Annales UMCS Informatica AI VIII, 2 (2008) 61–73
DOI: 10.2478/v10065-008-0025-1

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

New steerable pyramid steganography algorithm resistant to the Fisher Linear Discriminant steganalysis

Piotr Kopniak*

Institute of Computer Science, Lublin University of Technology,
ul. Nadbystrzycka 36b, 20-618 Lublin, Poland

Abstract

This paper describes a new steganography algorithm based on a steerable pyramid transform of a digital image and the steganalysis of the existence of secret messages hidden by this new method. The data embedding process uses the elements of a Lee and Chen steganography algorithm which is adapted to the steerable pyramid transform domain. This article describes the Fisher Linear Disriminant (FLD) analysis and its steganalysis application, too. The main part of the paper is the description of the conducted research and the results of FLD steganalysis of stegoimages produced by the new steganography algorithm.

1. Introduction

Steganography is a modern and dynamically developing part of information security which protects information by its hidding. Secure communication with steganography has been known since ancient times when slaves' heads were shaved and tatooed to hide some information [**1, 2**]. When the hair grew up, the message could be delivered. Today steganography has got many different ways to hide information.

* *e-mail address:* p.kopniak@pollub.pl

Almost all communication channels are digital and many different kinds of data are saved in a digital form i.e.: music, pictures and movies. Digital recording has very useful features for steganography. The first of them is high quality which assures that the information may be equally reconstructed even when it is partially destructed during transmission. The second one is a high time unvariability, even if the digital media were played many times. And, finally, digital data in many cases are redundant, i.e. wave music consists of frequencies not heard to human ear which is utilised during *mp3* compression. The redundant data may be replaced by secret information using the steganography algorithm, too.

Our research is concentrated on developing the most secure and efficient steganography method [**3, 4, 5, 6**] with digital image as a cover of the secret information. To reach this purpose, we have prepared a new steganography algorithm which hides data into digital images. This algorithm was developed during the research done for the PhD dissertation [**7**] and was described there in more detail. This algorithm possesses interesting features e.g. low cover image destruction and resistance to statistical steganalysis with *Fisher Linear Discriminant*.

2. Steerable pyramid transformation

The proposed stego-algorithm is based on a steerable pyramid transformation of a digital image [**8, 9, 10**]. In this linear multiresolution the image decomposition is subdivided into a collection of subbands localised in scale and orientation. The subbands have octave bandwidth and orientation bandwidth of $2\pi/m$ where m is an integer. Each next scale level is computed recursively using convolution and decimation operations.

This transform has some advantages compared to the wavelet transform which is the most known and frequently used method of multiresolution decomposition. The advantages of this representation are that [**10**]:

1. Subbands are translation– and rotation–invariant,
2. Subbands on each scale level are localised in many orientations (up to 85 with transform implementation used for our research),
3. No aliasing in transformation subbands so the subband coefficients are not altered,
4. Overcompletness which gives more space for information hidding and requires more time to extract the hidden data.

The steerable pyramid diagram is shown in Fig. 1a. The filters constructing the steerable pyramid are represented as rectangular blocks. Blocks with the symbol H represent non–oriented highpass filters, blocks with the symbol

L lowpass filters (L_1 are the narrowband filters) and blocks with the sybmol B bandpass filters. The diagram represents the first scale level of the decomposition only. We can get higher scale levels of the decomposition after the recursive including the dashed line around the part of the diagram into the extension point where the input image is after lowpass filtering and decimation. The recursion constraint is:

$$|L_1(\omega/2)|^2 = |L_1(\omega/2)|^2 \left(|L_1(\omega)|^2 + |B(\omega)|^2\right).$$

We can describe the system response in the frequency domain as follows:

$$\hat{X}\left(\overrightarrow{\omega}\right) = \left\{ |H_0\left(\overrightarrow{\omega}\right)|^2 + |L_0\left(\overrightarrow{\omega}\right)|^2 \left(|L_1\left(\overrightarrow{\omega}\right)|^2 + \sum_{k=0}^{n} |B_k\left(\omega\right)|^2 \right) \right\} X\left(\overrightarrow{\omega}\right) + a,$$

where a indicates the aliasing term which is eliminated by L_1 filter. This elimination is achieved thanks to that $L_1(\omega) = 0$ for $|\omega| > \pi/2$.

