
بسم الله الرحمن الرحيم

Geometrical Transformations Dependent Quantum Image Encryption and Decryption

By

Usman Ali

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2020

Geometrical Transformations Dependent Quantum Image Encryption and Decryption

By

Usman Ali

Supervised by

Prof. Dr. Tariq Shah

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2020

Geometrical Transformations Dependent Quantum Image Encryption and Decryption

By

Usman Ali

A Dissertation Submitted in the Partial Fulfillment of the Requirement for the Degree of

MASTER OF PHILOSPHY

IN

MATHEMATICS

Supervised by

Prof. Dr. Tariq Shah

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2020

Declaration

This dissertation is dedicated

To the Super hero of my life, My Father.

To the best Psychiatrist of the world, My Mother.

To My Grand Parents.

To My Uncles specially to Uncle Abdul Majeed.

To My Brothers (Afnan & Rehan) and Sister.

Acknowledgements

First and foremost, **ALLAH** Almighty for all the blessings. He has bestowed upon me. I pray to him to open my heart, make my work easy for me, remove the impediment from my speech and bless with courage to full my duties with honesty. I pay tribute to the **HOLY PROPHET HAZRAT MUHAMMAD** (peace be upon him) whose life has been forever a beacon of knowledge and guidance for whole humanity.

Writing this thesis ends the journey I started about two years ago in FALL 2018. Therefore, I want to take the opportunity to acknowledge all those who, in one way another, have contributed to this reaching of my goal. To their kindness and support, "THANK YOU VERY MUCH".

I like to offer my deepest gratitude to my supervisor **PROF. DR. TARIQ SHAH**, for giving me an opportunity to pursue my M. Phil thesis under his grand supervision. His kind attitude, his always having time for discussion, despite being a supervisor to many students, and his deep knowledge in the vast field of Pure Mathematics have always been a source of inspiration. I would never have made it that far and could not have completed my work without his continuous support, kindness and sympathy. I would also like to express my sincere thanks to my supervisors: **PROF. DR. TARIQ SHAH** for his constant, and constructive guidance throughout the study. I am very grateful to my dear parents, sweet brothers and sister, respected friend, teacher, guidance and supporter.

In this tenure, I have been blessed with a friendly and cheerful group of fellow colleagues and classmates. I would like to thank them for a wonderful company, outdoor trips and time-to-time discussions on various topics. Many thanks to my friends (Arif Hussain, Tasawar Hussain, Muhammad Ramzan, Muhammad Sajjad, Hafeez-ur-Rehman, Salah-ud-din, Zahid Saif Ullah, Asad Ullah Khan, & Naseem Abbas) for making my stay in the university a memorable part of my life. One simply couldn't wish for a better company which I had in last two years.

My endless gratefulness goes to my family, for loving and supporting me in every step of my life. I pride myself in having the most lovable Parents, today all I have is part of their tiring efforts and encouragement. My especial thanks go to my Uncle Abdul Majeed, to my friend Naveed Siddique and my family for all their love and care.

I am also thankful to my research fellows and all those who have always stood by me. Also, my seniors and juniors' fellows and those peoples who always remember me in special prayers.

Usman Ali

Preface

Over thousands of years ago, cryptography already come into know to make certain the secrecy of data, such as the ancient Egyptians, who used cipher to transmit military intelligence [1]. However not before the arrival of the secure communication information theory by C.E.Shannon in 1949 [2], did cryptography elaborated to a real science subject of cryptology.

In 1967, Diffie Hellman put forward the public-key cryptosystem [3] which constitute two branches of modern cryptography with the symmetric cryptosystem. However, with the fast development of calculations and advent of various advanced algorithms, including the classical [4] and quantum compliment [5,6], the security of symmetric and asymmetric cryptography has to be faced with the sever challenges. In 1994, Shor proposed the factorization of large number algorithm [5] which has formed a great threat to the public key cryptosystem that based on the problem of large number decomposition and discrete logarithm solution over finite field. The arrival of Grover quantum search algorithm in 1995 further proved the powerfulness of quantum computer [6].

Looking from other areas, as the great powerfulness of quantum computation, a supply of issues remained by classical computation are fixed. Therefore, more and more comprehensive disciplines combined with quantum information appeared [7] in which the quantum image processing included. In point of view of development of quantum image processing, there are two branches exposed their huge capacity: quantum image signal processing and quantum image transformation.

The storage of quantum image in quantum states is different in literature and can be studied in the [8], [9], [10], [11], [12]. Elementary gates which are used in this study are also given in [13] and the storage in quantum array is in [14] and the formation

of full binary tree is given in [15]. The geometric transformation which are major contribution in this thesis to perform the encryption and decryption procedure in image process is given in [16].

Chapter 1 contain the notations, basic discussions and notations used in the rest of the thesis. These specific definitions and discussions can be read out separately when needed. All the necessary prerequisites of quantum mechanics and cryptography may be found in many basic books of these subjects.

Chapter 2 contains the basic discussion about the storing expression of quantum image and all the quantum geometric transformations which are used in this thesis. Chapter 3 describes the geometric transformations that can be used in designing the encryption and decryption algorithm based of information given in chapter 1 and chapter 2, and the conclusion.

Contents

Table of Figures

Chapter 1

Quantum Mechanics and Cryptographic Background

1.1 Quantum related terms

1.1.1 Definitions

1.1.1.1 Definition

Quantum mechanics is science interacting with the behavior of matter and light at the atomic and subatomic level.

1.1.1.2 Definition

Quantum image contains image information in mechanical quantity schemes instead of conventional ones and replaces classical with quantity information processing.

1.1.1.3 Definition

Gray scale image is one in which the value of each pixel is single sample representing only an amount of light, that is it carries only intensity information.

1.1.1.4 Definition

A bijection of set having some geometric structure to itself or another such set is geometric transformation.

1.1.1.5 Definition

The collection of all relevant physical properties of a quantum system is known as the state of the system.

1.1.1.6 Traditional description of Quantum bits

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

1.1.1.7 Definition

Qubit is the basic unit of quantum information that is physically realized with a two-state system as the quantic version of the classic binary bit.

1.1.1.8 Definition

A quantum circuit is a quantity computation model in which a calculation is a series of quantity gates, which are reversible transformations on a n-bit register's quantum mechanical analog.

1.1.1.9 Definition

In mathematics a unitary transformation is a transformation that retains the inner product: after the transformation, the inner product of two vectors before the transformation is equal to their inner product.

1.1.1.10 Definition

The Hadamard gate works on a single qubit. It maps the basic state $|0\rangle$ and $|1\rangle$ to $\frac{|0\rangle+|1\rangle}{2}$ and $\frac{|0\rangle-|1\rangle}{2}$ respectively, which means measurement is equal probabilities to 1 or 0 range.

1.1.1.11 Definition

Let A and B are two matrices having order $m \times n$ and $p \times q$ respectively then their tensor product can be shown as

$$M \otimes N = \begin{pmatrix} M_{11}N & M_{12}N & \cdots & M_{1n}N \\ M_{21}N & M_{22}N & \dots & M_{2n}N \\ \vdots & \vdots & \vdots & \vdots \\ M_{m1}N & M_{m2}N & \dots & M_{mn}N \end{pmatrix}$$

In the above expression, $M_{11}N$, $M_{12}N$, $M_{13}N$, $\ldots, M_{1n}N$, $M_{2n}N$, $M_{mn}N$ are all the matrix of $p \times q$,M_{11}, $M_{12,} \ldots, M_{1n}, \ldots M_{mn}$ are the coefficient of matrix *N* respectively, where $M \otimes N$ is a matrix $mp \times nq$.

1.1.1.12 Definition

Quantum computing, which deals with, on the one hand, the question of how and whether a quantum computer can be constructed and, on the other, the search for algorithms which exploit its power.

1.1.1.13 Definition

Quantum computation which examines the computational complexity of different quantum algorithms.

1.1.1.14 Definition

Quantum entanglement is a phenomenon in which the quantum of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated.

1.1.1.15 Definition

Quantum communication is an area of applied quantum physics closely related to the transmission of quantum information and quantic teleportation. The most interesting use is to secure the communication networks by means of quantum cryptography against eavesdropping.

1.1.1.16 Definition

Superposition is the tendency of a quantum system to simultaneously be in several states before calculated.

1.1.1.17 Definition

A projection-valued measure (PVM) in mathematics, especially in functional analysis, is a function defined on certain subsets of a fixed set and whose values are self-adjoint projections on a fixed Hilbert space. PVMs are the statistical definition of projective measures in quantum mechanics.

1.1.1.18 Definition

Quantum image processing (QIMP) is primarily dedicated to the use of quantum computing and processing of quantum information to create and work with quantum images.

1.1.1.19 Definition

Eavesdropping is the intercepting and reading the message and conversation by unintended recipient. One who participates in eavesdropping, i.e. someone who secretly listens in on the conversation of others, is called eavesdropper.

1.2 Cryptographical Background

1.2.1 Definitions

1.2.1.1 Definition

Cryptography is the study of secure communication techniques that only allow a message to be read by the sender and intended recipient.

1.2.1.2 Definition

The primary information to be input and countable collection for possible plain texts is plain text space.

1.2.1.3 Definition

The result after encryption from the plain text and the countable collection for possible cipher texts is cipher text space.

1.2.1.4 Definition

The function to converting original plain text to cipher text and the whole set is controlled by encrypted key is encryption space.

1.2.1.5 Definition

The function to convert cipher text to plain text and whole set is controlled by decrypted key is decryption space.

1.2.1.6 Definition

The criterion to converts and the countable set of all keys is key space.

