BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 64, No. 2, 2016
DOI: 10.1515/bpasts-2016-0042

Joint compression and encryption of visual data using orthogonal parametric transforms

D. PUCHALA* and M. M. YATSYMIRSKYY

Lodz University of Technology, Institute of Information Technology, 215 Wolczanska St., Lodz, Poland

Abstract. In this paper, we introduce a novel method of joint compression and encryption of visual data. In the proposed approach the compression stage is based on block quantization while the encryption uses fast parametric orthogonal transforms of arbitrary forms in combination with a novel scheme of intra-block mixing of data vectors. Theoretical analysis of the method indicates no impact of encryption stage on the effectiveness of block quantization with an additional step of first order entropy coding. Moreover, a series of experimental studies involving natural images and JPEG lossy compression standard were performed. Here, the obtained results indicate a high level of visual content concealment with only a small reduction of compression performance. An additional analysis of security allows to state that the proposed method is resistant to cryptanalytic attacks known for visual data encryption schemes including the most efficient NZCA attack. The proposed method can be also characterized by high computational efficiency and feasibility of hardware realizations.

Key words: data encryption, parametric linear transforms, lossy data compression.

1. Introduction

For several years, we have been witnessing the rapid popularization of wireless systems for transmission of visual data, i.e. static images and video sequences. In such systems due to the openness of communication channels transmitted data can be easily intercepted by unauthorized recipients. At the present time, this problem may concern a number of practical applications including: communication in remote video surveillance systems for household and institutional usage, private and corporate multimedia transmissions, digital television broadcasts, media file sharing over public networks, etc. For this reason the designers of such systems are strongly advised to take advantage of secure transmission protocols which mostly employ symmetric encryption algorithms, e.g., IDEA, DES, 3DES, or AES [1]. In the case of real-time transmissions of visual data such algorithms may be computationally too expensive, in particular for portable devices with battery operation (see [2,3]). It should be noted, however, that visual data have a lower value than, e.g., financial or military ones. In such a case, cryptanalytic attack can by far exceed the value of a broadcast and for that reason it would be not of interest to potential adversaries. Summarizing, it can be said that transmission of images or videos requires large volumes of data, while the value of data is low (see [4, 5]). For this reason, it is still required to develop novel and computationally efficient encryption algorithms that guarantee adequate levels of security.

In the case of visual data, except safety, equally important is the reduction of data sizes, which translates directly into the reduction of bandwidth requirements for transmission channels. For this purpose lossy compression algorithms are commonly used in practical applications, e.g., JPEG standard for static images or MJPEG and MPEG standards for video sequences [6]. It is obvious, therefore, that developed encryption algorithms should not decrease significantly the possibilities of compression of visual data.

In the view of the above motivation, we propose in this paper a novel method for joint compression and encryption of visual data. In the proposed approach the compression stage uses block quantization, which is the core of existing standards such as: JPEG, MJPEG and MPEG. It allowed to keep compliance with known standards and to obtain comparable performance of data compression. The encryption process is based on fast parametric orthogonal transforms (FPOTs) and a novel scheme of *inter-block mixing* of data vectors. The proposed method can be characterized by higher combinatorial complexity than existing methods based on linear transforms and, in addition, it is resistant to cryptanalytic attacks known for visual data encryption algorithms.

In the research part of the paper it was proved theoretically that the proposed encryption scheme does not affect the compression performance based on block quantization with an additional step of first order entropy coding. Furthermore, a series of experiments concerning joint compression and encryption of natural images were performed by embedding the proposed encryption scheme into JPEG standard. Finally, we discuss in detail the aspects of computational complexity of the method and also provide a critical analysis of its resistance to the known types of cryptanalytic attacks.

2. Existing visual data encryption methods

The existing methods of visual data encryption can be divided into two groups: naive and selective. The naive approach

*e-mail: dariusz.puchala@p.lodz.pl

treats visual data as a sequence of bytes and hence data can be encrypted with conventional algorithms, e.g., IDEA, DES, 3DES, or AES (c.f. [7]). The disadvantage of this approach is high computational complexity and concealment of additional structures of data stream which in the case of MPEG transmission may cause difficulties with data synchronization in time. The selective approach is oriented to the type of encrypted data and takes advantages of some properties of data stream. In this group, methods operating in the domain of discrete cosine transform (DCT), i.e. spectral methods, and methods working with data representation obtained after entropy coding dominate. In the case of spectral methods, we can indicate approaches that are based on, e.g., permutation of DC and AC[1] coefficients within 8 on 8 pixel areas of an image [5, 8, 9], distribution of DC coefficients within and permutation of AC coefficients between image areas [10], encryption of selected spectral coefficients ordered by an amount of contained visual information [11, 12], or divided into bit layers [13, 14], and finally approaches that modify spectral coefficients with aid of bitwise operations [15–17], linear orthogonal matrices [18], or non-linear mappings [19]. In the group of methods that encrypt data obtained after Huffman entropy coding [20] the typical approaches simply change the order of symbols describing sequences of zeroed AC coefficients after the step of run-length encoding (RLE) [21], or modify the Huffman tables of codes maintaining the lengths of codes what ensures unchanged performance of compression [4].

Some of the mentioned visual data encryption methods found practical applications providing expected results. However, the practical compromise here is to keep high computational efficiency by ensuring safety only at the level appropriate for data value. Hence, a number of low-cost cryptanalytic attacks were developed which are well-fitted to selected encryption algorithms which operate in DCT domain [22, 23], as well as on Huffman codes representation of data [22]. The safety analysis of the proposed method in the context of known attacks is presented in the following part of the paper.

3. Fast parametric orthogonal transforms

Fast orthogonal parametric transforms (FPOTs) are the class of linear transformations with fast computational structures. They are computationally efficient and powerful tools of digital signal processing which find wide application in, e.g., compression, filtering, and encryption of data [24–32]. FPOTs usually adopt the computational structures of known transforms with determined basis vectors. However, the fundamental difference lies in their parametrization. Due to parametrization it is possible to adapt transform shape to the class of processed signals and to the type of performed operations.

In accordance with [25] any orthogonal transform can be represented as:

$$V = \left(\prod_{k=1}^{K} P_{K-k+1} U_{K-k} \right) P_0, \tag{1}$$

where P_k for $k = 0,1,\ldots,K$ are N on N element permutation matrices, N is a size of transformation, and U_k for $k = 0,1,\ldots,K-1$ denote N on N element block-diagonal matrices that contain rotation operations in $\mathscr{R}^2$ subspaces on main diagonals. Thus U_k matrices describe the subsequent stages on which operations on data are being performed while K is a number of stages. In this paper, we define rotations in $\mathscr{R}^2$ subspaces as follows:

$$O_{kl} = \begin{bmatrix} \cos(\alpha_{kl}) & \sin(\alpha_{kl}) \\ -\sin(\alpha_{kl}) & \cos(\alpha_{kl}) \end{bmatrix}, \tag{2}$$

for $k = 0,1,\ldots,K-1$ and $l = 0,1,\ldots,N/2-1$ where α_{kl} are angles of rotation for O_{kl} operators at each stage.

