RESEARCH PAPER

A BLEND OF ALGORITHMSRSAAND BIT, ADDITIVE-DIFFERENCE OPERATIONS AND ALGORITHMSINEL-GAMAL ENCRYPTION-DECRYPTION IMAGES

Anatoliy Kovalchuk*[1], Yuriy Borzov[2], Dmytro Peleshko[3], Igor Malets[4]

*[1] Publishing Information Technologies, Lviv Polytechnic National University, Lviv, Ukraine
dpeleshko@gmail.com[1]
[2] Department "Information Systems Publishing L'viv State University of Life Safety ", Lviv, Ukraine
borzovuo@ukr.net
[3] Publishing Information Technologies, Lviv Polytechnic National University, Lviv, Ukraine
dpeleshko@gmail.com[1]
[4] Department "Information Systems Publishing L'viv State University of Life Safety ", Lviv, Ukraine
igor.malets@gmail.com

Abstract: Presented digital watermarking method of speech signals based on a constructing of quasistationary intervals, pseudoinvariants and singular value decomposition. Proposed a solution to the problem of building quasistationary intervals of speech signal. This method is based on the characteristics of singular value decomposition of square matrices of operators defined on the elementary intervals. Feature of these methods is their independence from the model voice tract. Watermarking method not dependent on input signal and watermark itself.

Keywords: digital watermarking, singular value decomposition, speech signal, quasistationary intervals, invariant, topology, the operator.

INTRODUCTION

Image is one of the most commonly used types of information in today's information society. The urgent task is to protect the image from unauthorized access and use.

The problem of unauthorized use of images is solved by provisions of copyright law to the methods of cryptography and steganography, printing grids, etc.

The main basis for the organization of image protection is supported by the assumption: the image is a stochastic signal. This causes the transfer of classical methods of signal encryption to the case of images. However, a specific image signal, in addition to the standard informative (informative data), is still visual informative. And the latter brings to the protection of new challenges

These very developed modern informative methods of image processing allow for the organization of unauthorized access. In fact, a hacker attack on the encrypted image is possible in two cases: a traditional breaking of encryption or through methods of visual image processing (filtration techniques, edge detection, etc.). Using those encryption methods there is another task - the total noisiness of encrypted image. This is in order to prevent the use of visual methods of image processing.

The RSA algorithm is one of the most widely used industry-standard encryption of signals. In relation to the image, there are certain problems of its encryption, namely, partially retained the contours of fluctuating images [4, 5].

PURPOSE

The urgent task is to develop a modification of method RSA regarding images to:

- Save resistance to decipherment
- Ensure total noisiness, in order to prevent the use of visual methods of image processing.

One of the best solutions of this problem is to combine the properties of RSA algorithm with the bit-and additive-difference operations in software implementation.

CHARACTERISTICS OF IMAGE

A pattern ***P*** of width *l* and height *h* is given. It can be regarded as a matrix of pixels

$$<\delta\tau\pi_{\iota\varphi}>_{1\delta\ \iota\delta\ \nu,\ 1\delta\ \varphi\delta\ \mu}, \qquad (1)$$

where dtp_{ij} – is the pixel with coordinates*i* and *j*, *n* і *m* – a number of dots by width/and height.In general, *n* and *m*are dependent on *l* and *h*, and therefore more correct to write:

$$\nu = \nu(\lambda)\ \imath\ \mu = \mu(\eta). \qquad (2)$$

The Matrix(1) is put in to compliance matrix pixel intensities

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}, \qquad (3)$$

where c_{ij} – intensity value of pixel gray-scale images dtp_{ij} Here is equation [1]

$$P=\mathbf{P}_{l,h}=\left[pxl_{ij}\right]_{1\le i\le n(l),1\le j\le m(h)}\rightarrow\mathbf{C}=\left[c_{ij}\right]_{1\le i\le n(l),1\le j\le m(h)} \qquad (4)$$

For gradation of brightness a byte is usually given, with 0 - black and 255 - white (maximum intensity).

An important characteristic of image is the availability of contours. The task of edge detection requires certain operations of adjacent elements that are sensitive to changes in the area and reduce constant levels of brightness, i.e. contours: these are the areas of image becoming lighter, while others remain dark [2].

