THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 16, Special Issue 2015, pp. 271-286

KENKEN PUZZLE – BASED IMAGE ENCRYPTION ALGORITHM

Adrian-Viorel DIACONU

Lumina – The University of South-East Europe, IT&C Department, Romania
E-mail: adrian.diaconu@lumina.org

A novel chaotic, permutation-substitution architecture based, grayscale images' encryption algorithm is introduced in this paper. To reduce the redundancies of Fridrich's structure based image encryption scheme, a novel inter-intra bit-level permutation based confusion strategy is appealed. The confusion stage is developed with the aid of KenKen puzzles. Theoretical analysis and simulation results show that the proposed method has many of the desired properties of a secure cipher.

Key words: KenKen puzzles, chaos-based cryptography, image encryption, security analysis, inter and intra bit-level permutation.

1. INTRODUCTION

1.1. Games' theory and image encryption algorithms' designing

In recent years some scholars have overcome the barriers of harsh mathematics that chaos theory implies, more into practical and fun aspects of the reality (with its own tangled logic and math), proposing innovative digital image scrambling and ciphering schemes that are based on the rules sets of few of the most popular games. If it is to date the fruitful conjunction between games' theory (namely, their rules' design principles) and digital images' cryptography (either classical or chaos-based) the going back would not make more than five years (*i.e.*, a new-built and unique approach, which would crystallize in its early years, was identified).

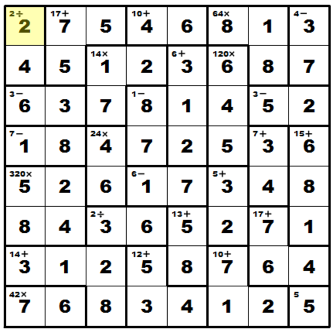
Of all games, whose principles are used in the designing of digital images' cryptographic algorithms, by far, the most popular is the Rubik cube. In [1] the first glimpses is given on how simple playing rules of this game could be used to encrypt an image. This simple idea was to be upgraded soon in [2] and then appealed with success within the construction stages (*i.e.*, confusion, *resp.*, diffusion processes) of other newly proposed image encryption algorithms [3 - 7]. Starting with the same period of time Y. Wu, S. Agaian and J.P. Noonan have started their study over two-dimensional bijective mappings (*i.e.*, provided by parametric Sudoku associated matrix elements representations) in the problem of image scrambling and have proposed a simple but effective Sudoku associated image scrambler [8]. Since, the use of Latin Square and (or) their subsequent Sudoku Grids within digital images encryption algorithms' designing was extensively studied, *e.g.*, [9 - 12]. While Chinese Chess gained its rightful place among the games used within designing stages of digital image scrambling and (or) ciphering algorithms, that is, through papers [13] and [14], another notable mention is attributed to X. Wang and J. Zhang who have developed an image scrambling encryption scheme using chaos-controlled Poker shuffle operation [15].

This is why, in this paper, the KenKen puzzle is approached and investigated under the hypothesis of a game with great potential in the problem of image scrambling designing.

The rest of this paper is organized as follows: sub-section 1.2 gives a brief review on the preliminary materials (*i.e.*, basic structure of KenKen puzzles and the new approach on using them in the problem of grayscale images' scrambling algorithms' designing); Section 2 discusses the simulation setups with extended performances analysis over the proposed image encryption scheme (*i.e.*, under various investigation methods, including the adjacent pixels' correlation coefficients' computation, global and local entropy assessment and other qualitative measurements' analysis, *e.g.*, NPCR – number of pixel change rate, *resp.*, UACI – unified average changing intensity), and finally Section 3 concludes the paper.

1.2. KenKen puzzles and grayscale images' scrambling

A KenKen puzzle of order n is an $n \times n$ array filled with n distinctive elements (*i.e.*, integer numbers from 1 to n), where each element appears exactly once in each row and each column. Basically, each array is divided in multiple non-overlapping cages (*i.e.*, blocks with thick borders) of different shapes and sizes. Each of these cages show a result and a mathematical operation (*i.e.*, on its upper left corner). The mathematical operation (either addition, subtraction, multiplication or division) is applied to the numbers within the cage to produce the target number [16]. Fig. 1 showcases a typical 8×8 KenKen puzzle.



2+ 2	17+ 7	5	10+ 4	6	64× 8	1	4− 3
4	5	14× 1	2	6+ 3	120× 6	8	7
3− 6	3	7	1− 8	1	4	3− 5	2
7− 1	8	24× 4	7	2	5	7+ 3	15+ 6
320× 5	2	6	6− 1	7	5+ 3	4	8
8	4	2+ 3	6	13+ 5	2	17+ 7	1
14+ 3	1	2	12+ 5	8	10+ 7	6	4
42× 7	6	8	3	4	1	2	5 5

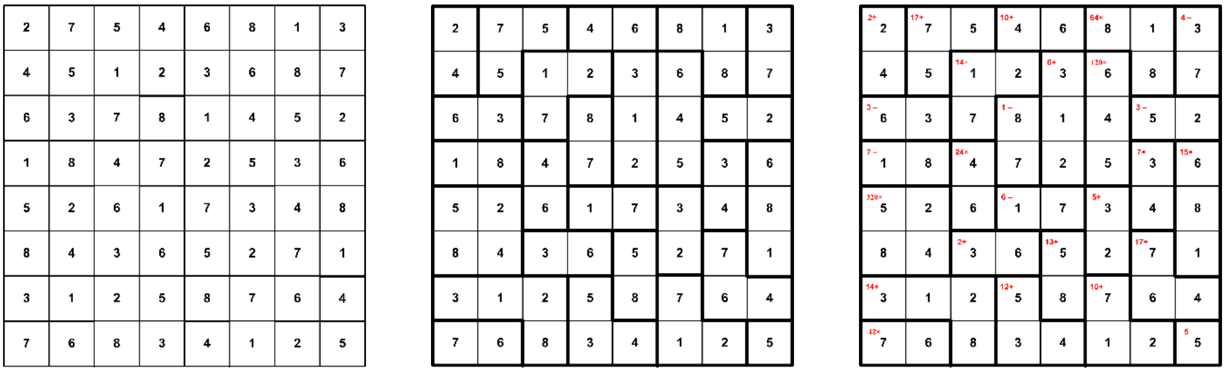
Fig. 1 – A typical 8×8 KenKen puzzle (www.kenkenpuzzle.com/gme).

Generation of a KenKen puzzle follows few simple steps:

(1) an empty $n \times n$ array is filled with n distinctive elements, as shown in Fig. 2. a); the filling must be done so that no element repeats itself in any row or column; the filling can be done either manually either by generating a Latin square which then is horizontally and vertically resampled, as shown in [11].

(2) multiple non-overlapping cages are drawn on the array, as shown in Fig. 2. b), so that each element is enclosed in a cage; each cage, typically, encloses between one and four elements.

(3) clues, i.e., the mathematical operation applied on elements within a cage and the resulted number, entered in the upper left corner of each cage, as shown in Fig. 2. c).



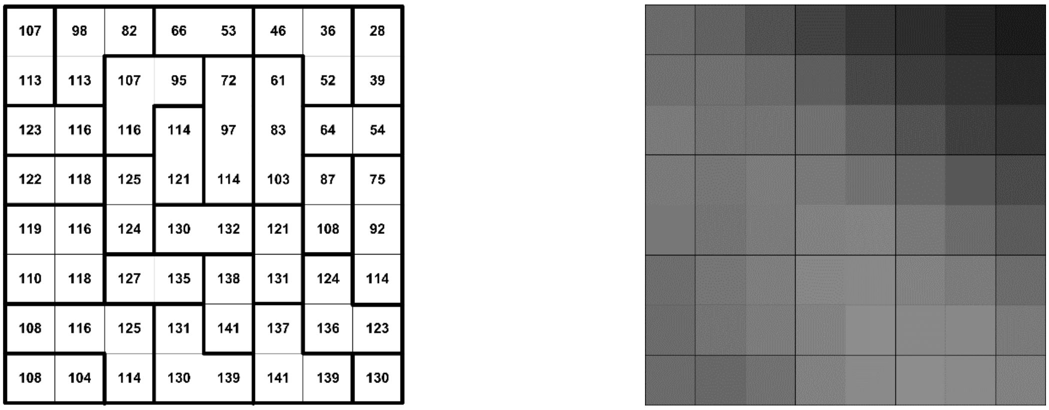
a b c

Fig. 2 – KenKen puzzle generation steps: a) 8×8 Sudoku Grid; b) Sudoku Grid with cages drawn; c) solved KenKen puzzle.