In Fig. 1 a data-flow graph of fast two-stage structure for $N = 8$, point transformation used in the following part of the paper is presented. This structure can be characterized by high combinatorial capacity allowing to realize any permutation of elements in input vector [33]. This is an important feature from the point of view of data encryption. This structure was also analyzed in terms of its suitability for encryption of data in paper [34]. The obtained results show high, i.e. equal about 200% of signal energy, expected values of mean square error of signal reconstruction in the case of exhaustive attacks.

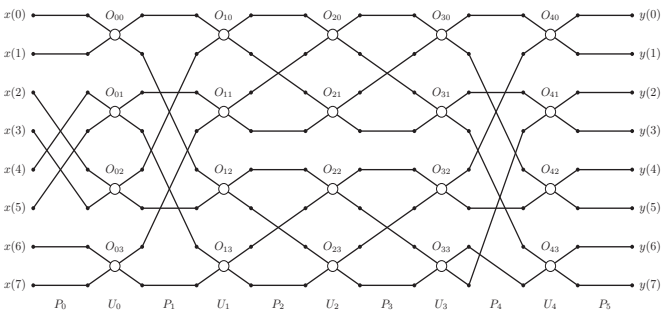


Fig. 1. Data-flow graph of fast two-stage parametric transform for $N = 8$

Symbolically by "o" we denote in Fig. 1 the rotation operators O_{kl} wherein operators with the same index k constitute stages represented in formula (1) by U_k matrices. Matrices P_k for $k = 0,1,\ldots,K-1$ describe connections between stages while matrices P_0 and P_K define permutations of elements in input and output vectors respectively. The parameter K defines a number of stages which for the given structure equals $K = 2\log_2(N)$. By taking into account the computational complexities of individual operators and their numbers in stages, it is clear that the computational complexity of a given structure can be estimated as $\mathscr{O}(N\log_2 N)$. Thus such a structure can be regarded as a fast one. The exact number of multiplications and additions can be expressed as: $\mathscr{L}_{MUL} = 2N(2\log_2 N - 1)$ and $\mathscr{L}_{ADD} = N(2\log_2 N - 1)$. The parameters that determine the shape of V transformation are the angles of rotation α_{kl} for

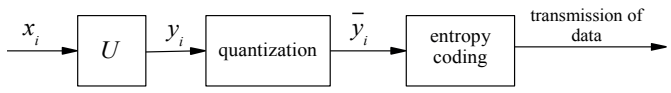
[1]DC coefficient is a constant component of two-dimensional DCT. AC refers to the remaining coefficients of that transformation.

$k = 0,1,\ldots,K-1$ and $l = 0,1,\ldots,N/2-1$. Hence, the total number of parameters for a given structure can be described by the following formula: $\mathscr{L}_{PAR} = \frac{N}{2}(2\log_2 N - 1)$.

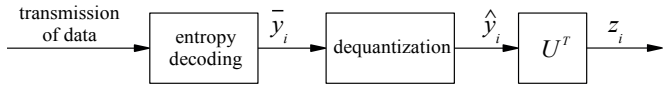
4. The proposed method of joint compression and encryption of data

In this paper the method of joint compression and encryption of data is proposed. The compression is based on a well-known and popular block quantization scheme which allows for lossy compression of data. The encryption stage takes advantage of orthogonal parametric transforms of arbitrary forms and it is implemented in a novel scheme of *intra-block mixing* of data vectors. In this section, we describe the mentioned issues.

4.1. Block quantization. Introduced in [35], block quantization is one of the most widely utilized schemes of lossy compression of visual data. It is the core of the following compression standards: JPEG, MJPEG, and MPEG [6]. The consecutive steps of data compression and decompression for block quantization are presented in Fig. 2.



a. Data compression stage.



b. Data decompression stage.

Fig. 2. Block quantization scheme with stages of data compression and decompression

At the compression stage we introduce to the input of the scheme N-element column vectors x_i for $i = 0,1,\ldots,M-1$ which contain real-valued samples of input signal. These vectors are then transformed into the domain of U transformation as $y_i = Ux_i$ where U is N on N element matrix. Here the orthogonality of U transformation is assumed, i.e. $U^T U = I$ where I is an identity matrix. The next step is a scalar quantization of vector components $y_i(n)$ which in practice takes the form of uniform scalar quantization (cf. [36]). The purpose of this step is to reduce the number of bits required for storing components of vectors $\bar{y}_i$ and this is a lossy operation. In the final step the components of vectors $\bar{y}_i$ are subjected to lossless entropy coding, e.g. using Huffman codes [20], and then are transmitted by a broadcast channel to the recipient. It can be proved [36] that with the optimal allocation of bits to individual vector components, the mean square error (MSE) resulting from quantization, i.e. the signal reconstruction error, equals:

$$\varepsilon_{MSE} = \frac{16}{3} N 2^{-2\Theta} \left(\prod_{n=0}^{N-1} \sigma^2_{y(n)} \right)^{\frac{1}{N}}, \tag{3}$$

where Θ is a mean number of bits allocated to components of vectors y_i, and $\sigma^2_{y(n)}$ are the variances of individual components $y_i(n)$ for $n = 0,1,\ldots,N/2-1$. In accordance with [37] the optimal transform U, i.e. the transformation that minimizes the value of the following product:

$$D_y = \left(\prod_{n=0}^{N-1} \sigma^2_{y(n)} \right), \tag{4}$$

is the orthogonal Karhunen-Loève transform (KLT). However, in practice due to high computational complexity of KLT its fast approximations with complexity reduced by one order of magnitude, i.e. to $\mathscr{O}(N \log_2 N)$ level, are preferred. In the case of natural images such approximation is the fast algorithm for discrete cosine transform of the second type (DCT) [6].

The decompression stage involves the following steps: entropy decoding, dequantization, and transformation to the signal domain, i.e. $z_i = U^T \hat{y}_i$. The MSE of signal reconstruction defined as: $\varepsilon_{MSE} = \frac{1}{M} \sum_{i=0}^{M-1} \|x_i - z_i\|^2$, where $\|\cdot\|$ is the Euclidean norm, is expressed in terms of formula (3).

4.2. Intra-block mixing scheme. The proposed approach extends the scheme from Fig. 2 by an additional step of data encryption. The natural assumption here is that the additional step *should not affect the compression efficiency*, i.e. it should not increase the reconstruction error ε_{MSE} for the given value of a mean number of bits Θ (see formula (3)).

