Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 8, No. 4, October 2020, pp.2007-2018

Image security system using hybrid cryptosystem

Zaid A. Abod [1*], Mustafa S. Abbas [2], Ali kadhim Bermani [2]
[1] College of Food Science, Al-Qasim Green University
[2] College of Information Technology, University of Babylon

ABSTRACT

This work presents and describes a novel method to hide messages in images in a hybrid manner, as steganography is combined with quantum cryptography. Through stimulating and implementing this hybrid approach, the least significant bit (LSB) substitution is employed for hiding secret messages within cover images that consist of three bands (Red, Green and Blue), after which the output is encrypted using quantum one-time pad encryption. The models are illustrated explicitly and tested. In addition, the test analysis uses a steganalysis tool called StegExpose to detect LSB steganography in images. The experimental results proved that the image hiding is reliably secure and undetectable, and hence the proposed new hybrid model provides a sufficient security level as well as we have tested the proposed system using robust state-of- the-art steganalysis techniques and found the low payload threshold maintained in the proposed system produces a high margin of communication security safety. No payload files were detected (0% detections), despite each file containing the entire content of the information as embedded text.

Keywords: Steganography, Cover Image Steganography, Least Significant Bit, Steganalysis, Quantum Cryptography, Quantum Encryption Algorithm, Quantum One Time Pad.

Corresponding Author:

Zaid A. Abod
College of Food Science, Al-Qasim Green University
Babil, Iraq.
E-mail: zaid@uoqasim.edu.iq , zaid.auw@gmail.com

1. Introduction

Cryptography is a wide science with many open horizons for developing new ideas that contribute to its evolution. The notion of combining cryptography and steganography is emerging, primarily aiming to provide a high level of security, as these two techniques together form a closely related approach. Steganography is considered to be the science of invisible communication, and it is accomplished through hiding secret information within transporter files like images. It is necessary to ensure that the provider does not seem suspicious after the secret data has been hidden, in order to conceal the actual existence of the embedded statistics. On the other hand, cryptography is the science of tightly closed communication, realized through the use of data encryption. The encrypted data is unreadable, but upon alert, any individual could doubtlessly decrypt the records whenever enough time is provided, which is thus regarded to be a drawback.
Therefore, the solution to this problem is the combination of cryptography and steganography, whereby the encrypted data will be hidden and unreadable, hence the consideration of them being a closely related method. Throughout the present study, a novel concept is presented, which involves joining the cryptography and steganography through the use of quantum cryptography [1], which in turn depends on quantum laws [2] [3]. A whole steganography system is integrated with quantum cryptography according to two main dimensions: Quantum One-Time Pad (QOTP) encryption, and Least Significant Bit (LSB) substitution adaptive

steganography technology [4] [5]. Using one of the steganalysis software tools, namely StegExpose, which appears to be resistant to several commonly occurring security analysis attacks, tests the hybrid system. In fact, several aspects in terms of combining cryptography and steganography have been proposed earlier, some of which are closely related to the concept presented in the current study.

According to [6], the authors first encrypt a text message by using one of the classical cryptography methods, namely the transposition cipher method, after which the encrypted text message is hidden within an image by means of the LSB insertion method.

The researchers in [7] suggested a technique for consolidating cryptography and steganography to get secure communication through the use of an image file. They employed the AES algorithm to perform the encryption process, after which it is hidden within the cover image via the steganography technique. The authors in [8] presented a rapid combination method based on DES encryption and LSB steganography. This is another scheme for incorporating cryptography and steganography in communicating security with the use of image files. The RSA scheme is employed in encrypting, whereas the LSB technique is used for steganography [9]. Recently, two models were introduced based on the combination of cryptography and steganography. One of them used quick response codes for encoding the encrypted message before hiding it in the image. The other model used classical hybrid algorithms, namely RSA and Diffie-Hellman, before hiding it in the image [10] [11]. The authors in [12] encrypted the key and the Xnor gate after that used colour images to hidden encrypted information based on LSB algorithm so that all bits of the encrypted message has been hidden inside the cover image. The combination of One-Time Pad encryption and steganography system involves the use of substantial software so as to achieve real-time communication, after which the software undergoes testing using steganalysis techniques [13]. Novel LSB techniques have been introduced for hiding information within cover images, as these techniques seem to have a relatively higher payload and lower perceptibility of secret information embedded within cover images [14] [15]. The chaos-based speech steganography and quantum cryptography methods have been combined to hide the information based on LSB and Quantum Onetime Pad encryption, as introduces in [4] [5]. The remainder of this study can be sketched as follows: Section 2 provides an overview of LSB steganography. Section 3 produces the main concepts of the Quantum One-Time Pad (QOTP) as related to the existing model. Section 4 introduces the proposed model for producing a secure steganography, whereas Section 5 involves the experimental results and discussion. Finally, the major concluding remarks are presented in Section 6.

2. LSB steganography

Among the easier and more commonly used image steganography methods is the Least Significant Bit (LSB) substitution [16]. It displaces the least full-size bits without delay through embedding messages into the cover image. To amplify the capability of hiding, it can use up to 4 LSBs (Red, Green, Blue, and Alpha color channels, respectively) for each pixel. It is characterized by a frequent vulnerable factor, i.e. the sampled values mutate in an asymmetrical manner. Whenever the LSB of the cover medium sample cost equals the message bit, then no exchange occurs. Otherwise, the value 2n is converted into 2n+1 or vice versa [17]. Several upgrades and changes were suggested for enhancing the method in case, including adaptive methods for altering payload distributions, which are primarily depend on the picture features. The overall security is improved whenever the message encryption process proceeds it's embedding.

