International Journal of Future Generation Communication and Networking
Vol. 2, No. 3, September, 2009

Improving Chaos Image Encryption Speed

Jiri Giesl
Tomas Bata University
Department of Applied Informatics
Czech Republic
jgiesl@fai.utb.cz

Ladislav Behal
Tomas Bata University
Department of Applied Informatics
Czech Republic
behal@fai.utb.cz

Karel Vlcek
Tomas Bata University
Department of Applied Informatics
Czech Republic
vlcek@fai.utb.cz

Abstract

Chaotic systems are extremely sensitive to control parameters and initial conditions. This feature is effective in the field of cryptography. In this paper we propose image encryption scheme which is based on the chaotic maps of Peter de Jong's attractor. The image is transferred into the wavelet domain and then appropriate modifications of the wavelet coefficients are done. The main purpose of application of the wavelet transformation is to reduce computation time needed for the encryption process and to reach higher or similar security of the encrypted image.

Keywords: *image encryption, strange attractor, chaotic maps, wavelet transformation*

1. Introduction

The problem of image protection has existed since the information technologies was growing up. Image is a multimedia signal providing the most information to a man. Above 80% of information is obtained from the vision apperceiving. That is the main reason of the protecting of an image against the unauthorized reading. Traditional symmetric encryption algorithm such as DES, IDEA or AES is not suitable for the image encryption because of different storage properties of an image. Position permutation and modification of the pixels belongs to basic methods of image encryption. These methods remain open for various encryption algorithms and that is the reason why the other algorithms can be used.

Chaotic systems have many properties which are suitable for the encryption process; the most important property is the sensitivity to initial conditions and control parameters. During the past decade a large number of chaos-based encryption systems have been proposed. Some of them are based on one-dimensional chaotic maps which are used for the generation of the encryption key [1,2]. The pixels of an image are then rearranged and modified according this key. Other encryption algorithms use two-dimensional maps because an image is represented as 2D matrix [3,4]. Most of those encryption schemes belong to the block ciphers; only a few of them were designed as stream ciphers [5] which can provide efficient way for the real-time image encryption. In our previous research work, we proposed an image encryption scheme [6] with high security but at the expense of the processing speed. Due to that complexity, it

cannot be applied in the real-time processes and this constraint was the main weakness of that algorithm.

The main purpose of this work is to reduce computation time by encrypting the most important information in the image. This information can be extracted by wavelet transformation. Then only the chosen wavelet coefficients are encrypted by the extended chaotic system of Peter de Jong.

The remainder of this paper is organized as follows. Section 2 provides methods used for the encryption purposes. Section 3 presents the experimental results and some security analyses. In Section 4 the performance of proposed scheme is evaluated and finally Section 5 concludes this paper.

2. Methods

2.1. Chaos and strange attractors

Chaos theory belongs to the field of deterministic dynamical systems, especially into the nonlinear dynamics. The dynamical system can be termed as chaotic, when the dynamical system is neither predictable nor repeatable and when the minimal divergence in initial conditions or parameters can cause different outcome of that system. The behaviour of the chaotic dynamical system takes place to a set of states, which is called an attractor. There are several types of an attractor – a point, a curve, a manifold or a complicated set with a fractal structure which is called strange attractor [11]. The fixed points of strange attractor are locally unstable but the system is globally stable. Strange attractors can be generated in several ways such as by quadratic (1) or trigonometric (2) maps. Control parameters a,b,c,d,e,f,g,h,i,j,k,l define behaviour of the chaotic system.

$$\begin{aligned} x_{n+1} &= a + b \cdot x_n + c \cdot x_n^{\,2} + d \cdot x_n y_n + e \cdot y_n + f \cdot y_n^{\,2} \\ y_{n+1} &= g + h \cdot x_n + i \cdot x_n^{\,2} + j \cdot x_n y_n + k \cdot y_n + l \cdot y_n^{\,2} \end{aligned} \tag{1}$$

$$\begin{aligned} x_{n+1} &= a \cdot \sin(b \cdot y_n) + c \cdot \cos(d \cdot x_n) \\ y_{n+1} &= e \cdot \sin(f \cdot y_n) + g \cdot \cos(h \cdot x_n) \end{aligned} \tag{2}$$

Necessary condition of the chaotic behaviour of the strange attractor is that the Lyapunov exponent of one map is positive. The positive exponent corresponds to the expansion; the negative exponent corresponds to the contraction of the system. Suppose that $x_{n+1} = f(x)$. The Lyapunov exponent Λ is then determined as (3).

$$\Lambda = \lim_{n=>\infty} \left(\frac{1}{n} \cdot \sum_{i=0}^{n-1} \ln \left| f'(x_i) \right| \right) \tag{3}$$

Strange attractor are markedly patterned, when they are geometrically represented. One of the strange attractors with predefined control parameters is shown in Figure 1. This attractor was found by Peter de Jong and this dynamical system is used for the encryption purposes in our algorithms.

