RSA ALGORITHM IN FRACTIONAL-RATIONAL N-ARY FORMS WHILE ENCRYPTION-DECRYPTION OF MONOCHROME IMAGES

Anatoliy Kovalchuk, Senior Lecture, Nataliia Kustra, PhD, Ass.-Prof., Svyatoslav Yatsyshyn, Dr.Sc., Prof.,
Lviv Polytechnic National University, Ukraine;
e-mail: akm0519@gmail.com

Abstract. The basis for image protection is the assumption that the image is a stochastic signal. But the image is a specific signal that possesses, in addition to typical informativeness (informativeness of data), also visual informativeness, which brings new challenges to the issue of protection. Therefore, the urgent task is to implement such application of the RSA algorithm that when encrypting an image: – the cryptographic stability of the RSA algorithm did not deteriorate; – achieves full image noise to prevent the use of visual image processing methods.

An algorithm for encryption-decryption of monochrome images in fractional-rational forms of order n using the elements of the RSA algorithm is proposed, as the most resistant to unauthorized decryption of signals. The proposed algorithm is applied to images with strictly separated contours. Elements of the RSA algorithm are applied to construct the coefficients of fractional-rational affine transformations. The developed algorithm is inherent in the higher cryptographic stability compared to the ordinary RSA algorithm. The possibilities of using the elements of the RSA algorithm in affine transformations while encrypting and decrypting images are described.

The results of encryption modeling for cryptographic transformations of monochrome images of a given dimension are given. Modified models and algorithmic procedures of key formation processes, direct and inverse cryptographic transformations, reduced to mathematical element-by-element operations, have been developed.

Key words: Encryption, Monochrome image, Fractional-rational affine transformation, Contour, Decryption.

1. Introduction

In the era of information technologies and mass communications, the need to solve the challenges of information security and achieve the necessary level of protection of information of various contents led to the corresponding accelerated development of cryptography.

An image can be defined as a two-dimensional function $f(x, y)$, where x and y are coordinates in space (specifically, on a plane). The value of $f(x, y)$ at any point is called the intensity or gray level at that point. If the values x, y, and $f(x, y)$ take a finite number of discrete values, then we consider a digital image. The latter's processing consists of the computer processing of digital images. Note that a digital image includes a finite number of elements, each of which is located in a specific place and acquires a certain value. These elements are denominated as picture elements or pixels.

Mathematically, a digital image is displayed by an n by m matrix of pixel intensities, where n is the number of image rows, m is the number of columns. The most common and stable information encryption algorithm is the RSA algorithm [1-2], which is one of the most used public key algorithms. The security of the RSA algorithm is based on the resource-intensive factorization of large natural numbers. The application of the RSA algorithm, as the most resistant to unauthorized decryption, concerning images in which contours are strictly separated, does not give satisfactory results. On the encrypted image, it is possible to distinguish the main contours of the input image or arise an effect of incomplete noise.

Extracting the contour means finding the maxima of the modulus of the gradient vector [2-3]. This is one of the reasons why contours remain in the image while encrypting by the RSA system since RSA encryption is based on exponentiation modulo of a certain natural number. The presence of contours in the image is an important characteristic of the image. The task of extracting a contour requires the use of operations on neighboring elements that are sensitive to changes and suppress the values of brightness levels. That is, contours are those areas where changes occur, becoming light, while other parts of the image remain dark [4-5]. At the same time, on the contour and the pixels adjacent to the contour, raising the luminance value to the power gives an even greater gap [8-17]. Considering the image, there arise particular problems with its encryption. Namely, contours on sharply fluctuating images are partially preserved. Therefore, the following consideration is based on an affine transformation of Euclidean space in Cartesian coordinates. In such a manner, a transformation of Euclidean space is called affine if this transformation maps every plane to a plane.

2. Drawback

Studies [6-7] have established that significant deviations in pixel intensity values can be created in the area of contours in the image during encryption, which makes it impossible to blur these contours at certain values of selected simple numbers.

3. The Aim of the Work

The aim is to create a modification of the RSA algorithm, using fractional-rational affine transformations and various elements of the RSA algorithm, for a complete visual blurring of image contours.

4. Encryption Method Issue

The elements of the RSA algorithm are the simple numbers ***P*** and ***Q*** as well as the numbers ***e*** and ***d***, obtained from the congruence $ed \equiv 1 \pmod{\varphi(N)}$, $N = P*Q$, where $\varphi(N)$ is the Euler function.

