AN IMAGE ENCRYPTION SCHEME UTILIZING HARPER'S MAP

Jakub ORAVEC, Ján TURÁN, Ľuboš OVSENÍK
Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics,
Technical University of Košice, Park Komenského 13, 042 00 Košice, Slovak Republic, Tel.: +421 55 602 4277,
E-mail: jakub.oravec@tuke.sk

ABSTRACT

This paper deals with an image encryption scheme, which could be used for improving security of steganographic algorithms. Higher level of security is reached by masking information contained in secret data by their encryption. Therefore in the worst case, the attacks would yield encrypted version of secret data in the worst case. After brief description of reasons for usage and drawbacks of already used solutions, the paper presents one of chaotic maps as possible tool for encryption algorithms construction. Properties of this map and proposed algorithms are discussed in detail. The effects caused by application of described encryption scheme are illustrated by performed experiments.

Keywords: *chaotic map, differential attack, Harper's map, image encryption, statistical attack*

1. INTRODUCTION

Despite easier means of steganalysis, algorithms of substitution steganography are still widely used. One of their biggest advantages is their simplicity. For ensuring that the secret message, which is being transmitted would be safe from possible attacks, it could be encrypted prior to its embedding [1]. However, many conventional ciphers (such as Advanced Encryption Standard – AES) were designed for input data in form of text strings. The properties of images, which are used in the majority of steganographic techniques are quite different. This fact can result in not sufficient performance of ciphers applied on an image.

Effects displayed on Fig. 1 are caused by the design of AES and used mode of operation. Used original image had resolution of 256x256 pixels and it was grayscale. Because AES is a block cipher, images have to be split into set of blocks. Block size of 128 bits means 16 bytes are encrypted at the same time, which can be represented as a block of 4x4 pixels. Used mode of operation determines how will be the values in blocks treated during the encryption. The simplest mode is called *Electronic CodeBook* (ECB). ECB uses only one value from processed image block for producing one encrypted value. This approach results in mapping of the input values set into set of encrypted values, which makes frequency analysis possible [2].

image before encryption image after encryption

Fig. 1 Image encrypted in ECB mode with key *thisisasecretkey*

On the other hand, stream ciphers suffer mainly from redundancy of image pixels. Similar intensities of adjacent pixels cause small differences between produced encrypted values. Hence, the rearrangement of image pixels before usage of a stream cipher can be considered as practical.

First attempts at creating ciphers based on chaos can be traced to the late 1980s [3]. In these cases, the algorithms use one of chaotic maps with behavior that is not easily predictable. Some of the chaotic maps use a parameter, which could be then used as a key in designed cipher.

Well-known architecture of chaotic ciphers was proposed by Fridrich in late 1990s [4]. In mentioned approach, encryption consists of two stages, confusion and diffusion. Confusion step is used for rearrangement of image pixels, while diffusion changes their intensities and makes attacks such as statistical and differential attack ineffective.

The rest of the paper is organized as follows: chapter II provides a brief review of related work and Harper's map, which is used for purposes of confusion and diffusion. Third chapter describes proposed algorithms. After that, performance of proposed solution, commonly used attacks and countermeasures taken by proposed solution are discussed in chapter IV. The paper ends with conclusion.

2. RELATED WORK

First encryption algorithms based on chaos utilized chaotic maps with one variable which changed its values in following iterations of the map. Later, the increasing performance of computers allowed usage of chaotic maps with more dimensions. As the digital images could be represented as matrices with two dimensions, many researchers tried to apply two dimensional chaotic maps for purpose of image encryption. However, majority of these maps have some disadvantages.

The bakers' map utilized by Fridrich in [4] requires a division of image into a set of regions. Then the pixels in these regions are shuffled. Because key is entered as set of region sizes, it is quite unpractical to remember for human user. Also the key values need to be chosen in a way that utilizes all image pixels in division to regions, so the key elements could not be arbitrary numbers from some range.

One of other frequently used two dimensional chaotic maps is Arnold's cat map. Because the equations of this map are quite simple, this map has numerous applications

in image encryption. However, drawback of the simplicity is well studied bevavior of the map [5]. This behavior includes relatively small periods of the map which could be used for extraction of data from encrypted image.

