IJICTR
International Journal of Information & Communication Technology Research

Volume 16- Number 4 – 2024 (1 -8)

Joint Use of RSA and Genetic Algorithm to Improve the Process of Image Encryption and Information Hiding

Ramin Biglou
Department of Electrical Engineering
Islamic Azad University North Tehran Branch
Tehran, Iran
ramin.beglo1375@gmail.com

Mohammad Mirzaei*
Department of Electrical Engineering
Islamic Azad University North Tehran Branch
Tehran, Iran
mohammad.mirzaei@iau.ac.ir

Pedram Hajipour
Satellite Communication Group
Faculty of Communications Technology
ICT Research Institute
Tehran, Iran
Hajipour@itrc.ac.ir

Received: 18 July 2024 – Revised: 2 September 2024 - Accepted: 13 October 2024

Abstract—**In this paper, the combined use of cryptography and information hiding in the image is discussed. First, the RSA method is used to perform encryption information. Secondly, steganography for the encrypted information has been used by genetic evolutionary algorithm (GA). Also, the evolutionary GA is used to find the best bit string length in order to maximize the peak signal-to-noise ratio (PSNR). A graphical user interface (GUI) has been provided to apply the proposed method to sentences of different lengths in four different images to obtain the mean squared error (MSE) and PSNR benchmarks relative to changing the image size and compression rate on the receiving side. In the proposed algorithm, the encryption sentences have been applied 10 times on the data by the proposed algorithm to improve the key strength. The simulation results showed higher efficiency of about 28.57 percent better than normal AES, 15 percent better than DSA, 18.01 percent better than ECC and about 7.76 percent better than RSA.**

Keywords: Robustness, Steganography, Cryptography, Compression rate, Evolutionary algorithm

Article type: Research Article

Publisher: ICT Research Institute

* Corresponding Author

[DOI: 10.61186/itrc.16.4.1]

I. INTRODUCTION

Today, with the increasing development of digital communications and computer science, maintaining security for image, video and other digital information has attracted a lot of attention. Two methods of steganography and cryptography, respectively to maintain the security of this type of information and image protection data is essential. The use of image cryptography differs from text cryptography due to the inherent characteristics of the image, such as the large volume of data and the high correlation between the pixels. For this reason, classical encryption methods are not suitable for use in image encryption [1].

The science of cryptography is looking for ways to encryption messages, and corresponding methods to decrypt them. In general, cryptography includes two categories of symmetric and asymmetric key cryptography. In symmetric key encryption systems, the sender and receiver of the message must know the password. When the sender of a message uses a unique, secret key for encryption and the recipients of the message use the same key to decrypt, disclosing the password through one of the recipients of the message endangers everyone's security. In this case, the sender must define the key to the number of recipients and maintain them, which in turn is a big challenge. The most popular symmetric algorithm is data encryption standard (DES), which is a product of the United States of America (USA) and is now recognized as an international standard and is most commonly used in smart cards and most information security systems. Other symmetric algorithms include advanced encryption standard (AES), Triple DES (3DES) and Rivest Cipher 4 (RC4) [2]. The asymmetric key encryption algorithm uses two completely different keys, including the public key and the private key. Asymmetric key cryptographic systems were introduced by Diffie and Hellman in the late 1970s. One of their main features is that they do not need a secure channel to distribute the key. Therefore, in this type of algorithm, it is no longer possible to deduce a private key by having a public key. In 1978, three people, Ron Rivest, Adam Shamir, and Len Adelman (RSA), introduced an algorithm to implement public key cryptography with a pair of keys (public and private) known as the RSA. This type of algorithm has been widely used over the last three decades and over time, the optimized hardware and software related to this algorithm have been released to the market.

Although, a more powerful algorithm called Elgamal was later developed, the RSA method still tops the list of public key cryptographic algorithms. The RSA method is one of the most common algorithms to encrypt data. This type of algorithm has withstood attempts to break it for about a quarter of a century [1]. Babaei and Pourneshli in 2019 encoded a color image based on Deoxyribonucleic Acid (DNA) algorithm [3]. In this research, a color image encryption system based on dynamic and chaotic DNA encoding is presented, which uses the second perturbation method to increase the security of encryption image.

