Beykent Üniversitesi Fen ve Mühendislik Bilimleri Dergisi 2022, 15(2), 77-88
Beykent University Journal of Science and Engineering 2022, 15(2), 77-88

Makale Türü: Araştırma Makalesi
Paper Type: Research Article

Geliş tarihi/Received: 10/05/2022
Kabul tarihi/Accepted: 06/06/2022

PERFORMANCE ANALYSIS APPLICATIONS OF SOME IMAGE ENCRYPTION TECHNIQUES

BAZI GÖRÜNTÜ ŞİFRELEME TEKNİKLERİNİN PERFORMANS ANALİZİ UYGULAMALARI

https://doi.org/10.20854/bujse.1114856

Cihan Tiken[1,*], Rüya Şamlı[2]

Abstract

Data security is now the most vital and most important issue of governments, companies, and individuals in the technology age we live in. Among the data types, images have a special importance because of the important information they contain. Transferring or storing images requires extra security measures. In this study, the performances of image encryption methods were compared with each other by applying them to the most popular and most used images in the image processing area. Four different experiments were carried out. The performances of seven particular encryption methods were compared with each other, and the observations and measurements were presented.

Keywords: Cryptology, Data Security, Image Processing

Özet

İçinde bulunduğumuz teknoloji çağında very güvenliği artık hükümetlerin, şirketlerin ve bireylerin en hayati ve en önemli konusu haline gelmiştir. Veri türleri arasında görseller içerdikleri öneml bilgiler nedeniyle özel bir öneme sahiptir. Görüntülerin aktarılması veya saklanması ekstra güvenlik önlemleri gerektirmektedir. Bu çalışmada, bazı görüntü şifreleme yöntemleri görüntü işleme alanında en popüler ve en çok kullanılan görüntülere uygulanarak performansları karşılaştırılmıştır. Dört farklı deney gerçekleştirilmiştir. Yedi farklı şifreleme yönteminin performansları birbirleri ile karşılaştırılarak yapılan ölçümler ve elde edilen gözlemler sunulmuştur.

Anahtar Kelimeler: Kriptoloji, Veri Güvenliği, Görüntü İşleme

[1,*] Corresponding Author: Harran University, Rectorate, ctiken@harran.edu.tr, orcid.org/0000-0001-7844-2579
[2] Istanbul University-Cerrahpaşa, Faculty of Engineering, Computer Engineering, ruyasamli@iuc.edu.tr, orcid.org/0000-0002-8723-1228

1. INTRODUCTION

The techniques used in this study are the most well-known techniques in the field of image encryption and have been chosen intuitively, not upon any parameter. These techniques are briefly explained below in a simple way.

In similar performance analysis studies, generally Histogram Analysis, Adjacent Pixel Correlation Analysis, Mean Value Analysis, and PSNR-Peak Signal-to-Noise Ratio Analysis were performed by the authors. These analyses are the analysis methods used in the measurement of the distortions or differences that occur after the encoding and decoding of the images. However, the focus of the first three experiments in this study is encryption and decryption speeds. Only in the last experiment is the image encoded by two different methods visually compared with the original.

2. IMAGE ENCRYPTION TECHNIQUES

2.1. Chaos Based Methods

Chaos theory is very sensitive to the initial conditions and control parameters of a nonlinear system or a continuous system, so that it is mostly used in image encryption area to increase randomness of keys and algorithms. A chaotic system has basic properties such as unpredictable and non-linear, deterministic and random-disorder (Srividya & Nandakumar, 2011; Chai et al., 2018). Implementation manner of a chaotic map is very important. Chaotic maps produce an entropy, and this produced entropy should generate enough complexity and diffusion in order to use in cryptography (Zhang et al., 2018).