Analyzing the KenKen puzzle shown in figure above one can notice that it offers all the required elements for a quality inter-intra bit-level permutation based confusion strategy. Therefore, the new approach on using a KenKen puzzle in the problem of grayscale images' scrambling algorithms' designing impose the following set of conventions:

(1) with l_0 representing the pixels' values matrix of an 8-bit grayscale image of the size m×m, l_0 is divided into equal, 8×8 pixels, non-overlapping blocks.

In Fig. 3, the pixels' values matrix associated to one block of pixels taken from the Lena 8-bit grayscale image (*i.e.*, downloaded from the USC-SIPI database [17]), *resp.*, its grayscale image representation are showcased. For practical reasons, over the pixels' values matrix (*i.e.*, Fig. 3.a)), associated KenKen puzzle's cages were highlighted.



107	98	82	66	53	46	36	28
113	113	107	95	72	61	52	39
123	116	116	114	97	83	64	54
122	118	125	121	114	103	87	75
119	116	124	130	132	121	108	92
110	118	127	135	138	131	124	114
108	116	125	131	141	137	136	123
108	104	114	130	139	141	139	130

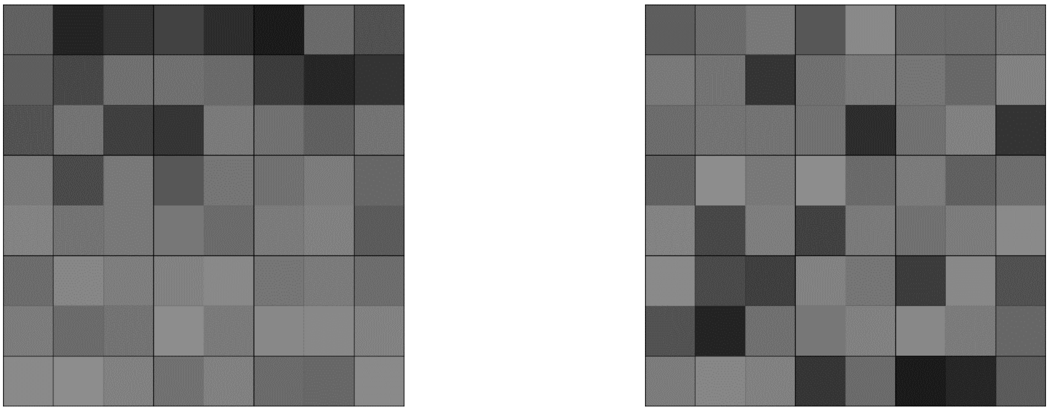
a

b

Fig. 3 – First stage output example: a) pixels' values matrix associated to one block of pixels taken from the Lena 8-bit grayscale image; b) pixels' values matrix represented in grayscale.

(2) going through the l_0 matrix from left to right and top to bottom, for each block of pixels (*i.e.*, taken from the l_0 matrix), the inter bit-level permutation based confusion strategy is employed. Basically, each pixel is permuted to a new location, as dictated by values inside each cell of the KenKen puzzle. For better mixing properties, each block of pixels is traversed twice, pixels being permuted both on rows and columns.

In Fig. 4, pixels' values matrix (*i.e.*, in grayscale representation) for the intermediary and second's stage output block are shown.



a

b

Fig. 4 – Second stage output example: a) pixels' values matrix represented in grayscale, after going through horizontal permutations; b) pixels' values matrix represented in grayscale, after going through vertical permutations.

Through a comprehensive study W. Zhang *et al.* [18] argued redundancy of Fridrich's structure based image encryption schemes (i.e., the sequence of complex confusion and diffusion operations lead to only 3.3% bit value modifications, while the remaining 96.7% are unchanged), highlighting three effects that need to be achieved during the confusion phase: (i) bit distribution of each bit plane is more uniform; (ii) correlation between neighboring higher bit planes is reduced; (iii) not only the positions, but also the pixel values are modified. In this sense, within the 3rd step of the newly proposed image scrambling approach, an efficient intra bit-level permutation based confusion strategy is employed. Thus, redundancies of Fridrich's structure based encryption scheme are greatly reduced.

(3) making use of the mathematical operation and the target number (*i.e.*, provided by the KenKen puzzle, on the upper left corner of each cage), the value of each pixel is modified as follows:

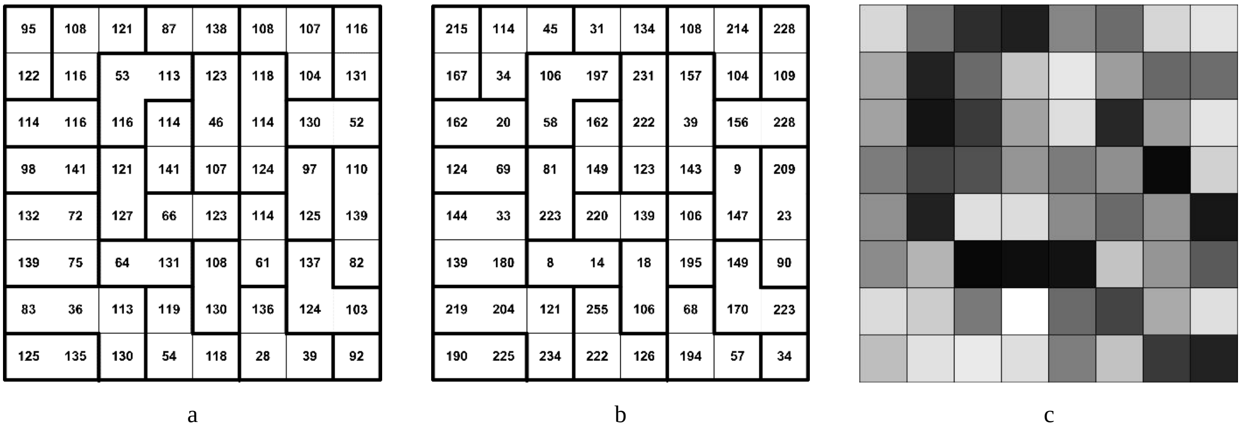
- for each pixel within a group included in a cage provided with the addition or subtraction operation: (i) pixel's value is converted from decimal to binary; (ii) binary representation is reversed (*i.e.*, bits order is inversed); (iii) the target number and the value inside of pixel's associated cell (*i.e.*, within the KenKen puzzle) are added or subtracted (*i.e.*, depending on the operation provided by the associated cage) to each pixel's value; (iv) the resulted binary number is reversed and converted to its decimal representation.
- for each pixel within a group included in a cage provided with the division or multiplication operation: (i) pixel's value is converted from decimal to its binary representation; (ii) the binary representation is circularly shifted to the right or left (*i.e.*, for multiplication, *resp.*, division operation) with a number of steps equal to the value inside of pixel's associated cell (*i.e.*, within the KenKen puzzle); (iii) the resulted binary number is converted to its decimal representation.

In Fig. 5. a), pixels' values matrix associated with third's stage input block of pixels is presented. In order to facilitate the understanding of the above intra bit-level scrambling rules, two examples will be taken into account:

(a) for the pixel located at the intersection of 8th row and 1st column we have: pixel's value ´125´, mathematical operation provided by the associated KenKen cage ´×´ and the integer value within pixel's associated KenKen cell ´7´. Therefore, following the rules described above we have: (i) pixel's value binary representation ´01111101´; (ii) pixel's binary value after circular shifts (*i.e.*, with 7 steps to the right) ´10111110´; (iii) pixel's decimal value after the intra bit-level permutation ´190´;

(b) for the pixel located at the intersection of 1st row and 2nd column we have: pixel's value ´108´, target number and the mathematical operation provided by the associated KenKen cage ´17+´, *resp.*, the integer value within pixel's associated KenKen cell ´7´. Therefore, following the rules described above we have: (i) pixel's value binary representation ´01101100´; (ii) binary representation's bits in reversed order ´00110110´; (iii) pixel's value after the addition of target number and of the integer value within pixel's associated KenKen cell ´01001110´; (iv) pixel's final value (*i.e.*, after bits reversion, *resp.*, binary to decimal conversion) ´114´.

In Fig. 5. b) and c), pixels' values matrix associated with third's stage output block of pixels, *resp.*, its grayscale representation are showcased.



