Nashat Al-Bdour, Ayman M Mansour

Tafila Technical University, Jordan

doi:10.15199/48.2021.06.02

Optimal Steganographic Method Based on Image Encryption

Abstract. *The paper investigates an image encryption method for the implementation of steganographic information protection. This paper aims to increase the volume of a secret message with fixed sized image. The proposed system represents an image in the form of a binary code. Each pixel code consists of 24 bits, which encode blue, green and red colors. The resulting image code is encrypted using a key set of encrypt codes generated by a pseudo-random number generator. The generation is based on cellular automata with active cells. As a result, the best bits in the color bytes of each pixel have been identified. The method provides a high degree of encryption due to the fact that, in addition to encrypting the selected bits of the pixel codes, the codes are changed due to the introduction of the bits of the secret message. The bits of the secret message have a random order since the secret message is determined by its internal content. Each new message is different from other messages and is additionally encrypted. This makes it possible to use several encrypt keys in conceal a message in an image.*

Streszczenie. *W artykule omówiono metodę szyfrowania obrazu w celu realizacji steganograficznej ochrony informacji. Ten artykuł ma na celu zwiększenie objętości tajnej wiadomości z obrazem o stałym rozmiarze. Proponowany system przedstawia obraz w postaci kodu binarnego. Każdy kod piksela składa się z 24 bitów, które kodują kolory niebieski, zielony i czerwony. Wynikowy kod obrazu jest szyfrowany przy użyciu zestawu kluczy szyfrujących kodów generowanych przez generator liczb pseudolosowych. Generacja oparta jest na automatach komórkowych z aktywnymi komórkami. W rezultacie zidentyfikowano najlepsze bity w bajtach koloru każdego piksela. Metoda zapewnia wysoki stopień szyfrowania dzięki temu, że oprócz szyfrowania wybranych bitów kodów pikselowych, kody ulegają zmianie w wyniku wprowadzenia bitów tajnej wiadomości. (**Optymalna metoda steganograficzna oparta na szyfrowaniu obrazu**)*

Keywords: Steganography, Image Encryption, Concealed Message, pseudo-random number generator, Cellular Automata.
Słowa kluczowe: steganografia, szyfrowanie, generator liczb pseudolosowych.

Introduction

Currently, events that are taking place are increasingly presented in the form of images, which are then transmitted as information to the recipient. This is due to the fact that a person perceives graphic pictures better and faster. Also, a large amount of information is contained in the image, which must be transmitted using various communication channels. However, there is a large number of images that require confidentiality. These images require high protection against unauthorized access by unauthorized users during their transmission over digital channels. This is especially true for the transmission of secret images over the Internet. In this regard, there is a need for a secure way to exchange confidential images. To implement this method, the most acceptable is image encryption, that gains high popularity. Nowadays, a large number of encryption methods have been developed, which are widely covered in various publications. [1-5].

For steganographic information protection, one of the main tasks is to transfer the maximum amount of information using a container of a fixed size. This can be done by creating a container that allows embedding of a large amount of information. If images are used as containers, then a search is made for bits in which the information bits are concealed. This approach solves the problem. If the image is not prepared in advance, then a method is used to concealed the bits independent of the structure of the container image. Such methods usually use bits that are inherent in its implementation and -are used for different containers.

In this paper, a new algorithm for selecting the best pixels of the image in a fixed container is developed. This selection allows embedding a secret message in the selected pixels a container. Among all the image encryption methods, the most acceptable method is based on the representation of the image as a sequence of bits. The encryption of this sequence uses a key sequence of bits [3, 5]. In this method, the encryption depends on the pseudo-random number generator (PRNG) method. This method forms a unique key bit sequence. One of the most common used encryption methods are Fourier Transform [6 - 8] and the Wavelet Transform [9]. However, such methods have problems when the used images is digitalized.

There is also a well-known method that uses scrambling of rows and columns in order to encrypt an image [10]. The used images are processed by XOR-function to obtain encrypted images. This method can cause confusion when choosing rows and columns, which can lead to false results.

Recently, the number of publications using chaos systems is increased [5, 11-14]. However, such methods are not secure because of the most common used operations.