In the group of known methods of encryption of visual data which are based on orthogonal transforms we can indicate such that do not change the product of variances D_y and hence do not affect the compression efficiency in terms of expression (3). We have here in mind approaches based on diagonal matrices with elements $\{-1,1\}$ [4] or permutation matrices [5]. In both cases input vectors for the encryption stage are directly multiplied by a ciphering matrix, i.e. $v_i = Au_i$ where $\{u_i\}$ is a set of plain vectors, $\{u_i\}$ is a set of encrypted vectors, and A is a ciphering transform. With such encryption formula the ciphering matrices of the mentioned forms do not change the value of D_y (see (4)) if only $u_i = y_i$ for $i = 0,1,\ldots,M-1$. It is clear then that in the case of method [4] the values and the order of variances are preserved. For the method from paper [5] the order of AC coefficients, and thus the order of their variances is modified. Although the change of order of variances does not affect the value of D_y product the permutation of AC coefficients can have a tremendous impact on the lengths of sequences of zeroed coefficients obtained after quantization, and for this reason it can also decrease the effectiveness of compression in such standards as: JPEG, MJPEG, or MPEG. In addition, the methods from [4, 5] take advantage of orthogonal transforms of specific and narrow classes and can be used only in the domain of U transform, i.e. they can operate only on the set of $\{u_i\}$ vectors.

In the proposed method we use a different approach which assumes that the encryption step operates not on individual vectors but on their disjoint blocks composed of N vectors with N elements each that are selected arbitrarily from the whole set of input data. The proposed encryption step is presented in the form of diagram in Fig. 3 and it is also formulated as the algorithm.

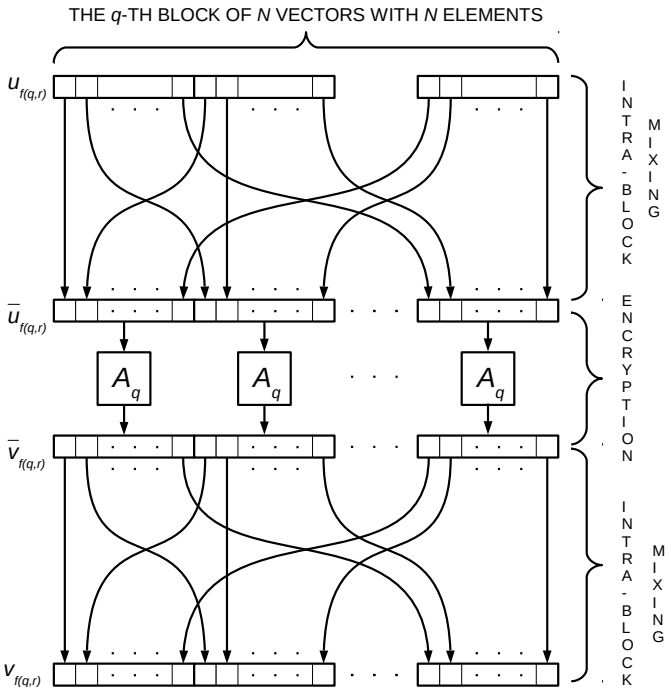


Fig. 3. Data encryption stage based on intra-block mixing of vectors

Algorithm. Let there be given a set of N-element plain vectors $\{u_i\}$ for $i = 0, 1, \ldots, M-1$.

1. Define injective function $f(q, r)$ that takes integer values in the range of 0 to $M-1$ for $q = 0, 1, \ldots, M/N-1$ and $r = 0, 1, \ldots, N-1$. The purpose of this function is to map plain vectors into vectors in blocks.
2. Prepare the list of orthogonal ciphering matrices $\{A_q\}$ for $q = 0, 1, \ldots, M/N-1$.
3. Group plain data vectors into M/N disjoint blocks $\{u_{f(q,r)}: r = 0, 1, \ldots, N-1\}$ for $q = 0, 1, \ldots, M/N-1$.
4. Within a given block q mix elements of vectors $\{u_{f(q,r)}\}$ for $r = 0, 1, \ldots, N-1$ in accordance with the following rule: the first resulting vector (obtained after mixing) holds 1st index elements from all plain vectors in the block, the second resulting vector holds 2nd index elements, etc. (see Fig. 3). This step is called *intra-block mixing* of vectors. As a result we obtain a set of vectors: $\{\overline{u}_{f(q,r)}\}$.
5. Encrypt individual vectors in block as $\overline{v}_{f(q,r)} = A_q \overline{u}_{f(q,r)}$ for $r = 0, 1, \ldots, N-1$.
6. Perform second intra-block mixing of vectors from the set $\{\overline{v}_{f(q,r)}\}$. As a result a set $\{v_{f(q,r)}\}$ of encrypted vectors is obtained.
7. Repeat steps 4–6 for each block of plain vectors, i.e. for $q = 0, 1, \ldots, M/N-1$.
8. Finish.

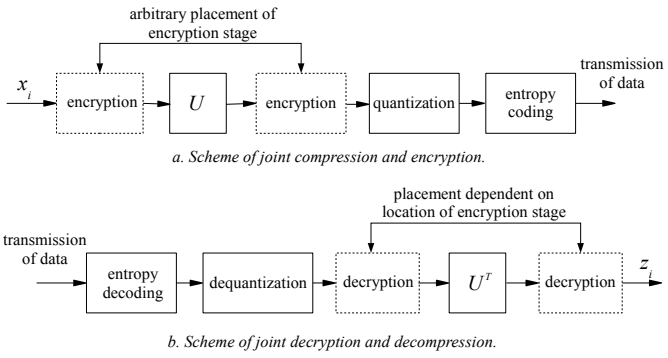
As a result of operation of the above algorithm, each block of plain vectors $\{u_{f(q,r)}\}$ is converted into one block of encrypted vectors $\{v_{f(q,r)}\}$. The list of orthogonal ciphering matrices $\{A_q\}$ can contain M/N distinct matrices. It means that each block of plain vectors can be encrypted with the aid of individual ciphering matrix.

4.3. Joint compression and encryption. Fundamental from the point of view of joint compression and encryption of data is the following theorem whose proof is given in Appendix A.

Theorem. Let there be given a set of N-element plain vectors $\{u_i\}$ for $i = 0, 1, \ldots, M-1$ grouped into a number of M/N disjoint blocks $\{u_{f(q,r)}: = 0, 1, \ldots, N-1\}$ where $q = 0, 1, \ldots, M/N-1$. Then the stage of data encryption based on intra-block mixing preserves equality of second order statistical characteristics between plain and encrypted vectors for any list $\{A_q: q = 0, 1, \ldots, M/N-1\}$ of orthogonal ciphering matrices. It means that the equality of autocovariance matrices holds.

In accordance with the theorem an encryption step based on intra-block mixing of vectors preserves the form of autocovariance matrix. Thus, it follows directly that data encryption step can be performed without affecting the compression efficiency in both input signal (i.e. $u_i = x_i$) and U transform (i.e. $u_i = y_i$) domains (see Fig. 2). By keeping the autocovariance matrix of input data $\{x_i\}$ unchanged we ensure no influence on the effectiveness of U transformation. In turn the preservation of autocovariance matrix for y_i vectors would not, in particular, affect the value of the product of variances described by formula (4). Then it is possible to formulate the scheme of joint compression and encryption of data (see Fig. 4) where the encryption step can be embedded arbitrarily into the domains of input signal or U transform. The practical application of this scheme requires: to choose the domain of placement of the encryption stage, to operate in accordance with block quantization procedure, and to follow the steps of the proposed algorithm of data encryption.