Mathematically, perfect contour is a gap of spatial features of brightness levels in the image plane. Therefore, the selection of contour means a search of the most drastic changes, i.e. the maximum of modulus of gradient vector [2]. This is one of reasons why the contours of image remain when encryption RSA, because encryption is based on exponentiation modulo some integer. In this case, exponentiati on brightness value gives an even greater gap on the contour and adjacent pixels.

USING OF BIT OPERATIONS. DESCRIPTIONS OF THE ALGORITHM RSAMODIFICATION

ENCRYPTION AND DECRYPTION OF ONE ROW OF IMAGE.

Suppose P and Q are arbitrary numbers, and $N = P * Q$. Encryption is performed item by item using further transformation matrix elements of C image:

1. Randomly selected integer $e < \varphi(N)$ and there is such integer d when the congruence is performed $ed \equiv 1 \pmod{\varphi(N)}$.
2. A number is constructed $A = (e<<k) + (d<<l) + (e<<l) + (d<<k)$, where $k < 16$, $l < 16$ –are natural numbers, $k \neq l$, <<- is logical shift left.
3. The logical shift left intensity value is in each line, I pixel $i = 1, 2, \ldots, m$, m– a number of elements in a row, the following rule: if $I \bmod 7 = 0$, then the logical shift left intensity value of pixel by the amount of $I \bmod 3$,if $I \bmod 11 = 1$, then the logical shift left intensity value of pixel by the amount of $I \bmod 4$.

Fig.1.Initial image

4. $B$is constructed by subtracting from the obtained number of pixel intensity values **(A– 3).**
5. Encrypted intensity value i pixel $i = 1, 2, \ldots, m$, m– a number of elements in a row selected by $C \equiv B^e \pmod{N}$ Decoding is performed in the reverse order to the encryption after the number of $C^d \equiv (B^e)^d \pmod{N}$, performing the opposite operations to the contents of paragraphs 4), 3), 2), 1).

The results are shown in Figures 1 – 3

Fig.2. Encrypted image

Fig.3. Decrypted image

ENCRYPTIONOF TWOROWS OF THE MATRIX

Encryption is performed using elements of two rows according to the algorithm described above to encrypt the elements of one row intensities, except item 5, where each row of the selected two lines is encrypted independently with its own algorithm item 5modified for it. Item 5is:

5.1.Forthe first row of encrypted value of intensity i pixel $i = 1, 2, \ldots, m$, m– a number of elements in arrow, selected number is$C \equiv B^e \pmod{N}$.

5.2. For the second row of encrypted value of intensity i pixel i

= 1, 2, … ,*m*, ***m*** a number of elements in arrow, selected number is$C \equiv B^d \pmod N$.

Decryption is in the reverse order with the items 5.1and 5.2. The results are shown in Figures 4- 6.

Fig.4. Initialimage

Fig.5. Encrypted image

Fig.6. Decrypted image

From a comparison of Fig. 2 and Fig. 5 is clear that the encryption of one row of the matrix (3) is not much different from the encryption of two rows of matrix. The contours of both encrypted images are missing. Primary and decrypted images are slightly different in brightness levels.

USING OF BIT OPERATIONS. DESCRIPTIONS OF THE ALGORITHM RSAMODIFICATION

ENCRYPTION AND DECRYPTION OF ONE ROW OF IMAGE

Suppose ***P, Q, U, V*** are arbitrary numbers and $N = P * Q$, $L = U * V$. Encryption is performed item by item using further transformation matrix elements of *C* image:

6. Randomly chosen integers $e<\varphi(N)$, $e_1<\varphi(L)$ and there are such integers ***d*** and $d_1$when the congruence is performed $ed \equiv 1 \pmod{\varphi(N)}$, $e_1 d_1 \equiv 1 \pmod{\varphi(L)}$.

7. Let ***a***is one of the numbers ***e*** or***d***, ***b***–is another. Two numbers are constructed: $A = (c_{i,\,j})^a \pmod N$ i$B = (c_{i,j+3})^b \pmod N$.

8. Let $\alpha$is one of the numbers $e_1$ord_1, β - is another. We construct two numbers: $D = (c_{i,\,j+1})^\alpha \pmod L$ i$E = (c_{i,\,j+2})^\beta \pmod L$, and two numbers $u_{i,\,j+1} = D + E$, $u_{i,\,j+2} = D - E$.