The decomposition subbands are polar–separable in the Fourier domain. The frequency tiling of the single stage for two of the badbass filters are shown in the Fourier magnitude spectrum in Fig. 1b. The subbands of the two–level and four–direction transform of the sample image are shown in Fig. 1c.

The bandpass filters of the transformation are highly constrained. Their Fourier transform radial component must obey a recursive system diagram requirement and the angular component is constrained by the property of *steerability* [**11**]. The steerability term means that we can synthesize any direction filter by linear combination of a few basis filters. Each filter from the basis is a rotated copy of each other.

In our case, the steerable basis is a set of $n+1$ nth–order directional derivatives of a circular symmetric function. The Fourier magnitude of the i–th oriented bandpass filter can be written in the polar–separable form:

$$B_i\left(\overrightarrow{\omega}\right) = A\left(\theta - \theta_i\right) B\left(\omega\right),$$

where $\theta = \tan^{-1}\left(\omega_y/\omega_x\right)$, $\theta_i = 2\pi/m$ and $\omega = |\overrightarrow{\omega}|$.

A directional derivative operation in the spatial domain corresponds to the multiplication by a linear ramp function in the frequency domain. We can write a derivative operator in the x direction in the polar coordinates as follows:

$$-j\omega_x = -j\omega\cos\left(\theta\right).$$

As the factor ω is reduced by a radial portion of the function derivative operator is thus $\cos\left(\theta\right)$. We can get higher order directional derivatives by multiplication a ramp raised to a power and the angular portion of the filter is $\cos\left(\theta\right)^n$, where n is the order of the derivative.

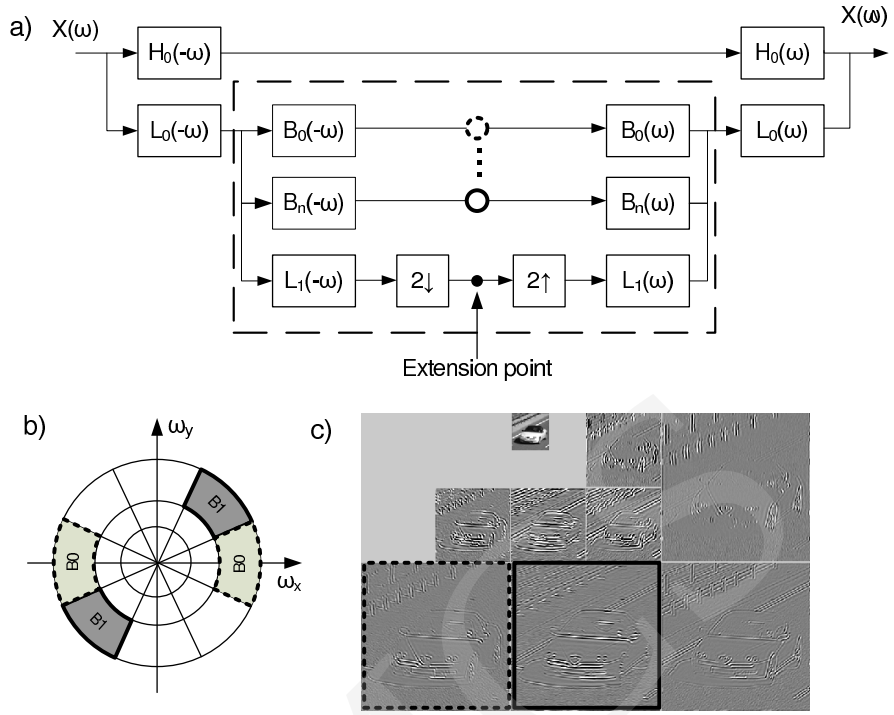

Fig. 1. Steerable pyramid transform: a) – the transformation filter structure, b) – the Fourier magnitude spectum with marked frequencies passed by the filters B_0 and B_1, c) – two levels of a sample image decomposition with four filtering directions

The steerable pyramid transform has another important feature for steganography. This is a flat system response, which can be described response as follows:

$$|H_0(\omega)|^2 + |L_0(\omega)|^2 \left(|L_1(\omega)|^2 + |B(\omega)|^2\right) = 1.$$

It means that the output image after the decomposition into subbands and reverse composition is the same as the input image.

