Image Encryption and Decryption Schemes Using Linear and Quadratic Fractal Algorithms and Their Systems

Anatoliy Kovalchuk [1] [0000-0001-5910-4734], Ivan Izonin [1] [0000-0002-9761-0096]

Christine Strauss [2] [0000-0003-0276-3610], Mariia Podavalkina [1] [0000-0001-6544-0654],

Natalia Lotoshynska [1] [0000-0002-6618-0070] and Nataliya Kustra [1] [0000-0002-3562-2032]

[1] Department of Publishing Information Technologies, Lviv Polytechnic National University, Lviv, Ukraine
akmn0548@gmail.com, ivanizonin@gmail.com, natlot@ukr.net, mariia.podavalkina.vp.2017@lpnu.ua, kno1935@ukr.net
[2] Department of Electronic Business, University of Vienna, Vienna, Austria
christine.strauss@univie.ac.at

Abstract. Image protection and organizing the associated processes is based on the assumption that an image is a stochastic signal. This results in the transition of the classic encryption methods into the image perspective. However the image is some specific signal that, in addition to the typical informativeness (informative data), also involves visual informativeness. The visual informativeness implies additional and new challenges for the issue of protection. As it involves the highly sophisticated modern image processing techniques, this informativeness enables unauthorized access. In fact, the organization of the attack on an encrypted image is possible in two ways: through the traditional hacking of encryption methods or through the methods of visual image processing (filtering methods, contour separation, etc.). Although the methods mentioned above do not fully reproduce the encrypted image, they can provide an opportunity to obtain some information from the image. In this regard, the encryption methods, when used in images, have another task - the complete noise of the encrypted image. This is required to avoid the use of visual imaging techniques. The paper describes the use of RSA algorithm elements in fractal quadratic transformations and fractal transform systems for encrypting / decrypting grayscale images. The values of pixel intensities in the matrix of such images are known to be in the range from 0 to 255. Noise functions in both methods were linear.

Keywords: encryption, decryption, fractal algorithm, contour, image, linear fractal, quadratic fractal, fractal algorithms system.

1. Introduction

Images are one of the most commonly used types of information in various industries [1, 2]. Accordingly, the crucial task is to protect images from unauthorized access and use [3]. The problem of protection against unauthorized access is more challenging

2019 DCSMart Workshop.

and complicated than the problem of protection of use [4]. The clarity of the image is reflected in the clarity of the contours in the image [5]. The task of separating an outline requires the use of operations on adjacent elements that are sensitive to changes and suppress the areas of constant brightness levels. Thus, outlines are the areas where changes occur, becoming light, while other parts of the image remain dark [6, 7].

Mathematically, the ideal outline is the break of the spatial function of the brightness levels in the image plane [5]. Therefore, the separation of the contour means the search for the most abrupt changes, that is, the maxima of the modules of the gradient vector [5, 7]. This is one of the reasons why the contours remain in the image when encrypted with the RSA system [5, 8], since the encryption here is based on raising to a degree the intensity of an individual pixel modulo some natural number [9]. At the same time, on the contour itself and adjacent to the contour pixels elevated to the degree of brightness value results in an even bigger contrast [7].

Various algorithms support the distinction of contours [11], such as tracking algorithms [12]. Tracking algorithms are based on the fact, that the image is searched for an object (the point of the object that is met first) and the contour of the object is tracked and vectorized. The advantage of this algorithm is its simplicity, the disadvantages include their consistent implementation and some complexity in the search and processing of internal contours [11].

An example of such algorithm is the "bug algorithm", which is shown in Fig. 1 The “bug” starts moving from the white area towards the black. As soon as it hits the black element, it turns left and moves on to the next one. If this element is white, then the “bug” turns to the right, otherwise, it turns to the left. The procedure is repeated until the “bug” returns to its starting point. The coordinates of the transition points from black to white and from white to black elements describe the outline of the object.

