Image Security Using Quantum Rivest-Shamir-Adleman Cryptosystem Algorithm and Digital Watermarking

Hend A. Elsayed[1], **Yasir Khalid Jadaan**[2], **and Shawkat K. Guirguis**[2]

[1]Department of Communication and Computer Engineering, Faculty of Engineering
Delta University for Science and Technology, Mansoura, Egypt
[2]Department of Information Technology, Institute of Graduate Studies and Researches
Alexandria University, Alexandria, Egypt

Abstract— Authentication and integrity are very essential security requirements for a secure transaction. To achieve these security goals, we use a combined technology of Rivest-Shamir-Adleman cryptosystem algorithm and digital watermarking. This work proposes the Rivest-Shamir-Adleman cryptosystem algorithm to work with quantum computing idea as simulation to encrypt the image and the goal of the quantum idea is to speed the process of the encryption. After that, the encrypted image is embedded in the cover image using its least significant bit. Digital watermarking is the process of embedding information into a digital signal. This paper uses the hybrid discrete wavelet transform and singular value decomposition algorithms for embedding and extracting process of digital watermarking. This scheme favorably preserves the quality for both the sender and receiver. The experimental results showed the efficiency of the proposed system in terms of time, integrity, and the authentication. The results showed the accelerate of the encryption process using RSA with quantum ideas compared with using RSA only, the results showed the histogram for both the sender or decrypted image and the receiver or the watermark image is the same. From the histogram diagrams, it is observed that they are quite similar and the difference is insignificant which the human eye cannot easily differentiate. Also the results showed the correlation coefficient between the original watermark and received watermark. The correlation coefficient has the value one if the two images are absolutely identical, has the value zero if the two images are completely uncorrelated. From the correlation coefficient results, it is observed that they are nearly one. This model maintains the image quality is good.

1. INTRODUCTION

Cryptography was created as a technique for securing the secrecy of communication. Many different methods have been developed to encrypt and decrypt data in order to keep the message secret [1]. Encryption is converting the image into an incomprehensible formula [2]. We use the Rivest-Shamir-Adleman cryptosystem (RSA) algorithm to encrypt the image to it's almost better security algorithms of hand but relatively slow in the encryption process [3]. In this paper, we use the benefit in quantum computing in order to accelerate RSA algorithm to encrypt image. We have benefited from the idea and state qubit in quantum computing and Adavchl to the RSA algorithm in order to speed up the encryption process. In [4] the authors suggested a comparison between RSA cryptosystem which is one of asymmetric cryptosystems and the two symmetric systems, data encryption standard (DES) and blowfish. The results showed that time taken using mathematical relations in RSA make steps faster implemented than DES and blowfish algorithms and with more secured data than symmetric systems. In [5] the authors perform the splitting of the images. Then we apply the RSA algorithm on the split. In [6], the authors presented a new proposal that merges between the merits of classical cryptography and quantum cryptography. It was also to take advantage of LSB algorithm to hide the cipher text process [7]. This process carries out authentication of the picture very shortly. RGB image was used for the process and sent to the recipient. In this research also we use the same image and create a watermark them using algorithms DWT and SVD to embed and extract of the watermark. This work has been on the same image but the format gray scale [8]. Finally, the power of this work increases when we link between encryption technology and concealment watermark.

The paper is organized as follows. Section 2 describes the quantum algorithm, Section 3 describes the proposed system, and Section 4 describes the simulation results. Finally, Section 5 concludes the paper.

2. QUANTUM ALGORITHM

The data in classical computing are stored in the form of binary digits or bits. A bit is the basic unit of information stored and manipulated in a computer, which in one of two possible distinct states (for instance: two distinct voltages, on and off state of electric switch, two directions of magnetization, etc.). The two possible values/states of a system are conventional computers operate on bits (classical bits — cbits) and the quantum computer performs computations on quantum bits (qubits). In the classical bit can be in one of the two states — either 0 or 1 in the same time. But the qubit can be in the superposition of the states $|0i$ and $|1i$. The notation $| \cdot i$ is called the Dirac notation and is the standard notation for states in quantum mechanics. The special states $|0i$ and $|1i$ are known as computational basis states and form an orthonormal basis for this vector space. Qubits can be realized by many different physical systems [9]. Both the classical and quantum bits have state. The state of cbit is always either a 0 or 1 [10].

