

CHAPTER I

INTRODUCTION

1.1 Background

Every day steps are taken to protect important things. are set the alarm systems in homes, put are valuables in safes, and lock cars. The reasons for doing so are simple not being exposed to strangers or distrustful people, and not having access to valuable property, and that these valuables are not harmed.

There are many things that could be considered information that are need to protect. We might have personal medical or financial records that we want to keep private. We usually don't want everyone in the world reading emails or social media posts that we send to friends or family. Also want to keep certain things, like our Internet passwords, credit card numbers, and banking information from getting into the wrong hands.

It is very important to encrypt messages while sending them to a client from another client without being tracked or interpreted by any person is not authorized. Encryption techniques are now a very important research field, cryptography scientist is trying to come up with a good encryption technique (algorithm) so that no hacker can interpret the encrypted message, one of the most important ways to hide data is the QR code.

QR code is matrix form 2-Dimensional it contains the rows and columns for storing the information in two directions. And its enhanced version of one-dimensional barcode. Countries like Japan use the QR code for storing the sensitive information. Nowadays United States also use the QR code, It is popular over the worldwide that will use for future uses[1].

There are so many methods available to hide private information encoded QR codes. Almost every method shows cased satisfactory performance parameters. It is found that Steganography when coupled with encryption algorithms like AES, RSA produced better results. These also provide high end data security to the private data[2].

The Advanced Encryption Standard (AES) is the more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays. It is found at least six time faster than triple DES[3].

As well as the need for a secure data transmission corridor the security techniques using optical and digital processing have been widely studied for various security purposes such as Arnold transform (AT) and Shearlet transform (SHT). The optical system for secure data transmission is investigated extensively because of their several advantages over electronic counterparts[4].

1.2 Problem Statement

Due to tremendous growth in technology the problem of securing and sending confidential information has become a real challenge given the enormous capacity of hackers, The QR code has high storage capacity and it has possibility of concealing different types of data within it, but these QR code can be easily decoded by any smart phone with built in camera therefore a new effective algorithm must be designed to secure QR code.

1.3 Research Objective

The main objective of this research is to develop a new method for ciphering a message using QR Code. The objective of that will be:

1. To Present the different techniques that may be used to hide data within the QR code.
2. To Propose a new strong method to encrypt messages by encryption in four levels.
3. To Achieve better security by encrypting QR code After conversion the messages.

1.4 Research Methodology

Description of the steps used to design the search tools (the used programs), In this method to secure a data are hide the secret message in double encryption method no one can extract the original secret message without knowing the exact method by Using the Following Steps:

1. Encrypt secret message by using AES Algorithm.
2. Converts the encrypted message to the QR code.
3. Scrambled QR code by using the Arnold transform.
4. The scrambled image is then encrypted using the Shearlet transform.

1.5 Research Organization

Chapter two is the Theoretical Background beside the Previous studies, chapter three Proposed Research Methodology and Procedures, chapter four will introduce Implementation and the Result discussion, the last chapter is the Conclusion and Future Work.

CHAPTER II

LITERATURE REVIEW

2.1 Theoretical Background

This chapter will address some of the key concepts related to this research as well as their definitions and reference to relevant scholarly literature, which will help us deepen the theoretical understanding and provide us with real information in the field.

2.1.1 Quick Response Code (QR code)

Bar codes have become widely popular because of their reading speed, accuracy, and superior functionality characteristics, the market began to call for codes capable of storing more information, more character types, and that could be printed in a smaller space. As a result, various efforts were made to increase the amount of information stored by bar codes, such as increasing the number of bar code digits or layout multiple bar codes. However, these improvements also caused problems such as enlarging the bar code area, complicating reading operations, and increasing printing cost. 2D Code emerged in response to these needs and problems[5].

QR code (quick response code) is a special type of two-dimensional barcode designed by Japanese automobile industry. The idea was first proposed by Denso Wave, QR code is usually attached to an item and it contains information about that item, information can be in form of numeric data, alphanumeric and binary, this makes the QR code capable of storing any kind of data.



Figure 2.1: A Sample QR code containing the text “Secure Data Using QR Code”

2.1.1.1 Structure of QR Code

QR code consist of different areas that are reserved for specific purposes. In the following figure we refer to version 2 of QR code[1].



Figure 3.1: Structure of QR Code Version 2

Finder Pattern (1): The finder pattern consists of three identical structures that are located in all corners of the QR Code except the bottom right one. Each pattern is based on a 3x3 matrix of black modules surrounded by white modules that are again surrounded by black modules. The Finder Patterns enable the decoder software to recognize the QR Code and determine the correct orientation.

Separators (2): The white separators have a width of one pixel and improve the recognizability of the Finder Patters as they separate them from the actual data.

Timing Pattern (3): Alternating black and white modules in the Timing Pattern enable the decoder software to determine the width of a single module.

Alignment Patterns (4): Alignment Patterns support the decoder software in compensating for moderate image distortions.

Format Information (5): The Formation Information section consists of 15 bits next to the separators and stores information about the error correction level of the QR Code and the chosen masking pattern.

Data (6): Data is converted into a bit stream and then stored in 8-bit parts (called codewords) in the data section.

Error Correction (7): Similar to the data section, error correction codes are stored in 8-bit long codewords in the error correction section.

Remainder Bits (8): This section consists of empty bits of data and error correction bits cannot be divided into 8-bit codewords without remainder.

2.1.1.2 The data can be stored in the QR code

QR code can contain many different types of information. Different app readers on Smartphone are able to act and read this data[6].

1. **Contact information:** QR code can contain contact information so someone can easily scan a QR code, view your contact details, and add you on their phone. You can input your name, phone number, e-mail, address, website, memo, and more.
2. **URL:** The possibilities of encoding URL into barcode are endless. You can use a link that takes someone to your Facebook fan page, LinkedIn or Twitter profile.
3. **Calendar event:** If you have an event you want to promote, you can create a QR code containing info for that event. QR code containing event info can contain event title, start and end date/time, time zone, location, and description. This could work well on an event flyer or possibly even on a website promoting.
4. **E-mail address:** A QR code can contain your e-mail address so someone can scan the code, see your e-mail, and then open an e-mail on their phones.
5. **Phone number:** Maybe e-mail isn't immediate enough and you want someone to call. Link them up to a phone number.
6. **Geo location:** you might want to stick a QR code linking someone to a Google Maps location. This will allow someone to scan your QR code and get directions so they don't have to manually type in an address.
7. **Wi-Fi network:** Do you hate telling someone a long WEP wireless key that's a pain to type out on a mobile phone? Set it up so someone can scan a QR code and automatically configure Wi-Fi on their phones.
8. **Text:** You can also just have a sentence or a paragraph of text.
9. **SMS:** The QR code can also be used to store confidential messages after encrypting, sending, or retaining them, this method will be suitable in any business house, government sectors, communication network to send their encrypted messages faster to the destination.

2.1.1.3 QR code versions

The data can be stored in QR code depends on version (1...40 indicating number of rows and columns), data type and error correction level. The maximum storage capacity of QR code for version 40 having 177x177 rows and columns respectively. The QR code version 1 contains 21x21, version 2 contains 25x25, version 3 contains 29x29, version 4 contains 33x33, version 10 contains 57x57 and version 25 contains 117x117 rows and columns respectively[7].

2.1.1.4 Generating Error Correction

QR code has error correction capability to restore data if the code is dirty or damaged. Four error correction levels are available for users to choose according to the operating environment. Raising this level improves error correction capability but also increases the amount of data QR code size.

There are four levels of error correction; Low (L) which can tolerate up to 7% damage, Medium (M) can tolerate up to 15% damage, Quartile (Q) can tolerate up to 25% damage and High (H) can tolerate up to 30% damage. The reason why the Low (L) error correction level is preferred is that the High error correction levels raise the percentage of code word used in error correction thereby decreasing the amount of data that can be stored in the code. The black and white modules of the QR codes comprise of the encoded data. This information isn't present in human readable form hence an individual cannot anticipate the information. Any smart phone with built-in camera can capture the image of the encoded QR Code and then decode the data present in it[8]. Figure 4 shows a QR code and Error Correction (EC) levels.

codewords to be corrected. In this case, the total codewords are 200, 50 of which can be corrected. Thus, the error correction rate for the total codewords is 25%. This corresponds to QR Code error correction Level Q.

2.1.1.6 Capacity of QR code

The reason for selecting the QR code is because they have higher or large storage capacity than any other normal conventional 'barcodes' and have fast response time. The following table shows the maximum number of characters encoded in a QR code (version 40)[8]:

Table 2.2: Capacity of QR code

No	Data Type	Characters
1	Numeric data	7,089
2	Alphanumeric data	4,296
3	8-bit byte data	2,953
4	Kanji data	1,817

Finally, after we got to know the QR code more clearly. As mentioned in the first chapter, combining the QR code with the advanced cryptographic algorithms gives the best results in hiding the data. Here are the most important algorithms that we will use in our search.

