Int. J. Nonlinear Anal. Appl. 12 (2021) No. 2, 1725-1734
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2021.5312

Application of modify RSA cryptography and randomly LSB steganography on color images of fluid flow in a channel

Hatem Nahi Mohaisen[a,*], Awad Kadhim Hammoud[b]

[a] *Ministry of High Education and Scientific Research, Applied Mathematics, Baghdad, Iraq*
[b] *Univesity of Information Technology and Communication, Baghdad, Iraq*

(Communicated by Madjid Eshaghi Gordji)

Abstract

This paper introduces a combination of three methods including a modified RSA cryptography, hidden text using steganography, and selection of random pixel from image to improve the general security level of the system. In this regard, the image is a carrier of the information transmitted through the media, and the fluid motion image is used to hide the information after it was encoded using modify RSA technique that before hiding it in a random way, because the image of fluid motion possesses the sinusoidal waves and turbulent motion. In this paper, a combination of three techniques is utilized in order to prevent the intruders and attackers from detecting the information and sharing it with others. LSB technique is used for hiding the message in image-based steganography. In addition, pseudo number to choose the random number of pixel when hiding the message after encryption. Four measures including Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM), and histogram are used to compare the original image and stego-image. The results demonstrated the outperformance of the proposed method so that neither the attacker nor the intruder could discover the information contained within the image, due to the large value of the PSNR, very small value of the MSE, stability of the SSIM, and matching the histograms.

Keywords: Steganography, PSNR, MSE, SSIM, Information hiding, Modified RSA cryptography, Seed number, Histogram.

[*] Corresponding author

Email addresses: ha19652010@yahoo.com (Hatem Nahi Mohaisen), Awadkadhim@uoit.edu.iq (Awad Kadhim Hammoud)

Received: February 2021 *Accepted:* June 2021

1. Introduction

Most of the systems in the world suffer from the intervention of attackers or intruders, and they change or tamper with the important information transmitted through those systems. To solve these problems, a lot of researchers have devised many ways to avoid these problems and prevent them from revealing and tampering with information. Cryptography and Steganography are the most well-known methods used to maintain the important information during transmission. An inclusion algorithm for concealment encrypted messages in non-contiguous and random pixel positions in edges and smooth regions of images [11]. Cryptography encoding and using suitable key, while the steganography is a method hiding information in the media [21, 13, 18]. Using hash function to generated modality for concealment data into LSB of RGB pixel values of the carrier media [10]. Using two versions of the suggested algorithm, named standard LSB and Condition Based LSB, the standard LSB version beat on the second suggested version [17]. A Mixed steganography and encryption technique is implemented on the time domain in which at the beginning, image encryption of the secret handwritten signature is done using RSA, then randomly enters in the last three bits dependent to mathematical randomized [22]. Combining phases of cryptography techniques: DNA algorithm, GZIP algorithm, AES and image, multiplying by laborer along the last phase of DNA encryption, LSB image steganography technology is used to conceal the encrypted letter in a high-quality image steganography [4]. Another method used image encryption scheme based on Lorenz hyperchaotic system and RSA Algorithm [16]. a new asymmetric image encryption scheme depended on the RSA algorithm and Arnold transformation, First, the asymmetric public key of RSA algorithm is utilized to generate the premier values for a quantum logistic chart. Second, the parameters of the Arnold chart are calculated. Then, Arnold creeping operation is procedure on the normal image to investigate the rough concealment of image information. Third, each column and each row of the image are possessed as various units respectively and then exclusive-OR (XOR) diffusion is applied [23]. Another approach is combining steganography and cryptography via concealment secret message in color image [13]. Combining human skin-color offer along with the LSB algorithm which can select the inclusion areas is another alternative. This idea is based on the fact that the Human Vision System (HVS) inclines to focus its notice on choosing certain structures of the visual sight instead of the whole image [20]. Another approach is based on data transfer department and data extraction department. In data transfer department, secret data is encrypted using RSA technique or algorithm mean while preprocessing of carries image is implemented and knight tour technique is used to make path for knight [6]. Another method studied hiding secret data into grayscale digital image. It benefits of combining the RSA encryption with steganography technique. This approach depends on searching for congruent bits - two by two bits - between the secret data bits and image pixel values. In case the bits are non-congruent, it hides the secret data bits at drag least significant bits (LSB). Using two kind of images are for applying the steganography technique, one is bright grayscale image and the other is dark grayscale image [5]. ST_R-indicator steganography algorithm for embedding data depends on the LSB, utilize benchmark RGB images as a cover media where each pixel is represented by three bytes (red, green, blue) in pixel [2]. Architecture expanded visual cryptographic sketch for color images utilized Arnold Mapping to certain that the partner pixels are quite scrambled and the random diffusion quite scrambled to elimination any engagement with the premier image contents, thus it improved the security [3]. This paper presents a new method to prevent the attackers, intruders and cryptanalysis to access, tamper or alter confidential data. We used three methods, cryptography (modify RSA), randomization of the selected pixel and hiding method (i.e. steganography).

