UDK 01.05.02; 05.13.06; 05.13.21

[1] A. Koval′chuk, [2]I. Tsmots′, [2]M. Stupen′
National University "Lviv Polytechnic",
[1] Department of Information Technology Publishing,
[2] Department of Management Information System

CUBIC AND LINEAR FRACTAL ELEMENTS RSA ALGORITHM ENCRYPTION AND DECRYPTION IMAGES

Proposed application of cubic fractal changes to the encryption and decryption, grayscale color using elements of the RSA algorithm.

Keywords: encryption, decryption, fractal algorithm, image

Introduction

As with traditional encryption scheme public key encryption is vulnerable in terms of analysis with over all keys. And countermeasures are the same - use long options. However, in this case, there are other options for protection. Public key cryptosystems depend on some reversible mathematical function with special properties. The complexity of this type of calculation functions may not depend linearly on the number of bits in the key, and grow more quickly. Therefore, the key length should be large enough to make brute-force analysis of all keys almost impossible, but small enough to ensure that in practice could use encryption and decryption operations. Suggested for use in practice, the length of the keys, of course, provide practical inefficiency analysis with over all keys, but are too slow to appropriate algorithms could be recommended for universal application. Therefore, as mentioned above, public key encryption is currently constrained areas key management and digital signature applications.

Another form of attack is to try to find a way to calculate the private key to the known public key. To date, no mathematical proof of the impossibility of this form of attack no one algorithm for public key encryption. From this perspective, any particular algorithm type, including widespread algorithm RSA, it turns out that this is not credible. A history of cryptography shows that the problem that seems unsolvable, can be quite solvable, if we look at it from some other, entirely new perspective. This applies to images.

An important characteristic of the image is the presence of image contours. Problem isolation circuit requires the use of operations on neighboring elements, which are sensitive to changes in the field and pryhashayut constant brightness levels, ie, contours - these are areas where there are changes, becoming light, while other parts of the image are dark [2].

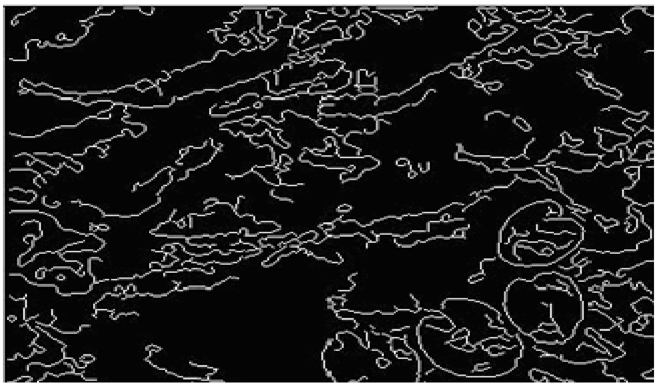
In the circuit image focused information that describes its shape, which is important for perception and pattern recognition. Contour points represent a small part of the entire image. With them you can effectively and simply describe analytically image objects that are invariant to the basic transformations (moving, scaling and rotation). Tasks actual contour analysis in automated image processing systems of various nature: computer vision, biological, medical, etc. [3].

Mathematically - ideal circuit is - the gap spatial features brightness levels in the image plane. Therefore, the selection circuit means finding the most drastic changes, ie the maximum modulus of the gradient vector [2]. This is one of the reasons that the contours of the image remains with encryption system RSA, since encryption is based on exponentiation modulo some integer. In this case, the path and the path to the neighboring pixels to the sublime degree of brightness value gives an even greater gap.

There are various algorithms that produce contours, such as tracking algorithms. Tracking algorithms based on the fact that the image is sought object (object point, which first met) and the contour of the object being tracked and vektorized. The advantage of this algorithm is its simplicity Disadvantages include their consistent implementation and some difficulty in finding and processing the internal circuits.

To determine the contours of zobrazhennnyah using statistical analysis of image fragments and their mutual correlation with the detection of discontinuous variation of color and light. A lot of methods based on the use of mathematical models that represent specific interactions between individual pixels or fragments of images. Also for problem solving object recognition using various methods of filtering, such inverse filters, Wiener Bayes. Thus, the analogy between the dynamics of image and physical processes such as diffusion. To solve some problems using stochastic models.