1.2.1.7 Definition

Symmetric cryptosystem requires the use of a single key for both encryption and decryption.

1.2.1.8 Definition

Asymmetric cryptosystem requires the use of different keys for encryption and decryption.

1.3 Quantum Cryptography

With the development of quantum physics, cryptographer have to think the new techniques to ensure security in conversation, particularly when quantum computer become reality. Classical cryptography uses the mathematical techniques, but quantum cryptography is focused on the physics of information. Quantum cryptography deals with the security of communication and this secure is best with only on the validity of quantum theory. The physics of quantum cryptography opens the door to huge intriguing ways for cryptography. The thing which lies at the root of quantum cryptography is indivisible quanta and entangled system which have a interesting characteristics in quantum mechanics. Quantum cryptography is one of the few commercial applications of quantum physics at a single quantum level. Other uses of quantum mechanics to cryptography, which tends to come in three ways:

- Quantum mechanics can be used to break the classical cryptographical protocol.
- Quantum states can make new or improved cryptographical protocols protecting classical information.
- Cryptographic method can be applied to prevent the quantum information instead of classical information.

The idea of quantum cryptography was first proposed in the 1970s, though it is only now that the field is applied to information security. The main advantage of quantum cryptography is that it gives us a perfectly secure transformation of data.

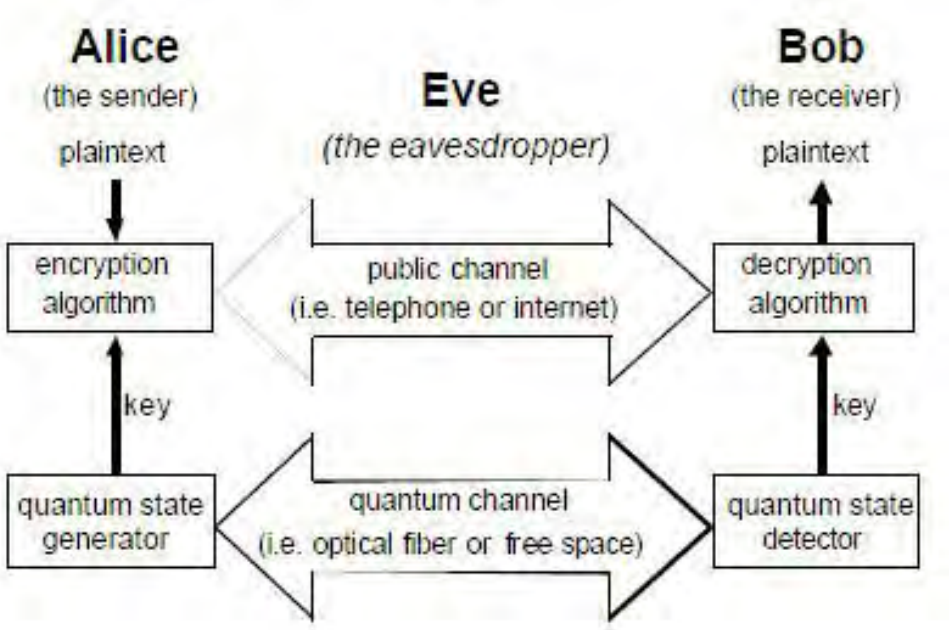

Figure 1.1

Quantum Cryptography is the study of leveraging mechanical quantity properties for cryptographical tasks. It enables two parties to generate a mutual, random bit string known to them only, which can be used as a key for encrypting and decrypting messages. Physicists have found a technique to share date on hidden keys by exploiting the random character of matter at quantum level. Quantum cryptography studies the drawbacks and difficulties arising from quantum opponents including the complexity of quantity bit interact ion, the difficulty of quantity rewinding and the concept of quantity safety models for classical primitives. Quantum cryptography has potential to guarantee exactly secure communication. Quantum cryptography depends upon the fundamental and unchanging principles of quantum mechanics.

Chapter 2

Quantum Gray Scale Image Storing Expression and Geometric Transformation.

2.1 Image storing preliminaries

Extracting, encoding and saving the data are operations that are considered simple and popular in classical computing. But on quantum level, they remain difficult. One of those tasks is to properly preserve and process image data. As more people look deeper into this area, the researchers aim to reduce the number of qubits used to represent images, as well as the number of simple operations needed to store and operate the image. This would be needed to reduce the loss of information and to make better use of the quantum channel of communication. A suitable representation using quantum properties is important for practical image analysis, allowing use of mathematical tools such as transformation of the quantum wavelet.

In the study of representation of quantum image, many algorithms provided the basis for the field and the resulting presentation opened the way for the region of the art development. I have also broadened our experience by introducing am algorithm to help understanding the complexities of how it works.

Several quantum representation models for quantum image have been developed. A commonly used quantum representation of quantum images named as flexible representation of quantum image was presented in Ref. [12]. Here another way is introduced to represent the quantum image. Take the quantum gray scale image instead of classical image. The gray scale of image is divided into 256 levels, between 0 to 255. Each level is considered as pixel and position information. Increasing the pixel of greyscale image consisting of greyscale and location knowledge has no color significance, the color saturation of each is 0.

The grey knowledge and position properties are derived from the grey level image to produce image representation in quantum state as follows

$$|Q\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|N\rangle \otimes |j\rangle \qquad (1)$$

Take the quantum gray scale image instead of classical image. The gray scale of image is divided into 256 levels, between 0 to 255. Each level is considered as pixel and position information.

Within this formula $|Q\rangle$ is storage for gray scale representation of all quantum states. The qubit binary string represents $|N\rangle$ used for encoding the greyscale of the quantum picture. Since the values of greyscale are from 0 to 255 which is not so big, it doesn't complicate to express. In different positions, it may be same of the greyscale, except opposite, the greyscale in the same location should distinct, so the image given can be determined by the quantum state. That is, the value of N is fixed in one place, while N is a chain variable value that ranges from zero to 255. $|j\rangle$ ciphers the quantum image position data, where j is yet a binary string. From description, $j = 0,1,2,3,\ldots 2^{2n}-1$, the we will have this $|j\rangle = |0\rangle, |1\rangle, |2\rangle, |3\rangle, \ldots |2^{2n}-1\rangle$. The greyscale picture reflects the 2nd quantum basic states. " $\otimes$ " is known as Kronecker product and works as following:

Consider that $M\ and\ N$ are two matrices having order $u \times v$ and $r \times s$ respectively. Then the act of tensor product can be shown as:

$$\mathrm{M}\otimes\mathrm{N} = \begin{pmatrix} \mathrm{M_{11}N} & \mathrm{M_{12}N} & \cdots & \mathrm{M_{1v}N} \\ \mathrm{M_{21}N} & \mathrm{M_{22}N} & \ldots & \mathrm{M_{2v}N} \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{M_{u1}N} & \mathrm{M_{u2}N} & \ldots & \mathrm{M_{uv}N} \end{pmatrix} \qquad (2)$$

In the above expression, $M_{11}N$, $M_{12}N$, $M_{13}N$, ... , $M_{uv}N$ are all the matrices of order $r \times s$, M_{11} , M_{12} , . . . , M_{1v} , . . . , M_{uv} are the coefficients of matrix N respectively , while $M \otimes N$ is matrix having order $ur \times vs$.

While processing quantum image, alike to classical image that each pixel can be shown by vertical and horizontal order. The way to break the presentation of $|j\rangle$ which explain the location information, as follows:

$$|j\rangle = |f\rangle|g\rangle \qquad (3)$$

Where $|f\rangle$ describe the data of x axis, while $|g\rangle$ represent the data for the y axis.

Let us consider that any image of 4×4 which is specified by the qubits.

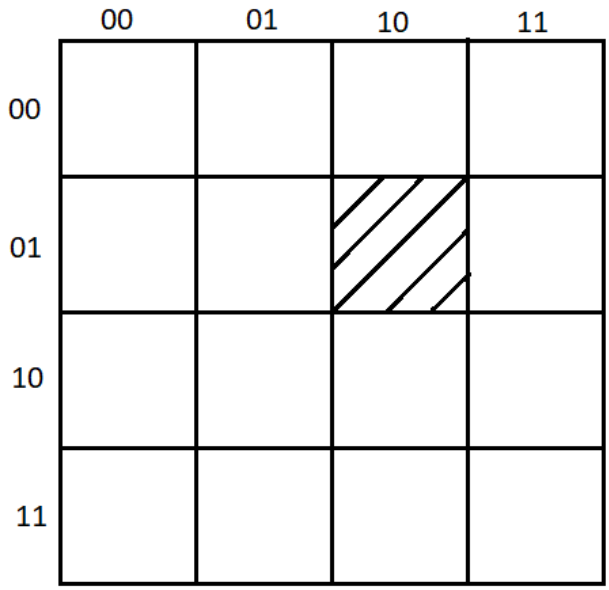

Figure 2 . 1 *Image of* 4×4

In the above figure, it is 4×4, each pixel has two double qubits. For indicated pixel in Fig. 2.1, specified location can be calculated as:

$$|j\rangle = |f\rangle|g\rangle = |10\rangle|01\rangle = |1001\rangle \qquad (4)$$

Again, consider a gray-scale image of 2×2

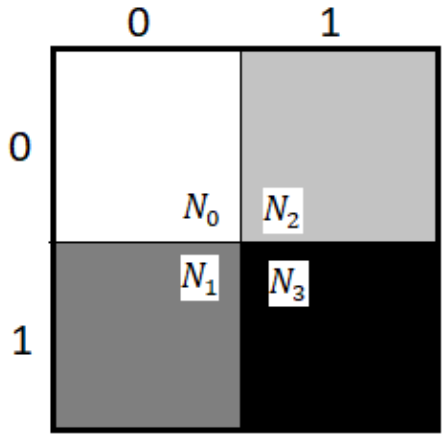

Figure 2.2 Grey − scale Image of 2×2

As a result of evolved expression for 2×2 Gray-scale image in Fig. 2.2, is represented as follows

$$|Q\rangle = \frac{1}{2}(|N_0\rangle \otimes |00\rangle + |N_1\rangle \otimes |01\rangle + |N_2\rangle \otimes |10\rangle + |N_3\rangle \otimes |11\rangle \quad (5)$$

In the Fig.2.2, each pixel in the grayscale is different from each other in the image. Also, note that N_0 , N_1 , N_2 and N_3 are explained by binary strings and are distinct. Also, gray-scale value of every location in the image is unconstrained.