3. PROPOSED METHOD

3.1. The Transmitter

In the transmitter, we suggest the protection of the original image using two methods:

The first method is the protection by two steps, the first step is encrypting the original image and the second step is hiding it into the cover image for integrity as shown in Fig. 1. The first step is to convert the image to a matrix of bytes as hexadecimal and then encrypt the image by one of two ways, the first is using RSA algorithm and the second using RSA algorithm and quantum ideas, then calculate the encryption time for the two methods. It was used qubit idea and states in quantum computing to speed up the encryption process. Now we have two dimension matrices of resulting bytes. In the RSA algorithm, we encrypt the bytes as sequentially. But with using the quantum computing ideas, each row represents as qubit, the row is state. All rows will be encrypted in the same time. The second step is hiding the encryption text in cover image as shown in Fig. 1.

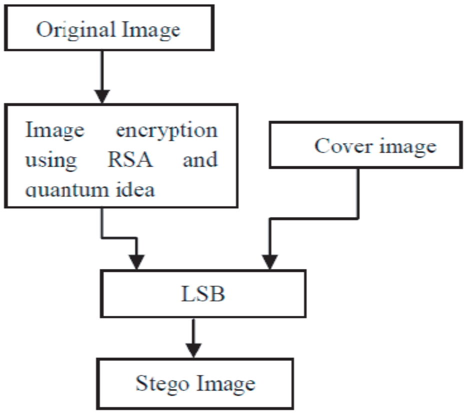


Figure 1: Image encryption and hiding in the cover image.

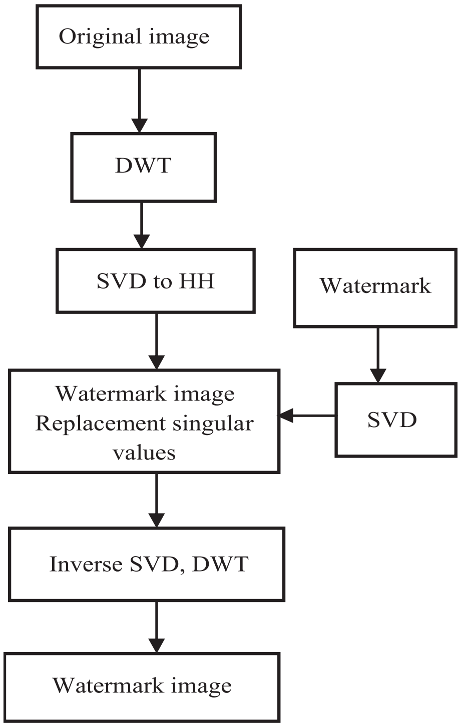


Figure 2: Creating the digital watermark of the image.

The second method is the protection by watermarking the original image for authentication; we create the digital watermarking for original image as shown in Fig. 2. The steps for watermark embedding algorithm are:

1- Apply SVD on the watermark: $W = Uw * Sw * Vw$.

2- Apply DWT on cover image and decompose into four sub-bands: LL, HL, LH, and HH.

3- Apply SVD to HH band: $H = UH * SH * VH$.

4- Replace the singular values of the HH band with the singular values of the watermark.
5- Apply inverse SVD to obtain the modified HH band $H' = UH * Sw * VH$.
6- Apply inverse DWT to produce the watermarked cover image.

3.2. The Receiver

The receiver is made by two steps, the first step is to Decrypt the and retrieval the original image and the second step is to verify of the digital watermark and extract the original image as shown in Fig. 3. The steps for the Watermark Extraction Algorithm are:

1- Apply DWT on watermarked image into four sub-bands: LL, HL, LH, and HH.
2- Apply SVD to HH band: $H = UH * SH * VH$.
3- Extract the singular values from HH band.
4- Use the SVD of the original watermark.
5- Extract the singular values from original watermark.
6- Match between singular values for both original watermark and HH band watermarked image using correlation coefficient function and between the two images extracted from the decryption and the watermark image are compared using the histogram analysis [11].