Algorithms for image segmentation based on one of two characteristics of the luminance signal - rozryvnosti or homogeneity. In the first case, the approach is based on partition image based on abrupt changes in the signal, such as variations in the brightness of the image. Usually breaks search by using sliding masks. The second category of methods is based on the determination of the homogeneity of the image according to pre-selected criteria.



Pict. 1. Singling out the contours of the image.

Further assume that the image is put into compliance matrix color [4,5]

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}. \qquad (1)$$

In relation to the image, there are some problems of its encryption, such as partially stored outlines to sharply fluctuating images [4]. In [5] for encryption - decryption of images in grayscale were asked to use the quadratic fractal transformation. This encryption - decryption of images is proposed to use cubic fractal transformation.

Encryption and decryption of one row of the matrix image.

Let $\boldsymbol{P}, \boldsymbol{Q}$ - arbitrary pair of prime numbers and $\boldsymbol{N = P \cdot Q}$, $\boldsymbol{e \cdot d \equiv 1(mod\ \varphi(N))}$, $\boldsymbol{\varphi(N) = (P\text{-}1)(Q\text{-}1)}$, $\boldsymbol{F = P^e(mod\ \varphi(N)), G = Q^d(mod\ \varphi(N))}$.

Encryption is using cubic fractal transform two neighboring elements in a matrix row panel $\boldsymbol{C}$ the following relations:

$$\begin{cases} u_{n,k} = F^3 u_{n,k-1}^3 + G^3 u_{n+1,k-1}^3 \\ u_{n+1,k} = F u_{n,k-1} + G u_{n+1,k-1} \end{cases} \qquad (2)$$

$n = 1, 2, \dots, N_0$, N_0 - number of elements in a row, $\boldsymbol{k}$ – fractal iteration number, $u_{n,0} = u_n$, $u_{n+1,0} = u_{n+1}$.

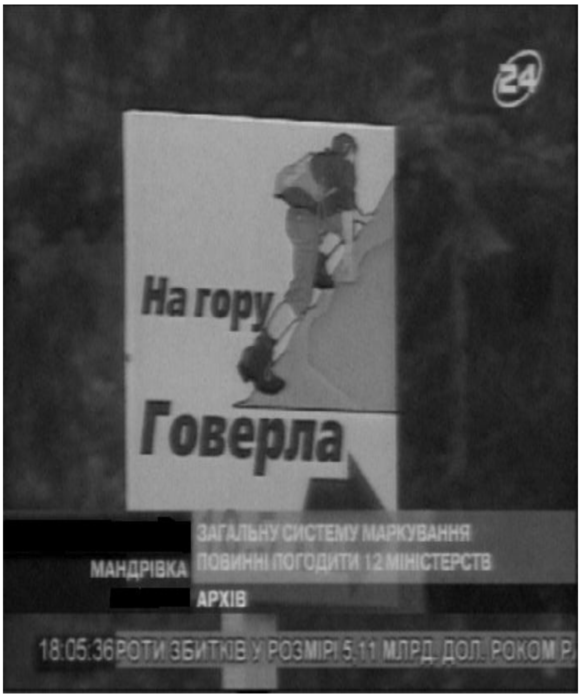
Decryption is performed by the formulas

$$u_{n,k-1} = \frac{3u_{n,k} \pm \sqrt{D}}{6F} , \qquad (3)$$

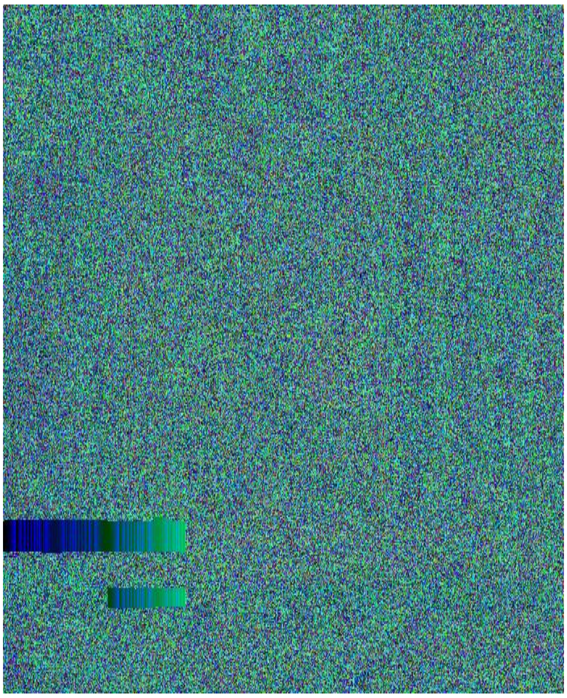
$$u_{n+1,k-1} = \frac{3u_{n,k} \mp \sqrt{D}}{6G} , \qquad (4)$$