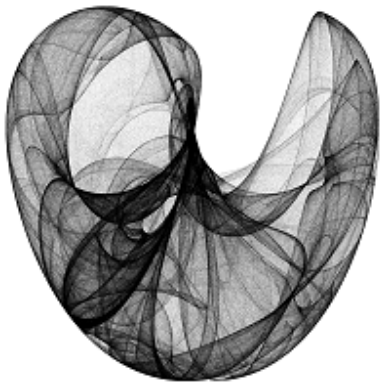


Figure 1. Example of Peter de Jong attractor

2.1. Image representation in the wavelet domain

For the extraction of information at various scales, the multi-resolution analysis is used. This analysis is provided by the fast discrete wavelet transformation. It is possible to gain specific components this way. An image must be processed by the quadrature mirror filterbanks with complementary bandwidths. There are used two different filters – scaling filter H as low-pass filter and wavelet filter G as high-pass filter. These filters are constructed as matrices in (4),

$$H = \begin{pmatrix} h_0 & h_1 & h_2 & h_3 & & & & \\ & & \cdot & \cdot & \cdot & \cdot & & \\ & & & & h_0 & h_1 & h_2 & h_3 \\ h_2 & h_3 & & & & & h_0 & h_1 \end{pmatrix}$$

$$G = \begin{pmatrix} g_2 & g_3 & & & & & g_0 & g_1 \\ g_0 & g_1 & g_2 & g_3 & & & & \\ & & \cdot & \cdot & \cdot & \cdot & & \\ & & & & g_0 & g_1 & g_2 & g_3 \end{pmatrix} \tag{4}$$

where coefficients of filter G must be created according (5) because of quadrature mirror character. Also matrices H and G must be orthogonal.

$$g_n = (-1)^n \cdot h_{N-1-n} \tag{5}$$

Wavelet transformation is computed as operation of vector X containing signal components and matrices H and G according (6). As a result we will gain vector of approximation A and vector of wavelet coefficients C.

$$X \cdot \begin{pmatrix} H \\ G \end{pmatrix} = \begin{pmatrix} A \\ C \end{pmatrix} \tag{6}$$

Vector A represents lower frequencies and vector C represents higher frequencies of the processed signal. [13]

Dyadic decomposition is used very often in the field of image processing. The basic structure of the dyadic decomposition of an image can be seen in the Figure 2. Blocks Hi or Lo represent impulse response of a high-pass filter or a low-pass filter and the block signed as 2↓ makes down-sampling by 2.

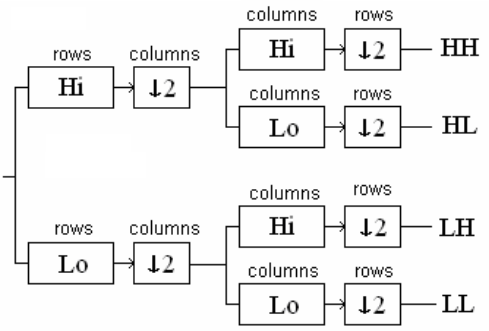


Figure 2. Basic structure of the dyadic decomposition of the image

Firstly, all pixels of the processed image in rows are transformed by the filters. Transformed rows are then down-sampled and the columns of analyzed data are processed again. As a result, four sets of coefficients are created after the dyadic decomposition of the image: LL – approximation of the image, LH – details of the image in the horizontal orientation, HL – details of the image in the vertical orientation, HH – details of the image in the diagonal orientation.

As can be seen in the Figure 3 the processed image was dyadic decomposed into some frequency sub-bands and the lowest frequency sub-band was iteratively decomposed.

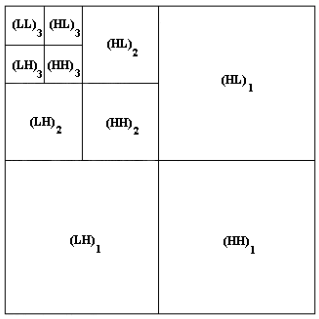


Figure 3. Dyadic decomposition of an image to the third level

The image can be reconstructed and transformed back into the time domain. Moreover, if the sub-bands LH, HL or HH are set to 0, the image is reconstructed without the appropriate details. This feature is very often utilized in the field of the lossy data compression or the signal denoising.