3. Quantum one-time pad (QOTP)

The "One-Time Pad" encryption technique was developed earlier and proven to be unbreakable, as it is fulfilled by means of employing an exclusive-or (XOR) addition for merging both the plain-text and key elements altogether. The ciphertext is shown to be unbreakable whenever the "One-Time Pad" condition is satisfied, namely that the key is totally random and should be used no more than once [18]. The major problem in One-Time Pad is the distributed key, where the key should be of similar length as the plaintext among N number of users. Classical key distribution protocols cannot detect an adversary between two

legitimate parties. Quantum key distribution (QKD) protocol provides a solution to this issue. The most commonly used (QKD) protocol is BB84 [19]. The security of (QKD) is ensures through the laws of quantum. The quantum uncertainty principle explained in [20] allows the secure sharing of secret keys among two legitimate parties.

The idea of a QOTP is presented in [21]. The protocol works by transmitting the quantum particles from receiver to sender, as the sender embeds his message and transmits it to the receiver using QOTP as an encrypting scheme for qubits.

4. Method

Throughout the present work, a novel idea is proposed of a double-stage secure technique that employs quantum cryptography and for securing and hiding secret messages, before transmitting them through a quantum communication channel.

The proposed model involves five major processes; dividing, embedding, encrypting, decrypting and extracting. For the division and embedding processes the message is divided into groups where each group has 8 character, after which the cover image is divided into three bands (Red, Green and Blue), where each band has "9*9" cells, having a symmetrical the division in all bands. The variance for the Blue band is calculated, and then the blocks that have the highest value of variance are chosen according to the number of groups of the characters. At the same time, the blocks in other bands are selected symmetrically. The blocks in Red and Green bands will be used in the hiding process, choosing the Blue band as indicator, as shown in Figure 1. To specify the blocks that are selected, the LSB of the center of the block is set at "1", whereas it will e set at "0" for the other unselected blocks. After these operations, the groups of messages will be hidden in the blocks of the image. The QOTP algorithm is made use of during the encryption process, for encrypting the data of the image which is already converted into quantum bits (Qubits), as illustrated in the subsequent algorithms.