9. Encrypted intensity values ***j***, ***j*** +**1**st, ***j*** +**2n**d, ***j*** +**3**rd, pixels, ***i*** **= 1, 2, … , *m***, ***m***– are the number of elements in a row, selected numbers: $A, u_{i,\,j+1}, u_{i,\,j+2}, B$.

Decoding is performed in the following way:

1. There are intensities $c_{i,\,j+1} = [(u_{i,\,j+1} + u_{i,\,j+2})/2]^\beta \pmod L$, $c_{i,\,j+2} = [(u_{i,\,j+1} - u_{i,\,j+2})/2]^\beta \pmod L$

2. There are intensities $c_{i,\,j} = A^b \pmod N$, $c_{i,\,j+3} = B^b \pmod N$.

3. Encrypted intensity values***j***, ***j*** +1st, ***j*** +2nd, ***j*** +3rd, pixels, ***i*** **= 1, 2, … , *m***, ***m***– are the number of elements in a row, selected numbers: $c_{i,\,j}$, $c_{i,\,j+1}$, $c_{i,\,j+2}$, $c_{i,\,j+3}$. The results are shown in Fig.7.

ENCRYPTION ANDDECRYPTION OFONE ROWOF MATRIXWITH ADDITIONALNOISE LEVEL.

Suppose *P, Q, U, V* - are arbitrary numbers and $N = P * Q$, $L = U * V$. Encryption is performed item by item using further transformation matrix elements of *C* image:

1. Random lactose integers $e<\varphi(N)$, $e_1<\varphi(L)$and there are such integers ***d*** and $d_1$when the congruence is performed$ed \equiv 1 \pmod{\varphi(N)}$, $e_1 d_1 \equiv 1 \pmod{\varphi(L)}$.Let ***a***–is one of numbers ***e*** or ***d***, ***b***–is the second. Numbers are constructed: $A = (c_{i,j})^a \pmod N + f(i, j)iB = (c_{i,j+3})^b \pmod N + f(i, j)$.

2.Let α is one of the numbers e_1 ord_1, β– is another. Two numbers are constructed: $D = (c_{i,\,j+1})^\alpha \pmod L$ i$E = (c_{i,\,j+2})^\beta \pmod L$, and two numbers $u_{i,\,j+1} = D + E + f(i, j)$, $u_{i,\,j+2} = D - E + f(i, j)$.

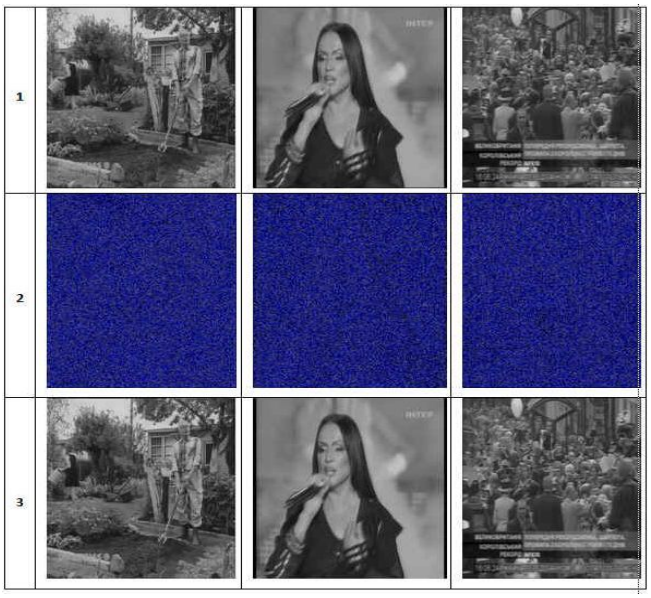

Fig.7. 1) Initial image 2) Encrypted image 3) Decrypted image

1.Encrypted intensity values j, j +1st, j +2nd, j +3rd, pixels, i = **1, 2, … ,** m, m–are the numbers of elements in a row, selected numbers: A, $u_{i,j+1}$,$u_{i,j+2}$, B.

Decoding is performed in the following way:

There are intensities$c_{i,j} = A^b(\mathrm{mod}N) - f(i,j) = A^b(\mathrm{mod}N)$, $c_{i,j+3} = B^b(\mathrm{mod}N) - f(i,j)$, $c_{i,j+1} = [(u_{i,j+1} + u_{i,j+2})/2]^\beta(\mathrm{mod}L) - f(i,j), c_{i,j+2} = [(u_{i,j+1} - u_{i,j+2})/2]^\beta(\mathrm{mod}L) - f(i,j)$.

