

Received May 17, 2020, accepted June 5, 2020, date of publication June 12, 2020, date of current version July 3, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3002081

Security Analysis With Novel Image Masking Based Quantum-Dot Cellular Automata Information Security Model

BIKASH DEBNATH¹, JADAV CHANDRA DAS², DEBASHIS DE¹, (Senior Member, IEEE), SANKAR PRASAD MONDAL³, ALI AHMADIAN^{4,6}, (Member, IEEE), MEHDI SALIMI^{5,6}, AND MASSIMILIANO FERRARA⁶

¹Department of Computer Science and Engineering, Maulana Abul Kalam Azad University of Technology, Haringhata 741249, India

²Department of Information Technology, Maulana Abul Kalam Azad University of Technology, Haringhata 741249, India

³Department of Natural Science, Maulana Abul Kalam Azad University of Technology, Haringhata 741249, India

⁴Institute of Industry Revolution 4.0, The National University of Malaysia, Bangi 43600, Malaysia

⁵Center for Dynamics, Institute of Analysis, Technische Universität Dresden, 01062 Dresden, Germany

⁶DiGiES & Decisions Lab, Mediterranean University of Reggio Calabria, 89125 Reggio Calabria, Italy

Corresponding authors: Ali Ahmadian (ahmadian.hosseini@gmail.com) and Jadav Chandra Das (jadav2u@gmail.com)

This work was supported by DiGiES & Decisions Lab, Mediterranean University of Reggio Calabria, Reggio Calabria, Italy.

ABSTRACT Mask of an image is generated in this article using Quantum Dot Cellular Automata. An encoder circuit is drafted to produce the Mask Image. This encoder can function as a decoder as well. A mask image is used to retrieve the original image, although the secret key remains unknown. Power dissipation calculations are performed to comprehend the proposed circuit consumes lower power dissipation at nano-scale level design. The security of the proposed circuit is guaranteed by validating with different security standards. The design paradigm matches the theoretical values, which authorizes the accurateness of the proposed circuit. The Structural Similarity (SSIM) index of the retrieved image is calculated to establish the degradation of the image quality is minimal. The stuck-at-fault analysis is performed to prove the stability of the circuit.

INDEX TERMS QCA, mask image, cipher image, power dissipation, SSIM, security.

I. INTRODUCTION

Complementary metal-oxide-semiconductor (CMOS) technology possesses some inherent as well as physical limitations [1]–[3], unfavorable to produce electronic devices to meet modern requirements. An alternative is keenly needed. Quantum-Dot Cellular Automata (QCA) [4]–[7] functions as a replacement for CMOS. It is a transistor-less architectonics useful to design nano-communication circuits. Each of the cells is constituted of two electrons embedded within two of the four dots which are capable of moving along the tunnels present within them. A cell is negative or positive in charge, according to the polarization obtained by the cell [8]–[11]. The cells are laid one after another to obtain a circuit. Columbic force acts among the cells, for which dual stability feature generated in QCA [12]–[16]. This conducts computation as well as transfer of binary information.

Nano-communication is performed through the nano devices using QCA cells. It is necessary to enhance the safety

The associate editor coordinating the review of this manuscript and approving it for publication was Luca Cassano.

feature of QCA devices during nano-communication. Masking of image is a method where an image is first encrypted with a random key to generate an encrypted image, called cipher image. The cipher image is then encrypted with the original image to obtain a mask image. Mask image is an obscure set of data for a user. Later this set can be used to retrieve an image from another cipher image, which is obtained by the same set of random keys. The key remains concealed.

A mask image is generated using the proposed QCA encoder to ensure the security feature in this article. This mask image is used to obtain the secret message even the secret key remains confidential.

The benefits of the paper are

- QCA technology produces mask image at nano-scale level. To serve the purpose a codec is designed. The data can be retrieved, when the key stays confidential.
- To verify the security of the proposed design, different security standard-based analysis is performed.
- The amount of power depletion of the proposed layout is calculated.

- Structural Similarity (SSIM) Index of the image is determined to verify the accuracy of the proposed method.
- The study of the stuck-at-fault effect on the proposed design is performed.
- Comparison with other existing security models is performed.

The paper comprises of six sections. Section II reveals the related works. The proposed encoder for image masking, its algorithm and procedure are explained in Section III. In this section, the mask image creation technique and actual image retrieval procedure are described. Section IV shows the design of the proposed encoder/ decoder architecture. Result analysis is done in Section V which comprise of complexity calculation for the suggested circuit, power dissipation calculation, and the security analysis part, respectively. The last part, Section VI, portrays the conclusion.

II. RELATED WORK

The work performed in the arena of image processing, in terms of QCA is reported in articles [17]–[21]. In [17], the mathematical derivation of a multichannel filter is proposed and implemented to perform image processing. Using QCA technology, the threshold of an image is calculated in [18]. Nano sized low power design obtained. Image negative operation is executed in [19] using QCA, nano-level architecture is proposed. The dark portion of an image is developed by enhancing the white and gray color pixels. Single-bit full adder and memory cells have been used to perform the task. In [20], implementation of a median filter and mathematical morphological processes are observed over binary images, comprehend using QCA based architectures. One of the fundamental functions related to image processing, convolution, and correlation is performed in [21].

Enhancement of nano-communication security is presented in the articles [22]–[31]. In [22], a ciphertext generation is implemented using QCA. In [23], A5/1 stream cipher is designed with QCA, which is an essential requirement for encryption algorithms in the global system for mobile communication (GSM). Article [24] presents a serpent block cipher utilizing QCA, which constitutes the fundamental segment for creating a block cipher. Another domain of security is steganography, which is introduced in QCA technology. Least significant bit (LSB) Steganography is implemented using QCA in [25]. In order to increase information security, information theory is used. A reversible architecture of concern [25] is designed in [26], where the circuit cost is calculated. Reversible logic is used for the implementation of secure authentication, merged with QCA technology. The respective circuit is designed in [27]. The ciphertext is generated using reversible design in combination with QCA explored in [28]. A reversible crossbar switch is presented in [29]. It introduces the switch operating technique used during the nano-communication process.

In comparison with the existing conventional circuits, it is more cost-efficient. The design of circuit switching is represented in [30], generated using QCA. It is comprised of

multiplexer, demultiplexer, and crossbar switch. The consequence of the control signal is conferred as a mask image formation and retrieval of the original image displayed in [31].

Article [32] introduces an unique optical multi-image hiding approach. It is centered upon two cascaded free-space transmissions. A photograph is encrypted to create one statistically unbiased phase mask. Using the standardized section mask inside the process recovery algorithm. In [33] the efficiency and protection of current masking algorithms developed in a parallel application on the 32-bit embedded computing framework for the AESR ijndael norm and the Fantomas bit-slice cipher. Article [34] suggests an image encryption algorithm. It focuses on the hyper-chaotic method. A 256-bit long secret key is utilized. It comprises of three sections. The second section employs the image masking method. Masking is employed to achieve greater susceptibility, complicacy, and security. A new masking method is proposed in [35]. A single Boolean matrix product combines with conventional Boolean masking additives. This masking adapts well for bitslice cipher applications.

An extensive security analysis is conducted. In [36], it is reported that people now a day's grab images from smart devices and transfer the data to cloud storage. It is generally utilized for storing client produced interactive media content. There is a danger of potentially private information spillage exists since cloud storage is an open space. A coordinated plan is proposed to secure the protection of data on cloud [36]. It includes undetectable watermarking, sharing strategies, and masking. The evaluation result proves that the proposed system may prevent malicious users from accessing private images. In [37], rear-mounted masked idea using Gyrator Transform (GT) is proposed to improve the protection of the second lens of the prevailing Double Random Phase Encoding (DRPE) system. It works on a spiral level approach.

III. PROPOSEDWORK

An " $m \times n$ " gray scale image is considered as an input image. The image is divided into slices of " 8×8 " pixels. A random key of size " 8×8 " pixels is generated for the image slice mentioned previously. American Standard Code for Information Interchange (ASCII) value of the key and the pixel values are bitwise XOR-ed. This procedure is continued for all slices of the image one after another. After the completion of the procedure, a Cipher image is obtained. The resultant image and the input image are XOR-ed to achieve the Mask image [31]. Algorithm 1 presents the procedure of the generation of Mask image. Algorithm 2 presents the retrieval of the second original image.