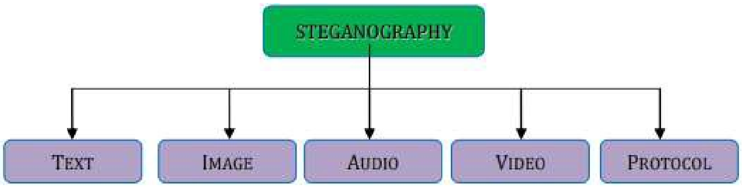


Figure 1: Data types of steganography [22]

2. Preliminaries

2.1. RSA cryptography

RSA encryption/decryption is used in defense, banking and internet transactions and different application. One of the first and the most widely used algorithms for public-key encryption is RSA. this algorithm is derived from the researchers named Ron Rivest, Adi Shamir and Leonard Adleman, who published it in 1977 during working at MIT institute. The RSA is commonly used to generate the public-key encryption and decryption [17]. The RSA algorithm is asymmetric. It is possess two keys: public and private keys. Then, it follows five step for key generation process:
1. Choose two large prime numbers (p and q).
2. Compute $n = p \times q$.
3. Calculate $\Phi(n) = (p-1) \times (q-1)$.
4. Choose an integer e such that $1 < e < \Phi(n)$, and:
(a) Ensure that $gcd(e; \Phi(n)) = 1$.
(b) Ensure that e and $\Phi(n)$ are coprime.
5. Compute an integer d, such that $d = e^{-1}\ mod\ \Phi(n)$.

We can use both generated asymmetric keys in the encryption and decryption. The private key consists of (d), and public key consist of (n,e). $Kpublic = (e, n)$, $Kprivate = (d, n)$ [7].

2.2. Pseudo-random number generator

Generating random numbers as "keys" to the most cryptography basics is a challenging task for computers. A function of pesudo-random number generator, once provided by an initialized random seed, produces a sequence of random numbers which means that an observer who does not know the value of seed number cannot recognize the result from random bit generation [12]. To generate random set from the pixels, the Linear Congruential Random Number Generator (LCRNG) first proposed by Lehmer [14] is applied. the LCRNG is one of the most common techniques to generate a sequence of random numbers $x_0, x_1, \dots$ in range $[0, n-1]$. The seed number is x_0. Every consecutive random number x_{i+1}

$$x_{i+1} = q \times x_i + z\ mod\ n \tag{2.1}$$

where q is constant multiplier, z is the increment, and n is modulus.

2.3. LSB Steganography

The word Steganography is originated from the Greek word "steganos" which means covered or secret and "graphy" which means writing or drawing. The goal of the steganography is to hide secret data inside the transmission media so as to prevent the enemy from discovering the presence of a secret message inside that media. Steganography can be applied to many types of data including audio, video, and images and it can hide any kind of digital information. The data types of steganography are shown in Figure 1 [8]. LSB is one of the simplest techniques in spatial domain image steganography [23]. It is easy to concealment and easy to enforcement by the following algorithm. The ploy behind

data inclusion is to simply alter the last bit value of pixel of the carrier media with the message. See the example bellow:
Image file bit: 10101101 11001010 10111010 01011001
Message: 0010
Stego Image: 10101100 11001010 10111011 01011000
Later, some expanded of this technique has been suggested, implemented by several researchers. A study [1] shows that bit replacement can also be done on the 6th, 7th, 8th bit and even on the combination of them.