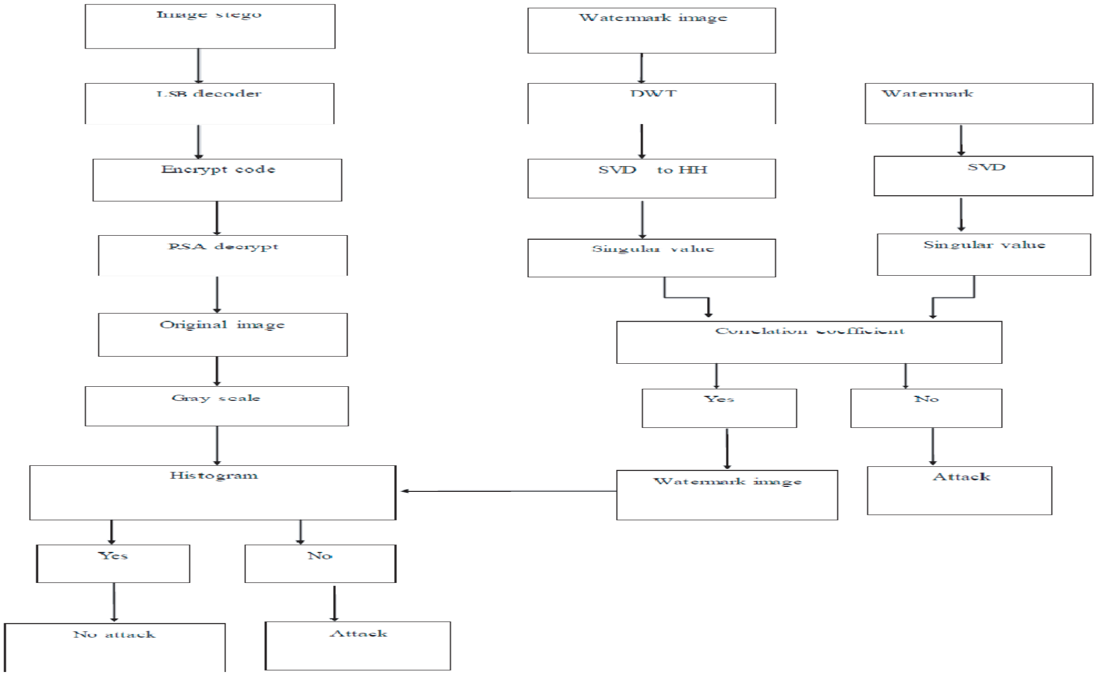


Figure 3: Image verification system received.

4. SIMULATION RESULTS

The results show the encryption and the hiding of the original image, the encrypted image using RSA algorithm but RSA algorithm take long time to encrypt the image as encrypted number. So, we use the combined between quantum ideas and RSA algorithm to speed up the encryption of the image. In Table 1, we test 10 images of different sizes. The experiment shows that to encrypt the image has become a very few when the combined between quantum ideas and RSA algorithm Compared to using the RSA algorithm only.

Then another image represents the cover image to hide the encrypted image to get the hiding image embedded in the cover image these called the original test image, the watermark logo, and the Watermarked image.

The correlation coefficient (CC) is widely used in Pattern reorganization and image processing methods [11]. The correlation coefficient has the value one if the two images are absolutely identical, has the value zero if the two images are completely uncorrelated, and has the value negative one if they are anti-correlated. It is used to compare the two images taken at different times.

Table 1: The processing time of RSA algorithm and quantum RSA algorithm.

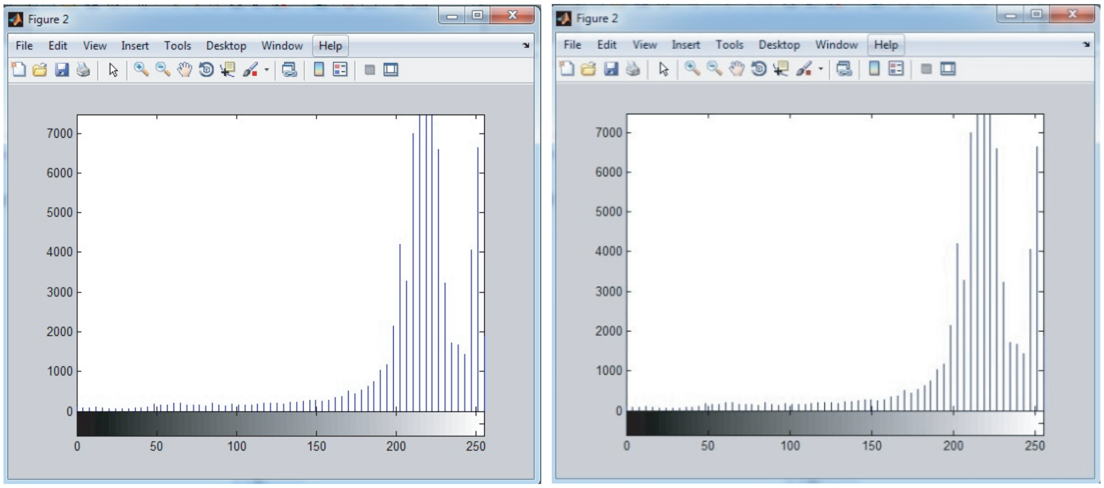
Image	**Size (K byte)**	**RSA algorithm Time (second)**	**Quantum and RSA algorithm Time (second)**
1	35	7.96	0.67
2	38.9	11.23	0.78
3	25.3	11.60	0.46
4	33.7	8.25	0.62
5	41.3	11.98	0.76
6	37.4	10.09	0.78
7	53	19.34	1.15
8	75.2	35.88	1.96
9	83	41.75	2.50
10	103	64.96	4.49