In this type of algorithm, a proposed super chaotic system is used to provide quasi-random sequences, which make the proposed encryption pattern stronger against attacks. Rajaei and Zeidabadi Nejad in 2013 provided a cryptographic algorithm using the RSA algorithm and the Chinese remainder theorem (CRT). In this research, it is pointed out that one of the disadvantages of using the RSA algorithm is the encryption speed, which uses the remaining CRT theorem to increase the efficiency and speed of the RSA algorithm used [4].

The accuracy of the limitation of chaotic method is one of the challenges of this method in image encryption. In [5], a new solution based on chaos sequence and the wavelet transform provided to improve the image encryption method.

Kaur and Singh in 2018 investigated a randomly selected block encryption method for secure encryption image with the Blowfish algorithm. In 2020, Saffar and et al., encoded images based on AES and RSA algorithms. The aim of this study was to compare advanced encryption AES and RSA) algorithms in encryption image.

Histogram analysis and correlation results in the above paper show that the AES algorithm with convergent columns in the histogram has better image encoding quality. In addition, the correlation coefficient of the AES algorithm is closer to zero [6]. In 2020, Jalal Saddam and et al., addressed lightweight image encryption and Blowfish decryption for Internet of Things (IoT) security. The internet of things (IoT) is expected to connect billions of users as an innovative technology in the future. Increased connectivity is expected to generate extensive data, and data protection could be a threat.

In this research, a light coding algorithm called stable IoT is proposed. The simulation results in [7], show that this type of algorithm provides sufficient protection in only five encryption steps. This algorithm is implemented through hardware with a low-cost 8-bit microcontroller.

Al-Kadei and et al. in 2020, provided accelerated image encryption using the RSA algorithm. In this paper, three experiments are performed to investigate the execution time of the encryption, decryption and compare the results together to extract the improved points and discuss them.

In addition, some programming techniques have been used to speed up the encryption or decryption process. The results show that the execution time of the encryption process in the experiment is improved by 14 percent using some methods to speed up the encryption process, and the decryption process is also improved by 22 percent [8]. In 2020, Liu and et al., introduced an optical image encryption algorithm based on chaos mapping and public key cryptography.

This algorithm provides with the aim of secure transfer and distribution of complex keys in the image encryption system based on optical transformation, an innovative optical image encryption algorithm based on chaos mapping and public key encryption is proposed. The simulation results of the above paper show that the proposed algorithm has high key sensitivity, uniform

[DOI: 10.61186/itrc.16.4.1]

statistical distribution properties and can withstand noise attacks with a magnitude of 0.1. In this type of model, asymmetric encryption and decryption times require only 0.045 seconds and 0.072 seconds, respectively. However, by combining excessive chaos and public key cryptography, key space is increased, key volume and computational complexity are reduced, and ultimately the efficiency of the algorithm is improved [9]. Another method of image encryption is the double random phase encoding (DRPE) method. Because the DRPE method is the same for encryption and decryption keys, this method is considered as a single key or symmetric key encryption system. As a result, when the encrypted image is sent, the key must be transmitted through another secure channel. This method is characterized by very high security and the power to confuse information [10].

As mentioned earlier, another way to increase the security of existing data is information hiding. The information hiding is a method to insert data inside an image so that it is invisible and also cannot be deleted by unauthorized users.

The main purpose of information hiding is to control copyright and authentication. However, the use of information hiding in special and important communications such as sending biographies and military maps on battlefields does not seem appropriate because it does not guarantee their security. Current methods of information hiding focus to increase the amount of confidential information that can be injected into a photo.

In general, information hiding is done in several ways, among which steganography and watermarking methods are more important than others. Steganography is one of the main methods in information hiding. The word is originally derived from the Greek word steganographia, which literally means "covered writing".

Steganography is in fact the art of certain information hiding in other information [11]. Watermarking is a way to increase the security of digital information against unauthorized counterfeiting. In this technique, in order to create protection against forgery of documents and unauthorized copying, specific and limited information is secretly embedded in digital media, including audio, video, video and even digital texts, so that this information is even watermarked at any time. It can be extracted despite noise and non-destructive changes (intentionally or unintentionally)- [11].

