A Hybrid Approach to Steganography System Based on Quantum Encryption and Chaos Algorithm

Zaid A. Abod
College of Food Science, Al-Qasim Green University, Babil, Iraq
zaid.auw@gmail.com

Abstract

This paper proposes a hybrid system for secretly embedding images into the dithered multilevel image. Confident hybridizations between steganography and quantum encryptions are either rare in literature or suffer a poor effectiveness in secure communication. This paper scrambles and divides the secret image into groups to be embedded in the blocks of the cover image using three chaos algorithms. These are Lorenz map, Henon map, and Logistic map algorithms. The encryption of embedded images conducted using the quantum one-time pad. Results showed that the proposed hybrid system succeeded in embedding and combining images with quantum cryptography algorithms.

Keywords: Least Significant Bit, Image Steganography, Steganography, Quantum Cryptography, Quantum One Time-Pad, Chaotic Maps.

الخلاصة

أستخدام في هذا البحث طريقة هجينه لاخفاء صورة في صورة متعددة المستويات متدرجة. يعتبر جمع علم الاخفاء مع تقنيات التشفير الكمي من العلوم الحديثة والنادرة في وقتنا الحالي وذلك لاعتماده بصورة اساسية على قوانين الكم والتي توفر امنية عالية لقنوات الاتصال. في هذا البحث المدخلات ستكون الصورة المراد اخفائها "الصورة السرية" بالاضافة الى الصورة التي سيتم الأخفاء فيها, بالأعتماد على المفاتيح الفوضويه سيتم اخفاء صوره سريه "secret image" في صوره اخرى "cover image" حيث سيتم بعدها بعثرة بتات الصورة السرية بأستخدام طريقه هجينه من الدوال الفوضية (Lorenz Map and Henon Map) ويتم بعدها تقسيم البتات الناتجه الى مجاميع وسيتم اخفاء هذه المجاميع بالصوره "cover image" بالأعتماد على الدالة الفوضية "logistic map", وأخيرا تشفير الصور الناتجه باستخدام واحدة من آليات التشفير الكم التي هي "quantum one time pad". وأظهرت النتائج التجريبية أن النظام الهجين المقترح نجح في أخفاء الصور والجمع بين خوارزميات التشفير الكمي ويعطي كفاءة عالية في الاتصالات الآمنة.

الكلمات المفتاحية : البت الأقل اهمية, الأخفاء الصوري, الأخفاء, التشفير الكمي, تشفير QOTP, الدوال الفوضوية.

I. Introduction

Information security becomes an important priority. Encryption and steganography are the two main ways to achieve secure communication. Steganography is the technique of invisible communication; it is achieved by hiding secret data inside a carrier file such as an image. The basic relationship between steganography and encryption is that while the encryption encrypts the plaintext to cipher text, steganography allows us to hide the cipher text itself. Therefore the combination of steganography and encryption increase the confidentiality, authenticity, non-repudiation, data security and integrity (Saini *et al.*, 2013). This paper harnessed the power of hybridization to present more effective, confident and more secure steganography systems.

II. Literature Review

There are many aspects proposed related to the combination of cryptography and steganography. Some of them are close to the idea of this paper. (Lifang Yu *et al.*, 2010) proposed an algorithm in the field of steganography for JPEG images based on chaos and genetic algorithm. In this method, improved adaptive Least significant bit (LSB) steganography are selected where the message order shuffle by chaos algorithm and the parameter by the genetic algorithm.(Sudha, K. L., 2012) presented a new method for hiding a secret message into an image using LSB insertion method along with chaos algorithm. (Singh et al., 2012) presented a steganographic method for secret sharing of information using discrete cosine transform and chaotic system. Arnold transforms to scramble the secret image and logistic map to generate random sequence. (Saini *et al.*, 2013) proposed two hybrid methods for image security. They have proceeded with an advanced encryption standard (AES) approach for encrypting an image. Then hide into cover image using steganography concept.

(Kumar *et al.,* 2014) introduced a new cryptography techniques named as chaos based encryption and decryption with the new steganography system based on LSB approach. The chaos based cryptography provides better security to data and the LSB approach increase the level of security in the system when combine with the chaos approach. (Devaraj *et al.,* 2017) presented steganography with non-linear riotous calculation (NCA) which utilizes control capacity and digression work rather than straight capacity. The message with the key is then consolidated with the cover image utilizing LSB installing and discrete cosine change. (Rajendran *et al.,* 2017) presented a new symmetric key based on image-hiding technique. Using one dimension logistic map generates pseudo random keys. Those keys are used for choosing the position of the cover image pixel randomly for hiding the secrete image and this is considered as the main security key point.