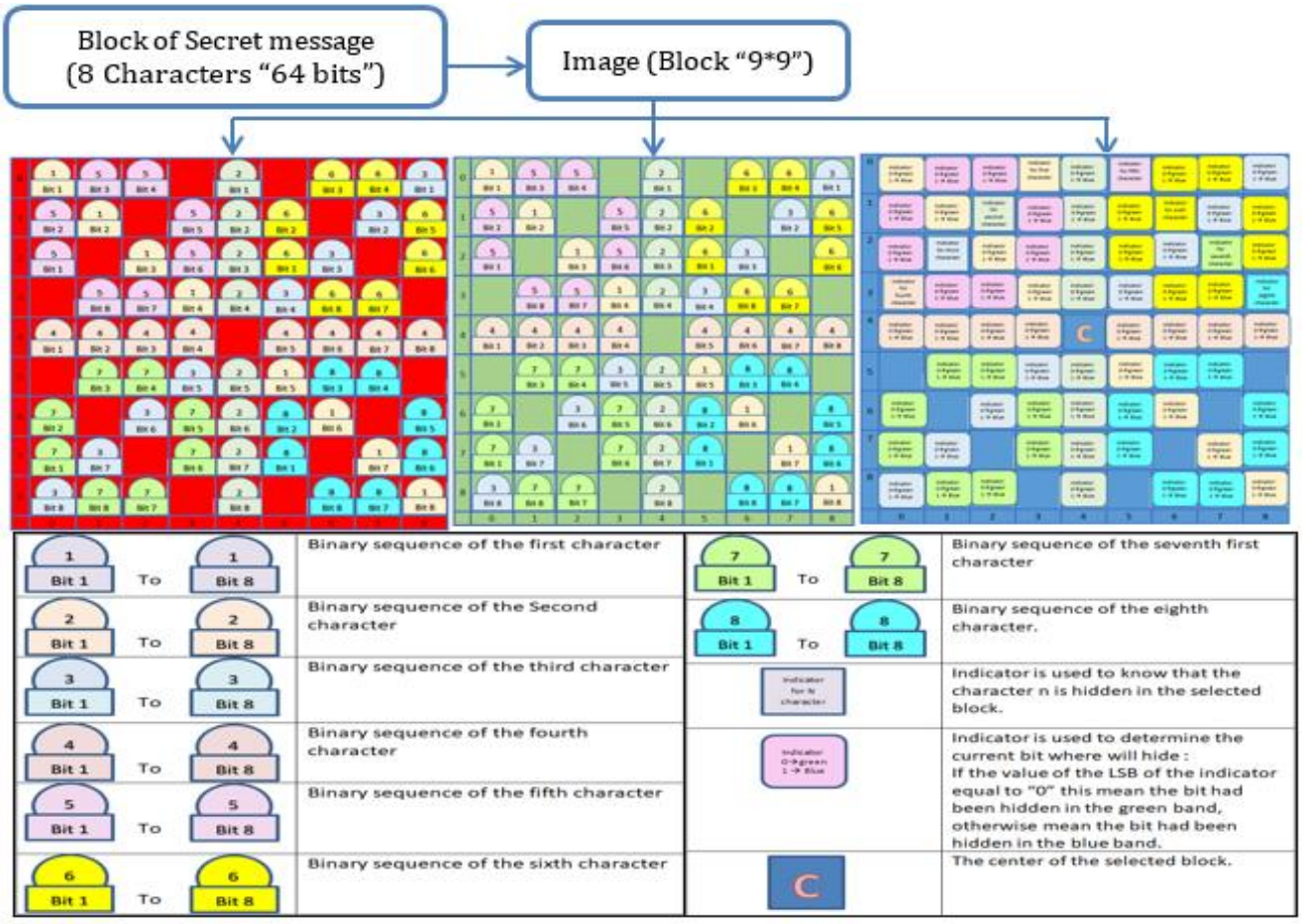


Figure 1. The strategy of hiding group n "8 character" of secret message in block N "9*9" of image

Algorithm of check and hide
Input: block of image $_i$, t, q, hidden bit $_k$
Output: detect band
Begin
If (LSB of red band (t,q) = hidden bit And LSB of blue band(t,q) = 0) then
No change
Else If(LSB of green band(t,q) = hidden bit And LSB of blue band(t,q) = 1) then
No change
Else If(LSB of red band(t,q) = hidden bit And LSB of blue band(t,q) <> 0) then
Change the LSB of blue band (t,q) to 0
Else If(LSB of green band(t,q) = hidden bit And LSB of blue band(t,q) <> 1) then
Change the LSB of blue band(t,q) to 1
Else If(LSB of red band(t,q) <> hidden bit And LSB of blue band(t,q) = 0) then
Change the LSB of red band(t,q) to hidden bit
Else If(LSB of green band(t,q) <> hidden bit And LSB of blue band(t,q) = 1) then
Change the LSB of green band(t,q) to hidden bit
Else If(LSB of green band(t,q) <> hidden bit) then
Change the LSB of green band(t,q) to hidden bit
Change the LSB of blue band(t,q) to 1
End of all if statement
End of algorithm

Algorithm of sender side
Input: message, cover image
Output: Qubits
Begin
Step 1: Divide the array of image to non-overlaying blocks, each block has 9*9 cells, and calculate the variance of each block in blue band.
Step 2: Divide the secret message to groups of eight characters.
Step 3: Select the blocks with a high rate of variance. In the blue band make the least significant bit of the center of each selected block to "1", and unselected block to "0".
Step 4: for (i<= 1 to no of groups)
4.1. If (i = no of group) then
No of char = no of char in last group
Make least significant bit of indicator cells in the blue band in the last block to "1" for all indicators that used and to "0" for all indicators that unused in the same last block in the blue band.
Else No of char = 8
End if
4.2. For j = 1 to no of char
Convert the character in index"j" to binary
For k = 1 to 8 do
If j=1 then determine the location (t,q) for each cell in the vertical diameter cells of the block $_i$.
If j=2 then determine the location (t,q) for each cell in the horizontal diameter cells of the block $_i$.
If j=3 then determine the location (t,q) for each cell in the diagonal at an angle of 45 cells of the block $_i$.
If j=4 then determine the location (t,q) for each cell in the diagonal at an angle of 135 cells of the block $_i$.
If j=5 then determine the location (t,q) for each cell in the first quarter cells of the block *i* in circular form.
If j=6 then determine the location (t,q) for each cell in the second quarter cells of the block $_i$ in circular form.
If j=7 then determine the location (t,q) for each cell in the third quarter cells of the block $_i$ in circular form.

If j = 8 then determine the location (t,q) for each cell in the fourth quarter cells of the block $_i$ in circular form.
Call check and hide algorithm (block of image $_i$, t, q, hidden bit $_k$)
Step 5: Convert the produced data of cover image to Binary form.
Step 6: Convert the binary data to Vector
Step 7: Perform QOTP through the application of bit flips with the vector and quantum key, as key is to be chosen through the use of the BB84 protocol between the sender and the receiver.
Step 8: Send the output data through quantum channel.
End of algorithm.

Figure 2 illustrates the block diagram of our proposed model, which includes the division, hiding and encryption processes.