2.2 Formation of Quantum Array

The designing of quantum collection is most considerable operation that optimal Quantum Binary Decision Diagram to be changed to a quantum collection. So that the wanted quantum positions can be stored.

QBDD can be built by superposition of quantum state. A simple QBDD is shown as:

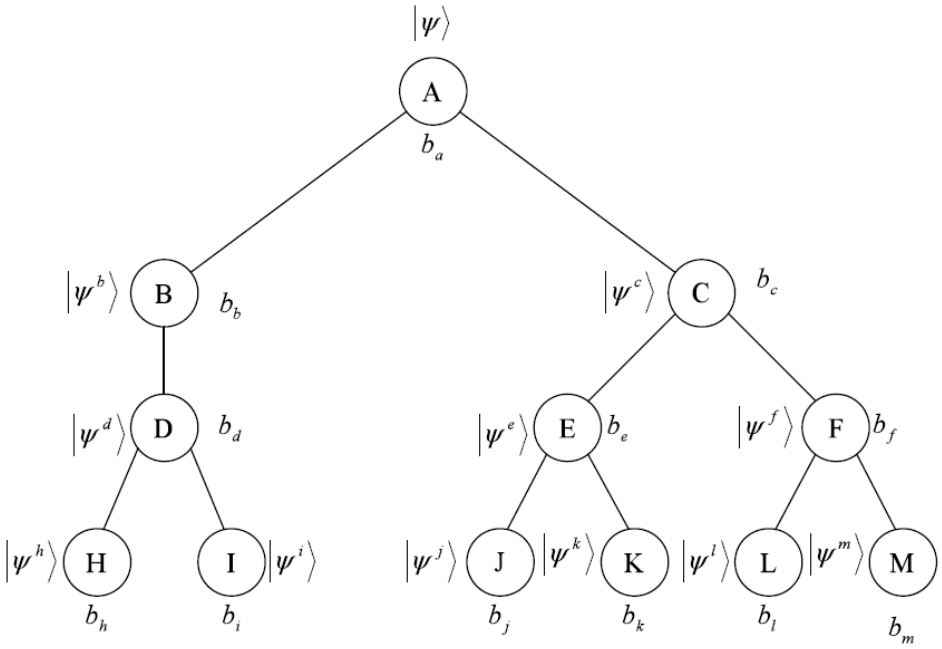

Figure 2 . 3 A simple QBDD

In the Fig.2.3 , the A, B , … , M are quantum gates , b_a , b_b , . . . , b_m are nodes , b_a is the root node , the $|\psi^h\rangle$, $|\psi^i\rangle$, $|\psi^j\rangle$, $|\psi^k\rangle$, $|\psi^l\rangle$, $|\psi^m\rangle$ are chosen quantum states. The gate which accord to node on every subdivision of QBDD is commanded by the path which is used to achieve it from the root of decision diagram. Thus, every branch of the QBDD represent a diverse component of the chosen quantum state.

The optimal QBDD can be obtained by reducing the nodes. QBDD has two directions as follows:

In two distinct subdivisions of unlike nodes which relate to the equivalent next nodes, so the node consolidates.

In unlike subdivisions of distinct nodes which produce a similar branch, the branch combines.

The number of nodes in simple QBDD can be reduced by using the above rules. Let us consider that the nodes b_d , b_e, b_f create the similar subdivisions in Fig. 3 , then QBDD with nodes b_h , b_i , b_j , b_k , b_l , b_m are merged in Fig. 2.4

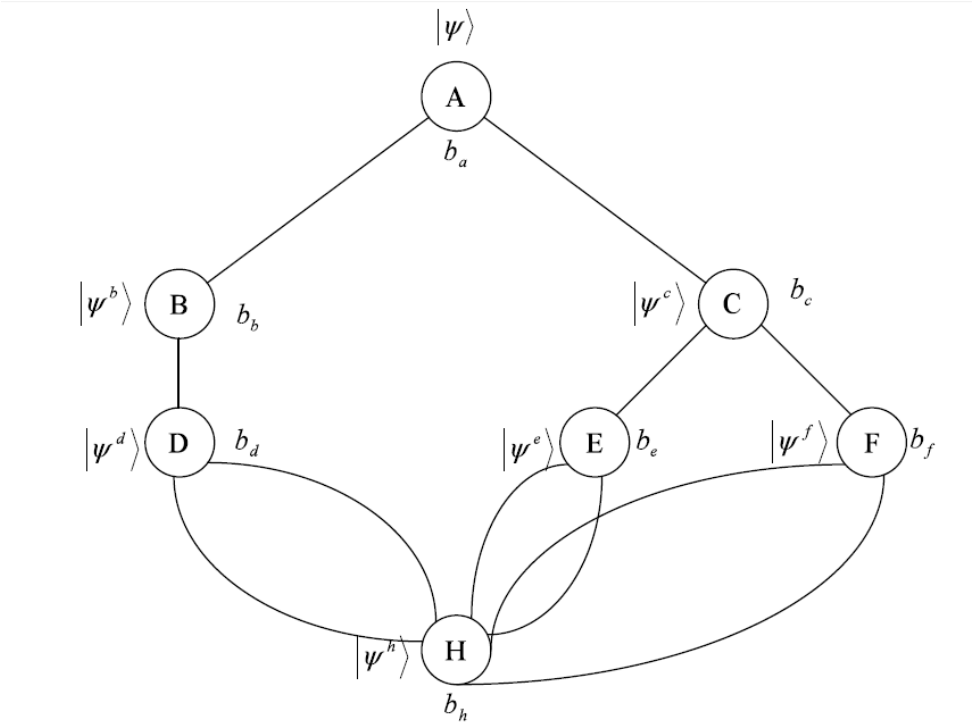

Figure 2 . 4 The QBDD in which nodes create the same branch

In the Fig. 2.4, H which represents the quantum gate in Fig. 2.3. In the same method, nodes will capable to further overthrown as long as they meet the above guidelines. At the end, the best QBDD will with the least number of nodes. The resultant optimal QBDD in Fig.2.5:

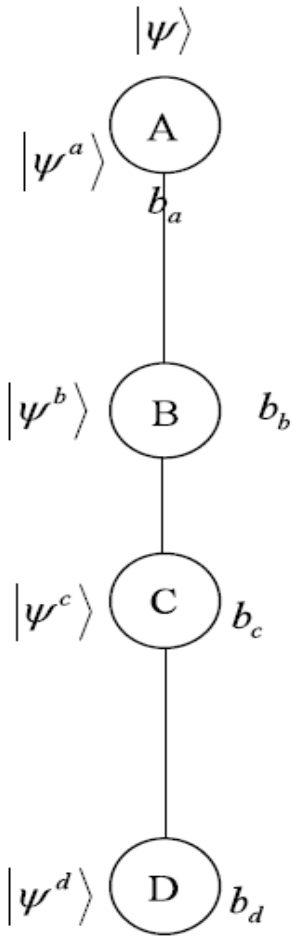

Figure 2 .5 *The optimal QBDD*

The picture given underneath portrays the quantum display which is comparing to Fig. 2.5. In the Fig. 2.6, the $|x_1\rangle$, $|x_2\rangle$, $|x_3\rangle$, . . . , $|x_n\rangle$ are qubits, then quantum states can be stored using the quantum array.