2D and 3D maps are often used to encrypt the image, which give an effective result [15-19]. Such maps use predefined shapes. Many publications image encryption by DNA [20, 21]. This method has the advantage of difficult to detect the encrypted images. There are many more methods, such as Rubik's cube transformation [22], elliptic curves [23], cellular automata [3, 24], neural networks [25], etc. All described methods that are characterized by complex algorithms have long computation time. However, a completely secure method with reduced computational time has not yet been proposed. Especially in present of new hacking methods to encrypt images.

Choosing a Key set of encrypt codes for Image Encryption

As mentioned earlier, the simplest and most reliable way to encode images is to rely on binary codes for every pixel in the image. In this case, it is necessary that the key bit sequence has the properties of a pseudo-random.

To form the key range, PRNGs are used, which have a number of requirements for their quality [26]. The main requirement is the impossibility of repetition under unknown initial conditions and states. Most often, images are encrypted with mathematical PRNGs [26]. However, such PRNGs do not provide high protection. It will be easily detected. Linear Feedback Shift Register (LSFR) generators also do not provide high quality encryption [26]. High quality is shown by PRNGs implemented on the basis of cellular automata (CA) [26- 28].The work proposes to use PRNG based on CA with active cells [26-28]. Recent studies have shown high quality PRNGs is based on CA with three active cells [28]. In such PRNGs, the initial two active cells form the third active cell during functioning. All three cells form bit sequences that can be used as key sequences.

Studies carried out in works [28, 29] have shown that the bit sequences formed by the third active cell, as well as common sequences as the bitwise XOR function of the bit sequences of active cells, are of high quality. Graphic and static tests showed high quality of such PRNGs [28, 29].
Thus, this work uses key sequences formed by the third active cell. The logical function of transitions for the first active cell selects the active cell at the next odd time step as the main zero cell in the neighborhood of the active cell.

The logical transition function for the second active cell selects the active cell at the next even step as the main unit cell in the neighborhood of the active cell. The logical function of transitions for the third active cell selects the active cell at the next time step using the binary code of the first two generated cells in the neighborhood of the active cell. Bit sequences is formed and it consisted of 240000 bits or more.To encrypt the text that is concealed in encrypted images, PRNGs are used. The PRNGs are implemented based on hybrid CAs with heterogeneous cells. These PRNGs are well described in [26, 28, 29]. They have shown a high quality of functioning.

Image encryption method

The image encryption method uses a set of codes that encode the color and brightness of each pixel. The pixel code consists of three parts (3 bytes). The first high-order byte of the code presents the blue color and its shades; the second and third bytes of the code presents the green and red colors and their shades, respectively. The general code of an image is represented as a bit sequence, which consists of 24 bit for each pixel. This forms the image matrix which is ordered based on the image contents from left to right and from top to bottom.

If the image is 100×100 pixels, then the constructed bit sequence has 240000 bits. In order to encrypt the image, a key set of encrypt codes of the same length is used. Such a key set of codes is generated using the PRNG described in previous section. The block diagram of developed methodology is shown in Fig.1.

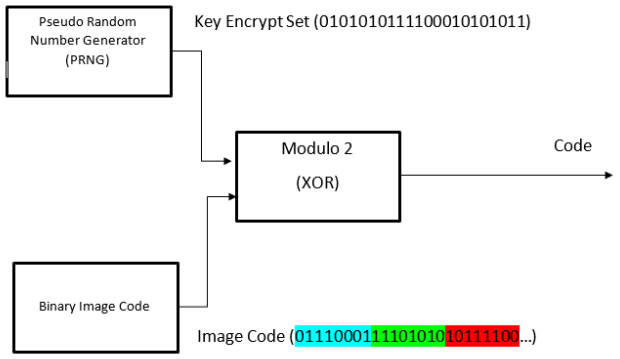

Fig.1. The developed methodology.

At the output of PRNG, a binary code with pseudo-random properties is formed. This code is hard to predict (hack). An image is composed of a matrix of pixels. The color and luminance of each pixel is supplied with a 24 bit binary code. The first 8 bits are encoded blue, 8 bits of the second encoded green, the third 8-bit coded red color. If all the codes of pixels lined up in a straight line, the resulted code for this image is for instance.

01101010 10111010 10101010 00010110 10101010 10101010 10101010 10111101 000000 01…

For example, if the PRNG generated the following bit sequence (01000111010101010110100010101101) and the image consists of initial image code,

01101010 10111010 10101010 00010110

then the code of the encrypted image will be after the execution of the XOR function.