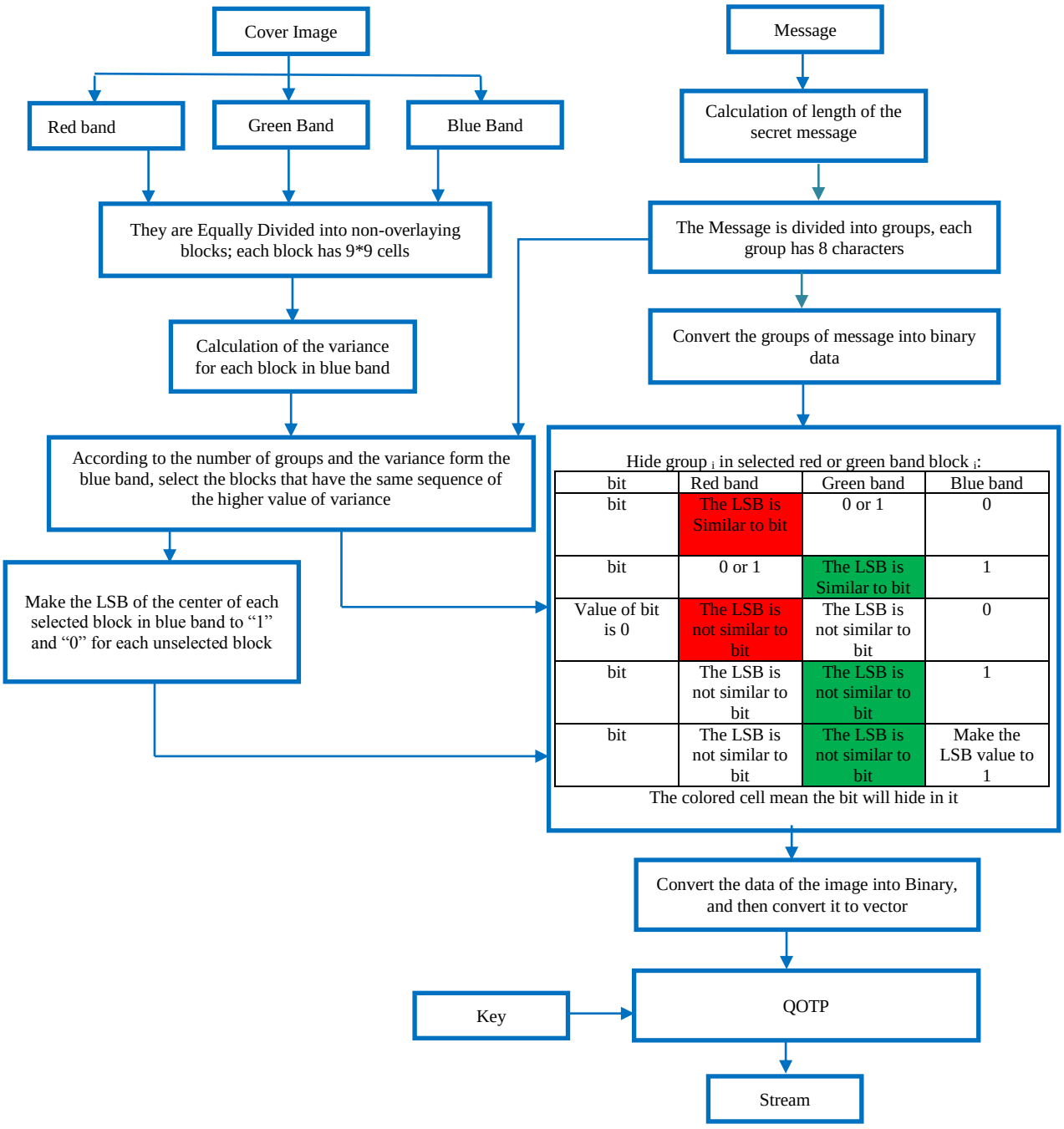


Figure 2. Block diagram of the suggested model for sender stage

Algorithm of receiver side
Input: Image Qubits
Output: Secret message
Begin
Step 1: Through the quantum channel receive the data (qubits).
Step 2: Perform QOTP through the application of bit flips with the vector and quantum key, as key is to be chosen through employing the BB84 protocol between sender and receiver.
Step 3: Convert the vectors to the Binary form.
Step 4: Convert binary data to Image data.
Step 5: Divide the image to non-overlaying blocks, each block has 9*9 cells.
Step 6: in the blue band searching about the blocks that have the least significant bit of the cells in center blocks equal to "1" and select them.
Step 7: for i =1 to number of selected blocks
7.1. If (The LSB of the vertical indictor cell in the blue band equal to "1") then
For k =1 to 8 do
If (The LSB of the vertical cell $_k$ in the blue band block $_i$ = 0) then
Get the LSB from the cell $_k$ in the vertical diameter of the block $_I$ from the red band.
Else get the LSB from the cell $_k$ in the vertical diameter of the block $_I$ from the green band.
7.2. If (The LSB of the horizontal indictor cell in the blue band equal to "1") then
For k =1 to 8 do
If (The LSB of the horizontal cell $_k$ in the blue band block $_i$ = 0) then
Get the LSB from the cell $_k$ in the horizontal diameter of the block $_I$ from the red band.
Else get the LSB from the cell $_k$ in the horizontal diameter of the block $_I$ from the green band.
7.3. If (The LSB of the diagonal at an angle of 45 indictor cell in the blue band equal to "1") then
For k =1 to 8 do
if (The LSB of the diagonal at an angle of 45 cell $_k$ in the blue band block $_i$ = 0) then
Get the LSB from the cell $_k$ in the diagonal at an angle of 45 diameter of the block $_I$ from the red band.
Else get the LSB from the cell $_k$ in the diagonal at an angle of 45 diameter of the block $_I$ from the green band.
7.4. If (The LSB of the diagonal at an angle of 135 indictor cell in the blue band equal to "1") then
For k =1 to 8 do
If (The LSB of the diagonal at an angle of 135 cell $_k$ in the blue band block $_i$ = 0) then
Get the LSB from the cell $_k$ in the diagonal at an angle of 135 diameter of the block $_I$ from the red band.
Else get the LSB from the cell $_k$ in the diagonal at an angle of 135 diameter of the block $_I$ from the green band.
7.5. If (The LSB of the first quarter indictor cell in the blue band equal to "1") then
For k =1 to 8 do
If (The LSB of the first quarter cell $_k$ in the blue band block $_i$ = 0) then
Get the LSB from the cell $_k$ in the first quarter diameter of the block $_I$ from the red band.
Else get the LSB from the cell $_k$ in the first quarter diameter of the block $_I$ from the green band.
7.6. If (The LSB of the second quarter indictor cell in the blue band equal to "1") then
For k =1 to 8 do
If (The LSB of the second quarter cell $_k$ in the blue band block $_i$ = 0) then
Get the LSB from the cell $_k$ in the second quarter diameter of the block $_I$ from the red band.
Else get the LSB from the cell $_k$ in the second quarter diameter of the block $_I$ from the green band.
7.7. If (The LSB of the third quarter indictor cell in the blue band equal to "1") then
For k =1 to 8 do
If (The LSB of the third quarter cell $_k$ in the blue band block $_i$ = 0) then
Get the LSB from the cell $_k$ in the third quarter diameter of the block $_I$ from the red band.
Else get the LSB from the cell $_k$ in the third quarter diameter of the block $_I$ from the green band.