The block quantization includes a step of entropy coding (c.f. Fig. 4). If we assume the entropy coding of the first order which operates on a random variable being a mixture of variables corresponding to each component $y(n)$ for $n = 0, 1, \ldots, N-1$, e.g. Huffman coding, then the stage of data encryption also does not affect the efficiency of entropy coding. This is due to the fact that the preservation of autocovariance matrix means, in particular, the preservation of variances of random variables. The distribution of random variables would always be Gaussian on the basis of the central limit theorem [38]. The expected values of random variables which are zeros would also be unchanged. Thus, the encryption step does not alter the values of parameters of random variables which are important from the point of view of entropy coding of the first order.



a. Scheme of joint compression and encryption.

b. Scheme of joint decryption and decompression.

Fig. 4. Scheme of joint compression and encryption of data

The stage of data decryption requires a scheme analogous to that depicted in Fig. 3. It is obvious that the ciphering matrices should be replaced by their inverses, i.e. $\{A_q^T\}$, and also the process of plain vectors mapping into blocks using $f(q,r)$ function should be reversed.

5. Experimental research

For experimental verification of the effectiveness of the proposed method we performed a series of experiments involving artificially generated model signals and natural images. The aim of the first part of research based on model signals was to experimentally confirm the lack of influence of the encryption stage on the effectiveness of block quantization with the first order entropy coding. In turn the second part involving natural images was performed in order to examine the possible impact of the proposed encryption scheme on the effectiveness of JPEG compression standard. It should be noted that in JPEG standard, although it is based on block quantization, the process of entropy coding is realized in a different way, which is not the first order entropy coding. The JPEG standard, except from Huffman codes, also exploits run length encoding (RLE) of sequences of zeroed AC coefficients obtained after quantization. As a consequence, the degradation of compression performance is expected.

In the first experiment as a model of input signal we adopted first order stationary Gauss-Markov process [6] with fixed variation and correlation coefficient $\rho = 0.9$. The variance was chosen to give entropy of the signal at the level of 8 bits per sample (bps). The input signal was compressed with the aid of joint compression and encryption scheme from Fig. 4 together with the step of first order entropy coding. The encryption step was embedded in U transform domain. As ciphering transforms we exploited FPOTs of the computational structure depicted in Fig. 1. Representative results for a number of $M = 8000$ input vectors and $N = 8$ point transformation are presented in Fig. 5. On the vertical axis we marked the values of relative MSE of signal reconstruction expressed in the percentage of energy of

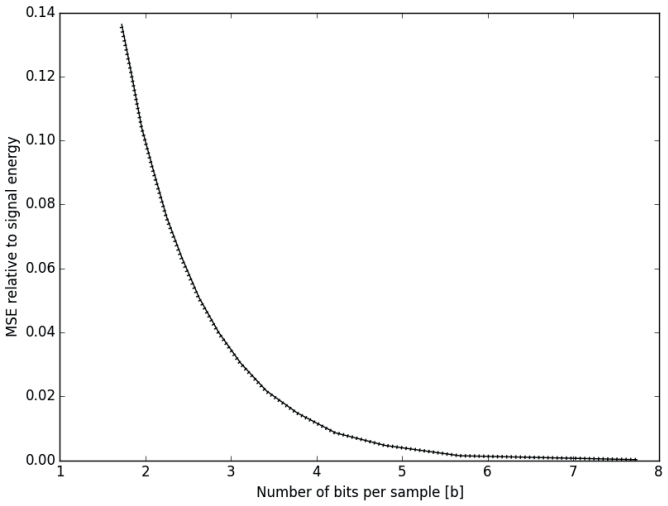


Fig. 5. Results in compression of model signal without encryption (solid line) and with encryption (dotted line)

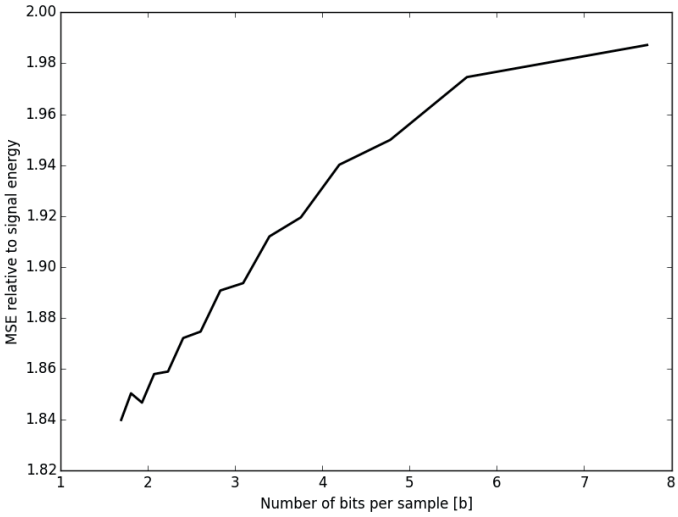


Fig. 6. The average value of relative MSE obtained in the case of signal reconstruction without knowledge of ciphering matrices

input signal. The horizontal axis holds the values of entropy of output signal expressed in bits per sample. The presented plots show results for compression without encryption (solid line) and joint compression with encryption (dotted line).

It should be noted that both plots from Fig. 5 strictly overlap. Based on this observation it can be concluded that the encryption process performed in accordance with the proposed encryption scheme had no affect on the effectiveness of data compression.

The second experiment involving model signals concerned the verification of the effectiveness of encryption method. In order to do it we executed a number of 1000 tests using constant ciphering matrices while deciphering matrices were randomized (simulation of exhaustive attack). The obtained results in a form of average value of relative MSE, i.e. calculated in relation to the total energy of signal, in a function of a number of bits per sample are given in Fig. 6.

The results of this experiment (see Fig. 6) are typical for orthogonal transforms [34]. The average value of relative MSE of signal reconstruction in the case of unknown ciphering matrices was approximately twice the signal energy (it ranged from 1.84 to 1.99 of signal energy). Such values of MSE of signal reconstruction can be considered as a high level of data concealment.

