International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 9, No.5 (Sep-2020)

http://dx.doi.org/10.12785/ijcds/090520

Taguchi Optimization Method for Testing Best Image Encryption Algorithm

Samer Hammed Majeed[1], Noor Kareem Jumaa[1] and Auday A.H. Mohamad[1]

[1] *Al-Mansour University College, Baghdad, Iraq*

Received 5 Dec. 2019, Revised 14 May 2020, Accepted 26 Aug. 2020, Published 1 Sep. 2020

Abstract: Images, plain text and multimedia files are the core of this era; one of the main challenges is transferring data from source to destination in an encrypted way, so in case a sniffing machine or a sniffing computer can not detect and fetch the original data. This article introduces the Taguchi design of experiments method as an optimization tool to measure the best encryption method of images through calculating SNR, Mean and other critical parameters. The test was done using three cryptographic methods (Advanced Encryption Standard AES_{128}, Deoxyribonucleic Acid DNA, and Secure Force SF) with key (Linear Feedback Shift Register LFSR, Message Digest MD5, and Random number) for each one. After that the encrypted images are applied to Taguchi orthogonal array to measure and calculate the conditional parameters; this method provides the user details of each test. The obtained results of Taguchi experiments prove some facts; the secure force cryptographic method is lightweight and provides better image quality as mentioned in several researches; also, jpg images have better image quality parameters for security purposes as proved in several studies.

Keywords: Taguchi Method, Image Quality, Image Encryption, Secure Force, MD5, AES

1. Introduction

"Taguchi method" (Tm) is a powerful technique for solving the problems to improve process performance and productivity. It reduces the costs of rework and manufacturing due to its excessive variability in processes and reduces scrap rates. "Dr. Genichi Taguchi" defined the Tm; he designed methods to use designed experiments in designing and improving processes and products. After World War II, the manufacturers in Japan were stressed to survive with very limited resources. "If it were not for the advancements of Taguchi, the country might not have stayed afloat let alone flourish as it has". Taguchi transformed the Japan's manufacturing process through saving of costs. Like many other engineers, he understood that all manufacturing processes are affecting by the outside influences and noise. However, Taguchi realized methods to identify those noise sources, which are affecting the product variability. [1, 2, 3]

Optimization of process parameters is done to have great control over productivity, quality, and cost aspects of the process; off-line quality control is considered to be an effective method to enhance the quality of goods at a pretty low cost. [8, 9] [3, 4]

As a brief introduction, "Taguchi" method is a statistical method described by "Genichi Taguchi" to improve the quality of manufactured products. More recently, Tm applied for engineering biotechnology, marketing, and advertising. Professional statisticians have welcomed the improvements and goals brought by "Taguchi method", particularly by Taguchi's development of designs for studying variation. [5, 6, 7]

The word encryption or cryptography is a definition to the transformation of a "plain message" into a senseless formula called a "cipher message" that cannot be understood or read through any persons without decrypting the "encrypted message". While decryption is the reverse process of "encryption" that defined as the conversion procedure of the "encrypted message" into its original plain form so, it is a readable message [8].

By the technological evolution, data aegis over the Internet and other communication systems will be a great concern. "Encryption" is a widespread technique to uphold the security of images. Video and image encryption has many applications in different fields with multimedia systems, Tele-medicine, internet communication, medical imaging, and military communication. Quandaries of image security arises due to the utilization of cell phones, mobile contrivances, computers, and many other communication contrivances. Security of digital images encryption is predicated on two levels: "low-level security encryption" and "high-level security encryption". In "low-level security encryption", the encrypted image has low visual quality by compression with that of the pristine image, but the image contents still understandable and visible to the viewers. In 'high-level security', the content is thoroughly scrambled and the image looks just like arbitrary noise. In this case, the image is not comprehensible absolutely to the viewers. [8, 9, 10]

E-mail address: samer.majeed@muc.edu.iq, noor.jumaa@muc.edu.iq, auday.mohamad@muc.edu.iq

Different cryptographic algorithms have developed and designed nowadays. This article encrypts grayscale digital images using three famous high-level encryption algorithms; then analyzes three of the most public symmetric key encryption algorithms to pick one of them as an ideal algorithm to encrypt images with enhanced image quality parameters using Taguchi method.

