TELKOMNIKA, Vol.17, No.6, December 2019, pp.2968~2974
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i6.10488

Evaluation of the quality of an image encrytion scheme

Osemwegie Omoruyi[1], Chinonso Okereke[2], Kennedy Okokpujie*[3], Etinosa Noma-Osaghae[4], Obinna Okoyeigbo[5], Samuel John[6]
[1,2,3,4,5]Deparment of Electrical and Information Engineering, Covenant University Ota, Ogun State, Nigeria
[6]Deparment of Electrical and Electronic Engineering, Nigerian Defence Academy Kaduna, Nigeria
*Corresponding author, e-mail: osemwegie.omoruyi@covenantuniversity.edu.ng[1], chinonso.okereke@covenantuniversity.edu.ng[2], kennedy.okokpujie@covenantuniversity.edu.ng[3], etinosa.noma-osaghae@covenantuniversity.edu.ng[4], obinna.okoyeigbo@covenantuniversity.edu.ng[5], samuel.john@nda.edu.ng[6]

Abstract

Encryption systems have been developed for image viewing applications using the Hill Cipher algorithm. This study aims to evaluate the image encryption quality of the Hill Cipher algorithm. Several traditional metrics are used to evaluate the quality of the encryption scheme. Three of such metrics have been selected for this study. These include, the Colour Histogram, the Maximum Deviation (comparing the original image) and the Entropy Analysis of the encrypted image. Encryption quality results from all three schemes using a variety of images show that a plain Hill Cipher approach gives a good result for all kinds of images but is more suited for colour dense images.

Keywords*: colour histogram, encryption quality, entropy analysis, Hill Cipher, image encryption*

1. Introduction

Encryption schemes [1-13] are only as good as the difficulty posed in attacking its results. This difficulty is a function of various factors dependent on the encryption scheme or method employed. With respect to images, the difficulty of retrieving an original image [14-16] from one that is ciphered is the clear objective in evaluating an encryption scheme's security and performance. Evaluation also helps in ascertaining that a good visual result is obtained for a variety of images whilst using an encryption scheme (encrypted images must leave nothing exposed from an original image). Another purpose of evaluating an encryption scheme is to improve the time performance of the encryption process whilst also ensuring that its result is not susceptible to any security attack.

This study details the evaluation of the performance and security (quality) of an encryption scheme implemented using the Hill Cipher algorithm. A number of studies have shown that a visual inspection is insufficient to estimate correctly the quality of an encryption scheme [17]. A number of novel tests and analyses have been introduced and these tests have been classified into various categories. Notably, Li et al [18] classified objective evaluation into two namely: reference and non-reference objective evaluation. Objective evaluation is done with the reference or original image in use whilst a non-reference evaluation does not rely on the reference image. All evaluation however, border on measuring the randomness introduced to an image by an encryption scheme. It may also seek to show its vulnerability to security attacks. This study is organized as follows; section two gives an overview of quality metrics and the various types of tests and analyses that can be carried out on an encryption scheme. Section three discusses the implementation of the encryption quality interface. Section four outlines the results obtained for various image types. Section 5 concludes the study.

2. Overview of Encryption Quality Analysis

This section discusses some well-known quality metrics, it includes Colour Histograms, Encryption Quality, Maximum Deviation, Entropy Analysis etc.

Received July 3, 2018; Revised February 5, 2019; Accepted March 12, 2019

2.1. Colour Histogram

Colour histograms are a pictorial representation of the occurrence frequency of 8 bit pixel values showing the Red-Green-Blue (RGB) component of an image. Colour histograms give an idea of the dominant occurring shades represented in an image. Histogram is used to show the confusion and diffusion properties of an image encryption scheme to resist any statistical attacks [19]. Uniform or fairly even distribution of a colour histogram show strong diffusion properties. Also, the distribution of an encrypted image should be significantly different from that of the original image [20]. Figure 1 shows a flow chart for obtaining the Colour Histogram.