3. Steganographic algorithm

Our steganographic algorithm is composed of a steerable transformation of the cover image and Lee and Chen steganography method [**12**] hidding secret message bits through the average values of image pixel blocks modification. The Lee and Chen algorithm was adapted to a new domain as can be seen in Fig. 2. The original method was prepared for grayscale images in the spatial domain. In our case some elements of this algorithm were used for *RGB* colour space images in the transform domain.

At the beginning of the steganography process the cover image is decomposed into a steerable pyramid transformation. The parameters of the transformation, i.e. the number of the scale decomposition levels and the number of different directions of image filtering are parts of stegokey which is needed to extract the hidden message. After that we get a set of different scale subbands and we can choose one to hide information in it. This is the first step shown in the algorithm diagram and the chosen subband index is the second part of the stegokey.

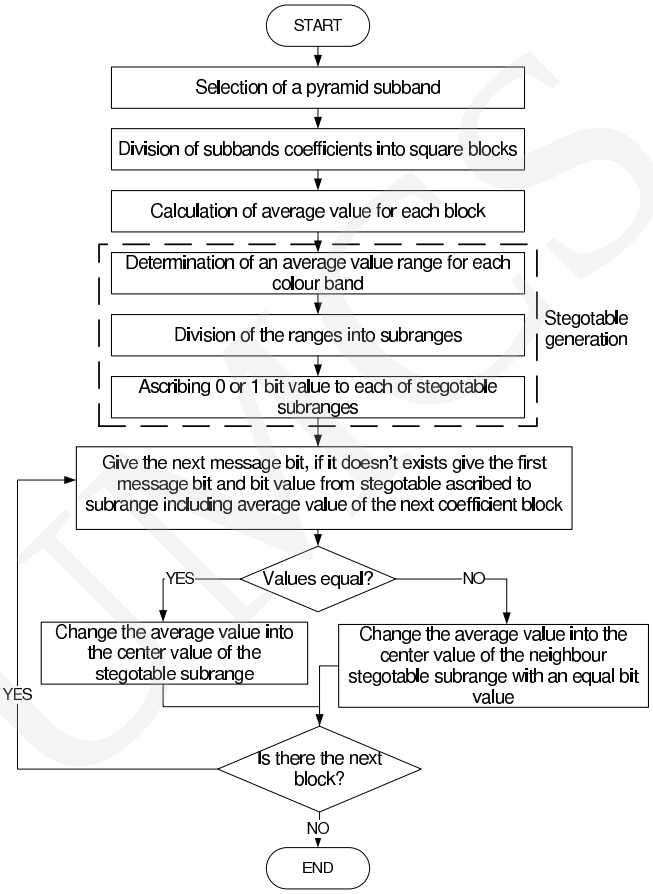

Fig. 2. Steganographic algorithm

The next coefficients of the subband are divided into equal size square blocks. The size of blocks is another part of the stegokey. The average value for each block is calculated and an algorithm begins the stegotable generation. A stegotable is a table of average value subranges covering all ranges of average values calculated for all blocks and pseudo random generated bit values ascribed to

them. The pseudo random generator's seed and number of subranges are the parts of the stegokey.

The final part of the algorithm is the message embedding. The average value for each coefficient block falls into one of the stegotable subranges and since then the block represents bit value ascribed to this subrange. If the next message bit which we want to hide in the block is equal to the value ascribed to this block, the algorithm modifies the average value into the center value of the stegotable subrange. If these values are different the algorithm changes the average value of the block to the center value of the neighbour stegotable subrange with the equal bit value. The hidden message is destruction resistant unless the average value is modified too much and remains in the same stegotable subrange.