00101101 11101111 11000010 10111011

From this example, the codes of the first pixel are different after encryption. These codes are underlined. Likewise, the codes for all pixels will be changed after the key set of encrypt codes is applied. If the most three significant bits for each color is used, then only the most significant two will be encrypted. In this example, the resulted sequence is:

011 01010 **111** 11010 **110** 01010 **101** 10110

Encrypted bits are in bold. All other bits are the same as in the original image.

With the help of the generated set of encrypt codes, it is possible to completely encrypt the entire bit sequence describing the image. Fig. 2 shows an initial image with a size of 100 × 100 pixels and the same image with the 50 top rows of the matrix encrypted using the key bit sequence formed by the third active cell.

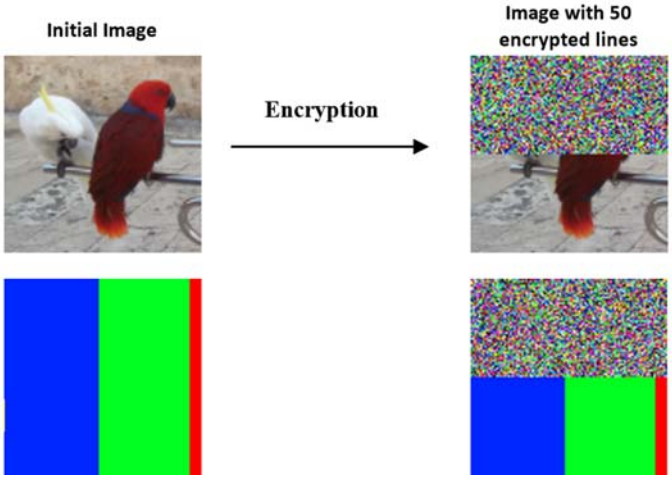

Fig.2. An example of encryption of the image code forming the first top 50 rows of the matrix.

This example shows high quality distribution of colors in the resulted image. This distribution makes it impossible to determine the original image. Fig. 3 shows distribution histograms of pixel codes of an encrypted images. Histograms are shown for each color. 5000 number are used for a 100x50 part of an image. Histograms show a good quality distribution for numbers between 5000 and 15000. This proves that the developed approach is suitable for encrypting images.

Experiments and Results

To conceal a text within image pixels, it is necessary to select a group of bits in the code to be used in encryption. Changing the states of selected bits should not affect the change of the concealed text in the remaining pixels. In Fig. 4, shows an example of image encryption based on the red bytes of each pixel. Top 50 lines of an image matrix are only encrypted.

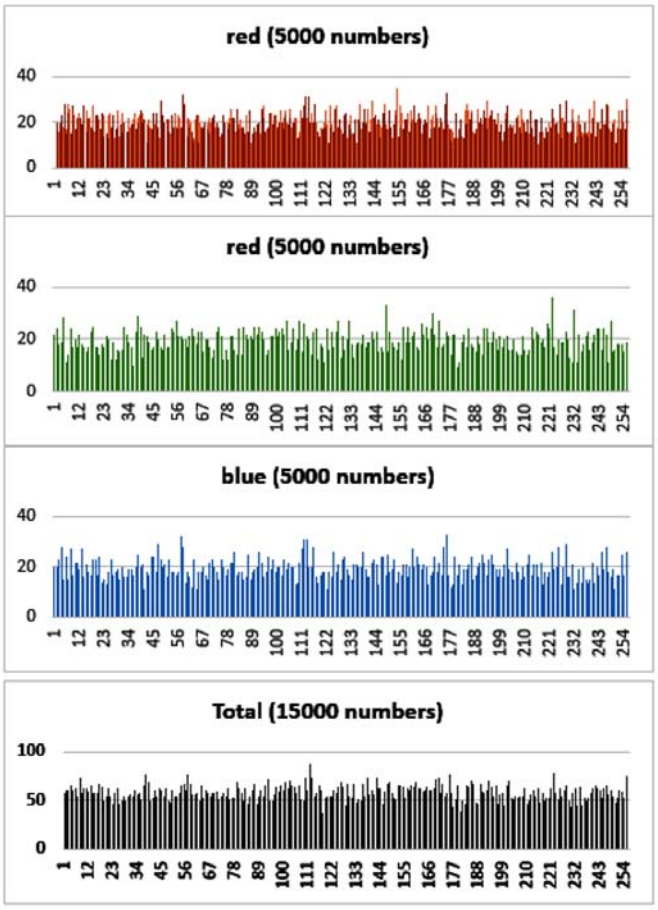

Fig.3. Distribution Histograms of pixel code for an encrypted image.