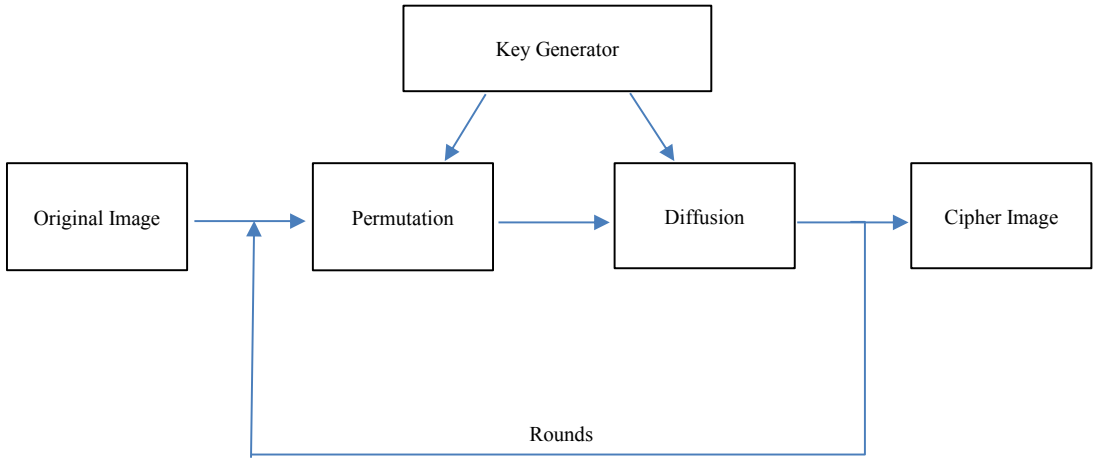

Figure 1: Block diagram of Chaotic encryption methods.

2.2. Least Significiant Bit (LSB) Based Methods

LSB method is based on embedding important data or secret messages into a cover image's (carrier image) least significant bits. Cover image and message bits create stego-image. It is possible to increase message embedding capacity by using more than 1 LSBs, but this process causes certain changes which can be seen by human eyes in the view of cover image. This method is widely used in the image encryption area. Although the implementation of this method is simple, it is not safe from attacks (Jiang et al., 2016; Muhammad et al., 2015).

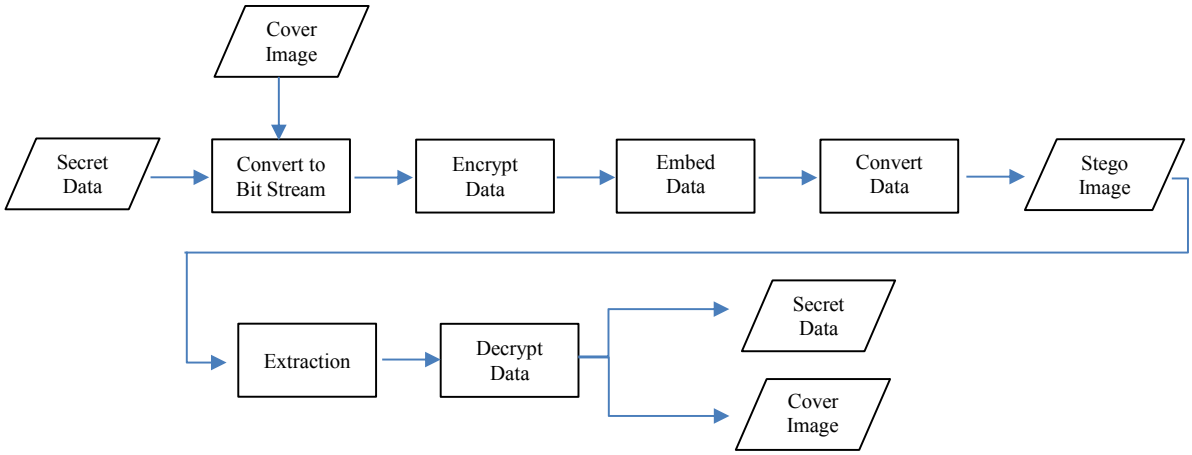

Figure 2: Block diagram of LSB based encryption methods.

2.3. Neural Network (NN) Based Methods

Neurons in the human nervous system combine thousands of temporal signals, thanks to their dendrites. The internal potential of these signals is complexly modified by the signals themselves. This change is based on the excitatory or restrictive nature of the synapses. A NN is a structure with a directed graph topology that represents a highly parallelized dynamic system. Interconnected groups of artificial neurons usually organized into layers, sublayers, or fields contain NNs. The behavior of such groups depends on changes in architectures as well as neuron signaling functions. Neurons are basic nonlinear computing elements; NNs are parallel networks of adaptive neurons. These neurons are designed to behave like a human neuron and perform some features of the human nervous system (Isac & Santhi, 2011).

2.4. Exclusive OR (XOR) Based Methods

In the XOR operation, there are two input grayscale images or binary images.These input images' pixel values must have the same number of bits; otherwise, some problems may occur. After implementing XOR operation on these two input images, an output image is generated. This output image consist of pixel values of first image and corresponding XORed pixel values from second image. (Gonzalez & Woods, 1993; Davies, 2012; Horn, 1986).

x_1	x_2	x_1 XOR x_2
0	0	0
0	1	1
1	0	1
1	1	0

Figure 3: XOR truth table.