95	108	121	87	138	108	107	116
122	116	53	113	123	118	104	131
114	116	116	114	46	114	130	52
98	141	121	141	107	124	97	110
132	72	127	66	123	114	125	139
139	75	64	131	108	61	137	82
83	36	113	119	130	136	124	103
125	135	130	54	118	28	39	92

a

215	114	45	31	134	108	214	228
167	34	106	197	231	157	104	109
162	20	58	162	222	39	156	228
124	69	81	149	123	143	9	209
144	33	223	220	139	106	147	23
139	180	8	14	18	195	149	90
219	204	121	255	106	68	170	223
190	225	234	222	126	194	57	34

b

c

Fig. 5 – Third stage output example: a) pixels' values matrix associated to third's stage input block of pixels; b) pixels' values matrix associated to third's stage output block of pixels; c) pixels' values matrix represented in grayscale.

1.3. Effectiveness of the proposed confusion phase

In this section it is aimed to study how the newly proposed KenKen puzzle – based confusion strategy handles the criteria stipulated by W. Zhang *et al.* [18], *i.e.*, if, how and in which amount redundancies implied by the Fridrich's structure based algorithm are reduced.

The fulfillment of these criteria can be validated through an assessment which include: (i) uniformity of the bit distribution within each bit plane (either visually and (or) statistically); (ii) computation of correlation coefficients between neighboring higher bit planes; (iii) pixels' position and value randomization analysis.

To assess the effectiveness of the proposed approach on digital images scrambling the 8-bit grayscale Lena testing image was taken into consideration (*i.e.*, it was subjected to the newly proposed KenKen puzzle based confusion strategy). To start with, in Fig. 6, Lena plain-image is shown, along with its scrambled version. Just by analyzing the second image (*i.e.*, Fig. 6 b)), as a result of newly proposed confusion strategy (*i.e.*, as described in Section 1.2), one can conclude that the third criteria - "[…] not only the positions, but also the pixel values are modified […]" [18], is satisfied.

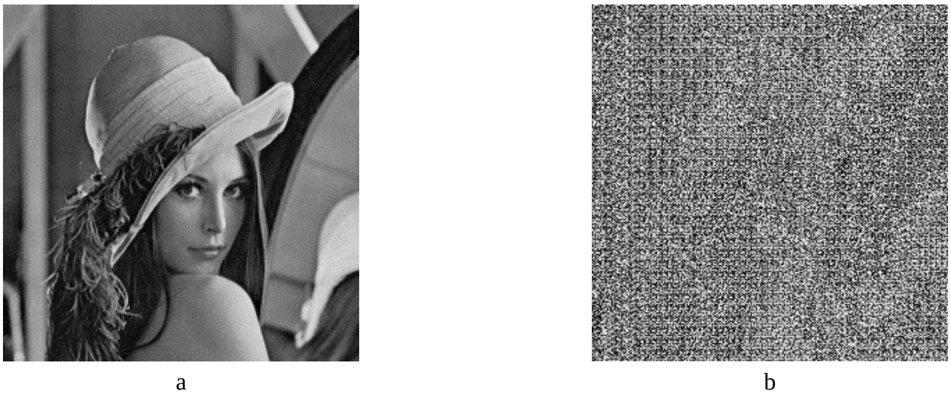


Fig. 6 – Lena: a) plain-image; b) scrambled image.

(A) Uniformity of the bit distribution within each bit plane

According to [18], the pursuit for a uniform bit distribution within each bit plane it's a must, in order to reduce considerable the redundancies of standard Fridrich's structure based image encryption algorithm, and is supposed to be achieved since the confusion phase. Uniformity of the bit distribution within each bit plane (mostly on image's higher bit planes) can be assessed either visually (*i.e.*, for a high performance confusion stage, at its output, is expected to obtain an image whose higher bit planes are random like in appearance) or statistically (*i.e.*, computing bit distributions within bit planes of the scrambled image).

Therefore, for the visual assessment of this criteria Fig. 7 and 8 are showcased, while for the statistical assessment Table 1 is subjected to a thorough screening. Thus, one can conclude that this criteria is fully satisfied (*i.e.*, bits distribution within scrambled image's bit planes is more uniform, in comparing with ones of the plain-image).

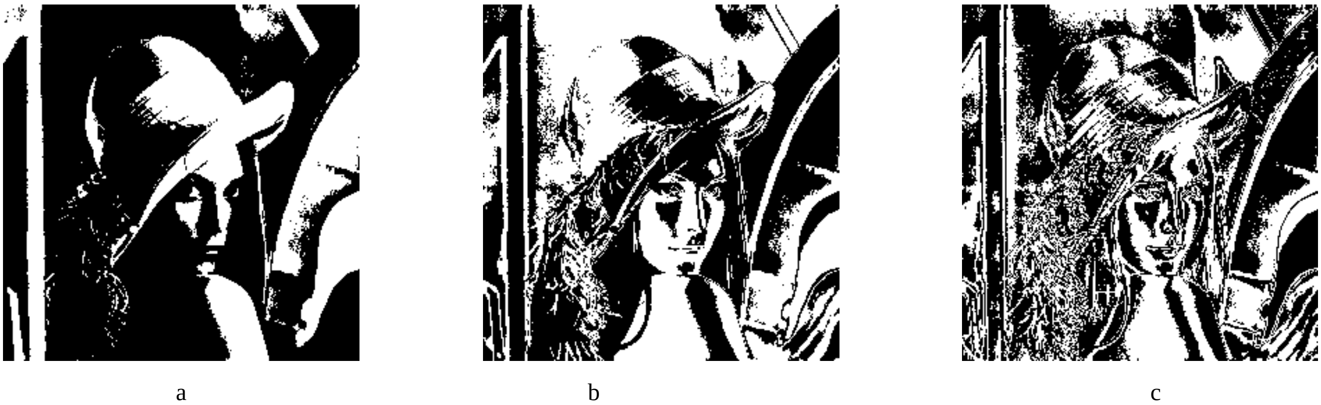
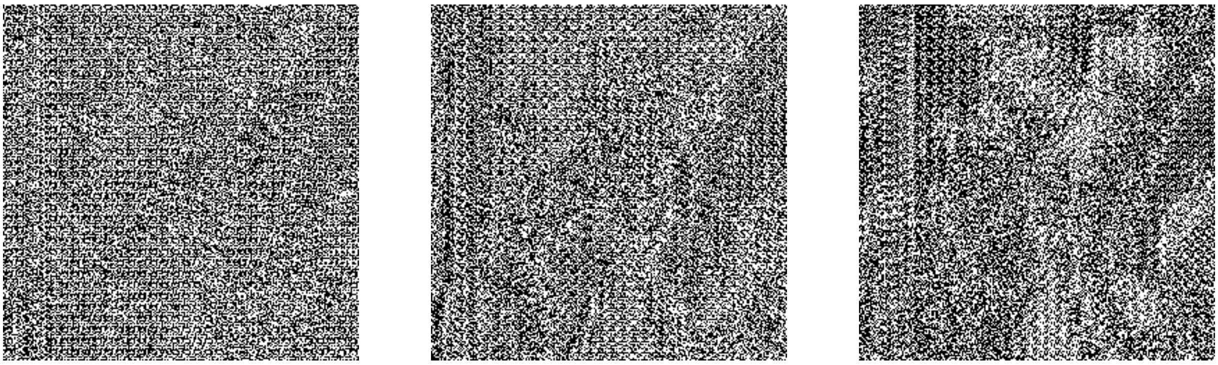


Fig. 7 – Higher bit planes of Lena testing plain-image: a) the 8th bit plane; b) the 7th bit plane; c) the 6th bit plane.



a b c

Fig. 8 – Higher bit planes of Lena scrambled image: a) the 8th bit plane; b) the 7th bit plane; c) the 6th bit plane.