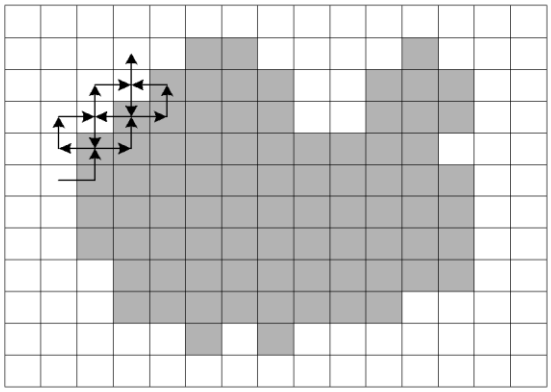


Fig. 1. Scheme of the tracking by “ bug algorithm”

2. Initial assumptions and basic definitions

We assume that the color matrix is matched to the image [5]:

$$\mathbf{C} = \begin{pmatrix} c_{1,1} & \dots & c_{1,M} \\ \dots & \dots & \dots \\ c_{N,1} & \dots & c_{N,M} \end{pmatrix} \quad (1)$$

In relation to the image there are certain tasks of its encryption, namely, the contours on the sharp-fluctuation images are partially preserved [5, 8, 9]. In [7], it was proposed to use linear fractal transformations to encrypt/decrypt grayscale images. In this paper we use quadratic fractal transformations and systems of fractal transformations to encrypt/decrypt grayscale images (the term fractal is derived from the Latin word "fractus" crushed, fractional) - irregular, self-similar structure [13, 14]. In a broad sense, a fractal means a figure whose small portions in an arbitrary magnification are similar to itself. The three common methods of fractals generation are as follows [13, 14]:

- **Iterative functions** are built in accordance with a fixed rule of geometric substitutions. Cantor set, dragon curve, Peano curve, Sierpinski carpet, Sierpinski triangle, Koch curve, T-Square and Menger sponge are examples of such fractals.
- **Recurrent relations** are fractals that are determined by the recurrent relation at each point in space (such as the plane of complex numbers). The examples of fractals of this type are the burning ship, the Mandelbrot set, and the Lyapunov fractal.
- **Stochastic processes** are fractals that are generated using stochastic rather than deterministic processes, such as fractal landscapes, the Levi trajectory, and the Brownian tree. The latter forms the clusters of diffusion concentrates and reaction concentrates.

3. Encryption and decryption using Quadratic Fractal Algorithms.

3.1. Algorithm 3.1: processing by one row of the image *C*.

We will assume that ***P, Q*** is a pair of certain prime numbers [5, 7]. The encryption is performed element by element using the quadratic fractal transformation of the elements of the image matrix ***C*** by the following formulas:

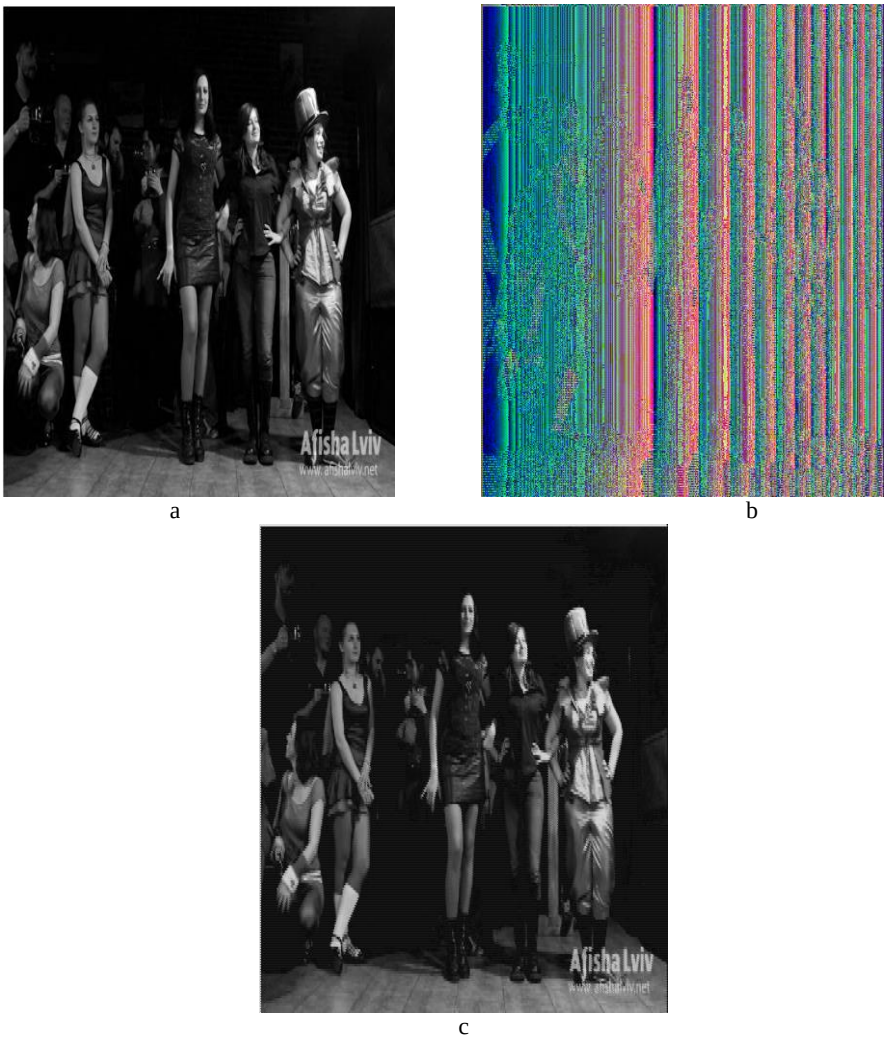
$$x_m^{(k)} = P(x_m^{(k-1)} + f(l))^2 - Q \;\; u = x^e \; (mod \; n), \;\; , \quad m = 1, 2, \dots, M \quad (2)$$