A. MASK IMAGE CREATION

The conversion of the image to mask image [38]–[42] depicted in Fig. 1(a). An image "Flower.jpg" shown in Fig.1 (b) is used as the input image. It is 128×128 pixels in dimension. It is a grayscale image. It contains 2^8 levels, where "0" represents black, and "255" represents a

Algorithm 1 Algorithm for Generation of Mask Image

Input: An Image (IM), p and q denotes the rows and columns
Output: A Mask Image (MASK)

/* Pixel data of the image IM is represented in the form of 2D array and stored in a 2D array A[][]*/
 1. For each pixel value in each row (p) and column (q) of the image
 $A[p][q] \leftarrow \text{Pixelvalue of IM.}$
 /* Randomly select an ASCII value within the range 0-255 to store the secret key bits in T[][]*/
 2. For rows (p) and columns (q)
 $T[p][q] \leftarrow \text{Randomly selected values within 0-255}$
 /* XOR the values in A[][] with T[][] to create CI[][] which contains the cipher image information */
 3. For each elements present in A[p][q] and T[p][q] of each row(p) and column(q)
 $CI[p][q] = A[p][q] \oplus T[p][q]$
 /* XOR operation between Cipher Image, CI[][] and the original image, A[][] performed to obtain the Mask Image and stored in MI[][] */
 4. For each element present in CI[][] and A[][] of each row(p) and column(q)
 $MI[p][q] = A[p][q] \oplus CI[p][q]$
 /* Mask Image is created by combining all 8 X 8 image slice*/
 5. For each values section of MI[][] each row(p) and column(q)
 $MASK \leftarrow MI[p][q]$

Algorithm 2 Algorithm for Retrieving the Original Image

Input: A new image (NIM) is taken. A new cipher image (NCI) is generated from NIM. It is obtained by the same set of key bits, T[][] used to produce the Mask Image (MASK), as stated in Algorithm 1. The Mask Image (MASK) and its 8 x 8 slices are represented by MI[[]]. Rows are denoted by using p, and columns are denoted using q.
Output: The second image is the new image (NIM)

/* Cipher image’s information of pixels are extracted and stored in a 2D array, NewCI[][]*/
 1. For each pixel values of the Cipher Image (NCI)
 $NewCI[p][q] \leftarrow \text{Pixelvalue of NCI}$
 /* Mask image’s information of pixels are extracted and stored in a 2D arrayNewMI[][]*/
 2. For each pixel values in each Row and Column of the image
 $NewMI[p][q] \leftarrow \text{Pixelvalue of MI}$
 /* XOR operation is performed bitwise between New Cipher image’s pixel values and the earlier obtained Mask Image to retrieve the second original image */
 3. For each element present in MI[][] and NewCI[][] each row(p) and column(q)
 $NewIM[p][q] = NewCI[p][q] \oplus MI[p][q]$
 /* New Image, NIM is created which is equivalent to second original image, obtained by combining all 8 X 8 image slices */
 4. For each values of NewIM[][] each row(p) and Column(q)
 $NIM \leftarrow NewIM[p][q]$

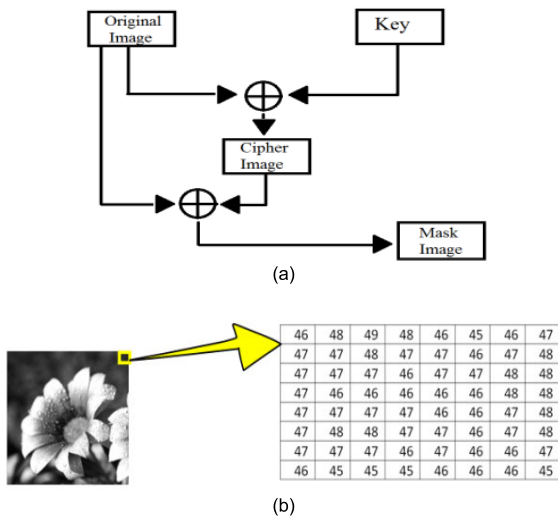


FIGURE 1. (a) Method of the generation of Mask Image, (b) Input image “Flower.jpg” and a slice of its pixel information in 8 x 8 pixels format.

white color. The image is then partitioned into 8 x 8 pixels. Table 1 denotes the corresponding binary values of Fig. 1(b).

- An ASCII value is randomly selected within the range 0-255, XOR operation is applied with the pixel value starting from the first pixel. It continues until all the

pixels within the slice are exhausted. The procedure continues for other slices similarly.

- On completion of the whole procedure, a cipher image is created “Flower_Cipher.jpg”, as shown in Fig. 2(a). This is an encrypted image. It is encrypted by randomly generated key, as mentioned earlier.
- XOR operation is performed between “Flower_Cipher.jpg” and the “Flower.jpg” to obtain the mask image, which is portrayed in Fig. 2(b), and termed as “Flower_Mask.jpg”. All the pixels of the mask image are explored in Fig. 2(b).

The Decimal Values Of Each Pixel Of Fig. 2(B) Are Converted Into Binary Values And Presented In Table 2

B. IMAGE RECOVERY USING MASK IMAGE

The procedure of retrieval of the second original image using the mask of the first image (MASK) from a new cipher image is shown in Fig. 3. A new cipher image is obtained, “Cipher_Image2.jpg”, using the pre-defined procedure as stated in Algorithm 1. The same key is used to generate the cipher and mask image of the first image. XOR operation is applied between the cipher image “Cipher_Image2.jpg” and the mask image,

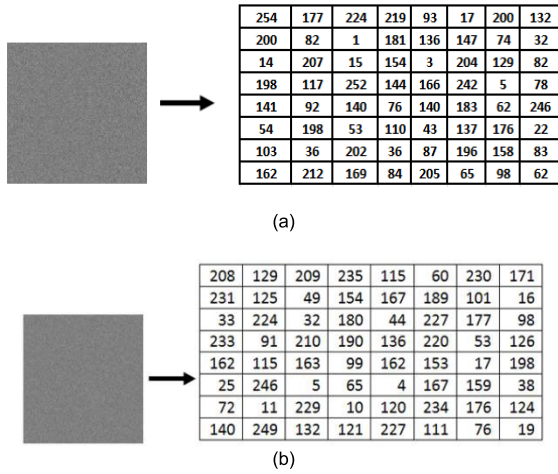


FIGURE 2. (a) Cipher image “Flower_Cipher.jpg” of Fig. 1b and corresponding pixel matrix, (b) Mask image “Flower_Mask.jpg” of Fig. 1b and corresponding pixel matrix.

TABLE 1. Binary representation of Fig. 1(b).

Pixel Position	Pixel Value	Binary Illustration							
^a IM[m][n]		^b X ₁	X ₂	X ₃	X ₄	X ₅	X ₆	X ₇	X ₈
IM[1][1]	46	0	0	1	0	1	1	1	0
IM[1][2]	48	0	0	1	1	0	0	0	0
IM[1][3]	49	0	0	1	1	0	0	0	1
IM[1][4]	48	0	0	1	1	0	0	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
IM[8][5]	46	0	0	1	0	1	1	1	0
IM[8][6]	46	0	0	1	0	1	1	1	0
IM[8][7]	46	0	0	1	0	1	1	1	0
IM[8][8]	45	0	0	1	0	1	1	0	1

^aIM[m][n] (m,n=1,2,...,8) -- Input data to be passed through different channels. The rows and columns are represented by m and n.
^bX_i (i=1, 2,...,8) –Binary data passed through different channels.

TABLE 2. Binary representation of Fig. 2(b).

Pixel Position	Pixel Value	Binary Illustration							
^a MI[m][n]		^b X ₁	X ₂	X ₃	X ₄	X ₅	X ₆	X ₇	X ₈
MI[1][1]	208	1	1	0	1	0	0	0	0
MI[1][2]	129	1	0	0	0	0	0	0	1
MI[1][3]	209	1	1	0	1	0	0	0	1
MI[1][4]	235	1	1	1	0	1	0	1	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
MI[8][4]	227	1	1	1	0	0	0	1	1
MI[8][6]	111	0	1	1	0	1	1	1	1
MI[8][7]	76	0	1	0	0	1	1	0	0
MI[8][8]	19	0	0	0	1	0	0	1	1

^aMI[m][n] (m, n=1,2,...,8) Output data obtained from different channels. The rows and columns are represented by m and n.
^bX_t (t=1, 2,...,8) is the binary output data obtained in different channels.

“Flower_Mask.jpg” to retrieve the second original image. Both the mask image “Flower_Mask.jpg” and the cipher image of the second image “Cipher_Image2.jpg” are produced using the same secret key. To obtain the second original image, the mask image, “Flower_Mask.jpg” and “Cipher_Image2.jpg” is required at the decoder section.

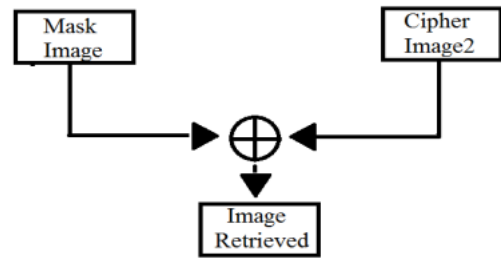


FIGURE 3. Retrieval procedure of the Original image.

Thus, the mask image, “Flower_Mask.jpg” is used as a secret key in this case, and it proves the non-requirement of the secret key at the decoder section. So, both the masked image and the ciphered picture must be transmitted to the receiver.

In the decoding phase, the mask image is used as a secret key to obtain the original image from the cipher image. The decoding is performed to show the decoding can be performed without the secret key used in encryption. So, any cipher image which was encrypted with the same secret key, used in the proposed encryption phase, can convert back to the original image using the mask image. The key remains hidden within the mask image, which is unknown to the attacker to prevent unauthorized access.