2.1. Image encryption scheme

Suppose the matrix P which contains the values of pixels $p_{i,j} \in P$ of an image, where $i \in (0,1,2,...W)$ and $j \in (0,1,2,...H)$, W and H represents the width and the height of the matrix/image. The matrix P is transformed into the wavelet domain using the dyadic decomposition. The resultant matrix C contains the wavelet coefficients $c_{i,j}$ which are the input data for the encryption algorithm.

The strange attractor of Peter de Jong is used for the encryption purposes here. This type of chaotic system consists of two maps, which can be used for the coefficients permutation. However, the permutation is not sufficient in terms of security, because this process can be revealed e.g. by the system of fuzzy ergodic matrices very easily [7]. Hence, there must be included also modification of coefficients into the encryption process. This improvement lies in the extension of the chaotic system to 3D version (7). Third map can be used for the modification purposes.

$$\begin{aligned} x_{n+1} &= \sin(a \cdot y_n) - \cos(b \cdot x_n) \\ y_{n+1} &= \sin(c \cdot y_n) - \cos(d \cdot x_n) \\ z_{n+1} &= \sin(e \cdot z_n) - \cos(f \cdot y_n) \end{aligned} \tag{7}$$

Idea of the encryption process is to encrypt each wavelet coefficient separately. The control parameters a, b, c, d, e, f in the chaotic system (7) play the role of the encryption keys here. Define c_A as the wavelet coefficient at coordinates (x_i, y_j). Position x_i, y_j and value c_A is put into (7) as initial condition of the appropriate map. Resultant values x_k, y_k and z_k are disposal after k-th iteration of the chaotic system and the quantization of the resultant values. The second wavelet coefficient c_B at coordinates (x_k, y_k) must be found. Coefficient c_B is then XOR operated with z_k and this modified value is swapped with coefficient c_A according to (8). Encrypted coefficient is gained this way.

$$c_A \leftrightarrow c_B \oplus z_k \tag{8}$$

This process must be done for every wavelet coefficient in the matrix C and can be done m times in order to increase the security of encrypted image. Flowchart of the encryption process is drawn in the Figure 4.

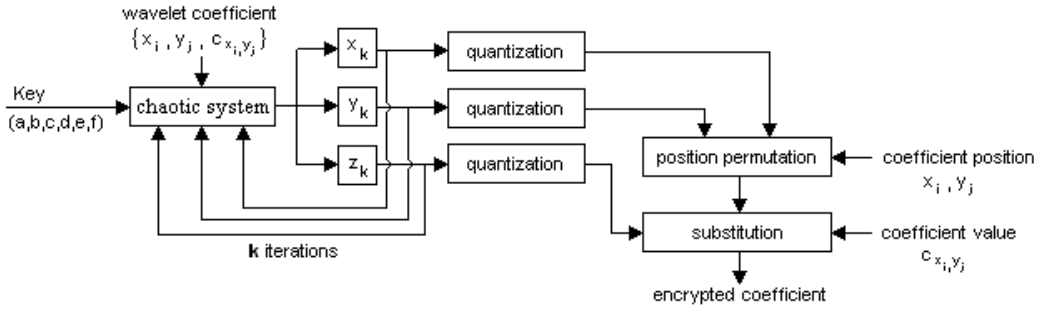


Figure 4. Flowchart of the encryption process

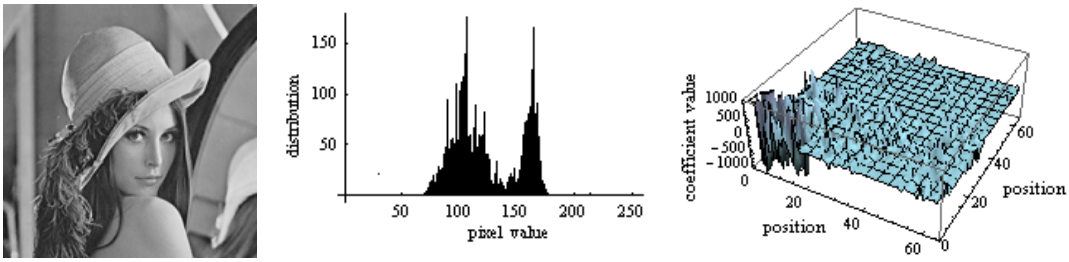
3. Experimental results and security analyses