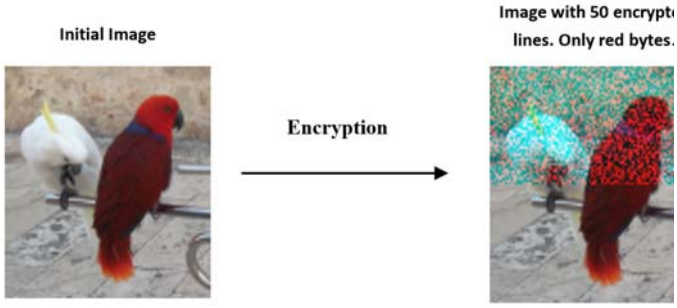

Fig.4. An example of image encryption based on the red bytes of each pixel.

The example shown in Fig. 4 is not reliable encryption. It is easily notable because the changes in brightness is clear. Weak encryption is resulted from using a poor-quality key set of encrypt codes. Fig. 5 shows the top 50 rows of an image are encrypted using a key set of encrypt code with values equals ones

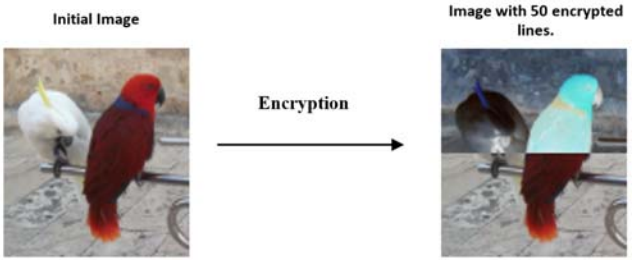

Fig.5. An example of image encryption based on all bytes of the code of each pixel.

The two and three most significant bits are the best pixels for reliable image encryption. It is shown in Fig. 6.

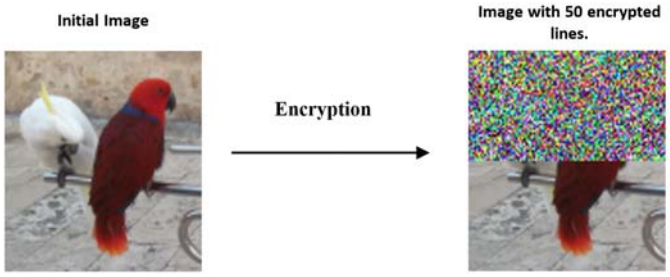

Fig.6. An example of image encryption using the two most significant bits of each color pixel.

This approach provides high quality encryption and preserves the six least significant bits of the color bytes. Bits of text can be concealed in these bytes with or without additional encryption. The results of encryption with concealed text is shown in Fig. 7.

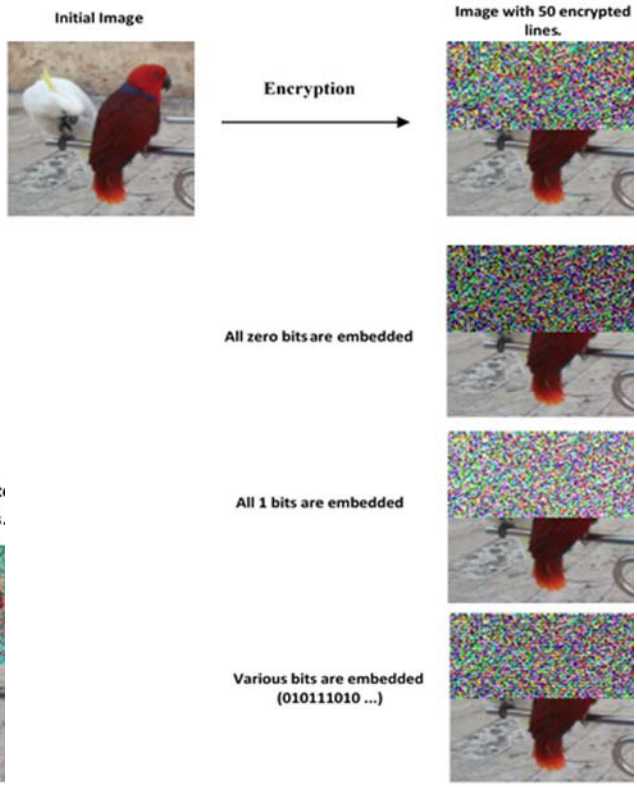

Fig.7. The results of encryption of the two most significant bits of the color bytes with concealed text.