7.8. If (The LSB of the fourth quarter indictor cell in the blue band equal to "1") then
For k =1 to 8 do
If (The LSB of the fourth quarter cell $_k$ in the blue band block $_i$ = 0) then
Get the LSB from the cell $_k$ in the fourth quarter diameter of the block $_I$ from the red band.
Else get the LSB from the cell $_k$ in the fourth quarter diameter of the block $_I$ from the green band.
Step 8: Collect the extracted series of bits and convert them to characters.
End of Algorithm

Figure 3 illustrates the block diagram of our proposed model, which includes the decryption process as well as the extraction of information and final message.

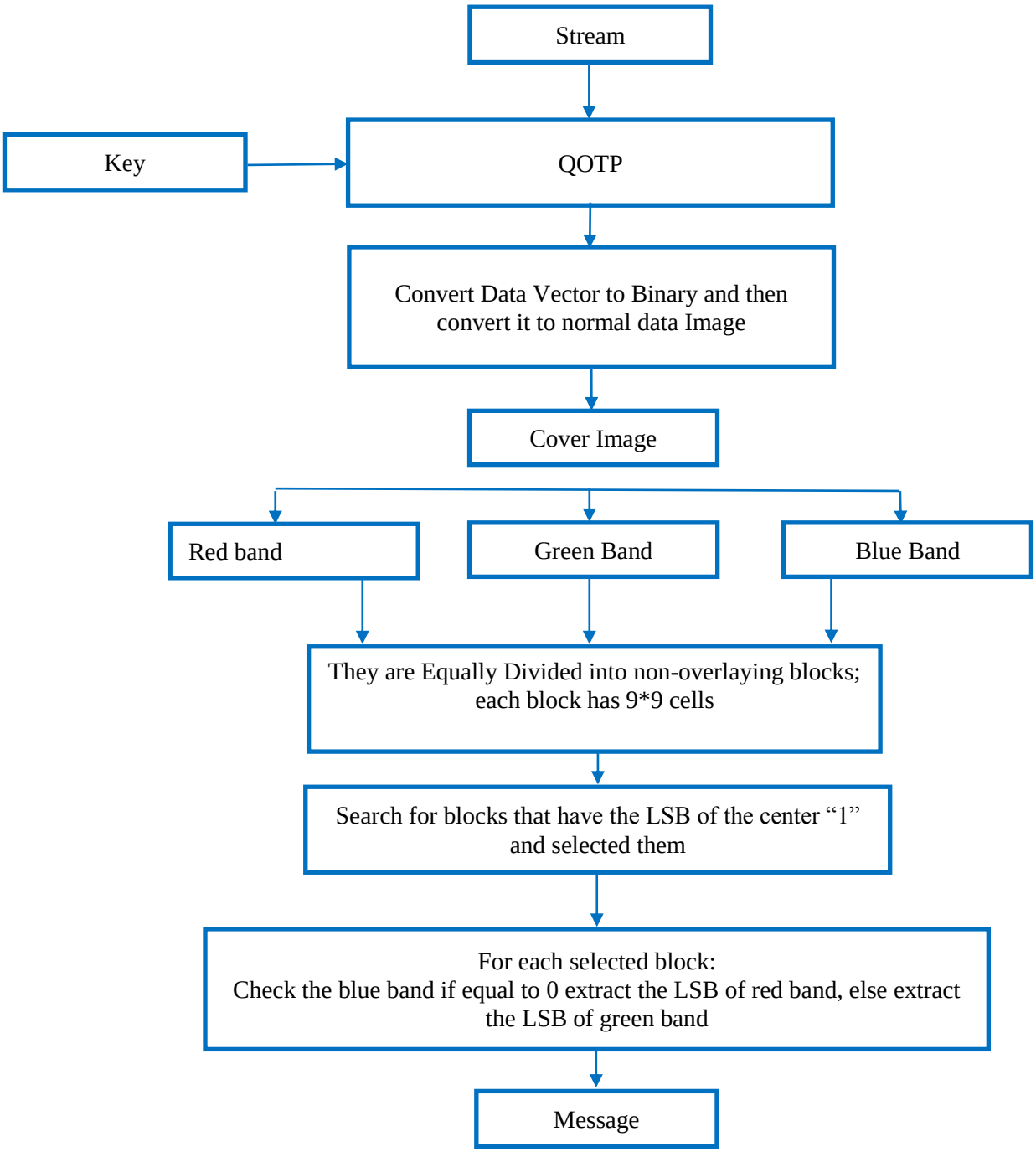


Figure 3. Block diagram of the suggested model at the receiver stage

5. Results and discussion

The application consists of two major parts; sender and receiver. As shown in Fig. 2, and Fig. 3, the user on the sender's side browses a cover image, and accesses secret quantum key that is shared by both parties of the BB84 protocol.

