Journal of Information Hiding and Multimedia Signal Processing
Ubiquitous International

Volume **7**, Number **4**, July **2016**

A Secure and Robust Image Encryption Based on Chaotic Permutation Multiple Circular Shrinking and Expanding

Yohan Suryanto[1], Suryadi[2], Kalamullah Ramli[3]

[1]Department of Electrical Engineering
Universitas Indonesia, Depok, Indonesia
[2]Department of Mathematics, Universitas Indonesia, Depok, Indonesia
[3]Department of Electrical Engineering, Universitas Indonesia, Depok, Indonesia
Email: yohan.suryanto@ui.ac.id, yadi.mt@sci.ui.ac.id, and k.ramli@ee.ui.ac.id

Received January, 2016; revised March, 2016

Abstract. *In this paper, we propose a secure and robust image encryption based on the chaotic permutation multiple circular shrinking and expanding. An image with the $n \times m$ size is encrypted in n set columns and m set rows using the permutation multiple circular and linked bitxor. The proposed method characterized by a very large key space, such that for an image size of 256×256, the key space reaches 2^{862208} which is probably the largest key space ever recorded in a chaotic image encryption. It is sensitive to changes in key, so that the change 1 bit in initial key among 2^{1684} possibilities is likely to produce a significant different ciphered images (for image peppers NPCR 99.65%, UACI 33.35, $r < 0.008$). It also resistant to differential attack due to a change 1 bit in the plain image lead to completely different ciphered image (for image lena NPCR 99.60% and UACI 33.47%). The proposed method is also resistant to JPEG compression, noise scheme (Gaussian, Poisson, Salt&Pepper, and speckle), data loss, and brightness-contrast adjustment, so the ciphered image can be stored in smaller file size and transmitted in a noisy communication system.*
Keywords: Image encryption; Large key space; Chaotic permutation; Robust to noise; Circular shrinking and expanding.

1. **Introduction.** The information era continues to grow, indicated by increasing the availability of public networks based on broadband Internet Protocol (IP), supported by software defined equipment and content over the top (OTT). Transfer information becomes cheaper and more reliable if done through a public networks, however it has a consequences that the information can flow through any point in the world. Therefore the encryption system to protect the confidentiality of data including image is needed.

Research in image encryption continues to evolve to improve the security aspects, such as resistant to brute force attack, resistant to deferential analysis, resistant to statistical analysis, and robust to noise. One of the challenges in image encryption is the high correlation of the adjacent pixels, either in horizontal, vertical, or diagonal one. Hence a conventional encryption method performed on plain image, sometimes can not produce a ciphered images that are visually different from the original one [9] . Beside that, a secure encryption scheme like AES [12] if applied directly to the plain image requires a relatively longer processing time [14].

One of the image encryption method that has been fastly developed recently is based on chaotic map. However a chaotic map having discretesize problem, which is the key space of the chaotic map will be limited in discrete domain, depend on the computer precision and number of pixels. Awad [17] concluded that the implementation of the chaotic map for image encryption has limitations in discretesize space. The recent image encryption papers commonly employ combined chaotic map using permutation and diffusion, however some of them has a weakness against known image attacks [18, 19] as analyzed by Xu [22]. Furthermore other Cryptanalysis [23-26] also found that some image encryption method based on chaotic map does not meet the adequate security level. Arroyo found that the total shuffling image [27] is insecure, meanwhile C. Li also found that the compound chaotic map is also relatively insecure [28].

Research on image encryption to enhance the security aspects continue to emerge recently. Parvin [2] applied circular shift row and circular shift column which is controlled by chaotic map and combined with bitxor. Sui [5] proposed a double image encryption method based on fractional random transform and chaotic logistic map. Enayatifar [3] proposed a combination of genetic algorithm, deoxyribo nucleic acid (DNA), and logistic map. Ye [4] proposed a method based on circular row and circular column combined with generalized arnold cat map and diffusion process. Gao [16] implemented total suffling method based on logistic map and bitxor diffusion based on lorenz and chenz chaotic map. Wang [7] proposed a double image encryption method based on encoding phase and amplitude in gyrator transform domain. Wang [11] proposed a chaotic image encryption scheme based on encoding DNA combined with logistic map . Patidar [8] implemented a pseudo random permutation-substitution scheme based on chaotic standard map. Bigdeli [15] proposed a chaotic neural network combined with tent map. Enayafitar [20] proposed a hybrid method between cellular outomata and DNA. Ping [1] proposed a metode based on non-affine and balanced cellular outomata. Zhang [13] employed a pixel substitution method based on circular S-Box and bitxor using stream key. Zhang [21] proposed a method based on DNA and multi chaotic map to improve the security aspect. Wang [10] proposed a method using game of life permutation based on logistic map combined with PWLCM chaotic system. However, all of them facing the same discretion phenomenon such that the key space commonly less than 2^{300}.

The recent encryption method exhibit characteristics that are resistant to differential analysis, statistical analysis and brute force attack, but not all of them resistant to noise. The interesting one is the single rotation method proposed by Parvin [2] that exhibit both high security aspect and robustness to noise at certain level. However, the key space of the Parvin proposed method is only 2^{202}, it is less then the key space figure required by a modern cryptography since appearance of the quantum computer [29]. A robust encryption method against JPEG compression, noise, and data loss allows the cipher image is stored in relative smaller file size than the original one, and tolerant to transmission error.

In this paper we propose an image encryption method based on the chaotic permutation multiple circular shrinking and expanding, where the key is generated by the expanded key, combined with linked bitxor to achieve both high security aspect and robustness to noise. The proposed method overcome the discretization problem, so that in a discrete system the key space is extremely large. This paper is presented in the following order: 1. Introduction, 2. The Chaotic Permutation Multiple Circular Shrinking and Expanding, 3. The Proposed Image Encryption Method, 4. The Experiment Platform, 5. The Result and Analysis, 6. Conclusion

2. **The Chaotic Permutation Multiple Circular Shrinking and Expanding.**

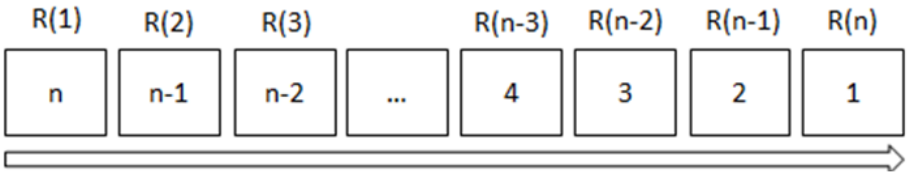

FIGURE 1. Number of element involved in every round R(i) of the permutation set P_n

2.1. **The Permutation Multiple Circular Shrinking and Expanding.** The chaotic permutation multiple circular shrinking and expanding (CPMCS and CPMCE) has a chaotic properties as discussed in Suryanto et al. [30]. Set X with n number of elements, has a possibility of as many as n factorial permutations. In the first round R(1) there are n elements that can be selected, in the second round R(2) there are *n-1* elements that can be selected, and so on reduce one element for the next round until round R(n) that consist of single remaining element as illustrated in Figure 1. Due to every element selected in each round is excluded in the next round, then surely the alternative number of unique arrangement set X in each round is equal to the number of involved elements. As a result, there is n factorial unique arrangement of set X for all round.