2.4. Fidelity Measure

This sort of measures is used to guess the difference level between the original image and the stego-image. The most famous measures are as follows [19]:

2.4.1. Mean Square Error(MSE)

It is the mean of the square error of two images:

$$MSE = \frac{1}{RC} \sum_{y=1}^{c} \sum_{x=1}^{R} (f_0(x,y) - f_e(x,y))^2 \tag{2.2}$$

2.4.2. Peak Signal to Noise Ratio (PSNR)

The values PSNR are used to compare between the original and stego- images, this values are measure the ratio of distortion, and determined by two equation(3,4):
A- in color image the equation is:

$$PSNR = 10\log_{10}(\frac{(\max_{xy} f_0(x,y) - \min_{xy} F_e(x,y))^2}{MSE} \tag{2.3}$$

B- In gray scale image

$$PSNR = 10\log_{10}(\frac{(252^2)}{MSE} \tag{2.4}$$

where f_o is original, f_e embedded image, $\max_{xy} f_0(x,y) = 255$ and $\min_{xy} f_e(x,y) = 0$.

2.4.3. Structural similarity index measure (SSIM)

A modern measure such as Structural Similarity Index Metric (SSIM) can supply a show comparison along with MSE and PSNR. The high SSIM close to one indicates more similarity. SSIM can be calculated by (5):

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + n_1)(2\sigma_{xy} + n_2)}{(\mu_x^2 + \mu_y^2 + n_1)(\sigma_x^2 + \sigma_y^2 + n_2)} \tag{2.5}$$

Where σ is standard deviation, μ is the mean intensity, constants n_1 and $n_2 > 0$ are used to assure stability when other parameters approximated to 0's.

3. Modify RSA and structure system

We proposed a new system using a modification of the RSA algorithm, when multiplying the standard RSA equation by integer number in case of encryption and divided by the same number in

