International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Design of Reversible Gates-Based Image Steganography using Quantum Dot Cellular Automata for secure Nano-Communications

V.Nancharaiah, B.Sridhar, S.Sridhar, N. Haritha, N.L.N.Keshav Kumar

Abstract: ***Image Steganography isa method of concealment secret information, by embedding it into a video, image. It is one in every of the methods employed to protect secret or sensitive information from malicious attacks. Here we are consider secure image data transmission through secure nano-scale communication circuit, Quantum-dot cellular automata (QCA), could be a new paradigm that replaces CMOS circuits by victimization the charge configuration. QCA is used to design the modern digital circuits at the Nanoscale. Thus, using QCA to implement the proposed design reduces 28.33% of area compared with CMOS implementation. When we consider the features of QCA nanotechnology, it performs well low power dissipation and nano scale size at high frequency is exploring as a emerging technology to replace CMOS based systems. The technology behind the QCA Feynman, Toffoli, and Fredkin universal reversible logic gates circuits in the base are implemented and analyzed. In order to optimize the design QCA technology extend up to 5-input majority gates and use a F-Gate. We are proposed reversible XOR gate like Feynman gate as an Encoder/Decoder circuit. Further consider the benifits of QCA the proposed circuit is encoder circuit is also used for reverse computing to encode the data and to use the LSB technique in the image pixels for secure nano communication circuit. We estimated the area and latency of the QCA circuit***

Keywords: Image stenography, nanoCMOS circuits, QCA, Feynman Gates, Toffoli Gate, Fredkin Gates, F-Gates, Nano communications circuit.

I. INTRODUCTION

Recently, the development of the Internet considering become the most important aspect of information technology. Therefore, providing security through various methods of protecting important transmission information is also an important issue. These methods are classified basically into three categories: steganography, watermarks and cryptography.

Manuscript published on November 30, 2019.
* Correspondence Author
V.Nancharaiah*, Associate Professor, Dept of ECE, LIET, Vizianagaram, India, nanch84@gmail.com
B.Sridhar, Professor,Dept of ECE, LIET, Vizianagaram, India srib105@gmail.com
S.Sridhar, Professor, Dept of ECE ,LIET, Vizianagaram, India sridhar.vskp@gmail.com
N. Haritha, Dept of ECE, LIET, Vizianagaram, India
N.L.N.Keshav Kumar, Dept of ECE, LIET, Vizianagaram, India

Cryptography is the science of protecting information through encryption. Since the password itself does not hide from view the states that the message is secret by use of this steganography. The ability to protect sensitive information, especially when it is transmitted through channels of opposition to vulnerabilities, is fundamental in the emerging world of cyber warfare. Nowa days, all modern and private intelligent systems with enormous computer capabilities constantly monitor all electronic communications.In particular, each cryptographic text transmission attracts the attention of these systems andchooses to be analyzed by rivals and any type of opposing forces. Electronic transmission media has requires a less focused approach to monitor automated systems. The level of service provided by Modern Steganography includes the authenticity,privacy, integrity and confidentiality of transmitted data.A better understanding of the different updated jobs is very useful to verify the new implementation and analyze its accuracy of performance in terms of security. Start by addressing the vulnerabilities of the standard LSB technology and then try to enrich your thinking. The standard LSB technique is very easy to implement, where the LSB / coverage bit sample of the pixel is replaced by the target bit [6].This approach may remain imperceptible, but with little robustness and capacity. T. Penvy et al. We present a safe steganographic algorithm HUGO that defeats almost all attacks of steganographic analysis by defining the distortion based on eigenvectors that are already used in steganographic analysis. It supports the capacity of Stego Media seven times more than the standard LSB technology. However, in the case of the multi-bit method BC Nguyen et al., the results were not satisfactory. [7] Improve the capacity of LSB replacement technology by introducing the popular multibit flat image steganography. The increase in capacity again reduces the imperceptibility of WC Kuo et al. [8] The capacity is increased by incorporating multiple bits of destination data encoded by the execution length coding (RLE), but the imperceptibility is maintained by considering the generalized use characteristics of multiple bits of the modified address (MGEMD). MGEMD not only reduces distortion, but also helps against modern steganotysis [9].

The robustness of the LSB replacement technique can be increased by embedding data in a higher LSB layer or by embedding random coverage locations and also by introducing double-layer security to increase N Cvejic et al. [10] In your work, the destination data is embedded in a higher bit plane and then adjusted to maintain quality. This method also extends the embedding error to the four predecessors of the current sample.

Although incorporation into higher bit planes increases robustness, five samples that involve the loss of a single bit of target data lose capacity [10]. K Gopalan in [11] provides two-layer security by embedding encrypted data bits in the audio samples of the k-th layer. This approach increases robustness and imperceptibility by using the properties of the human auditory system. When decomposing the intensity in another digital system to solve the problem of low robustness due to the incorporation of higher bit planes, the system uses more bits to represent numbers in the range of 0 to 255. F. Battisti et al. introduced this concept for the first time in steganography. Zekendorf's theorem use a generic Fibonacci sequence to generate virtual bitmaps and then perform embedding [12,13] on these bit planes.

The robustness and imperceptibility of the proposed method are improved by adjusting the value instead of directly replacing the coverage bits with the destination data. The secret message is embedded within the main image without impeding the imperceptibility of the intelligent pixel adjustment strategy based on having two average blocks. The resulting hidden image can tolerate operations such as edge sharpening, reversing, color quantization, truncation of pixels, JPEG etc[14]. The MOD-4 technique is used to embed two objective data in each R, G and each R. The B plane that covers the pixels is, therefore, 6 bits in each pixel, which helps increase capacity. This method only incorporates two destination bits, regardless of the limit value problem[15]. The main problem with steganography is the negative impact on visual quality. Steganography based on the region solves this problem by incorporating data in specific regions based on the selection of HVS characteristics and image attributes. Most binary imaging steganography techniques consider changing distortion based on HVS, although they are not safe for steganographic analysis attacks.

Feng et al. In [16], this problem is solved by measuring the distortion based on complementary, rotated and mirror invariant local texture patterns (crmiLTP) and using the syndrometrellis code (STC) to minimize distortion. K Qazanfari et al. [17] Maintain the statistical and perceptual properties of cover images in hidden media by completely overwriting the histogram. Its LSB ++ method results in less distortion in the co-occurrence matrix by protecting sensitive pixels from inserting additional bits. His method is more capacitive and maintains a histogram of JPEG images.

II. IMAGE STEGANOGRAPHY CIRCUIT DESIGN

Steganography is that the follow of concealing a various types of data such as image, or video, file, message, at intervalsimage, or video, another file, message. Here we tend to area unit victimization a picture to cover the message in it. The main advantage of this technique over cryptography alone is that the supposed secret messagesthat doesn't be a focus for attention to itself as an object of scrutiny. Plainly visible encrypted messages, in spite of however unbreakable they're, arouse interest and should in themselves be criminative in countries within which secret writing is against the law.In alternative words, steganography is a lot of discreet than cryptography after we wish to send a secret info. On the opposite hand, the hidden message is less complicated to extract.

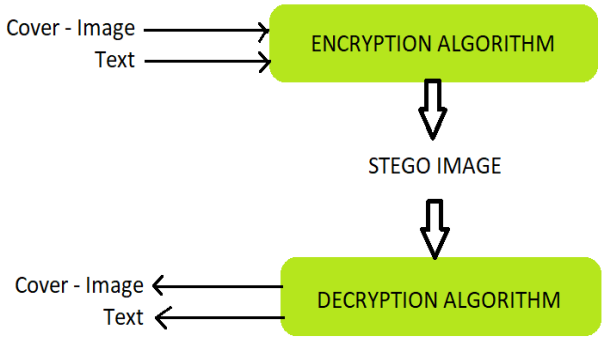


Fig.1: image steganography technique

A.Quantum-dot cellular automata (QCA) nanotechnology

CMOS technology has been considering a many problems in the last ten years. Power dissipation is the one of the major drawbacks. Use of quantum computing has the potential to overcome this disadvantage in that Reversible computing and reversible logic circuits operate acting as important role. Reversible computing also offers options for error diagnosis. The engineering of QCA is attributable to its distinctive options, such as extremely high operating frequency, extremely low power dissipation and nanoscale function size is becoming a promising candidate to exchange technology CMOS.

A nanostructure paradigm provided by Lent et al [1]. It is a cellular automaton of quantum dots QCA, which uses a coupled quantum matrix to implement Boolean logic functions. QCA has the advantage that extremely high compression is due to the small size of the points. Simplified interconnections and products with very low power delay, potential density. When using a QCA unit with a diameter of twenty nm, the entire adder will be placed between a millimeter two. The essential unit of QCA consists of 4 quantum dots in a highly coupled matrix through a tunnel barrier. The electrons will be tunneled between the points but cannot leave the cell. If 2 additional electron zone units are placed in the cell, Coulomb's repulsion can force electrons to create points at opposite corners. Therefore, there are surface unit 2 polarizations of the equivalent energy base state, which can be called logical "0" and "1". Coulomb's interaction between electrons causes the battery to signal an extremely bistable transition between polarization

HeumpilCho [2] offers different styles of addiction and abuse of QCA analysis. He also predicted that in QCA the elementary device, a quantum dot cell, would be used to build gates, nano wires and memories. In itself, it is the cornerstone of the engineer's science circuits. He also explained the QCA circuit styles with larger circuits and showed that the analyzes supported these styles.

