THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 18, Special Issue 2017, pp. 351-360

CORRELATION DISTRIBUTION OF ADJACENT PIXELS RANDOMESS TEST FOR IMAGE ENCRYPTION

Adrian-Viorel DIACONU[*], Ana Cristina DASCALESCU[**]

[*]Ministry of Justice, Information Technology Department, Bucharest, Romania
[**]Titu Maiorescu University, Faculty of Informatics, Department of Informatics, Bucharest, Romania
E-mail: adrian.diaconu@just.ro

Abstract. In this paper, we propose a new qualitative image randomness measure using Pearson's chi-squared test over the correlation distribution of adjacent pixels. The proposed measure overcomes the major weakness of the conventional quantitative adjacent pixels correlation coefficient, i.e., the possibility of inaccurate scores. Examples provided show that the proposed method is more accurate than the conventional adjacent pixel correlation coefficient measure, respectively, its subsequent testing by Student's t-distribution, thus being suitable for an effective use as complementary image randomness test.

***Key words*:** image encryption, security analysis, image randomness, statistical test, adjacent pixels correlation coefficient.

1. INTRODUCTION

1.1. Randomness tests for image encryption

As new image scrambling and (or) encryption algorithms are designed, scholars assess algorithms' efficiency and security level using a variety of methods, e.g., global Shannon entropy measure, histogram analysis, differential cryptanalysis and adjacent pixels correlation [1-4]. As a general requirement, any image scrambling/encryption algorithm should produce an output image which differs significantly in comparison with its plain version (i.e., from the statistical point of view). In this context, one major drawback of the conventional assessment techniques is that they provide quantitative rather than qualitative measures [5]. Thus, that is why, in recent years, many scholars have joined efforts to improve the conventional assessment methods, e.g., [6, 7], or to develop new statistical tests for image randomness, e.g., [5, 8-11].

When performing pixel position and value randomization assessment, one expects that both the position and pixel values to be modified during the encryption procedure [5, 6], and uses the histogram analysis to depict pixels' distribution within the plain vs. the encrypted image. Usually, histogram analysis is limited to a visual assessment, i.e., does (or doesn't) the histogram of the encrypted image gains a uniform distribution, meaningfully different than the one of the original image? But, more thorough analyses are assessing histogram's goodness-of-fit, i.e., with the aid of the chi-square test [8], as a qualitative measure of the extent to which distribution of values within encrypted image's histogram approaches the features of a uniform distribution (i.e., equiprobable frequency counts).

Information entropy [12, 13], i.e., mathematical property that reflects randomness of an information source, is conventionally used in the image encryption community to assess the performance of an image cipher, i.e., the extent to which it can produce a ciphered image having equiprobable grey levels. In an exhaustive study, performed by Wu *et al.* [5], the view was shifted from a global perspective, i.e., the global Shannon entropy, to a far more thorough one, i.e., the local Shannon entropy, which no longer raises the well-known weaknesses: inaccuracy, inconsistency and low efficiency.

On differential analysis, the number of changing pixel rate (NPCR) and the unified average changed intensity (UACI) are the two most common indicators used to assess the strength of an image encryption

algorithm, with respect to differential attacks. Yet, through another comprehensive study [10], the lack of a clear interpretation between the NPCR and UACI scores and the security level provided by the scrambled and (or) the encrypted images led to the establishment of a mathematical model for ideally encrypted images, resp., expectations and variances of NPCR and UACI tests. Wu's et al. studies on information entropy, resp., NPCR and UACI scores, are reflected in most recent papers such as [4], [14-16], [19], resp., [17-19].

Adjacent pixels correlation coefficient (APCC), another common measure used in the assessment of the security level for newly designed image encryption algorithms, is based on the well-known fact that, generally in plain-images, any arbitrarily chosen pixel is strongly correlated with its adjacent pixels (either they are diagonally, vertically or horizontally oriented). Consequently, in the case of high-performance image encryption algorithms, adjacent pixels' correlation scores are expected to be close to zero, i.e., al neighboring pixels considered in the test are weakly correlated. To verify whether the computed APCC is indeed a zero, given the previous study [20], Wu *et al.* have tested if the coefficient follows Student's t-distribution, thus confirming that for the encrypted image the adjacent pixels are truly uncorrelated [9].