(Zaid *et al.,* 2017) the researchers developed the idea of combining the cryptography and steganography by using quantum cryptography and chaotic maps, which relies on quantum laws. The combination is a complete steganography system with the quantum cryptography based on Quantum One-Time Pad (QOTP) encryption and least significant bit (LSB) substitution adaptive steganography technology. In this work, encryption and steganography are hybrid systems. Quantum One Time Pad (QOTP) uses the law of quantum mechanics and applies multiple chaos algorithms, e.g. Lorenz map, Henon map and Logistic map. Then by multiple steps, the secret image is concealed into the cover image to provide secure communication.

III. Chaotic Maps

Chaos theory is a phenomenon that possess inevitable latency rule behind irregular appearance. This theory might be regarded as one of the most difficult nonlinear problem. The origin the theory began in physics, math, and developed into engineering. Math described the theory as ‘random’, as a result of the simple inevitable system influenced by the initial circumstances of chaotic Maps. Presently, there are considerable interests in the application of chaotic system and its importance in interdisciplinary fields like cryptographies, physics, chemistry, neurophysiologies, engineering, etc. Chaos possesses a lot of substantial features involving the deterministic, the sensitive, the irregular, the

properties of nonlinear and the long-term predictions. In the last decades, researches concentrated on the uses of Chaotic in cryptography in order to get characteristics for achieving the security of the system based on this phenomenon (Ismael, Hussein A., and Sattar B. Sadkhan 2017). The following subsections briefly introduce Standard maps and Lorenz Chaotic Maps, which have been utilized for the suggested system.

II.1 The Map of Lorenz (MZ)

It is one of the most well-known Chaotic Maps (Chirikov, Boris Valerianovich 1971). It appears in (1963) by Edward Lorenz. This theory is regarded as one of the simple models for atmospheric convections. It is a normal differential equation, a 3-Dimansional map that can be mathematically detailed: (Chirikov, Boris Valerianovich 1971).

$$\dot{x}\,(n) = \sigma(y(n) - x\,(n)) \tag{3}$$

$$\dot{y}\,(n) = rx(n) - y(n) - x(x)z(n) \tag{4}$$

$$\dot{z}\,(n) = x(n)y(n) - bz(n) \tag{5}$$

In which 'σ', 'r' and 'p' are parameters with constants values (10, 28, 8/3) respectively. Lorenz Map initial values are x (0) y (0) and z (0).

II.2 The Map of Henon (MH)

This Chaotic Map is a 2-D map. It appears in (1969) showing a chaotic behavior. The map is dynamic systems in an unattached time. It is utilized to generate two two equations or two Chaos-signals as follows: (O. Ozgur Aybar et al., 2017)

$$x_{n+1} = y_n + 1 - ax_n^2 \tag{6}$$

$$y_{n+1} = bx_n \tag{7}$$

Where 'a' is a parameter with value (1.4). The 'b' is a parameter with value (0.3). X_n is an initial value of equation within the period [2, -2].

II.3 Logistic Map (LM)

It discovered by the Pierre Verhulst in 1845 (Ramos and Romell Ambal 2013), Logistic map (also called Verhulst model). It is regarded as one of the most well-known chaotic maps and widely utilized in the applications. It is a one-dimensional unattached chaotic map leads to chaotic performances and generates a sequence of chaotic within the period [0, 1], mathematically, it is expressed as a follows:

$$X_{(m+1)} = r\,X_m\,(1 - X_m) \tag{8}$$

In which $'r'$ is a parameter within the period [0, 4], when 'r' follows period [$3.57 < r \leq 4$] becomes chaotic performances, X_m within the period [0, 1], when any slight changes happen in any of the initial variables $'X_0'$ or a parameter $'r'$ lead to the generations of many real values sequences that are irregular and random (Yicong Zhou, et al., 2015) (Ramos and Romell Ambal 2013).

IV. Steganography of Least Significant Bit

(LSB) the least significant bits substitutions are the simplest and well-known steganography method (Johnson et al., 1998). This method is utilized with audios and images in which it directly substitutes the least significant bits through embedding a message into the cover images or cover audios. For rising the hiding ability, it could be utilized up to four significant bit (one bit for each color Green, Red, Alpha and Blue color channels respectively) per pixel with images. In audios, the data embeds in the inactive frame of low bit rates audio stream. The known weak points are the values of the samples change asymmetrically. When the values of the LSB of the medium cover samples are equal to the message bits, no change is made. Otherwise, the value 2n is altered to 2n+1 or 2n+1 is changed to 2n (Swain et al., 2014). There is an improvement and modification has been suggested for strengthening these techniques, like adaptive technique that alters payload distributions depending on the features of images and audios. If the messages are encrypted first and then embedded, security levels will be amended (Swain *et al.*, 2014).