In [12], it is mentioned that if an algorithm is able to detect the existence of the message in encrypted format with high probability of success, the steganography system will be broken. In order to protect message, the message is encrypted by one of the encryption methods. Then, the encrypted message is then hidden. Therefore, steganography is used to meet the security needs of cryptography.

A. Main Contribution

In this paper, to obtain more information security, the joint use of cryptography and steganography in the image has been provided.

In the first step, the RSA is used before information hiding and in the second step, the encryption of the information hiding is by GA.

In the proposed method, a GA will be used to find the PSNR. In addition, a new method of hiding information has been introduced based on the combined use of the advantages of DRPE methods and the public key RSA.

Therefore, in the proposed algorithm, DRPE will be used in information turbulence and their stability and a private key based on RSA method will be used to increase security.

For better performance of the proposed method and increase information security, find the direction and starting point in the host image to hide confidential information, the PSNR of the hiding image is maximized.

Therefore, in order to implement the proposed algorithm, two steps are envisaged. In the first step, the required information is hidden in the images using sensor encryption and compression. In the second step, the encryption information is decoded using the decoding operation, the signal and the information encryption are created and a watermark signal is created. This signal is finally decrypted and locked and the information hidden in the image is presented. In this paper, in section 2, the proposed algorithm is provided. Section 3 simulates and compares the results of the proposed algorithm. Section 4 summarizes and offers suggestions for future work.

II. SIMULTANEOUS USE OF DRPE AND RSA FOR IMAGE ENCRYPTION IN THE PROPOSED ALGORITHM

According to Fig.1, in the proposed algorithm, using the combined method of RSA and hiding information from steganography type, the information is hidden in different images. The implementation of the proposed algorithm is based on sub-byte blocks, row transfer, column composition, key rounding, static box and RSA cycle construction, which ultimately leads to data encryption. Finally, to compare the proposed algorithm, the key breaking parameter of the RSA algorithm with other cryptographic algorithms is used.

In the proposed algorithm, the confidential information in the proposed method is in the form of text and this information is embedded in the images after encryption RSA. To encrypt confidential information, there are two steps:

First, the text convert to an array of bits and encrypted. Secondly, the encrypted information becomes an array of bits to apply the information hiding method (steganography).

For this purpose, GA is used to embed encrypted information in the host image. GA is a method of computer science search to find an approximate solution to optimize the proposed algorithm. In GA, first, several answers to the problem are generated randomly. We call this set of answers the initial population. Also, we call each answer a chromosome. Then, using the generators of the GA, after selecting the better chromosomes, we combine the chromosomes and make a mutation in them.

[DOI: 10.61186/itrc.16.4.1]

Finally, we combine the current population with the new population resulting from the combination and mutation on chromosomes [13].

In order to implement the optimized RSA algorithm according to Table 1, the following functions have been implemented in the content program inspired by GA, the performance of each of which is presented in the proposed method.

In this paper, in order to evaluate the proposed encryption system, four different images have been used and the desired messages have been applied to the proposed images by the proposed method.

Finally, by comparing the image quality and compression rate and their effect on the hiding capacity, mean squared error (MSE) and PSNR are obtained for all 4 proposed images and compared with each other.

Hiding capacity is equal to the amount of bytes of hidden image information to the extent that the quality of the image is not lost [14].

In the proposed algorithm, the MSE parameter is used to quantitatively compare the difference between two images, the value of which will be in accordance with Equation (1)[15].

$$MSE = \frac{1}{M \times N} \sum_{m=1}^{M}\sum_{n=1}^{N}[\mathrm{Im}age_{changed}(m,n) - \mathrm{Im}age_{originial}(m,n)]^2 \quad (1)$$

In the above relation, M × N is the image size.