The second-order Daubechies wavelet was used for the dyadic decomposition of the image and only sub-matrix $C_0 \subset C$ with coefficients $c_{m,n} \in C_0$ where $m \in (0,1,2,...\frac{W}{4})$ and $n \in (0,1,2,...\frac{H}{4})$ is considered in the following experiments. It means that only one sixteenth of all coefficients is encrypted. Nevertheless, this sub-matrix contains the most significant coefficients which are representing the approximation and some details of the processed image. The encryption process is speeded up when the sub-matrix C_0 is processed only. However, the considering only of this approximation has a deep impact in the quality of the reconstructed image, due to the suppressing of the appropriate details in the image. This loss of information can be acceptable only in some applications, such as video-conferences.

The encryption scheme described above was experimentally tested on "Lena" image of 256x256 pixels size. Figure 5 shows original image, distribution of its pixel values and the sample of the wavelet domain which contains the most important coefficients. The image was encrypted by the keys (9). These keys are the control parameters of the chaotic system.

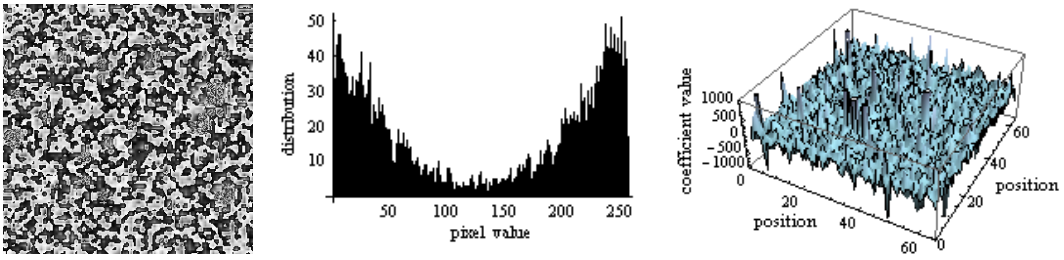
$$\{a = 1.4, \mathrm{b} = -2.3, \mathrm{c} = -2.4, \mathrm{d} = -2.1, \mathrm{e} = 1.2, \mathrm{f} = 1.6\} \quad (9)$$

Encrypted image after the reconstruction is shown in Figure 6. The distribution of pixels are not uniform, but the U-shape, because of the considering of the submatrix C_0 only and the loss of information. If we consider the whole matrix C containing all wavelet coefficients, the distribution will be very close to uniform. Uniformity is a sign of no statistical resemblance between the original and the encrypted image. The U-shape in the histograms is appearing at all encrypted types of images. Thus, we can say that the U-shape gives us the same statistical information as uniform-like distribution in the security view. The most significant wavelet coefficients are situated in the lowest band of the wavelet domain (in the first positions of the submatrix C_0).



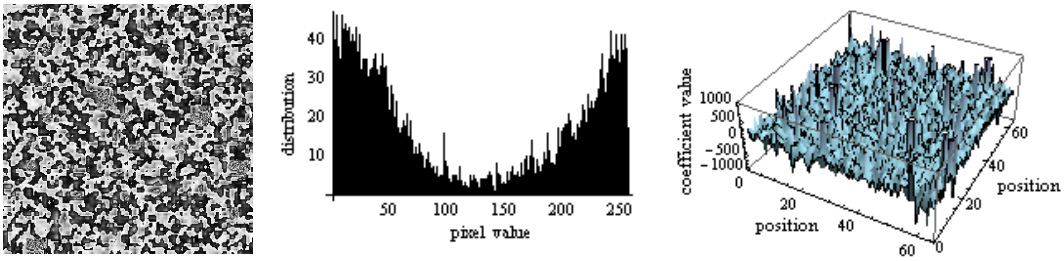
(a) (b) (c)

Figure 5. (a) original image, (b) histogram of original image, (c) sample of the wavelet domain



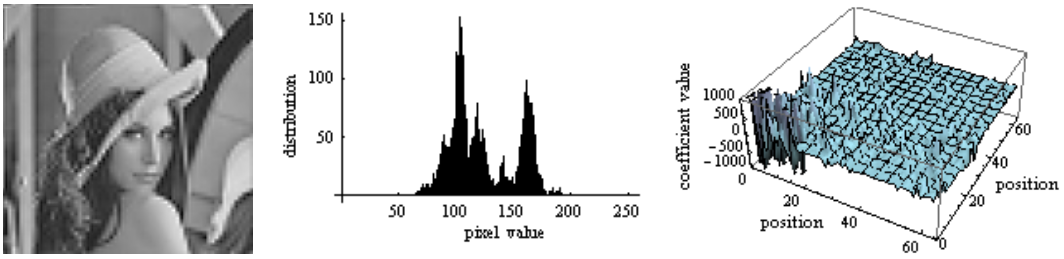
(a) (b) (c)