The second part of the study was concentrated on joint compression and encryption of natural images (see Fig. 7). For this

Lena image Baboon image

Fig. 7. Exemplary natural images in grayscale

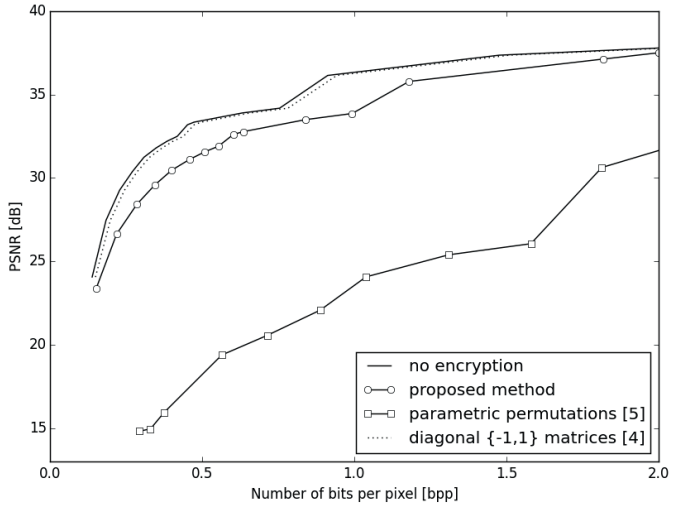


Fig. 8. Comparative results for joint compression and encryption of Lena.bmp image

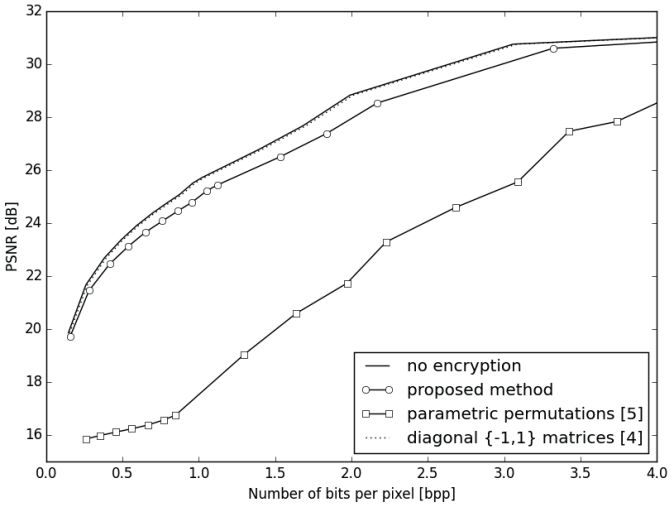


Fig. 9. Comparative results for joint compression and encryption of Baboon.bmp image

purpose, and comparison purposes, the proposed method of data encryption as well as methods presented in papers [4] and [5] were built into JPEG standard. In the case of the proposed method each block of plain vectors was composed of 64 vectors of coefficients of two-dimensional DCT which were calculated for separate 8 on 8 pixel areas of an image (according to JPEG standard specification). Hence, the sequences of coefficients of two-dimensional DCT calculated for such image areas allowed to create 64-element plain vectors. As ciphering transforms A_q we used 64-point FPOTs with computational structures from Fig. 1. The results for this experiment in the form of peak signal

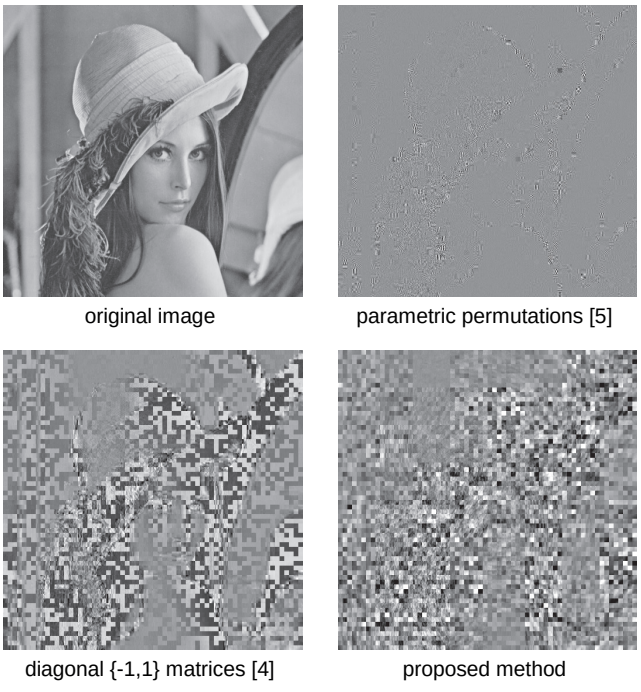


Fig. 10. Examples of image reconstruction in the case of unknown lists of ciphering matrices

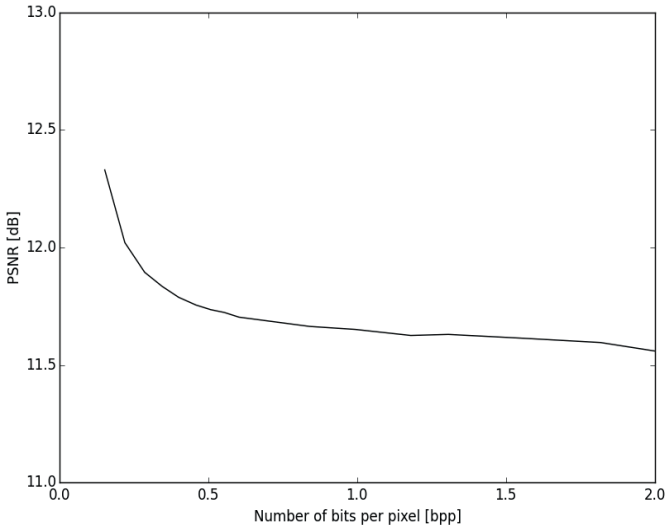


Fig. 11. The averaged PSNR values of the reconstruction of Lena.bmp image obtained for the proposed method at various levels of image compression in the case of unknown list of ciphering matrices

to noise ratios (PSNR) [6] expressed as a function of a number of bits per pixel (bpp) are shown Figs. 8 and 9.

An analysis of results shows relatively small impact of the encryption stage on the efficiency of JPEG compression in the case of the proposed method. The decrease of compression efficiency is fully expected due to the hybrid entropy coding (Huffman coding and RLE of zeroed AC coefficients) exploited in JPEG standard. For Lena.bmp image average lengths of sequences of zeroed AC coefficients equaled 12.84 and 9.26 for no-encryption and encryption scenarios respectively. The corresponding values for Baboon.bmp image equaled 4.87 and 4.32. Shorter sequences of zeroed AC coefficients explain the observed decrease in compression efficiency. It should be noted that for the data encryption method from [4] the obtained results are almost identical to those obtained for no-encryption case

(plots with dotted line). In turn for the method [5] we could record much higher decrease in compression efficiency (solid line with square markers) for both test images.

In Fig. 10 we present the results in decryption of Lena.bmp image in the case of uknown list of ciphering matrices for all three compared methods. Based on subjective evaluation it can be concluded that the proposed data encryption method allows to obtain images affected to the highest extent. It means that the proposed method conceals the content of encrypted image in the highest degree among the considered methods.

In turn Fig. 11 shows PSNR results of Lena.bmp image reconstruction at various levels of compression in the case of the proposed method when the list of ciphering matrices was guessed randomly. This experiment once again can be treated as the simulation of exhaustive attack. The obtained results were averaged over a number of 1000 trials. As it can be easily seen, the averaged values of PSNR are at very low level and range from 11.5 to 12.5 dB. Hence, it can be concluded that the proposed method has good properties of image content concealment in the case of exhaustive attacks.

6. Analysis of security and computational efficiency of the proposed method

Analysis of the proposed method in terms of security and computational efficiency is crucial from the point of view of its practical applications. In this section we consider various types of popular attacks performed on the basis of plain data or ciphertext together with the security analysis of the proposed method in the context of such attacks. The computational efficiency of the proposed method is also discussed in detail.