P. pol Tougaw and Craig S. Lent [3] propose that in quantum cells, each quantum cell contains 2 electrons that move in a coulombian manner with nearby cells. The distribution of the charges in each cell tends to align with one of the 2 perpendicular axes, which allows the encryption of the victimization of binary information of the state of the cell. The state of each cell is affected during a very non-linear approach by the states of its neighbors. A line of these cells often transmits binary information.

We tend to use these cells to design inverters, programmable logic gates, dedicated AND and OR gates and crossings without interference.

W.J. Chung, B. Smith and S.K. Lim [6] considered that QCA could be a new computational mechanism that could represent binary data that support the spatial distribution of the electron charge configuration in chemical molecules. The QCA circuit configuration is currently limited to one layer with a variety of terribly restricted cable crossings. They jointly explain the duplication of nodes and routing algorithms to reduce cable crossing

Ottavi, Setal [7] suggested that the QCA architecture, which incorporates the advantage of a minimized area of a serial memory with a reduced delay when reading a parallel memory, should be called "hybrid." They also said that the active area can be achieved by hybrid.

Kunal et al. [8] predicted that reversible logic would become a promising computing paradigm with applications of QCA and low power quantum computing in the field of VLSI. They explain that the crossing of the reversible logic gate and the conservative computer circuit is a computer circuit that retains parity, reversible or reversible conservative. They mentioned that, by victimization, the logical synthesis of each reversible computer circuit and each conservative computer circuit would be a promising step towards a low-power QCA.

B. QCA Cell

Unlike transistors compatible with physical science, QCA does not work by transporting electrons, but by tuning electrons in a small restricted area of only several square nanometers. The QCA is applied by quadratic cells. Each square contains exactly a four potential wells that have been measured and placed s properly, one in each corner of the QCA cell (see Figure 2). A precise 2 very square electrons in QCA cell exist in only in potential wells[42].

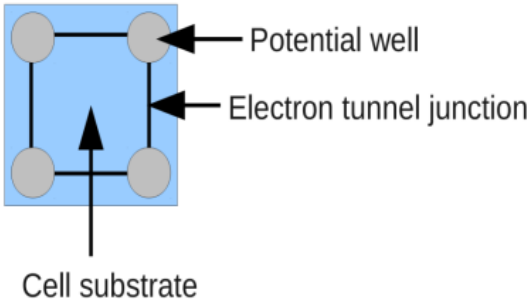


Fig.2: Anatomy of a QCA cell

Potential well surface unit coupled with electron tunnel junctions. Potential well will open so that electrons can cross them under specific conditions, by means of a clock signal without any interaction from the outside. The 2 electrons can try to become independent from each other as feasibly as expected, due to Coulomb's force interacting with each other. As an effect, they may exist in potential diagonal wells, since the diagonal is the greatest possible distance for them (see Figure 3).

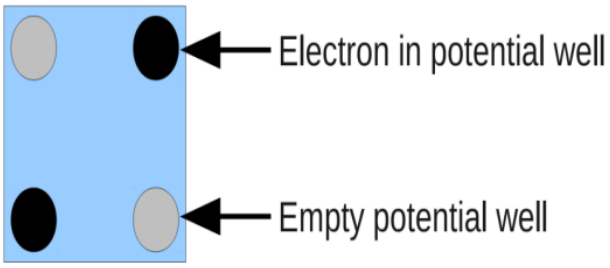


Fig.3:Potential wells

As shown in fig :3 two diagonals during a square, that suggest electrons will reside in 2 possible changes in the QCA cell. In regards to these 2 setup, those are considered as a binary 0 and a binary 1, that is, each cell will be in 2 states. The o &1 states are given in Figure 4. These elements represents a position since logic are properly explained in a present day computers.. In that binary digit 1 represents high voltage and binary 0 represents low voltage. [42].

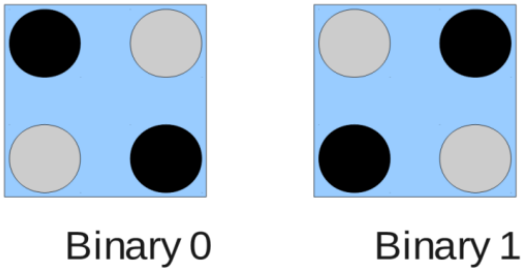


Fig.4: Binary representation of interpretation

C.Data and information transmission

If 2 QCA cells are located subsequently to to exchange their states, that is, the modifications of the electrons they contain. The tunnel connections of the QCA cell to transfer its state to a adjacent cell must be congested. QCA cell tunnels junctions of the neighboring cell should be opened in order to permit electrons to annoy the tunnel junctions among potential wells when they are opened, the electrons within the neighboring cell live as much of Coulomb's force as possible from the primary cell. When they are distant from each other, they will move in potential wells identical to those of the original cell. As at present, because the tunnel junctions have been closed again, the state transfer has been accomplished[42].

The position of a cell is often transferred to many neighboring cells. Works steadily as a neighboring cell, however, the joints of the tunnel of all the neighboring cells post must be opened at the same time, that makes the transfer quicker than the transfer of the state cell after cell, this allows the U. S .to manufacture "wires", made from QCA cells, to maneuver information over great distances[42].

D.Introduction of QCA concepts Gates:

It is understand that to transport information and interpret with QCA cell, but there is still a option of calculating (see Figure 5). QCA cells basically build a gate with three majority inputs aligned five basic cells that are arranged across the diagonal.

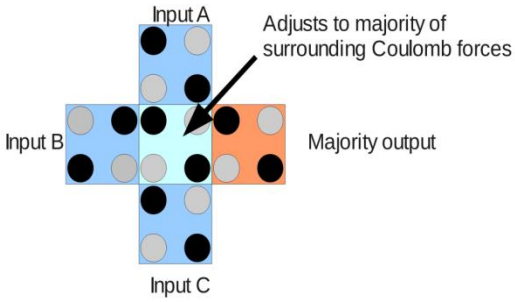


Fig.5: QCA Majority Gate

F. Majority gate

Many physicists postulates that become I famous a Coulomb forces a total of many electrons. A major gate takes advantage of this impact cells at the top, left and bottom of the rock function as affiliated cells. Coulomb forces of the electrons of all input cells are consider as total, central cell adjusts to most of the changes in the input affiliation cells. Finally, the output cell adapts to the central cell and, therefore, output cell gives a state of resulting block gate.

G. AND gate

we tend to add the QCA sector with the well-known binary illustration, it is desirable to have additional logic gates to which we tend to measure the usual square measurements. With a small alteration, it is possible to show the major Gate on an AND gate.

Boolean AND produces one if all entries are equal to one, if not zero. for 2 entries of the massive door, because the inputs of the AND gate and the gate do not have to generate one if 2 inputs is one, a defined cell is an additional third input, which invariably is in the zero state. each AND input measures one, the 2 1's added up to a Coulomb force greater than that of the fixed zero cell, and the majority gate has also become a two-entry gate (Figure 6), fixed cell be able to be occured by zeroing it and never opening the negatron tunnel junctions.

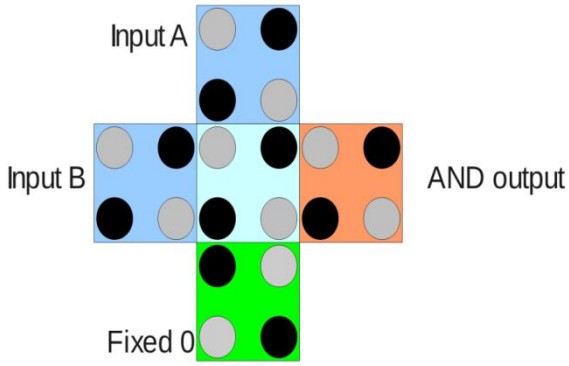


Fig.6: QCA AND Gate

H.OR gate

The process of implementation of OR gate is constructed similarly AND gate with consideration of a fixed 0, 1of QCA cell must be connected to an input. Stationary cell 1 adds a large Coulomb force, with only one other input set to 1, so that the OR gate leaves 1 if one of the free entries is 1 (see Figure 7).