IV. ARCHITECTURE FOR THE PROPOSED CIRCUIT

The procedure to obtain a mask image is depicted in Algorithm1. The technique of formation of mask image and its related data are shown in Table 1 and Table 2, respectively. From these two tables, a figure is constructed and revealed in Fig. 5(a). $IM_i[i = 1, 2... m]$ denotes the binary bit values of the individual pixel of the actual image. $KI_i[i = 1, 2 \dots n]$ represents the secret key and $CI_i[i = 1, 2... m]$ denotes the cipher image. The mask image $MI_i[i = 1, 2 \dots n]$ is obtained on the application of bitwise XOR between the cipher image, CI_i and the original image, IM_i . The corresponding logic expression can be drawn as

$$MI_i = CI_i \oplus IM_i \quad (1)$$

$$\text{Where, } CI_i = KI_i \oplus IM_i \quad (2)$$

The expression for majority gate (MV) obtained from (1) and (2) are

$$MI_i = M(M(IM'_i, CI_i, 0), M(IM_i, CI'_i, 0), 1) \quad (3)$$

$$\text{where, } CI_i = M(M(IM'_i, KI_i, 0), M(IM_i, KI'_i, 0), 1) \quad (4)$$

where, M denotes Majority gate expression, in (3) and (4). When 1-bit is considered, (1) expressed as

$$MI_1 = ((IM_1 \oplus KI_1) \oplus IM_1) \quad (5)$$

The majority voter(MV) based schematic diagram corresponding expression (5) is outlined in Fig. 4 (a). It comprises two XOR circuits, six MVs and four inverters (IV). Its equivalent QCA implementation is displayed in Fig. 4 (b). The truth table of this circuit is shown in Table 3. The QCADesigner

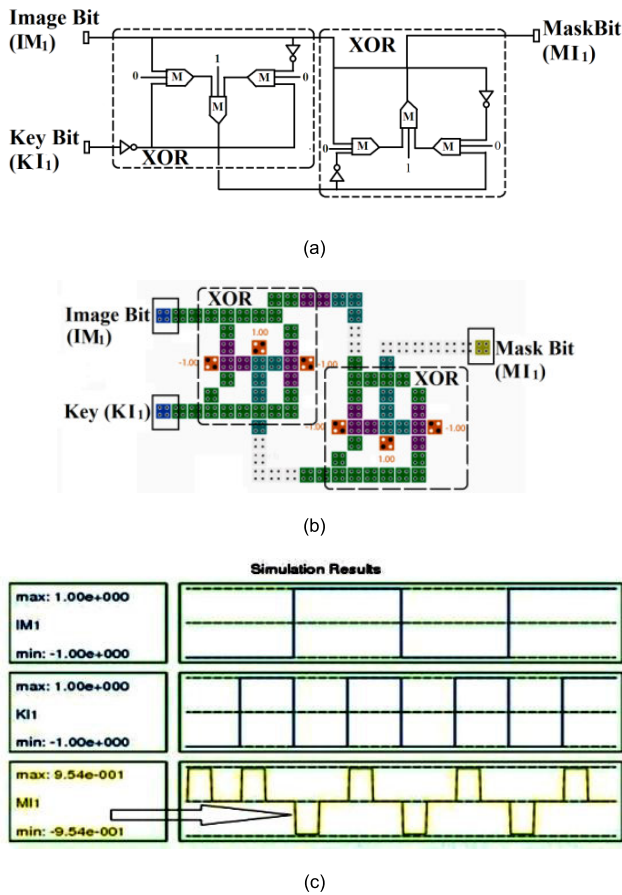


FIGURE 4. Building block (a) Schematic, (b) Layout, (c) The simulation result.

TABLE 3. Theoretical values for basic building block.

Image Bit		Mask Image bit
IM ₁	KI ₁	MI ₁
0	0	0
0	1	1
1	0	0
1	1	1

tool [43] based simulated waveform of Fig. 4(b) is shown in Fig.4(c). The valid output appears after two clock pulses, as shown with arrow. It is seen that for inputs IM₁(0, 0, 1, 1), KI₁(0, 1, 0, 1), the output is MI₁(0, 1, 0, 1) and thus satisfies the theoretical values presented in Table 3. This evaluation confirms the accuracy of the design.

The circuit shown in Fig. 4(b) is the building block of the encoder architecture for generation of mask image has been developed and shown in Fig. 5(c). This proposed architecture can process 8-bits of an image, 8-bits of the secret key, and produces an output of 8-bits of the mask image. The QCA schematic of the proposed encoder is explored in Fig. 5(b). This encoder circuit can used as decoder circuit. The QCADesigner tool [43] based simulated waveform of Fig. 5(c) is shown through Fig. 6 and Fig. 7. Figure 6(a) shows the input image bits. Figure 6(b) shows the input

key bits. Figure 7 shows the generated mask bits. The valid outputs have appeared after two clock pulses, shown with the rectangular box. It is seen from Fig. 6 and Fig. 7, the inputs and the outputs of Fig. 5(a), confirms the accuracy of the design. The Cipher bits are additionally shown in Fig. 5(a).

V. RESULT ANALYSIS

A. EXPERIMENTAL ANALYSIS OF THE PROPOSED METHOD

Three images considered in Fig. 8 are bitwise XOR-ed with three different sets of keys to form the cipher images. Each of the cipher images is bitwise XOR-ed with their respective original images to obtain the mask images, which is displayed in Fig. 8. The cipher image generation of the 2nd set of images is depicted in Fig. 9(a), formed using bitwise XOR operation with the same set of keys used during mask image formation in Fig. 8. The retrieval of the 2nd set of images is represented in Fig. 9(b). Bitwise XOR between the mask images formed in Fig. 8 with cipher images is displayed in Fig. 9(a) to retrieve the 2nd set of original images.

B. STRUCTURAL SIMILARITY INDEX (SSIM) AND STRUCTURAL DISSIMILARITY (DSSIM) MEASUREMENT

Human visual system (HVS) model proposes image quality. The three parameters on which HVS depends are luminance, contrast, and structure, respectively. SSIM [44] is the measurement of the degree of structural disparity occurs within an image when an image is modified. SSIM deals with the degree of deviation occur between the input image and the processed output image. The degree of deviation depends on contrast, luminance, and structural difference. Two blocks for each image of the same size a and b are considered to calculate the SSIM within two images, then SSIM is calculated using the formula as in (6).

$$SSIM(a, b) = \frac{(2\rho_a\rho_b + \gamma_1)(2\beta_{ab} + \gamma_2)}{(\rho_a^2 + \rho_b^2 + \gamma_1)(\beta_a^2 + \beta_b^2 + \gamma_2)} \quad (6)$$

The mean value of “a” is represented by ρ_a , the mean value of “b” is represented by ρ_b , the variance about “a” is β_a^2 , the variance about “b” is β_b^2 , the variance about “a” and “b” is β_{ab} . $\gamma_1 = (k_1L)^2$ and $\gamma_2 = (k_2L)^2$ are the two variables, which stabilize the division result having low denominator with default $k_1 = 0.01$, $k_2 = 0.03$, and $L = 2^{bits/pixel-1}$ represents the change in pixel value. The eqn. (6) has three tuples. Those components are structure (s), contrast (c), and luminance (l). They are defined elaborately in (7), (8), and (9), respectively.

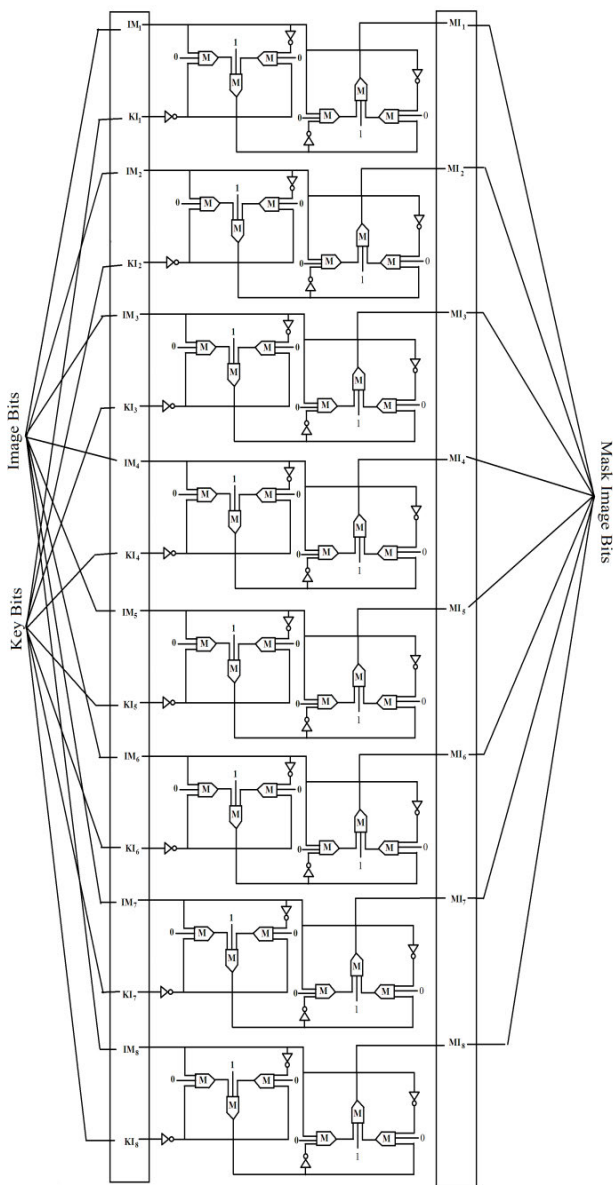
$$l(a, b) = \frac{(2\rho_a\rho_b + \gamma_1)}{(\rho_a^2 + \rho_b^2 + \gamma_1)} \quad (7)$$

$$c(a, b) = \frac{(2\beta_a\beta_b + \alpha_2)}{(\beta_a^2 + \beta_b^2 + \alpha_2)} \quad (8)$$