Encrypted intensity values j, j +1st, j +2nd, j +3rd, pixels, i = **1,2, … ,** m, m- a number of elements in a row, selected numbers: $c_{i,j}$, $c_{i,j+1}$, $c_{i,j+2}$, $c_{i,j+3}$.

Results are shown in Fig.8. To encrypt for additional noise such functions were selected: $f(i,j) = i^2$, $f(i,j) = i^2 + j^2$, $f(i,j) = j^2$.

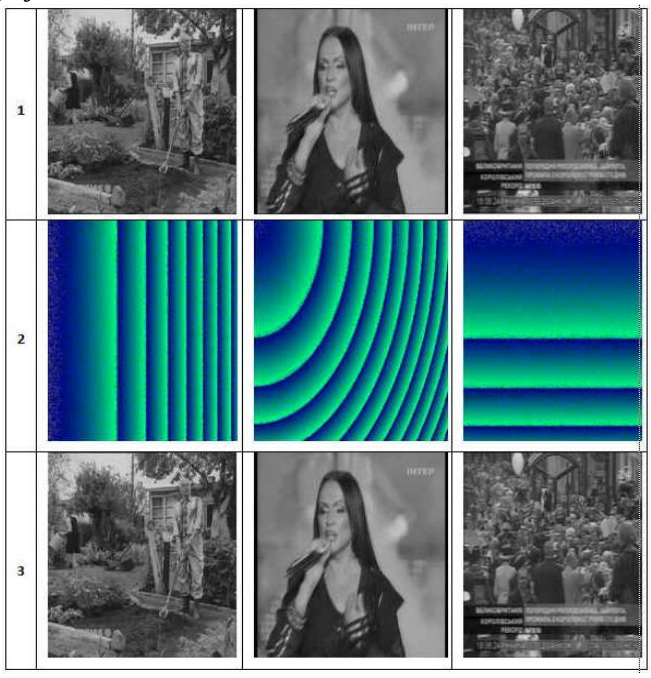

Fig.8.1) Initial image 2) Encrypted image 3) Decrypted image

A comparison of Fig. 7.2 and Fig.8.2 shows that the encryption with additional noise is different from the encryption with out it. The contours of both encrypted images are missing. Primary and decrypted images are slightly different in brightness level. Functions of additional noise $f(i, j)$ can be arbitrary and full functions, and, in addition to the noise generated by the RSA algorithm, increase the cryptographic security of the se modifications.

APPLYING OF EL-GAMAL CRYPTO SYSTEM. DESCRIPTION OFTHE ALGORITHM RSA MODIFICATIONS

ENCRYPTION ANDDECRYPTION OFONEROW OFIMAGE.

Suppose P, Q - are arbitrary numbers and$N = P*Q, \varphi(N) = (P-1)(Q-1)$. Encryption is performed item by item using further transformation matrix color intensity elements of C image:

1. Random lychosen integer $d<\varphi(N)$ and there is a natural number e, where the congruence is performed $ed \equiv 1(\mathrm{mod}\varphi(N))$.
2. Random lychosen integer x, $1 < x < P - 1$, and choose an integer k, $1<k<P-1.-1.$

3. Four numbers are constructed $a \equiv Q$, $b \equiv [(Q]^x \ (mod P])^k (\mathrm{mod} P)$, $a_{i,j} \ (i(i+j)^e \ (mod N) \ . b_{i,j} \equiv j(ij)^d (mod N)$,where$1 \leq i \leq n$, $1 \leq j \leq m$.

4. Matrix of encrypted pixel intensity values is constructed.

$$\tilde{C} = \begin{pmatrix} \tilde{c}_{1,1}, & \cdots & , \tilde{c}_{1,m} \\ & \cdots & \\ \tilde{c}_{n,1}, & \cdots & , \tilde{c}_{n,m} \end{pmatrix},$$

where

$\tilde{c}_{i,j} = ac_{i,j} - bc_{i,j+1} + a_{i,j} + f(i,j)$, $\tilde{c}_{i,j+1} = ac_{i,j} + bc_{i,j+}$, $f(i,j), g(i,j)$ – some functions of noise$1 \leq i \leq n$, $1 \leq j < m$.