Primarily, the capacity is employed an evaluating criterion, representing the quantity of hidden data within the cover of an image. In this case, it could be represented by means of numbers of 8 bits, thereby specifying the maximal message to be inserted within images. The histograms of the cover and stego-images are made use of so as to designate that the suggested algorithm is statistically robust. The histograms represent a communal technique for revealing the influence of data hidden within cover images.

A number of differing images are used in the test having diversified widths and heights for ensuring the stego-image quality, and Peak Signal-to-noise Ratio (PSNR). PSNR represents the ratio between the maximal values of measured signal to the quantity of noise affecting it [22]. The PSNR formula is shown in (1).

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

Where MSE refers to Mean Square Error, presented in (2).

$$MSE = \frac{1}{MN} \sum_{X=1}^{M} \sum_{Y=1}^{N} (S_{XY} - C_{XY})^2 \quad (2)$$

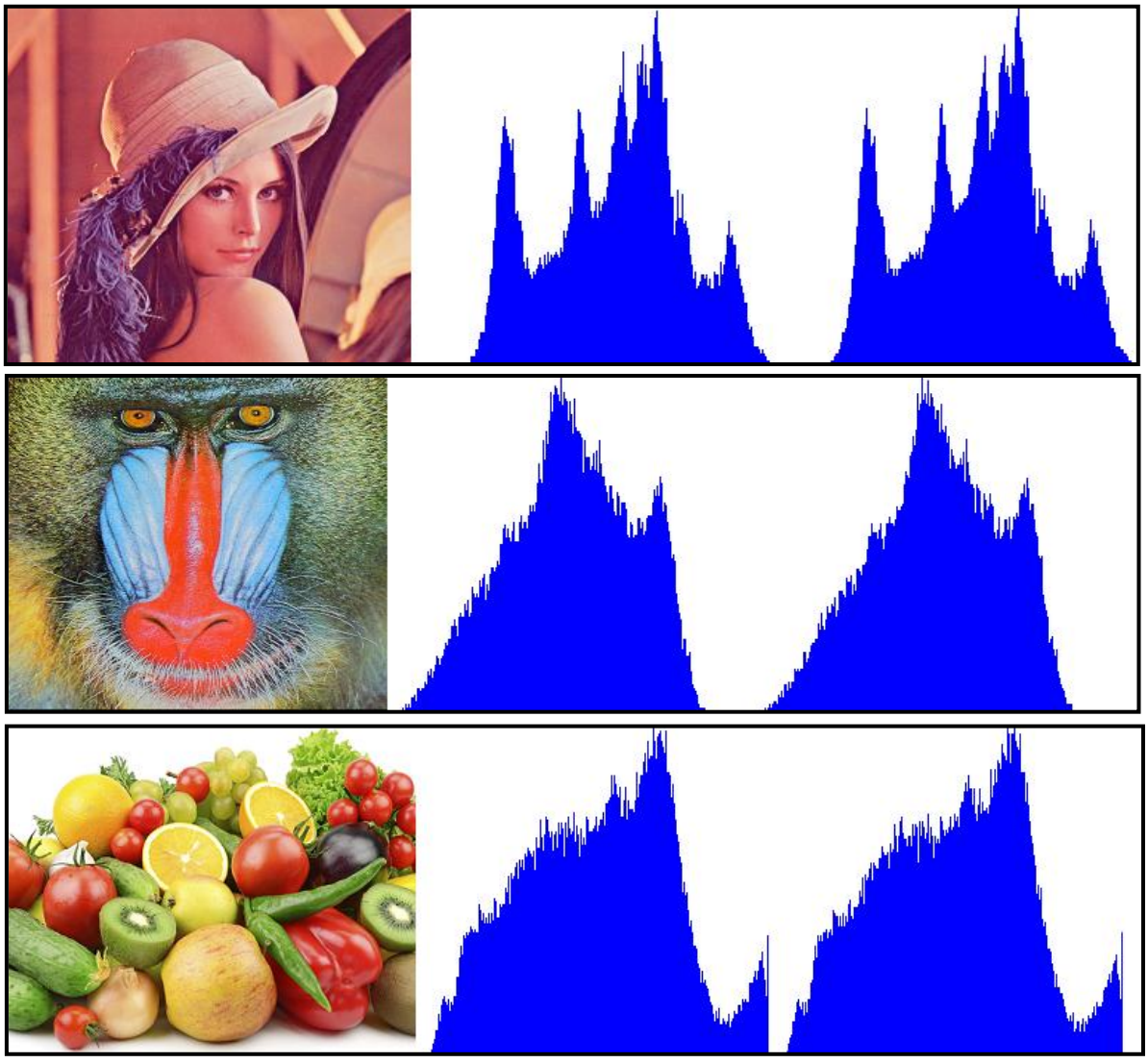
Cmax represents the maximal value within the original image, whereas S_{xy} and C_{xy} represent the pixel of cover and stego image, respectively, both at the coordination (x,y). M and N are the sizes of each of the cover image and the stego-image, respectively. In the experimental process, three images have been used in Figure 4.Thus, Table 1 shows the relatively higher value of PSNR complicates the process of recognizing the image, in addition to the fact that is decreases the occurrence of a possible variety of visual attack by human eyes.