where M - the number of elements in a row, $f(l)$ – functions of noise making, k – fractal iteration number, $x_m^{(0)} = c_{i,j}$ - matrix row element (1).

The decryption is done in reverse order using the following equation:

$$x_m^{(k-1)} = \sqrt{\left(x_m^{(k)} + Q\right)/P \; - \; f(l))} \; u = x^e \; (mod \; n), \qquad m = 1, 2, \ldots, M \quad (3)$$

The results are shown in Fig. 2 after the 5th fractal iteration.



a b c

Fig. 2. Results: a) original image, b) encrypted image, c) decrypted image

3.2. Algorithm 3.2: processing by two rows of the image *C*.

Assume that ***P***, ***Q***, ***R***, ***T*** - four certain prime numbers. The encryption is performed elementwise using the quadratic fractal transformation of the elements of two consecutive rows of the image matrix ***C*** by using the following equations:

$$x_m^{(k)} = P(x_m^{(k-1)} + f(l))^2 - Q \;\; u = \; x^e \; (mod \;\; n), \;\; m = 1, 2, \dots, M \qquad (4)$$

$$y_m^{(k)} = R(y_m^{(k-1)} + g(l))^2 - T \;\; u = \; x^e \; (mod \;\; n), \;\; m = 1, 2, \dots, M \,, \qquad (5)$$