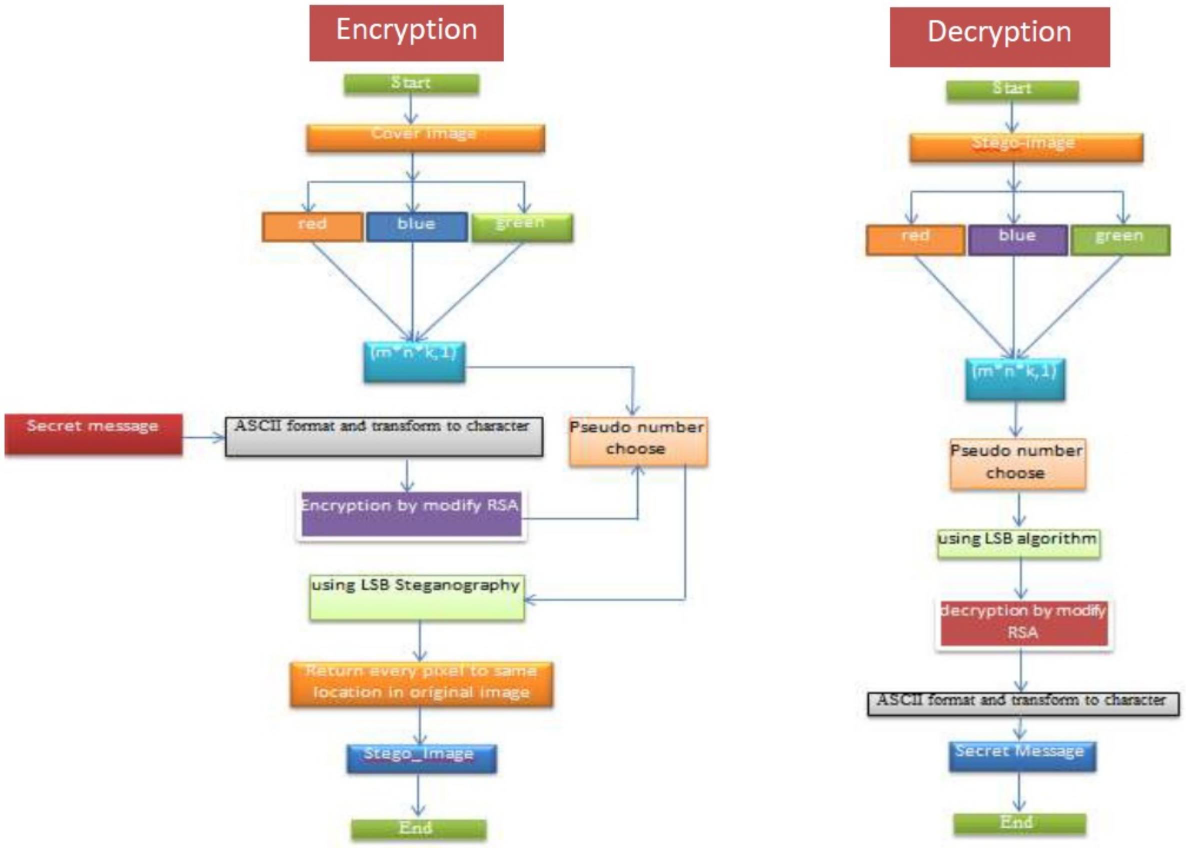


Figure 2: The encryption and decryption flowchart

case of decryption, and this number consider another key added to the private and public key. E is the cipher-text produce in equation (**??**), now, the equation of RSA becomes:

$$E = (M^e \ mod\ n) \times B \tag{3.1}$$

where B is a positive integer. The equation of decryption becomes in equation (3.2).

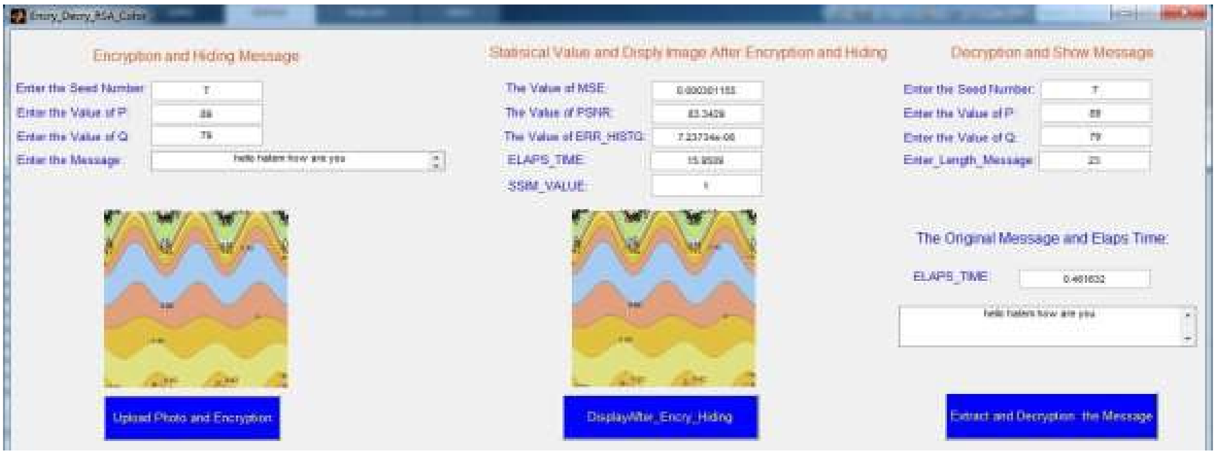
$$M = (\frac{E}{B})^d mod\ n \tag{3.2}$$

The main structure of the proposed system is illustrated in Figure 2.

4. Proposed method

The proposed method is applicable to color images. it is explained by two algorithms (i.e. encryption, decryption). Applying this algorithm on the color image represented the fluid move within a channel. The separation of image cover, encryption, embedded secure data, decryption and extract secret data clearly are explained in algorithms 1 and 2:

Algorithm 1 (sender part)
Input: B integer number, p, q, message, seed number and cover image $(m, n, 3)$.
Output: stego-image.



Encry_Decry_RSA_Color

Encryption and Hiding Message

Enter the Seed Number: 7
Enter the Value of P: 89
Enter the Value of Q: 79
Enter the Message: hello hatem how are you

Statiscal Value and Disply Image After Encryption and Hiding

The Value of MSE: 0.000301155
The Value of PSNR: 83.3429
The Value of ERR_HISTG: 7.23734e-06
ELAPS_TIME: 15.9599
SSIM_VALUE: 1

Decryption and Show Message

Enter the Seed Number: 7
Enter the Value of P: 89
Enter the Value of Q: 79
Enter_Length_Message: 23

The Original Message and Elaps Time:

ELAPS_TIME: 0.461632

hello hatem how are you

Upload Photo and Encryption
DisplayAfter_Encry_Hiding
Extract and Decryption the Message

Figure 3: The frontage of the suggested system

A- Cover image.
B- Convert message to ASCII format.
C- Apply equation (3.1) to encryption message.
D- Compute length of the cipher text.
E- Split the cover image to the one dimension $(m \times n \times 3, 1)$ with an index of each pixel.
F- Apply equation (2.1) using seed number to obtaining the random pixel from step (E) dependent on the length of cipher text.
I- Apply LSB steganography to hiding into random pixel chooses from (F).
J- Return every pixel to the original location dependent on the index of the cover image.
K- Converting the one dimension of cover image into three dimension $(n, m, 3)$ to rebuild the Stego-image.
L- output stego-image.

Algorithm 2 (Receiver part)

Input: B integer number, p, q, message, seed number and stego-image $(m, n, 3)$
Output: secret message.
A- stego-image.
B- split the stego- image to the one dimension $(m \times n \times 3, 1)$.
C- apply equation (2.1) and using the same seed number from sender and the length of message.
D- apply LSB to extract the secrete data from pixel chooses from (C).
E- apply equation (3.2) using the same B, p and q to obtained the ASCII format of message.
F- convert the ASCII to the character.
I- secret message.

5. Experiments and Results

The proposed system was implemented on a computer with CPU AMD $E-300$, HD Graphics 1.3 GHz, RAM 2.00 GB, with Window 7, and using MATLAB 2014a software. the system was applied on BMP images as cover images. The frontage of the suggested system is shown in Figure 3. The results show that the proposed algorithm achieves an important security. The results show that the suggested algorithm fulfill a serious security notes the figures 4-10, and the values of fidelity measures are summarized in Table 1.