M is the number of rows and N is the number of columns of the selected image. $\mathrm{Im}age_{changed}(m,n)$ is changed image and $\mathrm{Im}age_{original}(m,n)$ is main image. It is clear that increasing MSE means reducing image quality. The next parameter in the proposed algorithm according to Equation (2) is PSNR which reveals the quality of image. As you can see, PSNR is inversely related to MSE [16].

$$PSNR = 10 \times \log_{10}\left(\frac{\max(\mathrm{Im}age_{originial}(m,n))^2}{MSE}\right). \quad (2)$$

In Equation (2), $\max(\mathrm{Im}age_{originial}(m,n))$ is the maximum image size.

I. Simulation Results of the Proposed Algorithm

In order to evaluate and present the simulation results of the proposed algorithm, as mentioned in reference [1], a text will be generated first. This text contains the message "vijay how r u?" It is hidden in several different images and the amount of MSE and PSNR of each image is determined after encoding for encryption. Fig.2 shows the four images in which we intend to merge and hide the message. It should be noted that in this article, MATLAB software version 2019 has been used for coding. It also uses a system with 5-core processor power and 8 GB of RAM.

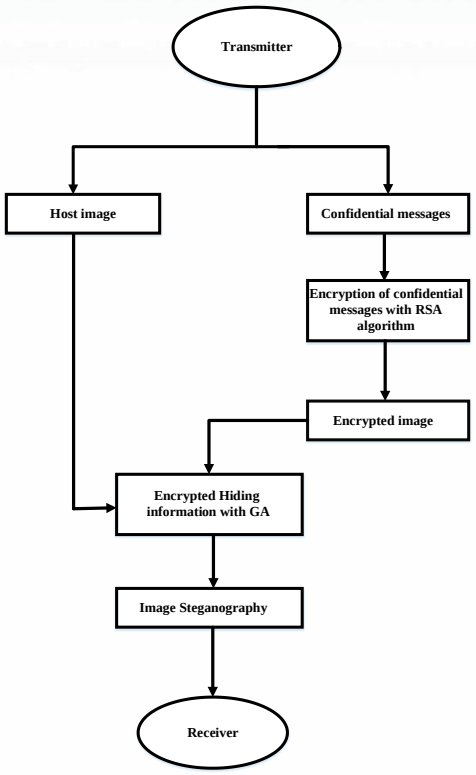
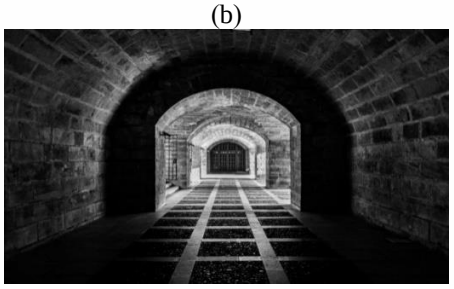


Figure 1. Flowchart of the proposed algorithm

(a)

(b)



(c)

[DOI: 10.61186/itrc.16.4.1]

(d)

Figure 2. Images used in the proposed algorithm [1]

In the proposed algorithm, first the desired message is "vijay how r u?" Converts to binary code. In the next step, the generated binary codes will be encrypted. Fig.3 shows some of these generated passwords for the message.

TABLE I. DEFINED FUNCTIONS TO IMPLEMENT THE PROPOSED ALGORITHM

Performance	Function	Num.
This function is repeated periodically.	Sub.Byte	1
	Shift Row	2
	Mix.Column	3
	Add Round Key	4
The 16 input bytes are replaced according to a fixed table according to the design.	Provide a fixed table	5

accihbidjixxxxxedefjchxxxxxxxfcgddxxacddfabcghxxxxxedefjc
hxxxxxxxfcgddxxacddfabcghxxxxxedcifedxxxxxxxfchgbxxacci
hbidjixxaccihbidjixxxxxedefjchxxxxxxxfchgbxxaccihbidjixxxxx
edcifedxxxxxxxfcgddxxacddfabcghxxxxxedefjchxxxxxxxfcgdd
xxaccihbidjixxaccihbidjixxxxxedefjchxxxxxxxfchgbxxaccihbidji
xxxxxedcifedxxxxxxxfcgddxxaccihbidjixxxxxedefjchxxxxxxxfc
hgbxxacddfabcghxxacddfabcghxxxxxedcifedxxxxxxxfchgbxxa

Figure 3. Encrypted message "vijay how r u?"