when D = $12 u_{n,k}/u_{n+1,k} - 3u_{n+1,k}$.

The results are shown in Pict. 2 – Pict. 4.


24
На гору
Говерла
[redacted]
ЗАГАЛЬНУ СИСТЕМУ МАРКУВАННЯ
МАНДРІВКА
ПОВИННІ ПОГОДИТИ 12 МІНІСТЕРСТВ
[redacted]
АРХІВ
18:05:36 РОТИ ЗБИТКІВ У РОЗМІРІ 5,11 МЛРД. ДОЛ. РОКОМ Р.

Pict.2. The original image.



Pict.3. Encrypted image.

24
На гору
Говерла
[redacted]
ЗАГАЛЬНУ СИСТЕМУ МАРКУВАННЯ
МАНДРІВКА
ПОВИННІ ПОГОДИТИ 12 МІНІСТЕРСТВ
[redacted]
АРХІВ
18:05:36 РОТИ ЗБИТКІВ У РОЗМІРІ 5,11 МЛРД. ДОЛ. РОКОМ Р.

Pict.4. Decrypted image.

Encryption using another cubic fractal transform two neighboring elements in a matrix row image C is realized by the following relations:

$$\begin{cases} u_{n,k} = F^3 u_{n,k-1}^3 - G^3 u_{n+1,k-1}^3 \\ u_{n+1,k} = F u_{n,k-1} - G u_{n+1,k-1} \end{cases} \tag{5}$$

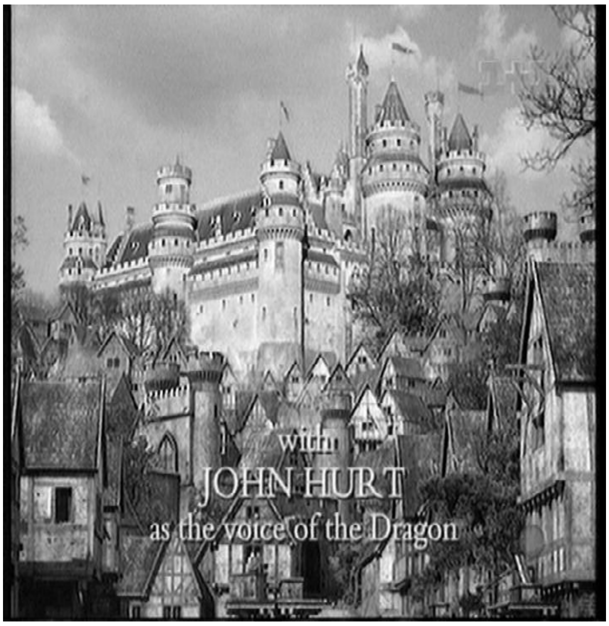
$n = 1, 2, \dots, N_0$, N_0 - number of elements in a row, ***k*** – fractal iteration number, $u_{n,0} = u_n$, $u_{n+1,0} = u_{n+1}$.