The periodicity issue is not as serious for standard map described by Chirikov in [6]. This map has one parameter which is usually set by portion of key entered by users. One of the first applications of standard map was described by Lian, Sun and Wang in [7]. Their encryption scheme uses the map for block processing during two stages of algorithm. This approach was further improved by Wong, Kwok and Law in [8], where the number of pixel shuffling rounds was reduced, but the results were still comparable. Another solution was provided by Fu et al. in [9], where the second stage uses two directions of spreading instead of one. However, the results of this proposal could not be compared with the others, as it uses different map - Chebyshev map for the changing of pixel intesities.

2.1. Harper's Map

Harper's chaotic map was firstly introduced as a model of electron movement in two-dimensional space under influence of magnetic field [10]. Harper's map can be used for design of chaotic cipher in same way like Arnold's cat map, standard or baker's map [4, 11].

The equations for Harper's map could be discretized for sets of integer pixel coordinates $x_i, y_i \in \{1, 2, ..., n\}$, where i is sequential number of iteration, n is the height and also the width of input image as (1):

$$\begin{aligned} x_{i+1} &= x_i + round(K \cdot sin\frac{2 \cdot \pi \cdot y_i}{n}) \pmod n, \\ y_{i+1} &= y_i - round(L \cdot sin\frac{2 \cdot \pi \cdot x_{i+1}}{n}) \pmod n, \end{aligned} \tag{1}$$

where *round* denotes operation of rounding to nearest integer, K and L are parameters of the map, $K, L \in \{1, 2, ..., n\}$. Effects of several iterations of Harper's map are displayed on Fig. 2. Used image has relatively small resolution (16x16 pixels), which is useful for highlighting the properties of Harper's map.

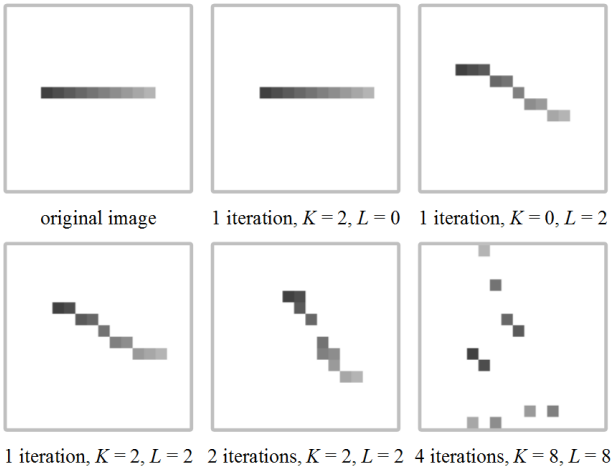

Fig. 2 Effects of Harper's map applied on image

Due to the fact that Harper's map was originally proposed for unit squares, the discretized version uses only images with square resolution (of *nxn* pixels). This can be considered as a drawback, however non-square images could be split to set of overlapping square blocks [12].

Discretized versions of chaotic maps tend to be periodic because of finite amount of possible pixel locations. The period can be calculated by construction of orbits, in case of Harper's map it depends on resolution of used image n and values of parameters K and L. The concept of orbits is further described in several sources, e. g. in [13].

Results in Table 1 show that Harper's map has relatively long period even for small values of resolution n. This fact is desirable for creating ciphers with large key space.

Table 1 Examples of Harper's map periods

nxn	K	L	period [iterations]
32	16	8	$\sim 8.888 \cdot 10^6$
64	32	32	$\sim 2.991 \cdot 10^{14}$
128	32	64	$\sim 2.883 \cdot 10^{44}$
128	64	64	$\sim 5.927 \cdot 10^{49}$

Original image can be achieved by computing set of equations, which are inverse to (1). This set is given as (2):

$$\begin{aligned} y_{i-1} &= y_i + round(L \cdot sin\frac{2 \cdot \pi \cdot x_i}{n}) \pmod n, \\ x_{i-1} &= x_i - round(K \cdot sin\frac{2 \cdot \pi \cdot y_{i-1}}{n}) \pmod n. \end{aligned} \tag{2}$$

3. PROPOSED SOLUTION

Algorithms used for encryption and decryption are similar, but steps of second mentioned operation are in reverse order [14]. Both operations are done in two stages. Encryption algorithm is described in detail in following chapters.

3.1. Confusion

Confusion is responsible for reduction of correlation between adjacent image pixels. This is done simply by calculation of new pixel coordinates with usage of Harper's map. Number of computed iterations n_{Ic} and values of parameters K_c and L_c are parts of key chosen by user.