The message is repeated many times during the hidding process to utilise all the coefficient blocks. If all the blocks are modified, the steganography process is harder to detect in a simple manner. The redundance is very important for the message extraction process, too, because the composition of the output image from many transform subbands made distortions into the average values of the coefficients. When the message is extracted by the message recipient, it is the averaged form of many instances to assure right extraction. The bit messages hidden in the three–colour band subbands are averaged, too. Thanks to that we get the simplest error correction based on the Hamming distance [**13**].

To assure the security of the secret information hidden into the image, the message is preprocessed by a bit permutation with a secret key which is the next part of the stegokey. The message may be encrypted and supplemented with the correction bits but it does not assure the steganographic security. By steganographic security we mean that the message remains undetectable. When the modification is detected by a steganaliser, he may try to destroy the embedded message or to stop the secret communication channel.

This new steganographic algorithm was tested with the RGB images of 256×256 pixels resolution and allows us to hide up to about 300 bits of secret information. The distortions made during the steganographic process are quite small $SNR \approx 39dB$ and in many cases lower those made by other steganographic tools like *EzStego* [**14**] or $F5$ [**15**]. The embedding methods result in the resistance of the hidden information (it must be short, about 70 bits) to $JPEG$ compression with a quality factor of 100%, too. It means that the input image is loss compressed with the ratio of 3:1 to 4:1 [**7**].

4. Fisher Linear Discriminant Steganalysis

Many steganalysis methods are built as the answers to the particular steganographic algorithms and they detect typical different steganography methods data modification [**16, 17, 18**]. We have developed a new information hidding algorithm. However the corresponding steganalysis method does not exist yet. If we want to test the hidden data security we must perform the blind steganalysis process (blind means that we do not know what steganographic technique was used). We should carry out blind steganalysis along with the statistical analysis because the information hidding disturbs the stastistics of the image [**18**].

Many steganalysis researchers believe that a good method for blind steganalysis was developed by Farid [**19, 20**]. This technique is based on *Fisher Linear Discriminant Analysis (FLD)* [**21**]. The Farid research shows that this algorithm is useful for steganalysis images stegoed by the classic steganography tools like *Jpeg-Jsteg* [**22**] and *OutGuess* [**23**].

The *FLD* algorithm classifies the objects into separate classes on the basis of their chosen features [**24**]. In the simplest case it recognises the objects belonging to two classes (Fig. 3).

The steganalysis target is to find that the particular image belongs to the class of stego–modified images or the class of untouched images. Classification features in the Farid's steganalysis method are higher–order image statistics.

At the beginning of the method, the statistic features from the training sets are collected. The first set includes the natural images set and the second modified ones. Then the algorithm looks for the deviation from these models to determine a threshold between two feature classes. Then this threshold is used to classify novel images.

As there exist strong high-order statistical regularities within a wavelet-like decomposition of natural images [**21**], the statistics are collected from the coefficients of the image decomposition with *Quadrature Mirror Filters (QMFs)* [**25, 26**]. The decomposition splits the frequency space of the image into multiple scales and three orientations: vertical, horizontal and diagonal.

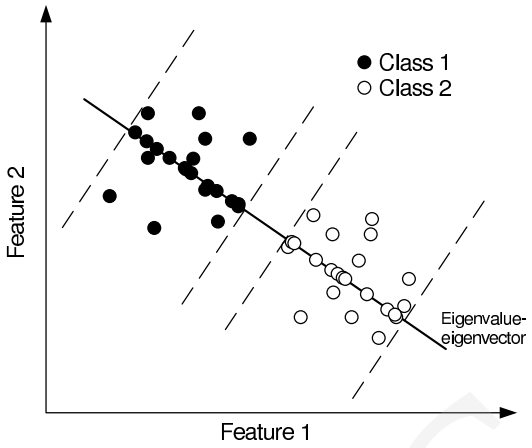

Fig. 3. Fisher Linear Discriminant analysis of the objects belonging to one of the two classes