2.1.2 Advanced Encryption Standard (AES)

All of the cryptographic algorithms we have looked at so far have some problem. The earlier ciphers can be broken with ease on modern computation systems. The DES algorithm was broken in 1998 using a system that cost about \$250,000. It was also far too slow in software as it was developed for mid-1970's hardware and does not produce efficient software code. Triple DES on the other hand, has three times as many rounds as DES and is correspondingly slower. As well as this, the 64-bit block size of triple DES and DES is not very efficient and is questionable when it comes to security.

On January 2, 1997 the National Institute of Standards and Technology (NIST) held a contest for a new encryption standard. After holding the contest for three years, NIST chose an algorithm created by two Belgian computer scientists, Vincent Rijmen and Joan Daemen. They named their algorithm Rijndael after themselves. On November 26, 2001 the Federal Information Processing Standards Publication 197 announced a standardized form of the Rijndael algorithm as the new standard for encryption. This standard was called Advanced Encryption Standard and is currently still the standard for encryption[10].

2.1.2.1 The AES cipher

Like DES, AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively.

2.1.2.2 Inner Workings of a Round

The algorithm begins with an add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes.
2. Shift rows.
3. Mix Columns.
4. Add Round Key.

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

5. Inverse Shift rows.
6. Inverse Substitute bytes.
7. Inverse Add Round Key.
8. Inverse Mix Columns.

Again, the tenth round simply leaves out the Inverse Mix Columns stage.

2.1.3 Arnold transform (AT)

The AT of a two-dimensional function $f(x_i, y_i)$ [11], which is also called cat face mapping is only suitable for encrypting $N \times N$ images [12], performs the scrambling operation by randomly changing the pixel positions of an image. After application of the ART, the pixels at (x, y) of an image $f(x, y)$ of size $N \times N$ pixels are moved to new positions (x', y') [4]. Mathematically, the two-dimensional AT can be defined as:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{ mod } n \quad \{1\}$$

Where:

(x', y') : pixel coordinates of the encrypted image (after executing ART).

(x, y) : pixel coordinates of the original image.

“mod”: represents modulus after division operation.

The AT is a periodic transform and after a set number of iterations, the original image will reappear. The period of ART is defined by:

$$\text{Period} = \min \{p: [\text{ART}\{f(x, y), N\}]^p = f(x, y)\} \quad \{2\}$$

Where:

‘min’: denotes the minimum value.

p : is the number of iterations.

Arnold transform has a property that the original image will appear when the equation {2} is iteratively calculated m times. The periodicity makes the encryption algorithm directly using Arnold transform unsecure. This is because one can easily obtain the original image by iterative computations once the encryption algorithm is known. The periodicity value $m \leq \frac{N^2}{2}$ and some specific values under different image sizes N are listed in table 2 [13].

Table 2.3: The periodicity values m under different image sizes N

N	60	100	120	128	256	480	512
m	60	150	60	96	192	240	384

Are find that Arnold transform has two weaknesses. One is the periodicity; the other is the requirement that image height must equal image width. The periodicity makes it unsecure, while the requirement limits its applications.

2.1.4 Shearlet transform (ST)

Shearlets transform one of the methods of image processing, possess a uniform construction for both the continuous and the discrete setting. They further stand out since they stem from a square-integrable group representation and have the corresponding useful mathematical properties[14]. Shearlets were introduced with the expressed intent to provide a highly efficient representation of images with edges. In fact, the elements of the shearlet representation form a collection of well-localized waveforms, ranging at various locations, scales and orientations, and with highly anisotropic shapes. This makes the shearlet representation particularly well adapted at representing the edges and the other anisotropic objects which are the dominant features in typical images[15].

Shearlets have been applied to a wide field of image processing tasks, e.g., DE noising, inversion of the Radon transform, inverse half toning, deconvolution, geometric separation, in painting and many more. also, the application of the shearlet representation turns out to be very beneficial, include image enhancement, image separation, edge detection, and estimation of the geometric features of an object.

Mathematically, the Shearlet transform is implemented using a Laplacian pyramid scheme and directional filtering. For an image I , the Shearlet transform is a mapping as[16]:

$$I \rightarrow SH_{\Psi}I(a, s, x) \quad \{3\}$$

The three parameters:

a: defined as the scale

s: orientation

and x: location

where $a > 0$ and $s \in Z$. The Shearlet transform can be expressed as:

$$I \rightarrow SH_{\Psi}I(a, s, x) = \int I(x') \Psi_{as}(x - x') dx' = I \cdot \Psi_{as}(x) \quad \{4\}$$

The Shearlets are generated by dilating, shearing and translating.

2.2 Previous studies

There is a variety of studies done in hiding data using QR code, most of these studies have focused on hiding images within the QR code where they private information inside a QR code is embedded in a cover image and send to the receiver. The following are some of these Related Work:

- 1) Remya Paul in 2018, A review on Steganography in QR Codes, survey various methods to hide private messages within a QR code. It is found that steganography when coupled with encryption algorithms like AES, RSA produced better result [2].
- 2) Ravi Kumar et al in 2018, QR code-based non-linear image encryption using Shearlet transform and spiral phase transform, Journal of Modern Optics, they propose a new non-linear technique for image encryption by converted the input image into a QR code and then scrambled using the Arnold transform. The scrambled image is then decomposed into five coefficients using the ST and the first Shearlet coefficient. The focus of this paper was to hide images within the QR code[4].
- 3) Sawsan K. Thamer and Basheer N. Ameen in 2016, a New Method for Cipherring a Message Using QR Code, Computer Science and Engineering, they converted the message into QR code and generate QR for mask (Key). It is used encryption technique by XORing part (series of bits) of QR message with the same part of QR mask (key) to encrypt any message and then embedding the key into the resulted QR. introduced a new data-hiding algorithm. But The message is not encrypted before it is entered into the QR code, so it can be decrypted using modern encryption techniques.[17]
- 4) M.Mary Shanthi Rani and K.Rosemary Euphrasia in 2016 Data security through QR code encryption and steganography, Advanced Computing: An International Journal (ACIJ), Follow two steps to hide the message inside the QR code firstly Encrypting the message by a QR code encoder and thus creating a QR code Second Hiding the QR code inside a color image. Experimental result shows that the proposed method has high imperceptibility, integrity and security. Only the QR code is included within the image which makes it very easy to get when you know that it is embedded within this image.[8]

- 5) Dipika et al in 2014 QR based Advanced authentication for all hardware platforms, International Journal of Scientific and Research Publications they implement the authentication using the QR code for all platforms such as PC, tablet and mobile phones and replace the demand draft and cheque by Cash Card and that is done by transmitted the information in QR code in the encryption form, QR code techniques introduced into one time password protocol. This paper mainly focuses on the system features of QR code Not on implemented.[18]
- 6) Somdip Dey, Asoke Nath and Shalabh Agarwal in 2013, Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System, in 2013, Communication Systems and Network Technologies (CSNT), They encrypted the mark sheet data using the TTJSA encryption algorithm. In which the encrypted marks are entered inside QR code and that QR code is also printed with the original data of the mark sheet. The marks obtained by a candidate will also be encoded in QR Code™ in encrypted form.[19]
- 7) Somdip Dey in 2012, SD-eqr: A new technique to use qr codestm in cryptography, he introduced a new method he called SD-EQR method, and that is done by storing messages in encrypted format with a password and send it to the required destination hiding in a QR Code, without being tracked or decrypted properly by any hacker or spyware. Even other encryption techniques / methods can be used with this method to add more level of security to the data or the message.[9]
- 8) A. Sankara Narayanan in 2012, QR codes and security solutions, International Journal of Computer Science and Telecommunications, discusses QR codes different data types, attack via QR codes and security solutions. How to verify whether the identifier written in the 2-D code is indeed issued by the authorized organization. In this paper examine outlined the dangers of possible malicious Without addressing the details of the fine penetration used by hackers. Only QR code risks were discussed and none were applied for accurate detection. [6]
- 9) Somdip Dey et al in 2012, Advanced steganography algorithm using randomized intermediate QR host embedded with any encrypted secret message: ASA_QR algorithm, International Journal of Modern Education and Computer Science present a new steganography algorithm to hide any small encrypted secret message inside QR Code. The secret message is encrypted first and hide it in a

QR Code™ and then again that QR Code™ is embed in a cover file in random manner, using the standard method of steganography. Only the QR code is included within the image which makes it very easy to get when you know that it is embedded within this image.[20]

CHAPTER III

RESEARCH METHODOLOGY AND PROCEDURES

3.1 Introduction:

This chapter proposes a new technique for data hiding in two level encryption techniques, In the first level the message (text) is encrypted using the AES algorithm Then the message is converted to the QR code, in second level the QR code is encrypted using the Arnold transform and then the Shearlet transform.