When testing if the adjacent pixels correlation score follows Student's t-distribution it should be noted that this test is subject to a method limitation, i.e., only a small percentage of image's pixels are considered (usually 10.000 pairs). Thus, although the resulted adjacent pixels' correlation score (given as a mean value of the correlation coefficients computed for each randomly chosen pair of pixels considered within the test) may follow Student's t-distribution (therefore confirming that for the encrypted image the adjacent pixels are truly uncorrelated) it may be considered an unreliable result (as it is true only for the specific testing conditions, i.e., those particular 10.000 pairs of pixels considered within the test).

In this paper, the above claim is further investigated and a new, straightforward, more accurate and effective measure for image randomness is proposed. Proposed method focuses on correlation distributions of the adjacent pixels which, totally independent of the way of choosing the pairs of pixels, must exhibit a uniform distribution. Using Pearson's chi-squared test, the proposed method works under the null hypothesis that there is no statistical difference between the observed values (i.e., the correlation distributions of the adjacent pixels) and the theoretical values (i.e., the uniform distribution), that is, the correlation distributions of the adjacent pixels followed the assumed distribution, with respect to a significance level α.

The rest of this paper is organized as follows: sub-section 1.2 gives a brief preview on the preliminaries of the proposed image randomness test (*i.e.*, weakness of the conventional quantitative adjacent pixels correlation coefficient, resp., proposal of the improved assessment methodology); Section 2 discusses the simulation setups, with extended performances analysis over some of the existing image encryption schemes (*i.e.*, showcasing the effectiveness of the proposed improved methodology for the assessment of adjacent pixels correlation), and finally Section 3 concludes the paper.

1.2. Preliminaries of the proposed randomness test

Let us consider an 8-bit grayscale encrypted image I of dimension $M \times N$, as shown in Fig. 1.a). In a first instance, we randomly selected 10.000 pixels and used eq. (1) [4] to compute the correlation coefficient with their vertically, horizontally and diagonally adjacent ones. Whilst APCCs (i.e., for all three directions) are summarized in Table 1, in Fig. 1.b), we showcased only the correlation distribution for the horizontally adjacent pixels. We repeated the trial for another series of 10.000 randomly selected pixels, the resulting APPCs being summarized in Table 1, resp., the correlation distribution for the horizontally adjacent pixels being showcase in Fig. 1.c). Finally, Student's t-distribution's statistic t, resp., p-value, were computed using eq. (2) – (4) [5], for each correlation score.

$$\rho(X,Y) = \frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sigma_X \sigma_Y} \tag{1}$$

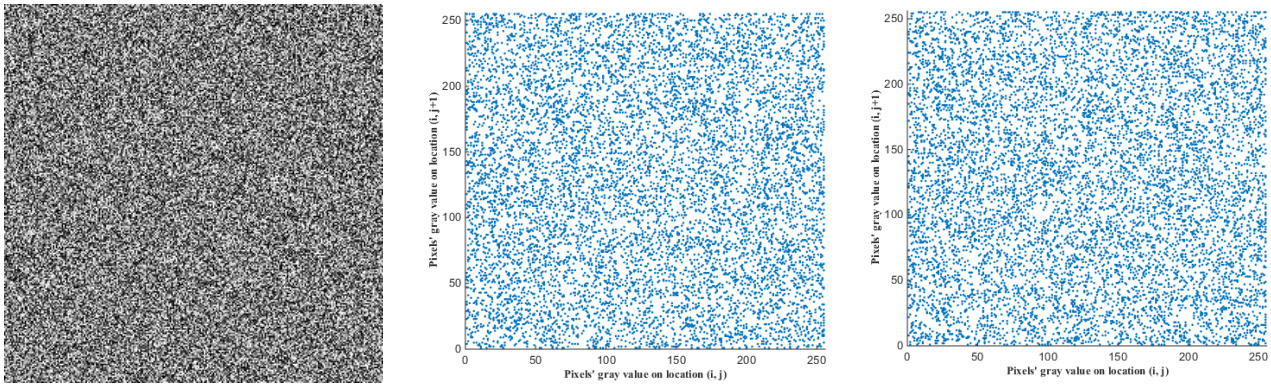
where X represents the series of pixels at position (i,j) and Y represents the series of adjacent pixels, i.e., at position $(i+1,j)$, $(i,j+1)$ or $(i+1,j+1)$, resp., μ is the mean value, σ is the standard deviation and $E[\cdot]$ is the expected value.