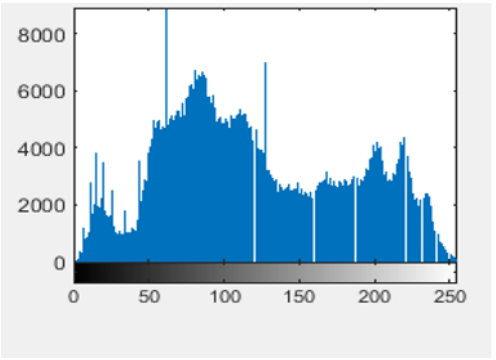
In the next step, select the image in which we intend to integrate the message to generate the desired image hiding using the combined steganography method. As an example in Fig.4, for image (1), the original image and the stegano image generated after merging the encrypted message are presented. Image (a) is the original image and image (b) is the stegano image.

(a)

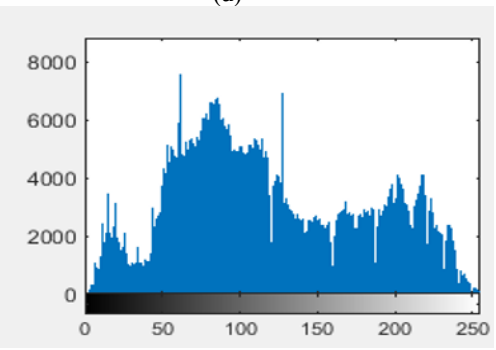
(b)

Figure 4. The main image (a) and hidden image (b)

The difference between two images can be compared by showing the histogram distribution in the programming code.
The histogram distribution shows the changes made in the image, which is the same as applying encrypted text to an image. Fig.5 shows these changes in the original and hidden image.



(a)



(b)

Figure 5. Histogram of the main image (a) and its inverted image (b) based on the number of pixels

According to Fig.6, the hiding capacity is 1534 bytes, the PSNR is 49.9085 and the MSE is 0.4702727. The results obtained for the proposed algorithm and all the images specified in Fig. 2 are presented in Table 2.
Now if the above items for the phrase "The weather is cold. Be careful Tommy" are presented again in Table 3.

[DOI: 10.61186/itrc.16.4.1]