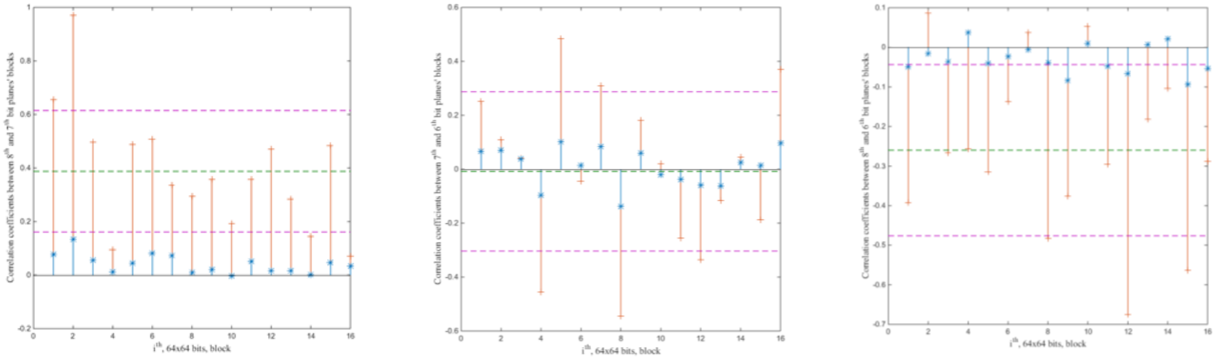
Table 1

Percentage of bit value information for each bit plane in Lena plain vs. scrambled image (percentage of 1s)

Lena	8th bit	7th bit	6th bit	5th bit	4th bit	3rd bit	2nd bit	1st bit
plain	30.2154%	47.9446%	42.3736%	51.7105%	49.8458%	49.8580%	50.2807%	49.7970%
scrambled	49.6353%	48.4512%	46.6094%	49.3331%	48.8876%	49.4552%	48.6740%	49.2767%

(B) Correlation between neighboring higher bit planes

For the assessment of this second criteria Lena plain and scrambled images were divided into sixteen non-overlapping blocks, 64 bits × 64 bits each. For each pair of these blocks (*i.e.*, belonging to different higher bit planes), the correlation coefficients were computed, as shown in Fig. 9.



a b c

Fig. 9 – Correlation coefficients within Lena plain vs. scrambled images: a) between 8th and 7th bit planes' blocks; b) between 7th and 6th bit planes' blocks; c) between 8th and 6th bit planes' blocks.

Here, with red stems being represented the correlation coefficients' values between pairs of blocks in higher bit planes of Lena plain-image, *resp.*, with blue stems being represented the correlation coefficients' values between pairs of blocks in higher bit planes of Lena scrambled image, one can notice that the correlation between neighboring higher bit planes is considerably reduced:

(i) from a mean of 0.3878 (*i.e.*, the dashed green line, computed for the entire series of 16 correlation coefficients) and a standard deviation of 0.2270 (*i.e.*, dashed magenta lines) between blocks of 8th and 7th bit planes within Lena plain-image, to a mean of 0.0416 and a standard deviation of 0.0367 between blocks of 8th and 7th bit planes within scrambled image (*i.e.*, Fig. 9.a));

(ii) from a mean of -0.0079 and a standard deviation of 0.2955 between blocks of 7th and 6th bit planes within plain-image, to a mean of 0.0097 and a standard deviation of 0.0722 between blocks of 7th and 6th bit planes within scrambled image (*i.e.*, Fig. 9.b));

(iii) from a mean of -0.2599 and a standard deviation of 0.2164 between blocks of 8th and 6th bit planes within plain-image, to a mean of -0.0299 and a standard deviation of 0.0372 between blocks of 8th and 6th bit planes within scrambled image (*i.e.*, Fig. 9.c)).

The same testing methodology was applied on other test images downloaded from the USC-SIPI image database, miscellaneous volume [17] and has provided similar results (*i.e.*, reduction, by one or two orders of magnitude, of the correlation coefficient between neighboring higher bit planes), as summarized in Table 2.

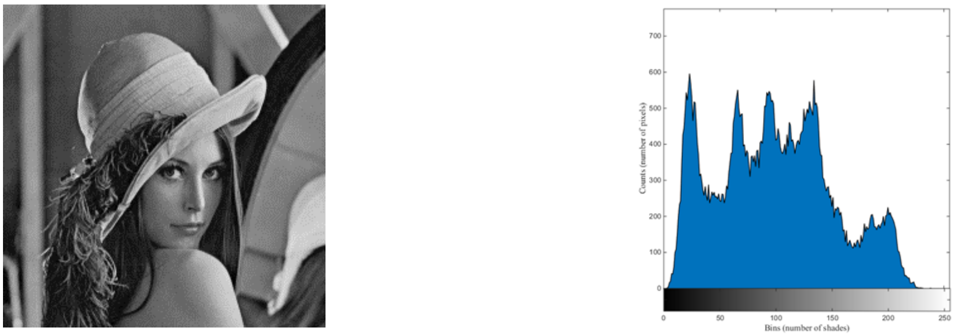
Table 2

Correlation coefficients between blocks of 8th and 7th bit planes, within different plain vs. scrambled images

Measure	Lena		Peppers		Baboon		Cameraman	
	plain	scrambled	plain	scrambled	plain	scrambled	plain	scrambled
mean	0.3878	0.0416	0.5209	0.0666	0.7695	0.0850	0.3908	0.0434
std_dev.	0.2270	0.0367	0.2224	0.0334	0.1683	0.0176	0.3613	0.0870

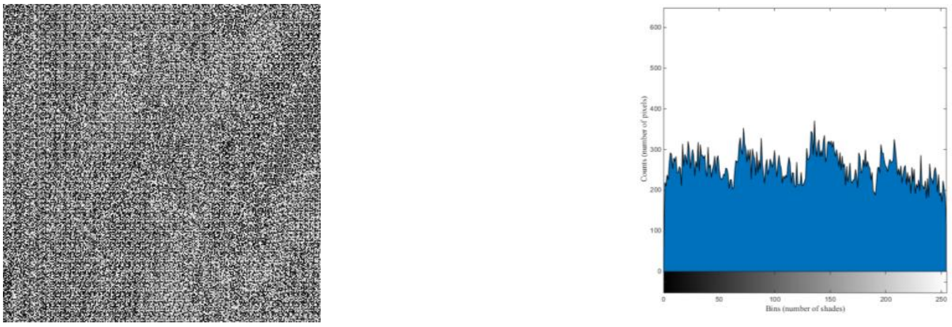
(C) Pixels' position and value randomization

Pixels' value randomization can be easily evaluated with the aid of histograms; thus, scrambled image's histogram is shown in Fig. 11. One can notice that during the newly proposed confusion phase not only pixels' position but their values were modified as also. Although histogram's distribution is visibly more uniform, assessing its goodness-of-fit (*i.e.*, with the aid of chi-square test [19]) the null hypothesis (that is, histogram distribution approaches features of a uniform distribution, *i.e.*, equiprobable frequency counts) is rejected at 5% significance level. The same conclusion is drawn for all images considered for tests, *i.e.*, passing through the confusion phase, images' histograms gain a more but not sufficiently uniform distribution.



a b

Fig. 10 – Lena: a) testing plain-image; b) plain-image histogram.



a b

Fig. 11 – Lena: a) scrambled image; b) scrambled image histogram.

At this point we can conclude that the newly proposed confusion strategy offers better performances in comparing with other Fridrich's structure based image encryption algorithm, *e.g.*, [3 - 7], [11], [13 - 15], *resp*., [20 - 23]. However, due to non-uniform histograms, in the following the second phase is approached (*i.e.*, the diffusion process) and performances of the resulted cryptosystem will be subjected to a thorough assessment.

2. THE COMPLETE CRYPTOSYSTEM AND ITS SECURITY ANALYSIS

2.1. The complete cryptosystem

At this point, first's phase output image (*i.e.*, the scrambled image) goes through the diffusion process, which involves a chaotic map (1), chosen due to its proved cryptographic properties (*i.e.*, high sensitivity to the initial conditions, attractor's fractal structure, system's ergodicity and good randomness etc.), as proven in [24]. During performances' testing procedures f_ps' initial seeding points' and control parameters' values were chosen with values: $x_0^1 = 0.68775497511773$, $r_1 = 5.938725725421$, *resp.*, $x_0^2 = -0.0134623754671$, $r_2 = 1.257490187615$.

$$y_i = f_1(x_i^1, r_1) \cdot f_2(x_i^2, r_2) = \frac{f_1(x_i^1, r_1) + f_2(x_i^2, r_2)}{1 - f_1(x_i^1, r_1) \cdot f_2(x_i^2, r_2)}, \tag{1}$$

where: x_0^1, x_0^2 and r_1, r_2 are the initial conditions, *resp.*, the control parameters of the f_1, f_2 chaotic maps; x_i^1, x_i^2 are the orbits obtained with recurrences $x_{i+1}^1 = f_1(x_i^1, r_1), x_{i+1}^2 = f_2(x_i^2, r_2), \forall\, i \in N$; one-dimensional chaotic discrete dynamical systems, *i.e.*, f_1 and f_2, are of the form:

$$f_p\colon [-1,1] \to [-1,1], f_p(x_i^p) = \frac{2}{\pi} arctg\left(ctg(x_i^p \cdot r_p)\right). \tag{2}$$

Using the random sequences of real numbers generated by y_i's orbits in conjunction with a multilevel discretization method [25] (e.g., with four thresholds, *i.e.*, 2-bit encoding of each interval), resulted di-bits are spread into two separate files (*i.e.*, *Bits_A.txt* - containing di-bit's 1st bit and *Bits_B.txt* containing di-bit's 2nd bit). A total number of $m \cdot m \cdot 8$ di-bit pairs have been generated (*i.e.*, 524.288 bits were written in each file), this number being, as seen, directly proportional to image dimensions (*i.e.*, m represents image's dimensions, where for the paper in question $m = 256$) [4].