The Taguchi method has been used in many topics to satisfy different objectives. But, few authors are used TM in the data security field. This article used TM to study and analyze the best encryption algorithm and the best algorithm for generating the symmetric encryption/ decryption key for different image types. The Taguchi method has applied on Advance Encryption Standard (AES), DNA cryptographic technique, Secure and force cryptographic method to encrypt/ decrypt PNG, JPG, and BMP grayscale images using manual key once, and generated keys using Linear Feedback Shift Register (LFSR) and Message Digestive (MD5).

The article is organized into six sections. Section 2 shows a brief literature survey of related works, section 3 discusses the Taguchi DOE, section 4 contains optimized image quality resulting from Taguchi experiments, and section 5 presents the results of encrypted / decrypted images, while the last section (section 6) concludes this article.

2. Literature Survey

Chuan-Kuei Huang et al [11] are implemented “quasi-optimal chaotic random codes (CRC)” and applied “Taguchi method” for optimization purposes. They apply Taguchi method to the control factors and levels then, generated a factor response graph for figuring out a set of chaotic initial values. Eventually, the quasi-optimal CRC is decided by these initial values. From the results of this paper, the authors prove that their proposed encryption schema is efficient and feasible.

A Taguchi method has been applied to health care for improving the quality of medical images as in [12].

In [13], design of experiment (DOE) using Taguchi approach is used to support the image processing system. Taguchi method is applied for different factors and levels combinations. They used factors of light intensity, camera distance, and other factors that are described deeply with their levels in. Taguchi OA with 27 experiments combinations has discussed in this reference.

Secure Force with Affine transform has been proposed to encrypt digital images as in [14]. Perform security analysis and evaluate the performance of the proposed algorithm is the objective of this paper. In [15], DNA algorithm is used to encrypt digital images. “These simulation results and security analysis show that the proposed algorithm not only has good encryption effect, but also has the ability to repel exhaustive, statistical, differential, and noise attacks”. This work presents a new direction of Taguchi method applications. Taguchi method is applied to select best encryption algorithm, key generator mechanism, and image type for grayscale image encryption. This paper is based on AES, DNA, and Secure Force as cryptographic algorithms; LFSR and MD5 as key generator mechanisms; th results prove that the JPG image has better image quality that PNG and BMP images.(i.e.JPG images have low noise) .

3. Taguchi Design of Experiments

In this article, an encrypted image quality optimization problem is introduced as a series of experiment design tests. According to Marco Cavazzuti [16] "Within the theory of optimization, an experiment is a series of tests in which the input variables are changed according to a given rule in order to identify the reasons for the changes in the output response".

Dr. Genichi Taguchi introduces a quality control optimization named "Taguchi Design of Experiments method". The Taguchi method is used to reach the optimal values of the factors that affect the steps of design to make the design (product design) with lower sensitivity to the variations of noise [17].

Orthogonal arrays (OA) are used in Taguchi design of experiment method. The principle of OA is used to measure the effect of controllable factors. Those arrays have columns of independent coefficients.

The size of Taguchi OA depends on the number of designed variables and their levels.

Let, M is the number of Taguchi factors and Z is the number of levels for each factor then Taguchi experiments number is M*f+1, where f = (Z-1) [15].

Three levels, four controllable factors with nine experiments (L9 (3) 4) Taguchi orthogonal array is shown in Table I [12].

The fitness function and signal to noise ratio (SNR) are used to evaluate the experiment

The signal to noise ratio is used to investigate the effect of factors to find the optimal solution. The signal to noise ratio is defined as in (1) [17].

$$SNR = 10 \log (MSD) \qquad (1)$$

Where MSD is mean squared deviation.

$$MSD = \sum_{n=1}^{N} \frac{y_n^2}{N} \qquad (2)$$

y_n is the results measured in terms of quality characteristics and N is the number of experiments.