Let's assume that the image is matched with a color matrix **C** (matrix of pixel intensities) [4, 6-7]:

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

The fractional-rational ***n***-ary form of the transformation of Euclidean space in Cartesian coordinates has the form:

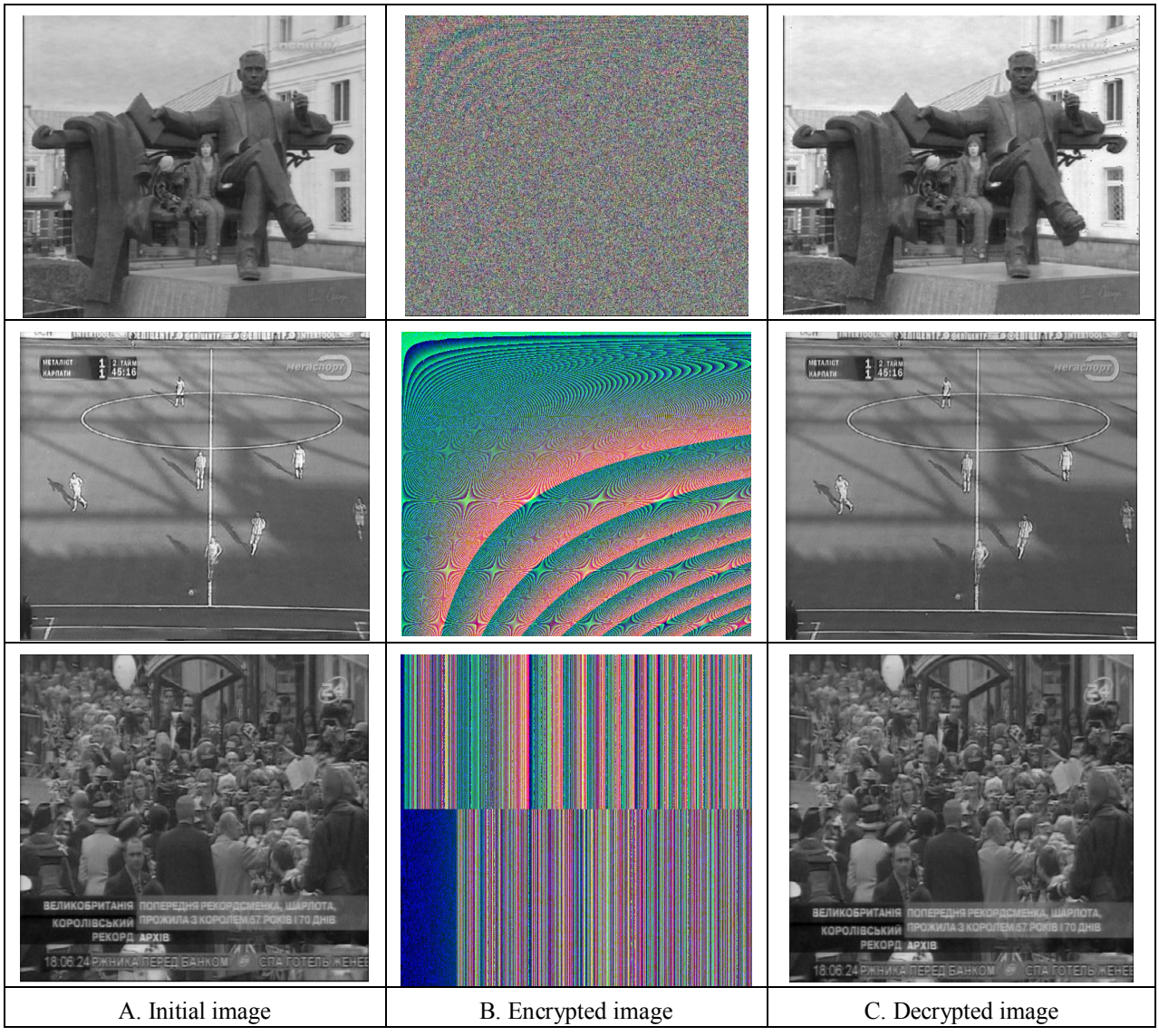
$$y = \frac{Ax^n - B}{Cx^n - D}, \quad (1)$$

here $n > 0$ is a simple number. The expression (1) display moves the dots $x = \sqrt[n]{\frac{D}{C}}$ to the point ∞. The inverse to formula (1) displaying leads to:

$$x = \sqrt[n]{\frac{Dy - B}{Cy - A}} \quad (2)$$

The inverse projective displaying (2) shifts a point $y = \frac{A}{C}$ to a point ∞, that is, it is not mutually exclusive if $A \neq D$. To obtain a reliable decrypted image, it must be taken into account during encryption and decryption.