Under the previous circumstances, ciphering matrices are computed as follows:

(1) open and read $Bits_A.txt$ and $Bits_B.txt$ files, then initialize a temporary counter C to zero;

(2) initialize I_{cipher_col} and I_{cipher_row}, where,

$$I_{cipher\_col} = I_{cipher\_row} = zeros\ (m, m). \tag{3}$$

(3) for $i = 1{:}m$, for $j = 1{:}m$,

a. take eight consecutive bits from each file,

$$\begin{aligned} Byte_A &= strcat\left(Bits_A.txt(C + k)\right),\ k = \overline{1,8}, \\ Byte_B &= strcat\left(Bits_B.txt(C + k)\right),\ k = \overline{1,8}. \end{aligned} \tag{4}$$

b. update I_{cipher_col} and I_{cipher_row},

$$\begin{aligned} I_{cipher\_col}(i,j) &= bin2dec(Byte_A), \\ I_{cipher\_row}(i,j) &= bin2dec(Byte_B). \end{aligned} \tag{5}$$

c. update temporary counter,

$$C = C + 8. \tag{6}$$

Steps (1) – (3) will produce the ciphering matrices.

With I_S representing the pixels' values matrix of an 8-bit grayscale scrambled image of the size $m \times m$, the confusion phase is done accordingly to the following:

(1) for $i = 1{:}\,m$,

a. cipher I_S's rows,

$$I_S(i,:) = I_S(i,:) \oplus I_{cipher\_row}(i,:). \tag{7}$$

b. cipher I_S's columns,

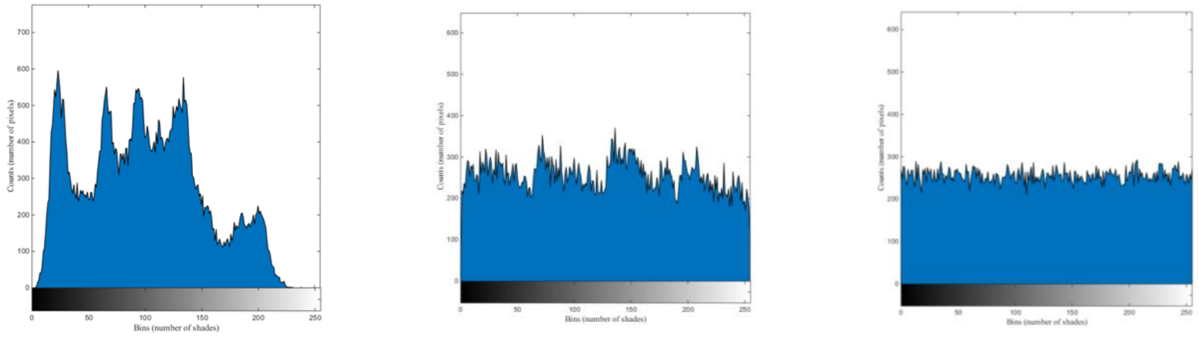
$$I_S(i,:) = I_S(i,:) \oplus I_{cipher\_col}(i,:)'. \tag{8}$$

2.2. Security analysis of the cryptosystem

In order to prove that the proposed image encryption system has the desired confusion and diffusion properties, in accordance to an already widely used conventional methodology [5, 20, 26, 27], a comprehensive security assessment is presented in the following (including histogram analysis, adjacent pixels' correlation coefficients' computation, global and local entropy assessment etc.).

(A) Histogram analysis

Pixels' distribution analysis (as histogram analysis may be called), as a general requirement, highlights the presence of similarities between the plain-image and its scrambled version (*i.e.*, if the scrambled image does or does not contain any features of the plain image). Fig. 12 depicts plain-image's histogram (a), along with the histograms of scrambled (b) and ciphered (c) images. It can be easily noticed that even after the confusion stage the image gains a more uniform distribution of pixel values, meaningfully different than the one of the plain-image (which contains large sharp rises followed by sharp declines). Yet, the chi-square test value (which assesses histogram's goodness-of-fit) falls within the confidence interval (*i.e.*, the null hypothesis is accepted at a significance level of 5%) only after the diffusion stage (where, as Fig. 12. c) shows, pixels distribution resembles the ideal). Thus, it can be said that the resulted image does not provide any clue for statistical attacks.



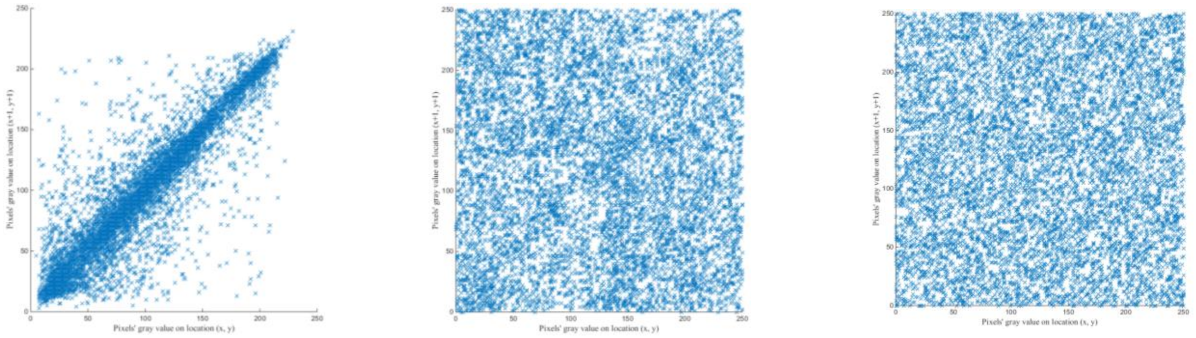
a b c

Fig. 12 – Lena: a) plain-image histogram; b) scrambled image histogram; c) ciphered image histogram.

(B) Adjacent pixels correlation coefficients

As helpful as pixels' distribution analysis (*i.e.*, when it comes to assess the strength of a newly proposed encryption algorithm against cryptanalytic attacks of statistical type) is adjacent pixels correlation coefficients' analysis. Unlike the correlation test conducted in Section 1.3 this one aims to study how close are the values of pixels that are found on the same bit plane and spatially closed one to another.

For this test, firstly, 10.000 pairs of adjacent pixels (on diagonal direction) were randomly selected from the plain, scrambled and ciphered images and plotted as shown in Fig. 13. Here, it can be easily noticed that neighboring pixels in the plain-image are highly correlated and, contrarily, in cases of scrambled and ciphered image pixels considered in tests are weakly correlated.



a b c

Fig. 13 – Correlation distribution of diagonally adjacent pixels in Lena: a) plain-image; b) scrambled image; c) ciphered image.

At the same time, all the correlation coefficient values (computed over 10.000 pairs of adjacent pixels, randomly selected, for each of the testing directions) are summarized in Table 3. Screening this table, one can confirm that, overall, the encryption process eliminates inherent strong correlation existing between the pixels of the plain-image.

Table 3

Correlation coefficients of adjacent pairs of pixels

Image	Stage	Testing direction		
		Vertical	Horizontal	Diagonal
Lena	plain	0.968302999373237	0.943332813021704	0.921609062275351
	scrambled	0.051963171338142	0.038145761034515	0.027356877841472
	ciphered	0.013461489708868	0.005027057562429	0.002524173156150
Baboon	plain	0.727462161419536	0.644330661135897	0.637533412449464
	scrambled	0.032112039649584	0.013275430567695	0.019123051722439
	ciphered	0.002287675069989	0.003205974482893	0.003251103143878
Peppers	plain	0.955077455006984	0.956938707381351	0.918211910800372
	scrambled	0.053704634809109	0.024618236840151	0.050157349394917
	ciphered	0.019838697880223	0.020919931913094	0.000513367107629
Cameraman	plain	0.959690890644183	0.933164880296896	0.910767915776454
	scrambled	0.075902376878876	0.003823208088292	0.020329768117064
	ciphered	0.007643693770102	0.011757833106938	0.012474106530361

(C) Information entropy analysis

The entropy of an information source is a mathematical property that reflects its randomness, *resp.*, unpredictability [28, 29]. Hence, any new algorithm for encryption of images should give at its output a ciphered image having equiprobable gray levels (*i.e.*, the entropy of the ciphered image should be, at least theoretically, equal to 8 bits, for gray scale images of 256 levels). Actually, in practice, the resulted entropy is smaller than the ideal one and as smaller is the resulted entropy as greater is the degree of predictability, a fact which threatens encryption system's security [4].