The first statistic set is composed of mean, variance, skewness and kurtosis of subband coefficients at each scale and orientation. The second statistics set is based on errors in an optimal linear predictor of a coefficient value. The subband coefficients are corelated to their spatial and scale neighbours. This fact allows to construct a predictor for the magnitude of coefficients in a subset of neighbours. The predictors for vertical (V), horizontal (H) and diagonal (D) bands and scale i can be described as follows:

$$\begin{aligned} V_i(x,y) &= w_1 V_i(x-1,y) + w_2 V_i(x+1,y) + w_3 V_i(x,y-1) + w_4 V_i(x,y+1) \\ &\quad + w_5 V_{i-1}(x/2,y/2) + w_6 D_i(x,y) + w_7 D_{i-1}(x/2,y/2) \end{aligned}$$

$$\begin{aligned} V_i(x,y) &= w_1 H_i(x-1,y) + w_2 H_i(x+1,y) + w_3 H_i(x,y-1) + w_4 H_i(x,y+1) \\ &\quad + w_5 H_{i-1}(x/2,y/2) + w_6 D_i(x,y) + w_7 D_{i-1}(x/2,y/2) \end{aligned}$$

$$\begin{aligned} D_i(x,y) &= w_1 D_i(x-1,y) + w_2 D_i(x+1,y) + w_3 D_i(x,y-1) + w_4 D_i(x,y+1) \\ &\quad + w_5 D_{i-1}(x/2,y/2) + w_6 H_i(x,y) + w_7 V_i(x,y) \end{aligned}$$

We can express the predictor in a matrix form (example for the vertical band):

$$\vec{\boldsymbol{V}} = \boldsymbol{Q}\vec{w}.$$

The coefficients are determined by a minimizing quadrature error function:

$$E\left(\vec{\omega}\right) = \left[\vec{\boldsymbol{V}} - \boldsymbol{Q}\vec{w}\right].$$

This minimization is calculated by differentiating with respect to w, setting the result equal to zero:

$$\frac{dE\left(\vec{\omega}\right)}{d\vec{\omega}} = 2Q^T\left[\vec{\boldsymbol{V}} - \boldsymbol{Q}\vec{\omega}\right] = 0.$$

The solvation vector is:

$$\vec{\omega} = \left(\boldsymbol{Q}^T\boldsymbol{Q}\right)^{-1}\boldsymbol{Q}^T\vec{\boldsymbol{V}}$$

and the error in the linear predictor can be described as:

$$\vec{E} = \log_2\left(\vec{\boldsymbol{V}}\right) - \log_2\left(|\boldsymbol{Q}\vec{\omega}|\right).$$

The second set of statistics: mean, variance, skewness and kurtosis is collected from this linear prediction error. This calculation is performed for all decomposition subbands for all scales and orientations. These statistics are combined with the coefficient statistics and results with $24(n-1)$ statistics feature vector which is used for discrimination between classes.

When the features are collected fom two training sets, the FLD calssification process begins. At the beginning the classification algorithm calculates within–class means for the two classes from the testing sets. These means are defined as:

$$\vec{\mu}_x = \frac{1}{N_x}\sum_{i=1}^{N_x}\vec{x}_i, \qquad \text{and} \qquad \vec{\mu}_y = \frac{1}{N_y}\sum_{j=1}^{N_y}\vec{y}_j$$

where:$\vec{x}_i$, $i = 1,\ldots,N_x$ and $\vec{y}_j$, $j = 1,\ldots,N_y$ are the examples from the two classes in the training sets. The second step is the determination of between–class mean:

$$\vec{\mu} = \frac{1}{N_x + N_y}\left(\sum_{i=1}^{N_x}\vec{x}_i + \sum_{j=1}^{N_y}\vec{y}_j\right).$$

Then the within–class S_w and between–class S_b scater matrices are calculated:

$$S_w = M_x M_x^T + M_y M_y^T,$$
$$S_b = N_x\left(\mu_x - \mu\right)\left(\mu_x - \mu\right)^T + N_y\left(\mu_y - \mu\right)\left(\mu_y - \mu\right)^T$$

where: the i–th column of matrix M_x contains the zero–meaned ith example given by $\vec{x}_i - \vec{\mu}_x$. Similarly j–th column of matrix M_y is defined.