Figure 5 represents a set of histograms for (a) the original images, (b) the cover images, and (c) the stego-images. The histogram for each of the stego-images resembles its respective original image during bare eye observation. Thereby emphasizing the fact that the distortion between these two images is minimal.

Table 1. The psnr value for the stego-images

Times of Sentences	Number of Characters	PSNR Value			Average PSNR
		Lena	Baboon	Fruits	
1	100	71.20	71.18	71.63	71.34
2	180	69.42	69.56	70.57	69.85
3	266	68.26	68.30	69.64	68.73
4	500	65.87	66.13	67.95	66.65
5	625	65.07	65.32	67.32	65.38
6	1000	63.22	63.28	65.75	64.08
7	1634	61.17	61.44	63.86	62.03
8	3000	58.63	58.88	61.48	59.66

Figure 4. Pictures used in the experiment



(a) (b) (c)

Figure 5. (a) Cover Image (b) Histogram of Cover Image (c) Histogram of Stego-image

StegExpose (the free, open-source download) is executed on a batch of 3 image files encoded by means of the quantum OTP-Steg software. The testing specifications and resulting data are depicted in Table 2. It has been noticed that neither of the files could be detected.

Table 2. StegExpose steganalysis test results

Cover Image	Length of MSG in Bytes	Above stego threshold	Secret message size in Bytes	Primary Sets	Sample Pairs	Chi Square	RS analysis	Fusion (mean)
Lena	100	False	4343	0.06155721 567353699	Null	0.007199344 538663201	0.031605947 979826306	0.033454169 397342165
	180	False	4913	0.07455797 194222978	Null	0.006584460 332020509	0.032395030 21956286	0.037845820 83127105
	266	False	4234	0.06107161 395312746	Null	0.004658016 635644421	0.032118756 783716576	0.032616129 12416282
	500	False	3382	0.04587531 4985823326	Null	0.003138289 571184212	0.029150872 333001114	0.026054825 630002887
	625	False	5278	0.07808873 534890103	Null	0.005747444 46921054	0.038138998 631498104	0.040658392 816536555
	1000	False	5952	0.06734504 239775724	Null	0.024394178 29851236	0.045806185 847454634	0.045848468 847908073
	1634	False	7388	0.08598050 510495232	Null	0.038555506 22264101	0.046203574 14759206	0.056913195 15839514
	3000	False	6519	0.06875416 879426366	Null	0.034741080 15161456	0.047170094 20845983	0.050221781 05144601
Baboon	100	False	4575	NaN	Null	0.050381865 467422425	0.089191538 44396593	0.031605947 979826306
	180	False	4612	NaN	Null	0.050909185 234369464	0.089793405 93420874	0.070351295 5842891
	266	False	4626	NaN	Null	0.049031322 47184711	0.092114801 22068127	0.070573061 84626419
	500	False	5149	NaN	Null	0.059296551 14915993	0.097795712 08048893	0.078546131 61482443
	625	False	4334	NaN	Null	0.038537503 7148145	0.093681234 18016336	0.066109368 94748892
	1000	False	5108	NaN	Null	0.058856614 313771725	0.096989131 47118776	0.077922872 89247975
	1634	False	3170	NaN	Null	0.005253597 934115469	0.091466934 31740487	0.048360266 125760165
	3000	False	4525	NaN	Null	0.065134452 98225373	0.072916313 51068409	0.069025383 24646891
Fruits	100	False	4285	0.04531201 4435292806	0.0	0.042665220 30034801	0.044063795 70570394	0.033010257 610336186
	180	False	4260	0.04489654 839685163	0.0	0.042505237 59600577	0.043869364 19294264	0.032817787 54645001
	266	False	4307	0.04671687 301982806	0.0	0.041903573 678795554	0.044105207 00129705	0.033181413 42498017
	500	False	4454	0.04858902 5035857075	0.0	0.044060703 32501713	0.044592177 447097356	0.034310476 451992894
	625	False	4505	0.04913552 357574107	0.0	0.044120673 440559886	0.045548246 17602536	0.034701110 79808158
	1000	False	4637	0.05079188 555953361	0.0	0.045872766 45779447	0.046212618 47080227	0.035719317 622032586
	1634	False	4653	0.04737039 436235874	0.0	0.047402446 60379058	0.048611921 66490236	0.035846190 65776292
	3000	False	4631	0.04590698 697908478	0.0	0.046378032 06818971	0.050403707 174837595	0.035672181 555528024

The capabilities of the proposed scheme compared to other schemes will be evaluated in the Table 3. The most common security parameters including amount of data embedded in byte, MSE, PSNR, and quantum property will be used for performance comparison. From this result, it is found that the proposed scheme has the lowest

value of MSE among the other schemes and with the same amount of data embedded roughly. In addition the largest value of PSNR among the other schemes and this means the restored image quality is better. Also our proposed scheme has the quantum property and this is means high security compared with the other schemes based on quantum law.