2.2. Maximum Deviation

Maximum Deviation is obtained by computing the difference between the cipher values and the encrypted values of the images. A three-step process is documented by El-Fishawy et al [21] for obtaining this metric namely:

- Get the frequency of image pixels of each grayscale value in the range from 0 to 255 and for both original and ciphered images.
- Compute the absolute difference or deviation between the original and ciphered image pixel frequency.
- From the absolute difference obtained, calculate the sum of deviations (D) and this represents the Maximum Deviation. D is given by (1).

$$D = \frac{h_0 + h_{255}}{2} \sum_{i=1}^{254} h_i \quad (1)$$

$$where \quad h_i = |h_{pi} - h_{ci}|$$

where L is the total grayscale levels and h_i is the value of the difference histogram obtained from step 2 above i.e. the deviation or absolute difference between the grayscale values of the plain h_{pi} and cipher image h_{ci} respectively.

2.3. Entropy Analysis

Information or Shannon entropy is a measure of the information or uncertainty in any random system or the quantity of information in a given source [22]. Shannon's entropy is given as:

$$H(X) = \sum_0^{L-1} P(x_i) \, log_2 \frac{1}{P(x_i)} \quad (2)$$

an ideal random source entropy is equal to 8 but most information sources seldom generate random messages, therefore their entropy value is much smaller than the ideal one.

2.4. Encryption Quality

Encryption quality is designed to measure the change rate of pixel values when encryption is applied to an image. The encryption quality may be expressed as the deviation between the original and encrypted image or as the total changes in pixels values between the plain-image and the encrypted image [23]. This is shown in (3)

$$EQ = \frac{\sum_{i=0}^{L-1} h_i}{L} \quad (3)$$

the gray level pixel values are used and are computed with (4):

$$GL = 0.299 * (R) + 0.587 * (G) + 0.114 * (B) \quad (4)$$

2.5. Irregular Deviation

The Irregular deviation factor takes a similar path as the maximum deviation factor with only extra computations needed. In a five-step process, here's how its obtained: D is absolute value gotten by subtracting the values of the image pixel after encryption (I) from the value of the image pixel before encryption (J). This is shown in (5). Figure 2 shows a flow chart for calculating Encryption Quality, Maximum and Irregular Deviation.