Permutation technique that maps the set X into n factorial possible unique arrangement can be done using multiple circular with moduli equal to the number of elements involved in each round. Circular method is chosen because it is easy to be implemented in a software or hardware and directly correlated with a key that determines distance of the shifting. A single circular shift function of the set X having n elements and the shifting distance as far as k is described in Equation (1). If we take the first element $X_n^{k(0)}(0)$ as the permuted element $Y_n(0)$ and exclude it for the next round, continuing the process and take $X_{n-1}^{k(1)}(0)$ as the permuted element of the $Y_n(1)$, $X_{n-2}^{k(2)}$ as $Y_n(2)$ an so on until $X_2^{k(n-2)}$ as $Y_n(n-2)$ and the remaining element as $Y_n(n-1)$, then we can write a complete set of permutations X_n become a set Y_n accordance with Equation (2). If we chose $\odot$ as an operator of the permutation multiple circular shrinking (PMCS) which is defined in the Equation (3), then the Equation (2) can be rewriten as Equation (4).

$$X_n^k(i) = X(mod(i+k,n)); n \in Z^+,\ 0 \le i < n,\ 0 \le k < n \tag{1}$$

$$Y_n = \ X_{n-j}^{k(j)}(0)]_{j=0}^{n-1}; n \in Z^+,\ 0 \le j < n\ ,\ 0 \le k < n \wedge k(j) < n-j \tag{2}$$

$$\odot(X_n) = \mathrm{X}_{n-j}^{k(j)}(0)]_{j=0}^{n-1} \tag{3}$$

$$Y_n = \odot(X_n) \tag{4}$$

To obtain set X_n from set Y_n can be done by permutation multiple circular expanding (PMCE) which is the number of involved elements is increasing for each round. If we have set Y_n having n elements and defined the last 2 elements as Y_2 , the last 3 elements as Y_3 and so on, and defined set X_2 as mapping of Y_2 at first round, the relation between X_2 and Y_2 can be writen in accordance with the Equation (5). In the second round of the circular expanding, set X_3 is a mapping of Y_3 according with the Equation (6). The circular expanding continue until Y_n([0,n-1]), then set X_n is a mapping of Y_n according with the Equation (7). If we chose $\otimes$ as an operator of the permutation multiple circular expanding

(PMCE) which is defined as Equation (8), then the Equation (7) can be rewriten as Equation (9). According with the Equation (4) and (9), PMCE is the inverse of PMCS.

$$X_2 = \mathrm{Y}_2^{k(n-2)}, Y\left(n-2, n-1\right) \ = X_2 \tag{5}$$

$$X_3 = \mathrm{Y}_3^{k(n-3)}, \ Y\left(n-3, n-1\right) = X_3 \tag{6}$$

$$X_n = \ Y_j^{k(n-j)}]_{j=2}^{n}; \ n \in Z^+, \ 0 \le j < n \ , 0 \le k < n \wedge (k < j \ ) \tag{7}$$

$$\otimes\left(Y_n\right) \ = \ Y_j^{k(n-j)}]_{j=2}^{n}; \ n \in Z^+, \ 0 \le j < n \ , \ 0 \le k < n \wedge (k < j \ ) \tag{8}$$

$$X_n = \otimes\left(Y_n\right) \tag{9}$$

2.2. **The Expanded Key.** The expanded key of the permutation multiple circular is key generator to generate a set key for the permutation multiple circular shrinking and expanding. The mapping $\odot(X_n)$ become Y_n or the mapping $\otimes Y_n$ become X_n is determined by a set k as described in section 2.1. Since the remaining element in the last round of PMCS is only 1 element, both PMCS and PMCE require set k consist of n-1 elements.

In order to make the both functions $\odot(X_n)$ and $\otimes Y_n$ having a chaotic behavior [30], then the set key should be derived from the initial key and the sequence. We proposed an expanded key to generate set key that related to initial key so that the output of the PMCS and PMCE sensitive to the initial key and each initial key having a unique domain sequence. The sequence number is distributed evenly in a key set according with the Equation (10), meanwhile the initial key is distributed in Key_k according with Equation (12). The moduli B_k is constructed according with Equation (11), meanwhile the numerator T is constructed according to Equation (13). The key set for PMCS and PMCE is constructed from Key_s and Key_k according to Equation (14).

$$Key_s\left(i\right) = mod\left(Sequence, n-i\right); \ n \in Z^+, 0 \le i \le n-2 \tag{10}$$

$$B_k\left(i\right) = \begin{cases} 1, \ (n-i) \in \ P \\ n-i, \ (n-i) \notin P\Lambda\omega\left(n-i\right) > 1 \\ \frac{n-i}{factor}, \ (n-i) \notin P\Lambda\omega\left(n-i\right) = 1 \end{cases} \tag{11}$$

$$Key_k\left(i\right) = mod\left(T\left(i\right), B_k\left(i\right)\right); \ n \in Z^+, 0 \le i \le n-2 \tag{12}$$

$$T\left(i\right) = \begin{cases} Initial \ key, \ i = 0 \\ \lfloor \frac{T(i-1)}{B_k(i-1)} \rfloor + Key_k\left(i-1\right), \ i \in Z \ \Lambda 0 < i \le n-2 \end{cases} \tag{13}$$

$$Key\left(i\right) = mod((Key_s + Key_k), n-i); n \in Z^+, 0 \le i \le n-2 \tag{14}$$

3. The Proposed Encryption and Decryption Algorithm.

3.1. **The linked and delinked bitxor.** Linked bitxor of the set P_n is bitxor between the element P_n with the previous bitxor results C_n written in Equation (15). If we define an operator linked bitxor [>] as Equation (16), then the Equation (15) can be writen as Equation (17). To obtain P_n from C_n is used de-linked bitxor according to Equation (18). If we define an operator delinked bitxor [<] as Equation (19), then the Equation (18) can be writen as Equation (20).

$$C_n\left(i\right) = \begin{cases} bitxor\left(P_n\left(0\right), c\right), \ i = 0, \ c \in \ Z\Lambda c < n \\ bitxor\left(P_n\left(i\right), C_n\left(i-1\right)\right), \ i \in \ Z\Lambda 0 < i \le n-1 \end{cases} \tag{15}$$

$$[>]\left(P_n\right) = \begin{cases} bitxor\left(P_n\left(0\right), c\right), \ i = 0, \ c \in \ Z\Lambda c < n \\ bitxor\left(P_n\left(i\right), C_n\left(i-1\right)\right), \ i \in \ Z\Lambda 0 < i \le n-1 \end{cases} \tag{16}$$

$$C_n = [>]\left(P_n\right) \tag{17}$$

$$P_n(i) = \begin{cases} bitxor(C_n(0), c), & i = 0,\ c \in Z\Lambda c < n \\ bitxor(C_n(i), C_n(i-1)), & i \in Z\Lambda 0 < i \leq n-1 \end{cases} \tag{18}$$

$$[<](C_n) = \begin{cases} bitxor(C_n(0), c), & i = 0,\ c \in Z\Lambda c < n \\ bitxor(C_n(i), C_n(i-1)), & i \in Z\Lambda 0 < i \leq n-1 \end{cases} \tag{19}$$

$$P_n = [<](C_n) \tag{20}$$

3.2. **The proposed image encryption algorithm.** An arbitrary initial key is selected along with the sequence number as input to the expanded key. The sequence number is the sum of all pixels of the plain image so that the ciphered image sensitive to changes in the plain image . The output of the expanded key is a set of keys to control multiple circular permutation shrinking (PMCS). Plain image is divided into m sets row, each consist of n elements referred as P_n . Each P_n starting from the first row to m^{th} row permuted using PMCS followed by linked bitxor in accordance to the Equation (21), so that would be obtained m x set C_n . Combined m x set C_n is ciphered image in stage 1, then it is divided into n x set column C_m. Each C_m permuted using PMCS in accordance to the Equation (22) . The combined set of C_m constitute ciphered image of the corresponding plain image. Overall, the proposed encryption method can be discribed in Figure 2.

$$C_n = [>](\odot(P_n)) \tag{21}$$

$$C_m = \odot(C_m) \tag{22}$$

3.3. **The proposed decryption algorithm.** The same initial key and the sequence number used in encryption process as input to the expanded key. The output of the expanded key is a set of keys to control multiple circular permutation expanding (PMCE). Ciphered image is divided into n x set column, each consist of m elements referred as C_m . Each C_m starting from the first column to the n^{th} column permuted using PMCE in accordance to Equation (23). The combined of n x set C_m constitute the deciphered image in the first stage. Then it is divided into m x sets of row referred as C_n . Each set C_n permuted using PMCE followed by delinked bitxor according to the Equation (24). The combined n x set C_n represent the coresponding plain image. Overall, the proposed decryption method can be shown in Figure 3.

$$C_m = \otimes(C_m) \tag{23}$$

$$P_n = [<](\otimes(C_m)) \tag{24}$$

4. **The Experiment Platform.** An experiment to analyze performance of the proposed method is performed using Matlab 8.5 on computer intel(R) core(TM) i7-5500U CPU @2.4 GH, RAM 8 GB windows 10, 64 bit. There are 7 sets of the plain image for each performed test, with the result as shown in Figure 4.