Encryption is carried out element by element according to formula (1), where $x = c_{i,j}$, $i = \overline{1,n}$, $j = \overline{1,m}$, $A = D = Q$, $B = P - Q$, $C = e - d$. Decryption is carried out according to the inverse transformation formula (2) with the same coefficients $A = D = Q$, $B = P - Q$, $C = e - d$. The results of encryption and decryption are shown in Fig. 1 for $n = 2$.



A. Initial image	B. Encrypted image	C. Decrypted image

Fig. 1. Encryption results

РОЗДІЛ 3

Підвищення стійкості алгоритму RSA афінними перетвореннями

3.1. Використання квадратичних форм для підвищення стійкості шифрування бінарними афінними перетвореннями

3.1.1. Теоретичні відомості про квадратичні форми

Формою називається однорідний поліном від двох або більше змінних, тобто поліном, всі елементи якого мають ту саму повну степінь по сукупності змінних; наприклад, $x^2 + xy + y^2$ - форма степеня 2, $x^3 - x^2y + 3xy^2 + y^3$ - форма степеня 3. Одним з основних є питання: які цілі числа можуть бути подані за допомогою форми (тобто які цілі значення може приймати форма) при цілих значеннях змінних? Для простоти ми обмежимося лише двома змінними, тобто формами виду $f(x,y) = ax^2 + bxy + cy^2$. Число $\Delta = 4ac - b^2$ називається дискримінантом форми $f(x,y)$.

Форми з додатнім дискримінантом називаються визначеними, тому що всі значення, набуті формою $f(x,y)$ у цьому випадку, мають той же знак, що й a. При додатньому a форма $f(x,y)$ завжди визначена і називається додатньо визначеною. Форми з від'ємним дискримінантом називаються невизначеними, тому що $f(x,y)$ приймає як додатні, так і від'ємні значення.

Якщо в $f(x,y)$ зробити заміну змінних $x = Au + Bv$, $y = Cu + Dv$, де A, B, C, D - цілі числа, що задовольняють умові $AD - BC = \pm 1$, то одержимо нову форму $g(u,v)$. Тому що будь-якій парі цілих чисел x , y відповідає пара цілих чисел u і v, то кожне ціле число, подане формою f, подається формою g, і навпаки. В такому випадку говорять, що f і g еквівалентні. Всі форми, еквівалентні даній, утворюють клас еквівалентності; число таких класів для