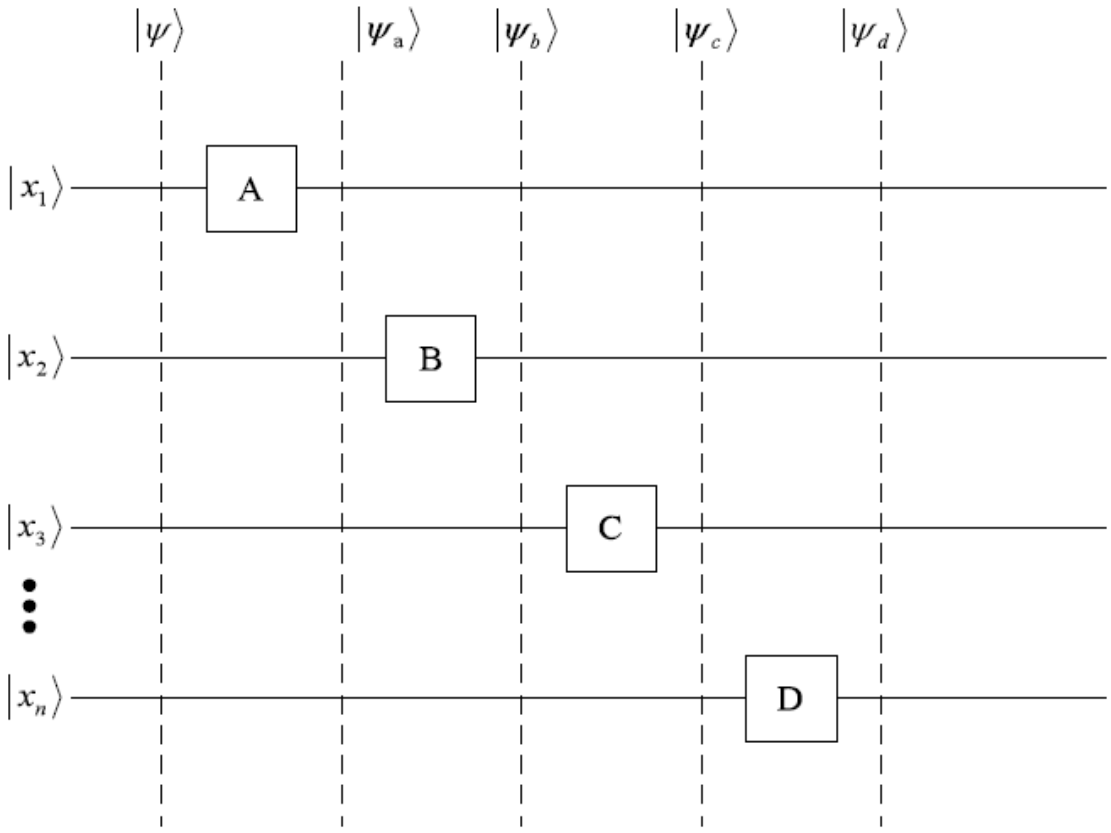

Figure 2 .6 Quantum Array

2.3 Image Storing Expression and demonstration

From the quantum computation, to establish the nature of execution we will turn by kinds of quantum gates into the expected description from the prepare initial quantity state.

Step 1: consider the elementary quantum state through a series of unitary transformation as

$$| initial \rangle = |0\rangle^{2n \otimes 8} \quad (6)$$

And disintegrating the initial quantum state, the gained elementary quantum state is:

$$| initial \rangle = |0\rangle^{2n} |0\rangle^{8} \quad (7)$$

Step 2: As Hadamard transformation in quantum computation is most useful than the other single quantum gates. So, establish the Hadamard gate for $2n$ times as $H^{\otimes 2n}$. It means that apply $2n$ Hadamard gates at the same time on $2n$ initial qubits. Then the result which is obtained after the application will be the middle quantum state as:

$$|middle\rangle = H^{\otimes 2n}(\,|0\rangle^{\otimes 2n}\,|0\rangle^{\otimes 8}\,) = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|Q_j^{middle}\rangle \qquad (8)$$

Step 3: Now the way ,we will use to store the state $|middle\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|Q_j^{middle}\rangle$ in quantum array to achieve the complete image in quantum state.

In the Fig. 2.6 , the $|\psi\rangle$ was the initial arranged state, $|\psi_a\rangle$, $|\psi_b\rangle$, $|\psi_c\rangle$, $|\psi_d\rangle$ was the central outcomes after the execution of gates according to A , B , C and D . $|x_1\rangle$, $|x_2\rangle$, $|\,x_3\rangle$, . . . , $|x_n\rangle$ represent the qubits respectively.

Step 4: To obtain $|Q_j\rangle = |N\rangle \otimes |j\rangle$, place elementary quantum gates into operation, then the position of $|0\rangle^{\otimes 8}$ can be altered to required state $|N\rangle$. Consequently

$$|final\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|Q_j\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|\,N\rangle \otimes |j\rangle \qquad (9)$$

$$|Q\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|\,N\rangle \otimes |j\rangle \qquad (10)$$

Which is a required formula for application.

2.4 Geometric Transformation

Geometric transformations are not only basis but also the key for encryption and decryption scheme of quantum image. Geometric transformations for the quantum pictures are understood by means of quantum circuits comprised with types of quantum logic gates, which correspond to the classical image. The use of some geometric transformations is image-translation, mirror transformation, image sub block substitution and image addition and subtraction.

2.4.1 Quantum Image Translation

Quantum image translation which maps each entity's location in a new position is a fundamental transformation of image. Two forms of quantum image translation: complete translation and cyclic translation are suggested by providing the circuits for quantum translation.

Complete translation translates the whole image. Use black or the other defined colors to fill the vacant position and leaves the pixels above the mage boundary.

Cyclic translation cyclically translates the whole image. To fill in the empty spot, cover the pixels around the image boundary. Quantum image translations perform good tracks in the procedure that can be conveniently done on quantum circuits at quantum bits transfer. The method will be implemented in depth as follows, in Fig. 2.7

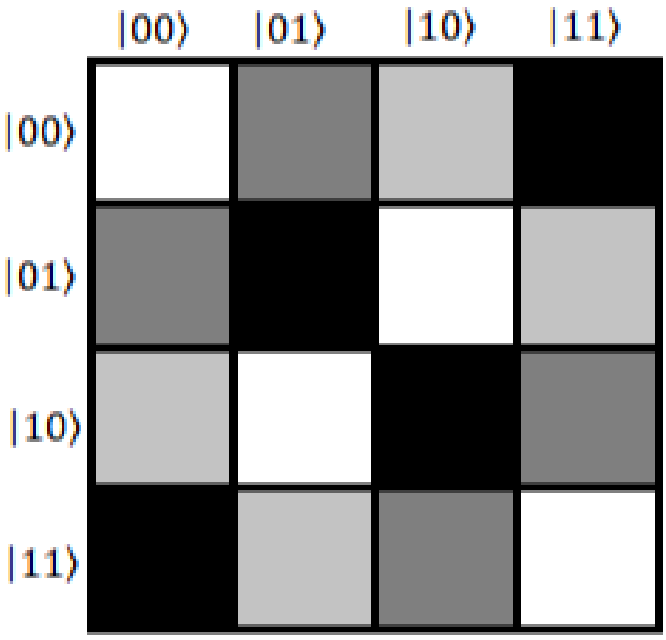

Figure 2 . 7

Consider that we are required to convert the complete image for one unit from right. Consequently, the column list is replaced by $|11\rangle - |00\rangle - |01\rangle - |10\rangle$ from the original sequence $|00\rangle - |01\rangle - |10\rangle - |11\rangle$. This process is completed into two steps.

Step 1: Reverse the qubit $|f_0\rangle$, the we will get the latest series $|01\rangle - |00\rangle - |11\rangle - |10\rangle$.

Step 2: To make a functional contrast between the consequence in pervious step and the genuine, one additional CNOT gate needs to be completed. So, image translation is implemented by quantum circuit is designed as given below:

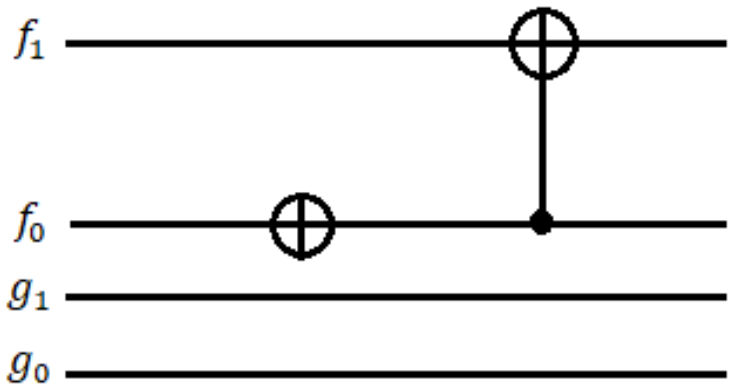

Figure 2 . 8

Final result can be seen in Fig. 2.9 given below

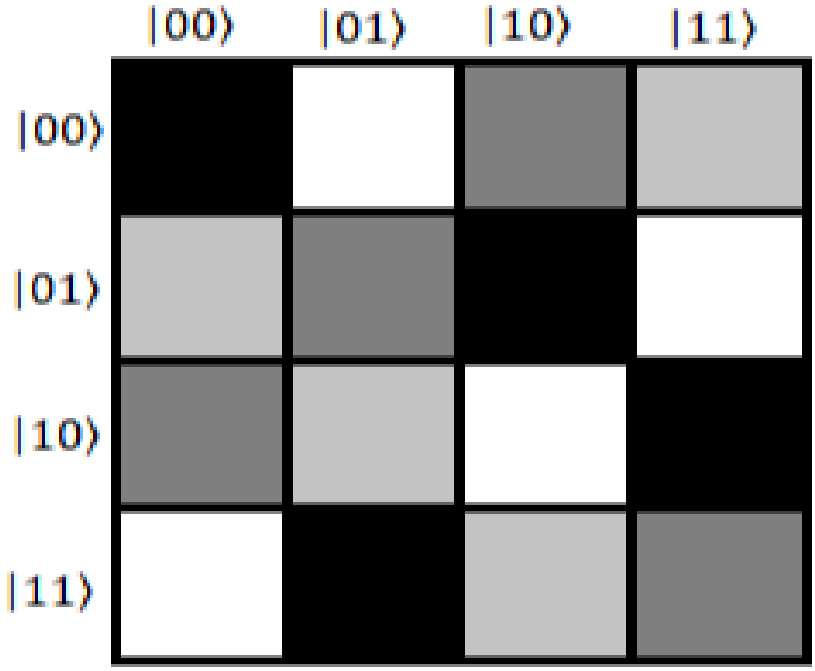

Figure 2.9

2.4.2 Image Mirror Transformation

Mirror transformation is used in geometric transformation in the classical image. The mirror transformation does not result in shape changes, separated into longitudinal, horizontal, and diagonal mirrors. However, equivalent volume can be obtained by modifying the gray scale size. Consider the Fig. 2.7 as given above.