6.1. Security analysis. As it was already mentioned the visual data have a lower value than financial or military ones. For this reason the safety requirements for data encryption methods are proportionally lower. This does not mean, however, that visual data should not be protected but the degree of security must be maintained at the level adequate to its significance. In the considered case it means that an attempt to break the cipher must be more expensive than the value of data itself.

Among known types of cryptanalytic attacks we consider in the first place those which operate on plain data. The proposed method is a linear technique and as such it is not resistant to this type of attacks. However, in the case of visual data, e.g. digital television broadcasts, it can be assumed that access to the source of data transmission in order to inject prepared content can be very difficult or even impossible. If such form of attacks is practically feasible it is possible to increase the level of security by modifying the cipher key frequently enough what in the case of the proposed method corresponds to the frequent modification of the list of ciphering matrices $\{A_q\}$.

Another type of intrusion are exhaustive attacks which consist in checking all possible combinations of ciphering keys. For the proposed method the size of a private key equals $\mathscr{L}_{KEY} = \mathscr{L}_B \mathscr{L}_{PAR}$ bits, where $\mathscr{L}_B$ is a number of bits per parameter. In paper [34], we proposed an effective way of mapping of private key bits to the values of transform parameters. It consists in dividing for each parameter an interval of angle variation (from 0 to 2π radians) into a number of $2^{\mathscr{L}_B}$ subintervals of equal lengths $2\pi/2^{\mathscr{L}_B}$. Then the value of parameter is calculated on the basis of a number of $\mathscr{L}_B$ bits of a private key assigned to it. Those bits represent in a natural code an integer number by which constant $2\pi/2^{\mathscr{L}_B}$ must be multiplied. If we assume such way of coding of parameter values and also consider FPOT with the computational structure from Fig. 1 it can be calculated that a number of possible private keys, e.g., for $N = 64$ and $\mathscr{L}_B = 2$, would be as high as $\mathscr{L}_{KEY} = 2^2 \frac{64}{2}(2\log_2 64 - 1) = 2^{1408} > 10^{423}$. In addition, in this paper (see Fig. 6, 11) and also in paper [34] it was shown experimentally that the values of relative MSE of signal reconstruction in the case of random guessing of a private key are very high. Also the probability of random generation of a key which is close to a given one in the sense of Hamming distance is very low (cf. paper [34]). In the view of the above, we can consider this type of attacks to be highly inefficient.

The remaining and far more feasible forms of attacks are based on ciphertext. It means that for such methods it would be enough to know only encrypted data which in the case of video transmissions can be freely accessible. In the literature [7, 22] several cryptanalytic methods which are tuned to the selected encryption algorithms were formulated. We mean here the encryption algorithms that modify the signs of DC coefficients [4], permute DCT coefficients [5], or consist in modification of the tables of Huffman codes. For the first of the listed algorithms it was proved in paper [22] that such encryption method is a variant of Vinegenèr cipher and can be cracked solely on the basis of known distribution of DC coefficients. Similarly permutations of DCT coefficients are subject to relatively easy cryptanalysis based on the knowledge of typical for natural images distribution of their variances which was proved in paper [7]. In addition the techniques that modify Huffman tables of codes are vulnerable to attacks based on similar statistics (see [22]). Since the proposed method does not change the statistical characteristics of the signal nor modify the Huffman tables of codes, then it is obvious that the mentioned cryptanalytic attacks would be ineffective here.

The latest cryptanalytic method based solely on ciphered data is the Non-Zero-Counting Attack (NZCA) technique formulated in paper [23]. This method is effective for encryption algorithms operating only in DCT domain. Its main advantage is versatility and the lack of knowledge of the encryption method. The principle of operation of NZCA is very simple and is based on counting a number of non-zero AC coefficients in DCT domain for each 8 on 8 pixel area of an image. Then, on the basis of that number and with aid of simple thresholding rules black or white colour is assigned back to the same area. Although this method does not allow for an exact reconstruction of plain image the obtained result in a form of binary image with eightfold reduced horizontal and vertical resolution usually allows to recognize the basic content (see Fig. 12). In paper [23] authors also provide several important hints which allow to design an encryption algorithm that is resistant to NZCA. Such algorithm should operate in a global sense, i.e.

regarding the whole image, by swapping between each other, image areas of sizes 8 on 8 pixels. The proposed method meets this requirement. Here, the areas are not only swapped but also mixed in the sense of orthogonal linear combinations. In Fig. 12 we present results of NZCA on Lena.bmp image encrypted with the proposed method and method from paper [5]. The content of an image encoded with the proposed method is entirely illegible. The visible square areas with sizes of 64 on 64 pixels result from the way of mapping data vectors into blocks. Here, the mapping took a simple form, i.e. the coefficients coming from neighboring 8 on 8 pixel areas formed 64-element plain vectors. It is well-know that such mapping may be arbitrary in accordance with the definition of the proposed method.

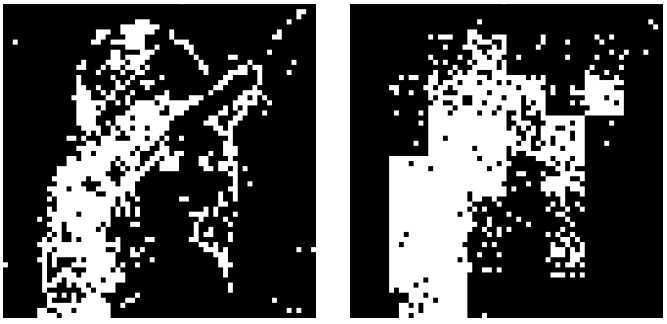


Fig. 12. NZCA on Lena.bmp image encrypted with parametric permutations [5] and the proposed method

6.2. Analysis of computational complexity. The computational complexity of the proposed method is strictly dependent on the complexities of encrypting transforms A_q. If in place of A_q matrices we take transforms described by the structures of FPOTs than the resulting computational complexity related to a single data vector would be of order $O(N\log_2 N)$. It is also obvious that in the general case the calculation of FPOT would require floating point additions and multiplications with a number of the same order. Then by comparing the proposed method with methods from [4] and [5], which in turn require $O(N)$ sign changes and $O(N\log_2 N)$ simple swaps of elements, it would turn out that the proposed approach has higher computational complexity. However, it should be noted that FPOTs have computational structures convenient for hardware implementations in ASIC or FPGA circuits, including mass-parallel and pipeline-parallel realizations. In addition, if the computational structure of FPOT is also a structure of the fast algorithm of DCT (the structure from Fig. 1 with proper values of parameters allows for fast calculation of DCT [39]) then it would possible to calculate DCT as well as ciphering transforms A_q with aid of the same hardware implementation. Hence, the proposed method still allows to construct computationally efficient systems of joint compression and encryption of data at potentially lower costs than in the case of hardware implementations of conventional data encryption algorithms, i.e. IDEA, DES, 3DES, AES, etc.