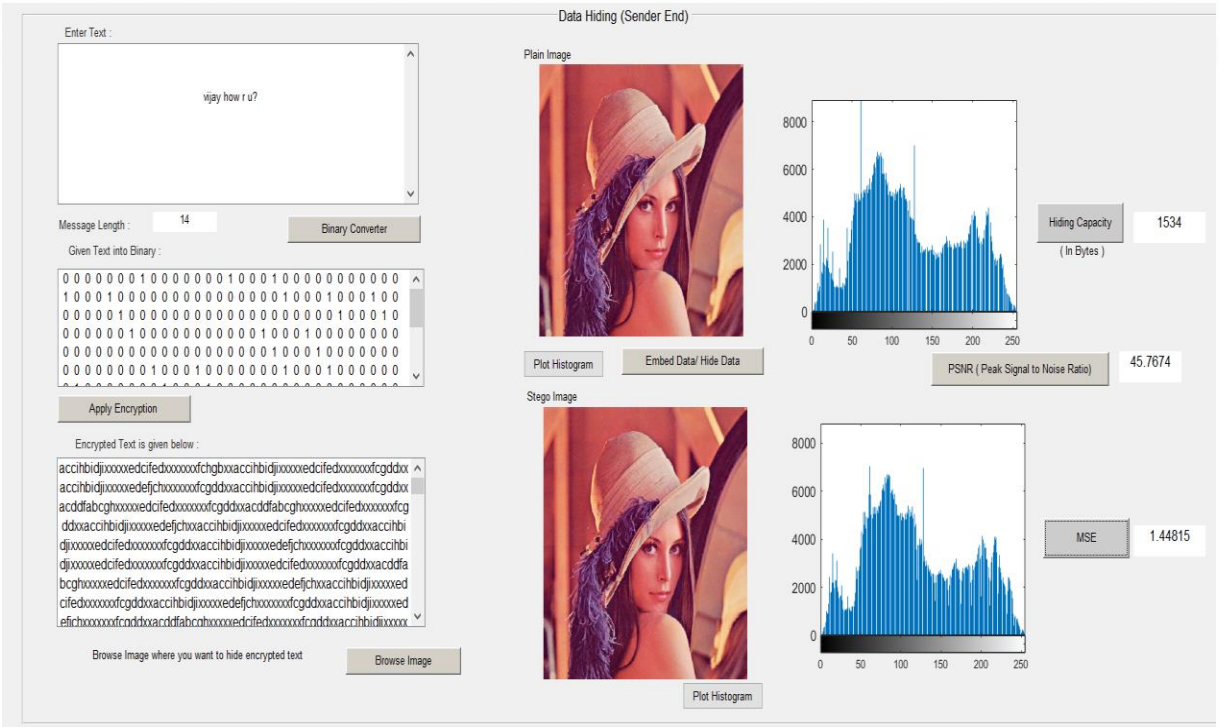


Figure 6. Capacity, PSNR and MSE in the proposed algorithm based on the number of pixels

TABLE II. THE PERFORMANCE OF THE PROPOSED METHOD IN DIFFERENT IMAGES WITH DIFFERENT QUALITIES

Image name	Image value	Hiding capacity (bytes)	PSNR (dB)	MSE
Picture number one	512×512×3	1534	49.9085	0.427027
Picture number two	1920×1200×3	5758	56.6646	0.0484151
Picture number three	4256×2832×3	12766	56.5987	0.0477329
Picture number four	600×600×3	1798	58.5624	0.041363

TABLE III. PERFORMANCE OF THE PROPOSED METHOD IN DIFFERENT IMAGES WITH DIFFERENT QUALITIES FOR SENTENCES WITH LONGER LENGTHS

Image name	Image value	Hiding capacity (bytes)	PSNR (dB)	MSE
Picture number one	512×512×3	1534	52.1122	0.172245
Picture number two	1920×1200×3	5758	55.4884	0.08977
Picture number three	4256×2832×3	12766	55.4979	0.0897788
Picture number four	600×600×3	1798	53.0226	0.269321

TABLE IV. EFFECT OF COMPRESSION RATE ON MSE AND PSNR

MSE related to the image	MSE related to the text	PSNR (dB)	Compression rate
0.001725	0.02415	54.63	60
0.002786	0.02266	55.41	75
0.004582	0.01725	57.96	90
0.000869	0.01241	58.69	100

[DOI: 10.61186/itrc.16.4.1]

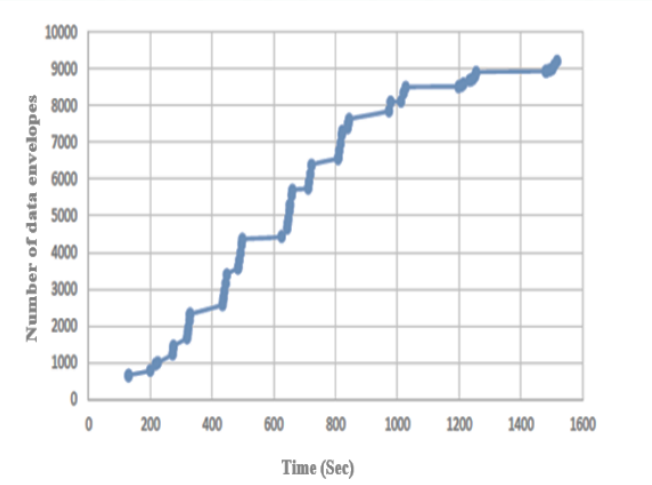


Figure 7. Breaking time of the proposed algorithm key with AES algorithm

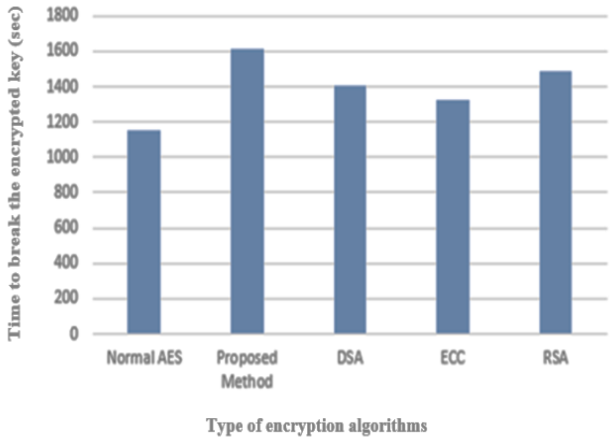


Figure 8. Comparative diagram of time to break the encryption in the proposed algorithm and other cryptographic algorithms [18-19]