The 15 recent proposed methods with a high level of security as discussed in the introduction is used as comparison. The data that has been published in each journal is used for the references except the PSNR values submitted by Parvin [2] need further adjustment due to maximum intensity for a gray image is 255. The PSNR data is corected based on the given MSE value accordingly.

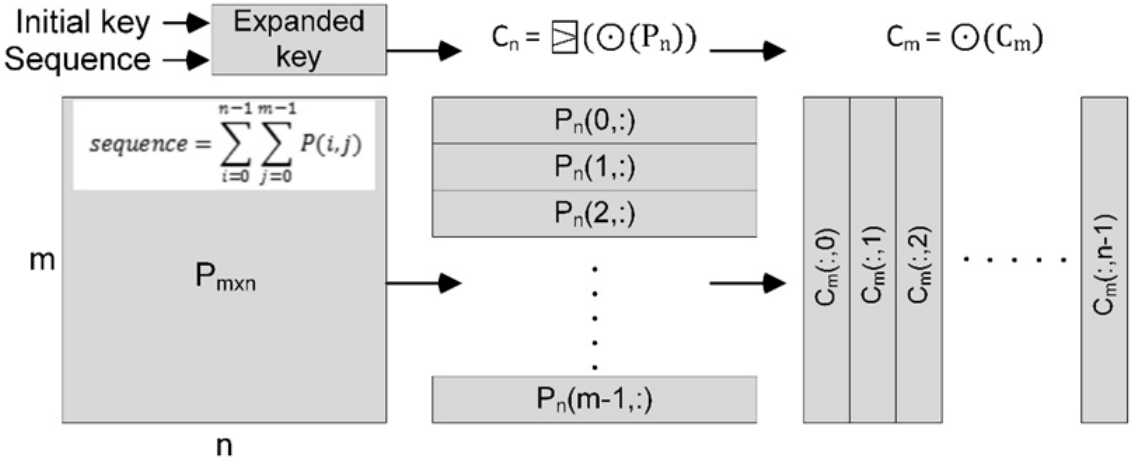

FIGURE 2. The proposed encryption algorithm

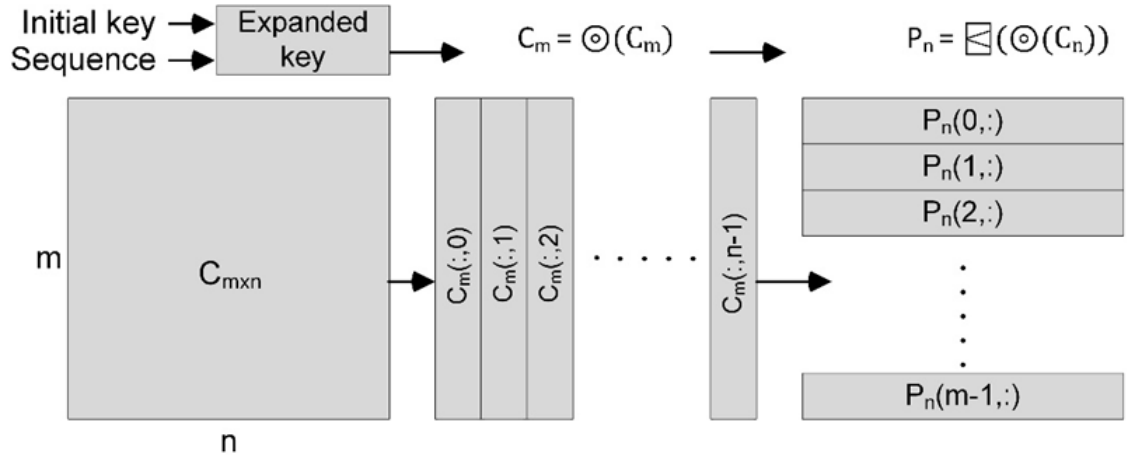

FIGURE 3. The proposed decryption algorithm

5. **The Result and Analysis.** Analysis schemes to measure performance of the proposed method are: visualization, statistical analysis (histogram, correlation, entropy analysis), differential analysis (NPCR, UACI), key sensitivity (NPCR, UACI, correlation), key space, speed of the encryption and decryption process, robustness to jpeg compression, robustness to noise, robustness to data loss, robustness to brightness and contrast adjusment.

5.1. **Visualization.** An image has a high correlation in adjacent pixels either horizontally, vertically or diagonally. Therefore, the ciphered image should be checked visually to determine whether the employed encryption scheme is able to produce a chippered image that completely different to the original one. According to the Figure 4, the proposed method produces a completely unrecognizable ciphered image. Meanwhile the deciphered image is visualy same as the coresponding plain image respectively.

5.2. **Statistical analysis (histogram, correlation analysis, entropy).** A histogram of an image is the distribution diagram of each pixel value of the image. Good ciphered image should have a uniform histogram to prevent an attacker exploit any useful statistical information. Histogram of the ciphered image for each set of the plain image can be seen