TABLE I. L9 Orthogonal Array

Exp. No.	Factor 1	Factor 2	Factor 3	Factor 4	Fitness Fun.	SNR
1	1	1	1	1	J1	SNR1
2	1	2	2	2	J2	SNR2
3	1	3	3	3	J3	SNR3
4	2	1	2	3	J4	SNR4
5	2	2	3	1	J5	SNR5
6	2	3	1	2	J6	SNR6
7	3	1	3	3	J7	SNR7
8	3	2	1	3	J8	SNR8
9	3	3	2	1	J9	SNR9

4. Taguchi Method Image Quality Optimization

The proposed system demonstrates Taguchi Method to study three factors that are impact on encrypted image quality; then conclude the best method depending on encryption algorithm and key generator. This system is based on three main factors. Those factors are encryption algorithm, random key generator and image type. The tested algorithms that are used in encryption factors are AES128 algorithm [18], DNA algorithm [19] and secure force algorithm [20].The random key that is used for each encryption algorithm is manual key, LFSR [8], and MD5 [18]. Also, the type of images that are applied for test are PNG, JPG, and BMP.

Image quality optimization experiments have three control parameters and three levels for each of the parameters, so, L_9 orthogonal array is selected. The parameters are:

P_1: Encryption algorithm. Where (L_1= AES, L_2=DNA, L_3=SF).

P_2: Key generation algorithm. Where (L_1=Manual, L_2=LFSR, L_3=MD5).

P_3: Image type. Where (L_1=boat.png, L_2=castle.jpg, L_3=wild.bmp).

Once the OA is selected, then the trials (iterations) of experiments can be carried out. The number of trials are finalized based on the cost of performing the experiments and the complexity of the experiments. For the image quality experiment, it may have three trials and at the end, each of the four experiments has four result values that are:

T_1: is the measured MSE.

T_2: is the measured PSNR.

T_3: is the measured NK.

T_4: is the measured NAE.

In this article, image quality are measured for optimization purpose. Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Normalized Correlation (NK), and Normalized Absolute Error (NAE) are measured as an image quality parameters [13, 16, 8 and 9]. Where:

I. MSE: “is the measurement of average of the square of the difference between the intensities of the cipher image and the original image”.

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{1}^{\mathrm{M}} \sum_{1}^{\mathrm{N}} \left(\mathrm{f(i,j)} - \bar{\mathrm{f}}(\mathrm{i,j})\right)^{2} \qquad (3)$$

II. PSNR: “it depicts the measure of reconstruction of the compressed image. This metric is used for discriminating between the cipher and original image”.

$$PSNR = \frac{10Log(512)^2}{MSE} \qquad (4)$$

III. NK: “Normalized Correlation measures the similarity between two images” (i.e. the cipher image and the original image).

$$\mathrm{NK} = \frac{\sum_1^{\mathrm{M}} \sum_1^{\mathrm{N}} [\mathrm{f(i,j)}.\bar{\mathrm{f}}(\mathrm{i,j})]}{\sum_1^{\mathrm{M}} \sum_1^{\mathrm{N}} (\mathrm{f(i,j)})^{2}} \qquad (5)$$

IV. NAE: “is the measure of how distant is the modified image from the original image with the value of zero being the perfect fit”.

$$\mathrm{NAE} = \frac{\sum_1^{\mathrm{M}} \sum_1^{\mathrm{N}} |[\mathrm{f(i,j)}.\bar{\mathrm{f}}(\mathrm{i,j})]|}{\sum_1^{\mathrm{M}} \sum_1^{\mathrm{N}} |(\mathrm{f(i,j)})|} \qquad (6)$$

Note that M and N are the dimensions of the encrypted image. In this research three grayscale images are used with [512 512] size so, for (3) through (6), M and N are 512.

Next, the SN ratio for each of the experiments are calculated using the following formula:

S_m, S_t, S_e, V_e, and SN.

$$S_m = \frac{(T1 + T2 + T3 + T4)^2}{N} \qquad (7)$$

$$S_t = T_1^2 + T_2^2 + T_3^2 + T_4^2 \qquad (8)$$

$$S_e = S_t - S_m \qquad (9)$$

$$V_e = \frac{\mathrm{Se}}{(N-1)} \qquad (10)$$

$$\mathrm{SN} = 10\mathrm{Log}\frac{(\mathrm{Sm} - \mathrm{Ve})}{(4\mathrm{xVe})} \qquad (11)$$

It should be mentioned that N=number of results which is 4. So, for (7) and (11), N=4.

Now, let’s put all the values to the L_9 OA and it will become as in Table II.

Experiments are performed and nine iterations of the experiment are done, the results are tabulated as in Table III.