Figure 6. (a) encrypted image, (b) histogram of encrypted image, (c) sample of the wavelet domain



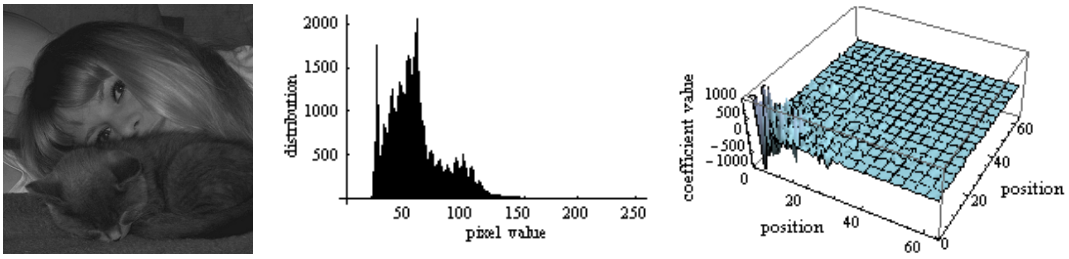
(a) (b) (c)

Figure 7. (a) incorrectly decrypted image, (b) histogram of incorrectly decrypted image, (c) sample of the wavelet domain



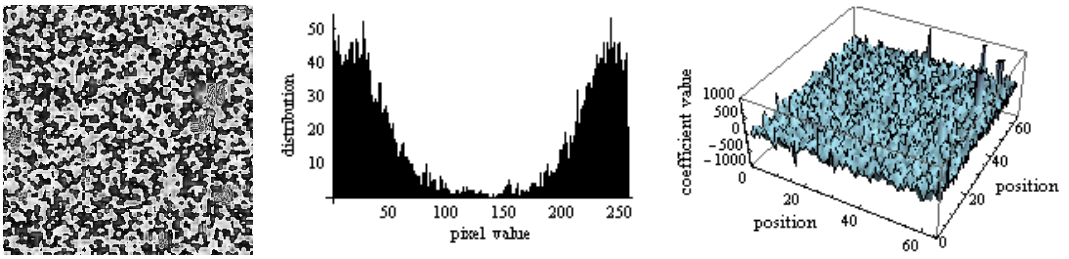
(a) (b) (c)

Figure 8. (a) decrypted image, (b) histogram of decrypted image, (c) sample of the wavelet domain



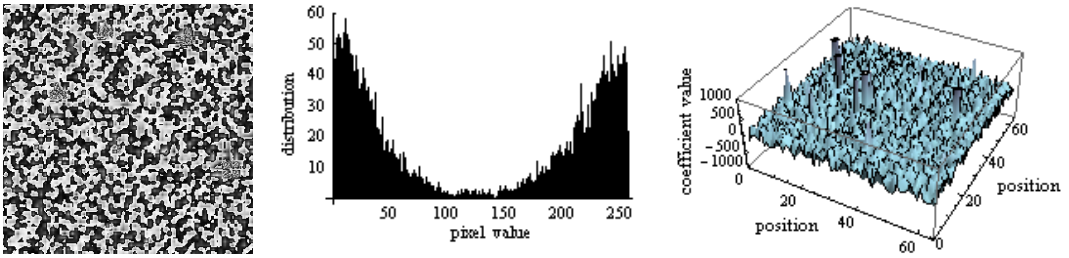
(a) (b) (c)

Figure 9. (a) original image, (b) histogram of original image, (c) sample of the wavelet domain



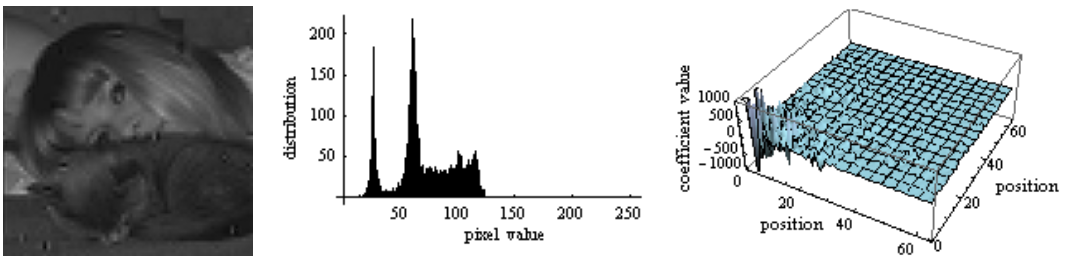
(a) (b) (c)