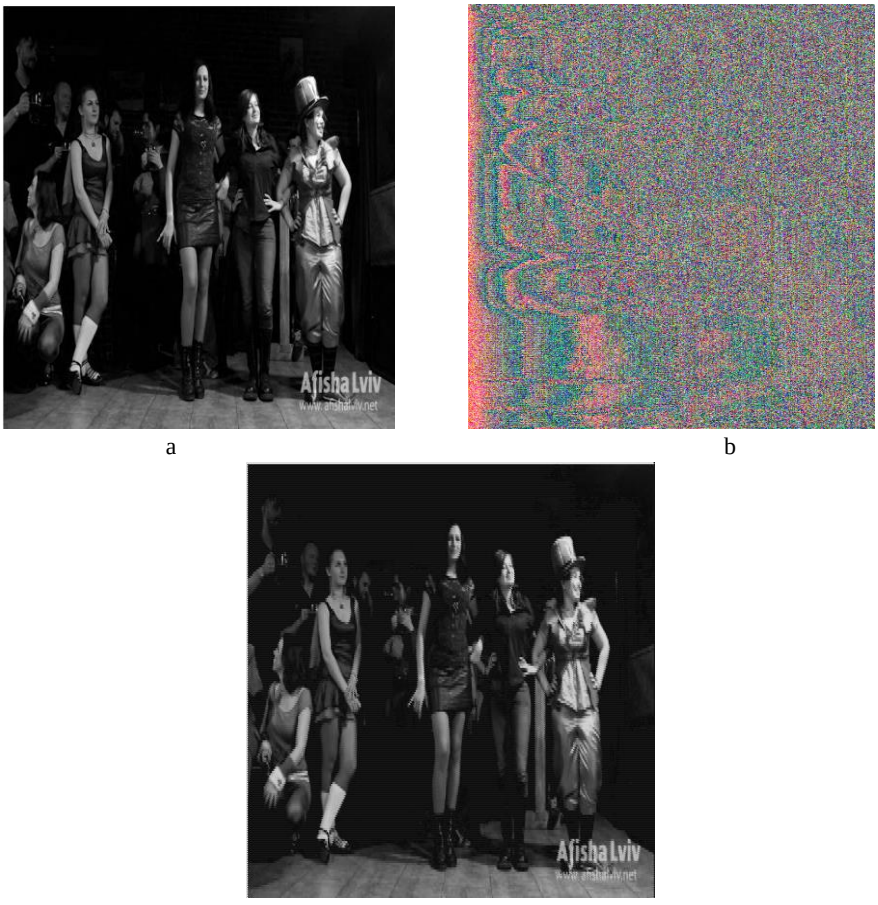
where N_0 - the number of elements in a row, $\boldsymbol{f(l)}$, $\boldsymbol{g(l)}$ –functions of noise making, $\boldsymbol{k}$ – fractal iteration number, $x_m^{(0)} = c_{i,j}$, $y_m^{(0)} = c_{i+1,j}$.

The decryption is done in reverse order using the following equations:

$$x_m^{(k-1)} = \sqrt{\left(x_m^{(k)} + Q\right)/P \; - \; f(l))} \;, \quad m = 1, 2, \dots, M \qquad (6)$$

$$y_m^{(k-1)} = \sqrt{\left(y_m^{(k)} + T\right)/R \; - \; g(l))} \;, \quad m = 1, 2, \dots, M \qquad (7)$$

The results are shown in Figure 3 after the 4th fractal iteration.



a b c

Fig. 3. Results: a) original image, b) encrypted image, c) decrypted image

4. Encryption and decryption using fractal algorithms systems

4.1 Algorithm 4.1: processing by two rows of the image *C*.

Assume that P, Q - a pair of certain prime numbers, $K = (P-1)(Q-1)$, $L = PQ$. The encryption is performed using a fractal transformation of two corresponding elements of two consecutive rows of the image matrix C by the following formulas:

$$\begin{cases} x_m = x_{m-1} - y_{m-1} + (M-i)j(P^e \bmod K - i) \\ y_m = 2x_{m-1}y_{m-1} + (M-i)j(Q^d \bmod K - i) \end{cases} \quad (8)$$
$$i = 1, 2, \dots, M, j = 1, 2, \dots, N$$

where N – image width, M – image height (in pixels) ,

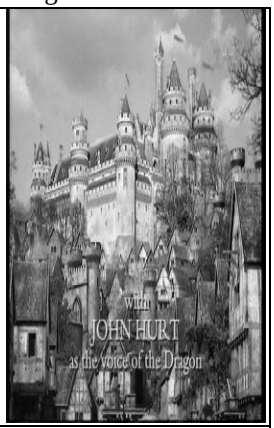
$$ed \equiv 1 \bmod L, \quad x_0 = c_{i,j}, y_0 = c_{i,j+1}.$$

The decryption is done in reverse order using the following formulas:

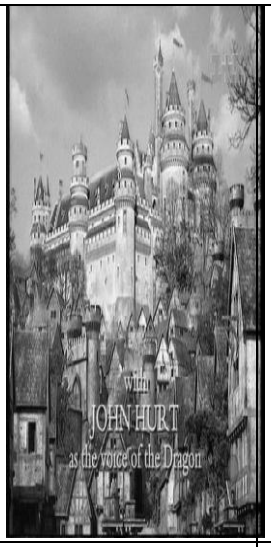
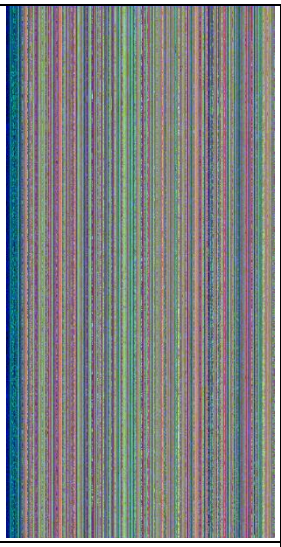
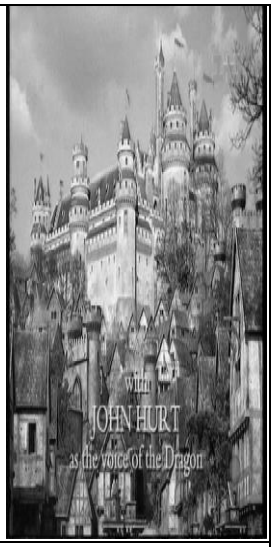
$$\begin{cases} x_{m-1} = \frac{A_m + \sqrt{D_m}}{2} \\ y_{m-1} = \frac{2B_m}{A_m + \sqrt{D_m}} \end{cases} \quad (9)$$

where $D_m = A_m^2 + 4B_m$, $A_m = x_m - (M-i)j(P^e \bmod K - i)$,
$B_m = (y_m - (M-i)j(Q^d \bmod K - i))/2.$

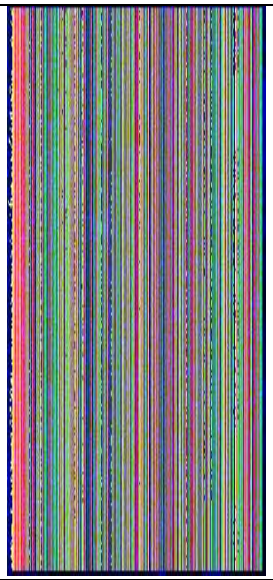
The results for the different values of P and Q are shown in Fig. 4.

P =13 Q=31			
	Original image	Encrypted image	Decrypted image

a

P =31 Q=47			
	Original image	Encrypted image	Decrypted image

b

P =11 Q=97			
	Original image	Encrypted image	Decrypted image

c

Fig. 4. An influence of the different ***P*** and ***Q*** values for image encryption-decryption by two rows: a) P=13, Q=31 , b) P=37, Q=47 , c) P=11, Q=97

4.2 Algorithm 4.2: processing by one row of the image *C*.

Assume that ***P***, ***Q*** - a pair of certain prime numbers, ***K* = (*P* – 1)(*Q* – 1), *L* = *PQ***. The encryption is performed using the fractal transformation of two in order of elements of each row of the image matrix ***C*** by the following formulas:

$$\begin{cases} u_m = u_{m-1} - v_{m-1} + (M+i)j(P^e \bmod K - i) \\ v_m = 2u_{m-1}v_{m-1} + (M+i)j(Q^d \bmod K - i) \end{cases} \quad (10)$$
$$i = 1, 2, \dots, N, j = 1, 2, \dots, M.$$

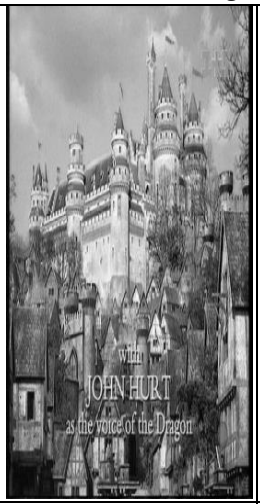
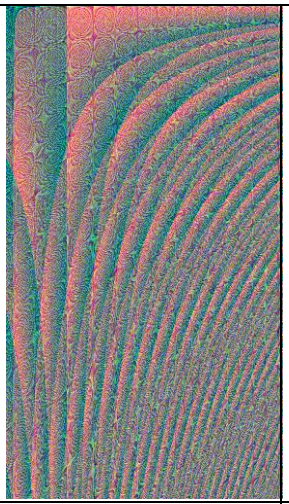
where M – image width, N – image height, $ed \equiv 1 \bmod L$,
$u_0 = c_{i,j}, v_0 = c_{i,j+1}$.