3.2. Diffusion

Diffusion algorithm modifies intensity of rearranged pixels. The set of pixels should produce balanced histogram, so the amount of information which could be used for analysis would be minimal. Newly computed values should also be sensitive to changes made in original image which helps preventing differential attacks. This could be achieved by *chaining*, which uses previously computed values in calculations done with actual pixel intensities [15].

Steps of direct diffusion are given as Algorithm 1. All operations with bits use big–endian ordering scheme.

Algorithm 1: Diffusion algorithm

Input : grayscale image *img*, number of computed iterations n_{Id}, parameters K_d and L_d

Output: grayscale image after diffusion *dif*

1. A value v from matrix *img* is obtained.

2. Chaining is performed by adding previously computed value to v. First value of v does not use chaining. The resulting values v_c are taken as moduli of 256.

3. Value v_c is decomposed to 8 bits b_1, b_2, ..., b_8.

4. Bits b_2, b_3, b_5 and b_8 are negated. This helps to achieve some diffusion also for values like 0, or 255.

5. Two coordinates x and y are computed from the bits using (3):

$$\begin{aligned} x &= 2^3 \cdot b_2 + 2^2 \cdot b_4 + 2^1 \cdot b_6 + 2^0 \cdot b_8, \\ y &= 2^3 \cdot b_1 + 2^2 \cdot b_3 + 2^1 \cdot b_5 + 2^0 \cdot b_7. \end{aligned} \tag{3}$$

6. At this point, each pixel intensity has two coordinates x, y in matrix with 16 rows and 16 columns. Harper's map (1) with parameters n_{Id}, K_d, L_d is used for mapping the set of coordinates into a new set.

7. Coordinates from new set x' and y' are decomposed to two sets of 4 bits x'_1, x'_2, x'_3, x'_4 and y'_1, y'_2, y'_3, y'_4.

8. New value v' after diffusion is calculated from obtained bits by applying (4):

$$\begin{aligned} v' = {} & 2^7 \cdot x'_4 + 2^6 \cdot y'_4 + 2^5 \cdot x'_3 + 2^4 \cdot y'_3 + \\ & + 2^3 \cdot x'_2 + 2^2 \cdot y'_2 + 2^1 \cdot x'_1 + 2^0 \cdot y'_1. \end{aligned} \tag{4}$$

9. After calculating value of v' for every pixel in *img*, the diffusion algorithm iterates for second time. In the second iteration first value v uses last value of v' from first iteration for chaining. The values of v' after second iteration are stored in matrix *dif*.

4. EXPERIMENTAL RESULTS

4.1. Key Space and Key Sensitivity

Encryption algorithms should provide sufficiently large key space for preventing brute-force attack. The key used in proposed algorithm consists of six values – n_{Ic}, n_{Id}, K_c, L_c, K_d and L_d. Range of first two values is given by period p_n which depends on image resolution n. Range of other four values is affected directly by image resolution n. Therefore the size of key space num_k can be computed as (5):

$$num_k = p_n^2 \cdot n^4, \tag{5}$$

where p_n is period for chosen value of n, K_c, L_c, K_d and L_d.

For original image from Fig. 3 (with n = 128), the size of key space num_k is approx. $5.984 \cdot 10^{106}$ which could be considered as sufficient against brute-force attacks.

The dependence on used keys is illustrated on Fig. 3.

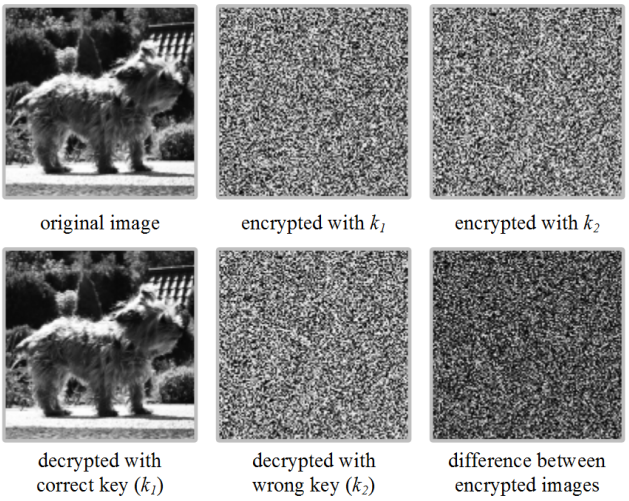

Fig. 3 Key sensitivity of proposed algorithm

Used image was grayscale with resolution of 128x128 pixels. Values of key k_1 were n_{Ic}, n_{Id} = 4 and K_c, L_c, K_d and L_d = 64. Key k_2 consisted of n_{Ic}, n_{Id} = 4, K_c, K_d, L_c = 64 and L_d = 63. Image in second row at right side shows the difference between images encrypted with k_1 and k_2.