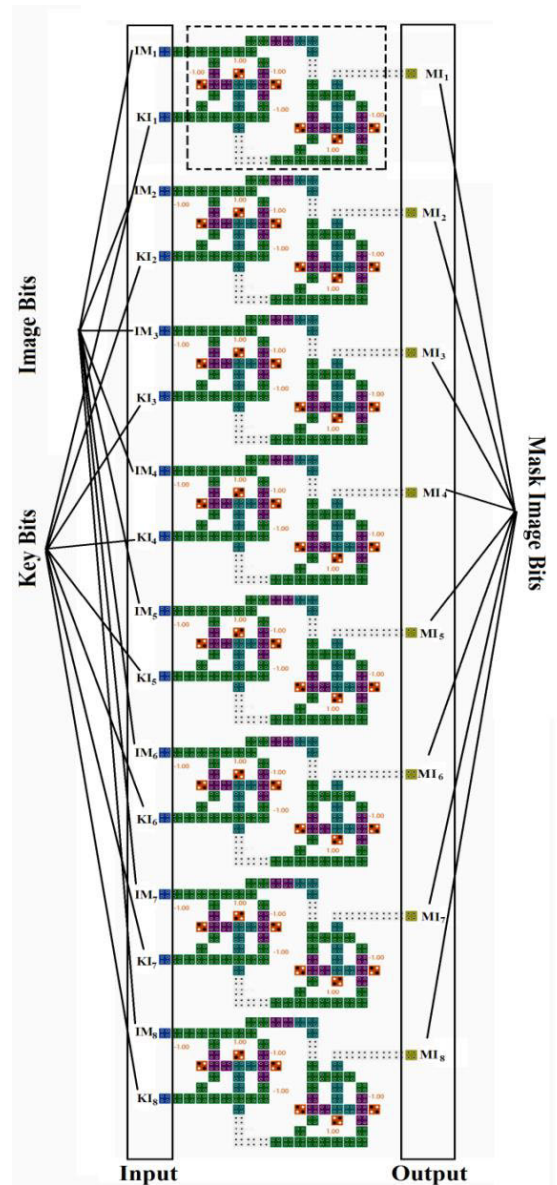
$$s(a, b) = \frac{(\beta_{ab} + \gamma_3)}{(\beta_a\beta_b + \gamma_3)} \quad (9)$$

Image bit (IM_i)								Key bit (KI_i)								Cipher Bit								Mask Bit (MI_i)							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
0	0	1	0	1	1	1	0	1	1	0	1	0	0	0	0	1	1	1	1	1	1	1	0	1	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	1	0	0	0	1	1	0	0	0	0	0	0	1
0	0	1	1	0	0	0	1	1	1	0	1	0	0	0	1	1	1	1	0	0	0	0	0	1	1	0	1	0	0	0	1
0	0	1	1	0	0	0	0	1	0	1	0	1	0	1	1	1	1	0	1	1	0	1	1	1	0	1	0	1	0	1	1
.	
.	
0	0	1	0	1	1	1	0	0	0	1	0	0	0	0	0	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	0
0	0	1	0	1	1	1	0	1	0	1	1	0	1	0	0	0	1	0	0	0	0	0	1	1	0	1	1	0	1	0	0
0	0	1	0	1	1	1	0	0	0	1	0	1	1	0	0	0	1	1	0	0	0	1	0	0	0	1	0	1	1	0	0
0	0	1	0	1	1	0	1	1	1	1	0	0	0	1	1	0	0	1	1	1	1	1	0	1	1	1	0	0	0	1	1

(a)

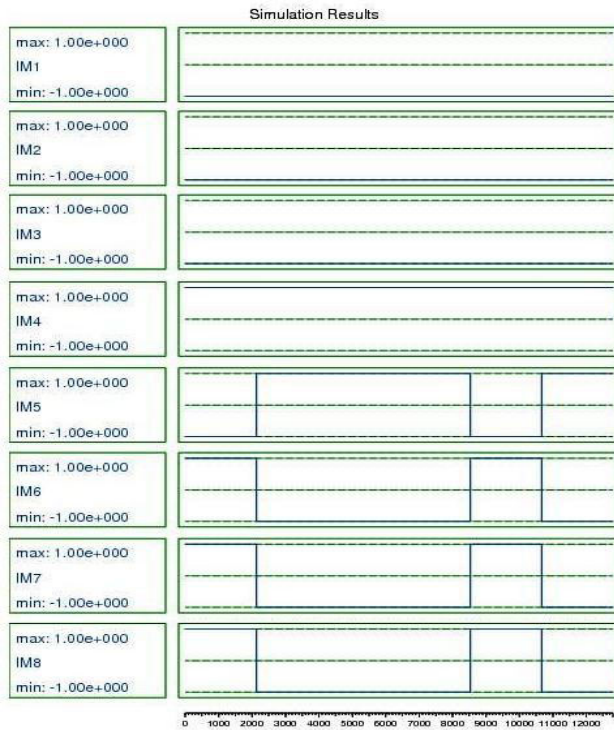


(b)

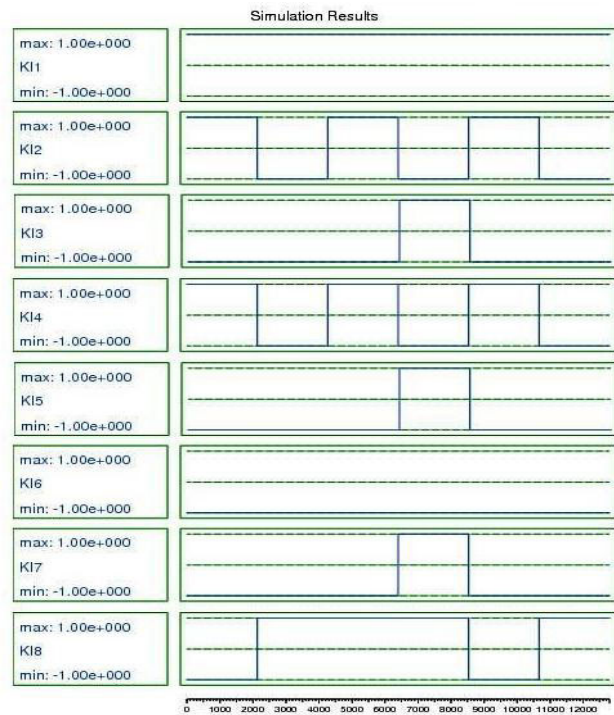


(c)

FIGURE 5. (a) Theoretical values for image masking, (b) Proposed encoder/ decoder, (c) Layout.



(a)



(b)

FIGURE 6. Proposed encoder/ decoder (a) Input image bits, (b) Input key bits provided to the proposed encoder/ decoder.

Here, $c_3 = 0.5c_2$. When $x = y = z = 1$, (6) is written as

$$SSIM(a, b) = [l(a, b)^x \cdot c(a, b)^y \cdot s(a, b)^z] \quad (10)$$

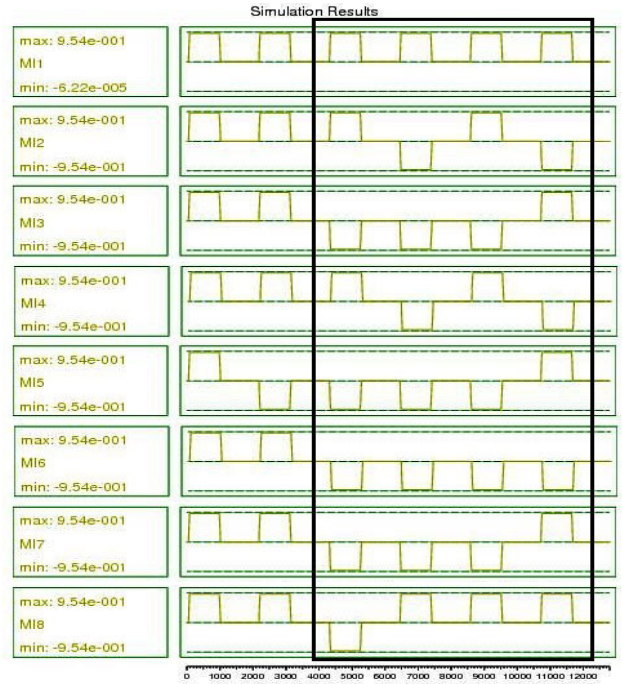


FIGURE 7. Output bits of proposed encoder/decoder.







Sample taken	1 st set of Input Image	Mask Image
1 st Sample	 child.jpg	 child_mask.jpg
2 nd Sample	 cloud.jpg	 cloud_mask.jpg
3 rd Sample	 clock.jpg	 clock_mask.jpg

FIGURE 8. Mask image “child_mask.jpg”, “cloud_mask.jpg”, “clock_mask.jpg” corresponding to the 1st set of input image “child.jpg”, “cloud.jpg” and “clock.jpg” respectively.






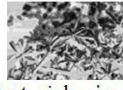
The dissimilarity is measured

$$DSSIM(a, b) = \frac{1 - SSIM(a, b)}{2} \quad (11)$$








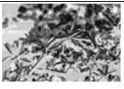

SSIM and DSSIM values represented in Fig. 10 of three different images “bird.jpg”, “balloon.jpg” and “plant.jpg”. SSIM presented in Fig. 10 are close to 1. The DSSIM measured also lies within the scale of 0.04 to 0.05, it proves the images are not degraded structurally, and the images obtained are innocent about the key.