2.5. RSA Based Methods

RSA algorithm is one of the most popular authentication and encryption algorithms. It is generally used for data transmission in a secure way. It is a public key cryptosystem. Public key is used during encryption process, but decryption process is done by secret key. Image is encrypted by the RSA encrypt key; thus, image becomes cipher text and stored as a text file. Decryption method is the opposite of the encryption, and it is done by secret RSA key. Finally image is reobtained (Anandakumar, 2015).

2.6. DNA Based Methods

DNA is a nucleic acid that contains genetic codes of the livinig organism . It consists of four bases named adenine (A), cytosine(C), guanine (G), and thymine (T). The binary values 00, 01, 10, and 11 are used to denote these four bases. For example, a single pixel value of “187” is in between a range of 0-255; this means it must consist of eight bits. So, this single pixel value is equal to “10111011” in binary presentation. Therefore, according to R1 rule, 187 pixel value corresponds to “GTGT” in genetic coding (Xue et al., 2020; Mousa, 2016).

Binary	R1	R2	R3	R4	R5	R6	R7	R8
00	A	A	C	C	G	G	T	T
01	C	G	A	T	A	T	C	G
10	G	C	T	A	T	A	G	C
11	T	T	G	G	C	C	A	A

Figure 4: Genetic coding rules.

2.7. DCT Based Methods

The discrete cosine transform (DCT) specifies an image as a total of sinusoids of varying frequencies and magnitudes. For a characteristic image, DCT has the property which is condensing most of the visually important data into a few DCT coefficients. That is why this method is generally used to compress an image. DCT is in the center of JPEG which is expressed as the international standard lossy image compression algorithm (Shaheen et al., 2019; Lian et al., 2004).

3. MATERIALS AND EXPERIMENTAL RESULTS

3.1. Materials

In this study, Tree, Splash, Sailboat, Peppers, Jelly Beans, House, Lena, Tiffany, Baboon, and Airplane images are used; all of these images are in “png” format and shown in between Figure 5 and Figure 14 respectively. These images are taken from a web site (SIPI Image Database, n.d.).

Figure 5: Tree.png

Figure 6: Splash.png

Figure 7: Sailboat.png

Figure 8: Peppers.png

Figure 9: Jelly Beans.png

Figure 10: House.png

Figure 11: Lena.png

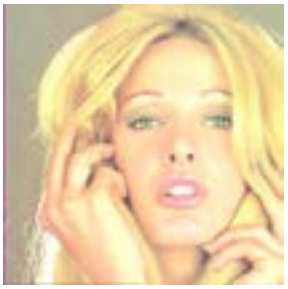

Figure 12: Tiffany.png

Figure 13: Baboon.png

Figure 14: Airplane.png

The results of the experiments are obtained on the Matlab R2015 enviroment which runs on a PC with a 64-bit Operating System, 1.99 GHz Intel i7 processor, and 8 GB of RAM.

3.2. Experiment I

In this experiment, the performance of some encryption methods was measured. Chaos Based Image Encryption, NN Based Image Encryption, LSB Based Image Encryption Methods were compared with each other in terms of the time it takes to encode the image. A gray scaled "Baboon.png" image with the size of 512x512 was used as the image to be encrypted in this experiment. The results of the experiment are shown in Table 1 below.

Table 1: Encryption times of the methods used.

	CAOS	NN	LSB
1. Encryption	0.35706	0.47459	0.21578
2. Encryption	0.37179	0.49557	0.21289
3. Encryption	0.36219	0.47195	0.23236
4. Encryption	0.35018	0.44983	0.22234
5. Encryption	0.37368	0.48632	0.24240
6. Encryption	0.36831	0.46814	0.22271
7. Encryption	0.36443	0.47226	0.23415
8. Encryption	0.34747	0.47917	0.21954
9. Encryption	0.37149	0.45637	0.22586
10. Encryption	0.39475	0.46587	0.25378
Average Time(sec.)	0.3661395	0.4720098	0.2281847

In order to obtain an average time value, each encryption method was run 10 times, and the data obtained are shown in the table above. When the data in the table is evaluated, the fastest average image encryption time among the methods used belongs to the LSB-based method with 0.2281847 seconds. The slowest encryption method also belongs to the NN-based image encryption method.

3.3. Experiment II

In the second experiment, it was observed whether the image features would affect the encryption method used. For this purpose, DCT-based and DNA-based methods were applied to all 512x512 sized images, and then application times were determined. The performance analysis of the DNA-based method is given in Table 2, and the performance analysis of the DCT-based method is given in Table 3.

Table 2: Performance of DNA-based method.