The decoding is as follows:

1. Decrypted pixel intensity values are obtained from the following relations:

$ac_{i,j} - bc_{i,j+1} = \tilde{c}_{i,j} - a_{i,j} - f(i,j)$, $ac_{i,j} + bc_{i,j+1} = \tilde{c}_{i,j+1} - b_{i,j} - g(i,j)$, $1 \leq i < n$, $1 \leq j < m$.

Then

$c_1(i,j) = (a(c^*_1(i,j) - a_1(i,j) - f(i,j)) + b(c^*_1(i,j+1) - b_1(i,j) - g(i,j)))/($,

$c_1(i,j+1) = (a(c^*_1(i,j+1) - b_1(i,j) - g(i,j)) - b(c^*_1(i,j) - a_1(i,j) - f(i,j)))/($,

$\delta = a^2 + b^2$.

Fig.9. – Fig.11 show the results of encryption-decryption for P= 53, Q = 67.

Fig.9.Initial image

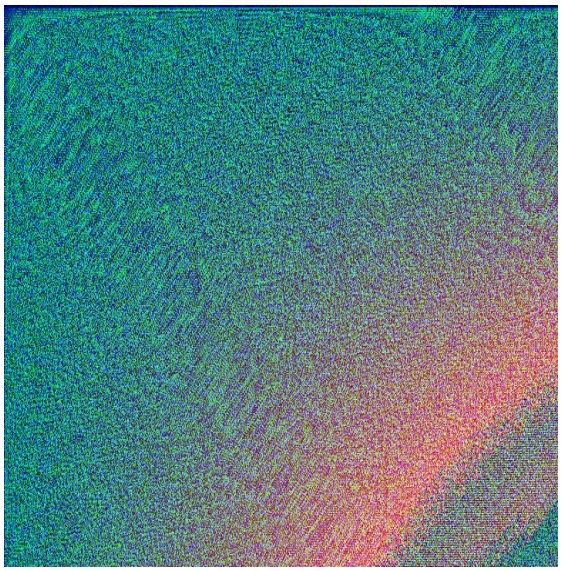

Fig. 10.Encrypted image

Fig.11. Decrypted image

ENCRYPTION AND DECRYPTION OF TWO ROWS OF MATRIX WITH ADDITIONAL NOISE IMAGES.

Suppose P,Q – are arbitrary integers and $N = P*Q, \varphi(N) = (P-1)(Q-1)$.

Encryptionisperformeditembyitemusingfurthertransformation matrixcolorintensityelementsof$C$image:

1. Randomly chosen integer $d<\varphi(N)$ and there is a natural number e, when the congruence is performed $ed \equiv 1 (\mathrm{mod}\, \varphi(N))$.
2. Randomly chosen integer x, $1<x<P-1$, and choose natural number k, $1<k<P-1$.
3. Four numbers are constructed $a \equiv Q$, $b \equiv [(Q]^x \ (mod P))^k (\mathrm{mod} P)$, $a_{i,j} \ (i(i+j)^e (mod N), b_{i,j} \equiv j(ij)^d (mod N)$, where $1 \le i \le n$, $1 \le j \le m$.
4. Matrix of encrypted pixel intensity values is constructed.

$$\tilde{C} = \begin{pmatrix} \tilde{c}_{1,1} & \cdots & \tilde{c}_{1,m} \\ \cdots & \cdots & \cdots \\ \tilde{c}_{n,1} & \cdots & \tilde{c}_{n,m} \end{pmatrix},$$

where

$\tilde{c}_{i,j} = ac_{i,j} - bc_{i+1,j} + a_{i,j} + f(i,j)$, $\tilde{c}_{i+1,j} = ac_{i,j} + bc_{i+1,j} + b_{i,j} + g(i,j)$, $f(i,j), g(i,j)$ – some functionsof noise, $1 \le i \le n$, $1 \le j < m$.