Table 4 summarizes the global and local entropy values for the ciphered images. For the computation of local entropy, according to the methodology described in [30], 31 non-overlapping blocks of pixels (each of them having 1936 pixels, taken from the ciphered image subjected to local entropy assessment) were considered. Analyzing table's entries (*i.e.*, global entropies of the cipher images are very close to the theoretical value of 8 bits, while all of local entropies fall within the acceptance intervals at 5%, 1%, 0.1% significance levels), one can say that the proposed encryption algorithm is highly robust against entropy attacks.

Table 4

Global and local entropy values of the ciphered images

Testing image	Global entropy	Local entropy	Local entropy critical values $k = 30, T_B^{L=256*} = 1936$		
			$h_{left}^{l*0.05} = 7.901901305$ $h_{right}^{l*0.05} = 7.903037329$	$h_{left}^{l*0.01} = 7.901722822$ $h_{right}^{l*0.01} = 7.903215812$	$h_{left}^{l*0.001} = 7.901515698$ $h_{right}^{l*0.001} = 7.903422936$
Lena	7.9973183427	7.9030081260	passed	passed	passed
Baboon	7.9962532687	7.9022749521	passed	passed	passed
Peppers	7.9985992525	7.9027496173	passed	passed	passed
Cameraman	7.9968665077	7.9097526421	passed	passed	passed

(D) Security assessment by differential analysis

Differential analysis – based assessment of an encryption algorithm uses two qualitative indicator, namely NPCR (*i.e.*, number of pixels change rate) and UACI (*i.e.*, unified average changing intensity) [31]. NPCR and UACI tests' results are shown in Table 5 and 6. Screening these tables and observing that the values of both indicators lie within the confidence intervals (*i.e.*, swiftly changes in the plain-image will result in negligible changes in its ciphered version), one can conclude that the proposed encryption algorithm ensures the required strength against any differential attack.

Table 5

UACI values for the proposed ciphering scheme

Testing image	UACI value	UACI critical values		
		$UACI_{0.05}^{*-} = 33.3730\%$ $UACI_{0.05}^{*+} = 33.5541\%$	$UACI_{0.01}^{*-} = 33.3445\%$ $UACI_{0.01}^{*+} = 33.5826\%$	$UACI_{0.001}^{*-} = 33.3115\%$ $UACI_{0.001}^{*+} = 33.6156\%$
Lena	33.4819	passed	passed	passed
Baboon	33.5101	passed	passed	passed
Peppers	33.5073	passed	passed	passed
Cameraman	33.5005	passed	passed	passed

Table 6

NPCR values for the proposed ciphering scheme

Testing image	NPCR value	NPCR critical values		
		$NPCR_{0.05}^{*} = 99.5893\%$	$NPCR_{0.01}^{*} = 99.5810\%$	$NPCR_{0.001}^{*} = 99.5717\%$
Lena	99.6182	passed	passed	passed
Baboon	99.5995	passed	passed	passed
Peppers	99.5943	passed	passed	passed
Cameraman	99.6067	passed	passed	passed

(E) Strength against different types of attacks

The encrypted image was subjected to additive noise and cropping attacks, in order to assess how the situation in which an attacker intercepts and modifies its structure (*i.e.*, so as, after decryption, the legitimate user cannot understand and (or) use the original one) is handled.

Thus, Fig. 14.a) and b) depicts the Lena recovered image when its encrypted version was attacked with ´speckle´ type of noise (with 0.01 variance), *resp.*, ´salt and pepper´ type of noise (with 0.01 densities). One can conclude that the proposed scheme handles, lightly, the additive noise attacks (*i.e.*, recovered images are intelligible, most of the informational content being passed to the legitimate user).

Same conclusion can be drawn regarding the cropping attacks, provided that the attacked area shows a negligible amount of information (*i.e.*, since it is the only area that cannot be recovered properly, as Fig. 14.c) suggests).

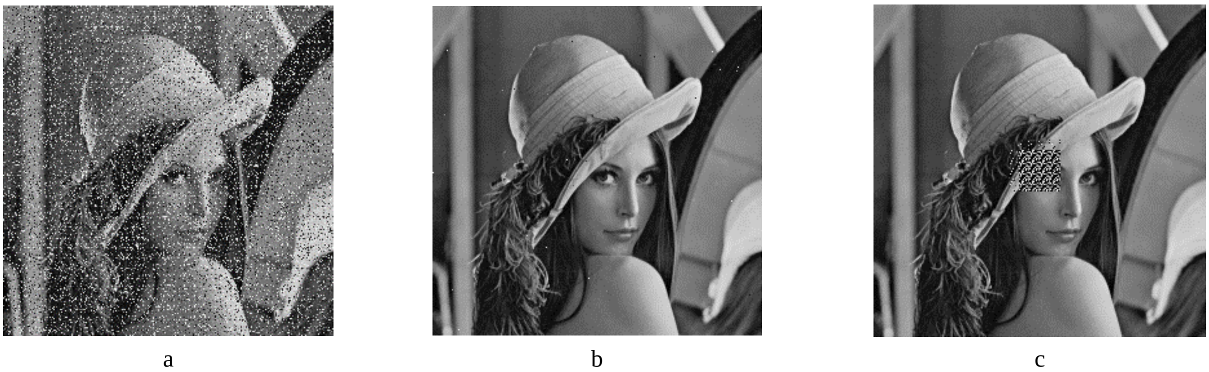


Fig. 14 – Lena recovered image, when its encrypted version was attacked: a) with ´speckle´ type of noise, with 0.01 variance; b) with ´salt and pepper´ type of noise, with 0.01 densities; c) by cropping 1/64th of the image on its center.

(F) Security assessment by key analysis

This assessment seeks to analyze the sensibility of the encryption key (*i.e.*, any small changes in the key should lead to significant changes in the scrambled and (or) encrypted, *resp.*, descrambled and (or) deciphered images) on one hand, and the searching space that the key offers (*i.e.*, the size of the secret key space should be as large as possible, to avoid guessing the key used at a given moment by exhaustive search in a reasonable time).

Thus, for the proposed cryptosystem, assessment of key's sensibility was made taking into consideration a ±LSB variation over one of key's elements. Fig. 15 and Fig. 16 highlight proposed cryptosystem's sensibility to small changes within the encryption key. Analyzing these two figures one can conclude that the proposed image encryption scheme is very sensitive to small changes within the secret key.

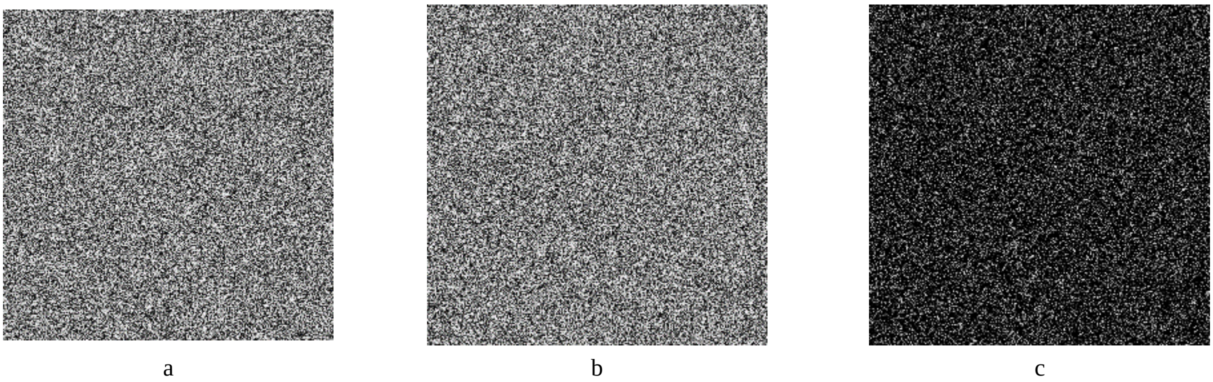


Fig. 15 – Proposed cryptosystem's sensitivity to small changes within the encryption key: a) image encrypted using a key K_1; b) image encrypted using a key which differs from K_1 with 10^{-19}; c) the image representing differences between (a) and (b).