4.2. Statistical Attack

These attacks try to get some information about image from its encrypted version. Robustness against these attacks is evaluated by shape of histograms of original and encrypted image or by scatter plots of adjacent pixel correlation.

Histograms of pair of corresponding images are shown on Fig. 4. Encryption should suppress major peaks visible in histogram of original image. This example used key k_1. Fig. 5 contains scatter plots for correlation of 1000 randomly chosen pairs of horizontally adjacent pixels. The distribution of points in plot for encrypted image should be near uniform for achieving sufficient level of diffusion.

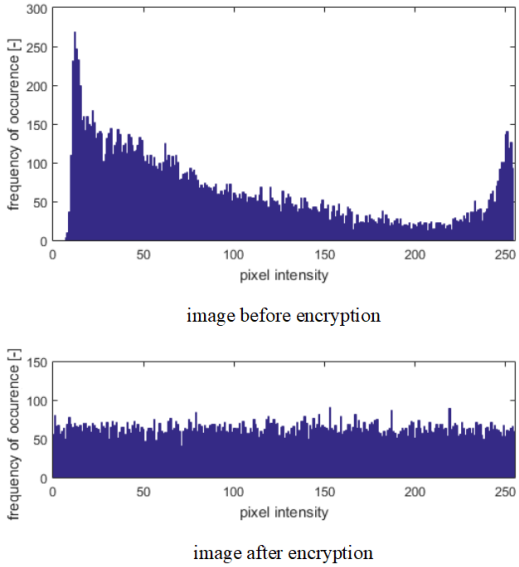

Fig. 4 Comparison of histograms

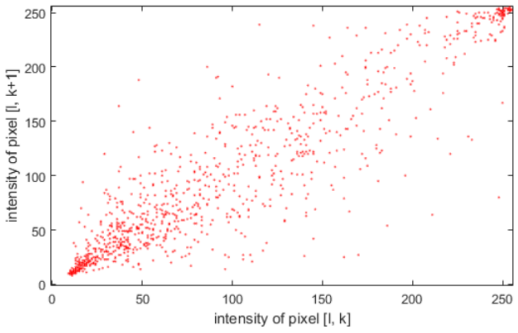

image before encryption

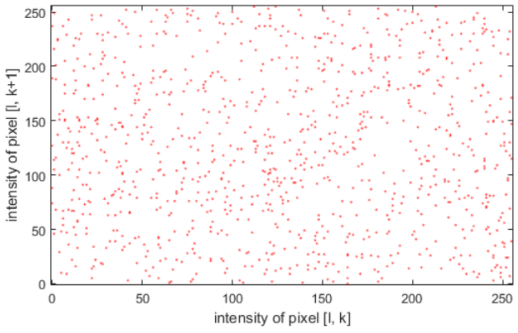

image after encryption

Fig. 5 Resulting scatter plots

4.3. Differential Attack

This kind of attack tries to determine operations done during the encryption by comparing encrypted versions of two input images with only small changes. In an ideal scenario, even one small change between two input images should create unpredictable differences between their encrypted versions. For this reason, the diffusion algorithm uses chaining. Second iteration of the algorithm is necessary for distribution of every change made in pixel intensities through all values, which are going to be calculated.

Robustness against differential attacks can be computed via two metrics [16]. These metrics use pair of images consisting of original image O and corresponding encrypted image E. First of the metrics, *Number of Pixels Changing Rate* (NPCR) simply computes the percentage of pixels with different intensities. Level of intensity change is taken into account in calculations of *Unified Average Changing Intensity* (UACI). Equations for NPCR and UACI are denoted as (6) and (7):

$$NPCR_{[\%]} = \frac{100}{h \cdot w} \cdot \sum_{l=0}^{h-1} \sum_{k=0}^{w-1} D_{l,k}, \tag{6}$$

$$UACI_{[\%]} = \frac{100}{h \cdot w} \cdot \sum_{l=0}^{h-1} \sum_{k=0}^{w-1} \frac{|O_{l,k} - E_{l,k}|}{2^L - 1}, \tag{7}$$

where l and k denote indices of rows and columns, h and w are height and width of image (in our case $h = w = n$), D is difference matrix, $D_{l,k} = 0$ if $O_{l,k} = E_{l,k}$ else $D_{l,k} = 1$; L is the color depth of image (8 bits for grayscale images).