Table 3. Comparison with other schemes

Scheme	Amount of data embedded in Byte	MSE	PSNR	Quantum property
Proposed Method	100	0.0044	71.63	Yes
Proposed Method	3000	0.046	61.48	Yes
[6]	4267	0.48	51.28	No
[7]	-	0.1167	59.1570	No
[10]	-	0.6420	50.055	No
[12]	3031	0.0339	53.65	No

6. Conclusions

Throughout this work, a complete hybrid approach has been introduced between the steganography system and quantum cryptography represented by Quantum One-Time Pad encryption (QOTP), covering all the software that is necessary to simulate, implement and test this methodology. The combination of the steganography system with the quantum encryption is presented for the first time in this way, where the least significant bit (LSB) is responsible for the embedding of secret messages inside an image that is divided into three bands (Red, Green and Blue), meanwhile the QOTP is used to involve the encrypting and decrypting processed of the stego-image. The model underwent testing and proved its robustness, as the extraction of data with no prior knowledge of the architecture of the suggested method is rather complicated. In addition, all classical data is converted to quantum bits (Qubits) that provide high confidentiality to the model, because it depends on the quantum laws, and hence the eavesdropper cannot obtain any information from the cover image. Based on the experimental results, it has been proven that this model produced a properly wild photo after embedding the higher potential of secret messages (for instance, 3000 characters with the common PSNR cost of 59.66 dB). The rise in secret message embedding capacity consequently leads to a moderate decrease in PSNR values.

We have analysed the model using one of the steganalysis tools (StegExpose) and it has been observed that there are no payload files detected throughout the proposed hybrid system.

References

[1] P. Hoffman, The Transition from Classical to Post-Quantum Cryptography, Wilmington - USA: Network Working Group, 2020.

[2] A. A. Abdullah, and Y. K. ABBAS, "Quantuam Audio Stegoangrhy Sstem", Journal of Engineering Science and Technology , vol. 15 no. 3, pp. 1562-1588, 2020.

[3] Y. H. Jassem, and A. A. Abdullah. "ENHANCEMENT OF QUANTUM KEY DISTRIBUTION PROTOCOL FOR DATA SECURITY IN CLOUD ENVIRONMENT", *ICIC International*, vol. 11, no. 3, pp. 279-288, 2020.

[4] Z. A. Abod, H. A. Ismael and A. A. Abdullah, "Chaos-Based Speech Steganography and Quantum One Time Pad," *Journal of Engineering and Applied Sciences*, vol. 13, no. 3, pp. 739-745, 2018.

[5] Z. A. Abod, "A Hybrid Approach to Steganography System Based on Quantum Encryption and Chaos Algorithm," *Journal of University of Babylon*, vol. 26, no. 2, pp. 280-294, 2018.

[6] S. A. Laskar and K. Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption," *International Journal of Database Management Systems*, vol. 4, no. 6, pp. 57-68, 2013.

[7] J. K. Saini and H. K. Verma, "A hybrid approach for image security by combining encryption and steganography," in *IEEE Second International Conference on Image Information Processing*, Shimla - India, 2013.

[8] Y. Ren-Er, Z. Zhiwei, T. Shun and D. Shilei, "Image steganography combined with DES encryption pre-processing," in *Sixth International Conference on Measuring Technology and Mechatronics Automation*, Zhangjiajie - China, 2014.

[9] S. Pund-Dange and C. . G. Desai, "Secured data communication system using RSA with mersenne primes and Steganography," in *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi - India, 2015.

[10] B. Karthikeyan, A. C. Kosaraju and S. G. S, "Enhanced security in steganography using encryption and Quick Response code," in *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai - India, 2016.

[11] M. S. Abbas, S. . S. Mahdi and S. A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography," in *International Conference on Computer Science and Software Engineering (CSASE)*, Duhok - Iraq, 2020.

[12] N. R. Mohammed, J. A. Abed and E. A. Abbood, "Hide text depending on the three channels of pixels in color images using the modified LSB algorithm," International Journal of Electrical and Computer Engineering 10.1, 809-815, 2020.

[13] M. J. Pelosi, G. Kessler and M. S. S. Brown, "One-Time Pad Encryption Steganography System," in *Annual ADFSL Conference on Digital Forensics, Security and Law*, Daytona Beach, Florida - USA, 2016.

[14] L. Y. Por, D. Beh, T. F. Ang and S. Y. Ong, "An enhanced mechanism for image steganography using sequential colour cycle algorithm," *The International Arab Journal of Information Technolog*, vol. 10, no. 1, pp. 51-60, 2013.

[15] Z. Khan, M. Shah, M. Naeem, T. Mahmood and S. Khan, "Threshold-based steganography: a novel technique for improved payload and SNR," *The International Arab Journal of Information Technology*, vol. 13, no. 4, pp. 380-386, 2016.

[16] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26-34, 1998.

[17] G. Swain and S. K. Lenka, "Classification of image steganography techniques in spatial domain: A study," *International Journal of Computer Science & Engineering Technology*, vol. 5, no. 3, pp. 219-232, 2014.

[18] Q. Saad, Y. Jeong and H. Shin, "Quantum One-Time Pad for Direct Communication," in *Korea Telecom Conference 2015 Autumn Conference*, Korea, 2015.

[19] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical computer science*, vol. 560, no. 1, pp. 7-11, 2014.

[20] P. Busch, T. Heinonen and P. Lahti, "Heisenberg's uncertainty principle," *Physics Reports*, vol. 452, no. 6, pp. 155-176, 2007.

[21] O. P. Boykin and V. Roychowdhury, "Optimal encryption of quantum bits," *Physical review A 67*, vol. 67, no. 4, p. 042317, 2003.

[22] A. G. Salman and B. Kanigoro, "Application Hiding Messages in JPEG Images with the Method of Bit-Plane Complexity Segmentation on Android-Based Mobile Devices," *Procedia Engineering*, vol. 50, pp. 314-324, 2012.