V. Quantum One-Time Pad

The encryption algorithms of "One-Time Pad" were created early and since then, they have been confirmed as unbreakable. The cipher texts are confirmed to be unbreakable when the "One-Time Pad" conditions are fulfilled where the "one-time pad" is carried out typically through the use of exclusive-or (XOR) additions for combining key elements with plaintext elements. The keys are completely random and they can be utilized one time only and this is the condition of the "one-time pad" to be unbreakable (Qaisar *et al.*, 2015).

The central problems in "One-Time Pad" are the distribution of keys. The key must be in the same length with the plaintexts among N users number. Traditional protocol of key distributions is unable to detect adversaries between two valid parties. Quantum key distributions (QKD) protocols solve these problems. The most well-known (QKD) protocol is BB84 (Bennett *et al.*, 2014). (QKD) security is assured by quantum laws. The quantum uncertain principles demonstrated in (Busch *et al.*, 2007) allow sharing the secret key securely among two valid parties.

"Quantum One-Time Pad" idea (QOTP) is given in (Boykin *et al.*, 2003). The protocols work through the transition of quantum particles from receivers to senders, where the senders embed their information and then from senders to the receivers where "Quantum One-Time Pad" is encryption schemes for qubits.

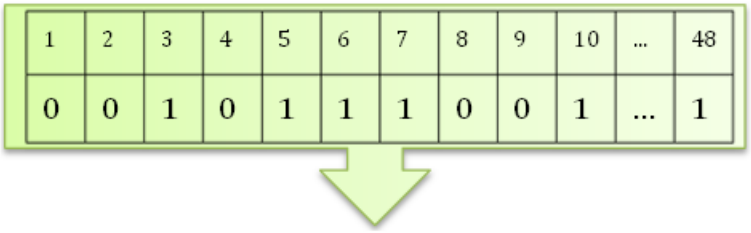
VI. Proposed Model

In this paper, we introduced a new model for two stages steganography: to secure and hide the secret image into the cover image using LSB algorithm, and secure mechanism: that uses quantum cryptography, prior to sending it via quantum communication channel. The following sections are represents the proposed models that include two main stages, steganography and encryption.

V.1 Sender Side

In the sender side the secret image is converted into binary bits, before embedding in the cover image. The chaotic Henon map HM and Lorenz map ZM is used for generating sequences pseudo random numbers that are used as the keys for scrambling of secret image bits. The output divided into groups each group has 48 bits. Furthermore, cover image divided into blocks where each block includes 7×7 pixels after save it in binary array. Then, compute the variance for each block to select the higher values where the number of blocks should equalize to the number of the groups as shown in figure 1.

Finally, use the Logistic chaotic map (LM) for selecting locations in the selected groups to embedded the secret image by using the least significant bit (LSB) substitution. For the encryption process, "Quantum One-Time Pad" algorithm has been used to encrypt the data of the image that already convert it to quantum bits (Qubits). The algorithm for the sender side is detailed as follows:



	1	2	3	4	5	6	7
1	Ind	Pixel 1 0	Pixel 2 1	Pixel 3 1	Pixel 4 0	Pixel 5 1	Pixel 6 1
2	Pixel 7 1	Pixel 8 0	Pixel 9 0	Pixel 10 1	Pixel 11 0	Pixel 12 1	Pixel 13 1
3	Pixel 14 0	Pixel 15 0	Pixel 16 0	Pixel 17 1	Pixel 18 0	Pixel 19 1	Pixel 20 1
4	Pixel 21 1	Pixel 22 1	Pixel 23 0	Pixel 24 1	Pixel 25 1	Pixel 26 0	Pixel 27 1
5	Pixel 28 0	Pixel 29 1	Pixel 30 0	Pixel 31 0	Pixel 32 1	Pixel 33 1	Pixel 34 0
6	Pixel 35 0	Pixel 36 1	Pixel 37 1	Pixel 38 0	Pixel 39 1	Pixel 40 1	Pixel 41 0
7	Pixel 42 1	Pixel 43 0	Pixel 44 1	Pixel 45 1	Pixel 46 0	Pixel 47 1	Pixel 8 0