To decrypt the formula used

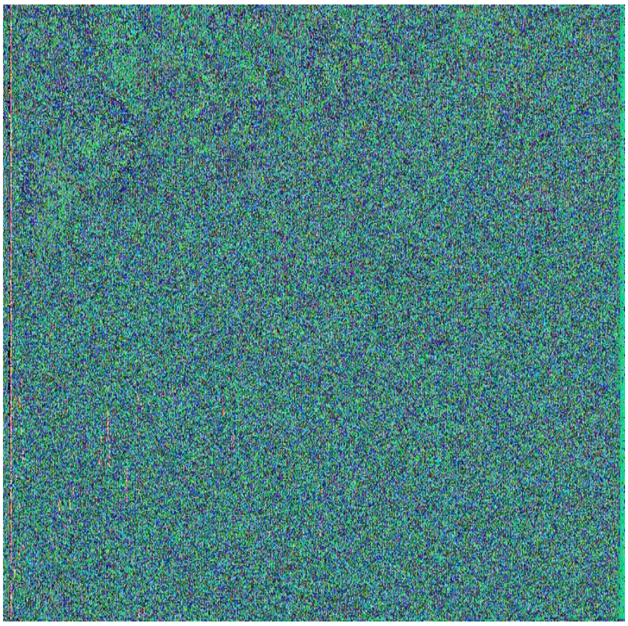
$$u_{n,k-1} = \frac{3u_{n,k} \ \pm \sqrt{\mathrm{D}}}{6F} \quad , \tag{6}$$

$$u_{n+1,k-1} = \frac{-3u_{n,k} \ \mp \sqrt{\mathrm{D}}}{6G} \quad , \tag{7}$$

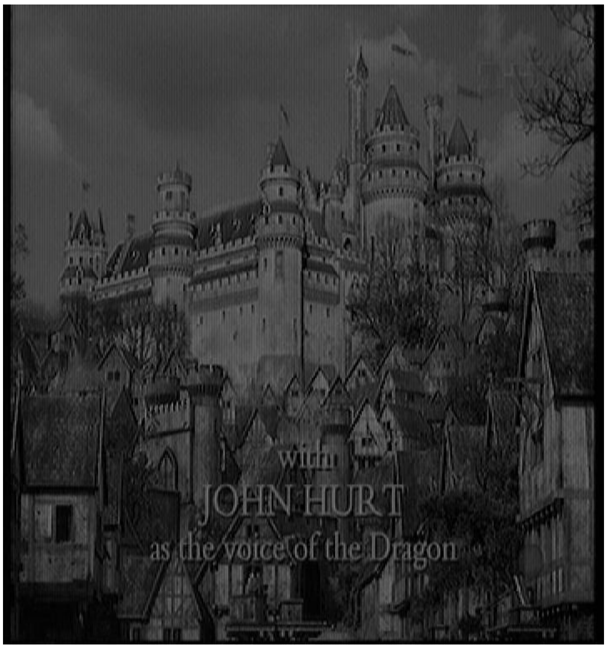
The results are shown in Pict. 5 – Pict. 7. Obviously, the encryption and decryption greatly depends on the choice of simple $\boldsymbol{P},\ \boldsymbol{Q},\ \boldsymbol{R},\ \boldsymbol{T}$ **,** and - the number of fractal iterations.



Pict.5. The original image.