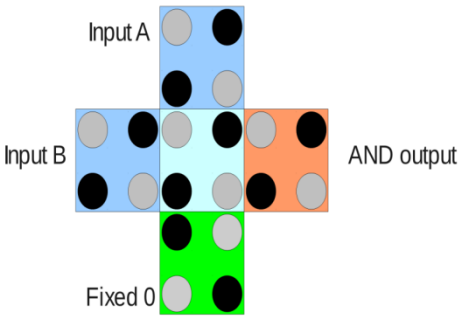


Fig.7: QCA OR Gate

I.NOT gate

The implementations in QCA take a help of cellular changes. A QCA cable is connected to 2 cables, the cell configuration is adjusted by inserting the output cell next to the divided cables so that the angles touch each other (see Figure 8). Since only the corner areas of the cells that touch the fork and the top of the fork can have equivalent damage ton the right side of the cell fork and it will not fit with the associated degree of negatron, but is not prepared to Associate degree Negatron. in the upper corner of the fork, the settings to the right of the fork will be reversed. That makes one at the entrance a zero at the exit and, on the contrary

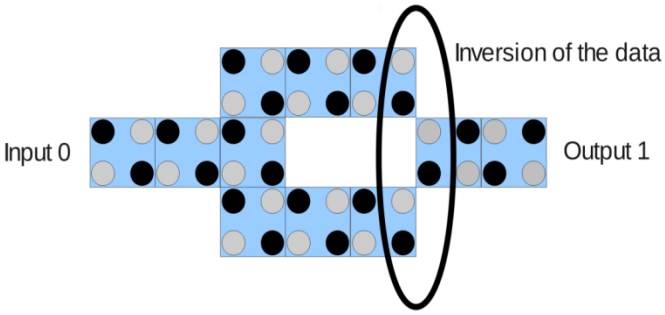


Fig.8: QCA NOT Gate

J. Symmetric cells and special cell arrangements

When planning a QCA circuit, problems are likely to occur, that the QCA cables must cross. Unlike conventional semiconductor device technology, where cables intersect by inserting another layer, QCA cables often cross over same layer works by introducing a type of cell, provided that the four potential wells do not appear to be in the edges of the cell, however ;located in the centre of the perimeters (Figure 9).

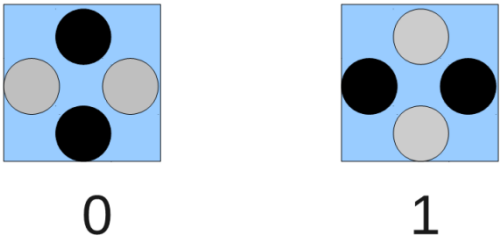


Fig.9: Symmetric adjustments of QCA cell.

If QCA zone units are square-sized organized to construct a cable, configuration of the next cell is reversed relative to those predecessors. The advantage of this type of QCA cell comes from its symmetrical results of Coulomb's strength in traditional cells.

Retrieval Number: D8400118419/2019©BEIESP
DOI:10.35940/ijrte.D8400.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Although, therefore, electrons move with the electrons in adjacent traditional QCA cells, although attributable to their symmetry, they are not pushing electrons to traditional QCA cells in an extremely specific environment. in an extremely different direction, the gift of electrons in an extremely traditional cell does not push them into a symmetrical cell in a specific potential extremely good (Figure 10). This makes it possible to make cable runs of those QCA cells by normal cells. A cross is created using a continuous thread of special cells, so a cross is made through a typical cell cable.

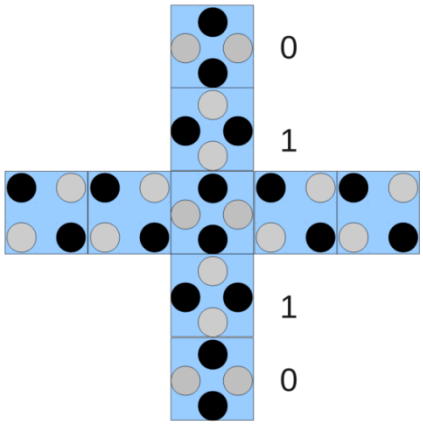


Fig.10: QCA wire crossing

It should be likely to fix symmetric QCA cells to regular cells and vice versa, placing a regular cell so close to two symmetric cells near the beginning or end of a symmetric cell cable. Two symmetric cells chosen must be taken into account because their neighbors are in reverse adjustment, according to the desired configuration, of the original or the inverse (Figure 11).

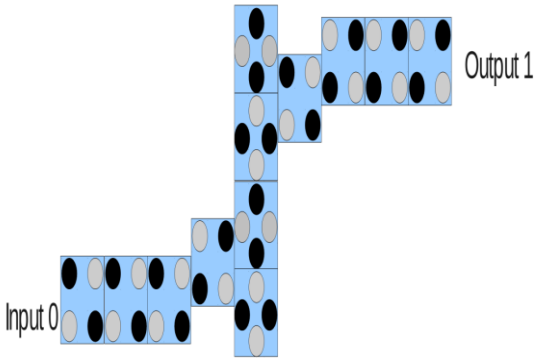


Fig.11: Connections of symmetric and normal QCA cells

K.Clock zones

The zone of clock is a complicated challenge of QCA cell gates. Further prevent random changes of QCA cells and Gate the flow of information, specifically the propagation of data, through QCA logic circuits. Unlike transistor-based circuits, example a clock cycle consists of three clock signals, that can be area unit delayed by 1/3 of the complete clock signal with each other, given in figure 12.

There is an area unit with four clock zones: Zero “Clock, Clock 1 and Clock 2”, systematically applied to each QCA cell in the QCA circuits. typically | this can often be for convenience; Actually, scan together as “clock n, clock n + one, clock n +” two. It is necessary, that precise groups of QCA cells unit area in many clock zones.[43,44]

Clock in each clock zone completely different states: change, maintain, release and relax. There is a half-turn of ninety degrees between four adjoining phases of a clock zone. Figure twelve illustrates four half shifts performed in each continuation half for numerous clock zones. Knowledge stream in an extremely channeled way from inputs to outputs in four clock zones

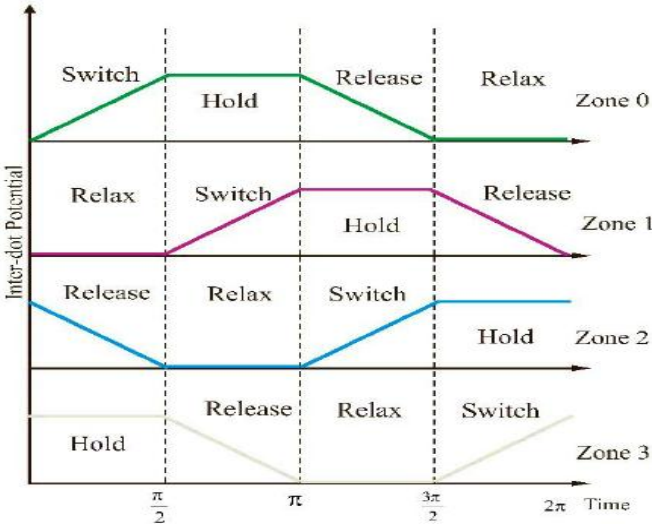


Fig.12: The four shifted clock signals

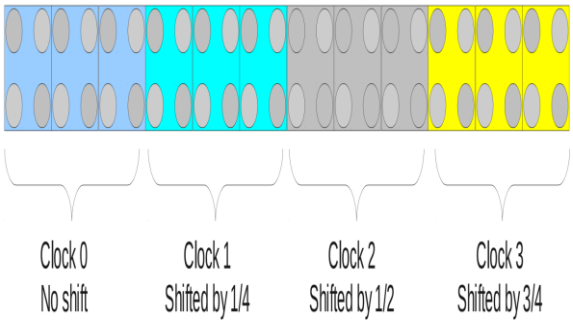


Fig.13: Controlling data propagation in a QCA cell

it opens the junctions of the electron tunnel in the QCA cells When the clock signal is high. In order for the data to propagate successfully through a QCA wire, the clock zones between the cable must be connected to serial clock signals in the direction of the desired data propagation (see figure 13). In QCA cables that have virtually no different QCA cells near the cable, that is, without the "noise" of the Coulomb force in the surrounding area, the clock zones are often giant. In areas with QCA cells around the cable, the clock zones should be smallerThere is no strict rule for the dimensions of a clock zone addicted to surround noise, however, in general, it seems that in areas of screaming the clock zones may need only 2 QCA cells. In areas with virtually no noise, the clock zones are often designed as giant as the QCA 12-14 cells.Although there are no strict rules for starting and finishing a clock zone, there are some better options, a way to place the clock zones around the basic doors, granted in the previous chapters. Once you design the QCA circuits, we have a tendency to strongly recommend staying in those clock zones, there are terribly rare cases in which the clock zones around the basic doors will disagree without moving the spread of reliable knowledge.

M. Clock zones for NOT gate

NOT gate incorporates a fairly essential area of organized QCA cells, NOT gate is vital to place the cells at intervals in the correct clock zones to avoid flipped changes of electrons near the derived cable.

The gate clock space must end at the beginning of the "fork." the entire fork itself, that is, the U-shaped wire, must be at intervals the area of the clock resulting from the input and, together, the output must be at intervals the area of the clock resulting from the fork[43,44].