C. SECURITY ANALYSIS

Security analysis [39]–[47] explores the vulnerability of any cryptographic or steganographic algorithm against different

Sample taken	2 nd set of Input Image	Cipher Image
1 st Sample	 bird.jpg	 bird_cipher.jpg
2 nd Sample	 balloon.jpg	 balloon_cipher.jpg
3 rd Sample	 plant.jpg	 plant_cipher.jpg

(a)

Sample Taken	Mask Image	Cipher Image	Image Received
1 st Sample	 child_mask.jpg	 bird_cipher.jpg	 bird.jpg
2 nd Sample	 cloud_mask.jpg	 balloon_cipher.jpg	 balloon.jpg
3 rd Sample	 clock_mask.jpg	 plant_cipher.jpg	 plant.jpg

(b)

FIGURE 9. Cipher image “bird_cipher.jpg”, “balloon_cipher.jpg” and “plant_cipher.jpg” corresponding to the 2nd set of input image “bird.jpg”, “balloon.jpg” and “plant.jpg” respectively. (b) Retrieval of the 2nd set of original image “bird.jpg”, “balloon.jpg” and “plant.jpg” using mask image “child_mask.jpg”, “cloud_mask.jpg”, “clock_mask.jpg” and cipher image “bird_cipher.jpg”, “balloon_cipher.jpg” and “plant_cipher.jpg” respectively.




Input / Output Image	SSIM	DSSIM
 bird.jpg	0.8840	0.058
 balloon.jpg	0.9014	0.0493
 plant.jpg	0.91	0.045

FIGURE 10. SSIM and DSSIM of the Images (a) bird.jpg (b) balloon.jpg (c) plant.jpg.

types of attacks. Security analysis is shown against five major attacks (1) Brute force attack, (2) Dictionary attack, and (3) Side-channel attack (4) Known plain text attack (5) Differential attack. Any attack on the system occur at the decryption end, where the attackers guess the exact key to decode the cipher message. In this proposed algorithm, both the cipher message and key are the image and the mask image, respectively.

1) BRUTE FORCE ATTACK

All the possible keys form the essential space supported by the cryptographic system applied to get the actual message in this attack [48]. It is a fundamental and primitive approach. According to the proposed algorithm, the key at the decryption end is an image having a similar size of the input image and the cipher image. Thus the size is known to the attacker. Let the size of the key $m \times n$, where m and n are the rows and columns, respectively. As a test case, a gray scale image is considered. Every pixel in such an image is eight-bit and ranges from 0 to 255. The number of possible mask image supported by the system at decryption end is $256^{m \times n}$ or $2^{8 \times q}$ where $q = m \times n$. The proposed system is also capable of encrypting RGB image, and the number of possible mask images supported by the system at decryption end is $2^{24 \times q}$.

2) DICTIONARY ATTACK

A brute force attack is useful when the number of keys supported by the system is considerably low. On exploration of more advanced technologies brute force attack became ineffective. Dictionary attack [49] is an approach where the selective key is enlisted to perform the attack at the decryption end. Using combination of some common words in our daily life a pattern is formed. The dictionary attack stores those common words and tries to find that pattern to decrypt the message in an unauthentic approach. The proposed method uses randomly generated keys of key length higher than ten. Thus the mask image at the decryption end is also random, and the Dictionary attack is ineffective for this algorithm.

3) SIDE CHANNEL ATTACK

This attack is different from traditional attacks. Brute force attack and dictionary attack depend on the key, cipher image as well as input message. A side-channel attack [50] possesses some features which have a physical influence on the cryptographic circuit. This type of attack can be analyzed based on following:

- The system’s electromagnetic emission
- The time required by the system
- The amount of power consumption

The system planned in this paper is based on QCA. It has static power dissipation for different key lengths. Apart from this, QCA circuits are resistant to power analysis attacks [43]. Thus, the proposed method is secured from the power analysis attack.

4) KNOWN PLAINTEXT ATTACK

The known-plaintext attack (KPA) is an assault model for cryptanalysis where the adversary approaches both the plain-text and its ciphertext. It is utilized to uncover further mystery data, for example, secret keys and codebooks.

According to the proposed algorithm, the key at decryption end is an image of similar size to the input image and the cipher image. Thus the size is known to the attacker. The

TABLE 4. UACI and NPCR test.

Original image	Cipher image	New cipher image	NCPR	UACI
child.jpg	child_cipher.jpg	child_cipher_new.jpg	99.8	32.2
cloud.jpg	cloud_cipher.jpg	cloud_cipher_new.jpg	99.73	36.2
clock.jpg	clock_cipher.jpg	clock_cipher_new.jpg	98.9	41.64
bird.jpg	bird_cipher.jpg	bird_cipher_new.jpg	99.54	33.25
balloon.jpg	balloon_cipher.jpg	balloon_cipher_new.jpg	99.84	29.87
plant.jpg	plant_cipher.jpg	plant_cipher_new.jpg	99.9	31.4

TABLE 5. Design complexity.

Proposed QCA circuit	No of MVs	Cell count	Total area (μm^2)	Cell area (μm^2)	Area usage (%)	Latency (clock cycle)
Building Block (Fig.4(b))	6 MVs and 4 IVs	89	0.1	0.036	36	2.0
Encoder / Decoder (Fig.5(c))	48 MVs and 32 IVs	712	0.86	0.285	33.14	2.0

secret key is nothing but the mask image. The mask image at the decryption end is random. The possible mask image support by our algorithm is $2^{8 \times m \times n}$ (Gray scale image) or $2^{24 \times m \times n}$ (color image).

In this way, assailants cannot take essential data by encoding some already designed exceptional pictures. So, the proposed calculation heartily opposed this type of attack.

5) DIFFERENTIAL ATTACK

The cryptosystem should be very susceptible to small changes introduced to the initial picture in order to withstand the differential attack. From each 8×8 block of the input image randomly a pixel is chosen within which a bit is changed to obtain a new image specified in Fig. 9 and Fig. 10. It is performed to check the strength of the suggested algorithm against differential attack. Then encryption is done using the same key to obtain the corresponding new cipher image. In order to prove that the changed image is different from its initial image, two measures of quantities are introduced. The measure is performed between the cipher image obtained from the original image and the new cipher image obtained from the altered image. They are the number of changing pixel rate (NPCR) and unified average change intensity (UACI). NPCR shows the percentage of the difference between two pictures, $C1(p, q)$, the pixel values of 1st encrypted image and the encrypted images at location (p, q) . $D(p, q)$ is either 1 and 0 depends on the condition. The measures mentioned above are defined in (12) and (13) of distinct pixels. UACI measures the average difference of pixel intensities between two cipher images.

Let I be the original image and I_{New} is the altered version of the image, both images are of size $X \times Y$ and let $C(p, q)$

TABLE 6. Comparison of different encryption method with QCA based encryption.

Parameters	RSA	AES	DES	Proposed Architecture
Key length	2048 bits	18, 192 or 256 bits	56 bits	$2^{8 \times m \times n}$ (Greyscale image) $2^{24 \times m \times n}$ (Color image) Same
Encryption and decryption key	Different	Same	Same	Same
Algorithm type	Asymmetric	Symmetric	Symmetric	Symmetric
Encryption and decryption algorithm	Same	Different	Different	
Encryption process	Slower	Faster	Moderate	Faster
Decryption process	Slower	Faster	Moderate	Faster
Simulation speed	Faster	Faster	Faster	Faster
Power consumption	High	Low	Low	Very low
Security	Least secure	Highly secure	Adequate	Highly secure
Brute force attack	Possible	Possible	Possible	Hard to achieve
Linear and differential attack	Hard to achieve	Hard to achieve	Possible	Hard to achieve
Data dictionary attack	Hard to achieve	Hard to achieve	Hard to achieve	Hard to achieve
Power analysis attack	Possible	Possible	Possible	Not possible
Scalability	Not scalable	Not scalable	Scalable	Scalable

and

$$NPCR = \frac{\sum_{p=1}^X \sum_{q=1}^Y D(p, q)}{XY} \times 100\% \quad (12)$$

$$\text{where, } D(p, q) = \begin{cases} 1, & \text{if } C(p, q) \neq C1(p, q) \\ 0, & \text{otherwise} \end{cases}$$

$$UACI = \sum_{p=1}^X \sum_{q=1}^Y \left[\frac{|C(p, q) - C1(p, q)|}{255} \right] \times \frac{100\%}{X \times Y} \quad (13)$$

TABLE 7. Comparison of the different QCA architecture with the proposed architecture.

QCA architecture	# QCA cell	Area	Latency (clock cycle)
Circuit Switched Network [30]	382	1.02	1.75
Nanocommunication Network [29]	679	1.03	3.75
Reversible cryptographic Nanocommunication Circuit [28]	100	0.103	2.75
Reversible User Authenticator [27]	84	0.091	0.75
Steganographic system [26]	483	0.335	2.5
Linear transform function for serpent block cipher [24]	154	0.179	3.0
A5/1 stream cipher (Register 1) [23]	1589	3.24	3.0
A5/1 stream cipher (Register 2) [23]	1503	2.664	2.25
A5/1 stream cipher (Register 3) [23]	1721	2.664	2.75
Cipher Text generator [22]	109	0.223	1.5
Correlation-Convolution Circuit [21]	208	0.245	1.25
Image Negation Circuit[19]	No QCA implementation		
Image Thresholding Circuit [18]	220	0.376	2.25
5-bit median filter [17]	Not reported	0.114	Not reported
Image steganographic architecture [33]	744	0.889	2.0
Proposed	712	0.86	2.0

The maximum value of NPCR is 100% to create an almost perfect picture encryption algorithm and UACI values must be around 33% [44]. Table 4 shows the values of NPCR and UACI of the images, as shown in Fig. 3. In most of the cases, the NPCR value is above 99.5%, clearly showing that the positions of the pixels have changed randomly—besides, the UACI. Values acquired are within an acceptable range [51]. Thus, it is concluded that the proposed scheme can prevent the differential attack.