The Steps:

1. Encrypt secret message using AES Algorithm.
2. Converts the encrypted message to the QR code.
3. scrambled QR code by using the Arnold transform.
4. The scrambled image is then Encrypted using Shearlet transform.

Most of the available encryption methods are concerned with only one aspect, either encrypting the message and hiding it in the QR code or encrypting the QR code without placing the importance of the hidden data in it. The following figure illustrates the encryption process.

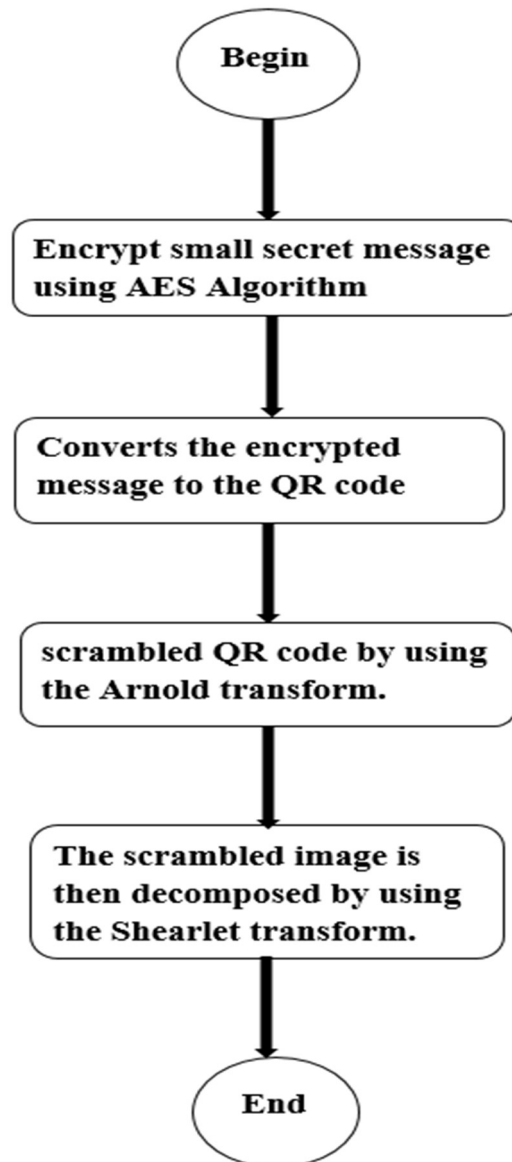


Figure 3.1: Encryption process.

3.2 The Encryption process involves the following steps:

3.2.1 Encrypt secret message using AES Algorithm:

to encrypted the message can chose 128, 192 or 256-bit long key size for encryption and decryption. So, there will be 10, 12 or 14 Rounds (depending on key size). Implementations of were tested in PHP languages for speed and reliability in encryption and decryption.

3.2.2 Converts the encrypted message to the QR code:

The QR code generation process is as follows:

Data Analysis and Encoding:

The QR encoding standards have 4 different models to encode data, these models are numeric, alphanumeric, byte, and Kanji data (characters used in Japanese writing). The output of any model is a series of bits, each model follows a different technique for generating the series of bits, since each model behaves differently and generate different length of bits the data should be analyzed to determine whether the text is preferred to be encoded in numeric, alphanumeric or byte mode, then select the most optimal model in terms of bits length to generate the stream of bits for QR code.

Error Correction Coding:

After encoding the secret text, error correction codes are generated to be embedded inside the bits stream to detect and correct errors, QR scanners read both the codewords and data and compare them together to detect errors.

Module Placement in Matrix:

After embedding the codewords inside the data bites, the data must be placed in the QR matrix along with pattern commonly used with QR codes such as black boxes in corners.

3.2.3 Scrambled QR code by using the Arnold transform (AT)

after message is converted to QR code $I_{QR}(x, y)$, which is then scrambled using the AT of order p, to get $I_{QR}(x', y')$ as:

$$I_{QR}(x', y') = AT^P\{I_{QR}(x, y)\} \quad \{5\}$$

3.2.4 Shearlet transform (ST)

The scrambled image is then decomposed into five coefficients using the Shearlet transform, Shearlets have been applied to image for enhancement, image separation, edge detection.

3.3 The decryption can be carried out using the following steps

3.3.1 Load inverse image Shearlet transform (SHT):

The inverse ST is performed on the encrypted image and get an enhanced image.

3.3.2 apply inverse Arnold transform (AT):

The inverse AT with an order, p is then applied to $D_1(x', y')$ to get the decrypted QR code, $D_{QR}(x, y)$ as:

$$D_{QR}(x, y) = AT^{N-P}\{D_1(x', y')\} \quad \{6\}$$

3.3.3 Scanning the resulted QR to get message:

The encrypt secret message finally can be retrieved easily from the decrypted QR code, using a QR code scanner. Specific patterns if found in QR matrix can make it difficult for QR scanners to correctly read the data, to avoid such case, QR code standards provide 8 different mask patterns that alters the QR code according to a particular pattern, the mask must be selected so that difficulties are minimal.

3.3.4 decrypt message using AES:

To retrieve the original message using an AES algorithm same key must be entered the which was used for encryption. The figure below shows the decryption process.

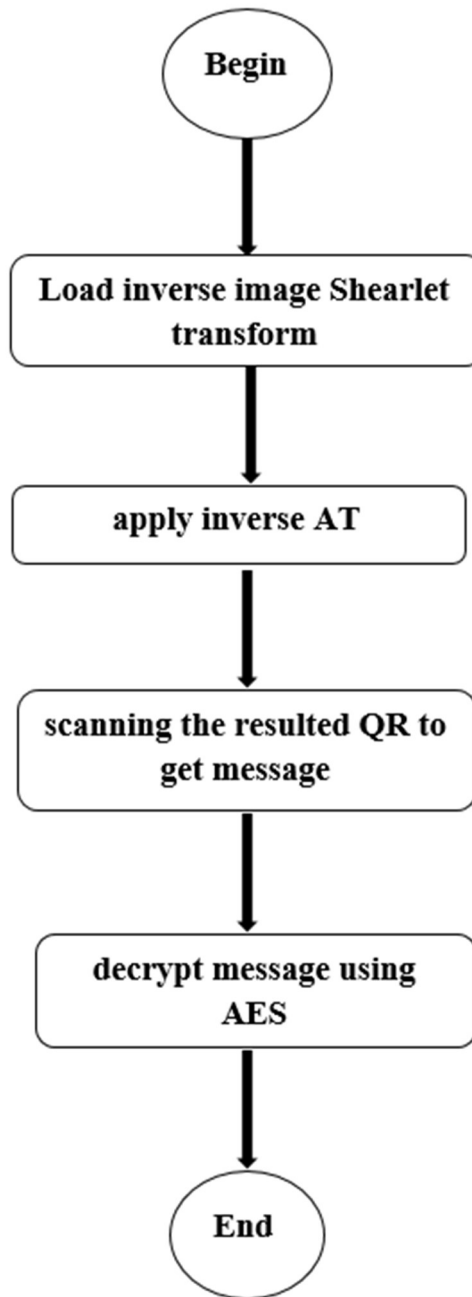


Figure 3.2: Decryption process

CHAPTER IV

IMPLEMENTATION AND THE RESULT DISCUSSION

4.1 Introduction

In the previous chapter the details of the proposed model were described and how to perform various encryption and decryption operations). This chapter show the implementation of the model in term of a computer program. A detailed description of how the program works by making a number of experiments as well as presenting the final results from the program operation will be included.

4.2 Programming languages used of the Implementation project

The implementation of this model is done by using PHP programming language xampp 5.6.21-0-VC11 to implementation all encryption and decryption steps, MATLAB version R2014a to implementation for Image Quality (PSNR & MSE) and histogram.

4.3 The Implementation

The Program that implemented by the tools above is contained a four main interfaces; First one is the step one of encryption (data ciphering), In this interface, the message is encrypted and converted to the QR code (a secret key must be entered as a password without which the four encryption and decryption phases are not completed. This password is used for more security) As shown in figures 4.1.