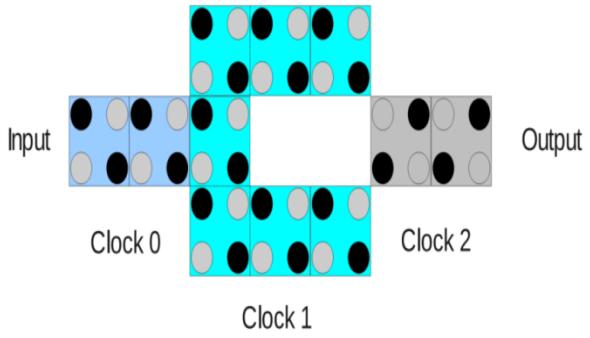


Fig.14: QCA NOT gate clock zones

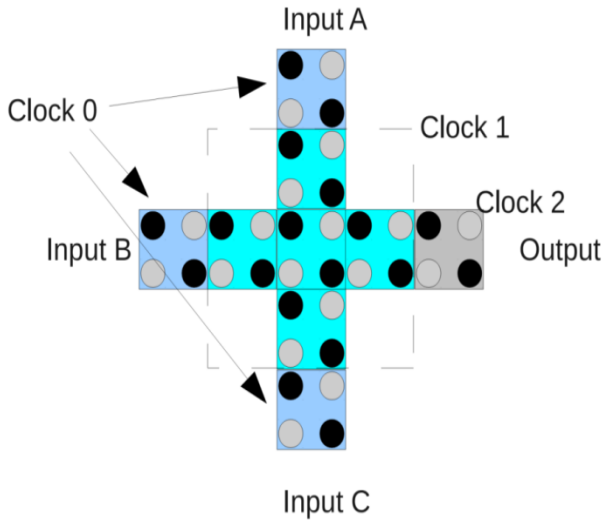


Fig.15:QCA majority gate clock zones

N. Majority gate clock zones

For the majority gate it is necessary that each cell be within the same clock zone. Put some cells in several clock zones will cause incorrect results in the central cell and, therefore, all 3 input and output cells must be within the same clock zone.

O. clock zonesWire crossing

Although wire crossing had been mentioned before, that special symmetric QCA cells don't have an effect on the normal ones in a cable crossing, this is often only true once the special cell area unit is in a very stable state, that is , low value in the clock signal and each electron resides in potential wells. Consider electron area unit moves through the tunnel junctions, they will have an uneven result in nearby regular QCA cells, probably pushing them to an incorrect setting. Crossover wires must be in several clock zones can solve the problem[43,44].

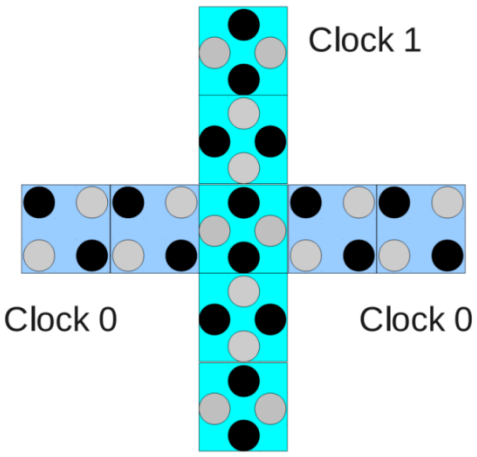


Fig.16: QCA wire crossing clock zones

P. QCA circuit design

QCA may be a technology, however, it is not ready for the market. As a result, design and simulate QCA circuits. For this, use the QCA Designer software system that allows circuit style with an easy-to-use graphical interface. The simulation has also finished QCA Designer. We have a tendency to select the QCA Designer, because it is the most realistic machine with a physical reading purpose, therefore, its simulations are terribly real.

Terribly realistic simulation allows observe disturbances of nearby QCA cells or areas of cells that should not move with each other.

III. EXISTED REVERSIBLE LOGIC GATES

Here we look three basic existed universal reversible logic gates namely:Feynman Gate,,Toffoli Gate and Fredkin Gate There are square measurements of several reversible door implementations based primarily on QCA (C-NOT), Toffoli and Fredkin. An optimized QCA implementations of those reversible doors in terms of space and delay.

A. Implementation of Feynman Gate

Feynman Gate includes a 2-bit input and a 2-bit output. If the primary bit is ready, flip the second bit. The output of the nuclear physicist's Feynman gate is delineated as mapping bits A and B to A XOR B. The Feynman gate is universal; this implies that for any Boolean performance, Toffoli gate will be used to create systems that will perform any desired Boolean calculation in an extremely reversible manner. If input A and B of 2 inputs and 2 outputs for the door area unit of Feynman A, B and X, Y, The process input and output shown in figi17[43,44].

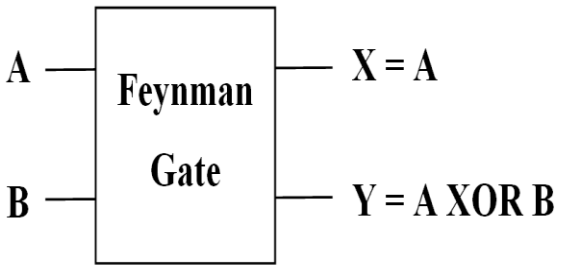


Fig.17:Feynman Gate

The QCA implementation of the planned Richard Phillips Feynman gate employs a pair of inverters, a 5-gate majority gate and a 3-entry majority gate. The 5-gate majority gate has been used to calculate the Boolean operation given in equation (1) as follows:

$$Maj5\ (I1, I2, I2, I3, 0) = I2(I1 + I3) \quad (1)$$

The two inputs "I2" of the 5-gate majority gate in the gate designed by Richard Phillips Feynman are properly configured for A + B, input "I1" is ready for B "and" I3 "for A", separately. Equation (1) is evaluated as an exclusive OR operation of inputs A and B; and is illustrated by equation (2) as follows:

$$Maj5(\bar{B}, A + B, A + B, \bar{A}, 0) = (A + B)(\bar{B} + \bar{A}) = A\bar{B} + \bar{A}B \quad (2)$$

The schematic of Feynman gate is shown in Fig. 18. The optimized layout of proposed QCA based Feynman gate is shown in Fig. 19.

The block diagram of the Richard Phillips Feynman gate is shown in Fig. 18 and final design of the planned QCA-based wire Feynman is shown in Fig. 19.

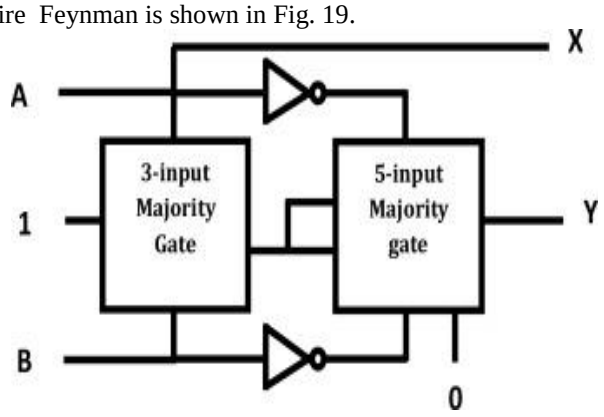


Fig.18: Feynman reversible gate

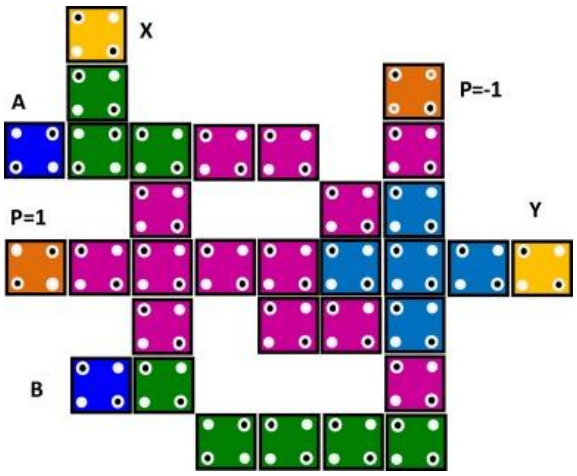


Fig.19:Efficient layout of 5-input majority gate based QCA Feynman gate

B.Toffoli Gate Implementation

Toffoli Gate encompasses a 3-bit input and a 3-bit output. If the set of primary square measurements of 2 bits, flip the third bit. The output of the Toffoli Gate is delineated as mapping bits A, B and C to A, B and C XOR (A and B). Toffoli's gate is universal; This suggests that for any mathematician who operates, Toffoli doors will be used to create systems that will perform any desired mathematical calculation to operate reversibly. If the 3 and 3 output inputs for the Toffoli gate square measure A, B, C and X, Y, Z separately, then their input and output configuration looks as shown in figure 20.