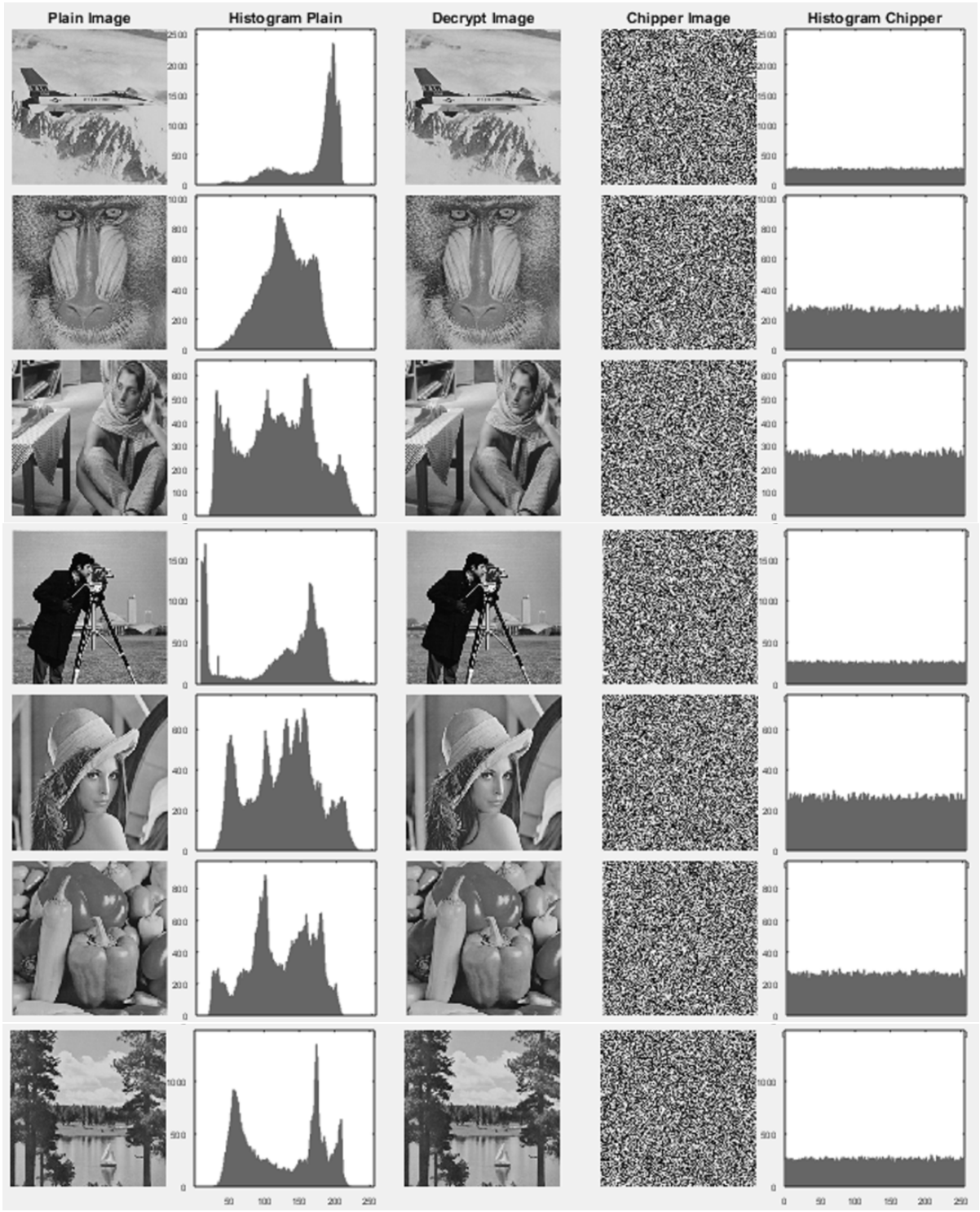

FIGURE 4. Visualization of the plain image, plain histogram, decrypted image, ciphered image, and the ciphered histogram

in fifth column of Figure 4. Clearly that the proposed method produce the ciphered image characterized by uniform histogram and completely different to the histogram of the coresponding plain image.

A correlation analysis is performed to test the correlation between the adjacent pixels of the ciphered image. A good ciphered image must have a low correlation coefficient as can be described according to the Equation (25) [31]. Where r_{xy} is the correlation

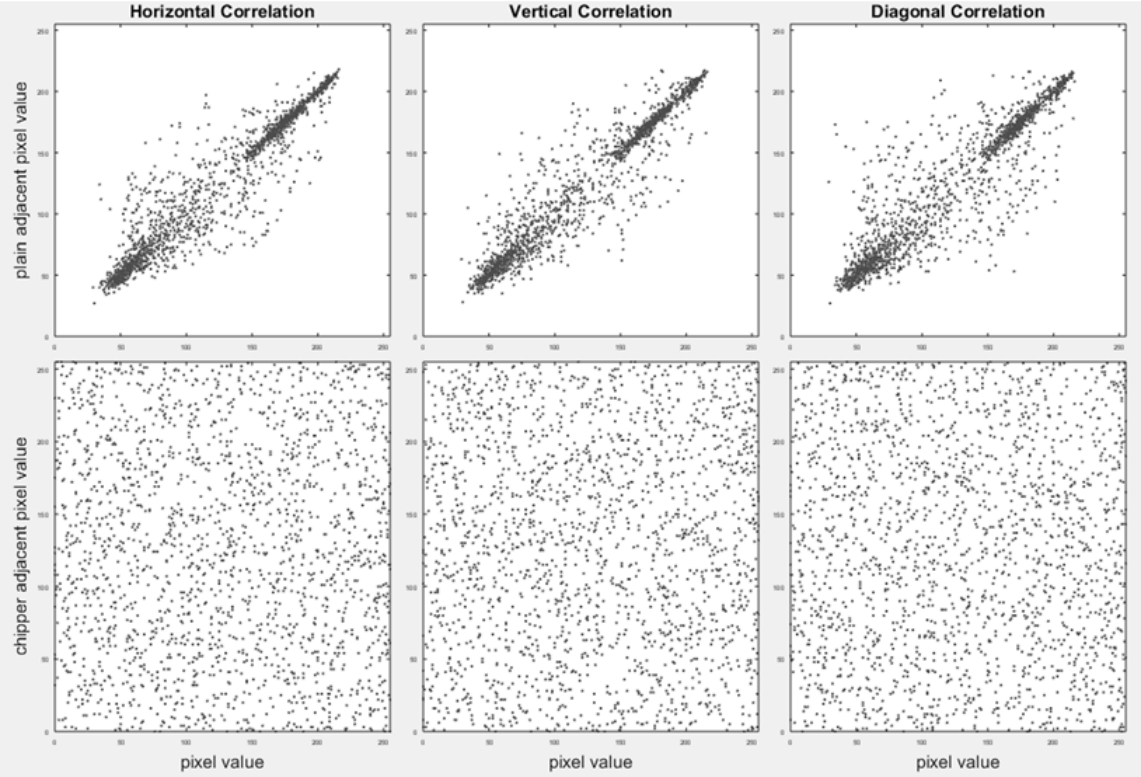

FIGURE 5. Distribution of the adjacent pixel correlation in horizontal, vertical, and diagonal respectively

coefficient between the vectors X and Y. Vector X is a vector consisting of 2500 pixels randomly selected from the ciphered image. Vector $Y_{horizontal}$, $Y_{vertical}$, and $Y_{diagonal}$, is a same size vector to X, chosen from ciphered image with position X (i, j+1), X(i+1, j), and X(i+1, j+1) respectively.

$$r_{xy} = \frac{\sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n} (x_i - \bar{x})^2 \sum_{i=1}^{n} (y_i - \bar{y})^2}} \tag{25}$$

Distribution of the adjacent pixels of the plain and ciphered image lena horizontally, vertically and diagonally can be observed in Figure 5. It appears that the distribution of the adjacent pixels of the ciphered image using the proposed method is highly dispersed which indicates the ciphered image has a very low correlation. Meanwhile, the correlation coefficient of the each ciphered image horizontally, vertically, and diagonally, can be seen in Table 1. It shows that the proposed method produces ciphered image caracterized by very low correlation. The comparison of the correlation coefficient with the reference scheme for the ciphered image lena can be observed in Table 2. It is clearly that the proposed method has the lowest correlation coefficient compared to the paper references, either in horizontal, vertical, or diagonal correlation respectively.

The Shannon entropy is performed in accordance to Equation (26) [8] to measure the average minimum number of bits need to encode a string of symbols in the plain and chipper image. P(i) represents the probability of a pixel i. For the 8-bit gray level image, there is 256 different values, so that if it spread evenly then the probability of each value is 1/256. This means that the perfect entropy for gray level image is 8. The entropy of the ciphered image using the proposed method can be explored in Table 3. It shows that the proposed method generate ciphered image exhibit very high entropy value, close

TABLE 1. Correlation between the plain image and the ciphered image

Image Correlation	Horizontal		Vertical		Diagonal	
	Plain	**Cipher**	**Plain**	**Cipher**	**Plain**	**Cipher**
Airplane	0.9374	0.0100	0.9390	0.0011	0.8921	-0.0164
baboon	0.8656	-0.0070	0.8163	0.0059	0.7716	-0.0090
barbara	0.9453	0.0138	0.9637	0.0046	0.9258	-0.0009
cameraman	0.9286	0.0096	0.9190	-0.0130	0.8682	-0.0132
lena	0.9468	-0.0003	0.9729	-0.0030	0.9219	0.0028
peppers	0.9627	0.0076	0.9732	-0.0074	0.9378	0.0128
sailboat	0.9547	-0.0047	0.9538	-0.0021	0.9231	0.0055

TABLE 2. The correlation comparison to the references scheme for lena image

Scheme	**Horizontal**	**Vertical**	**Diagonal**	**Total(abs)**
Plain image	0.9468	0.9729	0.9219	2.8416
Proposed algorithm	-0.0003	-0.0030	0.0028	0.0061
Parvin et al. [2]	0.0018	0.0345	0.0202	0.0565
Sui et al. [5]	-0.0069	-0.0188	-0.0482	0.0739
Enayatifar etal. [3]	0.0058	0.0072	0.0031	0.0161
Ye et al. [4]	0.0770	-0.0724	-0.0615	0.2109
Gao et al. [16]	-0.0131	-0.0273	-0.0313	0.0717
Ye et al. [6]	-0.0685	0.0087	-0.0739	0.1511