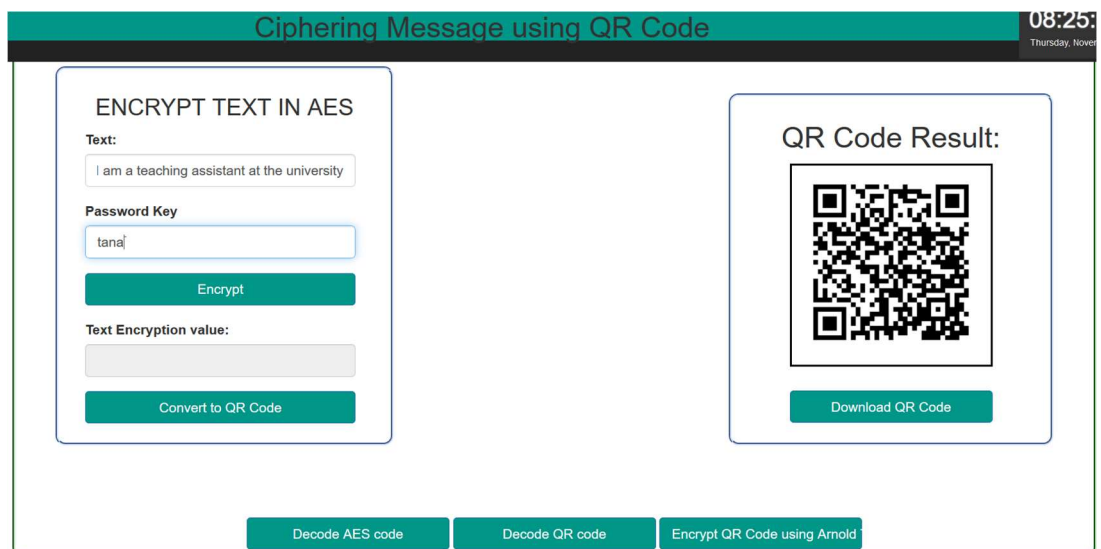
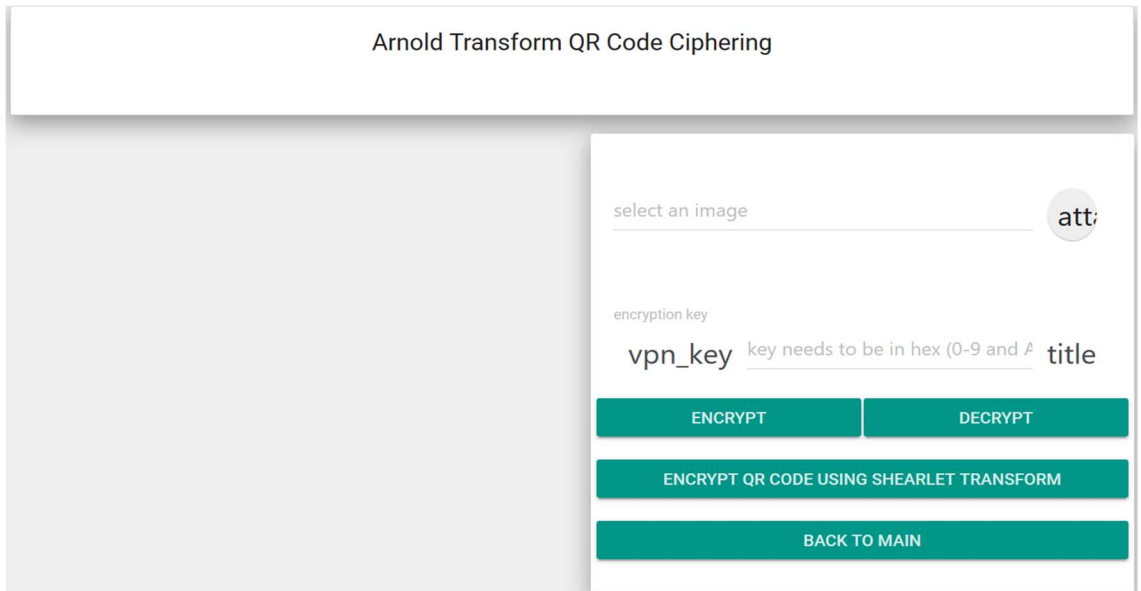


Figure 4.1: Encryption steps in the program.

In the figure 4.2 The second step of the encryption process, but you must choose the image of the QR code and enter the secret key entered in the previous stage to properly encrypt it. and Figure 4.3 after loading the QR code.



Arnold Transform QR Code Cipherring

select an image att:

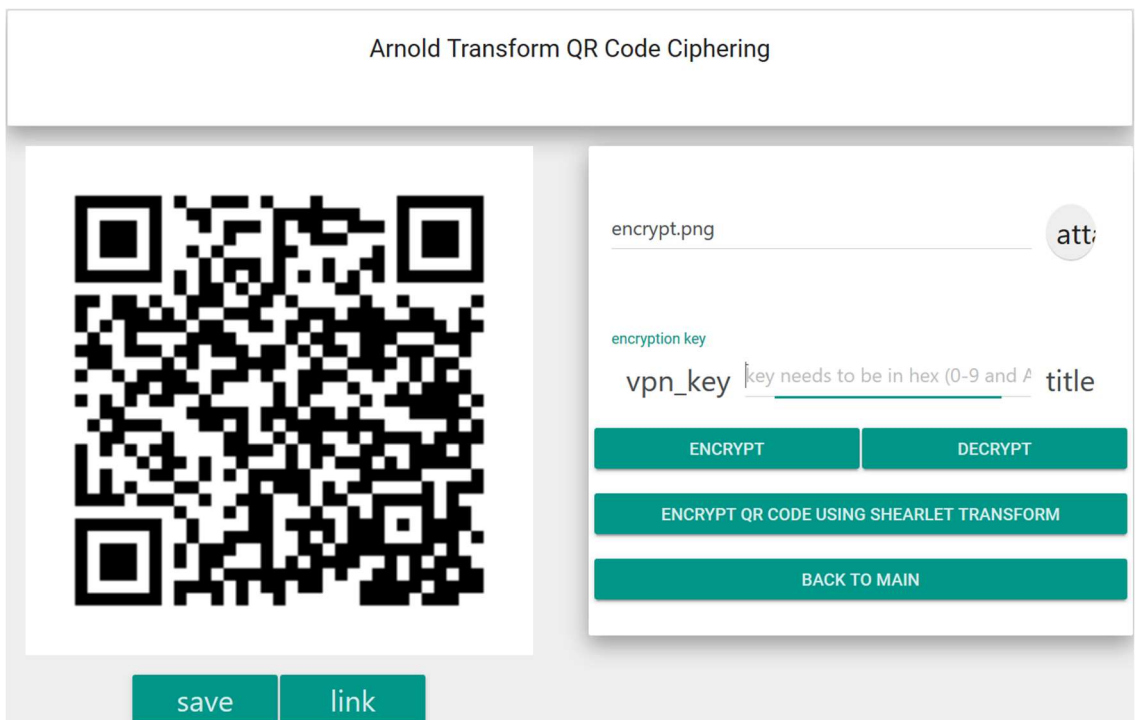
encryption key
vpn_key key needs to be in hex (0-9 and A) title

ENCRYPT DECRYPT

ENCRYPT QR CODE USING SHEARLET TRANSFORM

BACK TO MAIN

Figure 4.2: The step three Arnold transform Before loading the QR code.



Arnold Transform QR Code Cipherring

encrypt.png att:

encryption key
vpn_key key needs to be in hex (0-9 and A) title

ENCRYPT DECRYPT

ENCRYPT QR CODE USING SHEARLET TRANSFORM

BACK TO MAIN

save link

Figure 4.3: The step three Arnold transform after loading the QR code.

To encrypt the quick response code, enter the secret key and click the Encrypt button as shown in figure bellow:

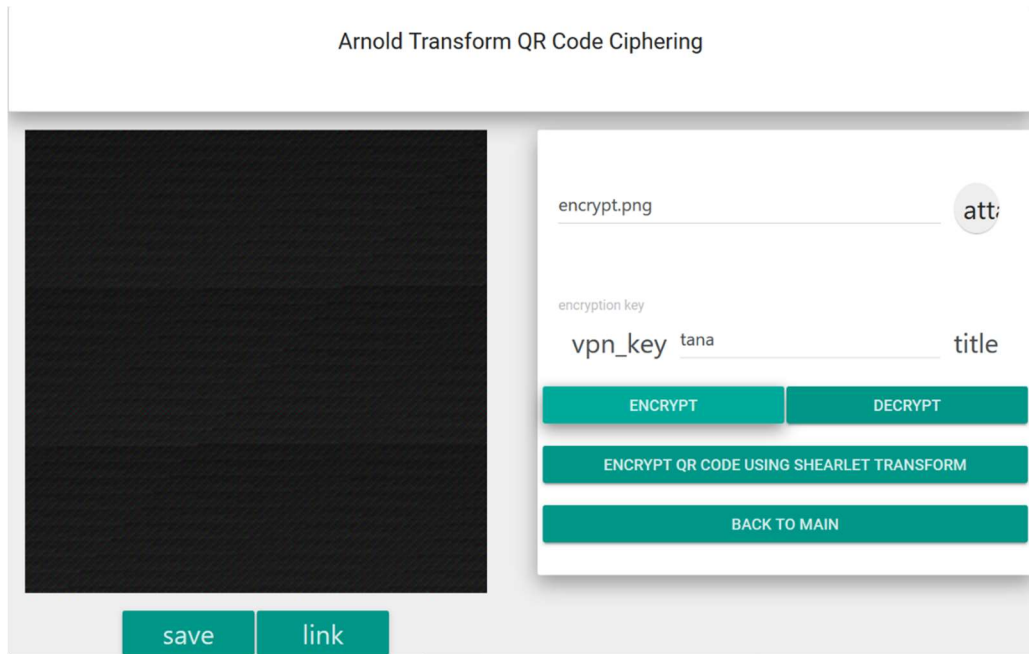


Figure 4.4: The Scrambled QR code by using the Arnold transform.