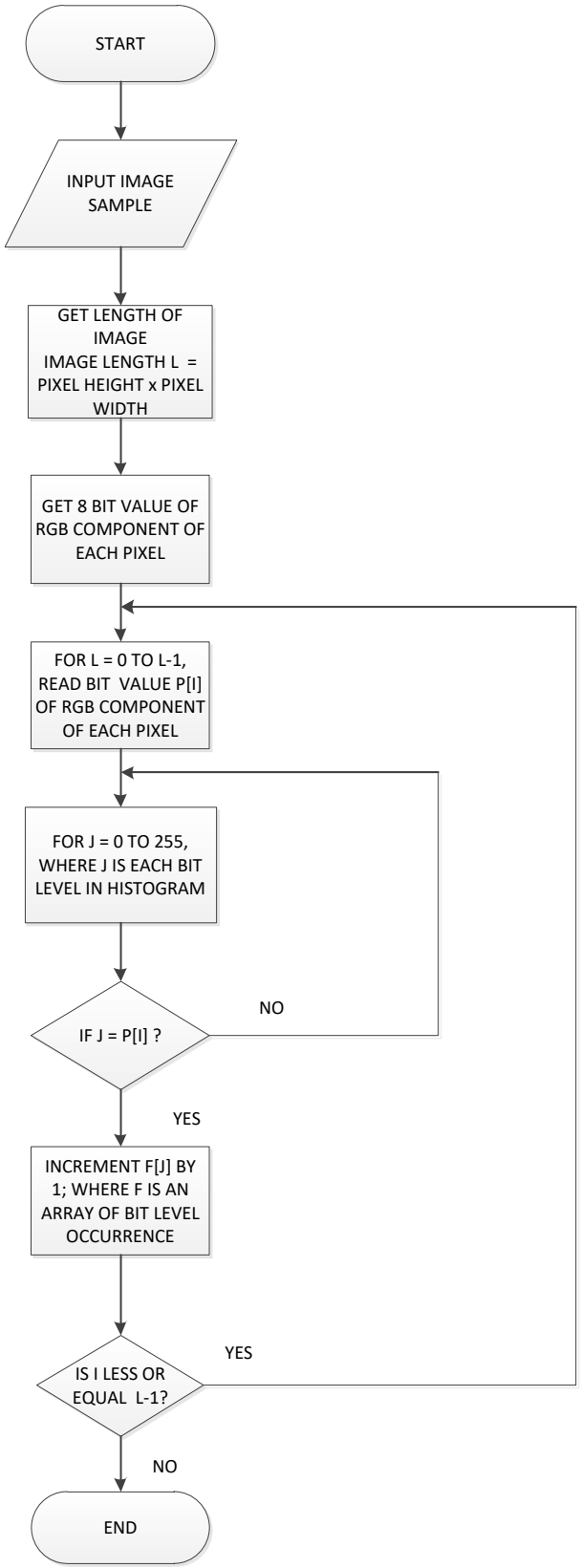

Figure 1. Flowchart of obtaining colour histogram

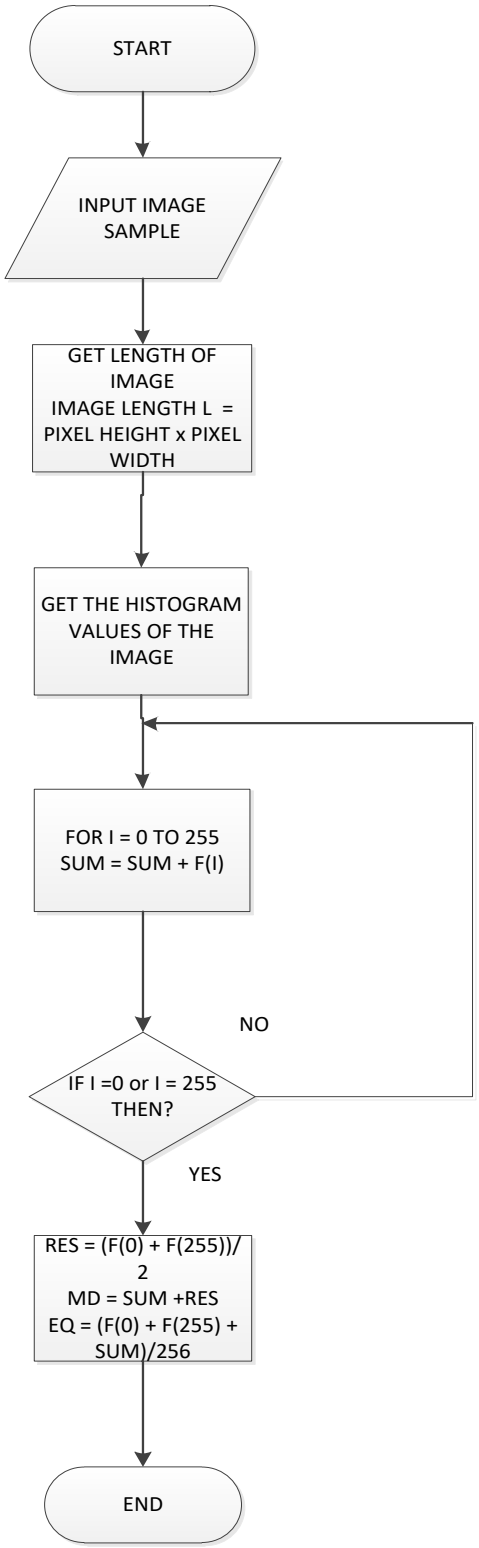

Figure 2. Flowchart for calculating encryption quality, maximum deviation and irregular deviation

$$D = |I - J| \quad (5)$$

DC is calculated by averaging the deviations obtained in step 1 as shown in (6).

$$DC = \frac{\sum_{i=0}^{255} D_i}{256} \quad (6)$$

the Irregular deviation is obtained by summing the absolute value obtained by subtracting the individual deviation from the average value.

$$AC(i) = |D(i) - DC| \quad (7)$$

$$ID = \sum_{i=0}^{255} AC(i) \quad (8)$$

3. Design of Encryption Quality Interface

Based on the algorithms discussed in the previous section, an encryption quality analysis interface has been created with all four of the methods discussed. The Encryption Quality interface has been developed in a software application already described in a previous work [24]. The algorithm to obtain the frequency of occurrence of each bit value as used in the colour histogram is shown in Figure 1.