Figure 10. (a) encrypted image, (b) histogram of encrypted image, (c) sample of the wavelet domain



(a) (b) (c)

Figure 11. (a) incorrectly decrypted image, (b) histogram of incorrectly decrypted image, (c) sample of the wavelet domain



(a) (b) (c)

Figure 12. (a) decrypted image, (b) histogram of decrypted image, (c) sample of the wavelet domain

The encrypted image was then decrypted by the keys (10). First control parameter has a minimal divergence from that parameter in (9).

$$\{a = 1.40001,\ \mathrm{b} = -2.3,\ \mathrm{c} = -2.4,\ \mathrm{d} = -2.1,\ \mathrm{e} = 1.2,\ \mathrm{f} = 1.6\} \tag{10}$$

Figure 7 shows that even a slight change in decryption keys will cause illegibility and indeterminateness of the reconstructed image. There is the U-shape in the pixel distribution again and the wavelet coefficients have different values and they are dislocated in the whole area of wavelet domain (the submatrix C_0 contains various values of coefficients in all positions).

When the image is decrypted by the correct keys (9), we will gain approximation of the original image. The loss of information is obvious from the Figure 8. The histogram representing distribution of the pixels is also a little different from that one in Figure 5. This loss of information is done due to the considering of the submatrix C_0, which does not contain the details of the original image. However, all wavelet coefficients of the submatrix C_0 are the same as before the encryption process.

The similarity between the original submatrix C_0 and its encrypted form can be proof of efficient confusion and diffusion properties of this encryption scheme. That similarity can be expressed by the cross-correlation. Cross-correlation is a standard method of estimating the degree to which two series are correlated. Consider two series x_i and y_i where $i = 1,2,.....,N$ and $E(x)$, $E(y)$ are the means of the corresponding series according to (11).

$$E(x) = \frac{1}{N} \cdot \sum_{i=1}^{N} x_i \tag{11}$$

The cross correlation r at delay d is defined as:

$$r(d) = \frac{\sum_i (x_i - E(x)) \cdot (y_{i-d} - E(y))}{\sqrt{\sum_i (x_i - E(x))^2} \cdot \sqrt{\sum_i (y_{i-d} - E(y))^2}} \tag{12}$$

Cross-correlation can be used as a measure of similarity of two images that differ only by a shift. Cross-correlation was computed from the delay $d = 0$ to $d = 127$. The denominator in the expression (12) normalizes the correlation coefficients such that $-1 \le r(d) \le 1$. This bound indicates maximum correlation and $r(d) = 0$ indicates no correlation. A high negative correlation indicates a high correlation in the case of inversion of one of the series [12].

Figure 13 shows cross-correlation of original and encrypted submatrix C_0. It is obvious that correlation value does not exceed ±0.04. That means very low correlation and very low similarity of the submatrices and their coefficients.

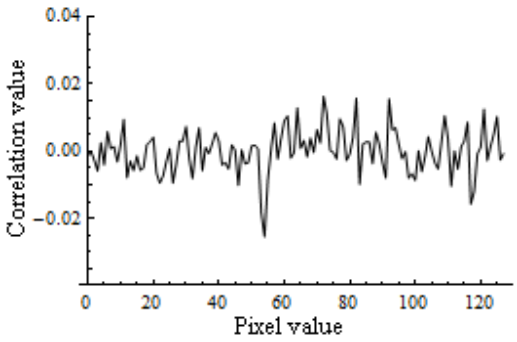


Figure 13. Cross-correlation of original and encrypted coefficients

In general, adjacent pixels of the most plain-images are highly correlated. One of the requirements of an effective image encryption process is to generate encrypted image with low correlation of adjacent pixels. Correlation between two horizontally, vertically and diagonally adjacent coefficients of the original and the encrypted submatrix C_0 was analyzed. Each pair of adjacent coefficients of the original submatrix was chosen and correlation coefficient was computed according (9). Then the same process was done for the encrypted submatrix. Correlation coefficients in different directions of adjacent coefficients are listed in Table 1. As can be seen, every encryption scheme [8,9,10] can effectively de-correlate adjacent pixels in the original image. The correlation coefficients are very low when the proposed encryption scheme is used. Thus, proposed scheme has efficient permutation and diffusion properties. However, it is important to notice that the wavelet coefficients are analyzed for this scheme, not values of pixels.