Let $\vec{e}$ be the maximal generalized eigenvalue–eigenvector of S_w and S_b. At the end the training examples are projected onto the one–dimensional linear subspace defined by $\vec{e}$ (i.e. $x_i^T e$ and $y_j^T e$). During this process the within–class scatter is minimized and the between–class scatter is maximized.

When the projection axis is determined, as can the seen in Fig. 3, a novel example from the testing set is classified by projection onto the same subspace (i.e. $\vec{z}^T\vec{e}$).

5. Research results

Farid in [**21**] describes the results of steganalysis with the two–class FLD. The steganalysis program was trained with the training set consisting of 1800 unmodified images cropped into 640×480 pixel area and random subset of the 1800 stegoed images with a varing message size and the same size. Steganography was performed with *Jsteg, OutGuess, EzStego* and by substitution of LSB. The classification accuracy for the tested tools and the message size 256×256 were quite large: 94% for the *Jsteg* stegoed images and 92.8% for *OutGuess* without statistical correction (option of the tool). For *EzStego* and LSB the message size was 194×194 and the accuracy was lower: 45.2% and 42.3% respectively.

In our case, the new steganography algorithm described above was tested by hidding binary messages within the RGB images of resolution 256×256. This type of stegoimage was used to verify steganalysis resistance, too.

Two training sets were prepared, too. The first of them included 400 untouched images and the second was the same set of images but modified steganographically. Different values of steganographic algorithm parameters were set during the preparation of the image set. For example, the number of stegotable subranges or the size of coefficient block used to hide one message bit.

Fig. 4. Sample images: a) – from the training set, b) – from the testing set

The testing group had 50 untouched images and 50 modified images of the same parameters like images from the training sets. The sources of the testing images were *FreeFoto* [**27**] web photobase and cropped center parts of pictures taken with the *Fuji FinePix 5500* digital camera. The examples of images are shown in Fig. 4.

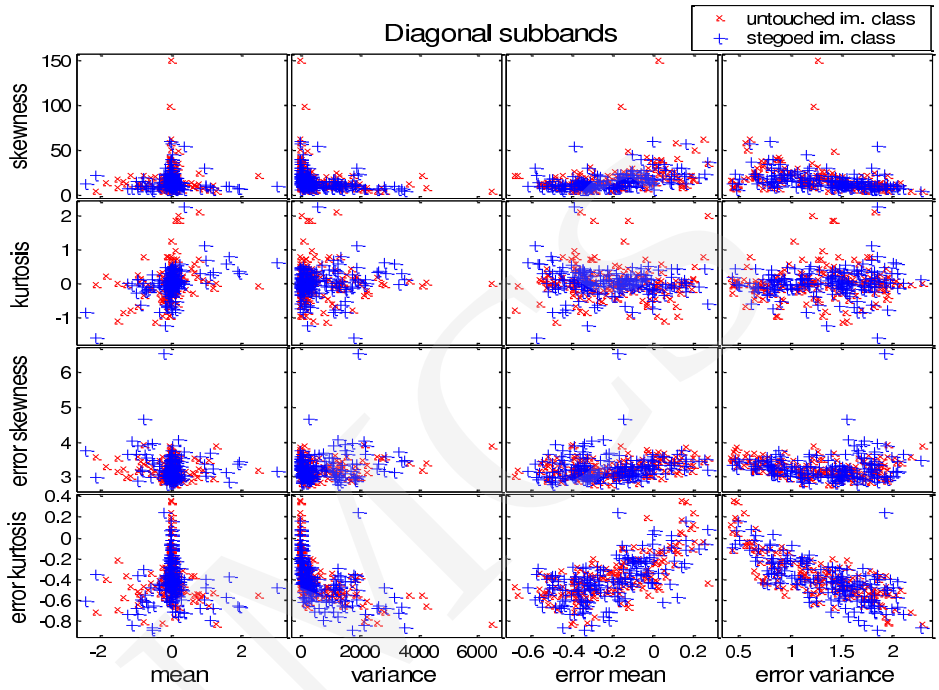

Fig. 5. Scatter plots of tested images from two classes: untouched image class and stegoed image class

The conducted steganalysis of images stegoed with the new stego–algorithm has shown that the Farid method with the mentioned assumptions (i.e. an image size and quantities of image sets) has not detected any steganographical modifications.