TABLE 3. The information entropy of the plain and the ciphered image

Entropy Image	**airplane**	**baboon**	**barbara**	**camera man**	**lena**	**peppers**	**sailboat**
plain image	6.5146	7.0092	7.5838	7.0383	7.4318	7.3611	7.2396
ciphered image	7.9973	7.9970	7.9975	7.9971	7.9975	7.9973	7.9972

TABLE 4. The comparison of information entropy with the references scheme

Analysis	Proposed Scheme	Parvin et al. [2]	Enaya-tifar et al. [3]	Wang et al. [11]	Big-deli et-al.[15]	Ping et al. [1]	Zang et al. [13]	Enaya-tifar et-al.[20]
Entropy	7.9975	7.9969	7.9992	7.9970	7.9972	7.9971	7.9850	7.9980

to 8. The entropy comparison of the ciphered image lena can be observed in Table 4. It indicates that the proposed method though not yield the highest entropy value, yet among the best.

$$H = -\sum_{i=0}^{2^n-1} P_i log_2 (P_i) \tag{26}$$

5.3. **Differential analysis (NPCR, UACI).** Differential analysis is intended to measure the difference between the ciphered images if the plain image changed one bit. Differential analysis was tested using the number of changing pixel rate (NPCR) and the unified averaged intensity changed (UACI). This method is used to test how much difference between the two images [32] in accordance to Equation (27-29).

TABLE 5. NPCR and UACI between two ciphered image respected to 1 bit difference in the plain image

Image	**NPCR (%)**	**UACI (%)**
airplane	99.56	33.38
baboon	99.60	33.40
barbara	99.64	33.38
cameraman	99.57	33.35
lena	99.60	33.47
peppers	99.59	33.44
sailboat	99.57	33.49

TABLE 6. The NPCR and UACI comparison in differential analysis

Scheme	**NPCR (%)**	**UACI (%)**
Proposed	99.60	33.47
Parvin et al.[2]	100.00	33.10
Ye et al.[4]	99.60	33.40
Ye et al.[6]	99.65	33.51
Zhang et al. [13]	99.61	33.46
Ping et. al[1]	99.66	33.48
Enayatifar et al.[20](airplane)	99.03	32.84

$$D_{ij} = \begin{cases} 0, \ if \ X_{ij} = Y_{ij} \\ 1, \ if \ X_{ij} \neq Y_{ij} \end{cases} \tag{27}$$

$$NPCR = \sum_i \sum_j \frac{D_{ij}}{N} \ x \ 100\% \tag{28}$$

$$UACI = \sum_i \sum_j \frac{|X_{ij} - Y_{ij}|}{F.N} \ x \ 100\% \tag{29}$$

The better an encryption method, then change one bit on the plain image will lead to significant difference in the ciphered image. The NPCR and UACI value between the two ciphered image generated by the proposed method when the plain image change one bit is very high as can be observed in Table 5. The comparison of the NPCR and UACI values for differential test statistic by a variety of methods can be explored in Table 6. According to it, Parvins method [2] despite having the highest NPCR value, however the UACI value is lower than the proposed method.

5.4. **Key Sensitivity (NPCR, UACI, Correlation).** Key sensitivity test is intended to determine how sensitive an encryption method to slightly changes in key. One bit change in key bring out significant changes both in the ciphered and the deciphered image. Tabel 7 exhibit the NPCR, UACI, and coefficient correlation values between two ciphered image respected to 1 bit difference in key using the proposed method. The first key is 987654321012345, meanwhile the second key is 987654321012346. Because the initial key space of PMCS for set P_{256} is 2^{1684}, then one bit change in the key means only change as many as 2^{-1684} in the key space. According to Tabel 7, it can be concluded that the proposed method extremely sensitive to the key changes.

TABLE 7. NPCR, UACI, and correlation coefficient between two ciphered image respected to 1 bit difference in key

Image	**NPCR (%)**	**UACI (%)**	**Correlation**		
			Horizontal	**Vertical**	**Diagonal**
airplane	99.55	33.54	-0.0060	-0.0145	-0.0121
baboon	99.61	33.44	0.0014	0.0213	-0.0206
barbara	99.63	33.49	-0.0019	-0.0047	0.0027
cameraman	99.62	33.60	0.0159	0.0005	0.0062
lena	99.65	33.22	0.0038	-0.0021	-0.0162
peppers	99.65	33.56	-0.0001	-0.0074	-0.0076
sailboat	99.59	33.47	0.0016	0.0057	0.0142

TABLE 8. The comparison of NPCR, UACI, and correlation coefficient between two ciphered image respected to 1 bit difference in key

Scheme	**NPCR (%)**	**UACI (%)**	**correlation**
Proposed scheme	99.64	33.45	-0.0021
Parvin et al.[2]	88.72	29.74	na
Patidar et al.[8]	na	na	0.0035
Ping et al.[1](peppers)	na	na	0.0370
Zhang et al.[13]	99.61	33.46	na

TABLE 9. The key space comparison

Analysis	Proposed Scheme	Parvin [2]	Ye et-al.[6]	Patidar [8]	Bigdeli [[15]	Ping [1]	Zhang [21]	Sui [5]	Wang [7]	Zhang [13]	Wang [10]
Key Space	2^{862208}	2^{202}	2^{242}	2^{161}	2^{224}	2^{256}	2^{279}	2^{256228}	2^{279}	2^{280}	2^{220}

TABLE 10. The processsing speed comparison

Analysis	Proposed Scheme	Ping et al.[1]	Enayatifar et al.[3]	Ye et al.[4]	Wang et al.[10]
Encryption speed (ms)	392	1184	3284	150	2837

The comparison of the NPCR, UACI, and correlation coefficient respected to 1 bit difference in key among the references paper is presented in Table 8. It indicates that the proposed method has the highest sensitivity in respect to the key change.

5.5. **Key Space.** As a result of the key space for each round in PMCS and PMCE is equal to the number of involved elements, then the key space for complete round of the PMCS and PMCE is n factorial, where n is the number of elements. According to the Equation (10-14), the initial key and sequence number is distributed into the set key uniquely. It brings a consequence that the key space of the combined initial key and the sequence number is also n factorial. Because the PMCS and PMCE is employed for each row and column of the image, then the different combined initial key and sequence can be used in the proposed encryption and decryption as depicted in Figure 2. As a result, the total key space of the proposed method to encrypt and decrypt an image with

a size of 256x256 pixels is equal to $(n!)^{(256+256)} = (256!)^{512} = 2^{862208}$. It is extremely high FIGURE, thus the proposed method is resistant to brute force attack.

The key space comparison among the references paper is listed in Tabel 9. It shows that the proposed method has the largest key space among the references paper. This figure is also much higher than the key space of the combination method based on chaotic map, Henon and logistic map reaching 2^{199} by Chong [33] or the combination method based on logistic map, tent map, and sine map reaching 2^{279} proposed by Zhou [34]. Futhermore it is probably the largest ever recorded key space for image encryption for image size 256×256 pixels.

5.6. **Speed performance of the encryption and decryption.** The speed performance depends on many factor such as the number of iterations, the type of performed calculations, as well as the performance of the used computer. Therefore, it is difficult to compare apple to apple the speed performance based on the published data, because it use different platform and employ different spesific programming approach. However the speed performance among the references paper is presented in Table 10. It is intended only as an general overview of the speed performance of the proposed method compare to the references method. According to Table 10, among the high secure encryption method, the proposed method offer a relatively fast processing speed.