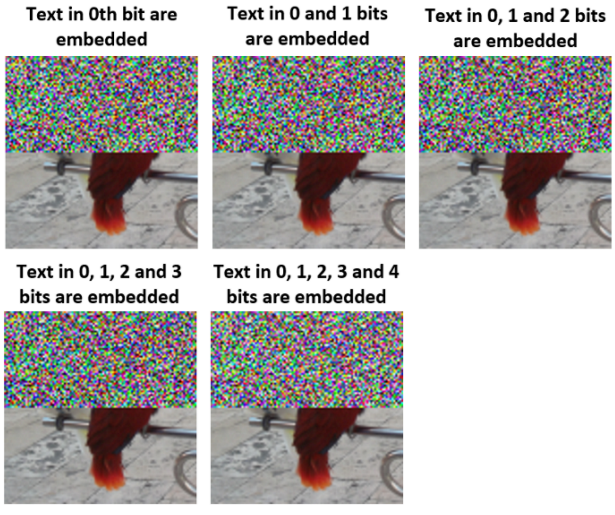

Fig.8. The results of encrypting most significant bits of the color bytes of an image.

As shown in Fig. 8 there are differences in color distribution. However, the encryption quality remains high. More reliable is encryption at the levels of the three most significant bits of each color byte. At the same time, the amount of concealed text is reduced. Examples of encrypting one or more of the most significant bits of each color byte of a pixel are shown in Fig. 7.

Fig. 9 and Fig. 10 shows another example of encrypted images.

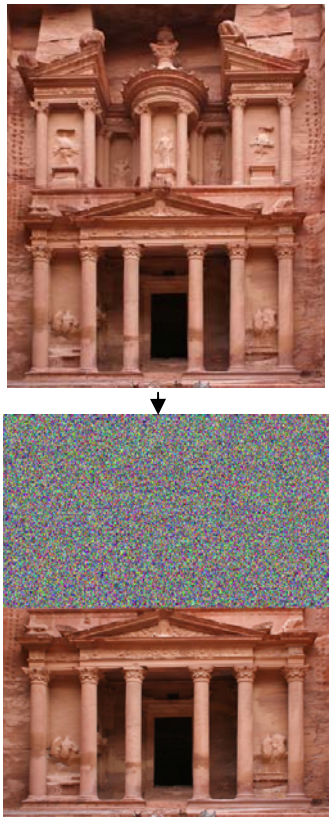

Fig.9. Encrypted Petra image.

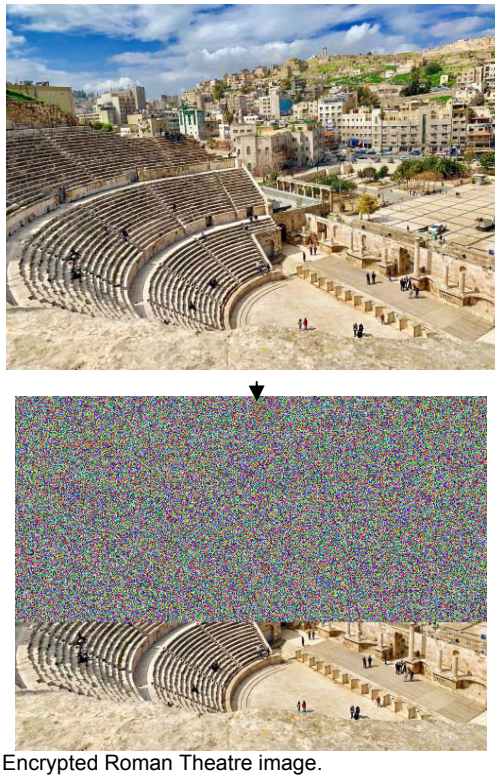

Fig.10. Encrypted Roman Theatre image.