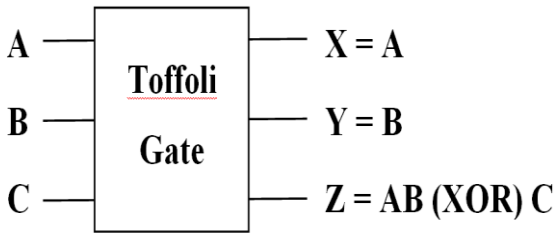


Fig.20:Toffoli Gate

The projected implementation based mainly on QCA of the Toffoli gate uses 2 inverters, a majority gate with 5 entrances and 2 majority gates with 3 entrances. The gate with a majority of 5 inputs has been used to calculate the Boolean performance in equation (1). The two inputs 'I2' of the 5-gate majority gate in equation (1) of the projected Toffoli gate area unit are properly adjusted to AB + C, the input 'I1' is ready for $\bar{C}$ and 'I3' to $\overline{(AB)}$, separately. Equation (1) is evaluated to understand the third exit 'Z' of the Toffoli gate and is represented in equation (3) as follows[43,44]

$$Maj5(\bar{C}, AB + C, AB + C, \overline{AB}, 0) = \bar{A}C + \bar{B}C + AB\bar{C} \quad (3)$$

The schematic of proposed Toffoli gate is shown in Fig. 21. The optimized layout of proposed QCA based Toffoli gate is shown in Fig. 22.

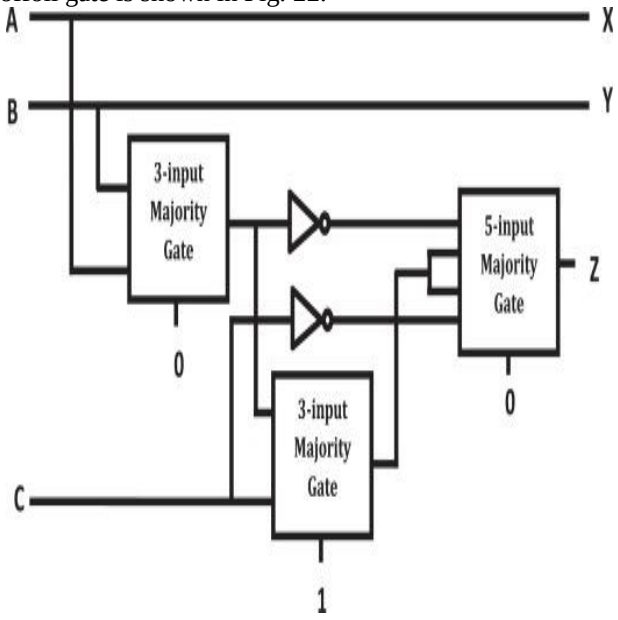


Fig.21: Schematic of designed 3-input Toffoli reversible gate

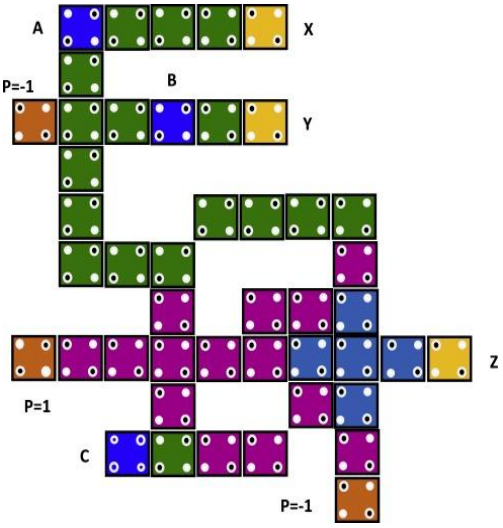


Fig.22:Efficient layout of QCA based Toffoli gate.

C.Fredkin Gate Implementation

The Fredkin gate is one of each of the most studied reversible gate with 3 inputs and 3 outputs. The Fredkin gate manufactures an equivalent range of 1 inside the exit as in the entrance, in addition to the changeability mapping function. Its input parity is equal to the output parity, therefore, Fredkin's

Gate protects the parity. If the 3 inputs and 3 outputs for the Fredkin gate area unit A, B, C and X, Y, Z separately, then its input and output configuration will look as shown in figure 23

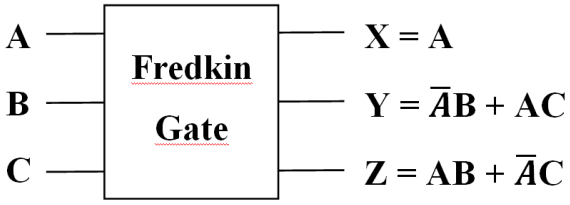


Fig.23: Block Diagram of Fredkin Gate

The projected implementation based primarily on the QCA of the Fredkin gate uses 3 inverters, 2 majority gates with 3 inputs and 2 majority gates with 5 inputs. The schematic of the projected Fredkin gate is shown in Fig. 13. The majority gate with 5 inputs in the right aspect has been used to encrypt the operating equation of the Boolean output "Y" (4) as follows[43,44]:

Maj5 (I1, I2, I2, I3,1) = I2 + I1I3 (4)

The two inputs "I2" of the majority gate of 5 inputs in equation (4) of the area unit of the Fredkin gate configure the AC capacity, input "I1" deals with capacity B and "I3" a $\bar{A}$, separately. The second exit of Fredkin's gate "Y" is completed from equation (4) and is given in equation (5) as follows:

Maj5 (B, AC, AC, $\bar{A}$, 1) = AC + $\bar{A}$B

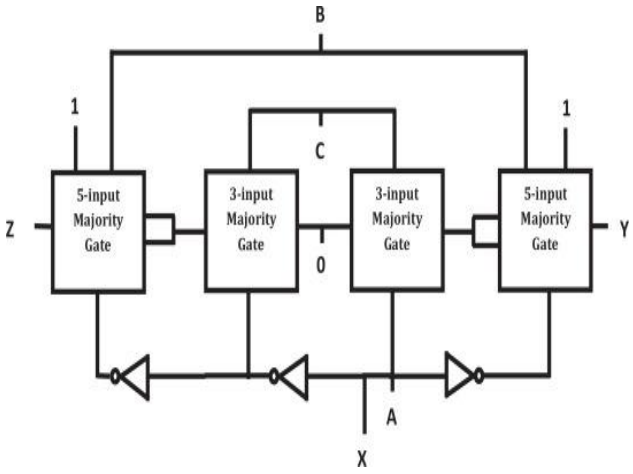


Fig.24:Schematic of proposed 3-input Fredkin reversible gate

The optimized layout of proposed QCA based Fredkin gate is shown in Fig. 25.

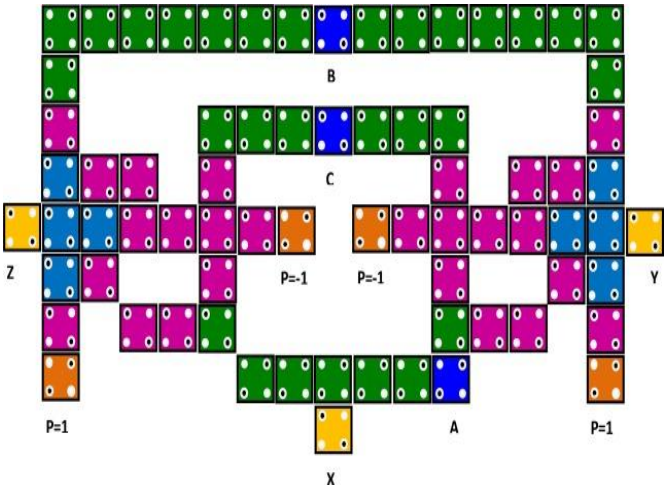


Fig.25: Efficient layout of QCA based Fredkin gate.

The gate with a majority of 5 entries in the left aspect of Fig. 2.8 has been used to calculate the output of the mathematician "Z" using equation (4). the 2 inputs "I2" of the majority gate of 5 inputs in equation (4) of the Fredkin gate area unit configure input A "C," I1 "is about capacity A and" I3 "to B , separately Equation (4) is evaluated to understand the third output 'Z' of Fredkin's door represented in equation (6) as follows[43,44]:

$$Maj5(A, \bar{A}C, \bar{A}C, B, 1) = \bar{A}C + AB$$

IV. PROPOSED METHOD.

A.Algorithm:

AA.Encoding Algorithm:

1. Convert each alphabet of the message (S) into corresponding ASCII value
2. Obtain the binary value from ASCII value
3. Partition the total bit-stream into sub bit-streams of 8-bit long each
4. Provide a secret key (K) of 8-bit long for encoding.

5. Perform XOR operation between key and each sub bit-stream of the message
6. Continue step-5 until all the sub bit-streams are XOR-ed with the key, to form the encoded message
7. Obtain pixel information from the gray scale image (GI)
8. Convert each pixel value into its corresponding binary value
9. Insert the encoded message bit one by one into the LSB bit of each pixel of the image, until all the message bits are embedded within the pixels.
10. Regenerate the image from the encoded pixels as produced in step-9, to obtain the stegono-image (SI).

B. Decoding algorithm

1. Obtain the pixel intensities from the stego image
2. Convert the pixels values into binary values.
3. Extract the LSB bit of each pixel from the binary values which has the information of encoded bits.
4. Divide the total bit stream into sub bit stream of 8 bit long.
5. Perform XOR operation between the key and each sub bit stream.
6. Continue above step until all bit stream are XOR-ed with the key.
7. Convert the result of the above operation into the decimal values.
8. Those decimal values give the ASCII values and with those values regenerate the character.