Fig. 2. The initial image

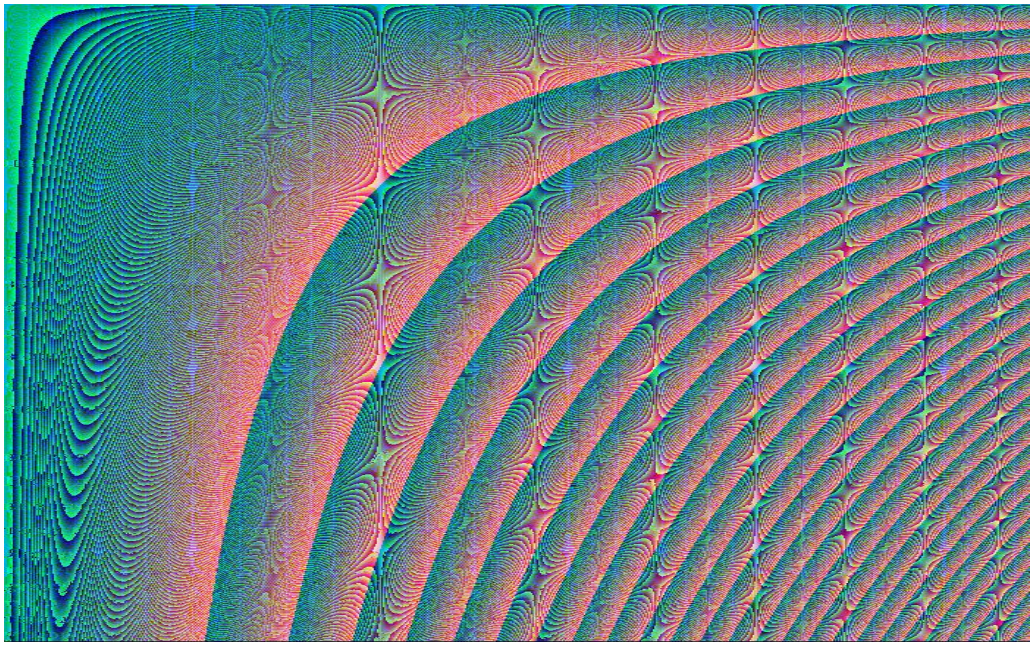


Fig.3. The encrypted image

РОЗДІЛ 3

Підвищення стійкості алгоритму RSA афінними перетвореннями

3.1. Використання квадратичних форм для підвищення стійкості шифрування бінарними афінними перетвореннями

3.1.1. Теоретичні відомості про квадратичні форми

Формою називається однорідний поліном від двох або більше змінних, тобто поліном, всі елементи якого мають ту саму повну степінь по сукупності змінних; наприклад, $x^2 + xy + y^2$ - форма степеня 2, $x^3 - x^2y + 3xy^2 + y^3$ - форма степеня 3. Одним з основних є питання: які цілі числа можуть бути подані за допомогою форми (тобто які цілі значення може приймати форма) при цілих значеннях змінних? Для простоти ми обмежимося лише двома змінними, тобто формами виду $f(x,y) = ax^2 + bxy + cy^2$. Число $\Delta = 4ac - b^2$ називається дискримінантом форми $f(x,y)$.

Форми з додатнім дискримінантом називаються визначеними, тому що всі значення, набуті формою $f(x,y)$ у цьому випадку, мають той же знак, що й a. При додатньому a форма $f(x,y)$ завжди визначена і називається додатньо визначеною. Форми з від'ємним дискримінантом називаються невизначеними, тому що $f(x,y)$ приймає як додатні, так і від'ємні значення.

Якщо в $f(x,y)$ зробити заміну змінних $x = Au + Bv$, $y = Cu + Dv$, де A, B, C, D - цілі числа, що задовольняють умові $AD - BC = \pm 1$, то одержимо нову форму $g(u,v)$. Тому що будь-якій парі цілих чисел x , y відповідає пара цілих чисел u і v, то кожне ціле число, подане формою f, подається формою g, і навпаки. В такому випадку говорять, що f і g еквівалентні. Всі форми, еквівалентні даній, утворюють клас еквівалентності; число таких класів для

Fig.4. The decrypted image

The proposed method can also encrypt textual information that was previously converted to a graphic format. The results of such encryption and decryption using the mentioned method are shown for $n = 2$ in Figs. 2-3.

From a visual comparison of the encrypted images, it can be seen that the encryption of the image matrix at $n = 2$ is different. There are no contours in both encrypted images.

The proposed modifications apply to any type of image, but the greatest benefits are achieved in the case of images with well-defined contours. This algorithm can be recommended while transmitting the coded graphic images. Also, the input and decoded images are slightly different.

That is, the use of the proposed algorithm does not degrade image quality. But in the situation of the existence of certain quality requirements of the input and decoded images and quality criteria, a certain number of attempts becomes necessary to select such simple numbers P and Q as well as numbers e and d in the congruence $ed \equiv 1 \pmod{\varphi(N)}$, $N = P * Q$ aiming the achievement of the high-mentioned criteria and requirements.

5. Conclusions

Using the RSA algorithm, based on numerical experiments with various monochrome images during encryption and decryption, it is established that the proposed modification has a certain advantage; it enhances the cryptographic stability of the RSA algorithm. The described modification is powerful for color images without any reservations. However, regardless of the image type, the size of the encrypted image also increases in proportion to the size of the input image.

6. Acknowledgment

The authors express their gratitude to the Staff of the Institute of Computer Technologies, Automation, and Metrology of Lviv Polytechnic National University.

7. Conflict of interest

The authors state that there are no mutual financial conflicts regarding the current paper.