TABLE II. L9 OA FOR IMAGE QUALITY EXPERIMENTS

EXP#	Algorithm (P1)	Key (P2)	Image (P3)
1	AES128	Manual Key	Png
2	AES128	LFSR	Jpg
3	AES128	MD5	Bmp
4	DNA	Manual Key	Jpg
5	DNA	LFSR	Bmp
6	DNA	MD5	Png
7	Secure Force	Manual Key	Bmp
8	Secure Force	LFSR	Png
9	Secure Force	MD5	Jpg

Next, SN Ratio is calculated using (7), (8), (9), (10) and (11). The full calculation for one experiment is shown in Table IV.

Next, the average SN value for each parameter based on the levels is calculated. The calculation for the Algorithm (**P$_1$**), Key Generation (**P$_2$**), and Image Type (**P$_3$**) are shown in Table V and Fig. 1.

The design of experiment (DOE) of the image quality is enough to notice that the Taguchi method show that best algorithm is the secure force, best key generator is the MD5, and best encrypted image is the jpg image type since they obtained the highest average of SNR. Table VI concluded the results.

5. Image Encryption-Decryption Results

According to the designed experiments OA of Taguchi method, each of the plain images is entered to the cryptographic system (AES, DNA, or SF) as an input simultaneously with the 128 bits key which is either a manual key or generated key using (LFSR or MD5 random key generator).

The plain image is broking to blocks, each with 16 bytes size. Each block is entered to the cryptographic system and encrypted using the 16 bytes (128 bits) and a cipher image is generated. Each block of cipher image is of 16 bytes sized collected together to procedure the cipher image which is a random image to the viewer.

Encryption performance is evaluated using Taguchi Method. Figure (1) shows the encryption/decryption image results for each experiment. Figures from (2) through (10) show the encryption/decryption images.

6. Conclusions

Taguchi Method can be implemented on different life branches not only the marketing branch. The experimental design of Taguchi method with L_9 OA was used for optimizing the process parameters for the best quality of an encrypted grayscale image. The optimized parameters of the experiments are: encryption algorithms (Secure Force affecting with SN=-32.8258 dB), symmetric encryption/decryption key (Manual key affect with SN=-33.0401 dB), and image extension type (JPG images affecting with SN=-33.0014 dB). It demonstrates Secure Force algorithm is the best cryptographic method with any manual key. The results are based on calculating and comparing SNR parameter from all tests for the three algorithms with proposed keys.

Also a lot of papers and researches mentioned that jpg image type is the best type for encryption and steganography; this article evinces the reason behind using image type jpg through applying Taguchi Method.

TABLE I. L9 OA FOR IMAGE QUALITY EXPERIMENTS

EXP#	Algorithm (P1)	Key (P2)	Image (P3)	MSE (T1)	PSNR (T2)	NK (T3)	NAE (T4)	Mean (M)
1	AES128	Manual Key	png	93.7078	1.3314	1.0144	2.4126	24.6166
2	AES128	LFSR	jpg	92.8933	1.3431	1.0142	2.4120	24.4157
3	AES128	MD5	bmp	93.4009	1.3358	1.0146	2.4131	24.5411
4	DNA	Manual Key	jpg	93.2634	1.3378	1.0138	2.4113	24.5066
5	DNA	LFSR	bmp	93.5261	1.3340	1.0141	2.4120	24.5716
6	DNA	MD5	png	93.5723	1.3334	1.0040	2.3878	24.5744
7	Secure Force	Manual Key	bmp	87.7381	1.4220	1.0164	2.4173	23.1485
8	Secure Force	LFSR	png	94.9453	1.3141	1.0106	2.4035	24.9184
9	Secure Force	MD5	jpg	87.7381	1.4220	1.0164	2.4173	23.1485

TABLE IV. OA FOR IMAGE QUALITY EXPERIMENTS WITH SN RATIO AVERAGE

EXP#	Algorithm (P1)	Key (P2)	Image (P3)
1	-33.3079	-33.0401	-33.4489
2	-33.3538	-33.3839	-33.0014
3	-32.8258	-33.0635	-33.0372

TABLE V. CONCLUSION FOR IMAGE QUALITY OPTIMIZATION USING TAGUCHI METHOD

Parameter	Optimum Value
Algorithm (P1)	Secure Force
Key Generator (P2)	Manual Key
Image (P3)	JPG image