Distribution Histograms of the numbers used in encrypting the most three significant bits of each color byte of the pixel code is shown Fig 11.

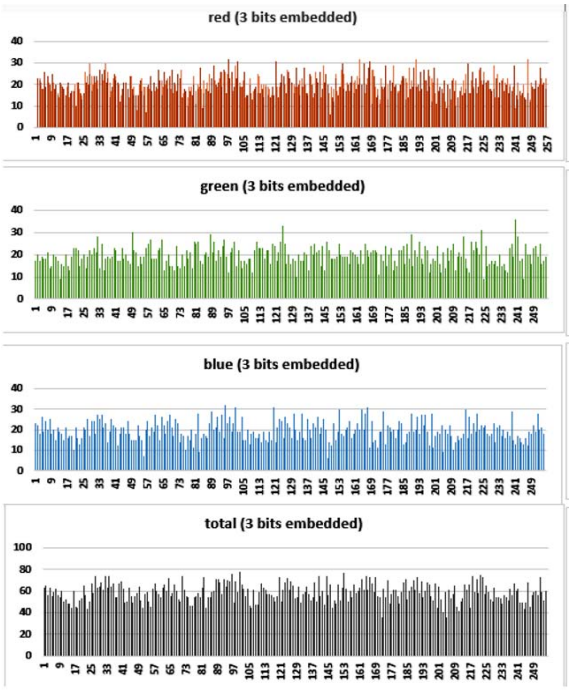

Fig.11. Distribution Histograms of the numbers used in encrypting the most three significant bits of each color byte of the pixel code.

Fig. 11 does not include distribution histograms of the numbers for the 1st and 2nd least significant bits. Using this approach, 12 bits of a secret message can be concealed in the code of one pixel. The resulting histograms indicate high quality encrypted images.

Conclusion

This paper considers the application of the PRNG-based image encryption method built based on a cellular automata with three active cells. Such PRNGs give high quality pseudo-random bit sequences. With this encryption, the best bits in the image pixel code were determined, which are then encrypted. These bits are the three most significant bits in each color byte of the pixel code. Thus, in each pixel code, only nine bits are encrypted, and a text can be concealed in the remaining bits. Based on the developed approach, it is possible, along with image encryption, to conceal a large amount of information. The developed method can be used to encrypt certain areas of the image (faces, numbers, etc.).

***Authors**: Dr. Nashat Al-Bdour, Department of Communication, Electronics and Computer Engineering, Faculty of Engineering, Tafila Technical University, Tafila 66110, Jordan ; Dr. Ayman M. Mansour, Department of Communication, Electronics and Computer Engineering, Faculty of Engineering, Tafila Technical University, Tafila 66110, Jordan, Email: mansour@ttu.edu.jo*

REFERENCES

[1] Liu, Y., Wang, J., Fan, J. H. & Gong, L. H. Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences. Multimed. Tools Appl. 75, 4363–4382 (2016).

[2] Nadzeya SHUTKO, Pavel URBANOVICH, Pawel ZUKOWSKA, "method of syntactic text steganography based on modification of the document-container aprosh",Przegląd Elektrotechniczny ,V(94),num(06),2018