Table 1. Correlation coefficients of original/encrypted image

Direction of adjacent components	**Original image**	**Encrypted image**	**Encrypted image by [8]**	**Encrypted image by [9]**	**Encrypted image by [10]**
Horizontal	0.942755	0.001936	0.005776	-0.014200	0.002637
Vertical	0.970970	0.007406	0.028434	-0.007400	0.009177
Diagonal	0.920081	0.004815	0.020662	-0.018300	0.003429

Sensitivity of decryption keys is very high as it was shown in Figure 7. This statement can be proved from the cross correlation view by simple experiment. Take parameter a of decryption keys (7) and compute cross-correlation values between original and decrypted submatrix C_0 from $a = 1.399999999$ to $a = 1.400000001$ by step 0.000000000001. It is obvious that the cross correlation will be maximal when the parameter is set to $a = 1.4$ (this value is correct). Figure 14 shows dependency of correlation values on different values of parameter a. The peak located in the middle of the plot signifies correct value of the parameter a and thus maximal correlation between original and decrypted submatrix C_0. However, correlations are very low when other values from the interval of the parameter a are used. Even if we are getting near to that correct value, the correlations are still low and contain no information (such as suspicious ascension) about the location of the correct value.

This experiment shows that even close neighbourhood of the correct decryption key cannot reconstruct submatrix C_0 neither to its approximately form.

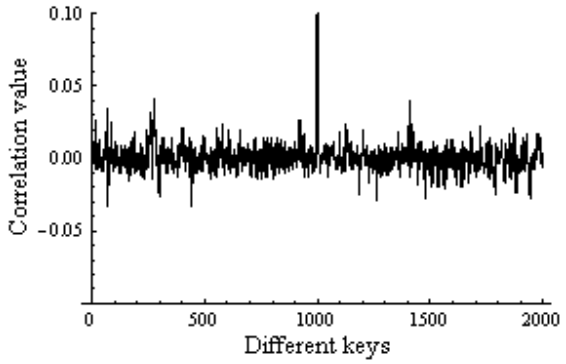


Figure 14. Cross-correlation of original and decrypted coefficients by different keys

Reliable encryption scheme must be resistant against any brute-force attacks, thus the key space must be too large. The total precision of the common PC processor is 16 decimal digits therefore the number of the different combinations of one parameter is 10^{16} and it corresponds approximately to 2^{53} size key space. Six attractor parameters are used in the proposed scheme; hence the key space is enlarged to 2^{318}. Also the number of the iterations k of the Peter de Jong's system (4) and number of the encryption rounds m can be considered as the keys. Thus, the key space of the proposed scheme is large enough to make the brute-force attack infeasible. Table 2 shows comparison of the key spaces of different encryption schemes. The proposed encryption scheme has the largest key space.

Table 2. Key space comparison

Encryption scheme	**Key space**
Proposed	2^{318}
[2]	2^{158}
[8]	2^{128}
[9]	2^{232}

4. Performance evaluation

One of the main goals of our work was to create encryption scheme which can be applied in the real-time processes. Performance of our scheme is evaluated with the un-optimized C# code. Table 3 presents computation time in seconds for different values of the parameters k and m. Security of the encrypted image is directly proportional to the height of the parameter values. There is also Table 4 showing encryption speed of our previous developed scheme [6] for comparison purposes.

Table 3. Encryption speed of proposed scheme

Iterations k / Rounds m	**1**	**5**	**10**	**25**
1	0.031	0.062	0.078	0.109
5	0.062	0.093	0.125	0.250
10	0.078	0.140	0.203	0.421
25	0.078	0.265	0.468	1.125

Table 4. Encryption speed of [6]

Iterations k / Rounds m	**1**	**5**	**10**	**25**
1	0.078	0.235	0.432	1.008
5	0.391	1.184	2.146	5.075
10	0.791	2.349	4.359	10.328
25	1.943	5.934	10.937	26.053

According to our previous research [6], the encryption speed is reduced in average 22 times. This significant reduction means that the maximal speed of the encryption process can reach up to 2064kB/s on 1.50-GHz AMD Athlon processor. The speed is about 688kB/s when the parameters k and m are set to 5. Thus, we can create secured video-conference at 10.75 FPS this way. We presume that the encryption speed should be higher when some improvements are done, such as optimization of the algorithms. We should be able to reach 15 FPS, which is sufficient speed for the video-conferences.