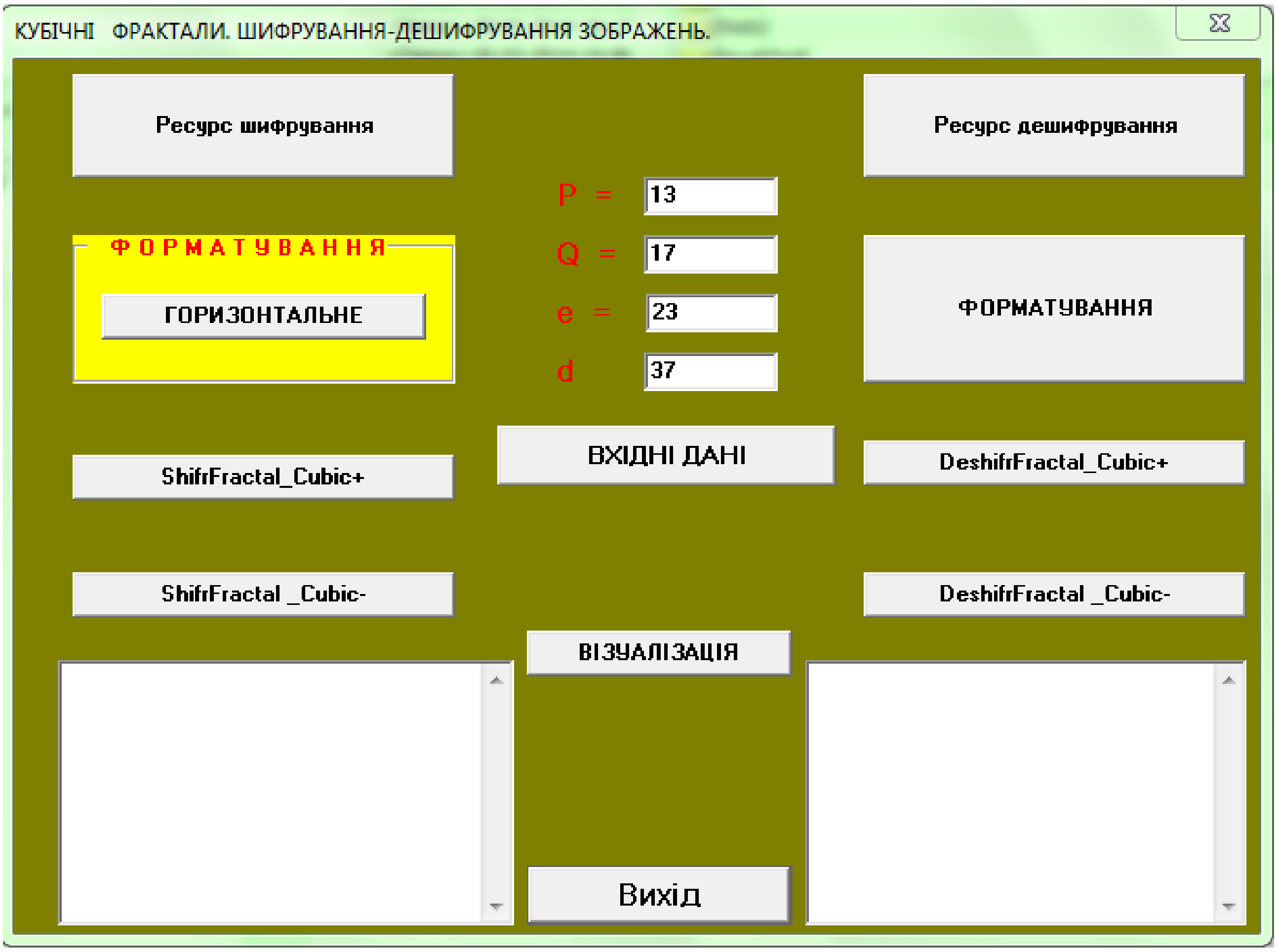


Pict.6. Encrypted image.



Pict.7. Decrypted image.

General view of the form of software encryption-decryption items by formulas (2) - (7) is shown in Pict. 8.



P = 13

Q = 17

e = 23

d 37

Pict.8. General view of the form of software items.

Conclusions

A comparison of Pict. 3 and Pict. 6 visually shows that encryption formulas (2) somewhat structurally different from the encryption formula (5). Contours in both encrypted images available. Decrypted image is both visually equivalent, although deciphering the formulas (5) there is a slight darkening the image. These algorithms can be used for the rapid transmission of graphics and can produce satisfactory results with respect to any type of image, but the biggest benefits are achieved when using the images makes it easy to highlight contours. Increases resistance encryption because encryption and decryption using random prime numbers, which can be quite large, and the elements of the algorithm RSA. And it affects the stability of the cryptographic algorithm. Cryptography stability of the proposed algorithm is higher than the algorithm of RSA.

Both types of algorithms proposed encryption - decryption can be used and for color images. However, regardless of the type of image you may have trouble solving the corresponding algebraic equations.

1. Брюс Шнайер. Прикладная криптография. – М.: Триумф, 2003. – 815с. 2. Б.Яне. Цифровая обработка изображений. – Москва, Техносфера , 2007.- 583с. 3. Прэтт У. Цифровая обработка изображений. Кн. 1,2. - М.: Мир , 1982. 4.Фабрі Л., Ковальчук А., Ступень М. Шифрування і дешифрування зображень з використанням квадратичних фрактальних алгоритмів. Вісник НУ «Львівська політехніка», «Комп'ютерні науки та інформаційні технології», №694, с.180-184. 5. Цмоць І., Ковальчук А., Ступень М. Системи фрактальних алгоритмів в шифруванні – дешифруванні зображень з додатковим зашумленням. Вісник НУ «Львівська політехніка», «Комп'ютерні науки та інформаційні технології», №732, с.288-293.