5.7. **Robustness to jpeg compression.** This test aims to measure the degree of similarity between the plain image and the deciphered image when the ciphered image is compressed using JPEG. Peak Signal to Noise Ratio (PSNR) [35] according to the Equation (30) and Mean Square Error (MSE) according to the Equation (31) is utilized to measure the robustness against jpeg compression. Where I_{max} is maximum intensity of the image (255 for gray level image). The higher the PSNR and the lower the MSE between the plain image and dechipered image after the ciphered image experiencing jpeg compression, indicating that the encryption method is more robust to JPEG compression.

$$PSNR = 10xlog_{10}(\frac{I^2_{\max}}{MSE}) \tag{30}$$

$$MSE = \frac{1}{mxn}\sum_{i=1}^{n}\sum_{j=1}^{m}(X_{ij} - Y_{ij})^2 \tag{31}$$

The deciphered lena when the coresponding ciphered image encounter JPEG compression with different levels of quality can be seen in Figure 6. It clearly indicates that the proposed method robust to JPEG compression. As a comparison, the PSNR value published by Parwin [2] is adjusted according to the corresponding MSE value, becouse the maximum intensity of a gray image is 255. Based on Tabel 11, the proposed method is more robust to the JPEG compression than Parvin [2], represented by PSNR 16.65 against PSNR 14.89 repectively. The ciphered lena can be stored in 1/1.88 of the original one when compressed using JPEG 70% yet still can be recostructed as can be seen in Figure 6.

5.8. **Robustness to noise.** The experiment analyze the degree of similarity between the plain image and the deciphered image when the ciphered image encounter noises such as Gaussian noise, Poisson noise, Salt and Pepper noise, and speckle. The higher the PSNR and the lower the MSE between the plain image and dechipered image when the ciphered image experiencing the noise, indicating the encryption method more robust to noise.
Figure 7 demonstrate that the decrypted image can be reconstructed even the ciphered image encounter noises ie: Gausian with v = 0:01, Poisson, salt & peppers, and speckle v

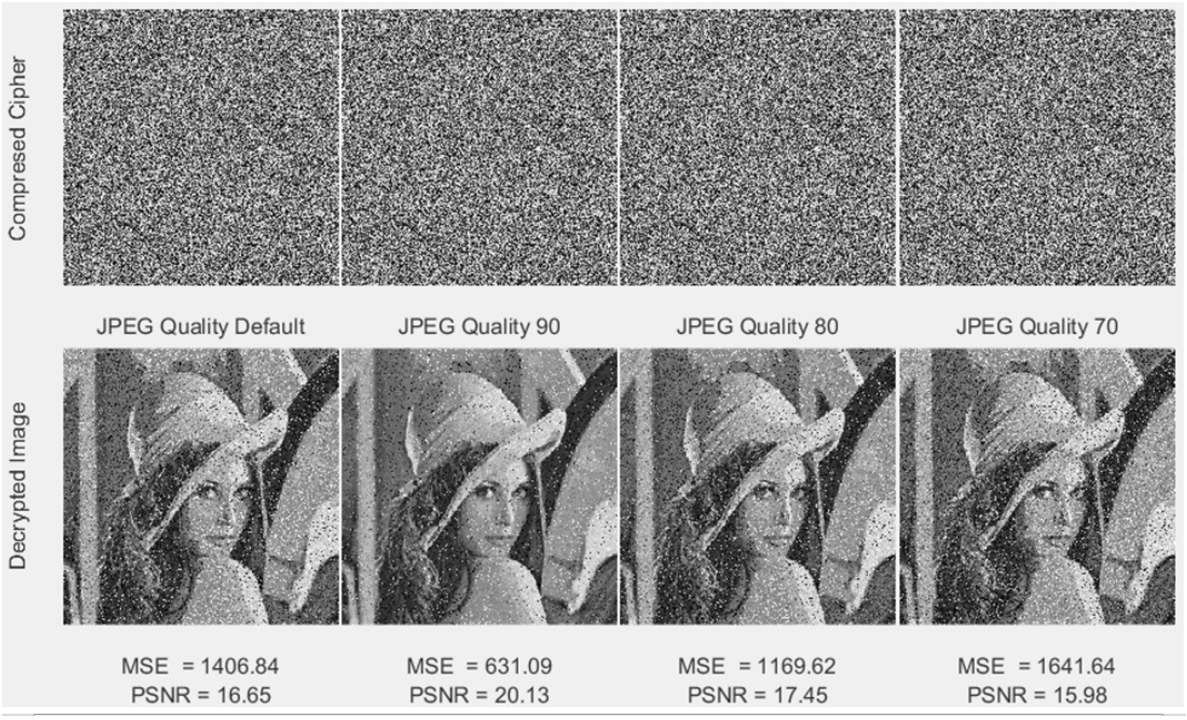

FIGURE 6. The decrypted image of the ciphered image in regard to jpeg compression with different quality respectively

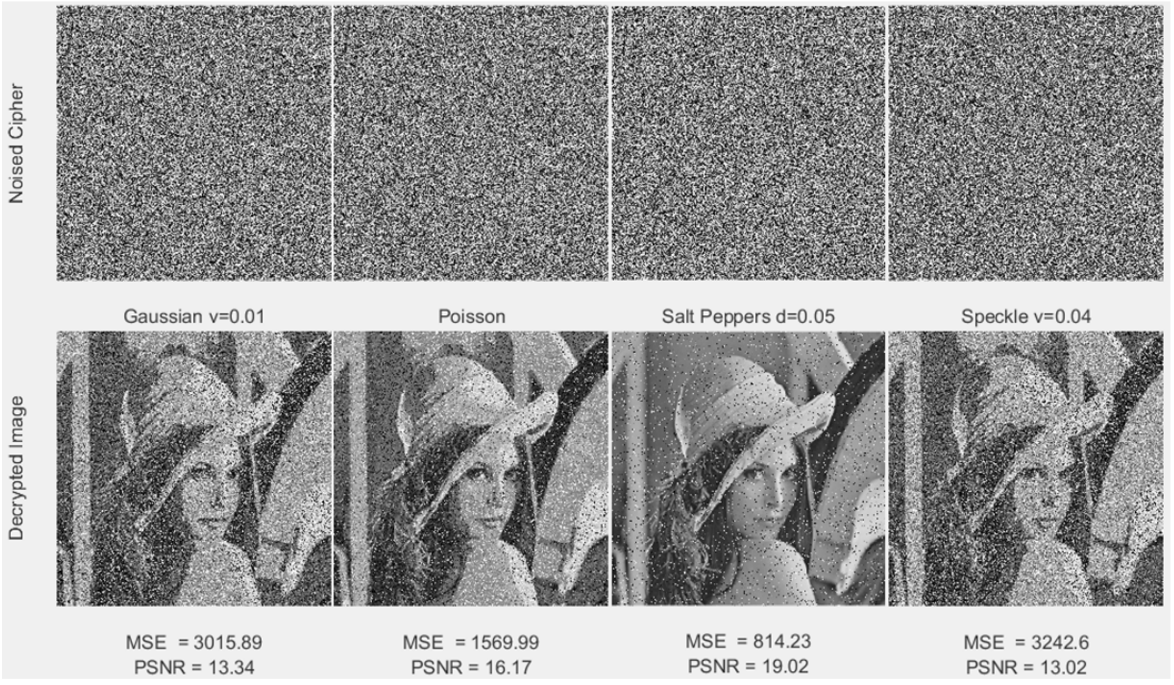

FIGURE 7. The decrypted image of the noised ciphered image with different noise scheme respectively

= 0:04. The relatively high value of the MSE and the PSNR indicates that the proposed method robust to noise. According to Tabel 12, the proposed method more robust to noise than Parvin [2] and comparable to Wang [7].