7. Summary and conclusions

In this paper the authors propose a novel method of joint compression and encryption of visual data, i.e. static images and video sequences. The method is designed to extend existing data compression standards for: static images (e.g. JPEG), sequences of images (e.g. MJPEG) or video sequences (e.g. MPEG). In the proposed approach the encryption of data is realized with aid of fast parametric orthogonal transforms, while the compression stage uses well-known scheme of block quantization with an additional step of entropy coding. It was shown in the paper that:

- in the case of the proposed method, the stage of data encryption does not affect the effectiveness of data compression in the case of entropy coding of the first order (e.g. using Huffman coding). This property allows to formulate the concept of *secure block quantization*;
- application of the proposed method in connection with JPEG standard results in relatively small impact on the effectiveness of compression, while the obtained level of image content concealment is high, i.e. visually higher than for comparable techniques based on orthogonal transforms (see [4, 5]).

Moreover, the proposed method extends existing techniques of visual data encryption [4, 5] to the case of parametric transforms of arbitrary shapes. This gives an immediate profit in the form of higher combinatorial complexity of the method.

In this paper the authors also concerned the security aspects of the method with respect to existing types of cryptanalytic attacks. It was shown that the proposed method is resistant to the types of attacks known for visual data encryption algorithms including the most effective NZCA [23]. In addition, the proposed method can be characterized as computationally highly effective since it allows to use fast parametric transforms at the stage of data encryption. In particular, it is possible to use the same hardware implementations for compression and encryption of data. Moreover, the encryption stage can be embedded directly into the domain of input signal, which is also a novelty in the case of visual data encryption algorithms.

In the view of presented results and discussion, we conclude that the proposed approach meets the requirements for this class of algorithms and hence, it can be successfully used in practical applications of compression and encryption of visual data with the compliance to existing standards, i.e. JPEG, MJPEG, or MPEG.

Appendix A. Proof of the Theorem

According to the initial assumptions of the theorem the set of plain vectors is divided into M/N non-overlapping blocks $u_{f(q,r)}$. Each block is indexed by $q = 0, 1, \ldots, M/N - 1$ and holds a number of N vectors for $r = 0, 1, \ldots, N - 1$. At the beginning we describe vectors obtained after the first step of intra-block mixing with respect to plain vectors, i.e. $\overline{u}_{f(q,r)}(k) = u_{f(q,k)}(r)$ for $q = 0, 1, \ldots, M/N - 1$ and $r, k = 0, 1, \ldots, N - 1$. It is possible to describe the relation between vectors $v_{f(q,r)}$ and $\overline{u}_{f(q,r)}$ in

the same way. It takes form: $v_{f(q,r)}(k) = \overline{v}_{f(q,k)}(r)$. Naturally vectors $\overline{v}_{f(q,r)}$ appear as the result of multiplication of matrix A_q by vectors $\overline{v}_{f(q,r)}$. Hence, we can write:

$$\overline{v}_{f(q,r)}(k) = \sum_{n=0}^{N-1} A_q(k,n)\overline{u}_{f(q,r)}(n).$$

By combining given expressions we have:

$$v_{f(q,r)}(k) = \sum_{n=0}^{N-1} A_q(r,n)u_{f(q,n)}(k). \tag{5}$$

It should be note that for the given division of vectors into blocks the autocovariance matrices for plain and encrypted vectors can be defined as:

$$\begin{aligned} R_{uu} &\triangleq \frac{1}{M}\sum_{i=0}^{M-1} u_i u_i^T = \frac{1}{M}\sum_{q=0}^{M/N-1}\sum_{r=0}^{N-1} u_{f(q,r)}u_{f(q,r)}^T, \\ R_{vv} &\triangleq \frac{1}{M}\sum_{i=0}^{M-1} v_i v_i^T = \frac{1}{M}\sum_{q=0}^{M/N-1}\sum_{r=0}^{N-1} v_{f(q,r)}v_{f(q,r)}^T. \end{aligned} \tag{6}$$

In accordance with definition (6) the elements of autocovariance matrices R_{uu} and R_{vv} can be calculated as:

$$R_{uu}(k,l) = \frac{1}{M}\sum_{q=0}^{\frac{M}{N}-1}\sum_{r=0}^{N-1} u_{f(q,r)}(k)u_{f(q,r)}(l) \tag{7}$$

for $k, l = 0, 1, \ldots, N-1$ and as:

$$R_{vv}(k,l) = \frac{1}{M}\sum_{q=0}^{\frac{M}{N}-1}\sum_{r=0}^{N-1} v_{f(q,r)}(k)v_{f(q,r)}(l) \tag{8}$$

for $k, l = 0, 1, \ldots, N-1$ respectively. Then substituting expression (5) into formula (8) we have:

$$\begin{aligned} R_{vv}(k,l) &= \frac{1}{M}\sum_{q=0}^{\frac{M}{N}-1}\sum_{r=0}^{N-1}\left(\sum_{n=0}^{N-1} A_q(r,n)u_{f(q,n)}(k)\right)\cdot \\ &\left(\sum_{m=0}^{N-1} A_q(r,m)u_{f(q,m)}(l)\right) = \\ &= \frac{1}{M}\sum_{q=0}^{\frac{M}{N}-1}\sum_{n=0}^{N-1}\sum_{m=0}^{N-1}\left(\sum_{r=0}^{N-1} A_q(r,n)A_q(r,m)\right)\cdot \\ &u_{f(q,n)}(k)u_{f(q,m)}(l). \end{aligned} \tag{9}$$

On the basis of the orthogonality properties of ciphering matrices we may observe that the sum: $\sum_{r=0}^{N-1} A_q(r,n)A_q(r,m)$ equals 1 for $m = n$ and 0 in other cases. Now by taking this into account we may rewrite formula (9) as:

$$R_{vv}(k,l) = \frac{1}{M}\sum_{q=0}^{\frac{M}{N}-1}\sum_{n=0}^{N-1} u_{f(q,n)}(k)u_{f(q,n)}(l) = R_{uu}(k,l). \tag{10}$$

From expression (10) it results immediately that elements $R_{vv}(k, l)$ for $k, l = 0, 1, \ldots, N-1$ of autocovariance matrix R_{vv} are equal to the corresponding elements $R_{uu}(k, l)$ of autocovariance matrix R_{uu}.□