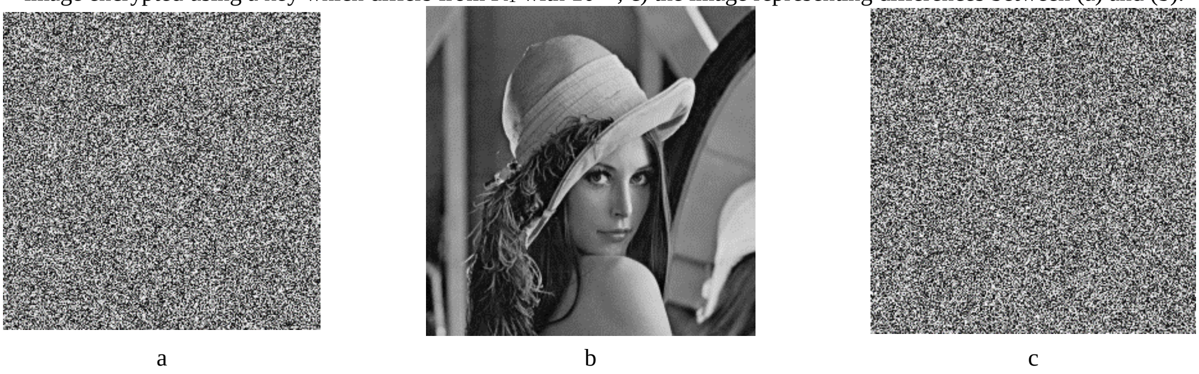


Fig. 16 – Proposed cryptosystem's sensitivity to small changes within the encryption key: a) image encrypted using a key K_1; b) image decrypted using the correct key K_1; c) image decrypted using the wrong key K_2.

A large key space is very important for an encryption algorithm, as to be able to repel brute-force attacks. In the case of newly proposed cryptosystem the key space is constructed with the aid of the chaotic map and KenKen puzzle.

Thus, taking into consideration only the chaotic map (*i.e.*, its initial seeding points' values, *resp.*, control parameters' values), the considered key, *i.e.*, $K = \{x_0^1, r_1, x_0^2, r_2\}$, generates a key-space sufficiently large (of at least 10^{67}, taking into consideration the fact that PRNG's seeding points, *resp.*, control parameters have been represented with an accuracy of up to 10^{-19}), as to ensure its immunity to these types of attacks, with respect to the current computers' capacities. But, if we take into account the fact that KenKen puzzles are basically derived from a Latin square, if it is to number all possible $n \times n$ Latin squares (9) [32], this key-space could be easily extended with a lower bound of 10^{15} (*i.e.*, for a typical 8×8 KenKen puzzle, excluding all cages and operations within).

$$L(n) \geq (n!)^{2 \cdot n} / n^{n^2}. \tag{9}$$

where, n represents Latin Square's order (*i.e.*, dimension).

(G) Computational and complexity analysis

Usually, after the security assessment, speed tests are performed over newly proposed image encryption algorithms in order to evaluate in which measure they can accommodate real-time multimedia applications, *resp.*, to compare its performances with other alternatives.

But, taking into account that scholars differ in term of programming skills and environments and (or) computer systems at their disposal (*i.e.*, different computational power), in what follows a different evaluation tool will be used, *i.e.*, the complexity of analysis.

For the proposed image cryptosystem the total complexity is given by the permutation stage, more accurately by the intra-pixel permutation process. Thus, with a time complexity in the intra-pixel permutation process of $\Theta(8 \times m \times m)$ and a time complexity in the inter-pixel permutation process of $\Theta(m \times m)$, *resp.*, a time complexity in the diffusion process of $\Theta(m \times m)$, the total time complexity of the proposed scheme is rounded to $\Theta(m \times m)$. The achieved time complexity is comparable with ones showcased in [5, 20, 21, 33, 34] and other recently proposed image cryptosystems.

2.3. Discussions

Within this sub-section some of the features which differentiates the newly proposed image encryption algorithm from the other existing solutions are highlighted.

Thus: (1) in comparing to traditional Fridrich's permutation-substitution model-based image encryption algorithms, the proposed image cryptosystem ensures (i) a more uniform distribution within each bit plane of the image, (ii) a reduced correlation between neighboring higher bit planes of the image and (iii) not only the position, but also the pixels' values are modified during the confusion phase; (2) in comparing with other bit-level permutation based image encryption schemes, *e.g.*, [35-39], one can notice that (i) the proposed scheme requires only one round in order to approach desirable cryptographic performances, in contrast with [39] where 3 rounds are required, *resp.*, [37, 38] where 5 rounds are appealed, (ii) the proposed cryptosystem makes use of a single chaotic map in comparing with [35, 37-39] that are using 2 or more different discrete dynamical chaotic systems.

(A) Performances comparison with other image cryptosystems

Analyzing previously presented testing results (*i.e.*, the entire section 1.3, *resp.*, sub-section 2.2) it can be concluded that the proposed cryptosystem has a desirable level of security and better or comparable performances with those reported by other scholars, *e.g.*, [23], [40–43], as shown in Table 7.

Table 7

Performances' comparison between the proposed encryption scheme and other pixel-level permutation based image cryptosystems

Criteria		Referenced works					Proposed
		[40]	[23]	[41]	[42]	[43]	
Testing image		Lena, 256 x 256 px, grayscale image					
Global entropy (mean)		7.9984	7.9992	7.9970	7.9976	7.9970	7.9972
APCC	H	0.0109	0.0011	0.0055	0.0040	0.0019	0.0046
	V	0.0139	0.0192	0.0041	-0.0018	0.0038	0.0102
	D	0.0081	0.0045	0.0002	0.0266	-0.0019	0.0037
NPCR		0.9684	0.9979	0.9965	NaN	0.9965	0.9960
UACI		0.3240	0.3335	0.3351	NaN	0.3348	0.3350

Also, when compared with other image cryptosystems of similar conception, the proposed image encryption scheme shows comparable performances, as with [35-39], as shown in Table 8.

Table 8

Performances' comparison between the proposed encryption scheme and other bit-level permutation based cryptosystems

Criteria		Referenced works					Proposed
		[35]	[36]	[37] *after 5 rounds	[38] *after 5 rounds	[39] *after 3 rounds	
Testing image		Lena, 256 x 256 px, grayscale image					
Global entropy (mean)		7.9995	7.9974	7.9994	7.9974	7.9993	7.9972
APCC	H	0.0201	0.0241	0.0010	-0.0022	0.0020	0.0046
	V	0.0129	0.0194	0.0021	0.0011	0.0009	0.0102
	D	0.0057	0.0243	0.0016	-0.0023	0.0016	0.0037
NPCR		0.9961	0.9367	0.9960	0.9960	0.9960	0.9960
UACI		0.3346	0.3333	0.3345	0.3353	0.333	0.3350

3. CONCLUDING REMARKS

In this paper, a chaos-based image encryption algorithm was presented. In other to reduce the Fridrich's structure based redundancies a new inter-intra bit-level permutation strategy was appealed. This strategy was developed using the KenKen puzzles. Through a comprehensive assessment the effectiveness of the proposed approach was demonstrated. Then, cryptosystem's security analysis was performed using various methods and the corresponding experimental results showed that the proposed image cryptosystem has a desirable level of security. Overall, the newly proposed image encryption scheme shows comparable performances with other recently proposed ones, either they feature pixel-level [5, 6, 20, 21] or bit-level [35-39] operations.

REFERENCES

1. L. ZHANG, X. TIAN, S. XIA, *A scrambling algorithm of image encryption based on Rubik's cube rotation and logistic sequence*, in Proc. of the IEEE 2011 Int. Conf. on Multimedia and Signal Processing (CMSP), **1**, pp. 312-315, Guilin, China, 2011.

2. X. FENG, X. TIAN, S. XIA, *An improved image scrambling algorithm based on magic cube rotation and chaotic sequences*, in Proc. of the IEEE 4th Int. Congress on Image and Signal Processing (CISP), **2**, pp. 1021-1024, Shanghai, China, 2011.

3. K. LOUKHAOUKHA, J.-Y. CHOUINARD, A. BERDAI, *A secure image encryption algorithm based on Rubik's cube principle*, Journal of Electrical and Computer Engineering, **2012**, Article ID: 173931, pp. 1-13, 2012. DOI: 10.1155/2012/173931.