$$p - value(t) = \int_{-\infty}^{-|t|} g(\tau)d\tau \tag{2}$$

$$g(t) = \frac{\Gamma\left(\frac{v-1}{2}\right)}{\sqrt{\pi v}\cdot\Gamma\left(\frac{v}{2}\right)}\left(1+\frac{t^2}{v}\right)^{-\frac{v+1}{2}} \tag{3}$$

$$t = \rho\sqrt{\frac{T-2}{1-\rho^2}} \tag{4}$$

where T is the number of pixels within image I, ρ is the adjacent pixels correlation coefficient (computed with the aid of (1)), $v = T - 2$ represents the number of degrees of freedom and $\Gamma[\cdot]$ is the Gamma function.



a b c

Fig. 1 – Experimental setup: a) an 8-bit grayscale encrypted image I; b) correlation distribution of horizontally adjacent pixels in image I – trial 1; c) correlation distribution of horizontally adjacent pixels in image I – trial 2.

Table 1

P-values of adjacent pixels correlation coefficients

Statistics (eq.)		Direction	Test images / Trial Size Degrees of freedom	
			Image I (Fig. 1.a) / Trial 1 *256x256* *65534*	*Image I (Fig.1.a) / Trial 2* *256x256* *65534*
ρ	(1)		-0.0037	-0.0015
Statistic t	(4)	horizontal	-0.9472	-0.3840
p-value (t)	(2)		**0.3435**	**0.7001**
ρ			0.0013	-0.0009
Statistic t		vertical	0.3328	-0.2304
p-value (t)			**0.7393**	**0.8178**
ρ			-0.0024	0.0067
Statistic t		diagonal	-0.6144	1.9712
p-value (t)			**0.5390**	**0.0487**

Screening Table 1 one can notice that, in both trials, the adjacent pixels correlation coefficients ρ are close to zero, which suggests that pixels spatially closed one to another are weakly correlated. To verify whether computed correlation scores are indeed zeros, assuming the null hypothesis (i.e., statistic t, derived

from ρ, follows Student's t-distribution thus implying that the correlation coefficients are indeed zeros, resp., the adjacent pixels are truly uncorrelated), statistic t and p-values were calculated.

Statistically speaking, a p-value is a measure of how much evidence we have under the null hypothesis. In other words, the smaller the p-value the more evidence we have against the hypothesis. Evidently, the range of a p-value is $[0,1]$, with respect to a significance level α. Commonly, $\alpha = 5\%$ is used in the statistics, implying to reject the null hypothesis if the p-value is less than 5%, resp., to accept the null hypothesis otherwise [5].

The intriguing paradox lies within the second trial where, for the same encrypted image, the p-value derived from the diagonally adjacent pixels' correlation coefficient is less than the significance level thus implying that the strong correlation between adjacent pixels isn't sufficiently broken by the underlying scrambling or encryption scheme. Therefore, one faces the situation of choosing which of the two sets of results are unreliable. Again, it must be stressed out that each of the two results is true only for the specific testing conditions, i.e., those particular 10.000 pairs of pixels considered within the trial (that have generated the correlation score which, on its turn, was the basis for calculation of p-value).

Obviously, a negative situation (as the one previously encountered, i.e., in the second trial) does not justify the rebuttal of image's randomness. Instead, it substantiates the need for an assessment tool which is more accurate and effective and, more than that, independent of the adjacent pixels correlation coefficient ρ.

2. ADJACENT PIXELS CORRELATION RANDOMNESS TEST

2.1. Proposed randomness test

In digital images the amount of redundant information is very high, a fact which translates in strong correlation of the adjacent pixels within. In contrast, digital image encryption schemes should greatly reduce these correlations, as closely possible, to a zero value. If one plots the correlation distributions for the plain and encrypted images will notice that the set of adjacent pixels are concentrated along the main diagonal, in the case of the plain images, resp., in the case of the encrypted images, same sets of adjacent pixels are well scattered in the plot [4], [5].