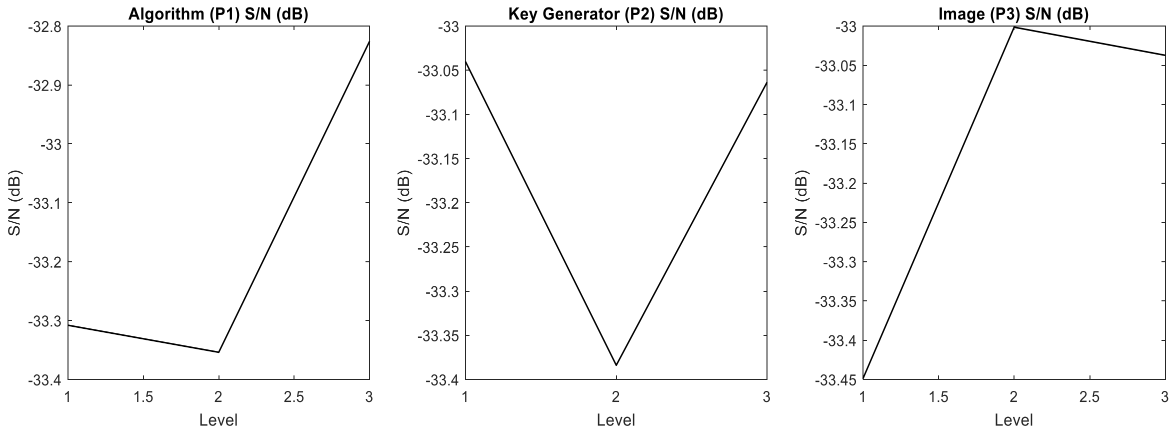

Figure 1. Average SNR of the Three Parameters

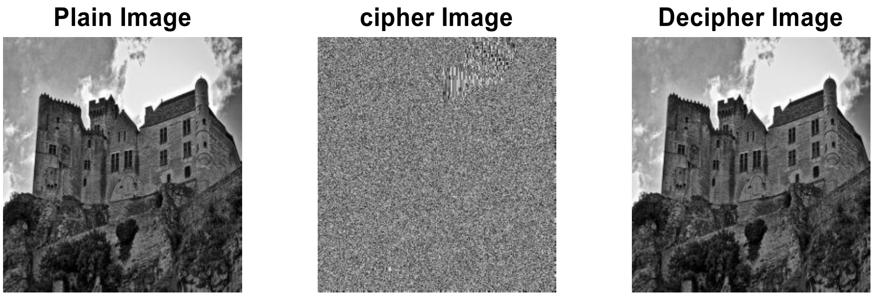

Figure 2. PNG image encryption/decryption resulted from Experiment (1)

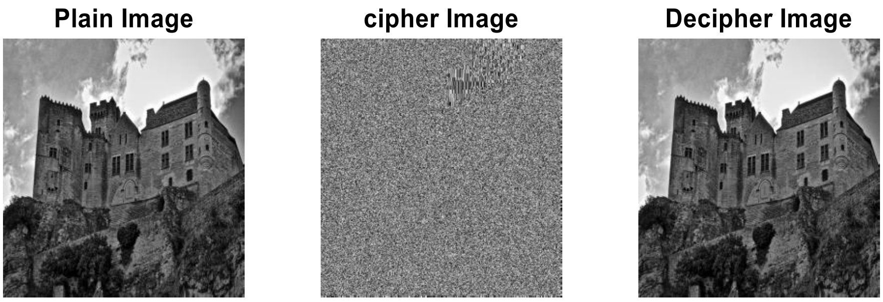

Figure 3. JPG image encryption/decryption resulted from Experiment (2)

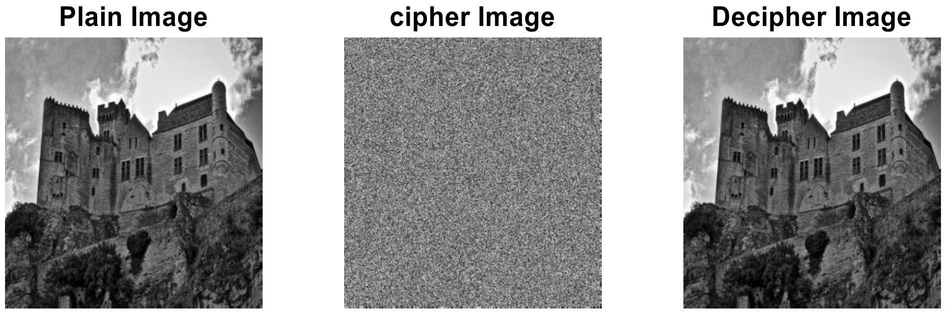

Figure 4. BMP image encryption/decryption resulted from Experiment (3)