The decryption is done in reverse order using the following formulas:

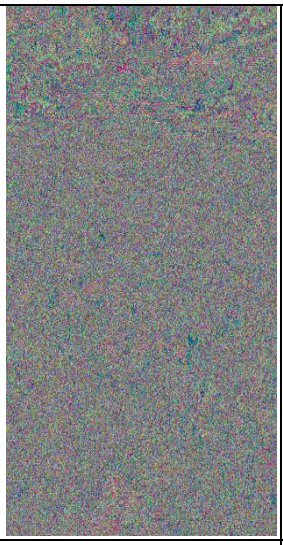
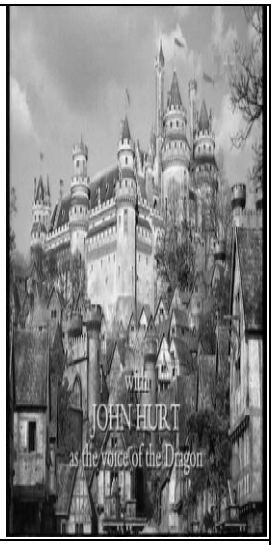
$$\begin{cases} u_{m-1} = \frac{A_m + \sqrt{D_m}}{2} \\ v_{m-1} = \frac{2B_m}{A_m + \sqrt{D_m}} \end{cases} \quad (11)$$

where $D_m = A_m^2 + 4B_m$, $A_m = u_m - (M+i)j(P^e \bmod K - i)$,
$B_m = (v_m - (M+i)j(Q^d \bmod K - i))/2$.

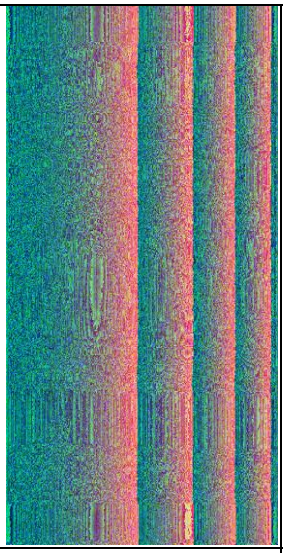
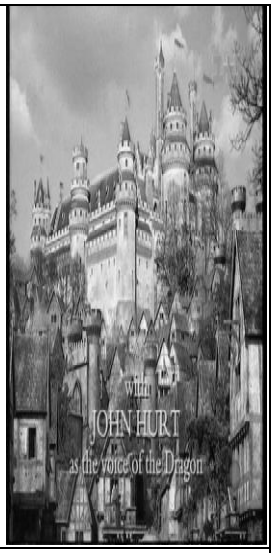
The results are shown in Figure 5 after the 8th iteration with the different ***P***,***Q***.

P =31 Q=97			
	Original image	Encrypted image	Decrypted image

a

P =13 Q=97			
	Original image	Encrypted image	Decrypted image

b

P =11 Q=97			
	Original image	Encrypted image	Decrypted image

c

Fig. 5. An influence of the different ***P*** and ***Q*** values for image encryption-decryption by one row: a) P=13, Q=31 , b) P=37, Q=47 , c) P=11, Q=97

5. Evaluation of encrypted and decrypted images

We have evaluate obtained results using mathematical expectation and dispersion.

5.1 By mathematical expectation.

Figure 6 shows the graphs of the mathematical expectation for the original and decrypted images (P = 13, Q = 97, for example, the selected Fig. 5b)) for the first 38 rows of the pixel intensity matrix. From the graphs, it can be seen that the mathematical expectations for the input and decrypted images are almost equal, so, the deviations of these quantities are small. This is confirmed by a visual comparison.