The correlation coefficient value indicates that image has been altered or moved. Table 2 shows the correlation coefficient (CC) between the original watermark and received watermark. In our experiment, it is closer to 1 it means it is identical images.

Table 2: Correlation coefficient between the original watermark and received watermark.

Test	**Correlation coefficient (CC)**
1	0.9994
2	0.9977
3	0.9988
4	0.9993

The histogram analysis clarifies how pixels in an image are distributed by plotting the number of pixels at each intensity level. The Fig. 4(a) shows the histogram of the decrypted image and the Fig. 4(b) shows the histogram of the watermark image. From the histogram diagrams it is observed that the figures are quite similar and the difference is insignificant which the human eye cannot easily differentiate [12]. The histogram of decrypted image contains large sharp rises followed by sharp declines as shown in Fig. 4(b).



(a)

(b)

Figure 4: The histogram of the images. (a) The histogram of the decrypted image. (b) The histogram of the watermark image.

5. CONCLUSION

The objective of this paper is the achievement of the processes of authentication and integrity of the image sent. In this paper, we proposed the encryption of image using RSA algorithm with quantum computing ideas. After that the encrypted code is included in the cover image. Digital watermark scheme is very important to complete the authentication process. Therefore, we use DWT and SVD to get digital watermarking image for the image. We will verify of singular value decomposition for the watermark and histogram for image for both the sender and receiver. Results showed accelerate the encryption process using RSA with quantum ideas compared with RSA only. This model maintains the image quality is good.

REFERENCES

1. Chandrakar, N. and J. Bagga, "Performance comparison of digital image watermarking techniques: A survey," *International Journal of Computer Applications Technology and Research*, Vol. 2, No. 2, 126–130, 2013.
2. Lakhtaria, K., "Protecting computer network with encryption technique: A Study," *Int. J. U-E-Serv. Sci. Technol.*, 44–51, 2011.
3. Madanan, A. and S. Poornachandra, "Comparative study on watermarking & image encryption for secure communication," *International Journal for Trends in Engineering & Technology*, Vol. 5, No. 1, 2015, ISSN: 2349-9303.
4. Taki El_Deen, A. E., E.-S. A. El-Badawy, and S. N. Gobran, "Digital image encryption based on RSA algorithm," *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, Vol. 9, 69–73, 2014.
5. Chandel, G. S. and P. Patel, "Image encryption with RSA and RGB randomized histograms," *International Journal of Advanced Research in Electrical*, Vol. 3, 2014.
6. Odeh, A., K. Elleithy, M. Alshowkan, and E. Abdelfattah, "Quantum key distribution by using public key algorithm (RSA)," IEEE, 2013.
7. Poonia, S., M. Nokhwal, and A. Shankar, "A secure image based steganography and cryptography with watermarking," *International Journal of Emerging Science and Engineering (IJESE)*, Vol. 1, 2013, ISSN: 2319-6378.
8. Bandyopadhyay, T., B. Bandyopadhyay, and B. N. Chatterji, "Image security through combined watermarking and encryption techniques," *International Journal of Electronics & Communication*, Vol. 1, No. 2, 2013.
9. Wang, Y., "Quantum computation and quantum information," *Statistical Science*, Vol. 27, No. 3, 373–394, 2012.
10. Patrzyk, B., "Review, analysis, and simulation of quantum algorithms in cryptography," AGH University of Science and Technology in Kraków, 2014.
11. Sirmou, S. and A. Tiwari, "A hybrid DWT-SVD based digital image watermarking algorithm for copyright protection," *International Journal of P2P Network Trends and Technology (IJPTT)*, Vol. 6, 2014.
12. Bandyopadhyay, T., B. Bandyopadhyay, and B. N. Chatterji, "Image security through SVD based robust watermarking and compression techniques," *International Journal of Emerging Trends & Technology in Computer Science*, Vol. 1, No. 3, September–October 2012.