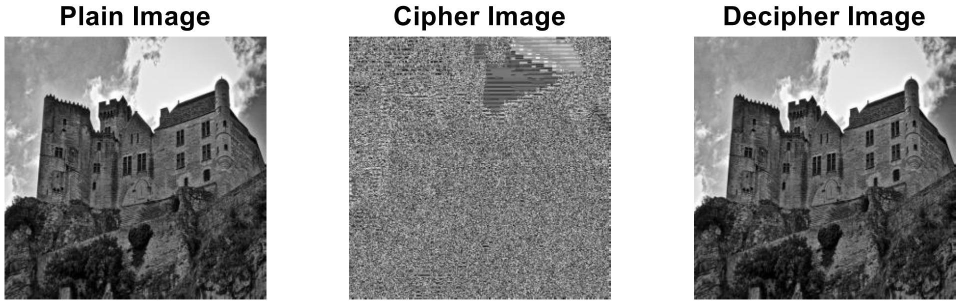

Figure 5. JPG image encryption/decryption resulted from Experiment (4)

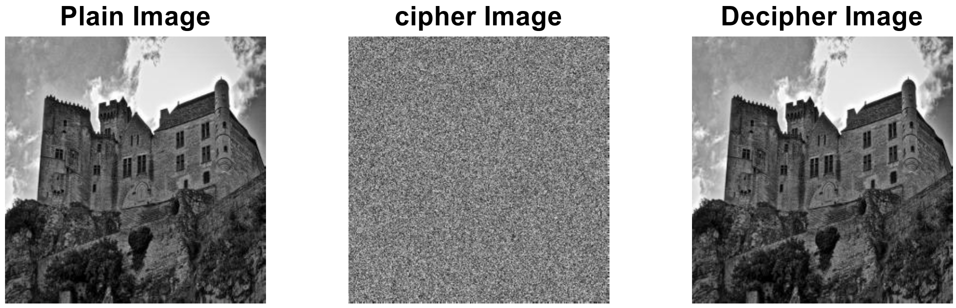

Figure 6. BMP image encryption/decryption resulted from Experiment (5)

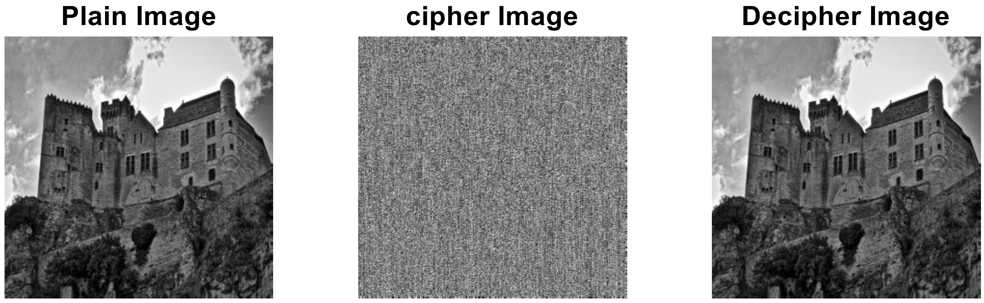

Figure 7. PNG image encryption/decryption resulted from Experiment (6)

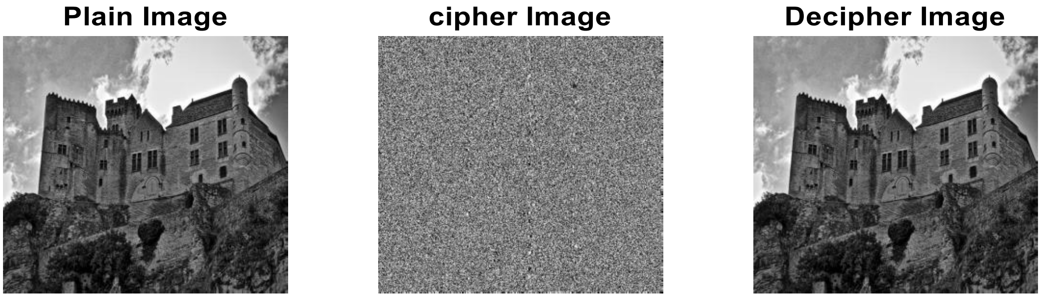

Figure 8. PNG image encryption/decryption resulted from Experiment (7)

