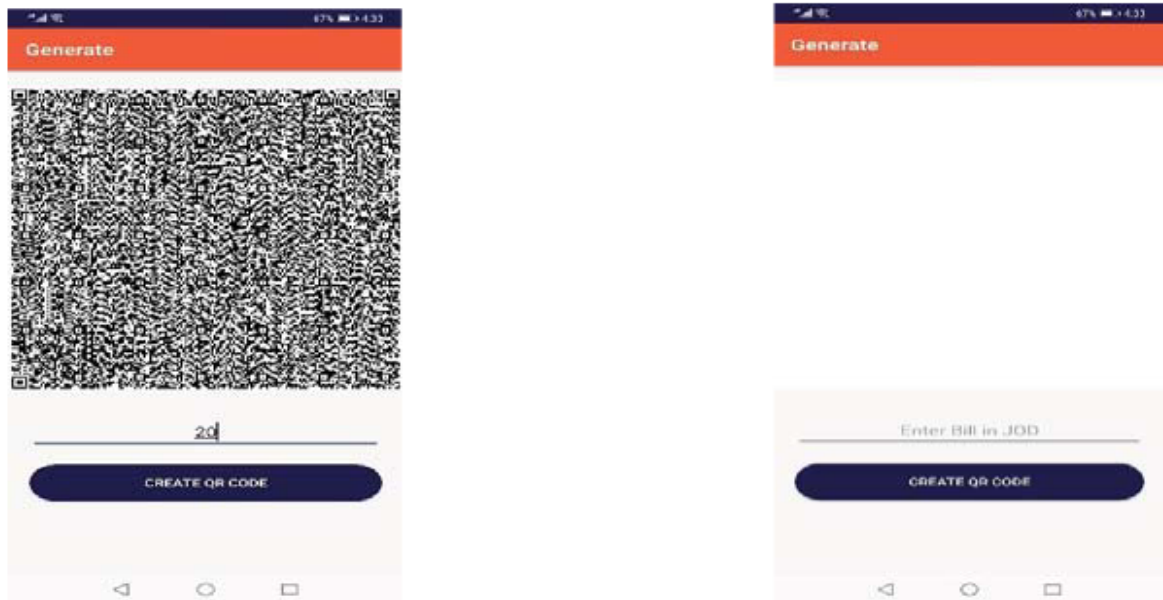


Fig 9.2. 'Generate QR code' page with a requested amount of 20 JOD.

When a consumer chooses to pay a QR bill, the application is brought to the Scan page once the customer selects the Scan QR Code option. The scan sheet has a camera, as seen in Fig 9.3. In order to have access to the phone's camera, the application must first receive permission from the user. After access is granted, the camera will instantly capture the QR code and transfer the scanned QR information to the server for processing. The bill amount and receiver of the funds are provided to the client as a confirmation box when the server has verified the transaction, giving them the option to accept or reject the payment.