The calculations of NPCR and UACI were repeated in 100 iterations for original image from Fig. 3 and its version encrypted with key k_1. Arithmetic means for NPCR and UACI were 99.0906 % and 33.5346 %.

5. COMPARISON WITH OTHER APPROACHES

Performance of our algorithm could be compared with results achieved by proposals that utilize standard map which is closely related to Harper's map. However some different properties of the algorithms do not allow 'direct' comparison. For instance, the size of key space for our solution depends on resolution of used image. Still, the key space produced for image with resolution of 128x128 pixels (approx. $5.984 \cdot 10^{106}$ or $2^{354.71}$) is much bigger than key spaces with sizes of 2^{256} in [7, 8] or 2^{167} in [9].

Values of NPCR and UACI were evaluated on image *lena* which was grayscale with resolution of 512x512 pixels. True color version of this image can be found in USC-SIPI image database [17]. In order to establish similar testing conditions for all proposals, our algorithm was used for the same amount of iterations as solutions given in [7,8] – it was used in six consecutive iterations of encryption with the same key ($K_c = K_d = L_c = L_d = 256$). The resulting values are shown in Table 2.

Table 2 Computed values of NPCR and UACI

approach	ref. [7]	ref. [8]	proposed
$NPCR_{[\%]}$	99.6109	99.6304	99.646
$UACI_{[\%]}$	33.4197	33.4865	33.4485

The results show that our solution reaches the best value of NPCR, while the value of UACI is between those yielded by [7] and [8]. However, the difference between values after smaller number of iterations is not so big in case of our algorithm (compare last paragraph of chapter 4.3 and Table 2 from [8] for more details).

6. CONCLUSION

This paper dealt with design of chaotic cipher based on Harper's map. The cipher uses conventional approach consisting of two steps, confusion and diffusion. Main difference of proposed technique is in the way how it treats pixel intensities in the diffusion stage. However, proposed solution has also some drawbacks, e. g. some keys from the key space could be considered as 'weak'. The algorithm for selection of suitable keys could be a topic for future work.

Properties of our algorithm were compared with those achieved by other solutions based on standard map which is closely related to Harper's map. As it was shown, the second mentioned map also shows sufficient chaotic behavior which could be used in various applications, such as in those requiring higher security of processed, stored or transmitted data [18, 19].

ACKNOWLEDGEMENT

This work was supported by following research grants: KEGA 023TUKE-4/2017, VEGA 1/0772/17 and ITMS 26220120055.

REFERENCES

[1] HAJDUK, V. – BRODA, M. – KOVÁČ, O. – LEVICKÝ, D.: Image Steganography with Using QR Code and Cryptography, *Proc. of Radioelektronika 2016*, Košice (Slovakia), 2016, pp. 350–353, ISBN 978-15-0901-673-0, DOI: 10.1109/RADIOELEK.2016.7477370.

[2] LEVICKÝ, D.: Kryptografia a bezpečnosť komunikačných sietí (in Slovak), Košice: *Elfa*, 2016, pp. 93–98, ISBN 978-80-8086-254-5.

[3] MATTHEWS, R.: On the Derivation of a 'Chaotic' Encryption Algorithm, *Cryptologia*, 1989, Vol. 8, No. 1, pp. 29–42, ISSN 0161–1194, DOI: 10.1080/0161-118991863745.

[4] FRIDRICH, J.: Symmetric Ciphers Based on Two–Dimensional Chaotic Maps, *Intl. J. of Bifurcation and Chaos*, 1998, Vol. 8, No. 6, pp. 1259–1284, ISSN 0218-1274, DOI: 10.1142/S021812749800098X.

[5] DYSON, F. J. – FALK, H.: Period of Discrete Cat Mapping, *The American Mathematical Monthly*, 1992, Vol. 99, No. 7, pp. 603–614, ISSN 0002-9890, DOI: 10.2307/2324989.

[6] CHIRIKOV, B. V.: A Universal Instability of Many-dimensional Oscillator Systems, *Physics Reports*, 1979, Vol. 52, No. 5, pp. 263–379, ISSN 0370-1573, DOI: 10.1016/0370-1573(79)90023-1.