Vertical mirror transformation is about the interchange of mirrors between top part of the horizontal axis and the lower piece. After implementation of vertical mirror transformation, the result image is Fig 2.10 given as:

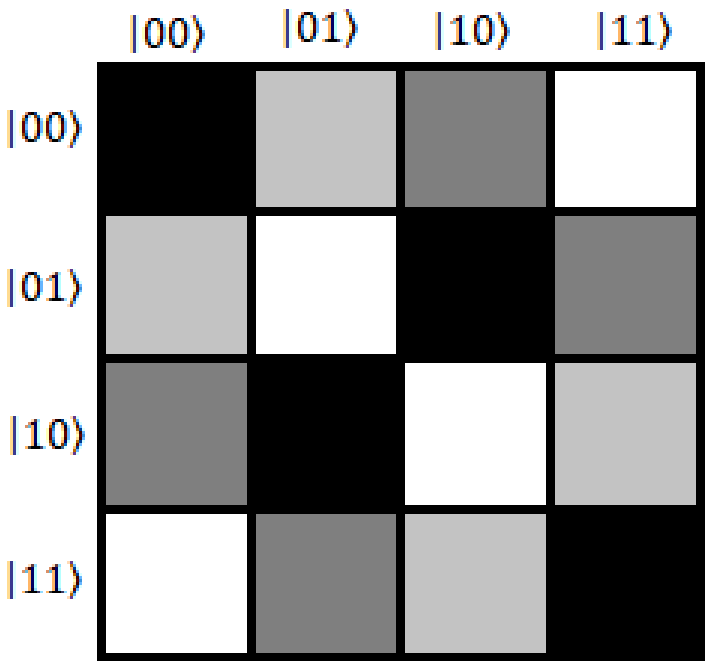

Figure 2 . 10

As described above, the pixel row of the following groups must be swapped to compose the corresponding accommodation between the top and bottom half: $|00\rangle$ & $|11\rangle$, $|01\rangle$ & $|10\rangle$. That is to say, the states of the quantum location in x direction will remain on its level, while the adjustment for the state in y branch is only necessary. In addition, the change in quantum state is only reflected to the transformation on the necessary qubit between $|0\rangle$ and $|1\rangle$. The achieved image is displayed through the circuit designed as:

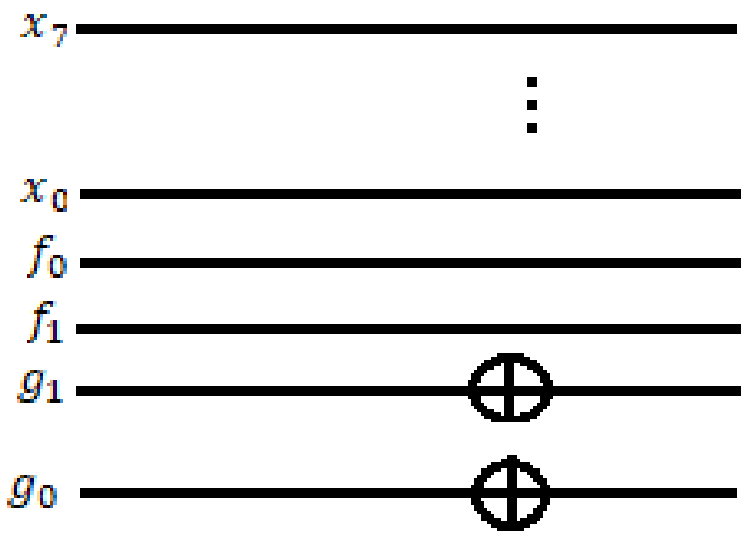

Figure 2.11

Like quantum image, the vertical mirror transformation, the horizontal transform is conducted based on horizontal central axis to interchange the left pixel and the right pixel.

2.4.3 Image Sub- Block Substitution

Moving the neighbor pixels into a sub-block, substitution the block with other equivalent, knowing through quantum circuits, this is a sub-block quantum image substitution.

Consider the Fig. 2.7 and break the complete image into four equal blocks $abcd$ as shown in below

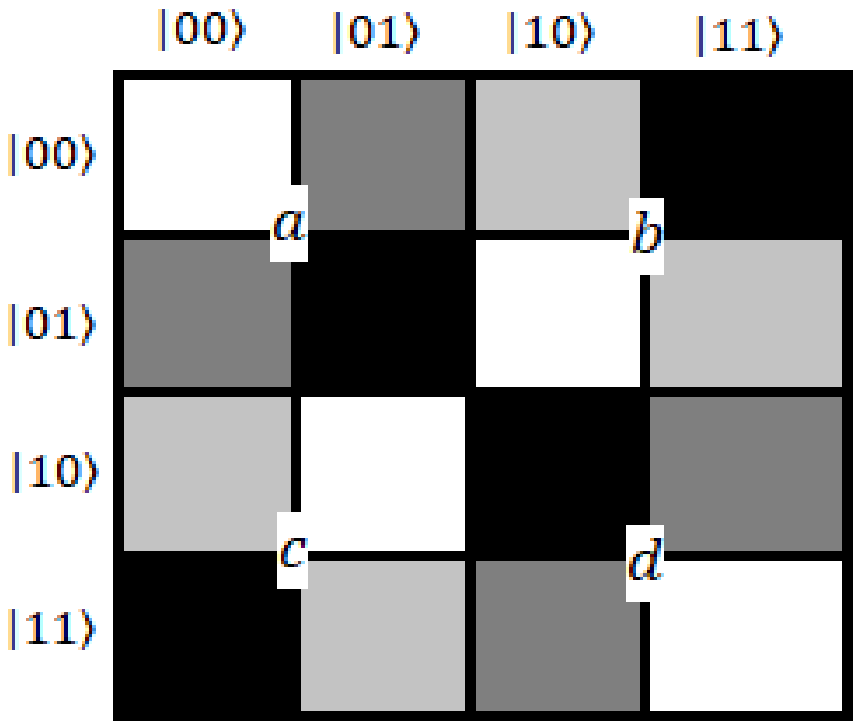

Figure 2.12

And the equal parts are as $T_a = \{|0000\rangle, |0100\rangle, |0001\rangle, |0101\rangle\}$, $T_b = \{|1000\rangle, |1100\rangle, |1001\rangle, |1101\rangle\}$, $T_c = \{|0010\rangle, |0110\rangle, |0011\rangle, |0111\rangle\}$, $T_d = \{|1010\rangle, |1011\rangle, |1110\rangle, |1111\rangle\}$

The aim is to subjectively achieve the exchange between the sub blocks. To direct the case a and b, examining the classes, we, can take note of that we can just flip the first qubit.

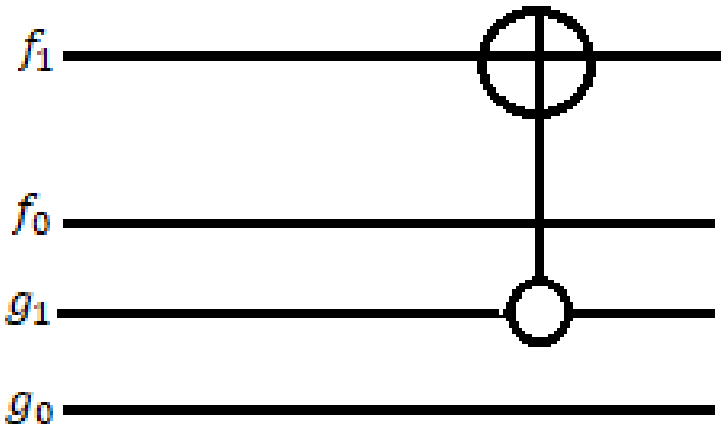

Figure 2 . 13 *Swap circuit ab*

Likewise, circuits to accomplish the interchanging among a and c , a and d are exhibited below respectively.

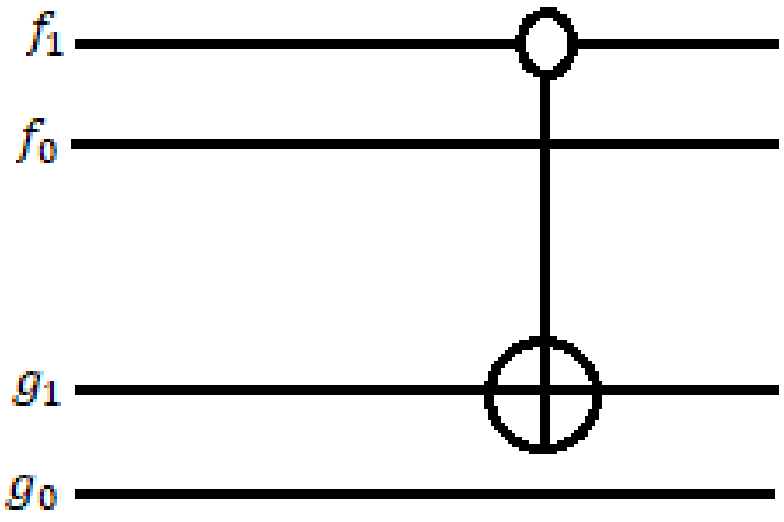

Figure 2 . 14 *Swap circuit ac*

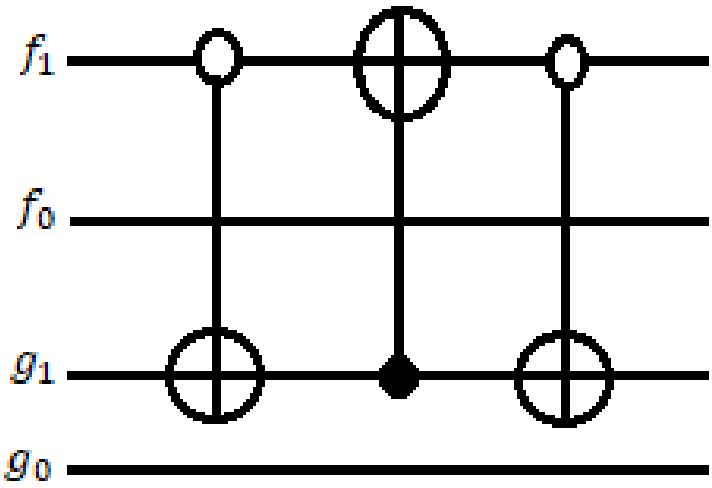

Figure 2 15 *Swap circuit ad*

2.4.4 Image Addition and subtraction

Image arithmetic is implementation of standard arithmetic operation, such as addition, subtraction, multiplication, and division, on image. Image arithmetic has many uses in image processing both as a preliminary step in more complex operation and by itself. For example, addition operation is also known as pixel addition, addition operator adds two images in pixel by pixel fashion. Subtraction which is known as pixel subtraction. Subtraction operator is used to detect the difference between two or more images of the same scene or object or subtract two images in pixel by pixel fashion.