Figure 2 shows the flowchart for calculating both the maximum deviation and irregular deviation algorithm. Figure 2 also shows the flow chart for deriving the encryption quality and Figure 1 shows the flowchart for obtaining the Colour histogram. The Graphical user interface is retained for display of histogram values as shown in Figure 3.

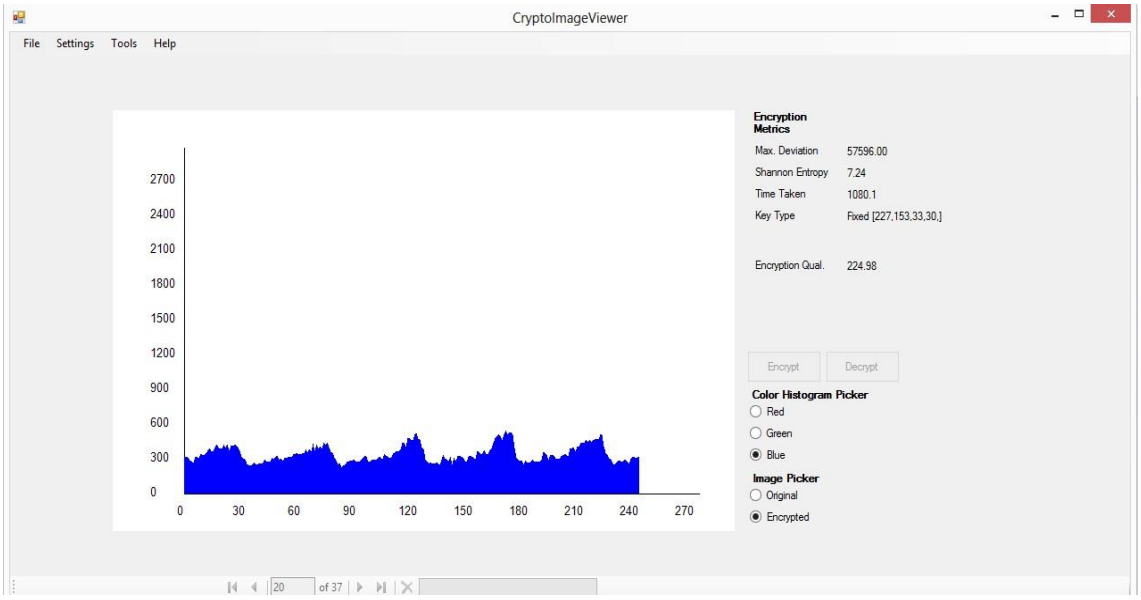

Figure 3. Encryption quality interface

4. Implementation and Evaluation of Results

This section presents the analysis of the results of three images: lena.jpg, pepper.jpg and watch.jpg.

4.1. Histogram Analysis

Results from histogram analysis are presented in Figures 3 and 4. The good uniformity of the histograms produced in Figure 4 (a), Figure 4 (b) and Figure 4 (c) confirm the result obtained

in a previous work; Chinonso et al [24] noted that low valued images with grey level pixels closer to maximum bound produced much better quality with the hill cipher encryption scheme. Image results will therefore be less prone to statistical attacks.

4.2. Maximum and Irregular Deviation

Larger values of maximum deviation indicate better encryption quality while for irregular deviation, the smaller the better. Based on these metrics, the pepper image performs least by both metrics while the watch image performs best in the encryption scheme based on maximum deviation. Lena image performs best based on irregular deviation. Lower values are required for irregular deviation. Therefore, based on the tests, it is seen that Lena image performs best and Pepper image still performs least by this metric.