Experimenting with all four images, the simulation results show that as the sentence length increases, the MSE error rate increases and the PSNR decreases. In addition, the effect of compression rate on PSNR, MSE text and MSE is shown in Table 4. In Table 4 Compression rate is the number of pixels remaining after compressing the original image [17].

As shown in Fig.7, the breaking time for key increases according to the number of data packets in the proposed algorithm. This indicates that the larger the data volume, the more time must be spent breaking the proposed algorithm.

Fig.8, shows the breaking time of the encrypted key of the proposed algorithm with other existing algorithms. It is clear that the proposed method takes longer than the encryption key to break. In particular, the proposed method had a higher ability of about 420 seconds (35.59 percent) to increase the strength of the encrypted key on the data.

Based on Fig. 8, it is concluded that in the proposed algorithm, the performance of the data encryption power in the images has increased due to the key being broken. Therefore, it can be argued that the proposed algorithm is about 28.57 percent better than conventional AES, 15 percent better than DSA, 18.01 percent better than ECC algorithm and finally about 7.76 percent better than conventional RSA.

II. CONCLUSION AND FUTURE WORKS

The simulation results in this paper show that the integrated RSA-based encryption algorithm has been able to improve the shortcomings of the previous methods and to operate significantly in the field of cryptography. According to the obtained results of the proposed algorithm, the length of the initial sentence increases, the amount of MSE increases and the amount of PSNR decreases. On the other hand, the hiding power of the proposed algorithm has been improved compared to other existing models.Therefore, the use of this type of proposed algorithm in hardware implementation is very important in order to reduce production costs, increase operational capacity and reduce power consumption.In order to continue this research, some solutions can be suggested as follows:

[DOI: 10.61186/itrc.16.4.1]

1- Determining the energy gradient of the blocks to increase the resistance.
2- Selection of blocks with more brightness to insert the brand,
3- Using the parameters of mathematical models for marking.

REFERENCES

[1] V.K Sharma, P.Mathur, DK.Srivastava, "Highly secure DWT steganography scheme for encrypted data hiding, " Information and Communication Technology for Intelligent Systems,vol.1, pp. 665-673, 2019.

[2] A.Gupta, S.Gupta, and N.Yadav, "Enhancement of security using B-RSA algorithm, " Inventive Communication and Computational Technologies, pp.439-450, 2020.

[3] M.Aghababaei and S. Jafarpourneshli, "Color Image Encryption Based on DNA Algorithm, " 5th National Conference on Electrical and Mechatronic Engineering of Iran, Tehran, https://civilica.com/doc/988464,pp.1-20, 1398.

[4] M.Rajaei and S.Zeidabadi Nejad, "Cryptography Using RSA Algorithm and the Remaining Chinese Theorem, "5th National Conference on Electrical and Electronic Engineering of Iran, Gonabad, https://civilica.com/doc/219747, 2013.

[5] Y.Pourasad, R.Ranjbarzadeh, A.Mardani, "A new algorithm for digital image encryption based on chaos theory, " Entropy, vol.23,no.3,pp.1-16, 2021.

[6] A.Kaur and G. Singh , "A random selective block encryption technique for secure image cryptography using blowfish algorithm, " 2th International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 1290-1293, 2018.

[7] M.J.Saddam, A.I. Abdullahi and A.Hamid Mohammed, "A Lightweight Image Encryption And Blowfish Decryption For The Secure Internet Of Things, " 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT),pp.1-5, 2020.