To complete the encryption steps, click on the previous screen button (encrypt QR code using shearlet transform) will appear a window asking to upload the image as shown in the figure 4.5 After loading the image of the encrypted QR code encrypted by Arnold transform must write the secret key to complete the process and click the encryption button to appear in the following figure:

Shearlet Transform QR Code Cipherring

The interface shows a form with the following elements:

- A placeholder text "select an image" with a circular "AT" icon to its right.
- An "encryption key" label above a text input field.
- The text input field contains "vpn_key" and has a tooltip that says "key needs to be in hex (0-9 and A-F)". A "title" label is to the right of the input field.
- Three teal buttons at the bottom: "ENCRYPT", "DECRYPT", and "BACK TO MAIN".

Figure 4.5: the step four Shearlet transform Before loading the encrypted QR code.

The interface shows the same form as Figure 4.5, but with the following changes:

- The image placeholder area is now a solid black rectangle.
- The text input field contains the filename "encrypted1543335305065.lec.png" and has a circular "AT" icon to its right.
- The "ENCRYPT" button is now highlighted in a darker teal color.
- Two new teal buttons, "SAVE" and "LINK", are located below the black image area.

Figure 4.6: the step four Shearlet transform after loading the encrypted QR code.

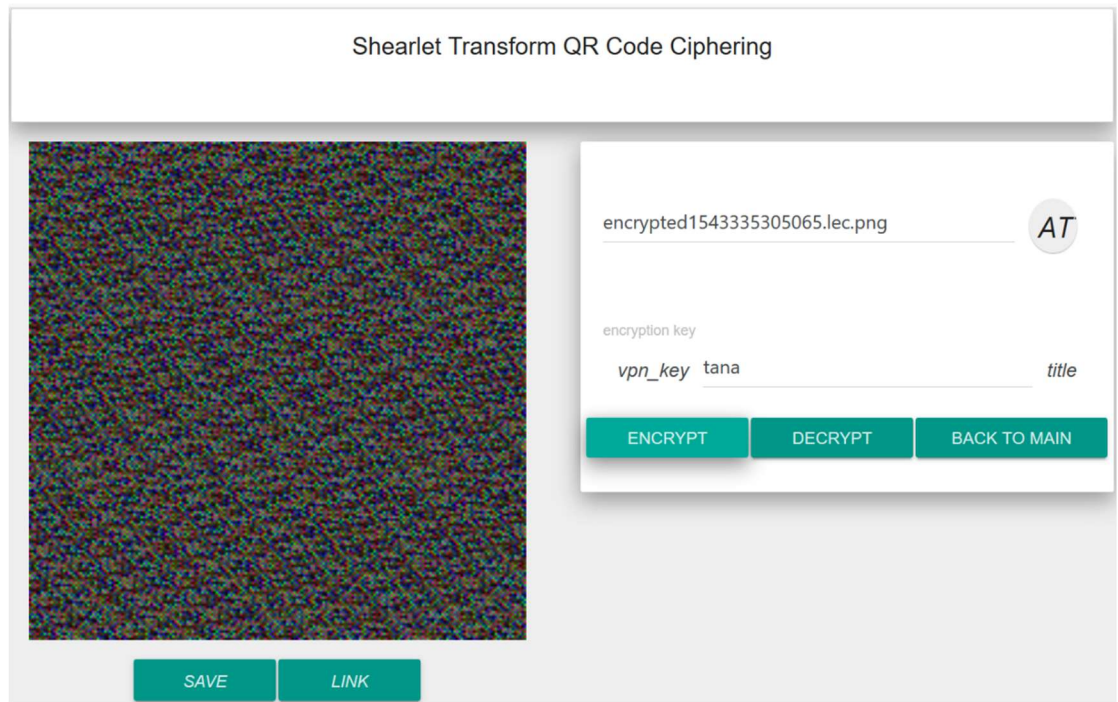


Figure 4.7: the encrypted QR code by using Shearlet transform (The image to be sent).

The decryption process is done for the last encrypted image by pressing the button (decrypt) in the Shearlet transform interface to obtain an encrypted image by Arnold transform, and the same step was done in the Arnold transform interface to get the QR code. to read the message from the QR code pressing the button (decode QR code) and load the image as shown in the figure 4.9 or scanning the code by using Camera and get the encrypted message.

To restore the original message, press the (decode AES code) button and enter the same password key as shown in the figure 4.10.

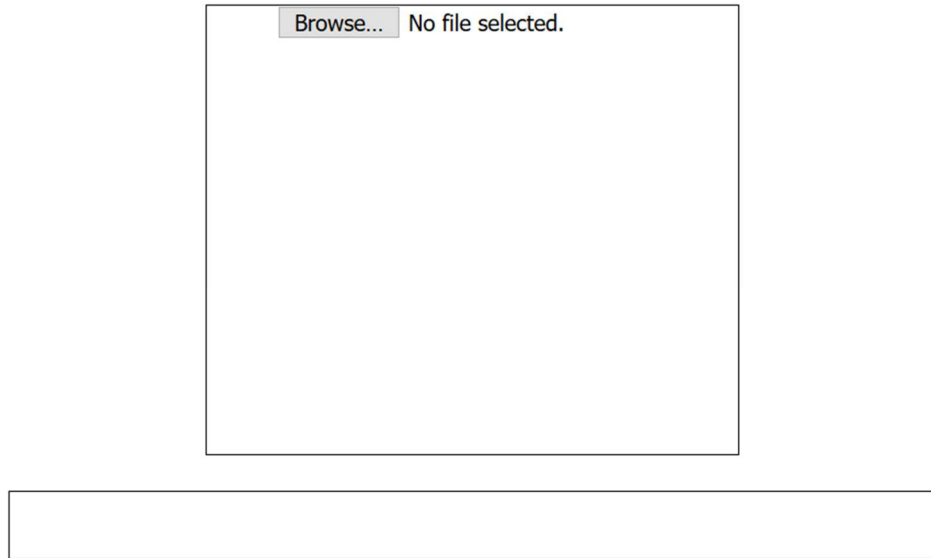


Figure 4.8: read the QR code before loaded.



Figure 4.9: Scanning the resulted QR to get message.

DECODE AES

DECRYPT AES TEXT

Text:

Password Key


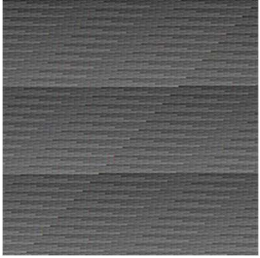
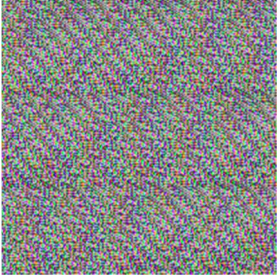


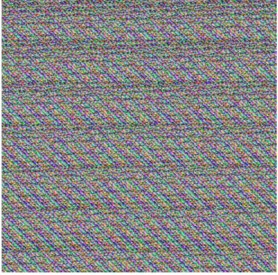


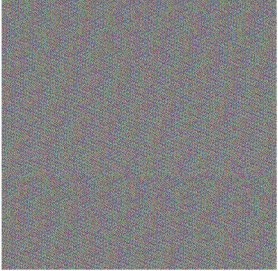
Original Text:

Figure 4.10: Decrypt message using AES.

4.4 Result and Analysis

The proposed system makes use of the advantages of QR code to enhance data security. In this method the secret message (Encrypted with the AES algorithm) is encoded into QR code using PHP (See Appendix for page 39,40,41). The table 4.1 shows that the pattern and the complexity of the QR code and Arnold transform and Shearlet transform differ according to the size of the message encrypted. The complexity will increase when huge amount of data is encrypted.