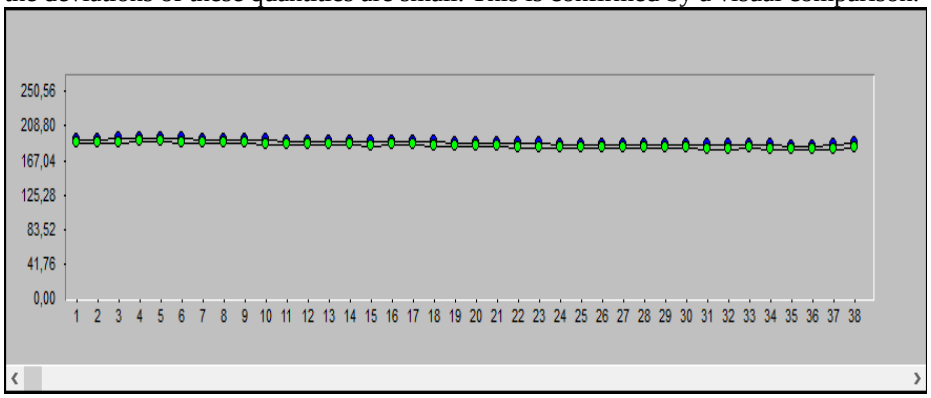


Fig. 6. Mathematical expectation of the original and decrypted images

Figure 7 shows the dispersion graphs for the original and decrypted images (***P*** = 13, ***Q*** = 97, Fig. 5b)) for the first 38 rows of the pixel intensity matrix. The figure shows that the variance of the input and decrypted images is almost equal, so, the variations of these values are even smaller.

5.2 By dispersion.

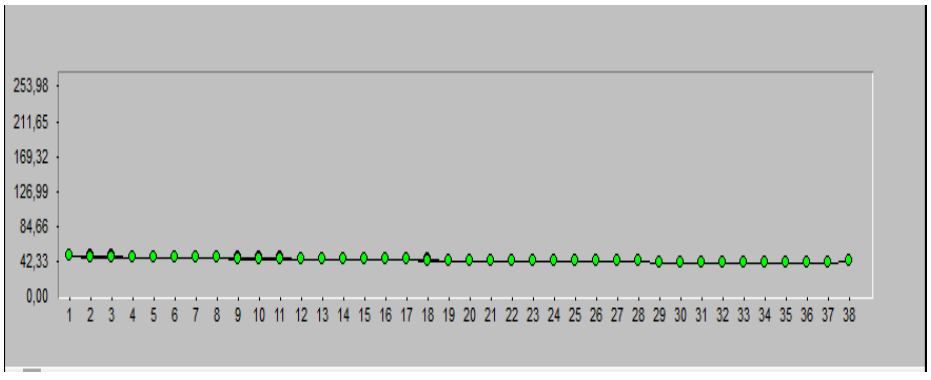


Fig. 7. Dispersion of the original and decrypted images.

6. Discussion and conclusions

Application of quadratic fractal algorithms. From visual comparison of Fig. 2 and Fig. 3, we can see that the encryption using Algorithm 3.1 is different from the encryption by Algorithm 3.2. An image outlines (silhouettes) in both encrypted images are missing. The decrypted image in Fig. 2c) is not visually different from the decrypted image from Fig. 3c. The encrypted images are also not different in color and structurally. These algorithms can be used in the transmission of graphic images and can be applied to any type of images, but the greatest advantages are achieved when using images with the well-defined contours.

Both algorithms (3.1 and 3.2) can also be applied to color images. However, regardless of the type of image, the size of the encrypted image can grow in proportion to the size of the input image.

Usage of fractal transformation systems. Visually comparing the encrypted images at different values of $\boldsymbol{P}$ and $\boldsymbol{Q}$ when encrypting two rows of the matrix (1) (Fig.4) shows that the encryption at different values of simple $\boldsymbol{P}$, $\boldsymbol{Q}$ can differ significantly. But the original image is not visually different from the decrypted one.

The same conclusion can be drawn regarding the encryption / decryption of one row of the matrix (1). The figures also show that encrypting / decrypting one row of an image matrix is different from encrypting two rows of that matrix.

The contours in both cases are missing in the encrypted images. The decrypted images in both cases are visually equivalent. The encrypted images differ structurally and in color.

These algorithms can be used in the transmission of graphic images and can give a satisfactory result for different image, but the biggest advantages are achieved when using images that allow clearly distinguishing the contours. In addition, encryption stability is increased because certain prime numbers (which can be quite large) are used for encryption and decryption, which depends on the stability of the cryptographic algorithm.

Both types of the mentioned encryption algorithms of image encryption/ decryption can also be applied to color images. However, regardless of the type of image, there may be problems in solving the corresponding algebraic non-homogeneous linear systems of equations.

Future research can be conducted to use combinatorics [15] for creating combinatorial encryption methods using [16-18].