[3] Ewa ŚWIERCZ, "Image encryption algorithms based on wavelet decomposition and encryption of compressed data in wavelet domain", Przegląd Elektrotechniczny ,V(94),num(02),2018.
[4] Manish Kumar, Rachid Ait Maalem Lahcen, R. N. Mohapatra, Chandan Alwala, and Surya Vamsi Krishna Kurella. Review of Image Encryption Techniques. - Journal of Computer Engineering.- Volume 22, Issue 1, Ser. I (Jan - Feb 2020), PP 31-37
[5] Lazaros Moysis, Aleksandra Tutueva, Christos Volos and Denis Butusov. A Chaos Based Pseudo-Random Bit Generator Using Multiple Digits Comparison.- CHAOS Theory and Applications. (2020). – V.2, N2, P. 58-68
[6] Juan M. Vilardy, Jorge E. Calderon, Cesar O. Torres, Lorenzo. Mattos, "Digital Images Phase Encryption using Fractional Fourier Transform", CERMA conference, Pages: 15–18, 2006.
[7] H Yoshimura, R Iwai," New encryption method of 2D image by use of the fractional Fourier transform", IEEE Conference on Signal Processing, Pages: 2182 – 2184, 2008
[8] Nadya SHUTKO,"The use of aprosh and kerning in text steganography",Przegląd-Elektrotechniczn, V(92), num(10), 2016.
[9] Xianye, Xiangfeng, Xiulun, Yurong, Yongkai Yin, Xiang Peng, Wenqi, Guoyan, Hongyi, "Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme", Volume 102, Pages 106–111, March 2018.
[10] Xing-Yuan, Sheng-Xian, Ying-Qian, "Novel image encryption algorithm based on cycle shift and chaotic system", Optics and Lasers in Engineering Volume 68, Pages 126–134, 2015.
[11] Chong Fu, Zhou-Feng Chen, Wei Zhao, Hui-yan Jiang, "A New Fast Color Image Encryption Scheme Using Chen Chaotic System", 18th IEEE conference, Pages: 121–126, 2017.
[12] Wenting Yuan, Xueiln Yang, Wei Guo, Weisheng Hu, "A double domain image encryption using hyperchaos", 19th ICTON conference, Pages: 1–4, 2017.
[13] Huang, X.; Ye, G. An efficient self-adaptive model for chaotic image encryption algorithm. Commun. Nonlinear Sci. Numer. Simul. 2014, 19, 4094–4104.
[14] Liu, H.; Wang, X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt. Commun. 2011, 284, 3895–3903.
[15] Mao, Y.; Chen, G.; Lian, S. A novel fast image encryption scheme based on 3D chaotic baker maps. Int. J. Bifurcation Chaos 2004, 14, 3613–3624.
[16] Wu, Y. Image encryption using the two-dimensional logistic chaotic map. J.Electron. Imag. 2012, 21, 013014.
[17] Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals 2004, 21, 749–761.
[18] Lian, S.; Sun, J.; Wang, Z. A block cipher based on a suitable use of the chaotic standard map. Chaos Solitons Fractals 2005, 26, 117–129.
[19] Ping, P.; Xu, F.; Mao, Y.; Wang, Z. Designing permutation substitution image encryption networks with Henon map. Neurocomputing 2018, 283, 53–63.
[20] Liu, H.; Wang, X.; Kadir, A. Image encryption using DNA complementary rule and chaotic maps. Appl. Soft Comput. 2012, 12, 1457–1466.
[21] K.R.Radhika, M.K.Nalini, " Biometric Image Encryption using DNA sequences and Chaotic Systems", ICRAECT conference, Pages: 164–168, 2017.
[22] Govinda.K, Prasanna.S, "A Generic Image Cryptography Based on Rubik's Cube", ICSNS conference, Pages: 1–4, 2015.
[23] Shahryar Toughi, Mohammad H. Fathi, Yoones A. Sekhavat, " An image encryption scheme based on elliptic curve pseudo-random and Advanced Encryption System", Volume 141, December 2017, Pages 217–227.
[24] Chai, X.; Zheng, X.; Gan, Z.; Han, D.; Chen, Y. An image encryption algorithm based on chaotic system and compressive sensing. Signal Process. 2018, 148, 124–144
[25] S H Kamali, R Shakerian, M Hedayati, M Rahmani, "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", ICEIE Conference, Year: 2010, Volume:1 Pages: 141–145.
[26] Stepan Bilan. Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities.- (2017).- IGI Global, USA.- P. 301.
[27] Bilan S., Bilan M., Motornyuk R., Bilan A., Bilan S. (2018) Designing of the Pseudorandom Number Generators on the Basis of Two-Dimensional Cellular Automata. In: Ntalianis K., Croitoru A. (eds) Applied Physics, System Science and Computers. APSAC 2017. Lecture Notes in Electrical Engineering, vol 428. Springer
[28] Stepan Bilan, Mykola Bilan, Sergii Bilan. Research of the method of pseudo-random number generation based on asynchronous cellular automata with several active cells.- MATEC Web of Conferences, - Vol. 125,- 02018 (2017), - P. 1-6.
[29] Stepan Bilan, Mykola Bilan, Sergii Bilan. Research of the Influence of the local Transition Function on the Formation of a New Active Cell in the PRNG Based on ACA.- WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS. - Volume 14, 2017. – pp. 167-173.