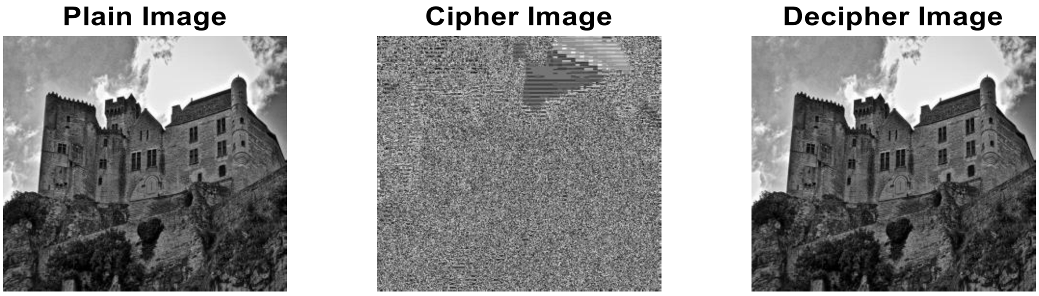

Figure 9. JPG image encryption/decryption resulted from Experiment (8)

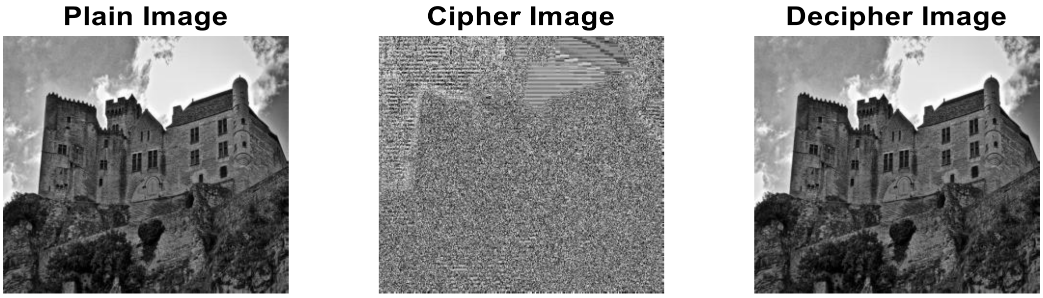

Figure 10. JPG image encryption/decryption resulted from Experiment (9)

REFERENCES

[1] Jiju Antony and Frenie Jiju Antony, “Teaching the Taguchi method to industrial engineers”, Work Study, Vol. 50 Issue 4, pp.141-149, 2001.

[2] Y. Wu, and A. Wu, “Taguchi Methods for Robust Design”, New York, USA: ASME, 2016.

[3] Shyam Kumar Karna and Dr. Rajeshwar Sahai, “An Overview on Taguchi Method”, International Journal of Engineering and Mathematical Sciences, Volume 1, pp.11-18, 2012.

[4] Khosrow Dehnad, “Quality Control, Robust Design, and the Taguchi Method”, Wadsworth & Brooks/ Cole Advanced Books & Software, Pacific Grove, California 93950, a division of Wadsworth, Inc. 1989.

[5] R. Sreenivas Rao, R.S Prakasham, K. Krishna Prasad, S Rajesham, P. NSarma, and L. Venkateswar Rao, “Xylitol production by Candida sp: parameter optimization using Taguchi approach”. Process Biochemistry, Vol. 39, Issue: 8, pp. 951–956, 2004.

[6] Rao RS, Kumar CG, Prakasham RS, and Hobbs PJ , “The Taguchi methodology as a statistical tool for biotechnological applications: A critical appraisal”, Biotechnology Journal, Vol. 3, Issue: 4, pp. 510–523, 2008.

[7] Paul H. Selden, “Sales Process Engineering: A Personal Workshop” Milwaukee, Wisconsin: ASQ Quality Press, 1997.