In our proposed work, we have tried to implement image masking architecture on the QCA platform for the first time. Thus we have considered regular XOR operation to perform image masking. It is noted that the key is itself the mask image and open to the network. Thus, when an adversary steals both the information from the public channels, the security issue will be the matter. The secret key in the proposed algorithm is the mask image. The mask image at the decryption end is random. Both of the algorithms support the possible size of mask image is $2^{8 \times m \times n}$ for gray scale image or $2^{24 \times m \times n}$ for RGB color image. Thus, $2^{8 \times m \times n}$ or $2^{24 \times m \times n}$ number of

TABLE 8. Fault description.

Test vector	Fault coverage (%)
Single fault	
00	50
01	50
Multiple faults	
00	50
01	50
Overall	
00	50
01	50

TABLE 9. Fault coverage.

I/O	Fault Category	Test Vector	Valid Code	Invalid Code
Single Fault				
IM ₁	s-a-0	Fault free		
	s-a-1	Fault free		
KI ₁	s-a-0	01	1	0
	s-a-1	00	0	1
MI ₁	s-a-0	01	1	0
	s-a-1	00	0	1
Multiple Fault				
IK ₁	s-a-0	01	1	0
	s-a-1	00	0	1

attempts is required to decrypt the key information. Besides, the size of the mask image and cipher image is the same. So, it adds confusion to the adversary about which image the adversary will analyze first to achieve the key information, as both are the same size and are in encrypted form.

D. COMPLEXITY OF THE DESIGN

The design complexity of the proposed circuitry represented in Table 5. It is observed from the Table that proposed The Encoder or Decoder is made up of 712 cells and space occupied by it is $0.86 \mu\text{m}^2$ area whereas the latency is 2.0

E. QCA BASED ENCRYPTION VERSUS TRADITIONAL ENCRYPTION

Comparison of proposed QCA based encryption with other well-known schemes like Rivest–Shamir–Adleman(RSA), Advanced Encryption Standard (AES), Data Encryption Standard (DES) has been performed in Table 6, which describes that the QCA based encryption are faster, easier, and more secure against many well-known attacks than the traditional approaches.

F. PROPOSED QCA ARCHITECTURE AND EXISTING

The comparison of proposed security architecture with other state-of-the-art designs performed in this section. The result is explored in Table 7, which describes that the proposed QCA

TABLE 10. PD (meV) OF XOR GATE AT $\gamma = 0.25E_k$.

IP	$MV1$	HD	PD	$MV2$	HD	PD	$INV1$	HD	PD	$INV2$	HD	PD	$MV3$	HD	PD	Total PD
00	001	1	2.3	011	2	25.3	0	0	0.8	0	0	0.8	101	1	2.3	31.5
01	000	1	2.3	010	2	25.3	0	0	0.8	1	1	28.4	100	1	2.3	59.1
10	011	1	2.3	001	2	25.3	1	1	28.4	0	1	28.4	110	0	0.8	85.2
11	010	1	2.3	000	2	25.3	1	0	0.8	1	1	28.4	100	2	25.3	82.1

TABLE 11. PD (meV) for proposed circuits.

Proposed QCA circuit	Dissipation of power (meV)				
		$\gamma=0.25E_k$	$\gamma=0.5E_k$	$\gamma=0.75E_k$	$\gamma=1.0E_k$
Building Block (Fig. 4(b))	Max	170.4	181.2	197.4	216.2
	Min	63	80.4	104	130.8
	Avg	128.95	142.6	162.05	184.35
Encoder/ Decoder (Fig. 5(c))	Max	1363.2	1449.6	1579.2	1729.6
	Min	504	643.2	832	1046.4
	Avg	1031.6	1140.8	1296.4	1474.8

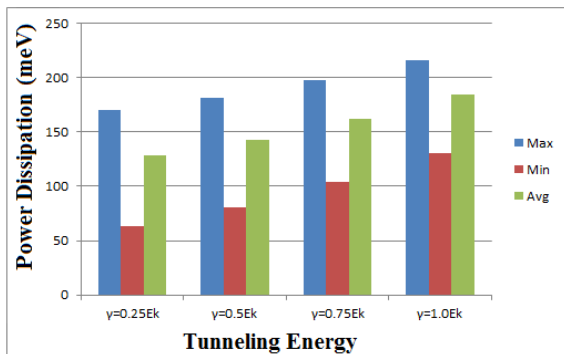


FIGURE 11. PD of building block at different γ .

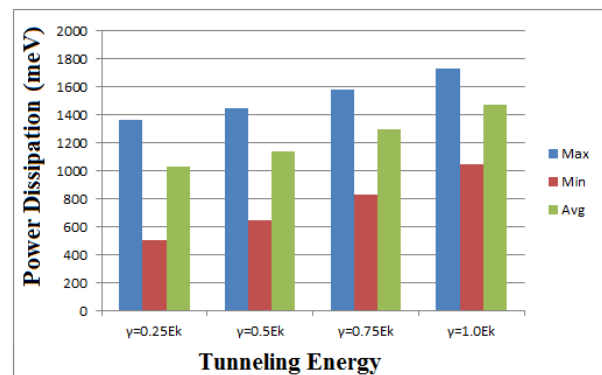


FIGURE 12. PD of encoder/decoder layout at different γ .

architecture requires lower cell count, area, and latency over some existing security architectures.

G. STUCK AT FAULT

This section demonstrates the effect caused by the stuck-at-fault on the building block of the designed encoder/decoder circuit, as given in Fig. 4(b). The result explored in Table 8 represent that when the input IM_1 fall in either “s-a-0”, stuck-at-zero or “s-a-1”, stuck-at-one, the result is fault-free. If input KI_1 fall in “s-a-0”, the result is “0” for input “01”. It is a faulty output. The correct output is “1”. So, for input “01”, the correct output and the faulty output can be compared to identify the fault at KI_1 for “s-a-0”. In such a case, <00> will be the test vector. However, when input KI_1 falls in s-a-1, the result is “1” for input “00”, it is the faulty output. The correct output is “0”. So, for input “00”, the correct output and the faulty output can be compared to identify

the fault at KI_1 for “s-a-1”. In such a case, <00> will be the test vector; the faults on the building block (Fig. 4(b)) of the proposed encoder/decoder circuit are analyzed and excelled in Table 9 ensuing similar approach. The same technique used to perform the fault analysis for the encoder/decoder circuit.

Table 9 illustrates both <00> and <01> are able to achieve 50% fault coverage during single input/output stuck-at-fault. Thus, in combination <00, 01> are enough to carry 100% fault exposure for both types of faults.

H. POWER DISSIPATION

The estimation of the amount of power dissipation (PD) is explored in this section. Hamming distance (HD) for each MV, as well as IVs [52] is used to compute the amount of power dissipation. The estimation is performed on different tunneling energy levels. For example, each of the XOR circuit (Fig. 4(b)) has 3 MVs and 2 IVs. Thus, based on

inputs, the HD for each MV and IV is calculated, as shown in Table 10. The corresponding PD of each MV and IV at $\gamma = 0.25E_k$ [52] is shown in Table 10. Finally, using those values, the total PD of the XOR gate at $\gamma = 0.25E_k$ has been estimated. The PD of the proposed encoder circuit and its building block is calculated. The results are displayed in Table 11. γ denotes the potential tunneling level, and E_k represents Kink energy. The graphical representation of the result is explored in Fig. 11, and Fig. 12.

VI. CONCLUSION

A detailed design approach on the encoder circuit is used to obtain a mask image. The same circuit can function as decoder. The mask image fetches the hidden knowledge of another cipher image to reconstruct the original image back, even in the absence of the secret key. QCA technology is used to build the proposed circuit, which acknowledges the circuit is nano-scale in size and employs meager power. The dissipated power of the circuit is verified to be low. The perfection of the circuit is verified as the experimental results are in relevance with the theoretical values. The system is secured, is justified by performing state-of-art security analysis. The SSIM based evaluation exhibits the precision of the proposed method. The stuck-at-fault analysis is performed to reveal the perfection of the circuit. In future, the proposed method can be modified for color images. A color image will be segregated into red, green and blue channels. So in order to perform mask operation for color image, the proposed encoder/decoder will be modified to process each of those red, green and blue channels. Thus the cost for color image masking will be increased by three times compared to the present. To function it as a practical system, in future, the architecture will be upgraded to work with QR code.