Table 4.1: Results of Encryption Process

NO. M	Original message (Different sizes)	Secret message	Corresponding QR code	Scrambled QR code (Arnold transform)	Shearlet transform
1.	I am a teaching assistant at the university	AiyUzuaBtP9tkBvv+sDkrlldBEDTGAF2Y+45xlwKVNgfo2zs4+M0aNJoC2+EVcLi			
2.	Everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory.	oXBM58pSAyuRn4HXkZkdyff+DSaB7v1sQAae0MutpuZ8E6dUdfs/z4+FnlmVeBWYquhjSvTX+z42oxeuhiTAKJE/qgXe/rVUdSj+us0y4QW+WUv7aZQ1XajqyWhiHPqRJK4TjHWu0Fkvpj5URBDGnl990SjgPjWvQ3plPyIUFdVJDmM+B1zJ48XCKc5rjwJAZmhMDFINRsDInoJT3wfFigg==			
3.	Due to tremendous growth in technology the problem of securing and sending confidential information has become a real challenge given the enormous capacity of hackers, The QR code has high storage capacity and it has possibility of concealing different types of data within it, but these QR code can be easily decoded by any smart	Vv9/S/1t6XcRaFP0ZnLmnowYKnMgAu9EK93QNiSxtU9OWLjiVWz6s8kNPEjVMer+Kz/LWApqyRrIREUxmHff7/PCm6HoRwC+Wmk57hgmveKsBMGgr7M6p9hAp6QKIRd6MgAunwEx2kR9AKd7CjF5hFTvNPSTWT4zeaWLMFuLhNuO8QIQxli5KDrCC2Ry84PaHqUMvgUE1X6JG45YKDAg9ByqIJdWmtk+wNcHCzUIGSYL4SUCLbd4OfNzUELXb69OHBCymBkBdYhvdwr9uq9At+9zG6XjDqCZQgKf8IL8Kt5Y2hUJN8AmvAnd5G8jbrNuEvdPcR0+9IDy9fMLpOf3ZqMHazjxVmDxF4BNFcAG7m54rHgFgkx6I4kRM87Hfi6tDCHoRtJ6j0p4AWC4+sdSpjDsB3ze1pQRo+SoDRw6xkTiJriaGGk7LwwhK6box8CRM+IgjMPX1Tvlpl6pCJcxV0OWrOuWJBEV4IYaJ2N			

	phone with built in camera therefore A new effective algorithm must be designed to secure QR code.	soVgloZ3MfclbMo/0hAs1oE3tdL6zhMvrIYj3xghSZjd9qGL3NkP2oVLB7DGBPboorcRgWEXMS3TTT39Q4xpJpyxs			
4.	Parents have a prior right to choose the kind of education that shall be given to their children.	swKH5OWgP10HU9c49z9lmZixAWAUeULhlGQP5zttWyxk+lMRoiCyAroTirB+k0CtzdJjQka5QqiyN+Us6z9seiXFiDI1zw1Yc+KtaqJPQ46iiBfwQZBF4Wx5jDvO1zI9Zegufzchg0vEIfH4fgCpNw==			
5.	Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.	VMHwsuiV14Wq2FEiZ6shCIArV9gF/aVA4OAE0LeCjJS01Uii5SqZb6zoW3X+/EQRrh6kB3kicSZKEm8VhNWCLml2hNjySTxpF2QiArePFjoAJsgXsAXch8DJhFa99unJZ2kB1mi5J5swJT9OkoWmCSdykSzkhh3B1XCb3qgSAo1AGToAv5Ce3fYISWHDbsh6RhCY4KnrF9GauDhkWRRTg==			

4.4.1 Message Integrity:

A security algorithm is considered as an efficient one if the receiver is able to extract the exact message that was hidden and sent. Message integrity means that a message has not been tampered with or altered. In this suggested mechanism the secret message is converted into QR code and the QR code is encrypted (confusion) by using Arnold and Shearlet transform, so the message retrieved in the extraction process is exactly the same as the hidden message. Thus, this method assures data integrity.

4.4.2 PSNR and MSE:

Any processing applied to an image may cause an important loss of information or quality, Image quality assessment plays an important role in image processing systems. Existing image quality evaluation methods can be divided into two kinds: Subjective evaluation and objective evaluation[21].

Objective quality assessment has been widely used in image processing for decades. In this research, we analyze the resulting images by using two well-known objective image quality metrics, the peak-signal-to-noise ratio (PSNR) and Mean Square Error (MSE). Given a reference image f and a test image g , both of size $M \times N$, the PSNR between f and g is defined by[22]:

$$\text{PSNR}(f, g) = 10 \log_{10}(255^2 / \text{MSE}(f, g)) \quad \{7\}$$

$$\text{MSE}(f, g) = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (f_{ij} - g_{ij})^2 \quad \{8\}$$

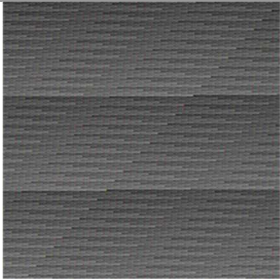
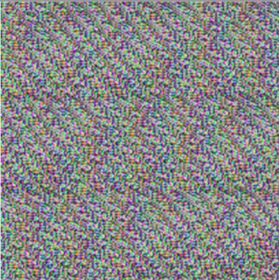
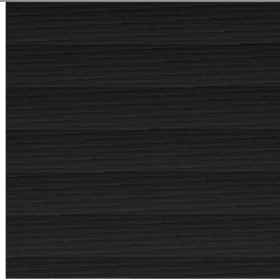
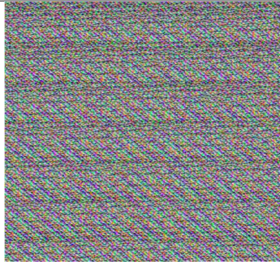

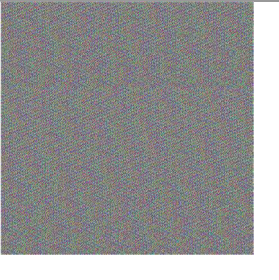
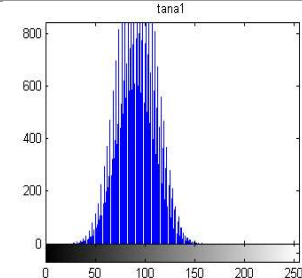
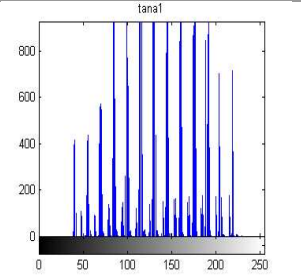
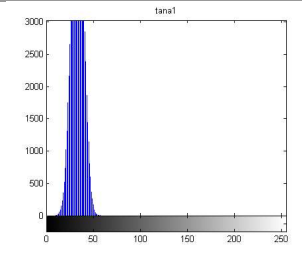
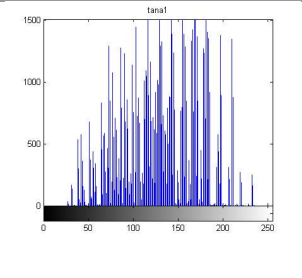
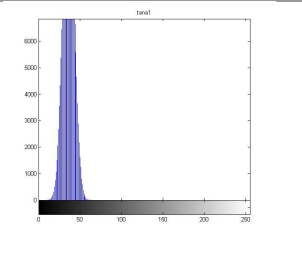
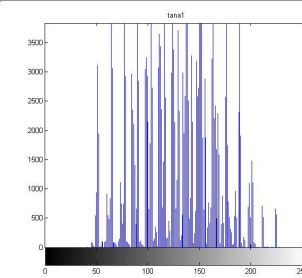
The PSNR value approaches infinity as the MSE approaches zero; this shows that a higher PSNR value provides a higher image quality. At the other end of the scale, a small value of the PSNR implies high numerical differences between images (See Appendix for page 44).

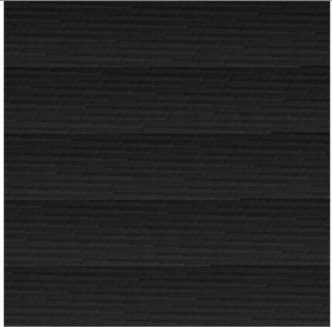
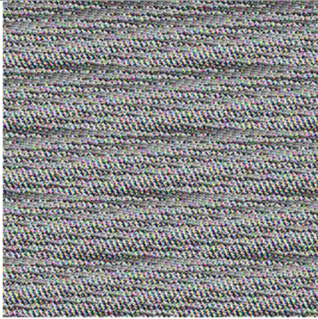
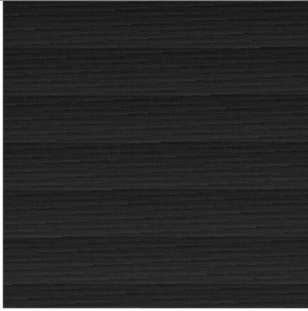
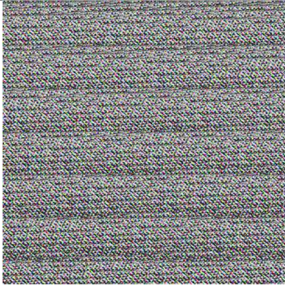
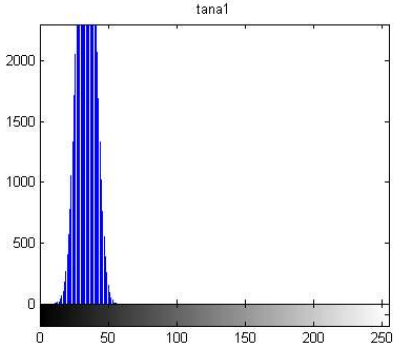
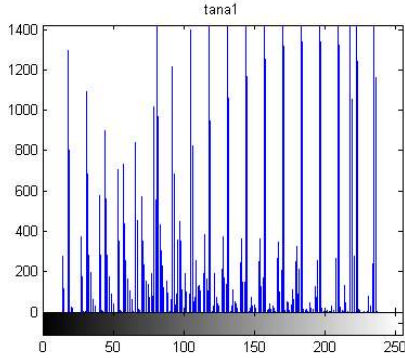
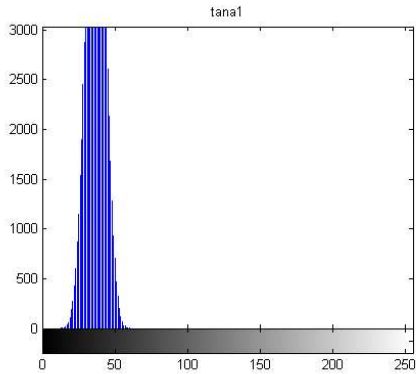
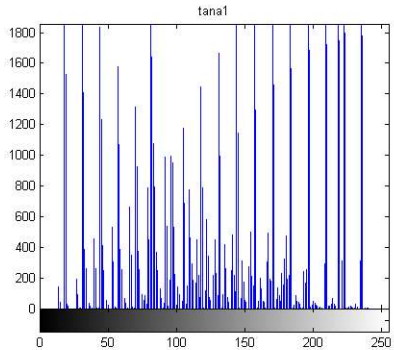
It can see that the PSNR is decreased semi-static for encrypted images by Shearlet transform when compared to the QR code and MSE is increase, this means that the noise and message size does not affect each other values, as shown in figure 4.9 and 4.10.