References

[1] J. Katz and Y. Lindell, "Introduction to Modern Cryptography: Principles and Protocols", *Chapman and Hall/CRC*, (2007).
[2] Y. Zhou, K. Panetta, and S. Agaian, "Image Encryption Using Discrete Parametric Cosine Transform", *Conf. Signals, Systems and Computers*, 395–399 (2009).
[3] M.V. Malakooti and M.R.N. Dobuneh, "A Lossless Digital Encryption System for Multimedia Using Orthogonal Transforms", *2nd Inter. Conf. Digital Information and Comm. Tech. and App. (DICTAP)*, 240–244 (2012).
[4] B. Bhargava, Ch. Shi, and Sh.Y. Wang, "MPEG Video Encryption Algorithms", *Multimedia Tools and App.*, 24 (1), 57–79 (2004).
[5] L. Tang, "Methods For Encrypting And Decrypting MPEG Video Data Efficiently", *ACM Multimedia, ACM Press*, 219–229 (1996).
[6] D.R. Rao and P. Yip, "Discrete Cosine Transform", *San Diego, CA: Academic*, (1990).
[7] L. Qiao and K. Nahrstedt, "Comparison of MPEG Encryption Algorithms", *Int. Journal on Computer and Graphics*, 22 (3), (1998).
[8] C. Kailasanathan and R.S. Naini, "Compression Performance of JPEG Encryption Scheme", *14th Int. Conf. on Digital Signal Processing*, 2, 1329–1332 (2002).
[9] R. Ridzoˇn, D. Levický, and T. Kanócz, "Information Hiding Within Still Images Based on the DCT Coefficients Flipping and Encryption", *52nd Inter. Symposium ELMAR-2010*, 147–150 (2010).
[10] F. Wang and S. Bai, "JPEG Image Encryption By Shuffling DCT Coefficients In Defined Block", *Inter. Conf. on Computational and Information Sciences*, 60–63 (2013).
[11] M.M. Fisch, H. Stögner, and A. Uhl, "Layered Encryption Techniques For DCT-Coded Visual Data", *12th European Signal Processing Conference*, 821–824 (2004).
[12] W. Puech and J.M. Rodrigues, "Crypto-Compression of Medical Images by Selective Encryption of DCT", *13th European Signal Processing Conference*, (2005).
[13] M.I. Khan, V. Jeoti, and M.A. Khan, "Perceptual Encryption of JPEG Compressed Images Using DCT Coefficients and Splitting of DC Coefficients into Bitplanes", *Inter. Conference on Intelligent and Advanced Systems*, 1–6 (2010).
[14] M.I. Khan, V. Jeoti, A.S. Malik, and M.F. Khan, "A Joint Watermarking And Encryption Scheme For DCT Based Codecs", *17th Asia-Pacific Conf. on Communications*, 816–820 (2011).
[15] Y. Liang, K. Guo, and J. Li, "An Improved Video Encryption Method Design", *10th Inter. Computer Conference on Wavelet Active Media Technology and Information Processing*, 95–99 (2013).
[16] C.N. Raju, K. Srinathan, and C.V. Jawahar, "A Real-Time Video Encryption Exploiting the Distribution of the DCT Coefficients", *IEEE Region 10 Conf.* 2008, 1–6 (2008).
[17] H. Seddik and E.B. Braiek, "Image Securing Based Chaotic Encryption Coupled With DCT Robust Watermarking", *Inter. Conference on Electrical Engineering and Software Applications*, 1–6 (2013).

[18] F. Ahmed, M.Y. Siyal, and V.U. Abbas, "A Perceptually Scalable and JPEG Compression Tolerant Image Encryption Scheme", *4th Pacific-Rim Symposium on Image and Video Technology*, 232–238 (2010).
[19] Y. Fengxia, "DCT Domain Color Image Block Encryption Algorithm based on Three-dimensional Arnold Mapping", *Inter. Conference on Computational and Information Sciences*, 682–685 (2013).
[20] D. Huffman, "A Method for the Construction of Minimum- Redundancy Codes", *Proceedings of the IRE* 40(9), 1098–1101 (1952).
[21] S. Auer, A. Bliem, D. Engel, A. Uhl, and A. Unterweger, "Bitstream-based JPEG Encryption in Real-time", *Inter. Journal of Digital Crime and Forensics*, 5 (3), 1–14 (2013).
[22] T.E. Seidel, D. Socek, and M. Šrámka, "Cryptoanalysis of Video Encryption Algorithms", *Tatra Mountains Mathematical Publication*s, 29, 79–87 (2004).
[23] W. Li and Y. Yuan, "A leak and its remedy in JPEG image encryption", *Inter. Journal of Computer Mathematics*, 84(9), 1367–1378 (2007).
[24] S. Agaian, K. Tourshan, and J. P. Noonan, "Parametric Slant- Hadamard transforms with applications", *IEEE Signal Processing Letters*, 9(11), 375–377 (2002).
[25] S. Minasyan, J. Astola, and D. Guevorkian, "On unified architectures for synthesizing and implementation of fast parametric transforms", *Proc. 5th Inter. Conference on Information, Communications and Signal Processing*, 710–714 (2005).
[26] S. Bouguezel, M. O. Ahmad, and M. N. S. Swamy, "New parametric Fourier and Hartley transforms, and algorithms for fast computation", *IEEE Trans. Circuits Systems*, 58(3), 562–575 (2011).
[27] M. Morháč and V. Matoušek, "Data compression using new fast adaptive cosine-Haar transforms", *Elsevier Digital Signal Processing Journal*, 8(2), 63–81 (1998).
[28] B. Stasiak and M. Yatsymirskyy, "Fast Orthogonal Neural Networks", *Lecture Notes in Computer Science, Artificial Intelligence and Soft Computing ICAISC 2006*, 4029, 142–149 (2006).
[29] D. Puchala and M. Yastymirskyy, "Fast parametrized biorthogonal transforms", *Electrical Review*, 88(4a), 123–125 (2012).
[30] D. Puchala and M. Yastymirskyy, "Fast Parametrized Biorthogonal Transforms With Normalized Basis Vectors", Electrical Review, 89(3a), *277–279 (*2013).
[31] J. Stolarek, "Adaptive synthesis of a wavelet transform using fast neural network", *Bull. Pol. Ac.: Tech., 59*, 9–13 (2011).
[32] P. Lipinski, "Robust digital watermarks in images. Adaptive selection of embedding domain", *Warsaw: EXIT, Academic Publishing House*, (2013), (in Polish).
[33] V.E. Beneˇs, "Mathematical Theory of Connecting Networks and Telephone Traffic", *Academic Press*, (1965).
[34] D. Puchala and K. Stokfiszewski, "Parametrized Orthogonal Transforms For Data Encryption", *Computational Problems of Electrical Engineering*, 3 (1), (2013).
[35] H.P. Kramer and M.V. Mathews, "A linear coding for transmitting a set of correlated signals", *IRE Transactions on Information Theory*, IT-2, 41–46 (1956).
[36] R.M. Gray and D.L. Neuhoff, "Quantization", *IEEE Trans. Inform. Theory*, 44(6), 2325–2383 (1998).
[37] J.J.Y. Huang and P.M. Schultheiss, "Block Quantization of Correlated Gaussian Random Variables", *IEEE Trans. On Communications Systems*, 289–296 (1963).
[38] A. Papoulis, "Probability and statistics", *Prentice Hall*, (1989).
[39] M.M. Jacymirski and D. Puchala, "Fast Time-Decimated Algorithms of One-Dimensional Discrete Cosine and Sine Transforms of Type II and Type IV", *Modeling and Information Technologies*, 27, 137–148 (2004).