REFERENCES

- [1] H. Cho and E. E. Swartzlander, "Adder designs and analyses for quantum-dot cellular automata," *IEEE Trans. Nanotechnol.*, vol. 6, no. 3, pp. 374–383, May 2007.
- [2] P. D. Tougaw and C. S. Lent, "Logical devices implemented using quantum cellular automata," *J. Appl. Phys.*, vol. 75, no. 3, pp. 1818–1825, Feb. 1994.
- [3] S. Babaie, A. Sadoghifar, and A. N. Bahar, "Design of an efficient multi-layer arithmetic logic unit in quantum-dot cellular automata (QCA)," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 6, pp. 963–967, Jun. 2019.
- [4] M. Zhang, L. Cai, X. Yang, H. Cui, and C. Feng, "Design and simulation of turbo encoder in quantum-dot cellular automata," *IEEE Trans. Nanotechnol.*, vol. 14, no. 5, pp. 820–829, Sep. 2015.
- [5] D. Abedi, G. Jaberipur, and M. Sangsefidi, "Coplanar full adder in quantum-dot cellular automata via clock-zone-based crossover," *IEEE Trans. Nanotechnol.*, vol. 14, no. 3, pp. 497–504, May 2015.
- [6] S. M. Mohaghegh, R. Sabbaghi-Nadooshan, and M. Mohammadi, "Innovative model for ternary QCA gates," *IET Circuits, Devices Syst.*, vol. 12, no. 2, pp. 189–195, Mar. 2018.
- [7] T. N. Sasamal, A. K. Singh, and U. Ghanekar, "Efficient design of coplanar ripple carry adder in QCA," *IET Circuits, Devices Syst.*, vol. 12, no. 5, pp. 594–605, Sep. 2018.
- [8] J. C. Das, D. De, S. P. Mondal, A. Ahmadian, F. Ghaemi, and N. Senu, "QCA based error detection circuit for nano communication network," *IEEE Access*, vol. 7, pp. 67355–67366, 2019.
- [9] G. Singh, B. Raj, and R. K. Sarin, "Fault-tolerant design and analysis of QCA-based circuits," *IET Circuits, Devices Syst.*, vol. 12, no. 5, pp. 638–644, Sep. 2018.
- [10] T. J. Dysart, "Modeling of electrostatic QCA wires," *IEEE Trans. Nanotechnol.*, vol. 12, no. 4, pp. 553–560, Jul. 2013.
- [11] S. Perri, P. Corsonello, and G. Cocorullo, "Area-delay efficient binary adders in QCA," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 22, no. 5, pp. 1174–1179, May 2014.
- [12] V. Pudi and K. Sridharan, "A bit-serial pipelined architecture for high-performance DHT computation in quantum-dot cellular automata," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 23, no. 10, pp. 2352–2356, Oct. 2015.
- [13] M. Vacca, J. Wang, M. Graziano, M. R. Roch, and M. Zamboni, "Feedbacks in QCA: A quantitative approach," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 23, no. 10, pp. 2224–2233, Oct. 2015.
- [14] J. F. Chaves, M. A. Ribeiro, L. M. Silva, L. M. B. C. de Assis, M. S. Torres, and O. P. V. Neto, "Energy efficient QCA circuits design: Simulating and analyzing partially reversible pipelines," *J. Comput. Electron.*, vol. 17, no. 1, pp. 479–489, Mar. 2018.
- [15] M. Tahmasebi, R. Faghieh Mirzaee, and S. H. P. Komleh, "On the design methodology of Boolean functions with quantum-dot cellular automata for reducing delay and number of wire crossings," *J. Comput. Electron.*, vol. 17, no. 4, pp. 1756–1770, Dec. 2018.
- [16] R. K. Nath, B. Sen, and B. K. Sikdar, "Optimal synthesis of QCA logic circuit eliminating wire-crossings," *IET Circuits, Devices Syst.*, vol. 11, no. 3, pp. 201–208, May 2017.
- [17] J. L. Cardenas-Barrera, K. N. Plataniotis, and A. N. Venetsanopoulos, "QCA implementation of a multichannel filter for image processing," *Math. Problems Eng.*, vol. 8, no. 1, pp. 87–99, 2002.
- [18] A. S. Anand, T. Adak, and B. K. Sikdar, "Thresholding using quantum-dot cellular automata," in *Proc. Int. Conf. Innov. Inf. Technol. (IIT)*, Abu Dhabi, United Arab Emirates, Apr. 2011, pp. 356–360.
- [19] P. J. Suganiya and J. A. E. J. Ferdin, "A novel structure for image negative using quantum cellular automata adder," *Int. J. Eng. Res. Technol.*, vol. 3, no. 7, pp. 84–88, 2014.
- [20] F. K. Panagiotopoulos, V. A. Mardiris, and V. Chatzis, "Quantum-dot cellular automata design for median filtering and mathematical morphology operations on binary images," in *Proc. Int. Conf. Cellular Automata*. Berlin, Germany: Springer, 2012, pp. 554–564.
- [21] B. Debnath, J. C. Das, and D. De, "Correlation and convolution for binary image filter using QCA," *Nanomaterials Energy*, vol. 5, no. 1, pp. 61–70, Jun. 2016.
- [22] J. C. Das and D. De, "Quantum dot-cellular automata based cipher text design for nano-communication," in *Proc. Int. Conf. Radar, Commun. Comput. (ICRCC)*. Tamilnadu, India: SKPEngg. College, Dec. 2012, pp. 343–348.
- [23] M. A. Amiri, M. Mahdavi, and S. Mirzakuchaki, "QCA implementation of A5/1 stream cipher," in *Proc. 2nd Int. Conf. Adv. Circuits, Electron. Micro-electronics*, Sliema, Malta, Oct. 2009, pp. 48–55.
- [24] M. A. Amiri, M. Mahdavi, R. E. Atani, and S. Mirzakuchaki, "QCA implementation of serpent block cipher," in *Proc. 2nd Int. Conf. Adv. Circuits. Electron. Micro-Electron.*, Sliema, Malta, 2009, pp. 16–19.
- [25] J. C. Das, B. Debnath, and D. De, "Image steganography using quantum dot-cellular automata," *Quantum Matter*, vol. 4, no. 5, pp. 504–517, Oct. 2015.
- [26] B. Debnath, J. C. Das, and D. De, "Reversible logic-based image steganography using quantum dot cellular automata for secure nanocommunication," *IET Circuits, Devices Syst.*, vol. 11, no. 1, pp. 58–67, Jan. 2017.
- [27] J. C. Das and D. De, "User authentication based on quantum-dot cellular automata using reversible logic for secure nanocommunication," *Arabian J. for Sci. Eng.*, vol. 41, no. 3, pp. 773–784, Mar. 2016.
- [28] J. C. Das, B. Debnath, and D. De, "Reversible gate-based cipher text using QCA for nanocommunication," *Nanomaterials Energy*, vol. 6, no. 1, pp. 7–16, Jun. 2017.
- [29] J. C. Das and D. De, "Nanocommunication network design using QCA reversible crossbar switch," *Nano Commun. Netw.*, vol. 13, pp. 20–33, Sep. 2017.
- [30] J. C. Das and D. De, "Circuit switching with quantum-dot cellular automata," *Nano Commun. Netw.*, vol. 14, pp. 16–28, Dec. 2017.
- [31] B. Debnath, J. C. Das, D. De, and T. Ghosh, "Image masking using quantum-dot cellular automata," in *Proc. 3rd Int. Conf. Devices, Circuits Syst. (ICDCS)*, Coimbatore, India, Mar. 2016, pp. 231–235.