4. A.-V. DIACONU, K. LOUKHAOUKHA, *An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher*, Math. Prob. Eng., **2013**, Article ID: 848392, pp. 1-10, 2013. DOI: 10.1155/013/848392.

5. B. STOYANOV, K. KORDOV, *Image encryption using Chebyshev map and rotation equation*, Entropy, **17**, *4*, pp. 2117-2139, 2015. DOI: 10.3390/e17042117.

6. K. LOUKHAOUKHA, M. NABTI, K. ZEBBICHE, *An efficient image encryption algorithm based on block permutation and Rubik's cube principle for iris images*, in Proc. of the IEEE 2013 8th Int. Workshop on Systems, Signal Processing and their Applications, Algiers, Algeria, pp. 267-272, 12-15 May 2013.

7. P. PRAVEENKUMAR, G. ASHWIN, S.P. KARTAVYA AGARWAL, B.S. NAVEEN, V. SURAJ VENKATACHALAM, K. THENMOZHI, R. AMIRTHARAJAN, *Rubik's cube blend with Logistic map on RGB: A way for image encryption*, Research Journal of Information Technology, **6**, *3*, pp. 207-215, 2014.

8. Y. WU, S.S. AGAIAN, J.P. NOONAN, Sudoku associated two dimensional bijection for image scrambling, arXiv: 1207.5856, 2012.

9. Y. WU, Y. ZHOU, J.P. NOONAN, K. PANETTA, S. AGAIAN, *Image encryption using Sudoku matrix*, in Proc. of SPIE, **7708**, pp. 77080P-1-77080P-12, 2010.

10. Y. WU, Y. ZHOU, J.P. NOONAN, S. AGAIAN, *Design of image cipher using Latin squares*, Inform. Sci., **264**, pp. 317-339, 2014. DOI: 10.1016/j.ins.2013.11.027.

11. A.-V. DIACONU, *An image encryption algorithm with a chaotic dynamical system based Sudoku Grid*, in Proc. of the IEEE 10th Int. Conf. on Communications, pp. 1-4, Bucharest, Romania, 29-31 May 2014.

12. H.T. PANDURANGA, S.K. NAVEEN KUMAR, KIRAN, *Image encryption based on permutation-substitution using chaotic map and Latin square image cipher*, Eur. Phys. J. Special Topics, **223**, pp. 1663-1677, 2014.

13. J. DELEI, B. SEN, D. WENNING, *An image encryption algorithm based on Knight's tour and slip encryption filter*, in Proc. of 2007 Int. Conf. on Science and Software Engineering, **1**, pp. 251-255, Wuhan, China, 12-14 December 2008.

14. A.V. DIACONU, A. COSTEA, M.-A. COSTEA, Color image scrambling technique based on transposition of pixels between RGB channels using Knight's moving rules and digital chaotic map, Math. Prob. Eng., **2014**, Article ID: 932875, pp. 1-15, 2014. DOI: 10.1155/2014/932875.

15. X. WANG, J. ZHANG, *An image scrambling algorithm encryption using chaos-controlled Poker shuffling operation*, in Proc. of the IEEE Int. Symp. on Biometrics and Security Technologies, pp. 1-6, Islamabad, 23-24 April 2008.

16. J.J. WATKINS, *Triangular numbers, Gaussian integers and KenKen*, The College Mathematics Journal, **43**, *1*, pp. 37-42, 2012.

17. USC-SIPI Image Database, University of South California, Signal and Image Processing Institute, last accessed on February 2014. ⟨http://sipi.usc.edu/database/database.php⟩.

18. W. ZHANG, K.W. WONK, H. YU, Z.L. ZHU, *A symmetric color image encryption algorithm using the intrinsic features of bit distributions*, Commun. Nonlinear Sci. Numer. Simulat., **18**, pp. 584-600, 2013.

19. N.D. GAGUNASHVILI, *Chi-square tests for comparing weighted histograms*, Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, **614**, *2*, pp. 287-296, 2010.

20. R. BORIGA, A.-C. DASCALESCU, I. PRIESCU, *A new hyperchaotic map and its application in an image encryption image*, Signal Processing – Image, **29**, *8*, pp. 887-901, 2013.

21. A.-C. DASCALESCU, R.-E. BORIGA, *A novel fast chaos-based algorithm for generation random permutations with high shift factor suitable for image scrambling*, Nonlinear Dynam., **73**, pp. 307-318, 2013.

22. Y.Q. ZHAN, X.Y. WANG, A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice, Inform. Sci., **273**, pp. 329-351, 2014.

23. X. WANG, D. LUAN, *A novel image encryption algorithm using a chaos and reversible cellular automata*, Commun. Nonlinear Sci. Numer. Simulat., **18**, pp. 3075-3085, 2013.

24. A.-V. DIACONU, A.-C. DASCALESCU, R.-E.BORIGA, *Study of a new chaotic dynamical system and its usage in a novel pseudorandom bit generator*, Math. Prob. Eng., **2013**, Article ID: 769108, pp. 1-10, 2013. doi: 10.1155/2013/769108.

25. A.-V. DIACONU, *Multiple bitstreams generation using chaotic sequences*, The Annals of "Dunărea de Jos" University of Galaţi, Fascicle III, **35**, *1*, pp. 37-42, 2012.

26. A.J. MENEZES, P.C. OORSCHOT, S.A. VANSTONE, *Handbook of applied cryptography*, CRC Press, 1997.

27. B. FURHT, D. KIROVSKI, *Multimedia security handbook*, CRC Press, 2004.

28. C.E. SHANNON, *Communication theory of secrecy systems*, Bell. Syst. Tech. J., **28**, pp. 656-715, 1949.

29. C.E. SHANNON, *A mathematical theory of communications*, Bell. Syst. Tech. J., **27**, pp. 379-423, 1948.

30. Y. WU, Y. ZHOU, G. SAVERIADES, S. AGAIAN, J.P. NOONAN, P. NATARAJAN, *Local Shannon entropy measure with statistical tests for image randomness*, Inform. Sci., **222**, pp. 323-334, 2013.

31. Y. WU, J.P. NOONAN, S. AGAIAN, *NPCR and UACI randomness tests for image encryption*, Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications, pp. 31-38, 2011.

32. J.H. LINT, R.M. WILSON, *A course in combinatorics*, Cambridge University Press, 2001.

33. X.Y. WANG, X.M. WANG, *A novel block cryptosystem based on the coupled chaotic map lattice*, Nonlinear Dynam., **72**, pp. 707-715, 2013.

34. Y.-Q. ZHAN, X.-Y. WANG, *A new image encryption algorithm based on non-adjacent coupled map lattices*, Appl. Soft. Comput., **26**, pp. 10-20, 2015.

35. C. FU, J.B. HUANG, N.N. WANG, Q.B. HOU, W.M. LEI, *A symmetric chaos-based image cipher with an improved bit-level permutation strategy*, Entropy, **16**, 2, pp. 770-788, 2014.

36. L. TENG, X. WANG, A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive, Opt. Commun., **285**, *20*, pp. 4048-4054, 2012.

37. W. ZHANG, K.W. WONG, H. YU, Z.L. ZHU, *A symmetric color image encryption algorithm using the intrinsic features of bit distribution*, Commun. Nonlinear Sci. Numer. Simulat., **18**, pp. 584-600, 2013.

38. W. ZHANG, K.W. WONG, H. YU, Z.L. ZHU, *An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion*, Opt. Commun., **285**, *9*, pp. 2343-2354, 2012.

39. Z.L. ZHU, W. ZHANG, K.W. WONG, H. YU, *A chaos-based symmetric image encryption scheme using a bit-level permutation*, Inform. Sci., **181**, *6*, pp. 1171-1186, 2011.

40. R. ENAYATIFAR, A.H. ABDULLAH, I.F. ISNIN, *Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence*, Opt. Laser. Eng., **56**, pp. 83-93, 2014.

41. C.Y. SONG, Y.L. QIAO, X.Z. ZHANG, *An image encryption scheme based on new spatiotemporal chaos*, Optik, **124**, pp. 3329-3334, 2013.

42. L. SUI, K. DUAN, J. LIANG, Z. ZHANG, H. MENG, *Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain*, Opt. Laser. Eng., **62**, pp. 139-152, 2014.

43. X. WANG, L. LIU, Y. ZHANG, *A novel chaotic block image encryption algorithm based on dynamic random growth technique*, Opt. Laser. Eng., **66**, pp. 10-18, 2015.