In order to measure the gradient for all pixels in quantum image and remove its characteristics points further, the emphasis must be on adding and subtracting two quantum images. The resulting image pixel undergo numerical addition of the gray scale of the respective pixels in the two images with respect to the color addition procedure on the two images.

In the classical image, the addition and subtraction of images is the straight procedure between the greyscale value of participating pictures, the number of which should be equal or greater than two.

The target image pixel number is changed when the outcome exception exists which exceeded the values between 0 to 255. To cite a sample of an image in unit 8 format, the directions are:

1. If the total pixel value exceeds 255 then 255 will be maximum value.
2. If the subtraction is less than 0, then at least 0.
3. For the general consequence that the value would take the real data from 0 to 255.

Implementing the above rules, result will unique. However, the addition and the subtraction of images in the quantum gray-scale image will fulfill standardization requirement of the quantum superposition to maintain the quantity state after implementation. Therefore, if coefficient adhere to the normalized position, the terminus image generated by addition and subtraction will be countless as would the greyscale states.

Assume that images A and B are stored in states $|Q_A\rangle$ and $|Q_B\rangle$ respectively. Then the expression for image A would be

$$|Q_A\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1} |N_A\rangle \otimes |j\rangle \tag{11}$$

Also, the expression for the image B would be

$$|Q_B\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1} |N_B\rangle \otimes |j\rangle \tag{12}$$

Note $|Q_U\rangle$ as the product of addition of the image and $|Q_v\rangle$ as the one subtracted, while the meaning of the addition and subtraction as the image may be summarized as:

$$|Q_U\rangle = \alpha|Q_A\rangle + \beta|Q_B\rangle \ (0 \le \alpha \le 1\ ,0 \le \beta \le 1\ ,\ |\alpha|^2 + |\beta|^2 = 1) \tag{13}$$

$$|Q_V\rangle = \omega|Q_A\rangle + \mu\,|Q_B\rangle \tag{14}$$

(one of the values of ω and μ should less than $0 \le |\omega| \le 1\ , 0 \le |\mu| \le 1\ , |\omega|^2 + |\mu|^2 = 1$.)

In the above equation (14), each coefficient for defining the relationship between images in subtraction should be less than 0. Furthermore, it is important that addition and subtraction on image should be of equivalent volume for experiment. It can only function on the same dimension. It can have corresponding location. Here is an example of an addition to the image.

The image- adding operation is possible in combination with the definitions of $|Q_A\rangle$, $|Q_B\rangle$ and $|Q_U\rangle$ shift to the quantum place state superposition which could be described as:

$$|Q_U\rangle = \alpha|Q_A\rangle + \beta|Q_B\rangle$$

$$= \frac{\alpha}{2^n}\sum_{j=0}^{2^{2n}-1}|N_A\rangle \otimes |j\rangle + \frac{\beta}{2^n}\sum_{j=0}^{2^{2n}-1}|N_B\rangle \otimes |j\rangle$$

$$= \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}\alpha|N_A\rangle \otimes |j\rangle + \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}\beta|N_B\rangle \otimes |j\rangle$$

$$= \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}(\alpha|N_A\rangle + \beta\,|Q_B) \otimes |j\rangle$$

$$= \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|N_U\rangle \otimes |j\rangle \qquad (15)$$

The process of image addition is defined on the unique properly state superposition through the above steps as:

$$|N_U\rangle = \alpha|N_A\rangle + \beta|N_V\rangle \qquad (16)$$

Based on transferred argument, the final optimal superposed quantum state can eventually be transformed be changing the coefficient of α and β to achieve separate overlapping of the gray scale states.

Thus, in picture subtraction the idea of (14) could be moved to a like superposition of grey scale state $|N_V\rangle = \omega|N_U\rangle + \mu|N_B\rangle$ by means of which the transition could be completed.

Chapter 3

Implementation of Geometric Transformations in Image Encryption and Decryption

The art and science of covering up messages to add confidentiality in security of information is known as cryptography. Plaintext (sometimes called cleartext) is a document. Encryption is the method of trying to hide a message in such a way as to hide its content. Ciphertext is an encrypted file. Decryption is the method of converting ciphertext back into plaintext. A cipher is an encryption or decryption algorithm — a sequence of well-defined steps that can be followed as a method.

In traditional communication, when Bob and Alice communicate with one another, they will encode data in order to secure it from third party and altered. In other words, Bob and Alice both have their own private keys for encryption and decryption the data to read. Bob will read the received data with a private key which she has. And as simple as that implies, it retains the basic features in the private key cryptosystem as seen in Fig. 3.1: original text, encipher algorithm, keys, encrypted text and decryption scheme.

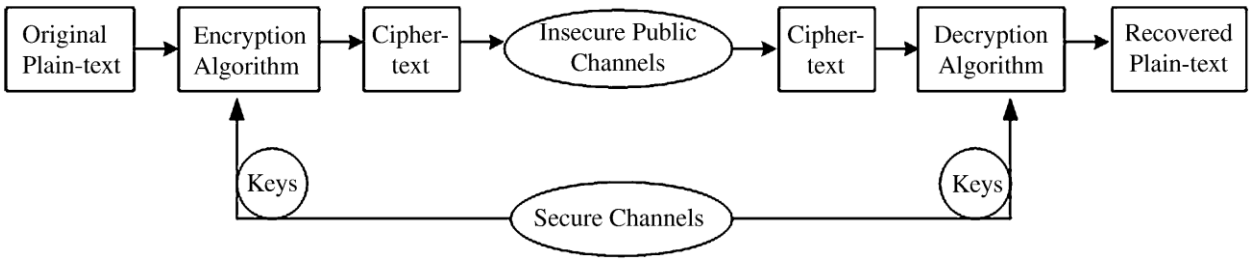

*Figure*3.1 *The private key cryptosystem*

Here, since the encryption item is a grey image that is contained in the quantum statements, the related original text and encrypted text are both quantified gray size photos in situations of a symmetrical cryptosystem.

3.1 Geometric Transformations for Encryption process

The geometric transformation of the image encryption has of particular importance. As we are studying the symmetric cryptosystem, we have a quantum image, but first of all we must talk about its storage.

3.1.1 Storage and Binary Tree Arrangement of Quantum Image

The picture information should first be stored in a quantum state to use quantic mechanics to process an image.

The storing expression is given by

$$S = \{|Q\rangle, i\}, |Q\rangle = \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} |N\rangle \otimes |j\rangle, \qquad i = 1, 2, 3, \dots, m \qquad (17)$$

Here, S represents storage set, i is number of layer and $|Q\rangle$ is stated in expression (1). In above expression, the N decodes the quantum greyscale image. The above equation will store the image in n-layers. Storage of image for n-periods will give us n-copies as n-layer images. These copies are now easy to use for further process.

Now arrange the n-layers images into a full binary tree array. A binary tree consists of nodes, where each node has a "left" pointer, a "right" pointer, and an element of data. The pointing "root" points to the top node in the tree. The left and right pointers on both sides point recursively to smaller "sub trees." After putting the n-layers of image into full binary tree display categorize the layers into left subtree, the right subtree and the roots as exposed in Fig. 3.2