[8] Noor Kareem Jumaa, “Digital Image Encryption using AES and Random Number Generator”, Iraqi Journal of Electrical and Electronic Engineering, Vol. 14, No. 1, 2018.

[9] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, “A Modified AES Based Algorithm for Image Encryption”, International Journal of Computer Science and Engineering, Vol. 1, No. 1, 2007.

[10] Priya Deshmukh, “An image encryption and decryption using AES algorithm”, International Journal of Scientific & Engineering Research, Vol. 7, Issue 2, 2016.

[11] C. K. Huang, H. H. Nien, S. K. Changchien, and H. W. Shieh, “Image encryption with chaotic random codes by grey relational grade and Taguchi method”, Optics Communications, vol. 280, No. 2, pp. 300–310, 2007.

[12] Taner MT and Sezen B, “Taguchi's experimental design method on improvement of medical image quality”, Leadersh Health Serv (Bradf Engl), Vol. 20, No. 2, pp. 42-51, 2007.

[13] Ditha Yusfiana Maryani, Haris Rachmat, and Denny Sukma Eka Atmaja, "Design of Experiments Application Using Tacuchi Approach to Identify Woven Fabrics Defects by Image Processing AT CV. Maemunah Majalaya", e-Proceeding of Engineering, Vol.3, no.2, 2016.

[14] P.Lakshmi Sowjanya and K.J.Silva Lorraine, "Image Encryption Using Secure Force Algorthim with Affine Transform for WSN", International Journal of Sciences & Research Technology, Vol. 5, No. 8, 2016.

[15] Jian Zhang, DongXin Fang, and Honge Ren, "Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps", Mathematical Problems in Engineering, 2014.

[16] Marco Cavazzuti, "Optimization Methods from Theory to Design Scientific and Technological Aspects in Mechanics", Springer, 2013.

[17] Ranjit Roy, "A Primer on the Taguchi Method", ISBN 0-442-23729-4, Van Nostrand Reinhold, 1990.

[18] W. Stallings, "Cryptography and Network Security: Principles and Practices", 3rd ed. Upper Saddle River, NJ: Prentice-Hall, 2003, Guest Editorial, S. Pankanti, R. Bolle, A. K. Jain (Guest Editors) Special Issue of IEEE Computer on Biometrics, 2000.

[19] O. Tornea, M.E. Borda,"DNA Cryptographic Algorithms", International Conference on Advancements of Medicine and Health Care through Technology IFMBE Proceedings, vol. 26, pp. 223-226, 2009.

[20] Mansoor Ebrahim, Chai Wai Chong, "Secure Force: A Low-Complexity Cryptographic Algorithm for Wireless Sensor Network (WSN) ", 2013 IEEE International Conference on Control System Computing and Engineering, 2013.

Samer Hameed Majeed received his M.Sc. in Computer Engineering from Cankaya University, Turkey, in 2014. He received his B.Sc. in Computer Engineering from University of Technology, Iraq in 2005. Currently, he is a Ph.D degree student at UNIVERSITI SAINS MALAYSIA (USM) majoring in (Image Processing and Artificial Neural Network). Previously, he worked as telecommunication engineer in several national and international companies; such as Huawei, Ericsson and Itisaluna, Iraq. Also he worked as assistant lecturer (Computer Technology Engineering) in Al-Mansour University College-Iraq.

Noor Kareem Jumaa was received her B.Sc degree in computer engineering from university of Baghdad, Iraq in 2010 and the M.Sc degree in quantum cryptography and data security from the department of electronics and communication engineering, university of Baghdad in 2013. Currently, she is an instructor at the Computer Technology Engineering Department, Al-Mansour University College, Baghdad, Iraq.

Auday A.H. Mohamad received his Ph.D. in Electrical and Electronics Engineering from Omdurman Islamic University, Sudan, in 2012. He received his B.Sc. and M.Sc. in Electrical Engineering (Computers and Control) from University of Baghdad, Iraq in 1997 and 2000, respectively. Currently, he is an Assistant. Prof. (Head of Communication Engineering Department) in Al-Mansour University College-Iraq. Previously, he worked as lecturer (Electrical Engineering, 2000-2003) in College of Engineering-University of Baghdad, Iraq, and as Assistant professor (Electrical and Electronics Engineering, 2003-2013) in Faculty of Engineering Sciences- Omdurman Islamic University, Sudan.