Figure (1): Divide Image to non-overlaying blocks, each block 7*7 cells

Algorithm 1: The Sender Side Algorithm

Algorithm of Sender side
Input: Secret image, Cover image, Keys
Output: Qubits
Begin
Step 1: Call convert_to_binary (secret image).
Step 2: Call Encrypt (secret image) : by applying the chaotic maps using hybrid technique (Lorenz Map and Henon Map).
Step 3: Divide the array of cover image to non-overlaying blocks(7*7) cells.
Step 4: For each block in array of cover image do
- call variance (block $_i$)
End For
Step 5: Divide the encrypted array of secret image to groups of 48 bits.
Step 6: number_groups=length (encrypted array of secret image) DIV 6
6.1 flag=false
6.2 if length (encrypted array of secret image) MOD 48 > 0 then
6.3 flag=true
6.4 number_groups=number_groups+1
6.5 no of Bits in last group = length (encrypted array of secret image) MOD 48
6.6 end if
Step 7: for I = 1 number_groups do
Get Blocks from array of cover image that have higher value of variance
End for
Step 8: Make LSB of the first pixel of each selected block to "1".
Step 9: Make the LSB the first pixel of each unselected block to "0".
Step 10: While(i <= 1 TO number_groups)
Begin
10.1. If i = number_blocks AND flag = true then
10.2. No_of_bits = no of bits in last group
10.3. Second significant bit for each pixel in the block $_i$ = "0".
10.4. No_of_pixel = No of bits / 8
10.5. For i= 1 to pixel No_of_pixel do
10.6. Second significant bit of pixel $_i$= "1".
10.7. Else No_of_bits = 48
10.8 End if
10.9. By using chaotic "logistic map" hide the No_of_bits of group $_i$ randomly in LSB of 48 pixels of block $_i$
End While.
Step 11: Call convert_to_binary(produced cover image)
Step 12: Call convert_to_ vector (binary data of cover image)
Step 13: Apply QOTP by applying a bit flips with the vector and quantum key, where key is choosing by using BB84 protocol between sender and receiver.
Step 14: Send the output of the algorithm via quantum channel.
Step 15: Send the initial values and keys of chaotic maps by using diffie hellman
End.

V.2 Receiver Side

For decryption process, after the sender and receiver exchange the quantum key by using BB84 protocol the "Quantum One-Time Pad" algorithm has been used to decrypt the quantum bits (Qubits) that the receiver receives it and then convert to data of the image. The algorithm for the receiver side is detailed as follows:

Algorithm 2: The Receiver Side Algorithm

Algorithm of the Receiver Side
Input: Qubits
Output: Secret image
Step 1: Received data (qubits) via quantum channel.
Step 2: Receive the initial values and keys of chaotic maps by using diffie hellman.
Step 3: Apply QOTP by applying a bit flips with the vector and quantum key, where key is choosing by using BB84 protocol between sender and receiver.
Step 4: Call vector_to_binary (vector).
Step 5: Call binary_to_data_image (binary data).
Step 6: Divide the array of cover image to non-overlaying blocks (7*7) cells.
Step 7: If LSB of the first pixel of block $_i$ ="1" then select it.
Step 8: While i <= number of selected blocks
Begin
8.1. If i = number of selected blocks then
8.2. If the second significant bit in indicators block $_i$ = "1" then
8.3. Count them and save the result in to no_pixel
8.4. End if
8.5. Else
8.6 no_pixel=6
8.7. End if
8.8. no_of_bits= no_pixel *8
8.9. By using chaotic "logistic map" extracting the no_of_bits bits from the LSB of block $_i$ and save them in group $_i$.
End.
Step 9: Collect all the groups of bits and save them in array of one dimension.
Step 10: Collect all the groups and Decrypt them by applying the chaotic maps using the hybrid technique (Lorenz Map and Henon Map).
Step 11: Convert the produced data from the above step from binary to data image.
Step 12: Save the resulted image.

The complete our model process as depicted in figure 1-A and 1-B.