The proposed randomness test for image encryption aims to evaluate how effective is the scattering in the correlation distributions plots, thus substantiating the idea according to which for true random images the correlation distributions of the adjacent pixels exhibit a uniform distribution.

To assess image's randomness based on the correlation distribution of adjacent pixels using Pearson's chi-squared test, the following methodology should be applied:

(i) divide adjacent pixels correlation distribution plot into $\boldsymbol{k}$ non-overlapping blocks, e.g., squared pattern; in other words, the $\boldsymbol{q}$ points within the correlation distribution plot are divided into $\boldsymbol{k}$ different classes;

(ii) with the aid of eq. (5) compute the statistic $\boldsymbol{\chi^2}$, where $\boldsymbol{v_i}$ represents the number of observations within the $\boldsymbol{i}$-th class, resp., $\boldsymbol{v_o}$ is the expected number of observations within each class;

$$\chi^2 = \sum_{i=1}^{k} \frac{(v_i - v_o)^2}{v_o} \tag{5}$$

(iii) get the lower-tail $\boldsymbol{\chi^2_{r,\alpha}}$, resp., the upper-tail $\boldsymbol{\chi^2_{r,(1-\alpha)}}$ critical values of the statistic $\boldsymbol{\chi^2}$, with respect to a significance level $\boldsymbol{\alpha}$ [21];

(iv) with the aid of eq. (6) compute the $\boldsymbol{p}$-value of statistic $\boldsymbol{\chi^2}$, where $\boldsymbol{r = k - 1}$ represents the number of degrees of freedom for the random variable $\boldsymbol{\chi^2}$;

$$p - value(\chi^2) = \frac{1}{\Gamma\left(\frac{r}{2}\right) \cdot 2^{r/2}} \int_{\chi^2}^{\infty} \tau^{(r/2)-1} e^{-\tau/2} d\tau \tag{6}$$

(v) under the null hypothesis that there is no statistical difference between the observed values and the expected ones, i.e., sampled data followed assumed uniform distribution with respect to significance level $\boldsymbol{\alpha}$, verify (7) and: if the inequality is true, accept the null hypothesis with the statistical confidence given by $\boldsymbol{p-value(\chi^2)}$, otherwise reject the null hypothesis.

$$\chi^2_{r,\alpha} < \chi^2 < \chi^2_{r,(1-\alpha)} \tag{7}$$

Let us consider, once again, the $\mathbf{8}$-bit grayscale encrypted image $\boldsymbol{I}$ of dimension $\boldsymbol{M \times N}$ (as shown in Fig. 1.a)), resp., the correlation distributions for the horizontally adjacent pixels shown in Fig. 1.b) and c).

For $\boldsymbol{q = 10.000}$ pairs of adjacent pixels that have generated each of the correlation distribution plots, resp., $\boldsymbol{k = 64}$ non-overlapping blocks considered within the test, distribution of the $\boldsymbol{q}$ points within each $\boldsymbol{i}^{\text{th}}$ class (i.e. the observed values) are shown in Fig. 2.

Under the above circumstances, with $\boldsymbol{v_o = q/k = 156.25}$ (the expected number of observations within each class), $\boldsymbol{\alpha = 0.05}$ (the considered significance level), $\boldsymbol{r = k - 1 = 63}$ (number of degrees of freedom), resp., $\boldsymbol{\chi^2_{r,\alpha} = 45.741}$ and $\boldsymbol{\chi^2_{r,(1-\alpha)} = 82.529}$ (the lower and upper tail critical values of the statistic $\boldsymbol{\chi^2}$), we computed:

- statistic $\boldsymbol{\chi^2 = 69.453}$ and the corresponding $\boldsymbol{p}$-value $= \mathbf{0.2692}$, i.e., in case of correlation distribution shown in Fig. 1.b);
- statistic $\boldsymbol{\chi^2 = 63.130}$ and the corresponding $\boldsymbol{p}$-value $= \mathbf{0.4717}$, i.e., in case of correlation distribution shown in Fig. 1.c).