C.Encoding and Decoding using a image

1. A Grey scale Lena image is taken into consideration and compressed into pixel size of 8x8

Using MATLAB for the implementation in the circuit is shown in the fig 26(a). Matrix representation of its pixels and its binary values are represented in fig 26(b) and fig 26(c) respectively.

Fig.26(a): Original image

151	111	129	138	127	143	160	89
125	108	120	167	182	136	118	86
122	114	132	141	171	184	110	143
125	115	107	85	161	122	97	157
118	107	73	118	153	97	126	171
112	98	90	91	140	87	144	196
120	81	84	77	151	138	144	132
128	71	70	108	149	175	123	91

Fig.26 (b): matrix representation of pixels

pixel position	pixel value	binary representation							
1	151	1	0	0	1	0	1	1	1
2	111	0	1	1	0	1	1	1	1
3	129	1	0	0	0	0	0	0	1
4	138	1	0	0	0	1	0	1	0
5	127	0	1	1	1	1	1	1	1
6	143	1	0	0	0	1	1	1	1
7	160	1	0	1	0	0	0	0	0
8	89	0	1	0	1	1	0	0	1
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
57	128	1	0	0	0	0	0	0	0
58	71	0	1	0	0	0	1	1	1
59	70	0	1	0	0	0	1	1	0
60	108	0	1	1	0	1	1	0	0
61	149	1	0	0	1	0	1	0	1
62	175	1	0	1	0	1	1	1	1
63	126	0	1	1	1	1	0	1	1
64	91	0	1	0	1	1	0	1	1

Fig.26(c): binary representation

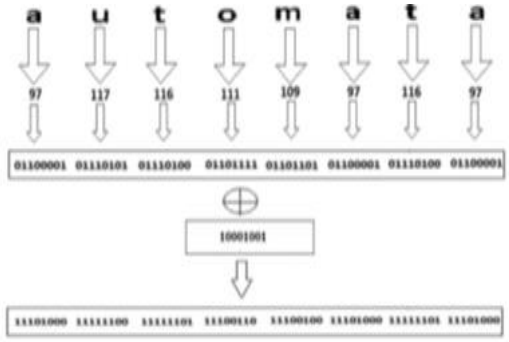


Fig.27: Generation of encoded data bits from string 'automata'

(ii) An eight-bit secret key "10001001" is taken into account for encryption.

(iii) An "automatons" message is taken into account to embed and be reborn in its corresponding binary price, as shown below.

(iv) currently to encrypt and implement the bits of the 'automatons' string within the initial seven-bit image transfer of the binary illustration of each image element through the input channel A1-A7 of the planned encoder circuit. Replace the eighth price of the binary illustration of the image with the binary knowledge of chain 'automata' and transfer it through the information channel inside the gate feynman Richard Phillips Feynman of the planned encoder circuit and secret key bits through the key channel inside the Feynman gate within the planned encoder circuit

(v) The operation of the XOR circuit between the binary knowledge of the chain and, therefore, the key produces the output coded bits of channel B8 of the encoder and decoder circuit planned in Figure Four.7, which can replace the octave binary position Image element illustration. that the intensities of the elements of the image will be modified.

(vi) As shown in the decoder or reversible decoder circuit planned in Figure Four.7, the outputs obtained from output lines B1 to B8, which square the bits of each element of the encoded image. The outputs on the B8 road represent the embedded message bits and, therefore, the outputs on the 'GAR' output line are considered as garbage output.

(vii) The bit stream obtained from the output lines B1 to B8 of the square measurement is reborn in their corresponding element intensities, that square measurement will not generate the image of the stego. His binary illustration of each element is shown twenty eight

pixel position	pixel value	binary representation							
1	150	1	0	0	1	0	1	1	0
2	111	0	1	1	0	1	1	1	1
3	129	1	0	0	0	0	0	0	1
4	138	1	0	0	0	1	0	1	0
5	126	0	1	1	1	1	1	1	0
6	142	1	0	0	0	1	1	1	0
7	160	1	0	1	0	0	0	0	0
8	89	0	1	0	1	1	0	0	1
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
57	128	1	0	0	0	0	0	0	0
58	71	0	1	0	0	0	1	1	1
59	69	0	1	0	0	0	1	1	1
60	108	0	1	1	0	1	1	0	0
61	150	1	0	0	1	0	1	0	0
62	176	1	0	1	0	1	1	1	0
63	127	0	1	1	1	1	0	1	0
64	91	0	1	0	1	1	0	1	1

Fig.28: binary representation of stego image

(viii) throughout the method of secret writing, the SI are reborn in intensities of image elements. These square pixels measure rebirth in binary values of length of eight bits each. Next, the LSB bit of each image element is extracted, that is, the eighth bit of each bit stream to obtain the encoded bits. These coded bits measure whatever is used as input to the projected encoder / decoder during a bit stream. In a constant instance, the key bits of the key must be transferred through the "Key" channel. during this case, outputs B1 - B8 are the bits of the original message. currently, the square measure of B8 bits taken and the square measure are divided into sequences of eight bits and are reborn in the decimal type provided that the decimal type provides EE. UU. the US standard code for the information exchange values of the chain.

D. Proposed ENCODER and DECODER block:

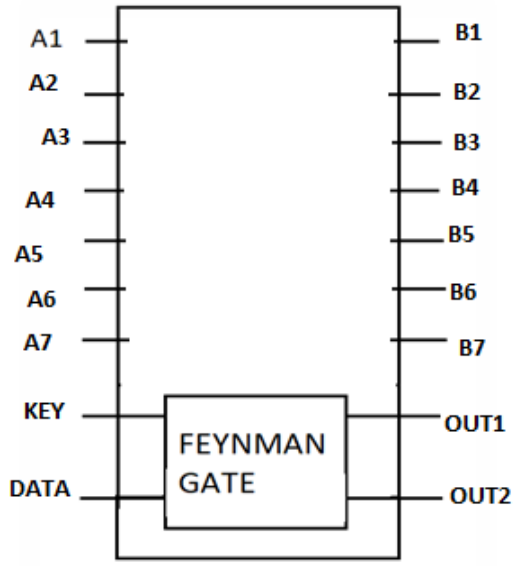


Fig. 29: Proposed Reversible Encoder/Decoder circuit

D. Proposed ENCODER and DECODER circuit using QCA:

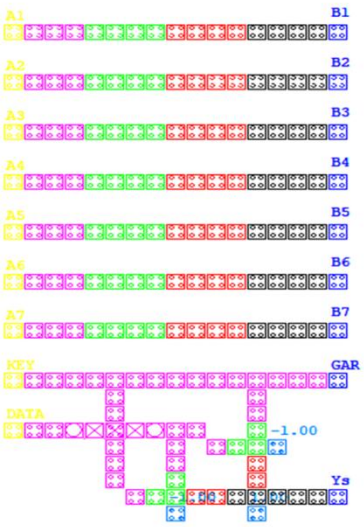


Fig.30: QCA layout of proposed reversible Encoder/Decoder circuit

E. Proposed circuit of Nano communication

The below circuit is the proposed efficient circuit of secure Nano communication technique using image. At the sender's end, the encoder embedded the text within image along with secret key. Then, the generated encrypted image is transmitted through communication medium. On receiving the encrypted image at the receiver's end, decoder retrieves the text using the secret key. The QCA layout of the Nano communication circuit is shown in Fig.30

The next circuit is the planned economic circuit of the image of abuse of the Nano secure communication technique. At the end of the sender, the encoder embeds the text inside the image next to the secret key. Then, the generated encrypted image is transmitted through the communication medium. Upon receiving the encrypted image at the end of the receiver, the decoder recovers the battered text of the key key. The QCA design of the Nano communication circuit is shown in Figure 31.

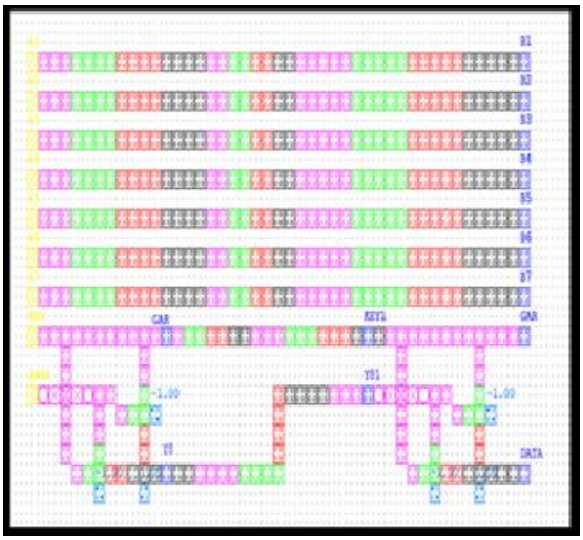


Fig.31: Nano communication circuit using encoder/decoder

V. RESULTS AND DISCUSSIONS

To verify the practicality of compact QCA designed with efficiency based mainly on Richard Feynman and, therefore, the victimization by nano communication of the encoder / decoder circuit, the widely used QCADesigner version two.0.3 tool has been used. The simulation parameters used the area unit of the consistency vector simulation engine configuration. The delay of the projected spatial economic designs of the reversible logic gates is only 3/4 of a clock cycle. The input signals are marked in blue, the output signals in yellow and the clock signal in red alter all waveforms. Figure 32 represents the results of the Richard Feynman door simulation results