5. Conclusion

Proposed encryption scheme uses wavelet transformation for the extraction of the most important information from the image. When the image is transferred into the wavelet domain, chosen wavelet coefficient is encrypted by the chaotic system of Peter de Jong. Coordinates and value of each coefficient becomes initial condition for the appropriate map of the chaotic system; new coordinates and value is created after several iterations. The computation time was reduced rapidly because of encrypting only the most important coefficients and the security of encrypted image is still high enough. However, there is a loss of information when reconstructing the image because of omitting some details. Nevertheless, this encryption scheme can be applied to the real-time processes, such as encrypted video-conferences, where the requirements to quality of reconstructed images are inferior.

References

[1] Fu, Ch., Zhang, Z., Chen, Z., Wang, X. An Improved Chaos-Based Image Encryption Scheme. ICCS 2007, Springer-Verlag, Berlin, 2007.

[2] Fu, Ch., Zhang, Z., Cao, Y. An Improved Image Encryption Algorithm Based on Chaotic Maps. ICNC 2007.

[3] Fridrich, J., Symmetric Ciphers Based on Two-dimensional Chaotic Maps, International Journal of Bifurcation and Chaos. 1998, vol. 9, is. 6, pp. 1259-1284. ISSN 0218-1274.

[4] Zhai, Y., Lin, S., Zhang, Q. Improving Image Encryption Using Multi-chaotic Map, Workshop on Power Electronics and Intelligent Transportationi System, 2008.

[5] Hossam, A., Hamdy, K., Osama, A. An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption. Informatica 31, 2007.
[6] Giesl, J., Vlcek, K., Image Encryption Based on Strange Attractor, ICGST-GVIP Journal. 2009, vol. 9, is. 2, pp. 19-26. ISSN 1687-398.
[7] Zhao., X-y., Chen, G., Zhang, D., Wang, X-h., Dong, G-c. Decryption of pure-position permutation algorithms. JZUS, Hangzhou, 2004.
[8] Mao, Y., Chen, G. Chaos-Based Image Encryption. Springer-Verlag, Berlin, 2003.
[9] Gao, T., Chen, Z. A new image encryption algorithm based on hyper-chaos, ScienceDirect, 2007.
[10] 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, is. 15, pp. 2645-2652. ISSN 0375-9601.
[11] Sprott, J.C. Chaos and Time-Series Analysis, Oxford University Press, 2003, ISBN 978-0-19-850840-3.
[12] Bourke, P. Cross Correlation [online]. Available at WWW: http://local.wasp.uwa.edu.au/~pbourke/miscellaneous/correlate/ , 2006.
[13] Vlcek, K., Komprese a kodova zabezpeceni v multimedialnich komunikacich, Technicka literature BEN, Praha, 2004, ISBN 80-7300-134-9.

Authors

Jiri Giesl received his Masters Degree in Information Technologies from Tomas Bata University in Zlin, Czech Republic in 2007. He is PhD candidate in the Department of Applied Informatics currently. His areas of interest are Digital signal processing, Encoding and Compression, Wavelet theory, Chaos & Fractals and their application for signal analysis and synthesis.

Ladislav Behal received his Masters Degree in Information Technologies from Tomas Bata University in Zlin, Czech Republic in 2007. He is PhD candidate in the Department of Applied Informatics currently. His areas of interest are: Chaos theory, Chaos encryption schemes, Evolutionary algorithms, Game theory and their application for channel communications and decryption.

Karel Vlcek received his Masters Degree from University of Technology in Brno, Czech Republic in 1971, Doctoral Thesis (1989) and Assoc. Prof. Defence (1993) from Czech Technical University in Prague, and Full Professorship from VSB Technical University of Ostrava, Czech Republic in 2003. His professional carrier starts in the company TESLA Roznov (1973), as a development specialist in the group of "Testing of integrated circuits", and continues in the company TESLA Valasske Mezirici (1982), in the working group of "Application of Microprocessors". His research activities at the universities are Digital Signal Processing, Theory of Information and Coding, Design of Electronic Circuits with support VHDL, Telecommunications, and Biomedical Engineering. Currently he is at the Department of Applied Informatics of Faculty of Applied Informatics, Tomas Bata University in Zlin, Czech Republic.