In both cases, as the statistic $\boldsymbol{\chi^2}$ satisfies (7), with a statistical confidence above the significance level (i.e., $\boldsymbol{p}$-value $> \boldsymbol{\alpha}$), the null hypothesis is accepted, that is, adjacent pixels correlation distributions exhibit a uniform distribution. Hence, one can conclude that the encrypted image is random, with respect to adjacent pixels correlation distributions.

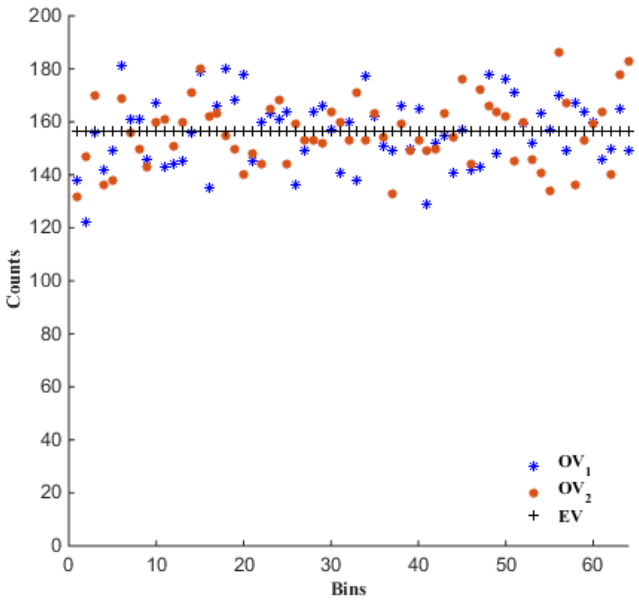


Fig. 2 – Distribution of $\boldsymbol{q}$ points within each $\boldsymbol{i}$-th class, i.e., $\mathbf{OV_1}$ represents the observed values for the correlation distribution plot from Fig. 1.b), $\mathbf{OV_2}$ represents the observed values for the correlation distribution plot from Fig. 1.c), resp., **EV** represents the expected values for each $\boldsymbol{i}$-th class.

2.2. Experimental results and discussions

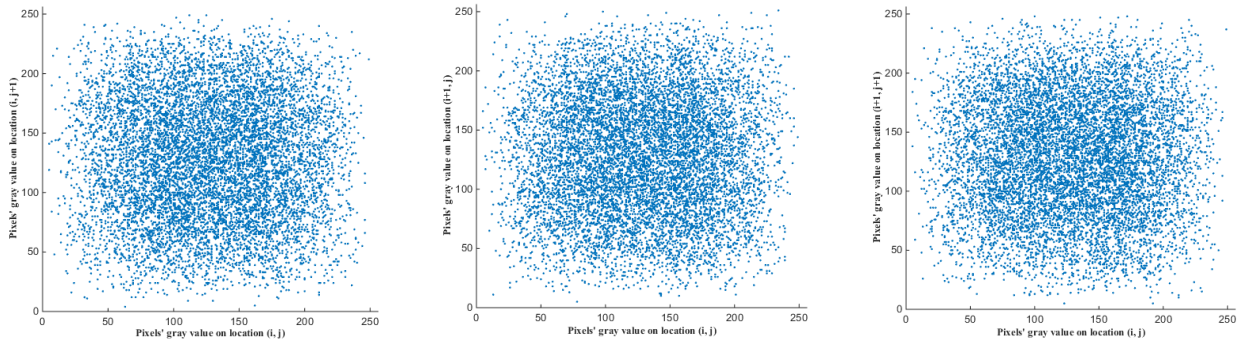
In what follows, the extended analysis on Boriga's *et al.* image encryption algorithm [4] highlights the scrutiny of the newly proposed image randomness assessment method.

Considering the $\mathbf{8}$-bit grayscale, $\mathbf{256 \times 256}$ pixels, standard test image Lenna from USC-SIPI Image Database [22], the encryption scheme [4] was applied to obtain the encrypted image which will be subjected to our testing methodology. After the encryption process, we randomly selected $\mathbf{10.000}$ pairs of two adjacent (i.e., for each of the three directions) and calculated the correlation scores, as summarized in Table 2. Correlation distributions for same pairs of adjacent pixels are shown in Fig. 3. Statistics of the proposed assessment method are summarized in Table 2 while, under the same testing conditions as in the previous section (i.e., $\boldsymbol{q = 10.000}$, resp., $\boldsymbol{k = 64}$), distribution of the $\boldsymbol{q}$ points within each $\boldsymbol{i}$-th class are shown in Fig. 4.