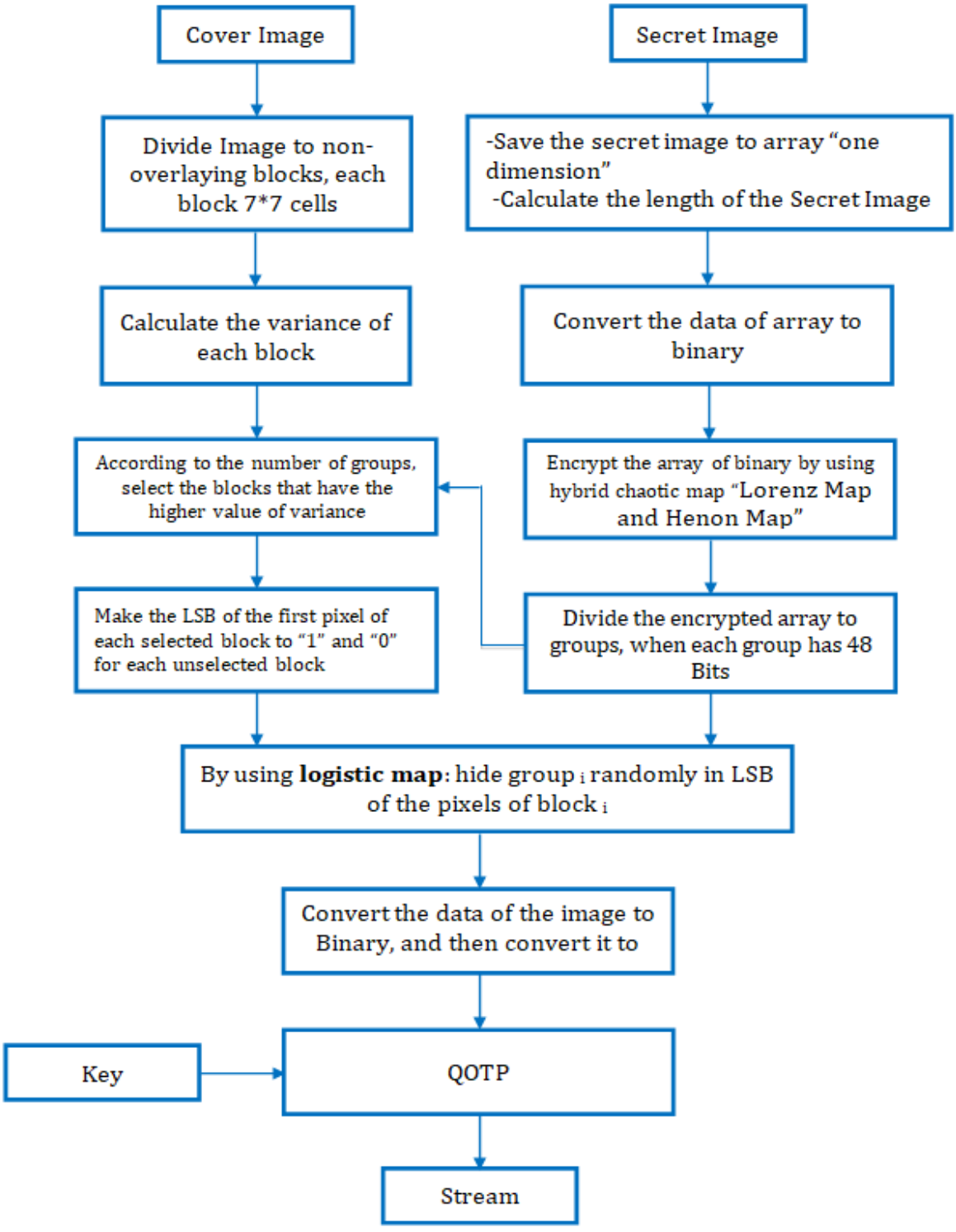


Figure (2-A): Block Diagram of the Proposed Model.