4.4.3 Histogram

A histogram is an accurate representation of the distribution of numerical data, also is a plot that lets you discover, and show, the underlying frequency distribution of a set of continuous data. The following histograms are drawn between pixel value of Arnold and pixel value of Shearlet transform. The histograms generated before and after Shearlet transform for different image sizes and are shown in Table 4.2. very large pixel values are changed When converting the encrypted image from Arnold to Shearlet transform (See Appendix for page 45).

Table 4.2: Comparison of histograms of Arnold and Shearlet image.

	AT	SHT	AT	SHT	AT	SHT
Encrypted QR Code						
PSNR & MSE	mse = 0.1351 psnr = 56.8253	mse = 0.3654 psnr = 52.5037	mse = 0.0160 psnr = 66.0974	mse = 0.3441 psnr = 52.7637	mse = 0.0196 psnr = 65.2174	mse = 0.3341 psnr = 52.8921
Histogram						
No. M	Message1		Message2		Message3	

	AT	SHT	AT	SHT
Encrypted QR Code				
PSNR & MSE	mse = 0.0178 psnr = 65.6311	mse = 0.3657 psnr = 52.4991	mse = 0.0207 psnr = 64.9747	mse = 0.3636 psnr = 52.5251
Histogram				
No. M	Message4		Message5	

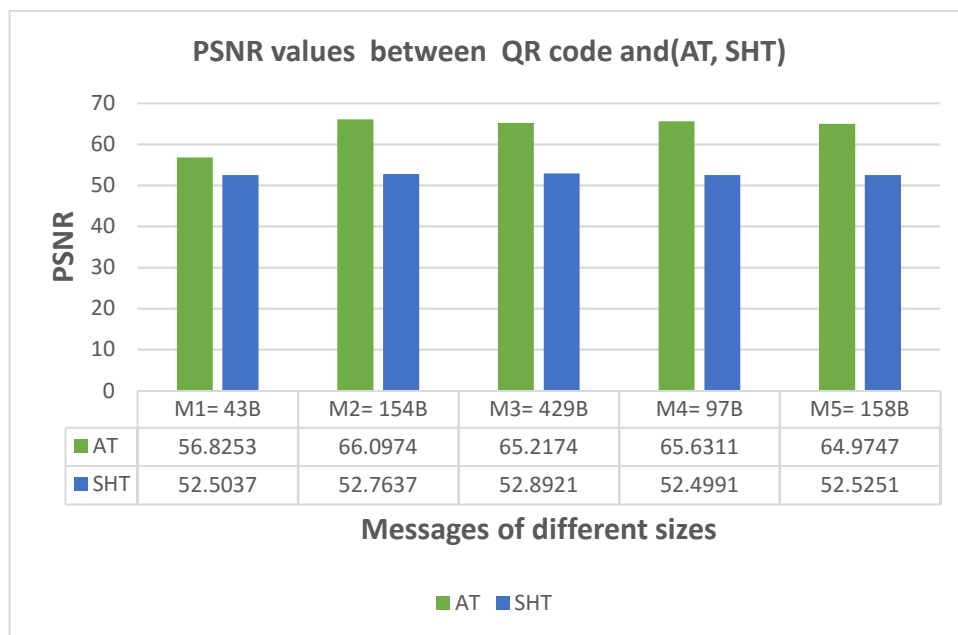


Figure 4.11. PSNR variation with Proposed Method

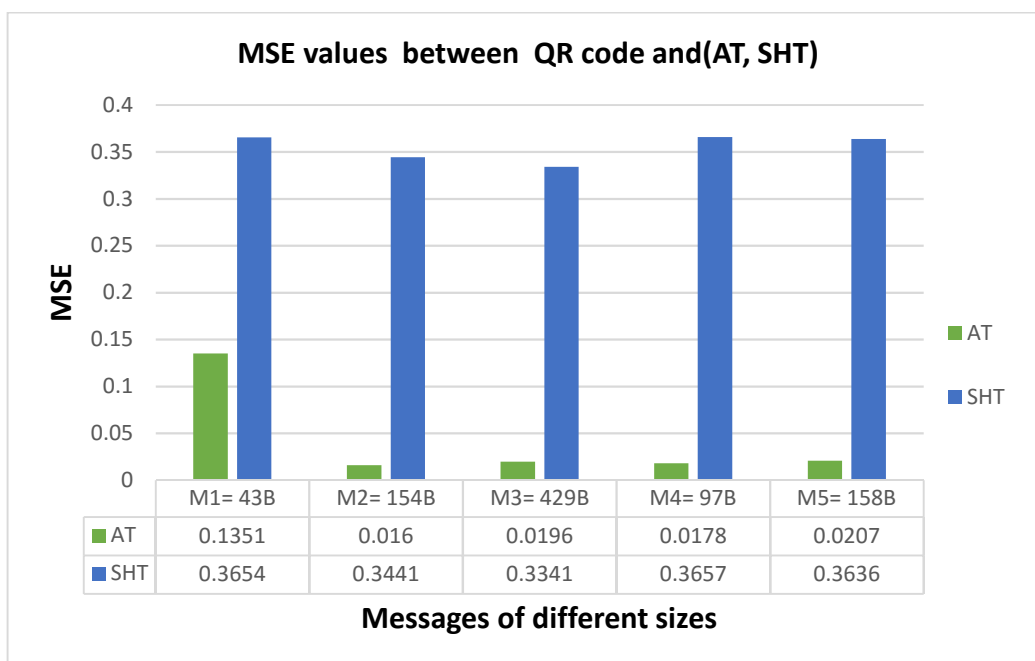


Figure 4.12. MSE variation with Proposed Method

4.4.4 Discussion of standard attacks

In order to evaluate the robustness of the proposed method against attacks, the proposed scheme is checked against Some attacks are known.

The proposed scheme provides a large set of security parameters that includes the AT, the decomposition of the ST, a password key when the message is encrypted, and attacker knows the encryption process, it is still very difficult to decode the encrypted image, which is very hard to retrieve the password key. Which makes a brute force attack difficult to execute.

It is important to note that chosen-plaintext attack (CPA) works against the linear schemes and the encryption processes known to attacker. However, the proposed scheme is resistant to CPA. Thus, if someone attempts such attack, the information about the security image and the number of decompositions used for the ST, their order, along with the scrambling parameters should be known to him. Also, a private key is used at all stages of encryption. So, the complexity of the proposed scheme makes it resistant to this type of attack.

The password key is generated during the encryption process, the receiver should have this key for correct decryption. The private key can be sent to the receiver using a different channel instead of sending it along with the encrypted image. Thus, we do not have to put our private key in the code book. Also, the hacker cannot decrypt the original image he must have the password security key.

CHAPTER V

THE CONCLUSION AND FUTURE WORK

5.1 The Conclusion

Securing confidential data is very important, so the data cannot be intercepted or misused for any kind of unauthorized use. The proposed technique is to conceal the secret information from any unauthorized use by using QR code to hide the secret message in different levels of security with the ability to retrieve the secret message again from all those levels. It has no size limitation, meaning that it can be applied to encrypt QR code images of any size. After converting the message to QR code, Arnold transform is used for scrambling the QR code, in addition to a layer using Shearlet transform for further improvement and security.