Table 2

Statistics of the adjacent pixels correlation coefficients, resp., statistics of the correlation distributions

Statistics (eq.)		Test images Size Degrees of freedom Direction		
		Lenna *256x256* *65534* *Horizontal*	*Vertical*	*Diagonal*
ρ	(1)	-0.0025	0.0006	-0.0021
Statistic t	(4)	-0.6399	0.1536	-0.5376
p-value (t)	(2)	0.5222	0.8779	0.5909
χ^2	(5)	$8.7988 \cdot 10^3$	$8.7433 \cdot 10^3$	$8.8832 \cdot 10^3$
p-value (χ^2)	(6)	**0**	**0**	**0**



a b c

Fig. 3 – Correlation distributions of: a) horizontally, b) vertically and c) diagonally adjacent pixels from Lenna encrypted image [4].

Screening Table 2, one can notice that the correlation scores $\boldsymbol{\rho}$ are reduced closely to the ideal value, being confirmed as zeros when tested against Student's $\boldsymbol{t}$-distribution (i.e., for each of the testing directions, statistic $\boldsymbol{t}$ follows the assumed distribution and null hypothesis is accepted with a statistical confidence given by each associated $\boldsymbol{p}$-value $(\boldsymbol{t})$), consequently adjacent pixels are considered as being truly uncorrelated [5].

However, this assumption is proved erroneous.

Under the proposed image randomness assessment methodology, the null hypothesis is rejected (i.e., adjacent pixels correlation distributions do not exhibit a uniform distribution). Rejection of null hypothesis is

based on the fact that statistic $\boldsymbol{\chi^2}$ does not satisfy inequality (7), with respect to a significance level $\boldsymbol{\alpha = 0.05}$.

For reliability purposes, both testing methodologies were repeated $\mathbf{1.000}$ times and each time $\mathbf{10.000}$ different random pairs of adjacent pixels were considered. At the end of the trials, the following notable aspect was revealed:

- whilst in $\mathbf{78.2}$% of the cases adjacent pixels correlation scores were accepted as being valid, i.e., for all three directions simultaneously, when tested against Student's $\boldsymbol{t}$-distribution (for the remaining $\mathbf{21.8}$% of the cases adjacent pixels correlation scores being rejected for at least one of the testing directions), when subjected to the newly proposed randomness assessment methodology, all were proved as being false positives.

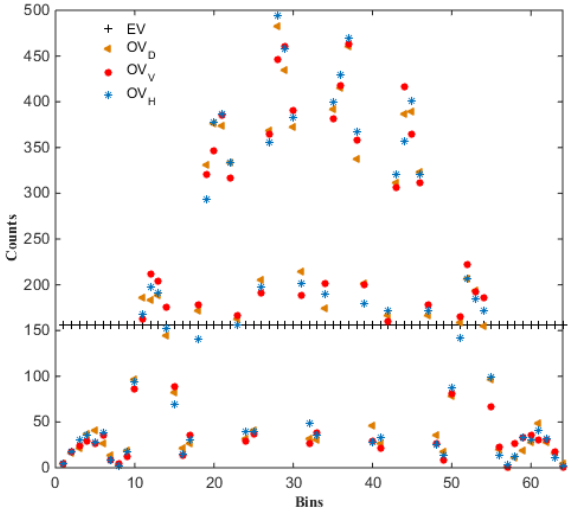


Fig. 4 – Distribution of $\boldsymbol{q}$ points within each $\boldsymbol{i}$-th class, i.e., $\mathbf{OV_1}$ represents the observed values for the correlation distribution plot from Fig. 3.a), $\mathbf{OV_2}$ represents the observed values for the correlation distribution plot from Fig. 3.b), $\mathbf{OV_3}$ represents the observed values for the correlation distribution plot from Fig. 3.c) resp., **EV** represents the expected values for each $\boldsymbol{i}$-th class.