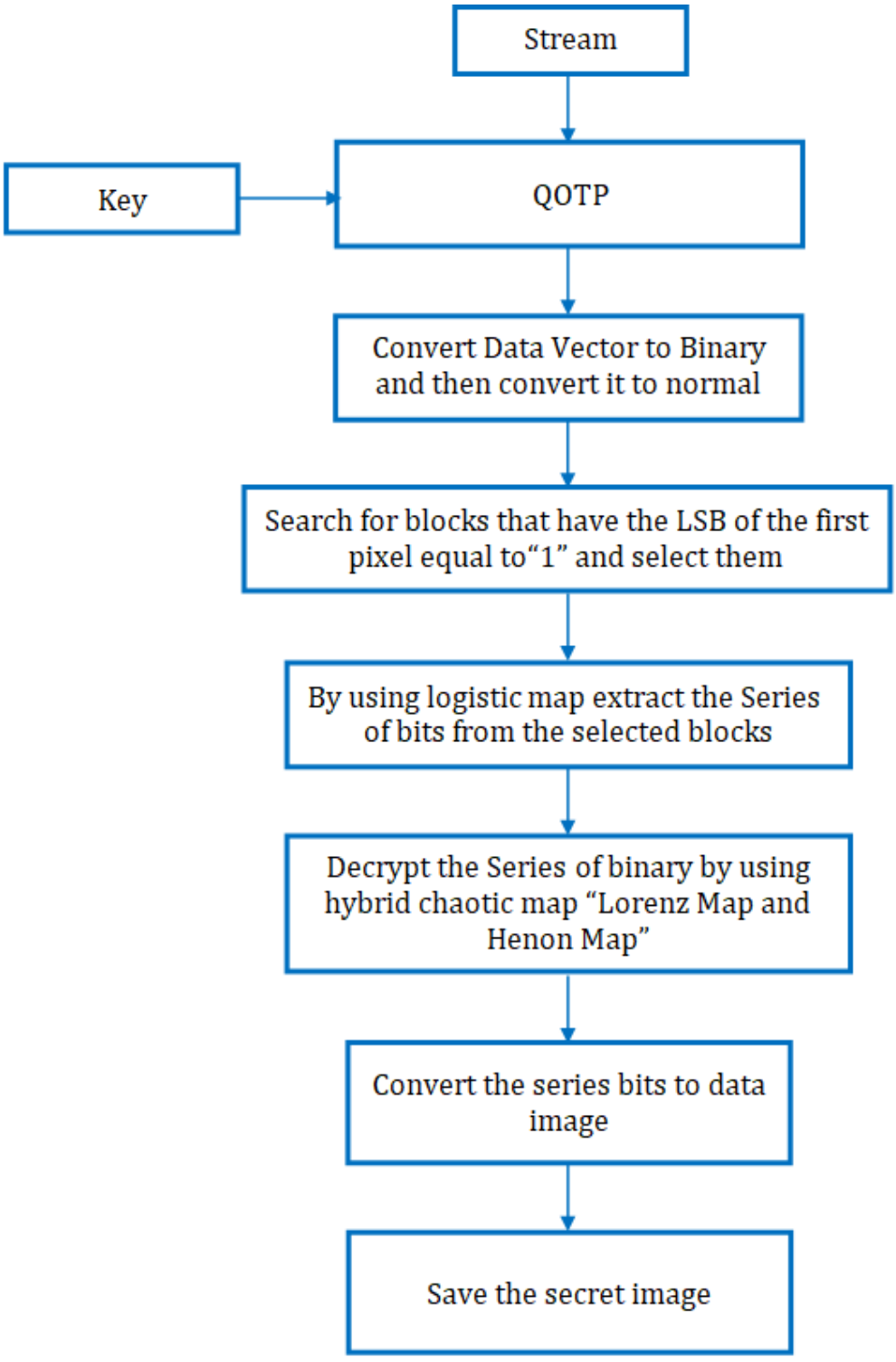


Figure (2-B): Block Diagram of the Proposed Model.

VII. Experimental Result

The proposed model involves two main modules; sender and receiver respectively. Where, the sender and receiver shared secret quantum key by using the BB84 protocol. Principally, capacity is used as one of the evaluation criteria. Capacity can be defined as the amount of information that can be hidden within the cover image. By using the proposed algorithm, capacity can be expressed as a secret image, which indicates the suitable size that might be inserted into an image. The histograms of cover and stego-images have been used to indicate that the proposed algorithm is very much statistically strong. The histograms are the common method to discover the effect of hiding data inside the cover image.

For testing purpose, several different images have been used with different width and height. In order to ensure the quality of the stego-image, (PSNR) Peak Signal-to-noise percentage in accordance with (Salman et al., 2012), PSNR is the percentage between the signal maximum values calculated by the quantity of noise that influence the signal. PSNR formula measures are defined in the following equation.

$$PSNR = 20 \log_{10} \frac{C_{max^2}}{MSE} \quad (1)$$

In which MSE refers to Mean Square Error that are showed in formula in the following equation.

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} \left(S_{xy} - C_{xy}\right)^2 \quad (2)$$

C_{max} carries the original image maximum values. S_{xy} is cover image pixel where coordinate C_{xy} and (x, y) is the pixel of the stego-image in the coordinate (x, y). M and N cover image size and the stego-image.

In the experimental process, three images have been used as in Figure (6).