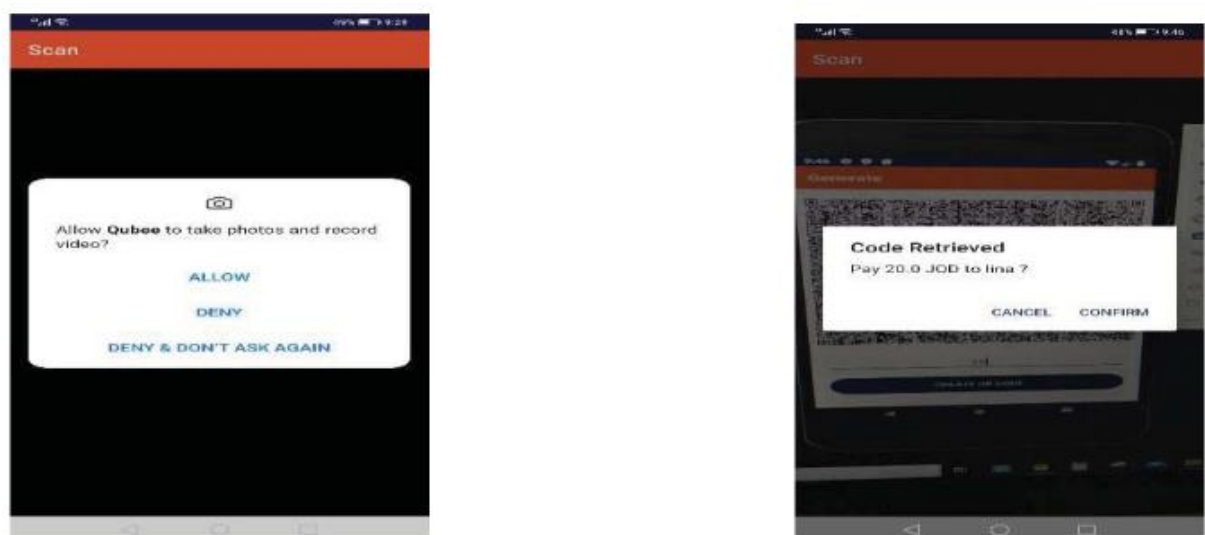


Fig 9.3. Scan QR-code.

10. CONCLUSION

In conclusion, the continuous evolution of online payment technologies has significantly benefited businesses and enhanced consumer satisfaction. While these advancements aim to streamline and secure payment processes, the inherent complexity, and concealed nature of such transactions necessitate ongoing efforts to address potential vulnerabilities. Online payment systems, despite their user-friendly interfaces, remain susceptible to various cyber threats, including data theft, denial of service, and fraud. To counteract these risks, numerous solutions of varying sophistication levels have been proposed, reflecting the industry's commitment to enhancing security measures.

This research introduces a secure QR-based online payment system, leveraging visual cryptography to augment a single algorithm for delivering essential security services- confidentiality, integrity, and authentication. A notable feature of the suggested system is its ability to allow users to generate static QR codes uniquely tied to their accounts. This innovation enhances security by limiting the information exposed in these static QR codes, particularly omitting sensitive balance details. Looking ahead, potential improvements include incorporating sessions to maintain user login status for added convenience and implementing multithreading on the server to efficiently manage and eliminate QR codes that have been stored for more than five minutes, further fortifying the system's overall security posture.

11. FUTURE SCOPE

The envisioned secure QR-based online payment system provides a robust foundation for continual development and refinement. Future enhancements could focus on dynamic QR codes, incorporating features such as biometric authentication and blockchain integration for heightened security. User experience improvements, tokenization for card security, and AI-powered fraud detection are areas that can contribute to a more seamless and secure transaction process. Additionally, exploring multi-currency support, extended mobile device integration, and ongoing security audits will further align the system with evolving industry needs. Collaborating with stakeholders and embracing emerging technologies will be instrumental in ensuring the system remains resilient, user-friendly, and at the forefront of innovation in the rapidly evolving landscape of online payments.

12. BIBLIOGRAPHY

Websites

- [1] <https://www.geeksforgeeks.org/visual-cryptography-introduction/>
- [2] https://en.wikipedia.org/wiki/Visual_cryptography
- [3] <https://www.ijraset.com/research-paper/qr-code-analysis>
- [4] <https://stripe.com/in/resources/more/qr-code-payments>

Journal Papers

- [1] S. Tiwari, "An Introduction to QR Code Technology," 2016 International Conference on Information Technology (ICIT), Bhubaneswar, 2016, pp. 39-44.
- [2] M. Naor and A. Shamir, "Visual cryptography," Lecture Notes in Computer Science vol.950, 1994, pp.1-12
- [3] Kamal, Sawsan & Ameen, Basheer. (2016). A New Method for Cipherring a Message Using QR Code. Computer Systems Science and Engineering. 6. 19-24.
- [4] Y.C. Hou , Z.Y. Quan , C.F. Tsai , D.S. Wang, "(3, n)-Visual Secret Sharing Scheme with Unexpanded Shares". Chinese Journal of Computers, vol.39, Mar 2016
- [5] Klein, Aaron (2019). "Is China's New Payment System the Future?" Brookings Institution Report, June.
- [6] Jianfeng Lu, Zaorang Yang, Lina Li, Wenqiang Yuan, Li Li, and Chin- Chen Chang, "Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography," Mobile Information Systems, vol. 2017, Article ID 4356038, 12 pages, 2017.