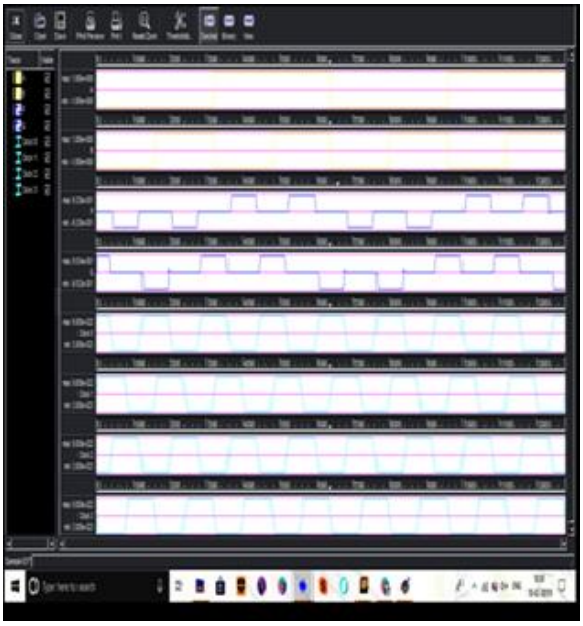


Fig.32: Simulation waveform for Feynman design 1

The fig 33, fig 34, fig 35 describes the simulation results of the design of Feynman gates for the circuits shown in fig 17,fig 18, fig 19 respectively.

Fig.33: Simulation waveform for Feynman design 2

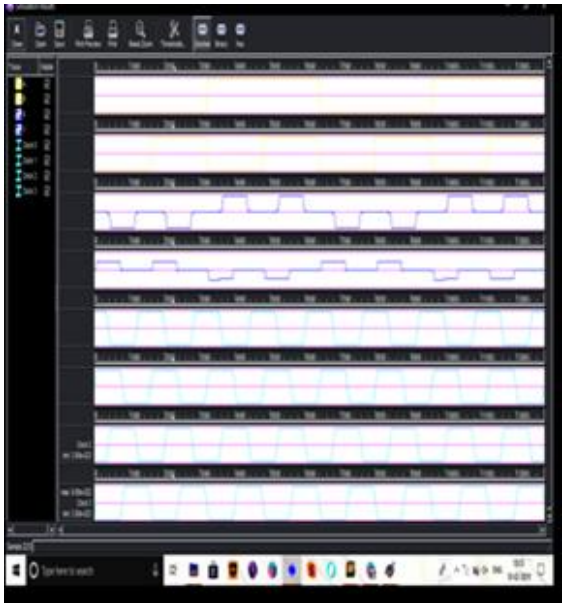
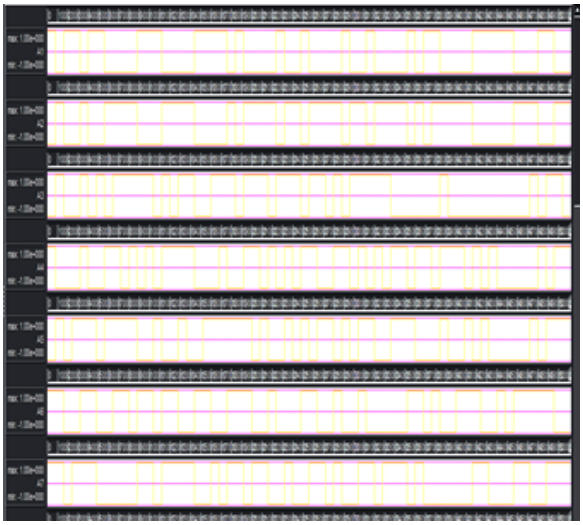


Fig.34: Simulation waveform for Feynman design

Fig.35: Simulation waveform for Feynman design 4

The fig 36 shows the final stimulation results of the Nano communication channel encoder decoder circuit.



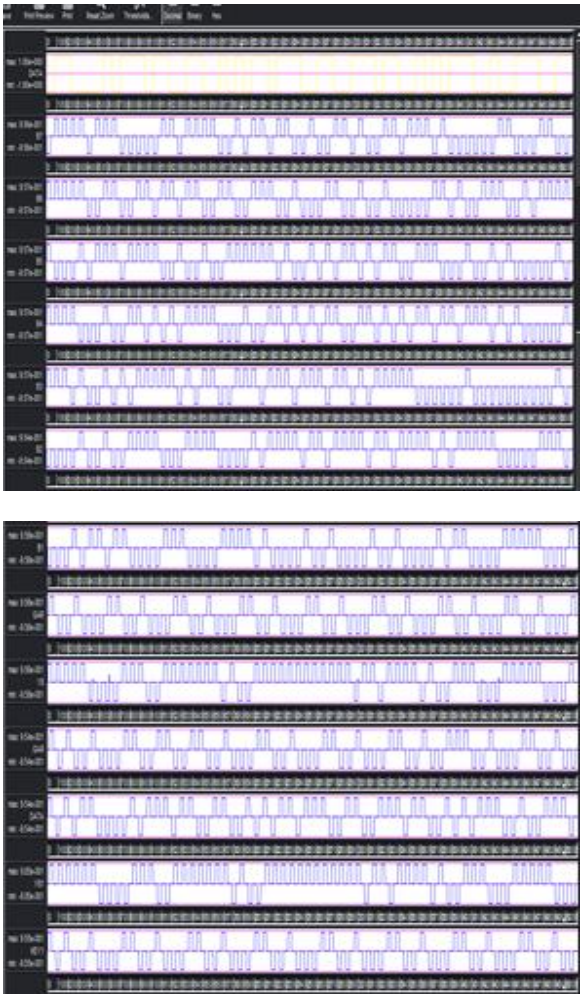


Fig.36: output waveform for nanocommunication channel

A detailed report on the hardware costs achieved from the QCA implementations of various designs of Feynman gate, Reversible Encoder/Decoder circuit and Nano communication Steganographic circuit, in terms of area, cell counts and clock delays are provided in Table 1

Table.1:Detailed Report on hardware of implemented structures

Implemented Structures	Circuit Complexity (Cell-Counts)	Area (μm^2)	Latency (Clock delays)
Feynman Design 1	53	0.060	3-clock phases = (0.75)
Feynman Design 2	32	0.028	3-clock phases = (0.75)
Feynman Design 3	65	0.078	4-clock phases = (1.0)
Feynman Design 4	54	0.046	4-clock phases = (1.0)
Reversible Encoder/Decoder circuit	146	0.112	4-clock phases = (1.0)
Nanocommunation Steganographic ciruit	467	0.388	12-clock phases = (3.0)

VI. CONCLUSIONS

QCA technology is expected to be a possible candidate to exchange CMOS technology due to its distinctive options, such as a terribly high operating frequency, an extra ordinarily low power dissipation and the size of nano scale functions. This proposed method presents a Feynman multi-gate space-economy style, a reversible encoder / decoder circuit for the image steganography technique and also the Nano channel for image steganography.

The proposed method system is a response to QCA circuit implementations based primarily on minimal variety of QCA cells, lower clock delays and reduced space. This method has incontestable planning for an improved QCA logic gate and its implementations as new adder and subtractor structures, which can be useful as an quality building blocks for larger arithmetic units. The simulation results of the planned adder and subtractor circuits are verified by QCA Designer. The planned style area unit is a response to QCA circuit implementations based primarily minimal variety of QCA cells, lower clock delays and reduced space. The results of the simulation of the planned encoder / decoder circuit and the Nano communication image steganography circuit are verified with the QCA Designer.