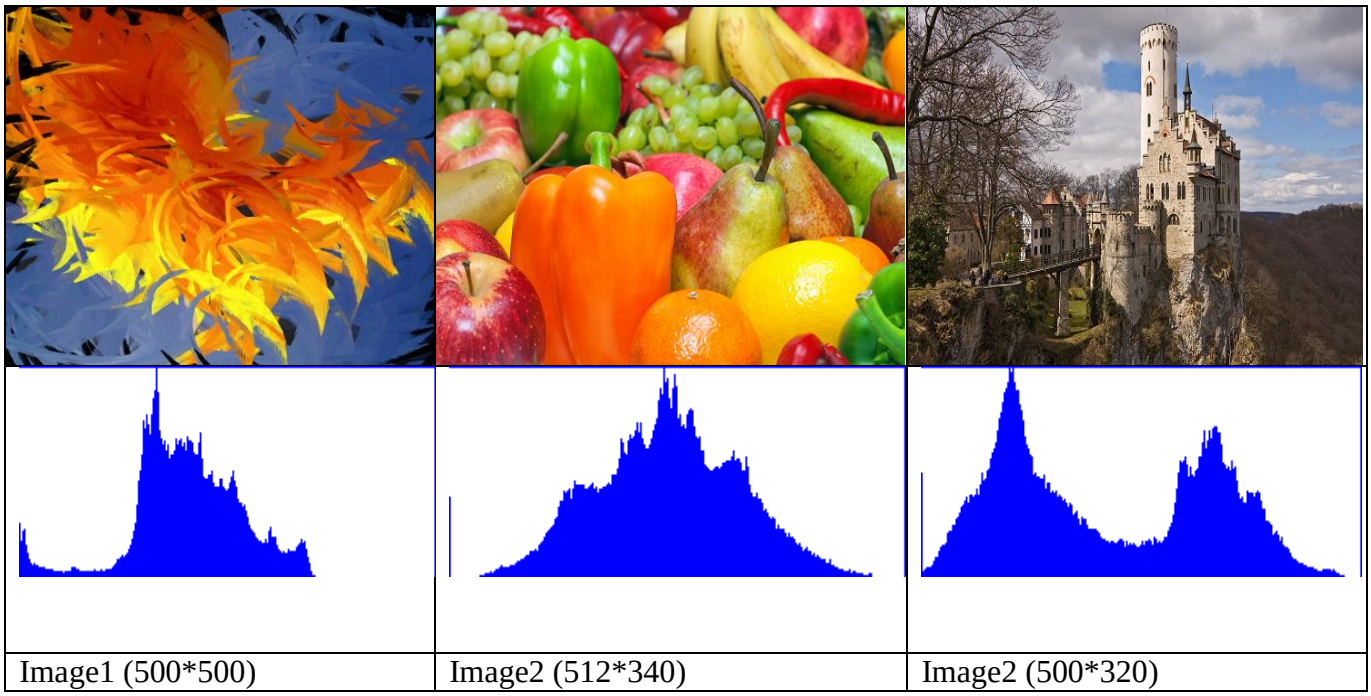


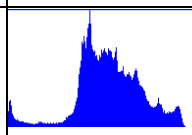
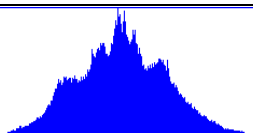
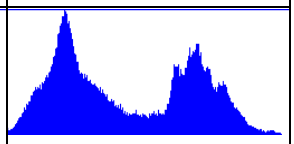
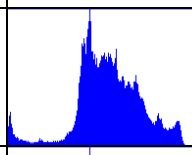
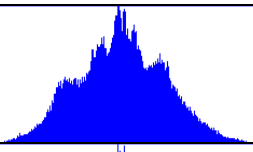
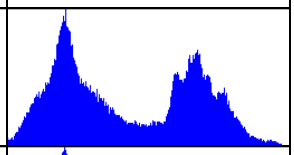
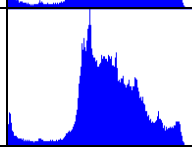
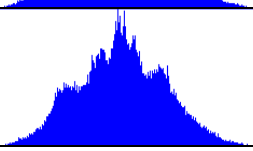
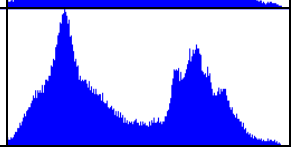
Image1 (500*500)	Image2 (512*340)	Image2 (500*320)

Figure (6): Pictures Used in Experimental.

The dimensions of the pictures are different. The secret image is different dimension. Table (1) shows the PSNR value for each stego-image with histograms for the images. For comparison, the calculated PSNR values vary from (60.19 dB to 51.75dB).

This results show that the proposed algorithm produced a high capacity of secret image. In practice, it becomes very difficult to see the differences between the cover image and the produced image especially in the high PSNR values. It is a well-known fact that the value of the PSNR is high; the distortion of images will be low. In other words, the high value of PSNR will make the recognition of the image difficult and the possibility of a variety of visual attacks by human eyes is low.

Table (1): The PSNR Value for Stego-Image with the hisogram

	Secret Image	PSNR			Histogram Image1	Histogram Image2	Histogram Image3
		Image1	Image 2	Image3			
1	132*132	53.72	52.16	51.75			
2	100*148	54.44	52.86	52.45			
3	80*50	60.19	58.67	58.08			

For the histogram of the images, when we compare the original images after the process of hidden and encryption by QOTP in the sender side and the received images in the receiver side, we noticed that the histogram for the stego-images is similar to their respective original images using naked eyes. This emphasizes on the results that the distortion between the cover image and the stego-image is minimum.