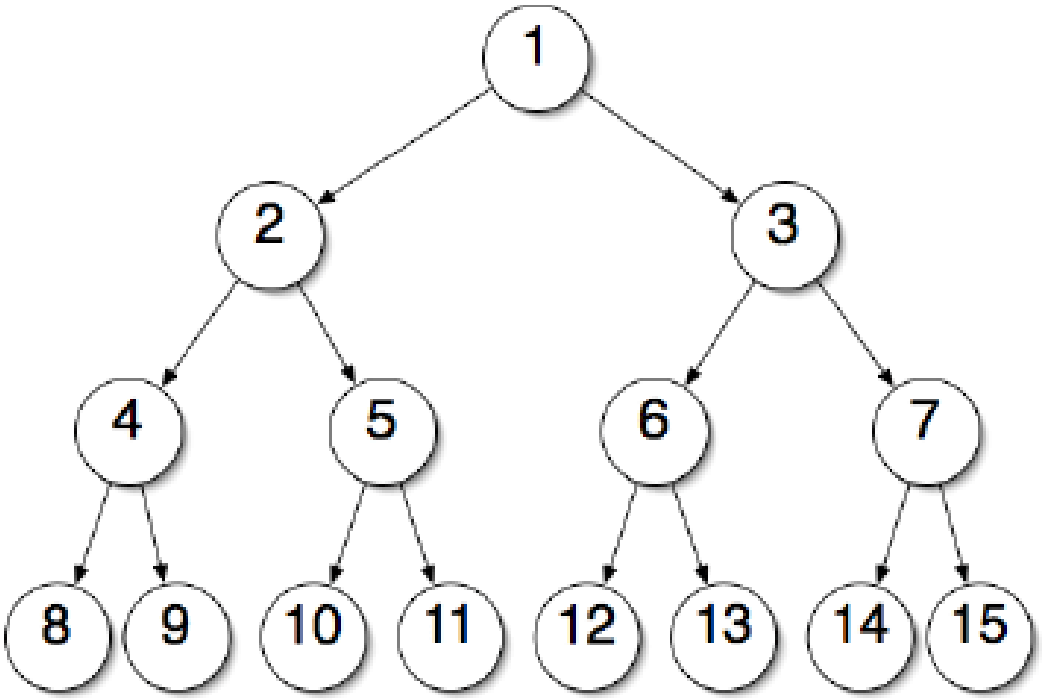

*Figure*3. 2 *Display of full − binary tree*

The arrangement of image layers into complete binary tree would establish a new technique for enciphering the image which will improve the eavesdropper 's difficulty in deciphering even if the ciphered information is intercepted. On the binary tree will be addressed the implementation of quantum-image-translation, image subblock substitution, image mirror transformations and image subtraction and addition amongst all quantum geometric transformations.

3.1.2 Relation Between Transformations and Binary Tree

Here, we establish of interaction among transformations and entire binary tree. In addition, separate geometric transformations are implemented in each sheet. Geometric transformations such as image-translation, image subblock substitution, and image mirror transformations can operate on the left and right subtree, and root as realized in Fig. 3.3

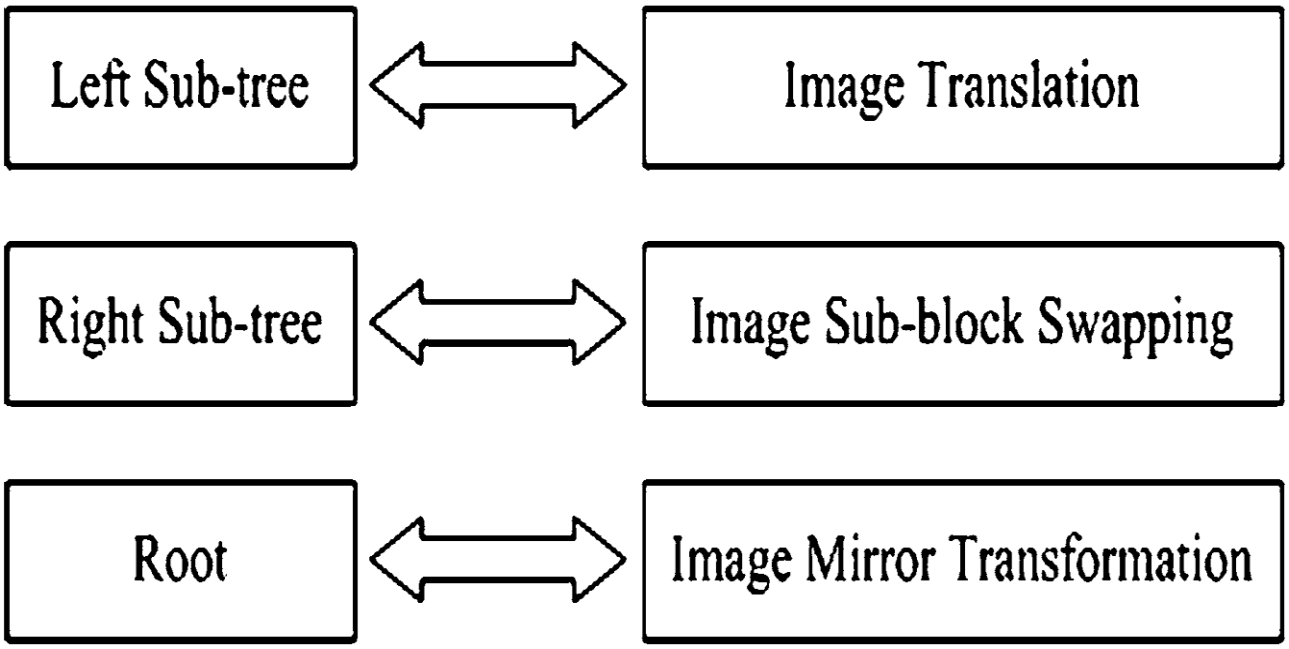

*Figure*3.3 *Matches with binary tree and transformations*

In the preceding stage the preparation makes no variations to n images. These are exactly same images as the prepared ones. First phase of transformations in encryption is the relation of left sub-tree, right sub-tree and root of complete binary tree with image-translation, image subblock substitution and image mirror transformation.

Suppose the transformation of the n-layer image is G_i according to the ith layer. And the image translation , sub block swapping and the mirror transformation is expressed by G_{trans} , G_{swap} , G_{mirror} respectively , which satisfy $G_i \in \{ G_{trans} , G_{swap} , G_{mirror} \}$. After the transformations are applied, the image will be represented as $|Q_i\rangle = G_i |Q\rangle$ in every layer. i.e.

$$|Q_i\rangle = G_i |Q\rangle \tag{18}$$

Image translation will be performed on the left sub-tree by splitting the picture into the left sub-tree, which is given by the four orders down, up, right and left. The way we use the left sub-tree

to express it will be divided into four sections each section performs the translating process left, right, down and up respectively. Then transfer images across any direction (down, up, right and left) as number of pixels equivalent to number of former images in the list.

Image sub block transformation substitution will be performed in right sub tree. First, divide each image into equal blocks in right sub tree and organize layers with respect to number of image layers from low to high to perform this transformation. The layers of the picture must finish the swap between two consecutive smaller layers and the last layers must swap to the first. Here the example is given in Fig. 3.4

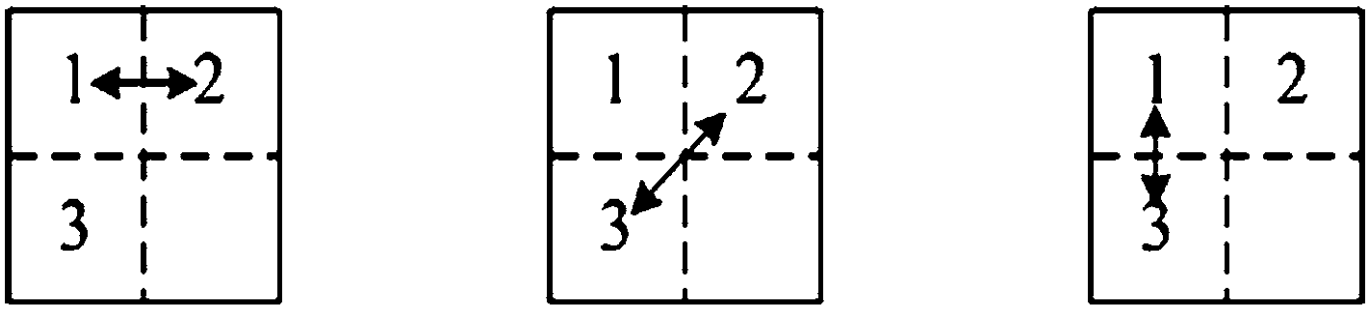

*Figure*3. 4 *Sub − block Division*

For the roots, image mirror transformation will be performed. The horizontal mirror transformation, vertical mirror transformation, or diagonal mirror may be used for this. All these transformations are understood by quantum circuits.

3.1.3 Superposition of Transformed Layers

The 2nd phase of transformations is now the joint superposition among the image layers. Developed enciphering process would be effective. As in the transformations of first phase, the n-layers of image are totally different. Now it is 2nd turn named joint transformations which will transform among layers as principles in expression given below.

$$
\begin{aligned}
|Q_1'\rangle &= \alpha_1|Q_1\rangle + \beta_1|Q_2\rangle \\
|Q_2'\rangle &= \alpha_2|Q_2\rangle + \beta_2|Q_3\rangle \\
|Q_3'\rangle &= \alpha_3|Q_3\rangle + \beta_3|Q_4\rangle \\
&\vdots \\
|Q_{m-1}'\rangle &= \alpha_{m-1}|Q_{m-1}\rangle + \beta_{m-1}|Q_m\rangle \\
|Q_m'\rangle &= \alpha_m|Q_m\rangle + \beta_m|Q_1\rangle
\end{aligned} \tag{19}
$$

Where $|Q_i'\rangle$ represent the image after superposing, $\alpha_i \; and \; \beta_i$ are the image superposing coefficient which should satisfy the normalization condition of quantum superposition $|\alpha|^2 + |\beta|^2 = 1$. Take the rules into the matrices.

$$
\begin{pmatrix} |Q_1'\rangle \\ |Q_2'\rangle \\ |Q_3'\rangle \\ \vdots \\ |Q_{m-1}'\rangle \\ |Q_m'\rangle \end{pmatrix} = \begin{pmatrix} \alpha_1 & \beta_1 & 0 & 0 & \dots & 0 \\ 0 & \alpha_2 & \beta_2 & 0 & \dots & 0 \\ 0 & 0 & \alpha_3 & \beta_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 \dots & \alpha_{m-1} & \beta_{m-1} \\ \beta_m & 0 & 0 & 0 & \dots & \alpha_m \end{pmatrix} \begin{pmatrix} |Q_1\rangle \\ |Q_2\rangle \\ |Q_3\rangle \\ \vdots \\ |Q_{m-1}\rangle \\ |Q_m\rangle \end{pmatrix} \tag{20}
$$