Different images are analyzed using MSE and PSNR values between the original QR code images and encrypted ones by Arnold and Shearlet transform as shown in figures 4.9 and 4.10. The robustness of the proposed method against brute force and chosen-plaintext attack is analyzed. Simulation results show the effectiveness of the proposed technique with enhanced security.

This method could be used in a large scope and to encrypt any type of messages (numeric, URLs, alphanumeric and so on) and send it to the receiver safely. Also, the method enables the user to store important data or information safely.

5.2 Future work

This study can provide the base for several future researches, the following points are suggested for further study:

1. Alter the design to accept different types of data (image, audio, Video).
2. Use QR Code to store files.

References:

- [1] P. Kieseberg *et al.*, "QR code security," in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, 2010, pp. 430-435: ACM.
- [2] R. Paul, "A review on Stegnography in QR Codes," 2018.
- [3] A. G. Sawant, V. N. Nitnaware, and A. A. Deshpande, "Advanced Encryption Standard Block Cipher Algorithm," 2018.
- [4] R. Kumar, B. Bhaduri, and B. Hennelly, "QR code-based non-linear image encryption using Shearlet transform and spiral phase transform," *Journal of Modern Optics*, vol. 65, no. 3, pp. 321-330, 2018.
- [5] D. Wave, "To two-dimensional code from the bar code," ed, 2014.
- [6] A. S. Narayanan, "QR codes and security solutions," *International Journal of Computer Science and Telecommunications*, vol. 3, no. 7, pp. 69-71, 2012.
- [7] S. Vongpradhip, "Use multiplexing to increase information in QR code," in *Computer Science & Education (ICCSE), 2013 8th International Conference on*, 2013, pp. 361-364: IEEE.
- [8] M. M. S. Rani and K. R. Euphrasia, "Data security through qr code encryption and steganography," *Advanced Computing: An International Journal (ACIJ)*, vol. 7, no. 1/2, pp. 1-7, 2016.
- [9] S. Dey, "SD-eqr: A new technique to use qr codestm in cryptography," *arXiv preprint arXiv:1205.4829*, 2012.
- [10] D. Selent, "Advanced encryption standard," *Rivier Academic Journal*, vol. 6, no. 2, pp. 1-14, 2010.
- [11] M. R. Abuturab, "Securing color information using Arnold transform in gyrator transform domain," *Optics and Lasers in engineering*, vol. 50, no. 5, pp. 772-779, 2012.
- [12] Z. Tang and X. Zhang, "Secure image encryption without size limitation using Arnold transform and random strategies," *Journal of multimedia*, vol. 6, no. 2, p. 202, 2011.
- [13] S. Wei, "The Periodicity of Arnold Transformation [J]," *Journal of North China University of Technology*, vol. 1, p. 006, 1999.
- [14] S. Häuser and G. Steidl, "Fast finite shearlet transform," *arXiv preprint arXiv:1202.1773*, 2012.
- [15] G. R. Easley and D. Labate, "Image processing using shearlets," in *Shearlets*: Springer, 2012, pp. 283-325.
- [16] W.-Q. Lim, "The discrete shearlet transform: a new directional transform and compactly supported shearlet frames," *IEEE Trans. Image Processing*, vol. 19, no. 5, pp. 1166-1180, 2010.
- [17] S. K. Thamer and B. N. Ameen, "A New Method for Cipherring a Message Using QR Code," *Computer Science and Engineering*, vol. 6, no. 2, pp. 19-24, 2016.
- [18] D. Sonawane, M. Upadhye, P. Bhogade, and S. Bajpai, "QR based Advanced authentication for all hardware platforms," *International Journal of Scientific and Research Publications*, vol. 4, no. 1, pp. 1-4, 2014.
- [19] S. Dey, S. Agarwal, and A. Nath, "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System," in *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, 2013, pp. 512-517: IEEE.
- [20] S. Dey, K. Mondal, J. Nath, and A. Nath, "Advanced steganography algorithm using randomized intermediate QR host embedded with any encrypted secret message: ASA_QR algorithm," *International Journal of Modern Education and Computer Science*, vol. 4, no. 6, p. 59, 2012.

- [21] G.-H. Chen, C.-L. Yang, and S.-L. Xie, "Gradient-based structural similarity for image quality assessment," in *Image Processing, 2006 IEEE International Conference on*, 2006, pp. 2929-2932: IEEE.
- [22] A. Hore and D. Ziou, "Image quality metrics: PSNR vs. SSIM," in *Pattern recognition (icpr), 2010 20th international conference on*, 2010, pp. 2366-2369: IEEE.

APPENDIX: Source Code

```
<?php

include('libs/phpqrcode/qrlib.php');

if(isset($_POST['submit1']) ) {

    $plaintext = $_POST['txt'];

    $password = $_POST['pass'];

    $method = 'aes-256-cbc';

    $key = substr(hash('sha256', $password, true), 0, 32);

    $iv = chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) .
chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0);

    $encrypted = base64_encode(openssl_encrypt($plaintext, $method, $key,
OPENSSL_RAW_DATA, $iv));

}

if(isset($_POST['submit2']) ) {

    $tempDir = 'temp/';

    $filename = "encrypt";

    $codeContents = $_POST['eTxt'];

    QRcode::png($codeContents, $tempDir.".$filename.'.png', QR_ECLEVEL_L, 5);

}

?>
```

```
<!DOCTYPE html>
```

```
<html lang="en-US">
```

```
  <head>
```

```
    <title>Ciphering Message using QR Code</title>
```

```
    <link rel="icon" href="img/favicon.ico" type="image/png">
```

```
    <link rel="stylesheet" href="libs/css/bootstrap.min.css">
```

```
    <link rel="stylesheet" href="libs/style.css">
```

```
    <script src="libs/navbarclock.js"></script>
```

```
    <script type="text/javascript" src="/js/llqrcode.js"></script>
```

```
    <script type="text/javascript" src="/js/webqr.js"></script>
```

```
</script>
```

```
function ShowPopUp(popUpPage)
```

```
{
```

```
  window.open(popUpPage,
```

```
  'window','toolbar=0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=900  
,height=700');
```

```
}
```

```
function ShowPopUp2(popUpPage)
```

```
{
```

```
  window.open(popUpPage,
```

```
  'window','toolbar=0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=700  
,height=700');
```



```
}
```

```
</script>
```

```
</script>
```

Decode QR code:

```
<head>
```

```
<style type="text/css">
```

```
body{
```

```
    width:100%;
```

```
    text-align:center;
```

```
}
```

```
#qrfile{
```

```
    width:320px;
```

```
    height:240px;
```

```
}
```

```
#qr-canvas{
```

```
    display:none;
```

```
}
```

```
#outdiv
```

```
{
```

```
    width:320px;
```

```
    height:270px;
```

```
border: solid;

border-width: 1px 1px 1px 1px;

}
```

```
#result{

border: solid;

border-width: 1px 1px 1px 1px;

padding:20px;

width:57.3%;

}
```

```
#imghelp{

position:relative;

left:0px;

top:-160px;

z-index:100;

font:18px arial,sans-serif;

background:#f0f0f0;

margin-left:35px;

margin-right:35px;

padding-top:10px;

padding-bottom:10px;

border-radius:20px;
```

```
}
```

```
p.helpertext{
```

```
margin-top:54px;
```

```
font:18px arial,sans-serif;
```

```
}
```

```
p.helpertext2{
```

```
margin-top:100px;
```

```
font:18px arial,sans-serif;
```

```
}
```

```
</style>
```

```
</head>
```

```
<script type="text/javascript" src="js/llqrcode.js"></script>
```

```
<script type="text/javascript" src="js/webqr.js"></script>
```

```
<body onload="load(); setimg();">
```

```
</body>
```

```
<center>
```

```
<div id="main">
```

```
<div id="mainbody">
```

```
<div id="outdiv">
```

```
</div>
```

```
<br/>
```

```
<div id="result" ></div>
```

```
</div></div>
```

```
<canvas id="qr-canvas" width="800" height="650"></canvas> <!--Canvas to draw image --
```

```
>
```

```
</center>
```

```
</body>
```

```
</html>
```

PSNR&MSE:

```
%save this matlab function as mse_psnr.m
%To calculate PSNR follow instruction
%function [mse,psnr] = mse_psnr(imshearletcoefficientst,invsh)
% find the size of image l
z=imread('o.png');
%L = (0:255);
%pixel_max= (L-1);
N = size(z)

%convert image into double
x=im2double((imread('o.png')));
y=im2double((imread('d.png')));
%Now calculate MSE then PSNR for a original and encrypted image
acc = 0;
for k1=1:N(1)
for k2=1:N(2)
acc = acc+ ( x(k1,k2) - y(k1,k2) )^2;
end
end
mse = acc/(N(1)*N(2))
%calculate psnr for the original and encrypted image
psnr = 10*log10((255^2)/mse)
%imshow(acc);
```

Histogram:

```
x=imread('712.png');  
imshow(x);  
a_gray=rgb2gray(x);  
imhist(a_gray); title('tana1');
```