References

1. Höckner, M., Hartjes, R., Strauss, C., Kryvinska, N.: "Memoxo" - Browser-based prototype for the audio/video messages recording. In: 2011 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2011, 136-142 (2011)
2. Kryvinska, N., Strauss, C., Collini-Nocker, B., Zinterhof, P. Enterprise network maintaining mobility - architectural model of services delivery. International Journal of Pervasive Computing and Communications 7:114-131 (2011)

3. Nazarkevych M., Lotoshynska N., Klyujnyk I., Voznyi Y., Forostyna S., Maslanych I. Complexity Evaluation of the Ateb-Gabor Filtration Algorithm in Biometric Security Systems. In: 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2019, 961-964 (2019).
4. Nazarkevych M., Riznyk O., Samotyy V., Dzelendzyak U.: Detection of regularities in the parameters of the ateb-gabor method for biometric image filtration. Eastern-European journal of enterprise technologies. № 1(2), 57–65 (2019).
5. Kovalchuk, A., et. al. An efficient image encryption scheme using projective transformations. Procedia Computer Science, vol. 160 : 10th International conference on emerging ubiquitous systems and pervasive networks (EUSPN-2019), 9th International conference on current and future trends of information and communication technologies in healthcare (ICTH-2019) Halifax, Canada, 19-21 August 2019, 584–589 (2019)
6. Rashkevych, Yu. Yu., et. al. The use of disjunctive covering of images to increase strength of the RSA algorithm. In: 2011 Proceedings of 7th International Conference on Perspective Technologies and Methods in MEMS Design, 168-169 (2011)
7. Kovalchuk, A., Lotoshynska, N. Elements of RSA Algorithm and Extra Noising in a Binary Linear-Quadratic Transformations during Encryption and Decryption of Images. In: Proceedings of the 2018 IEEE 2nd International Conference on Data Stream Mining and Processing, DSMP 2018, 542-544 (2018)
8. Iovane, G., Amorosia, A., Benedetto, E., Lamponi G.: An Information Fusion approach based on prime numbers coming from RSA algorithm and Fractals for secure coding. Journal of Discrete Mathematical Sciences and Cryptography, vol. 18, is. 5, 455-479 (2015)
9. AL-Saidi, M.G., et. al.: Efficiency Analysis for Public Key Systems Based on Fractal Functions. Journal of Computer Science, vol. 7, is. 4, 526-532 (2011)
10. Medykovskyy, M., et. al.: Methods of protection document formed from latent element located by fractals. In: 2015 Xth International Scientific and Technical Conference Computer Sciences and Information Technologies (CSIT), IEEE, 70-72 (2015).
11. Maire, M.: Contour Detection and Image Segmentation. Ph.D. dissertation, University of California, Berkeley, 86 (2009)
12. Bruce Schneier. Applied Cryptography. M.: Triumph, 2003. – 815c.
13. Agarwal, S.: Image Encryption Techniques Using Fractal Function: A Review. International Journal of Computer Science & Information Technology (IJCSIT), vol. 9, no 2, 53-68 (2017)
14. Ortiz, S.M., Parra, O., Miguel, J., Espitia, R.: Encryption through the Use of Fractals. International Journal of Mathematical Analysis, vol. 11, no. 21, 1029 – 1040 (2017)
15. R. Oleg, et. al.: Information technologies of optimization of structures of the systems are on the basis of combinatorics methods. In: 2017 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), Lviv, 232-235 (2017) doi: 10.1109/STC-CSIT.2017.8098776.
16. Riznyk, O., Balych B., Yurchak, I.: A synthesis of barker sequences is by means of numerical bundles. In: 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), Lviv, 82-84 (2017) doi: 10.1109/CADSM.2017.7916090.
17. Lu, J., Mo, J., Lv, X., Zhang, Z.: Research on combinatorial encryption method. In: 2014 International Conference on Information Science, Electronics and Electrical Engineering, Sapporo, 1722-1727 (2014) doi: 10.1109/InfoSEEE.2014.6946217
18. O. Riznyk, et. al.: Composing method of anti-interference codes based on non-equidistant structures. In: 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), Lviv, 15-17 (2017) doi: 10.1109/MEMSTECH.2017. 7937522.