References

[1] B. Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C*, Moscow: Triumf, 2003 https://www.amazon.com/Applied-Cryptography-Protocols-Algorithms-Source/dp

[2] B. Jane. *Digital Image Processing*. Springer–Verlag Berlin Heidelberg, 2005, https://www.amazon.com/Digital-Image-Processing-Algorithms-Applications/dp/3540592989

[3] R.C. Gonzales and R.E. Woods. *Digital image processing*. Prentice Hall, Upper Saddle River, NJ, 2nd ed.,2002. https://www.amazon.com/Digital-Image-Processing-Algorithms-Applications/dp

[4] Tsmots I., Riznyk O., Rabyk V., Kynash Y., Kustra N., Logoida M. (2020) Implementation of FPGA-Based Barker's-Like Codes. In: Lytvynenko V., Babichev S., Wójcik W., Vynokurova O., Vyshemyrskaya S., Radetskaya S. (eds) "*Lecture Notes in Computational Intelligence and Decision Making*". ISDMCI 2019. Advances in Intelligent Systems and Computing, vol 1020. Springer, Cham. doi: 10.1007/978-3-030-26474-1_15.

[5] Rafael C. Gonzalez, Richard E. Woods, "*Digital Image Processing*", published by Prentice Hall Upper Saddle River, New Jersey, 07456, http://sdeuoc.ac.in /sites/default /files/sde_videos.pdf

[6] A. Kovalchuk, I. Izonin, C. Strauss, M. Podavalkina, N. Lotoshynska, N. Kustra. "*Image encryption and decryption schemes using linear and quadratic fractal algorithms and their systems*", CEUR Workshop Proceedings, Vol. 2533, 2019, pp. 139-150. https://doi.org/10.23939/istcmtm2020.04.025

[7] A. Kovalchuk, I. Izonin, Gregush Ml, M., N. Lotoshyiiska, "*An approach towards image encryption and decryption using quaternary fractional-linear operations*", Procedia Computer Science, Vol. 160, 2019, pp. 491-496. Conference Paper (Open Access), DOI > 10.1016 /j.procs. 2019.11.059.

[8] B. Girod "*The information theoretical significance of spatial and temporal masking in video signals*", Proc. of the SPIE Symposium on Electronic Imaging.1989.–Vol. 1077.–P.178–187, https://typeset.io/papers/the-information-theoretical-significance-of-spatial-and-2bas6i0mgw.

[9] Majid Rabbani, Rajan Joshi. "*An overview of the JPEG2000 still image compression standard*", Eastman Kodak Company, Rochester, NY 14650, USA, Signal Processing: Image Communication. – 2002. – Vol. 17. – P. 3–48, https://scirp.org/reference/referencespapers.aspx?referenceid=727652

[10] S. X. Liao and M. Pawlak *On image analysis by moments*, IEEE Transaction on Pattern Analysis and Machine Intelligence. – 1996. – 18, No 3. – P. 254–266, https://ieeexplore.ieee.org/document/485554

[11] E.M. Haacke, R.W. Brown, M.R. Thompson and R. Venkatesan. *Magnetic Resonance Imagin: Physical Principles and Sequence Design*. John Wiley & Sons, New York, 1999, https://www.wiley.com/ensg/Magnetic+Resonance+Imaging:+Physical+Principles+and+Sequence+Design,+2nd+Edition-p-9780471720850

[12] J.T. Kajiya. The rendering equation. *Computer Graphics,* 20: 143-150, 1986, https://dl.acm.org/doi/10.1145/15886.15902

[13] M. Sarfraz. *Introductory Chapter: On Digital Image Processing*. 2020, DOI: 10.5772 intechopen.92060, https://www.intechopen.com/chapters/71817

[14] Ehsan Samei, Donald J Peck, Projection X□ray Imaging, Hendee's Physics of Medical Imaging, 10.1002 9781118671016, (217-242), (2019), https://onlinelibrary.wiley.com/doi/10.1002/9781118671016.ch6

[15] Michael Vollmer, Klaus□Peter Mollmann, Fundamentals of Infrared Thermal Imaging, Infrared Thermal Imaging, 10.1002 9783527693306, (1-106), (2017), https://www.wiley.com/enus/Infrared+Thermal+Imaging:+Fundamentals,+Research+and+Applications,+2nd+Edition-p-9783527413515

[16] Usmonov, B., Evsutin, O., Iskhakov, A., Shelupanov, A., Iskhakova, A., & Meshcheryakov, R. (2017, November). The cybersecurity in development of IoT embedded technologies. In 2017 International Conference on Information Science and Communications Technologies (ICISCT) IEEE, pp. 1-4. DOI: 10.1109/ICISCT.2017.8188589.

[17] Wagh, D. P., Fadewar, H. S., & Shinde, G. N. (2020). Biometric Finger Vein Recognition Methods for Authentication. In Computing in Engineering and Technology, pp. 45-53. DOI: 10.1007/978-981-32-9515-5_5.