VIII. Conclusion

This study presents full "Quantum One-Time Pad" (QOTP) encryptions and steganography systems depend on chaotic map algorithm, involving all software needed for the completion of practical communications. This study is a pioneer in combining between steganography systems and quantum encryptions. In this model, the least significant bits (LSB) are responsible for embedding the secret images into cover images. While "Quantum One-Time Pad" (QOTP), is responsible for decrypting and encrypting the secret images. This model is strong due to the extraction of data without knowing the architectures of the proposed techniques and the extraction of data is difficult due to all the traditional data transformed in to quantum bits (Qubits). In which the eavesdropper can't get the information from the cover speech signals; it could not read the secret messages because it is in the forms of quantum cipher text. Experimental results revealed that effectiveness of the suggested hybrid model. For steganography, the chaotic map has given us a high random sequence. So, it will increase the system's complexity. For encryption, the quantum key used in quantum one-time pad algorithms give us high privacy depending on quantum law.

References

Lifang Yu, Yao Zhao, Rongrong Ni, Ting Li., 2010 "Improved adaptive LSB steganography based on chaos and genetic algorithm", EURASIP Journal on Advances in Signal Processing, 876946.

Sudha, K.L., 2012, "Text Steganography using LSB insertion method along with Chaos Theory", arXiv preprint arXiv: 1205.1859.

Singh, Siddharth, and Tanveer J. Siddiqui, 2012 "A security enhanced robust steganography algorithm for data hiding", IJCSI International Journal of Computer Science Issues 9.3,1694-0814.

Saini, Jaspal Kaur, and Harsh K. Verma, 2013, "A hybrid approach for image security by combining encryption and steganography", Image Information Processing (ICIIP), IEEE Second International Conference on. IEEE.

Kumar, Manish, et al. , 2014, "Chaos based encryption and decryption of image with secure image steganography", International Journal of Scientific Research And Education 2: 296-306.

Devaraj, S. Allwin, and Blanie Scrimshaw William. "Image Steganography Based On Non Linear Chaotic Algorithm", 2017, IJARIDEA International Journal of Advanced Research in Innovative Discoveries in Engineering and Applications.

Rajendran, Sujarani, and Manivannan Doraipandian, 2017, "Chaotic Map Based Random Image Steganography Using LSB Technique", IJ Network Security 19.4: 593-598.

Zaid A. Abod , Hussein A. Ismael and Alharith A. Abdullah., 2017, ” Chaos-Based Speech Steganography and Quantum One Time Pad”, Journal of Engineering and Applied Science.

Ismael, Hussein A., and Sattar B. Sadkhan., 2017, "Security enhancement of speech scrambling using triple Chaotic Maps", New Trends in Information & Communications Technology Applications (NTICT), Annual Conference on. IEEE.

Chirikov, Boris Valerianovich., 1971, "Research concerning the theory of non-linear resonance and stochasticity", No. CERN-Trans-71-40. CM-P00100691.

Ozgur Aybar, O. ; A.S. Hacinliyan and I. Kusbeyzi Aybar., 2013, " Stability and Bifurcation in the Henon Map and its Generalizations ", pp. 529-538.

Ramos, Romell Ambal., 2013, "Logistic function as a forecasting model: It’s application to business and economics", International Journal of Engineering 2.3: 2305-8269.

Yicong Zhou, et al, 2015, "Cascade Chaotic System With Applications", IEEE transactions on cybernetics, vol. 45, no. 9, pp. 2001-2012.

Johnson, Neil F., and Sushil Jajodia., 1998, "Exploring steganography: Seeing the unseen", Computer 31.2.

Swain, Gandharba, and Saroj Kumar Lenka., 2014, "Classification of image steganography techniques in spatial domain: a study", International Journal of Computer Science & Engineering Technology 5.3: 219-232.

Qaisar, Saad, Youngmin Jeong, and Hyundong Shin., 2015, "Quantum One-Time Pad for Direct Communication", Korea Telecom Conference 2015 Autumn Conference: 9-10.

Bennett, Charles H., and Gilles Brassard., 2014, "Quantum cryptography: Public key distribution and coin tossing", Theoretical computer science 560: 7-11.

Busch, Paul, Teiko Heinonen, and Pekka Lahti., 2007, "Heisenberg's uncertainty principle", Physics Reports 452.6: 155-176.

Boykin, P. Oscar, and Vwani Roychowdhury., 2003, "Optimal encryption of quantum bits", Physical review A 67.4: 042317.

Salman, Afan Galih, and Bayu Kanigoro., 2012, "Application Hiding Messages in JPEG Images with the Method of Bit-Plane Complexity Segmentation on Android-Based Mobile Devices", Procedia Engineering 50: 314-324.