The decoding is as follows:

Decrypted pixel intensity values are obtained from the following relations:

$ac_{i,j} - bc_{i+1,j} = \tilde{c}_{i,j} - a_{i,j} - f(i,j)$, $ac_{i,j} + bc_{i+1,j} = \tilde{c}_{i+1,j} - b_{i,j} - g(i,j)$, $1 \le i < n$, $1 \le j < m$.

then $c_1(i,j) = (a(\tilde{c}_1(i,j) - a_1(i,j) - f(i,j)) + b(\tilde{c}_1(i+1,j) - b_1(i,j) - g(i,j)))/($,

$c_1(i+1,j) = (a(\tilde{c}_1(i+1,j) - b_1(i,j) - g(i,j)) - b(\tilde{c}_1(i,j) - a_1(i,j) - f(i,j)))/($,

$\delta = a^2 + b^2$.

Fig.12. Initial image

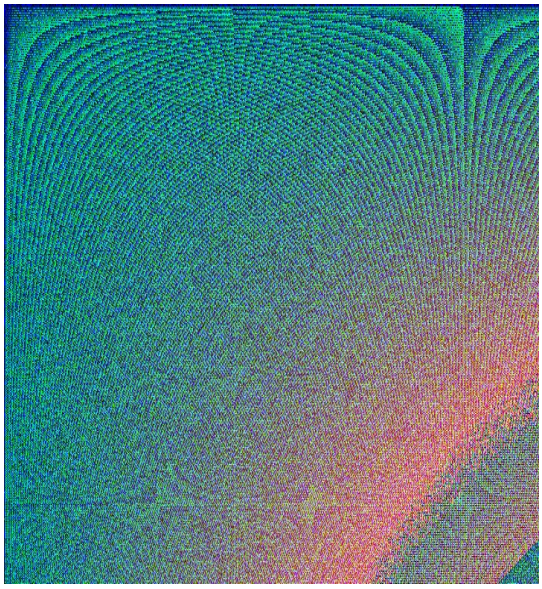

Fig. 13.Encrypted image

Fig.14.Decrypted image

Note that the encryption of noise structure with additional properties is visually different, depending on the choice of structure and the order of selected noise pixels of input image. It can be used in a topological modifications encryption-decryption algorithm.

CONCLUSIONS

1. Proposed modifications are intended to encrypt the grayscale images and are based on the use of basic algorithm RSA.
2. Suggested modifications can be used for any type of image, but the greatest results are obtained in case of images which can clearly detect contours.
3. Both types of modifications for sure can be applied for color images.

However, regardless of the type of image, proportionally to the dimension of input image, the size of the encrypted image can grow.

4. Resistance to unauthorized decryption of proposed modification provides algorithm RSA.
5. In case of El-Gamal algorithm the stability of modified cryptographic algorithm is determined by resistance of two used algorithms - El-Gamal and RSA, and while ensuring the quality of image, it does not require much processing power.

REFERENCES

[1] Bruce Schneier. Applied Cryptography-Protocols, algorithms, and source code in C. Second edition. New York, Issue John Wiley & Sons, 1996.

[2] Ch.K. Volos, I.M. Kyprianidis, I.N. Stouboulos. (2013) Image encryption process based on chaotic synchronization phenomena. Signal Processing. Vol. 93, Issue 5, 2013, Pages: 1328-1340.

[3] Feng Huang, Yong Feng, Xinghuo Yu. A symmetric image encryption scheme based on simple novel two-dimensional map. International Journal of Innovative Computing, Information and Control, 2007, Vol. 3, Number 6(B), pp. 1593—1602.

[4] Fengling Han, Jiankun Hu, Xinghuo Yu, Yi Wang. (2007) Fingerprint images encryption via multi-scroll chaotic attractors. Applied Mathematics and Computation. Vol. 185, Issue 2, 2007, Pages: 931-939.

[5] Gaochang Zhao, Xiaolin Yang; Bin Zhou; Wei Wei. RSA-based digital image encryption algorithm in wireless sensor networks. Proc. Of Signal Processing Systems (ICSPS), 2010 2nd International Conference on 5-7 July 2010, Vol., Issue 2, Page(s), Issue V2-640 - V2-643.

[6] Gonzalo Alvarez, Shujun Li. Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos. Vol. 16, No. 08, 2005, pp. 2129-2151.

[7] GuanrongChen,YaobinMao,Charles K. Chui. A symmetricimageencryptionschemebasedon 3D chaoticcatmaps. Chaos, Solitons&Fractals. Vol. 21, Issue 3, 2004, Pages: 749–761.