If we make the replacements

$$
B' = \begin{pmatrix} |Q_1'\rangle \\ |Q_2'\rangle \\ |Q_3'\rangle \\ \vdots \\ |Q_{m-1}'\rangle \\ |Q_m'\rangle \end{pmatrix}, \qquad B = \begin{pmatrix} |Q_1\rangle \\ |Q_2\rangle \\ |Q_3\rangle \\ \vdots \\ |Q_{m-1}\rangle \\ |Q_m\rangle \end{pmatrix}, \qquad C_1 = \begin{pmatrix} \alpha_1 & \beta_1 & 0 & 0 & \dots & 0 \\ 0 & \alpha_2 & \beta_2 & 0 & \dots & 0 \\ 0 & 0 & \alpha_3 & \beta_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 \dots & \alpha_{m-1} & \beta_{m-1} \\ \beta_m & 0 & 0 & 0 & \dots & \alpha_m \end{pmatrix}
$$

Then (20) can be written as:

$$B' = C_1 B \tag{21}$$

Geometric transformations up to this equation can be used in any encryption algorithm. Before this the image layers to which the geometric transformation is applied are present. Now, the task is to combine these layers of image to gain a new encrypted image. This work can be done by the superposition or addition of layers of image. After the superposition, we will get a picture that we have to share to the other party. And that image will be encrypted image. The geometric transformations which are to be used in encryption process can be seen the following flowchart.

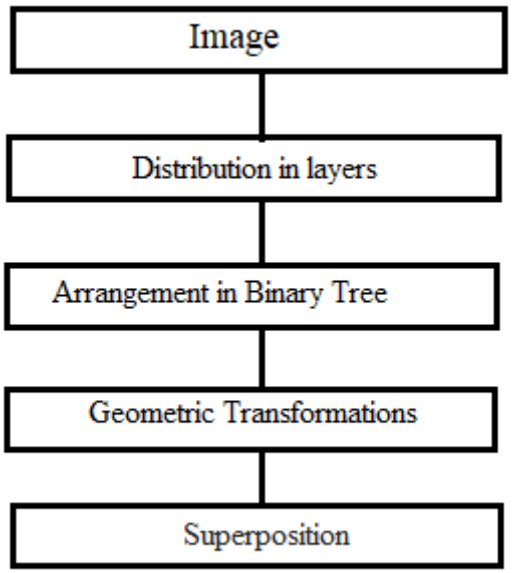

*Figure*3.5

3.2 Key generation

When the other party gets the picture, they have to decrypt it in order to read it. It will need a key to decrypt it. As we are studying the symmetric cryptosystem, so in order to decrypt the image, we have to give the selected key to the other party. For this encryption and decryption key will be same. In cryptography a key is a piece of information (a parameter) which determines a cryptographic algorithm's functional performance. In encryption, a key specifies plaintext transformation into ciphertext, and vice versa for decryption algorithms. For geometric transformation encryption, the key set consists of the matrix coefficient C_1 as a private key, and the transformed root operation which is either horizontal mirror transformation, vertical mirror transformation, or diagonal transformation. Both the parties will use same key as described above.

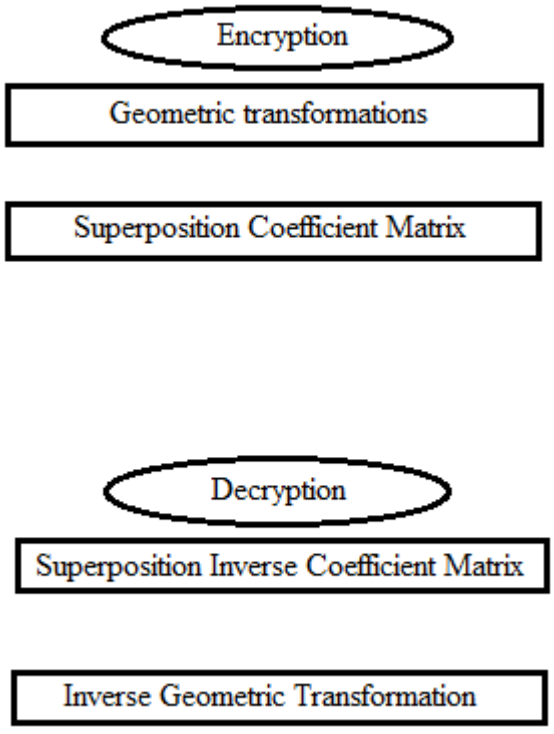

*Figure*3.6

3.3 Geometric Transformations for Decryption process

Decryption is reverse process of encryption. Now we will decrypt with given key to the encrypted image. Whatever algorithm we use in the encryption and decryption of images, we are simply studying the significance and use of geometric transformations for secure communication. After that the implementation of algorithm, we measure the image matrix B. Where B is the matrix stands for the representations of n-layers after the geometric transformations for the encryption process are implemented. With this set the private key as C_1 will be useful. And C_1 represent the coefficient matrix of B.

So, we have that

$$B = C_1^{-1} B' \tag{22}$$

Where B' is matrix and C_1^{-1} is reverse matrix of the private key coefficient matrix C_1.

The achievement of matrix B gives the solid information about the n-layers image. After this we have to apply the inverse transformation as another private key, which delivers the information about the root layer of binary tree. It is easy to design the inverse transformation G_1' .

Then we have

$$|Q\rangle = G_1' G_1 \, |Q_1\rangle \tag{23}$$

The decryption process of geometric transformations is seen as below

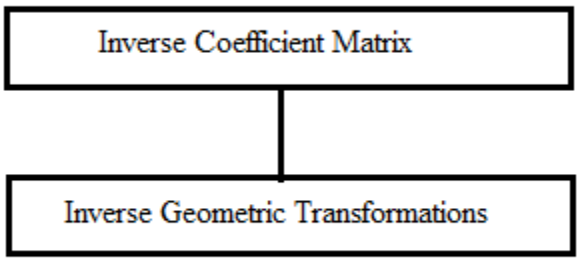

*Figure*3.7

The geometric transformations in either encryption and decryption are done by quantum circuits. A quantum circuit is a sequence of quantum gates. Here the work of geometric transformations is completed.

Conclusion

This thesis realizes the implementation of geometric transformations in quantum image enciphering and deciphering by means of quantum circuits. Geometric transformations create a great complexity in the processing. Before the application of geometric transformations, arrangement of layers of image in binary tree is a huge complex. The future work is besides it to use the other theories of quantum mechanics with geometric transformations to protect a communication through an insecure channel.

References

[1] Dagmar, B., Gabor, E., Tim, M., Tobias, R., Jorg, R., " Quantum Cryptography: a survey" ACM Comput. Surv . 39(2), 6(2007)

[2] Shannon, C.E. : "Communication theory of Secrecy system". Bell Syst. Tech. J. 28(4), 656-715 (1949)

[3] Diffie, W., Hellman, M. E. : "New direction in cryptography". IEEE Trans. Inf. Theory, 22, 6644-654 (1967)

[4] Wang, X.Y., Feng, D.G., Lai, X.J., et al.: "Collision for Hash function MD4, MD5, HAVAL-128 and RIPEMD (2002)". http://Eprint.iacr.org/2004/199

[5] Shor, P.W.: "Algorithm for quantum computation: discrete log and factoring. In: "foundations of computer Science, proceeding of the 35th Annual Symposium", pp,124-134 (1994)

[6] Grover, L. K.: "A fast quantum mechanical algorithm for database search. In.: "proceeding of the twenty eight Annual ACM Symposium on theory of computing", pp. 212-219 (1995)

[7] Nielson, M., Chuang, I.L.: "Quantum Computation and Quantum Information". Cambridge University press, Cambridge (2000)

[8] Venegas-Andarca, S.E., Bose, S.: "Storing, Processing and retrieving and image using quantum mechanics". Quantum Inf.Comput. 5105, 137-147 (2003)

[9] Venegas-Andarca, S.E., Ball. J. L.: "Processing images in entangled quantum system". Quantum Info. Process 9(1), 1-11 (2010)

[10] Pang, C., Zhou, Z.W., Guo, G.: "Quantum discreate cosine transformation for image compression". Quantum phys. (2006).arXiv:quant-ph/0601043v2

[11] Latorre, J. I.: "Image compression and entanglement".Quantum phys. (2005). arXiv:quant-ph/0510031

[12] Le, P.Q., Dong, F., Hirota, K.: "A flexible representation of quantum image for polynomial preparation. Image processing, image compression, and processing operation".Quantum Inf. Process. 10, 63-84 (2010)

[13] Barenco, A., Bennett, C.H., Cleve, R., DiVincenzo, D.P., Margolus, N., Shor, P., Sleator, T., Smolin, J.,Weinfurter, H.: Elementary gates for quantum computation. Phys. Rev. A, Gen. Phys. **52**(5), 3457–3467 (1995)

[14] Zhou, R., Wang, H., Wu, Q., Shi, Y.: Quantum associative neural network with nonlinear search algorithm. Int. J. Theor. Phys. **51**(3), 705–723 (2012)

[15] Payne,H.J., Meisel,W.S.: An Algorithm for Constructing Optimal Binary Decision Trees
[16] Zhou , R. G., Wu , Q. ,Zhang , M.Q., Shen, C.Y.: Quantum Image Encryption and Decryption Algorithms Based on Quantum Image Geometric Transformations. Int. J. Theor. Phys. **52**,1802–1817 (2013)