After a short survey of the current literature, we found some other references that are worth mentioning:

- Li et al. [23] proposed a joint image compression and encryption algorithm compliant to JPEG standard which, instead of using the $\mathbf{8 \times 8}$ DCT alone, makes use of a new order-8 orthogonal transforms. Besides the fact that, for 5 out of 10 standard test images from USC-SIPI Image Database [22], the correlation scores are not sufficiently reduced (i.e., the null hypothesis of Student's $\boldsymbol{t}$-distribution is rejected for the corresponding statistic $\boldsymbol{t}$ and $\boldsymbol{p}$-values), the scattering in the correlation distributions plots is poor (i.e., main axis behaves as an attractor for most of the points)1;
- Vashisth et al. [24] proposed a phase-image watermarking scheme which uses gyrator transform in the input and the frequency domains to encrypt the input phase image before combining it with a host image. Singh et al. [25] showcased a method for fully phase image encryption based on double random-structured phase mask encoding in the gyrator transform domain. In both cases, the correlation distribution plots exhibit same properties (i.e., points are accumulating towards the origin of the first quadrant)2;
- Huang et al. [26] developed an image encryption scheme based on a new image permutation approach using combinational chaotic maps. Here, although points seem to be fairly scattered within the correlation distribution plot it is done so for a smaller centered area3.

[1] Assessment based on computations performed for values found in Table 2, resp., on the correlation plot presented in Fig. 11 [23].
[2] Assessments based on the correlation plots presented in Fig. 4.d) [24], resp., in Fig. 5.b) [25].
[3] Assessment based on the correlation plots presented in Fig. 6.b) and c) [26].

These types of behavior exhibited by the correlation distributions of adjacent pixels, i.e., as in [23-26], which undoubtedly rejects the null hypothesis of the proposed method but, not in all cases, the null hypothesis under which Student's ***t***-distribution test works, suggests a careful and thorough reassessment of pixel value randomization, e.g., including computation and assessment of global and local Shannon entropy scores. Nevertheless, previously referenced works will be extensively analyzed in a future paper.

3. CONCLUDING REMARKS

In this paper, we have introduced a new image randomness measure using Pearson's chi-squared test over correlation distributions of the adjacent pixels.

Both the theoretical approach and the experimental results have proved that the proposed qualitative method is more accurate than the conventional, rather quantitative, adjacent pixel correlation coefficient, i.e., by overcoming its major weakness – possibility of computation of inaccurate scores. More than that, being independent of the adjacent pixels correlation coefficients, the proposed method proves itself more effective than the tests involving Student's t-distribution.

Thus, the newly proposed method is suitable for use as a complementary image randomness test.