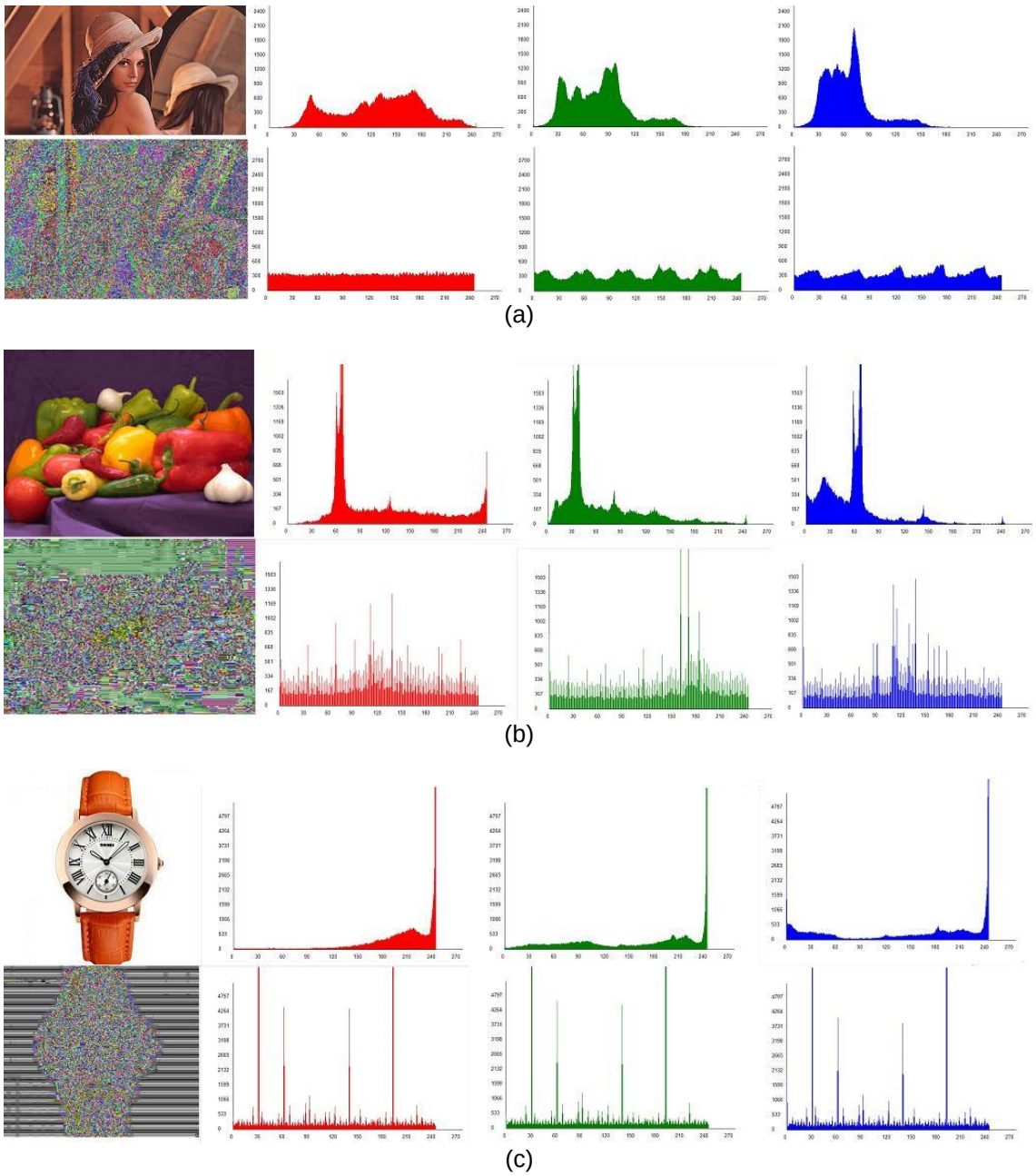

Figure 4. (RGB colour histograms of original images and encrypt ed images);
(a) lena, (b) pepper, (c) watch

4.3. Encryption Quality

Encryption quality shows how deviated the encrypted image is from the original as shows in Table 1. Based on this metric, Pepper image performs least. This means that it is least deviated from the original. While on the other hand, watch image is encrypted significantly well and is relatively highly deviated. This means that the encryption algorithm is most effective on the Watch image.