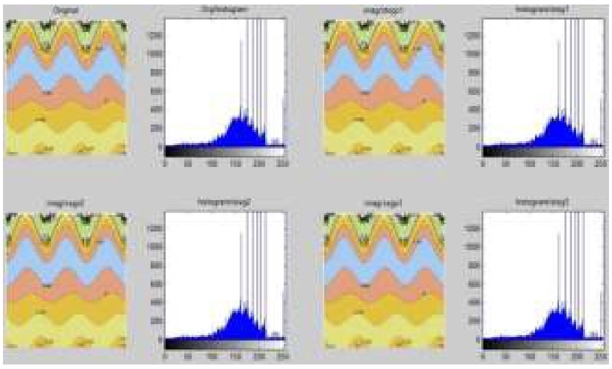


Figure 4: Image 1 with different length message

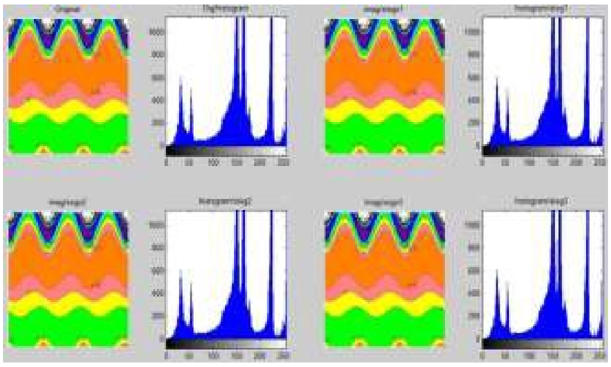


Figure 5: Image 2 with different length message

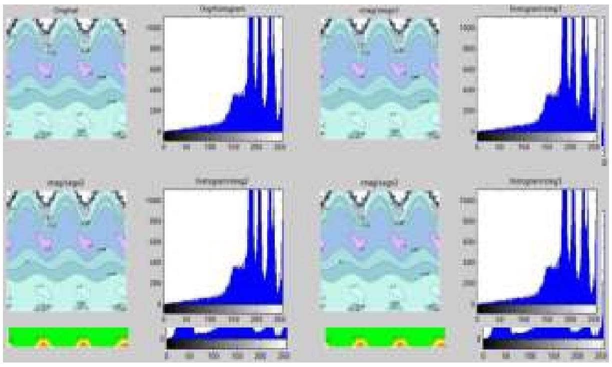


Figure 6: Image 3 with different length message

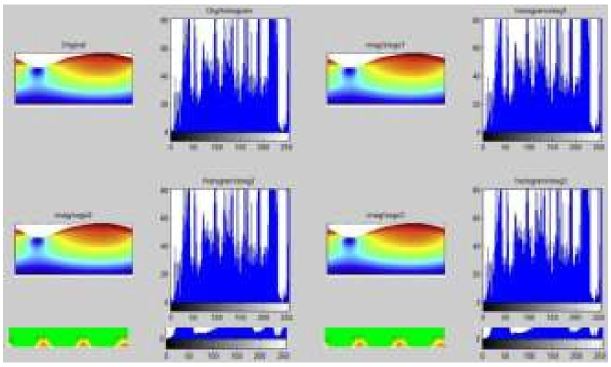


Figure 7: Image 4 with different length message

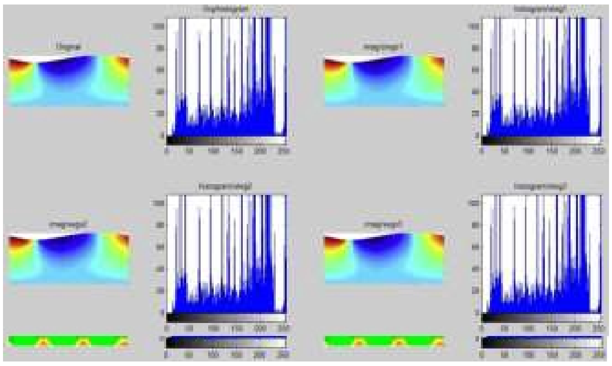


Figure 8: Image 5 with different length message

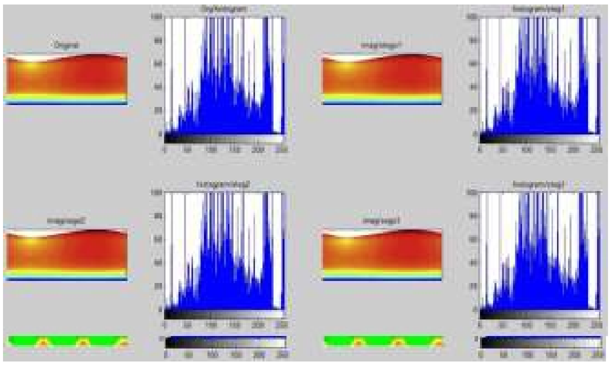
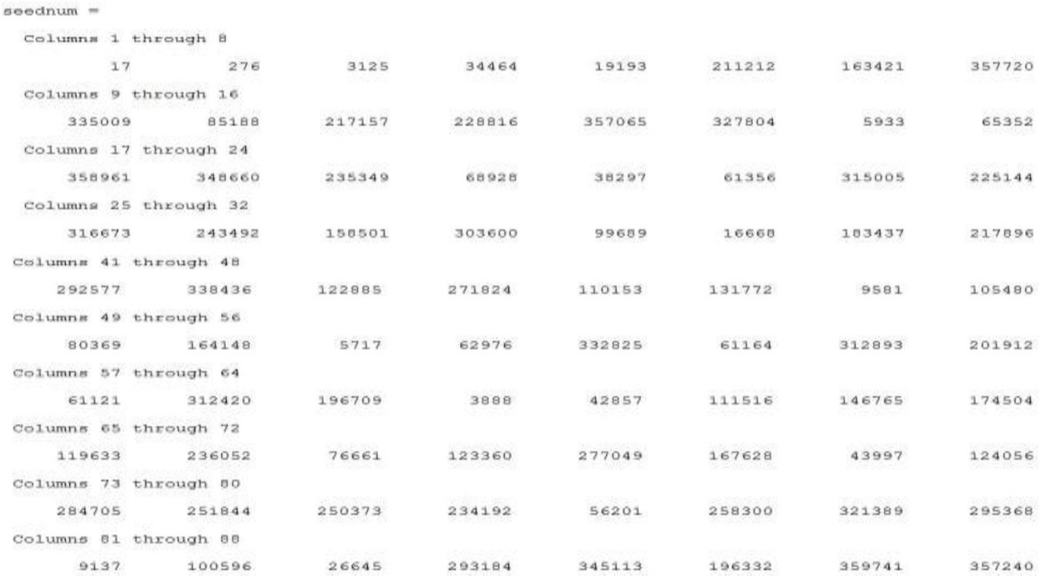