Table 11. The comparison of robustness to jpeg compression

JPEG Quality	Proposed Algorithm				Parvin et al.[2]	
	MSE	PSNR	Size(kB)	Ratio	MSE	PSNR
default	1406.84	16.65	36	1.78	2110.04	14.89
90	631.09	20.13	50	1.28		
80	1169.62	17.45	41	1.56		
70	1641.64	15.98	34	1.88		

Table 12. The comparison of robustness to noise

Noise Scheme	Proposed Algorithm		Parvin et al.[2]		Wang et al.[7] v=0.04	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
Gaussian v=0.01	2946.19	13.34	4410.1	11.69	2013	15.09
Poisson	1581.70	16.17				
Salt &Peppers d=0.05	765.06	19.02	869.89	18.74		
Speckle v=0.04	3267.99	13.02				

Table 13. The comparison of robustness to data loss

Loss Scheme	Proposed Algorithm		Parvin et al.[2]	
	MSE	PSNR	MSE	PSNR
Loss 20 row	1253.42	17.15	1073.08	17.86
Loss 20 column	1437.11	16.56	946.02	18.41
Loss 50x50(1)	636.62	20.09		
Loss 50x50(2)	612.31	20.26		

5.9. **Robustness to Data Loss.** The test measures the degree of similarity between the plain image and the deciphered image when the ciphered image encounter data loss. The higher the PSNR and the lower the MSE between the plain image and deciphered image when the ciphered image experiencing data loss, indicates the encryption method more robust to data loss. FIGURE 8 shows that the decrypted image can be reconstructed even the ciphered image encounter some data loss scheme ie: loss 20 row, loss 20 collumn, and loss 50x50 pixels. The relatively high value of the MSE and the PSNR demonstrate that the proposed method robust to data loss. Correspond to Table 13, despite the proposed method less robust to data loss than Parvin [2], however the NPCR and MSE score is comparable, for instance incase data loss 20 row it is 17.15 against 17.86 respectively.

5.10. **Robustness to Brightness and Contrast Adjustment.** The test analyze the degree of similarity between the plain image and the deciphered image when the ciphered image encounter brightness and contrast adjustment. The higher the PSNR and the lower the MSE between the plain image and deciphered image when the ciphered image experiencing brightness and contrast adjustment, demonstrates that the encryption method more robust to brightness and contrast adjustment. Figure 9 exhibit that proposed method able to reconstruct decrypted image even the coresponding ciphered image encounter change in 10% in intensity and contrast respectively.

6. **Conclusion.** The proposed method based on chaotic permutation multiple circular shrinking and expanding (PMCS/ PMCE) combined with linked bitxor. According to the correlation analysis, it is clearly that the proposed method has the lowest correlation

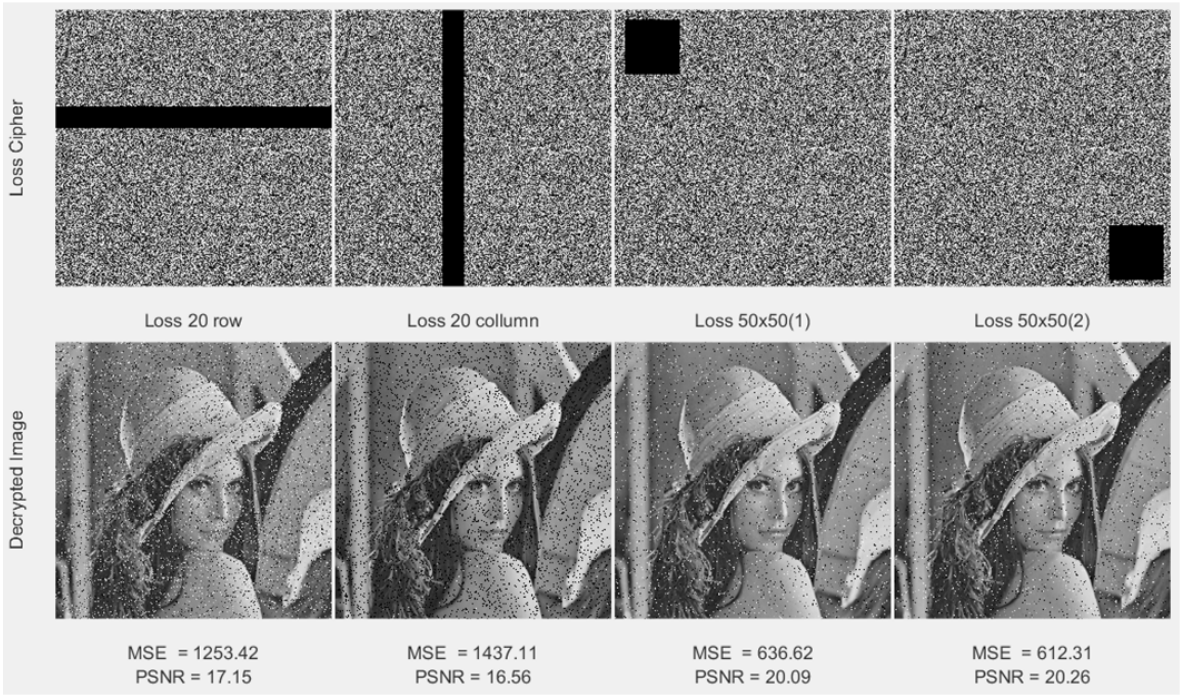

FIGURE 8. The decrypted image of the ciphered image with different data loss scheme respectively

coefficient compared to the paper references, either in horizontal, vertical, or diagonal correlation respectively. The proposed method extremely sensitive to the key changes. One bit change in the key means only change as many as 2^{-1684} in the key space lead to significantly different ciphered image, for the image peppers it indicates by the NPCR 99.65%, the UACI 33.35, and the correlation < 0.008. It also characterized by very large key space, such that for an image size of 256×256, the key space reaches to $(n!)^{(256+256)} = (256!)^{512} = 2^{862208}$. It is probably the largest ever recorded key space for image encryption for image size 256×256 pixels.

Based on the statistical analysis (histogram, correlation, dan entropy) the proposed method resistant to statistical attack. It also resistant to differential attack due to change a single bit in the plain image causes a significant change in the ciphered image (for image lena NPCR 99.60% and UACI 33.47%). The proposed method is also resistant to JPEG compression, noise scheme (Gaussian, Poisson, Salt&Pepper, and spekle), data loss, and brightness-contrast adjustment, so the ciphered image can be stored in smaller file size and transmitted in a non error free communication system.

Acknowledgment. Prof. Akhmad Herman Yuwono, Associate Dean for Research and Community Services Faculty of Engineering-Universitas Indonesia in providing highly valuable advice during writing our research. Yohan also acknowledges to Rambinet Digital Network in providing research grant ($RDN\_RG/III/2015$).

REFERENCES

[1] P. Ping, F. Xu, and Z. J. Wang, Image encryption based on non-affine and balanced cellular automata, *Signal Processing*, vol. 105, pp. 419-429, 2014.

[2] Z. Parvin, H. Seyedarabi, and M. Shamsi, A new secure and sensitive image encryption scheme based on new substitution with chaotic function, *Multimedia Tools and Applications*, pp. 1-18, 2014.

[3] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence, *Optics and Lasers in Engineering*, vol. 56, pp. 83-93, 2014.