Table 1. Encryption Quality Metrics Obtained from Analysis

Image	Size	Time Taken (ms)	Maximum Deviation	Entropy	Encryption Quality	Irregular Deviation
Lena	400x225	1081	57596	7.24	224.98	36636.72
Pepper	259x194	632.4	47264	6.82	184.66	42933.61
Watch	400x400	1919.3	194889	4.25	929.92	371748.48

4.4. Entropy Analysis

Based on the entropy metric, all images perform lower than the ideal random source entropy which is 8-bit. With watch image having the lowest entropy value and Lena image having the highest entropy value. This means that information leakage in the watch image is most possible and Lena image least possible. It is advised that other encryption algorithms be used for the watch image and pepper image since the encryption algorithm used is prone to entropy attack.

4.5. Key Sensitivity Analysis

Zhang et al [25] showed using a key sensitivity test where values of the key used for image encryption was analysed to see similarities in the encrypted images produced by these keys. Table 2 shows the observation when various image keys where tested against the Lena image for the corresponding results. The results show metrics for ID, EQ, MD and Entropy. The entropy remains the same for all three keys showing a similar strength. It can be seen that keys with higher absolute determinant give better maximum deviation. However, Maximum and irregular deviation values look significant.

Table 2. Testing with Various Keys using the Lena Image

Key	Time Taken (ms)	Maximum Deviation	Entropy	Encryption Quality	Irregular Deviation
$\begin{bmatrix} 11 & 49 \\ 187 & 53 \end{bmatrix}$	1069.7	57816	7.24	225.84	38123.5
$\begin{bmatrix} 34 & 139 \\ 69 & 113 \end{bmatrix}$	1078.7	57432	7.24	224.34	35882.69
$\begin{bmatrix} 212 & 187 \\ 143 & 25 \end{bmatrix}$	1039.2	58462	7.24	228.37	37090.94

5. Acknowledgement

We acknowledge the support of Covenant University in conducting this research and the cost of publication.

6. Conclusion

Image Encrytion schemes experience a variety of security attacks. Although these attacks are known, the susceptibility of encryption schemes have to be effectively investigated. This study suggests an approach to investigating the risk of image encryption schemes to some of this attack. The hill cipher scheme shows a lot of weakness to a number of attacks as the results from the previous section suggests. This study hopes to further evaluate using a variety of other encryption quality metrics and the effectiveness of hill cipher approach against other algorithms for image encryption.

References

[1] John S, Anele C, Olajide F, Kennedy CG. *Real-time Fraud Detection in The Banking Sector Using Data Mining Techniques/Algorithm*. International Conference on Computational Science and Computational Intelligence (CSCI). Las Vegas, NV, USA. 2016