Figure 9: Image 6 with different length message

The images from figure 4, 5, and 6 represented the cross section of moving fluid into channel, and images from figure 7, 8, and 9 are cross section of moving fluid turbulence move into channel. Taken difference image compression the histogram of the original image with different length message, not the change of shape of histogram is imperceptible change to the beholder. An example of selecting random number from color image of size 400 × 300 of message "hello hatem" for 88 generation of pixels is shown in Figure 10.



```
seednum =
  Columns 1 through 8
         17        276       3125      34464      19193     211212     163421     357720
  Columns 9 through 16
     335009      85188     217157     228816     357065     327804       5933      65352
  Columns 17 through 24
     358961     348660     235349      68928      38297      61356     315005     225144
  Columns 25 through 32
     316673     243492     158501     303600      99689      16668     183437     217896
 Columns 41 through 48
    292577     338436     122885     271824     110153     131772       9581     105480
 Columns 49 through 56
     80369     164148       5717      62976     332825      61164     312893     201912
 Columns 57 through 64
     61121     312420     196709       3888      42857     111516     146765     174504
 Columns 65 through 72
    119633     236052      76661     123360     277049     167628      43997     124056
 Columns 73 through 80
    284705     251844     250373     234192      56201     258300     321389     295368
 Columns 81 through 88
      9137     100596      26645     293184     345113     196332     359741     357240
```

Figure 10: Random numbers selection from image after cryptography of message

NO.image	Length of message	MSE	PSNR	SSIM	Histogram_Error	m*n
1	23	0.000301	83.349	1	7.237E-8	400*404
	40	0.00056	80.6089	1	2.9248E-7	400*404
	53	0.00062	80.1577	1	3.786E-7	400*404
2	23	0.00037	82.4095	1	3.699E-8	399*405
	41	0.0006226	80.186	1	3.9214E-8	399*405
	53	0.000839	78.8904	0.999999	9.3368E-8	399*405
3	23	0.0003237	83.029	1	7.2237E-9	398*401
	41	0.00069	79.734	0.999999	2.685E-8	398*401
	53	0.00089	78.268	0.999999	4.232E-8	398*401
4	23	0.00316	73.131	0.999999	4.683E-7	213*97
	41	0.00513	71.0293	0.999999	1.054E-6	213*97
	53	0.00695	69.7088	0.999999	1.663E-6	213*97
5	23	0.00314	73.157	0.999996	8.676E-7	218*90
	41	0.00433	71.7636	0.999995	2.083E-6	218*90
	53	0.00452	71.58	0.999995	2.156E-6	218*90
6	23	0.0024	73.5	0.999999	3.938E-7	220*96
	41	0.005	71.03	0.999999	8.564E-7	220*96
	53	0.0066	69.9165	0.999999	1.1388E-6	220*96

Table 1: represent the different images with different length messages

6. Conclusions

Notes that using the fluid move images which has strength in terms of intensity of colors and wave gradients and the turbulent movement of waves within the channel, and observing that:
A- Values of $PSNR$ are very high and MSE are very small, as well as the $SSIM$ is close to 1.
B- The histograms of the original and stego-image are almost identical.
C- LSB steganography with randomized choosing pixels from color image as well as modifying RSA were results in a new algorithm which has the ability to block any attackers or intruders.
D- Using modify the RSA by cryptography given the suggested system and inter the alternative make task of attacker or intruder is very difficult to guess the factor which adding to the RSA algorithm, specially enter another element for the algorithm.
E- It is better to choose a proper value for the seed number, p, q, and B, to prevent repeating the number of pixel.
F- The algorithm is provided to the suggested system, secure to concealment any secret data with a guarantee that the image is not distorted even prevent of the attackers or intruders discovering that, and attempt hack it.
H- The proposed system works well, effectively and quickly, despite the weak capabilities of the computer on which the system is implemented.

References

[1] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. S. M. El- Rabaie and G. M. El-Banby, *High security data hiding using image cropping and LSB least significant bit steganography*, Colloq. Inf. Sci. Tech. (2017) 400–404.

[2] Sh. M. Abo Mousa, *LSBs steganography based on R-Indicator*, M.Sc. Thesis, Faculity of Information Technology, the Islamic University-Gaza, 2017.