[8] F.H. Mohammed Sediq Al-Kadei, H. Abdalkaream Mardan and N. A. Minas, "Speed Up Image Encryption by Using RSA Algorithm, " 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1302-1307, 2020.

[9] Y.Liu,Z.Jiang,X.Xu,F.Zhang and J.Xu, "Optical image encryption algorithm based on hyper-chaos and public-key cryptography, " Optics and Laser Technology, vol.127,no.7,pp.1-10, 2020.

[10] Z.Xin, L.Dong, Y.Sheng, L.Da-hai, H.Jian-Ping, "A method for hiding information utilizing double random phase encoding technique, "Optics and Laser Technology, vol .39,no.7,pp.1360-1363,2007.

[11] S.Katzenbeisser, P.Fabien A.P, "Information Hiding Techniques for Steganography and Digital Watermarking, "Artech House, pp.1-220, 2000.

[12] J.Islampanah, S.N.Razavi, "Presenting a New Method for Image Encryption Using Fuzzy System, " 3th National Congress of New Technologies of Iran with the Aim of Achieving Sustainable Development, Tehran, https://civilica.com/doc/463566, pp.1-19,2015.

[13] M.Mitchell, "An introduction to genetic algorithms, " MIT press,pp.1-209,1998.

[14] MA.Ali, EH.Houssein, NA.Eldemerdash, AE, "Hassanien. Increasing the hiding capacity in image steganography using Braille code, " International Journal of Intelligent Engineering Informatics,vol.5, no.4, pp.327-341, 2017.

[15] X.Zhou, JG.Chen, "Information hiding based on double-random phase encoding technology, " Journal of Modern Optics,vol.53,no.12,pp.1777-1783,2006.

[16] K.Mishra, SK.Singh, P.Nagabhushan, "An improved SVD based image compression, " Conference on Information and Communication Technology (CICT), pp. 1-5, 2018.

[17] A.Alkholidi, A.Alfalou, H.Hamam, " A new approach for optical colored image compression using the JPEG standards, " Signal Processing, vol.87,no.4,pp.569-583,2007.

[18] S.Chandra, S.Paira, S.Safikul Alam and G.Sanyal, "A Comparative Survey of Symmetric and Asymmetric Key Cryptography, " International Conference on Electronics, Communication and Computational Engineering (ICECCE), pp.83–93,2014.

[19] S.Sharifi,M.Esmaeildoust, M. R.Taheri and K.Navi, "Efficient Implementation of RNS Montgomery Multiplication Using Balanced RNS Bases, " Journal of Mathematics and Computer Science (JMCS), vol.12, pp.51–64,2014.

Ramin Biglou received his B.Sc. and M.Sc. degrees in Electrical Engineering from the Islamic Azad University North Tehran Branch,Tehran, Iran. His research interests include: Signal Processing and Image Processing.

Mohammad Mirzaei received his B.Sc. degree in Electrical Engineering from the Khaje Nasir Toosi of Technonlogy,Tehran, Iran in 2005, and the M.Sc. degree in Digital Electronic Systems from Sharif University of Technology,Tehran,Iran, in 2007. He received the Ph.D. degree in Digital Electronic System at Sharif University of Technology. During his M.Sc. study, he worked on the application of world-level canonical decision diagrams to formal verification of arithmetic circuits. His current research interests include the Development of High-Level Design Tools with Emphasis on Testing and Design for Testability.

Pedram Hajipour received his B.Sc. in Communication System Engineering from Yadegar-e-Imam Khomeini (RAH) Shahr-e-rey Branch, Islamic Azad University in 2005 and M.Sc. in Communication System Engineering from Khajeh Nasir-edin-toosi University of technology in 2007, respectively. He also received the Ph.D. degree in Department of Communication, College of Electrical Engineering, Yadegar-e-Imam Khomeini (RAH) Shahr-e-rey Branch, Islamic Azad University in 2017. He is a faculty member of ICT Research Institute (ITRC) since 2014. His research interests include: The Satellite Networks and Intelligent Telecommunication Systems with the Approach of using them in the Fifth and Sixth Generations (5G and 6G) of Communication Networks.

[DOI: 10.61186/itrc.16.4.1]