Image	Encryption Time (sec.)	Decryption Time (sec.)
Airplane	0.978	1.756
Lena	0.984	1.777
Baboon	0.982	1.808
House	0.950	1.761
Jelly Beans	1.008	1.753
Peppers	1.270	1.794
Sailboat	0.966	1.760
Splash	0.990	1.738
Tiffany	1.034	1.702
Tree	1.008	1.842

In this process, DNA image encryption technique was applied to 10 images selected from the most known images in the image processing field, and the measurement values obtained from the encryption and decryption processes are given in terms of seconds. Encryption and decryption were applied to each image 15 times, and the average of these values are shown in the table above. The most important factor for users in encryption and decryption processes is to perform the desired operation in the shortest time and in the most secure way. The image that reached the shortest encoding and decoding time obtained by summing the encoding and decoding times in DNA-based encoded images was “House.png”, and the longest time

consuming image was “Peppers.png”. But the other images gave approximate results; there is not a remarkable difference between them.

Table 3: Performance of DCT-based method.

Image	Encryption Time (sec.)	Decryption Time (sec.)
Airplane	1.967	2.991
Lena	1.944	2.927
Baboon	2.008	2.945
House	1.934	2.989
Jelly Beans	2.039	3.062
Peppers	2.117	3.135
Sailboat	2.026	3.118
Splash	2.025	3.106
Tiffany	2.088	3.090
Tree	2.102	3.058

The mean values were obtained by applying DCT-based image coding to all samples 15 times, and the image that achieved the total shortest encoding and decoding times in all images was “Lena.png.” The longest encoding and decoding values belong to “Peppers.png” image. Except these two images, the other images have aproximate results. In this context, DNA-based image encryption method was the fastest method among the two methods discussed. The total time taken for encoding and decoding is 2.75 seconds on average for all images for the DNA method and 5.67 seconds for the DCT method. The DCT-based encoding method takes slightly more than twice the average time of the DNA-based image coding method.

3.4. Experiment III

As a third experiment, XOR-based and RSA-based methods were applied to all images, and encryption and decryption times were determined. The performance analysis of the XOR-based method is given in Table 4, and the performance analysis of the RSA-based method is given in Table 5.

Table 4: Performance of XOR-based method.

Image	Encryption Time (sec.)	Decryption Time (sec.)
Airplane	0.53	0.60
Lena	0.51	0.57
Baboon	0.52	0.58
House	0.53	0.58
Jelly Beans	0.52	0.59
Peppers	0.53	0.60
Sailboat	0.54	0.59
Splash	0.53	0.60
Tiffany	0.56	0.63
Tree	0.53	0.59

In this process, XOR image encryption technique was applied to 10 images selected from the most known images in the image processing field. The images used were 512x512, and the measurement values obtained from the encryption and decryption processes are specified. Encryption and decryption were applied to each image 10 times, and the average of these

values is shown in the table above. Although the image that achieves the shortest encryption and decryption times in XOR-encrypted images is the “Lena.png” image. There is no significant time difference between “Lena.png” image and other images, it has almost approximate results.

Table 5: Performance of RSA-based method.

Image	Encryption Time (sec.)	Decryption Time (sec.)
Airplane	0.17	1.15
Lena	0.14	1.09
Baboon	0.15	1.11
House	0.14	1.13
Jelly Beans	0.13	1.09
Peppers	0.14	1.10
Sailboat	0.14	1.12
Splash	0.14	1.05
Tiffany	0.15	1.15
Tree	0.15	1.10

“JellyBeans.png” image had the shortest encryption and decryption times while RSA-based encryption was applied. There was a small time difference with the rest of the images as in XOR-based encryption method. While applying each method, the hardware used and the images processed were the same. Consequently, the RSA-based method was the fastest method among these two methods considered; the encryption time of each image was approximately 1/6th of a sec.

3.5. Experiment IV

Although performance analysis is a very important issue for an encryption method, the change ratio in visual of the encrypted image is another very important issue. In this application, the “JellyBeans.png” image which is one of the images that emerged as a result of the two encryption methods whose performance analyses were performed in the previous application were examined and their differences with the original image are observed. Figures are shown below.

Figure 15: Original image.

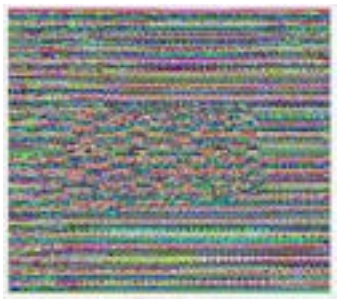

Figure 16: XOR-based encrypted image.