[2] Awodele O, Okesola OJ, Okokpujie KO, Damilola F, Kuyoro A, Adebiyi A. Cryptography and the Improvement of Security in Wireless Sensor Networks. 2018.
[3] Jiang N, Dong X, Hu H, Ji Z, Zhang W. Quantum Image Encryption Based on Henon Mapping. *International Journal of Theoretical Physics*. 2019; 58(3): 979-991.
[4] Luo Y, Yu J, Lai W, Liu L. A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia Tools and Applications*. 2019: 1-21.
[5] Chai X, Gan Z, Yuan K, Chen Y, Liu X. A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neural Computing and Applications*. 2019; 31(1): 219-237.
[6] Piao ML, Piao YL, Kim N, editors. 3D image encryption based on computer-generated hologram in the fractional Fourier domain. Practical Holography XXXIII: Displays, Materials, and Applications. *International Society for Optics and Photonics*. 2019.
[7] Gong L, Qiu K, Deng C, Zhou N. An image compression and encryption algorithm based on chaotic system and compressive sensing. *Optics & Laser Technology.* 2019; 115: 257-267.
[8] Liansheng S, Xiao Z, Chongtian H, Ailing T, Asundi AK. Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms. *Optics and Lasers in Engineering*. 2019; 113: 29-37.
[9] Mani P, Rajan R, Shanmugam L, Joo YH. Adaptive control for fractional order induced chaotic fuzzy cellular neural networks and its application to image encryption. *Information Sciences*. 2019; 491: 74-89.
[10] Cheng Z, Haitao X, Meiqin W, Qianwen C, editors. Compressive Optical Encryption of Three-dimensional Image. Digital Holography and Three-Dimensional Imaging. *Optical Society of America*. 2019.
[11] Khan JS, Ahmad J. Chaos based efficient selective image encryption. *Multidimensional Systems and Signal Processing*. 2019; 30(2): 943-961.
[12] Nardo LG, Nepomuceno EG, Arias-Garcia J, Butusov DN. Image encryption using finite-precision error. *Chaos, Solitons & Fractals*. 2019; 123: 69-78.
[13] Aslam MN, Belazi A, Kharbech S, Talha M, Xiang W. Fourth Order MCA and Chaos-based Image Encryption Scheme. *IEEE Access.* 2019; 7: 66395-66409.
[14] El Fishawy NF, Zaid OMA. Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms. *IJ Network Security*. 2007; 5(3): 241-251.
[15] AlQaisi A, AlTarawneh M, Alqadi ZA, Sharadqah AA. Analysis of color image features extraction using texture methods. *TELKOMNIKA Telecommunication Computing Electronics and Control*. 2019; 17(3): 1220-1225.
[16] AbdelWahab OF, Hussein AI, Hamed HF, Kelash HM, Khalaf AA, Ali HM. Hiding data in images using steganography techniques with compression algorithms. *TELKOMNIKA Telecommunication Computing Electronics and Control*. 2019; 17(3): 1168-1175.
[17] Azeta J, Okokpujie IP, Okokpujie KO, Salawu EY. Analytical Study of a Road Traffic Conflict at the T-Junction of University of Benin Main Gate. *International Journal of Civil Engineering and Technology (IJCIET).* 2018; 9(8): 1048-1061.
[18] Li S, Sun W. Image encryption performance evaluation based on poker test. Advances in Multimedia. 2016.
[19] Hamid A, Ragab M, Alla OSF, Noaman AY. Encryption quality analysis of the rcbc block cipher compared with rc6 and rc5 algorithms. 2014.
[20] Ismail IA, Amin M, Diab H. A digital image encryption algorithm based a composition of two chaotic logistic maps. *IJ Network Security*. 2010; 11(1): 1-10.
[21] AL-Mousa MR, Al-salameen F, Al-Qawasmi K. Using Encryption Square Keywith One-dimensional Matrix for Enhancing RGB Color Image Encryption-Decryption. *Indonesian Journal of Electrical Engineering and Computer Science*. 2018; 9(3): 771-777
[22] Gamido HV, Sison AM, Medina RP. Implementation of Modified AES as Image Encryption Scheme. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI).* 2018; 6(3): 301-308.
[23] Ali-Pacha H, Hadj-Said N, Ali-Pacha A. *Encryption System based on a Structured Matrix: Vandermonde Matrix.* Proceeding of the Electrical Engineering Computer Science and Informatics. 2017; 4: 503-506.
[24] Chinonso O, Omoruyi O, Okokpujie K, John S. Development of an Encrypting System for an Image Viewer based on Hill Cipher Algorithm. *Covenant Journal of Engineering Technology*. 2017; 1(2): 65-73.
[25] Zhang J, Wang J, editors. *A Chaos-Based Digital Image Cryptosystem with an Improved Diffusion Strategy.* Springer, Proceedings of the 9th International Symposium on Linear Drives for Industry Applications. 2014; 1.