[8] HongjunLiu,XingyuanWang. Abdurahmankadir. Imageencryptionusing DNA complemen-tary ruleandchaoticmaps. AppliedSoftComputing. Vol. 12, Issue 5, 2012, Pages: 1457–1466

[9] HongjunLiu,XingyuanWang. Colorimageencryptionbasedon one-timekeysandrobustchaoticmaps. Computers&MathematicswithApplications. Vol. 59, Issue 10, 2010, Pages: 3320–3327.

[10] KaiWang, Pei, LiuhuaZou, AiguoSong, ZhenyaHe. Onthesecurityof 3D Catmapbasedsymmetricimageencryptionscheme. PhysicsLetters A. August 2005, Vol. 343, Issue 6, 2005, Pages: 432–439.

[11] KristinaKelber, Wolwang Schwarz. Some design rules foe cgaos-based encryption systems. InternationalJournalofBifurcationandChaos. Vol. 17, Issue 10, 2007, Pages: 3703-3707.

[12] M. François,T. Grosges,D. Barchiesi,R. Erra. A newimageencryptionscheme based on a chaoticfunction. Signal Processing, IssueImageCommunication. Elsevier. Vol. 27, Issue 3, 2012, Pages: 249–259.

[13] RhoumaRhouma,SoumayaMeherzi,SafyaBelghith. OCML-basedcolourimageencryption. Chaos, Solitons&Fractals. Elsevier. Vol. 40, Issue 1, 2009, Pages: 309–318.

[14] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan. A fastchaoticencryptionschemebasedonpiecewisenonlinearc

haoticmaps. PhysicsLetters A. Vol. 366, Issue 4-5, 2007, Pages: 391-396.

[15] SaharMazloom,AmirMasud Eftekhari-Moghadam. ColorimageencryptionbasedonCoupledNonlinearChaotic Map. Vol. 42, Issue 3, 2009, Pages: 1745–1754.

[16] SeyedMohammadSeyedzadeh,SattarMirzakuchaki. A fastcolorimageencryptionalgorithmbasedoncoupled two-dimensionalpiecewisechaoticmap. Signal Processing. Vol. 92, Issue 5, 2012, Pages: 1202–1215.

[17] ShiguoLian, JinshengSun, ZhiquanWang. A blockcipherbasedon a suitableuseofthechaoticstandardmap. Chaos, Solitons&Fractals. October 205, Vol. 26, Issue 1, 2005, Pages: 117–129.

[18] ShiguoLian, JinshengSun, ZhiquanWang. Securityanalysisof a chaos-basedimageencryptionalgorithm. Physica A, IssueStatisticalMechanicsanditsApplications. Vol. 351, Issues 2–4, 2005, Pages: 645–661.

[19] Sun Fu-Yan, Liu Shu-Tang, Lü Zong-Wang. Imageencryptionusing high-dimensionchaoticsystem. ChinesePhysics. Vol. 16, Issue 12, 2007, Pages: 3616-3623.

[20] TaoXiang, Kwok-Wo Wong, XiaofengLiao. A novelsymmetricalcryptosystembasedondiscretized two-dimensionalchaoticmap. PhysicsLetters. Vol. A 364, Issue 3-4, 2007, Pages: 252-258.

[21] TiegangGao, ZengqiangChen. A newimageencryptionalgorithmbasedon hyper-chaos. PhysicsLetters A. Vol. 372, Issue 4, 2008, Pages: 394-400.

[22] WeiZhang, Kwok-woWong, HaiYu, Zhi-liangZhu. Animageencryptionschemeusingreverse 2-dimensional chaoticmapanddependentdiffusion. CommunicationsinNonlinearScienceandNumericalSimulation. Vol. 18, Issue 8, 2013, Pages: 2066–2080.

[23] XiaojunTong, MinggenCui,ZhuWang. A newfeedbackimageencryptionschemebasedonperturbation withdynamicalcompoundchaoticsequenceciphergenerator. OpticsCommunications. Vol. 282, Issue 14, 2009, Pages: 2722–2728

[24] XiaojunTong, MinggenCui. Imageencryptionwithcompoundchaoticsequenceciphershifting dynamically. ImageandVisionComputing. Vol. 26, Issue 6, 2, 2008, Pages: 843–850.

[25] XingshaLiu, LiMin, FEI Yao-ping. A high-securitydigitalimageencryptionalgorithm [J]. MicroelectronicsandComputer, 2007, 24 (2), Issue 21-23, 27.