REFERENCES

1. Y. LI, C. WANG, H. CHEN, *A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation*, Opt. Laser. Eng., **90**, pp. 238-246, 2017. doi: 10.1016/j.optlaseng.2016.10.020.
2. L. XU, Z. LI, J. LI, W. HUA, *A novel bit-level image encryption algorithm based on chaotic maps*, Opt. Laser. Eng., **78**, pp. 17-25, 2016. doi: 10.1016/j.optlaseng.2015.09.007.
3. A. BELAZI, A.A. ABD EL-LATIF, S. BELGHITH, *A novel image encryption scheme based on substitution permutation network and chaos*, Signal Process., **128**, pp. 155-170, 2016. doi: 10.1016/j.sigpro.2016.03.021.
4. R.-E. BORIGA, A.-C. DASCALESCU, I. PRIESCU, *A new hyperchaotic map and its application in an image encryption scheme*, Signal Process. Image., **29**, pp. 887-901, 2014. doi: 10.1016/j.image.2014.04.001.
5. Y. WU, Y. ZHOU, G. SAVERIADES, S. AGAIAN, J.P. NOONAN, P. NATARAJAN, *Local Shannon entropy measure with statistical tests for image randomness*, Inf. Sci., **222**, pp. 323-342, 2013. doi: 10.1016/j.ins.2012.07.049.
6. 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. doi: 10.1016/j.cnsns.2012.08.010.
7. Z.L. ZHU, W. ZHANG, K.W. WONG, H. YU, *A chaos-based symmetric image encryption scheme using a bit-level permutation*, Inf. Sci., **181**, pp. 1171-1186, 2011. doi: 10.1016/j.ins.2010.11.009.
8. 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.
9. Y. WU, Y. ZHOU, S. AGAIAN, J.P. NOONAN, *2D Sudoku associated bijection for image scrambling*, Inf. Sci., **327**, pp. 91-109, 2016. doi: 10.1016/j.ins.2015.08.013.
10. Y. WU, J.P. NOONAN, S. AGAIAN, *NPCR and UACI randomness tests for image encryption*, Cyber J.: Multidiscip. J. Sci. Technol. (J. Sel. Areas Telecommun.), **270**, pp. 31-38, 2011.
11. R. YE, H. LI, *A novel image scrambling and watermarking scheme based on cellular automata*, Proc. of the IEEE Int. Symp. on Electronic Commerce and Security, Guangzhou, China, pp. 938-941, 3-5 August 2008. doi: 10.1109/ISECS.2008.138.
12. C.E. SHANNON, *Communication theory of secrecy systems*, Bell. Syst. Tech. J., **28**, pp. 656-715, 1949.
13. C.E. SHANNON, *A mathematical theory of communications*, Bell. Syst. Tech. J., **27**, pp. 379-423, 1948.
14. M. ZHANG, X. TONG, *Joint image encryption and compression scheme based on IWT and SPIHT*, Opt. Laser. Eng., **90**, pp. 254-274, 2017. doi: 10.1016/j.optlaseng.2016.10.025.
15. X. CHAI, Z. GAN, K. YANG, Y. CHEN, X. LIU, *An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations*, Signal Process.-Image., **52**, 6-19, 2017. doi: 10.1016/j.image.2016.12.007.
16. Z. HUA, Y. ZHOU, *Image encryption using 2D Logistic-adjusted-Sine map*, Inf. Sci., **339**, pp. 237-253, 2016.
17. D. RAVICHANDRAN, P. PRAVEENKUMAR, J.B.B. RAYAPPAN, R. AMIRTHARAJAN, *Chaos based crossover and mutation for securing DICOM image*, Comput. Biol. Med., **72**, pp. 170-184, 2016. doi: 10.1016/j.compbiomed.2016.03.020.
18. J.-X. CHEN, Z.-L. ZHU, C. FU, H. YU, L.-B. ZHANG, *An efficient image encryption scheme using gray code based permutation approach*, Opt. Laser. Eng., **67**, pp. 191-204, 2015. doi: 10.1016/j.optlaseng.2014.11.017.
19. A. BELAZI, A.A. ABD EL-LATIF, A.-V. DIACONU, R. RHOUMA, *Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms*, Opt. Laser. Eng., **88**, pp. 37-50, 2017. doi: 10.1016/j.optlaseng.2016.07.010.
20. A. DONNER, B. ROSNER, *On inferences concerning a common correlation coefficient*, J. R. Stat. Soc. C − Appl. Stat., **29**, 1, pp. 69-76, 1980. doi: 10.2307/2346412.
21. ***, *NIST/SEMATECH e-Handbook of Statistical Methods*, http://www.itl.nist.gov/div898/handbook, June 8, 2017.

22. ***, *USC-SIPI Image Database, USC Signal and Image Processing Institute*, http://sipi.usc.edu/database/database, June 8, 2017.
23. P. LI and K.-T. LO, *Joint image compression and encryption based on order-8 alternating transforms*, J. Vis. Commun. Image. R., **44**, pp. 61-71, 2017. doi: 10.1016/j.jvcir.2017.01.021.
24. A.K. YADAV, S. VASHISTH, H. SINGH and K. SINGH , *A phase-image watermarking scheme in gyrator domain using devil's vortex Fresnel lens as a phase mask*, Opt. Commun., **334**, pp. 172-180, 2015. doi: 10.1016/j.optcom.2015.01.019.
25. H. SINGH, A.K. YADAV, S. VASHISTH and K. SINGH, *Fully phase image encryption using double random-structured phase masks in gyrator domain*, Appl. Opt., **53**, 28, pp. 6472-6481, 2014. doi: 10.1364/AO.53.006472.
26. F. HUANG and G. ZHANG, *A new image permutation approach using combinational chaotic map*, Inf. Tech. J., **12**, 4, pp. 835-840, 2013. doi: 10.3923/itj.2013.835.840.