- [32] L. Sui, X. Zhang, and A. Tian, "Multiple-image hiding based on cascaded free-space wave propagation using the structured phase mask for lensless optical security system," *IEEE Photon. J.*, vol. 9, no. 5, pp. 1–14, Oct. 2017.
- [33] A. Journault and F. X. Standaert, "Very high order masking: Efficient implementation and security evaluation," in *Proc. Int. Conf. Cryptograph Hardw. Embedded Syst.* Cham, Switzerland: Springer, 2017, pp. 623–643.
- [34] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos," *Multimedia Tools Appl.*, vol. 74, no. 3, pp. 781–811, Feb. 2015.
- [35] W. Wang, F. X. Standaert, Y. Yu, S. Pu, J. Liu, Z. Guo, and D. Gu, "Inner product masking for bitslice ciphers and security order amplification for linear leakages," in *Proc. Int. Conf. Smart Card Res. Adv. Appl.* Cannes, France: Springer, 2016, pp. 174–191.
- [36] M.-Y. Wu, M.-C. Yu, J.-S. Leu, and S.-K. Chen, "Enhancing security and privacy of images on cloud by histogram shifting and secret sharing," *Multimedia Tools Appl.*, vol. 77, no. 13, pp. 17285–17305, Jul. 2018.
- [37] M. Khurana and H. Singh, "A spiral-phase rear mounted triple masking for secure optical image encryption based on gyrator transform," *Recent Patents Comput. Sci.*, vol. 12, no. 2, pp. 80–94, Feb. 2019.
- [38] N. Ghoshal, A. Sarkar, D. Chakraborty, S. Ghosh, and J. K. Mandal, "Masking based data hiding and image authentication technique (MDHIAT)," in *Proc. 16th Int. Conf. Adv. Comput. Commun.*, Chennai, India, Dec. 2008, pp. 119–122.
- [39] J. O. Kim, K. S. Seo, C. H. Chung, J. Hwang, and W. Lee, "On facial expression recognition using the virtual image masking for a security system," in *Proc. Int. Conf. Comput. Sci. Appl.* Berlin, Germany: Springer, 2004, pp. 655–662.
- [40] J. Chen, Y. Zhang, J. Li, and L.-B. Zhang, "Security enhancement of double random phase encoding using rear-mounted phase masking," *Opt. Lasers Eng.*, vol. 101, pp. 51–59, Feb. 2018.
- [41] J. Balasch, S. Faust, B. Gierlichs, C. Paglialonga, and F.-X. Standaert, "Consolidating inner product masking," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Hong Kong. Cham, Switzerland: Springer, 2017, pp. 724–754.
- [42] H. S. Yaragunti, M. Ashok, and T. B. Reddy, "Image masking and compressing using bit shifting," *Global J. Comput. Technol.*, vol. 2, no. 1, pp. 66–74, 2015.
- [43] K. Walus, T. J. Dysart, G. A. Jullien, and R. A. Budiman, "QCADesigner: A rapid design and simulation tool for quantum-dot cellular automata," *IEEE Trans. Nanotechnol.*, vol. 3, no. 1, pp. 26–31, Mar. 2004.
- [44] B. Debnath, J. C. Das, and D. De, "Design of image steganographic architecture using quantum-dot cellular automata for secure nanocommunication networks," *Nano Commun. Netw.*, vol. 15, pp. 41–58, Mar. 2018.
- [45] E. Biham and A. Shamir, "Differential cryptanalysis of Des-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, Jan. 1991.
- [46] A. Bogdanov and V. Rijmen, "Linear hulls with correlation zero and linear cryptanalysis of block ciphers," *Designs, Codes Cryptography*, vol. 70, no. 3, pp. 369–383, Mar. 2014.
- [47] N. K. Nishchal, "Optical security keys/masks," in *Optical Cryptosystems*. Bristol, U.K.: IOP, 2019. [Online]. Available: <https://iopscience.iop.org/book/978-0-7503-2220-1>
- [48] J.-S. Cho, Y.-S. Jeong, and S. O. Park, "Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol," *Comput. Math. Appl.*, vol. 69, no. 1, pp. 58–65, Jan. 2015.
- [49] D. Wang and P. Wang, "Offline dictionary attack on password authentication schemes using smart cards," in *Proc. 16th Int. Conf. Inf. Secur. (ISC)*, vol. 7807, Nov. 2013, pp. 221–237, doi: 10.1007/978-3-319-27659-5_16.
- [50] T. Hisakado and N. Yamashita, "Device for evaluating side-channel attack resistance, method for evaluating side-channel attack resistance, and program for evaluating side-channel attack," U.S. Patent 8 848 903, Sep. 30, 2014.
- [51] M. Preishuber, T. Hutter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2137–2150, Sep. 2018.
- [52] W. Liu, S. Srivastava, L. Lu, M. O'Neill, and E. E. Swartzlander, "Are QCA cryptographic circuits resistant to power analysis attack?" *IEEE Trans. Nanotechnol.*, vol. 11, no. 6, pp. 1239–1251, Nov. 2012.



BIKASH DEBNATH received the M.Tech. degree in software engineering from the West Bengal University of Technology, West Bengal, India, in 2012. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Swami Vivekananda Institute of Science and Technology under West Bengal University of Technology, Kolkata, India. He has more than ten publications with more than six SCI journal publications. His research interests include

image processing, steganography, and QCA based image processing and nanocommunication. He received the IET Premium Award for Best Journal Paper in *IET Circuits Devices & Systems* journal in 2018.



JADAV CHANDRA DAS received the M.Tech. degree in multimedia and software systems and the Ph.D. degree in computer science and engineering (nanotechnology) from the West Bengal University of Technology, West Bengal, India, in 2011 and 2019, respectively. He is currently an Assistant Professor with the Department of Information Technology, Maulana Abul Kalam Azad University of Technology, Haringhata, West Bengal. He has ten years of teaching experiences and

has eight years of research experience during which he has published more than 50 research articles in peer-reviewed journals and conferences. He has more than 30 SCI journal publications. He received many prestigious honors for best paper publication in SCI journal. He has good scholarly records. He received the IET Premium Award for Best Journal Paper in *IET Circuits Devices & Systems* journal in 2018 and the J. C. Bose Memorial Award for Best Journal Paper in *IETE* journal of Research in 2016. He has more than 40 publications with more than 25 SCI journal publications. His research interests include cryptography, steganography, QCA based image processing, reversible logic design with QCA, and nano-communication network design.



DEBASHIS DE (Senior Member, IEEE) received the M.Tech. degree in radio physics and electronics in 2002 and the Ph.D. degree in engineering from Jadavpur University, in 2005. He worked as a Research and Development Engineer of Teletronics. He is currently a Professor with the Department of Computer Science and Engineering, West Bengal University of Technology, India, and also an Adjunct Research Fellow with the University of Western Australia, Australia. His research inter-

ests include location management and power consumption control in mobile network and low power nano device design for mobile application and disaster management. He was awarded the prestigious Boyscast Fellowship by the Department of Science and Technology, Government of India to work at Herriot-Watt University, U.K. He is also awarded Endeavour Fellowship Award from 2008 to 2009 by DEST Australia to work in the University of Western Australia. He received Young Scientist award both in 2005 at New Delhi and in 2011 at Istanbul by International Union of Radio Science, H.Q., Belgium.

SANKAR PRASAD MONDAL, photograph and biography not available at the time of publication.



ALI AHMADIAN (Member, IEEE) received the Ph.D. degree, as the best postgraduate student, from Universiti Putra Malaysia (UPM), in 2014. He is currently a Fellow Researcher with the Institute of Industry Revolution 4.0, UKM. As a Young Researcher, he is dedicated to research in applied mathematics. In general, his primary mathematical focus is the development of computational methods and models for problems arising in AI, biology, physics, and engineering under fuzzy and

fractional calculus (FC); in this context, he worked on projects related to drug delivery systems, acid hydrolysis in palm oil frond, and carbon nanotubes dynamics, Bloch equations, and viscosity. He could successfully receive 13 national and international research grants and selected as the 1% top reviewer in the fields of mathematics and computer sciences recognized by Publons from 2017 to 2019. He is a member of editorial board in *Progress in Fractional Differentiation and Applications* (Natural Sciences Publishing) and a Guest Editor in *Advances in Mechanical Engineering* (SAGE), *Symmetry* (MDPI), *Frontier in Physics* (Frontiers), and the *International Journal of Hybrid Intelligence* (Inderscience Publishers). He has authored more than 70 research articles published in the reputed journals including the IEEE TRANSACTIONS ON FUZZY SYSTEMS, *Fuzzy Sets and Systems*, *Communications in Nonlinear Sciences and Numerical Simulations*, and *Computational Physics*. He also presented his research works in 38 international conferences held in Canada, Serbia, China, Turkey, Malaysia, and United Arab Emirates. He was a member of programme committee in a number of international conferences in fuzzy field at Japan, China, Turkey, South Korea, and Malaysia. He is also serving as a referee in more than 80 reputed international journals.



MEHDI SALIMI received the master's degree in pure mathematics in Tehran, Iran, in 2006, and the Ph.D. degree in applied mathematics (game theory) from Universiti Putra Malaysia (UPM), in 2011. He was also a Postdoctoral Fellow with the Center for Dynamics (CfD), Dresden University of Technology, Germany, and finished the position in January 2015. Then, he moved to the MEDALics—Research Centre of the University "Dante Alighieri," Reggio Calabria, Italy, for

another postdoctoral position and he finished the position in August 2015. He was a Visiting Professor with the Dresden University of Technology, Germany, and the University Mediterranea of Reggio Calabria, Italy, from 2017 to 2019. He is currently a member of the Center for Dynamics, Department of Mathematics, Technische Universität Dresden, Germany. He has published several articles. His research interests include game theory, pursuit-evasion differential games, data science, data analysis, machine learning, and numerical analysis.



MASSIMILIANO FERRARA received the master's degree (*cum laude*) in economics and the Ph.D. degree (*cum laude*) from the University of Messina, and the two master's degree (*cum laude*) from the University of Naples Federico II and Scuola Normale Superiore di Pisa. He was the General Counsel of Fondazione Banco di Napoli, a Vice Rector at University for foreigners "Dante Alighieri" of Reggio Calabria, and the Head of the Regione Calabria Department for Cultura,

Research and Education. He was a Visiting Professor with Harvard University, Cambridge (USA), Western Michigan University (USA), Morgan State University, Baltimore (USA), Northeastern University di Boston (USA), and recently at the Center for Dynamics, Dresden University of Technology, Germany. He has been a Research Affiliate with the Invernizzi Center for Research on Innovation, Organization, Strategy and Entrepreneurship (ICRIOS), University Bocconi of Milan, since 2013, also the President of the Scientific Committee of MEDALics research Centre, and also the Scientific Director of the DECISIONS Lab. He is currently a Full Professor of mathematical economics, statistics, business analytics and decision theory, applied economics with the Mediterranean University of Reggio Calabria, where he is also the Chairman of the Department of Law, Economics and Human Sciences and also a member of the Academic Senate. He has authored and coauthored upto 200 articles on peer-review and ISI journal and ten research monographs.

He has been a Knight Order of Merit of the Italian Republic since 2010 "for international scientific merits." He is in the prestigious U.S. Encyclopedia Hmolpedia on thermodynamics and the theoretical and applied physics, for offering a decisive contribution to the creation and development of the scientific theory called "Economic Geometric Dynamics." He is an editor, a co-editor, an associate editor, and a referee of reputable international scientific journal in economics, pure and applied mathematics.

• • •