[3] M. O. Alsadeg Ali, *Visual cryptography scheme for color images using Arnold mapping and modified RSA algorithm*, M.Sc. Thesis, Sudan University of Science and Technology, 2018.

[4] Q. S. Alsaffar, H. N. Mohaisen and F. N. Almashhdini, *An encryption based on DNA and AES algorithms for hiding a compressed text in colored Image*, IOP Conf. Series Materials Sci. Engin. 1058(1) (2021) 012048.

[5] S. O. Alsharkasi, M. M. Elsheh and F. O. Ehtiba, *Evaluation of using steganography technique to hide a text in grayscale digital images*, J. Acad. Res. Appl. Sci. 19 (2021) 1–6.

[6] Ambika, R. L. Biradar, V. Burkpalli, *Efficient approach for steganography using DWT and RSA algorithm*, Int. J. Engin. Adv. Tech. 8(5)(2019) 1435–1443.

[7] S. Asjad, *RSA Algorithm*, University of South-Eastern Norway Campus Kongsberg, (2019).

[8] B. Chitradevi, N. Thinaharan and M. Vasanthi, *Data hiding using least significant bit steganography in digital images*, Statistical Approaches on Multidisciplinary Research, 2017.

[9] M. Evans, *RSA Encryption*, Australian Mathematical Sciences Institute (AMSI), 2013.

[10] R. Halder, S. Sengupta, S. Ghosh and D. Kundu, *A secure image steganography based on RSA algorithm and hash-LSB technique*, IOSR J. of Comput. Engin. 18(1) (2016) 39–43.

[11] M. Juneja and P. S. Sandhu, *An improved LSB based steganography technique for RGB color images*, Int. J. Comput. Commun. Engin. 2(4) (2013) 513–517.

[12] F. Koeune, *Pseudo-Random Number Generator*, In: H. C. A. van Tilborg (eds) Encyclopedia of Cryptography and Security Springer, Boston, MA, 2005.

[13] K. Kordov and S. Zhelezov, *Steganography in color images with random order of pixel selection and encrypted text message embedding*, Peer J. Comput. Sci. 7 (2021) e380.

[14] D. Lehmer, *Mathematical methods in large-scale computing units*, In: U. S. N. D. B. o. Ordnance and H. University (eds) Proceedings of the second symposium on large-scale digital computing machinery, Harvard University, 1951, 141–146.

[15] L. Li, B. Luo, Q. Li and X. Fang, *A color images steganography method by multiple embedding strategy based on sobel operator*, 1st Int. Conf. Mult. Inf. Network. Secur. 2(1) (2009) 118–121.

[16] R. Lin and SH. Li, *An image encryption scheme based on Lorenz hyperchaotic system and RSA algorithm*, Secur. Commun. Networks (Hindawi), 2021 (2021).

[17] S. Manaseer, A. Aljawawdeh and D. Alsoudi, *A new image steganography depending on reference and LSB*, Int. J. Appl. Engin. Res. 12(9) (2017) 1950–1955.

[18] S. Majumder and M. M. Rahman, *Implementation of security enhanced image steganography with the incorporation of modified RSA algorithm*, Int. Conf. Elect. Comput. Commun. Engin. (2019) 1–5.

[19] H.N. Mohaisen, *Secure data hiding technique using steganography and watermarking*, M.SC. Thesis, College of Science, Baghdad University, 2016.

[20] S.A. Naji, H.N. Mohaisen, Q.S. Alsaffar and H.A. Jalab, *Automatic region selection method to enhance image-based steganography*, Period. Engin. Natural Sci. 8(1) (2020) 67–78.

[21] M. E. Saleh, A. A. Aly and F. A. Omara, *Data security using cryptography and steganography techniques*, Int. J. Adv. Comput. Sci. Appl. 7(6) (2016) 390–397.

[22] Y. M. Wazery, S.G. Haridy and A.A. Ali, *A hybrid technique based on RSA and data hiding for securing hand-written signature*, Int. J. Adv. Comput. Sci. Appl. 12(4) (2021).

[23] G. Ye, H. Wu, K. Jiao and D. Mei, *Asymmetric image encryption scheme based on the Quantum logistic map and cyclic modulo diffusion*, Math. Biosci. Engin. 18(5) (2021) 5427–5448.