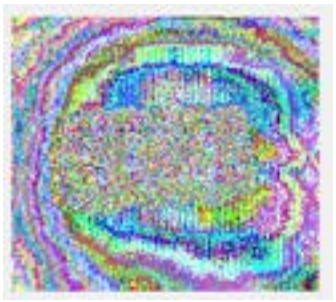

Figure 17: RSA-based encrypted image.

Although RSA-based method is faster than XOR-based method in terms of encryption and decryption times, when the encrypted images are examined, it is seen that the faster encryption method gives some idea at least about the edge boundaries of the original image. Accordingly, it seems a logical approach to use RSA-based methods in studies where time is important and XOR-based methods in studies where visual unpredictibility is important.

4. CONCLUSONS

There are important considerations in encrypting image data. One of these is the time spent on encryption and decryption, and the other one is that the content of the encrypted image must not be understandable by third parties. In this paper, the performances of various image encryption techniques have been analyzed and the observations obtained are presented for each particular experiment. In the first experiment, LSB-based is the fastest of the three methods evaluated. In the second experiment, the DNA-based method is about 2 times faster than the DCT-based method. In the third experiment, the encryption time of both methods took less than one second. In the last experiment, the XOR-based method was visually better encrypted and hard to predict according to the other method. All these used methods and some other methods all together can be observed and analyzed in a single experiment as a future work.

REFERENCES

Anandakumar, S. (2015). *Image Cryptography Using RSA Algorithm in Network Security*.

Chai, X., Zheng, X., Gan, Z., Han, D., & Chen, Y. (2018). An image encryption algorithm based on chaotic system and compressive sensing. *Signal Processing*, *148*, 124–144.

https://doi.org/https://doi.org/10.1016/j.sigpro.2018.02.007

Davies, E. R. (Ed.). (2012). Front-matter. In *Computer and Machine Vision (Fourth Edition)* (Fourth Edition, pp. i–iii). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-386908-1.00028-8

Gonzalez, R. C., & Woods, R. E. (1993). *Instructor's manual for digital image processing*. Addison-Wesley. https://books.google.com.tr/books?id=W51PPwAACAAJ

Horn, B. K. P. (1986). *Robot Vision*. MIT Press. https://books.google.com.tr/books?id=13a2vAEACAAJ

Isac, B., & Santhi, V. (2011). A Study on Digital Image and Video Watermarking Schemes using Neural Networks. *International Journal of Computer Applications*, *12*(9), 1–6. https://doi.org/10.5120/1715-2299

Jiang, N., Zhao, N., & Wang, L. (2016). LSB Based Quantum Image Steganography Algorithm. *International Journal of Theoretical Physics*, *55*(1), 107–123. https://doi.org/10.1007/s10773-015-2640-0

Lian, S., Sun, J., & Wang, Z. (2004). A novel image encryption scheme based-on JPEG encoding. *Proceedings. Eighth International Conference on Information Visualisation, 2004. IV 2004.*, 217–220. https://doi.org/10.1109/IV.2004.1320147

Mousa, H. M. (2016). DNA-Genetic Encryption Technique. *International Journal of Computer Network and Information Security*, *8*, 1–9.

Muhammad, K., Ahmad, J., Farman, H., & Zubair, M. (2015). *A Novel Image Steganographic Approach for Hiding Text in Color Images using HSI Color Model*. 1–11. https://doi.org/10.5829/idosi.mejsr.2014.22.05.21946

Shaheen, A. M., Sheltami, T. R., Al-Kharoubi, T. M., & Shakshuki, E. (2019). Digital image encryption techniques for wireless sensor networks using image transformation methods: DCT and DWT. *Journal of Ambient Intelligence and Humanized Computing*, *10*(12), 4733–4750. https://doi.org/10.1007/s12652-018-0850-z

SIPI Image Database. (n.d.). https://sipi.usc.edu/database/

Srividya, G., & Nandakumar, P. (2011). A Triple-Key chaotic image encryption method. *2011 International Conference on Communications and Signal Processing*, 266–270. https://doi.org/10.1109/ICCSP.2011.5739316

Xue, X., Zhou, D., & Zhou, C. (2020). New insights into the existing image encryption algorithms based on DNA coding. *PloS One*, *15*(10), e0241184. https://doi.org/10.1371/journal.pone.0241184

Zhang, Y., Li, Y., & Su, J. (2018). Iterative learning control for image feature extraction with multiple-image blends. *EURASIP Journal on Image and Video Processing*, *2018*(1), 100. https://doi.org/10.1186/s13640-018-0336-0