REFERENCES

1. BikashDebnath, Jadav Chandra Das ,Debashis De.: 'Reversible logic-based image steganographyusing quantum dot cellular automata for secure Nano communication', IET Journals and Magazines.,2017,Vol 11.
2. Cho, H., Swartz lander, E.E.: 'Adder designs and analyses for quantum-dot cellularautomata', IEEE Trans. Nanotechnol., 2007, 6, (3), pp. 374–383
3. Tougaw, P.D., Lent, C.S.: 'Logical devices implemented using quantum cellular automata', J. Appl. Phys., 1994, 75, pp. 1818–1825
4. Jendernalik, W., Szczepanski, S., Koziel, S.: 'Highly linear CMOS triode transconductor for VHF applications', IET Circuits Devices Syst., 2012, 6, (1), pp. 9–18
5. Fredkin, E., Toffoli, T.: 'Conservative logic', Int. J.Theor. Phys, 1982, 21, pp. 219–253
6. Chung, W.J., Smith, B., Lim, S.K.: 'Node duplication and routing algorithms for quantum-dot cellular automata circuits', IEE Proc., Circuits Devices Syst., 2006, 153, (5), pp. 497–505
7. Ottavi, M., Pontarelli, S., Vankamamidi, V., et al.: 'QCA memory with parallel read/serial write: design and analysis', IEE Proc., Circuits Devices Syst., 2006, 153, (3), pp. 199–206
8. Das, K., De, D.: 'Characterization, test and logic synthesis of novel conservative &reversible logic gates for QCA', Int. J. Nanosci., 2010, 9, (3), pp. 201–214
9. Das, K., De, D.: 'Characterization, applicability and defect analysis for tiles nanostructure of quantum dot cellular automata', J. Mol. Simul., 2011, 37, (3), pp. 210–225
10. Das, J.C., De, D.: 'Quantum dot cellular automata based cipher text design for nanocommunication'. Proc. Conf. on Radar, Communication and Computing, TiruvannamalaiTamilnadu, India, December 2012, pp. 343–348
11. Das, J.C., De, D.: 'Reversible binary to grey and grey to binary code converter using QCA', IETE J. Res., 2015, 61, (3), pp. 223–229
12. Arjmand, M.M., Soryani, M., Navi, K.: 'Coplanar wire crossing in quantum cellular automata using a ternary cell', IET Circuits Devices Syst., 2013, 7, (5), pp. 263–272
13. Das, K., De, D., De, M.: 'Realisation of semiconductor ternary quantum dot cellular automata', IET Micro Nano Lett., 2013, 8, (5), pp. 258–263
14. Dysart, T.J.: 'Modeling of electrostatic QCA wires', IEEE Trans. Nanotechnol., 2013, 12, (4), pp. 553–560
15. Perri, S., Corsonello, P., Cocorullo, G.: 'Design of efficient binary comparators in quantum-dot cellular automata', IEEE Trans. Nanotechnol., 2014, 13, (2), pp. 192–202

16. Sen, B., Dutta, M., Sikdar, B.K.: 'Efficient design of parity preserving logic in quantum-dot cellular automata targeting enhanced scalability in testing', Microelectron. J., 2014, 45, pp. 239–248
17. Arafat, M.A., Harun-ur-Rashid, A.B.M.: 'A novel 7 Gbps low-power CMOS ultrawide band pulse generator', IET Circuits Devices Syst., 2012, 6, (6), pp. 406–412
18. Das, J.C., De, D.: 'Novel low power reversible binary incrementer design using quantum dot cellular automata', Microprocess. Microsyst.,2015,doi:10.1016/j.micpro.2015.12.004
19. Das, J.C., De, D.: 'User authentication based on quantum-dot cellular automata using reversible logic for secure Nano communication', Arab. J. Sci. Eng., 2016, 41, (3), pp. 773–784
20. Ali, M.T., Wu, R., Mao, L., et al.: 'High frequency CMOS amplifier with improved linearity', IET Circuits Devices Syst., 2014, 8, (6), pp. 450–458
21. Werner, C., Backs, B., Wirnshofer, M., et al.: 'Resilience and yield of flip-flops in future CMOS technologies under process variations and aging', IET Circuits Devices Syst., 2014, 8, (1), pp. 19–26
22. Das, J.C., Debnath, B., De, D.: 'Image steganography using quantum dot cellular automata', Quantum Matter, 2015, 4, (5), pp. 504–517
23. Das, J.C., De, D.: 'Reversible comparator design using quantum dot-cellular automata', IETE J. Res., 2015, doi: 10.1080/03772063.2015.1088407
24. Das, J.C., De, D.: 'Quantum dot-cellular automata based reversible low power parity generator and parity checker design for Nano communication', Front. Inf. Technol. Electron. Eng., 2015, 17, (3), pp. 224–236
25. Roy, D., Maitra, S., De, D., et al.: 'Analysis of effect of temperature variation on computational faithfulness of a QCA XOR gate'. Int. Conf. on Electronics, Communication and Instrumentation (ICECI), Kolkata, West Bengal, India, January 2014, pp. 1–4
26. Boneh, D., Sahai, A., Waters, B.: 'Functional encryption: definitions and challenges'. Eighth Theory of Cryptography Conf. (TCC), Berlin, March 2011, (LNCS, 6597), pp. 253–273
27. Liu, W., Srivastava, S., Lu, L., et al.: 'Are QCA cryptographic circuits resistant to power analysis attack?', IEEE Trans. Nanotechnol., 2012, 11, (6), pp. 1239–1251
28. Pudi, V., Sridharan, K.: 'Efficient design of a hybrid adder in quantum-dot cellular automata', IEEE Trans. Very Large Scale Integr. (VLSI) Syst., 2011, 19, pp. 1535–1548
29. Walus, K., Dysart, T.J., Jullien, G.A., et al.: 'QCADesigner: a rapid design and simulation tool for quantum-dot cellular automata', IEEE Trans. Nanotechnol., 2004, 3, pp. 26–31
30. Basu PN, Bhowmik T On embedding of text in audio - a case of steganography. inproc of IEEE International Conference on Recent Trends in Information, Telecommunication and Computing, India. (2010)
31. Pevny T, Filler T, Bas P Using high-dimensional image models to perform highly undetectable steganography. Information Hiding (2010) 6387: 161-177.
32. Nguyen BC, Yoon SM, Lee HK Multi bit plane image steganography. International Workshop on Digital Watermarking (2006) 4283: 61-70.
33. Kuo WC, Kuo SH, Wu LC Multi-bit data hiding scheme for compressing secret messages. ApplSci(2015) 5(4): 1033-1049.
34. Cvejic N, Seppanen T Reduced distortion bit-modification for LSB audio steganography. Journal of Universal Computer Science (2005) 11(1): 56- 65.
35. Gopalan K, Shi Q, Audio steganography using bit modification - a tradeoff on perceptibility and data robustness for large payload audio embedding. inProc of IEEE 19th International Conference on Computer Communications and Networks (ICCCN), Switzerland. 2010
36. Mammia E, Battisti F, Carlia M, Neria A, Egiazarianb K, et al. A novel spatial data lhiding scheme based on generalized Fibonacci sequences. inProc of SPIE, Mobile Multimedia/Image Processing, Security, and Applications (2008) 6982: 1-7.
37. Pund-Dange S, Desai CG Data hiding technique using catalanlucas number sequence. Indian Journal of Science and Technology (2017) 10(4): 1-6. [38]Yang CY, Wang WF Block-based colour image steganography using smart pixel-adjustment. Genetic and Evolutionary Computing (2015) 329: 145-154. [39]. Chugh G, Yadav R, Saini R A new image steganographic approach based on mod factor for RGB images. International Journal of Signal Processing, Image Processing and Pattern Recognition (2014) 7(3): 27-44.
38. Feng B, Lu W, Sun W Secure binary image steganography based on minimizing the distortion on the texture. IEEE Transactions on Information Forensics and Security (2015) 10(2): 243-255.
39. Qazanfari K, Safabakhsh R (2014) A new steganography method which preserves histogram: generalization of LSB++. Elsevier Journal of Information Sciences 277: 90-101.
40. www.informatik.uni-erlangen.de
41. Gurumohansingh,R.K.Sarin,BalwinderRaj,"Design reversible logic gates", Microprocessors and Micro systems, 2017
42. Mehta, Usha&Dhare, Vaishali. (2017). Quantum-dot Cellular Automata (QCA): A Survey.

AUTHORS PROFILE

Mr.V.Nancharaiah is completed M.Tech and pursuing Ph.D from JNTU Kakinada. Currently he is working Associate professor in Lendi Institute of Engineering and TechnologyVizianagram.He published many research papers in VLSI , signal and Image Processing. Heis a life memberfrom IETE,IE.

Dr. B.Sridhar obtained the Ph.D degree in medical image processing from theJNT University Kakinada in the year 2015. He has joined the Electronics and communication Engineering Department at Lendi Institute of Engineering and Technology in 2011 and continues to work as Professor. His research interests are Medical Image Processing, Machine Learning and nano VLSI design. He is a life member from IEEE,IETE,IE.He has a strong basic knowledge on image processing techniques using advanced and hybrid methods in both spatial and frequency domain. He also have a very good knowledge on neural networks and deep learning methods, Good programming skills using MATLAB,PHYTON applied on medical image data sets. He has published 29 research papers in, National, International Journals so far.

Dr.S.Sridhar obtained his doctorate degree in Artificial Neural Network based VLSI medical image processing techniques from theJNT University Kakinada in the year 2016. He joined as a professor at the Electronics and communication Engineering Department at Lendi Institute of Engineering and Technology in 2012 and continues to work as Professor. His research interests are VLSI Signal and Medical Image Processing, Machine Learning. He is a life member of MISTE, MIE etc. He is having good knowledge in developing MATLAB, VHDL codes coding various image compression techniques and few other hybrid methods. He also have a very good knowledge on neural networks and deep learning methods and their VLSI Implementation.He has published 20 research papers in high index, National, International Journals so far

Myself **N. Haritha**.I pursued my Under graduation from Lendi institute of engineering and technology. I am very much interesting to work on VLSI based design projects

Myself **N.L.N.KeshavKumar**.I pursued my Under graduation from Lendi institute of engineering and technology. I am very much interesting to work on VLSI based design projects