[7] LIAN, S. – SUN, J. – WANG, Z.: A Block Cipher Based on a Suitable Use of the Chaotic Standard Map, *Chaos, Solitons and Fractals*, 2005, Vol. 26, No. 1, pp. 117–129, ISSN 0960-0779, DOI: 10.1016/j.chaos.2004.11.096.

[8] WONG, K.-W. – KWOK, B. S.-H. – LAW, W.-S.: A Fast Image Encryption Scheme Based on Chaotic Standard Map, *Physics Letters A*, 2008, Vol. 372, No. 15, pp. 2645–2652, ISSN 0375-9601, DOI: 10.1016/j.physleta.2007.12.026.

[9] FU, C. – CHEN, J.-J. – ZOU, H. et al.: A Chaos-based Digital Image Encryption Scheme with an Improved Diffusion Strategy, *Optics Express*, 2012, Vol. 20, No. 3, pp. 2363–2378, ISSN 1094-4087, DOI: 10.1364/OE.20.002363.

[10] LIMA, R. – SHEPELYANSKY, D.: Fast Delocalization in a Model of Quantum Kicked Rotator, *Physical Review Letters*, 1991, Vol. 1, No. 11, pp. 1377–1380, ISSN 0031-9007, DOI: 10.1103/PhysRevLett.67.1377.

[11] ORAVEC, J. – TURÁN, J. – OVSENÍK, Ľ.: DWT Steganography with Usage of Scrambling, *Carpatian J. of Electronic and Computer Engineering*, 2016, Vol. 9, No. 1, pp. 26–29, ISSN 1844–9689.

[12] OVSENÍK, Ľ. – KAŽIMÍROVÁ KOLESÁROVÁ, A. – TURÁN, J.: Video Surveillance Systems, *Acta Electrotechnica et Informatica*, 2010, Vol. 10, No. 4, pp. 46–53, ISSN 1335-8243.

[13] OTT, R.: Chaos in Dynamical Systems, Cambridge: *Cambridge University Press*, 1993, pp. 610, ISBN 978-05-2143-215-4.

[14] STEINGARTNER, W. – NOVITZKÁ, V.: Categorical Model of Structural Operational Semantics for Imperative Language, *J. of Information and Organizational Sciences*, 2016, Vol. 40, No. 2, pp. 203–219, ISSN 1846-3312.

[15] HARASTHY, T. – OVSENÍK, Ľ. – TURÁN, J.: Current Summary of the Practical Using of Optical Correlators, *Acta Electrotechnica et Informatica*, 2012, Vol. 12, No. 4, pp. 30–38, ISSN 1335-8243.

[16] WU, Y. – NOONAN, J. – AGAIAN, S.: NPCR and UACI Randomness Tests for Image Encryption, *J. of Selected Areas in Telecommunications*, 2011, Vol. 2, No. 4, pp. 31–38, ISSN 1925-2676.

[17] USC-SIPI *'Miscellaneous'* image database, Available at: http://sipi.usc.edu/database/, Cited 05-12-2017.

[18] KOVÁČ, O. – MIHALÍK, J.: Estimation of Spatial Coordinates of 3D Objects by Stereoscopic Scanning, *Acta Electrotechnica et Informatica*, 2014, Vol. 14, No. 3, pp. 43–48, ISSN 1335-8243.

[19] HAJDUK, V. – DZIAK, M. – VOZŇÁK, M. – LEVICKÝ, D.: Analysis of Steganographic Methods in DCT Domain, *Acta Electrotechnica et Informatica*, 2017, Vol. 17, No. 3, pp. 13–16, ISSN 1335-8243.

Received September 7, 2017, accepted January 25, 2018

BIOGRAPHIES

Jakub Oravec received his M.Sc. degree from Faculty of Electrical Engineering and Informatics, Technical University of Košice in 2015 and now he continues as PhD student. His research interests include image encryption algorithms, steganography and digital image processing.

Ján Turán received his M.Sc. and RNDr. degrees from Czech Technical University, Prague in 1974 and Charles University, Prague in 1980. He received his PhD. and DrSc. degrees from Technical University of Košice in 1983 and 1992. Since March 1979, he works at the Technical University of Košice, now as a Professor. His research interests include digital signal processing and fiber optics.

Ľuboš Ovseník received his M.Sc. and PhD. degrees from Faculty of Electrical Engineering and Informatics, Technical University of Košice in 1990 and 2002, respectively. He works at the Technical University of Košice, now as an Associate Professor. His research interests include photonics, fiber optic communication systems and sensor networks.