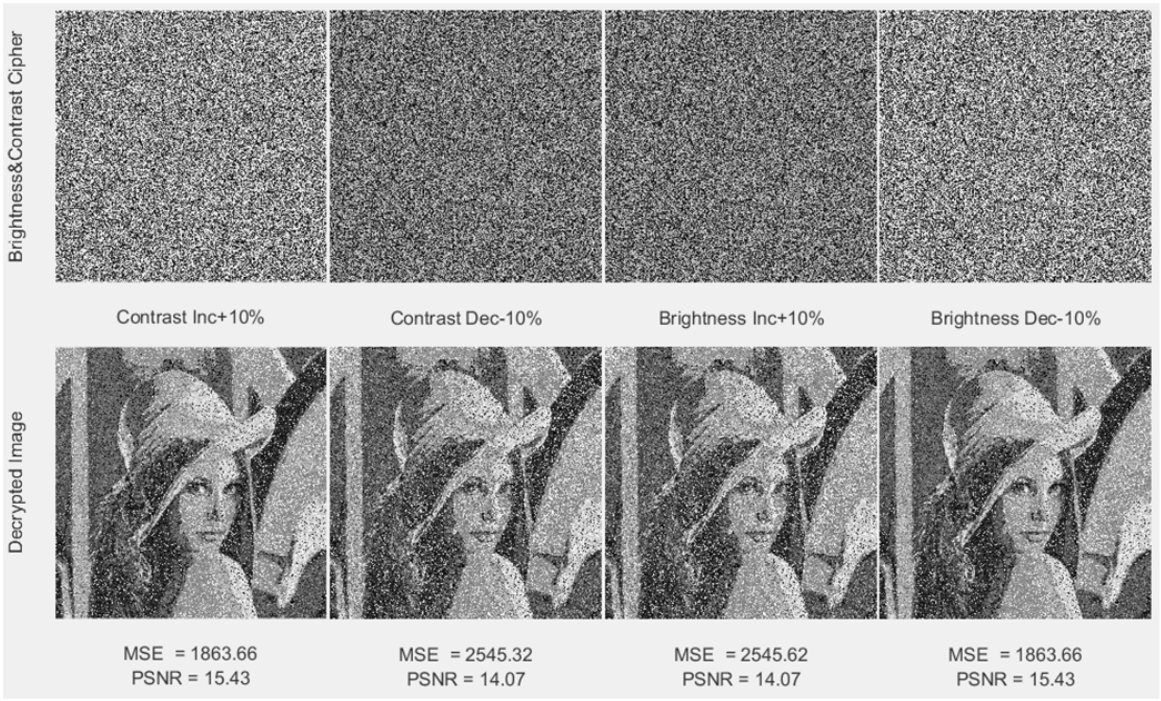

FIGURE 9. The decrypted image of the ciphered image with brightness and contrast adjustment

[4] G. Ye and K.-W. Wong, An efficient chaotic image encryption algorithm based on a generalized Arnold map, *Nonlinear dynamics*, vol. 69, pp. 2079-2087, 2012.
[5] L. Sui, H. Lu, Z. Wang, and Q. Sun, Double-image encryption using discrete fractional random transform and logistic maps, *Optics and Lasers in Engineering*, vol. 56, pp. 1-12, 2014.
[6] G. Ye and J. Zhou, A block chaotic image encryption scheme based on self-adaptive modelling, *Applied Soft Computing*, vol. 22, pp. 351-357, 2014.
[7] Q. Wang, Q. Guo, and L. Lei, Double image encryption based on phaseamplitude mixed encoding and multistage phase encoding in gyrator transform domains, *Optics & Laser Technology*, vol. 48, pp. 267-279, 2013.
[8] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption, *Optics Communications*, vol. 284, pp. 4331-4339, 2011.
[9] A. Soleymani, Z. M. Ali, and M. J. Nordin, A survey on principal aspects of secure image transmission, *World Academy of Science, Engineering and Technology*, 2012.
[10] X. Wang and C. Jin, Image encryption using Game of Life permutation and PWLCM chaotic system, *Optics Communications*, vol. 285, pp. 412-417, 2012.
[11] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, A novel chaotic image encryption scheme using DNA sequence operations, *Optics and Lasers in Engineering*, vol. 73, pp. 53-61, 2015.
[12] Y. S. e. al, Dual Key Triple Encryption Text Based Message using Cryptography and Steganography, *International Journal of Computer Technology & Applications (IJCTA)*, vol. 4, pp. 43-50, 2013.
[13] X. Zhang, Z. Zhao, and J. Wang, Chaotic image encryption based on circular substitution box and key stream buffer, *Signal Processing: Image Communication*, vol. 29, pp. 902-913, 2014.
[14] A. Soleymani, M. J. Nordin, and E. Sundararajan, A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map, *The Scientific World Journal*, vol. 2014, 2014.
[15] N. Bigdeli, Y. Farid, and K. Afshar, A novel image encryption/decryption scheme based on chaotic neural networks, *Engineering Applications of Artificial Intelligence*, vol. 25, pp. 753-765, 2012.
[16] T. Gao and Z. Chen, Image encryption based on a new total shuffling algorithm, *Chaos, Solitons & Fractals*, vol. 38, pp. 213-220, 2008.
[17] A. Awad and A. Saadane, New chaotic permutation methods for image encryption, *IAENG Int. J. Comput. Sci*, vol. 37, 2010.

[18] Z.-H. Guan, F. Huang, and W. Guan, Chaos-based image encryption algorithm, *Physics Letters A*, vol. 346, pp. 153-157, 2005.
[19] A. Akhshani, H. Mahmodi, and A. Akhavan, A Novel Block Cipher Based on Hierarchy of One-Dimensional Composition Chaotic Maps, *Image Processing*, 2006 IEEE International Conference, pp. 1993-1996, 2006.
[20] R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata, *Optics and Lasers in Engineering*, vol. 71, pp. 33-41, 2015.
[21] Q. Zhang, L. Liu, and X. Wei, Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps, *AEU-International Journal of Electronics and Communications*, vol. 68, pp. 186-192, 2014.
[22] X. Shujiang, W. Yinglong, W. Jizhi, and T. Min, Cryptanalysis of Two Chaotic Image Encryption Schemes Based on Permutation and XOR Operations, *Computational Intelligence and Security*, pp. 433-437, 2008.
[23] S. Li and X. Zhen, On the security of an image encryption me, *Image Processing*, vol. 2, pp. II-925, 2002.
[24] L. Shujun and Z. Xuan, Cryptanalysis of a chaotic image encryption method, *Circuits and Systems*, IEEE International Symposium, vol. 2, pp. II-708-II-711 , 2002.
[25] S. Lian, J. Sun, and Z. Wang, Security analysis of a chaos-based image encryption algorithm, *Physica A: Statistical Mechanics and its Applications*, vol. 351, pp. 645-661, 2005.
[26] S. Li, C. Li, K.-T. Lo, and G. Chen, Cryptanalysis of an image encryption scheme, *Journal of Electronic Imaging*, vol. 15, pp. 043012-043012, 2006.
[27] D. Arroyo, C. Li, S. Li, G. Alvarez, and W. A. Halang, Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm, *Chaos, Solitons & Fractals*, vol. 41, pp. 2613-2616, 2009.
[28] C. Li, S. Li, G. Chen, and W. A. Halang, Cryptanalysis of an image encryption scheme based on a compound chaotic sequence, *Image and Vision Computing*, vol. 27, pp. 1035-1039, 2009.
[29] NSA. (29 August 2015, 17 January 2016). Cryptography Today. Available: https://www.nsa.gov/ia/programs/suiteb_cryptography/
[30] Y. Suryanto and K. Ramli, Chaos properties of the Chaotic Permutation generated by Multi Circular Shrinking and Expanding Movement, *Quality in Research (QiR)*, International Conference ,pp. 65-68, 2015.
[31] J. A. E. Fouda, J. Y. Effa, S. L. Sabat, and M. Ali, A fast chaotic block cipher for image encryption, *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, pp. 578-588, 2014.
[32] Y. Wu, J. P. Noonan, and S. Agaian, NPCR and UACI randomness tests for image encryption, Cyber journals: multidisciplinary journals in science and technology, *Journal of Selected Areas in Telecommunications (JSAT)*, pp. 31-38, 2011.
[33] F. Chong, Z. Guo-yu, G. Meng, and M. Hong-feng, A chaotic symmetric image cipher using a pixel-swapping based permutation, *TENCON 2013 - 2013 IEEE Region 10 Conference* (31194), pp. 1-6, 2013.
[34] Y. Zhou, L. Bao, and C. P. Chen, A new 1D chaotic system for image encryption, *Signal processing*, vol. 97, pp. 172-182, 2014.
[35] N. Instruments. (2013, 5/8/2015). Peak Signal-to-Noise Ratio as an Image Quality Metric. Available: http://www.ni.com/white-paper/13306/en/