The result of the classification of stegoed images as the images after modification amounts to 0.67% of the tested images only and the result of the classification of untouched images as the images without modification amounts to 98.67% of the tested images. These very good results come from the fact that the features of images from both classes overlap which can be seen on the scatter plots in Fig. 5. It means that the right discrimination is impossible in this case.

6. Conclusions

We have developed a new steganographic method with a digital image as an information cover and based on a steerable pyramid transform. The information embedding part of the algorithm is a steganography method developed by Lee and Chen tailored to the transform domain. The new method hides about 300 bits of information into 256×256 size colour image with minimal cover image distortions ($SNR \approx 39dB$) and prevents from the resistance of short (about 70 bits) hidden messages to the JPEG compression with the quality factor 100% and noise adding [**7**].

This method is resistant to statistic steganalysis with FLD proposed by Farid. This fact results from a minimal data modification and an overlapping class of features taken from untouched and stegoed images.

Our future research will be concentrated on testing the FLD classification with larger image sets and the utilisation of different size covers. Different statistical steganalitic methods, for example Support Vector Machines (SVM) will be verified too.

References

[1] Davern P., Scott M., *Steganography: its history and its application to computer based data files*, Workomg Papers, CA-0795, School of Computing, Dublin City University (1995).

[2] Katzenbeisser S., Petitcolas F. - editors, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House (2000).

[3] Garbarczuk W., Świć A., *Podstawy ochrony informacji*, (a cooperation author of chapter 3 - Kopniak P.), Politechnika Lubelska, Lublin (2005).

[4] Kopniak P., *Porównanie odporności na zniekształcenia danych ukrytych w obrazie metodą LSB i metodą modyfikacji widma*, Algorytmy, metody i programy naukowe, Polskie Towarzystwo Informatyczne, Lublin (2004).

[5] Kopniak P., *Robustness of Data Hidding in Image Fourier Spectrum*, Annales UMCS-Informatica, Lublin (2006).

[6] Kopniak P., *Wykorzystanie transformacji obrazu do przestrzeni częstotliwościowej w steganografii*, VI Międzynarodowe Warsztaty Doktoranckie, OWD 2004 - Wisła, 16-19 października 2004, Archiwum Konferencji PTETiS, 19 (2004).

[7] Kopniak P., *Metody cyfrowego przetwarzania sygnałów na potrzeby steganologii komputerowej*, Politechnika Lubelska (2007).

[8] Freeman W. T., Adelson E. H., *The Design and Use of Steerable Filters*, IEEE Trans. Patt. Anal. and Machine Intell., 13(9) (1991) 891.

[9] Karasaridis A., Simoncelli E., *A Filter Design Technique for Steerable Pyramid Image Transforms*, Proc. ICASSP-96, May 7-10, Atlanta, GA (1996).

[10] Simoncelli E. P., Freeman W. T., *The Steerable Pyramid: A Flexible Architecture For Multi-Scale Derivative Computation*, 2nd IEEE International Conference on Image Processing, Washington, DC. III (1995) 444.

[11] Simoncelli E. P., Freeman W. T.,Adelson E. H., Heeger D. J., *Shiftable Multi-scale Transforms*, IEEE Trans. Information Theory, 38(2) (1992) 587.

[12] Lee Y. K., Chen L. H., *A Secure Robust Image Steganographic Model*, Tenth National Conference of Information Security, pp. 275-284, Hualien, Taiwan, May 5-6 (2000).

[13] Wayner P., *Disappearing Cryptography. Information Hiding: Steganography & Watermarking*, Morgan Kaufman Publishers (2002).

[14] Machado R., EzStego, <http://www.stego.com> (1997).

[15] Westfeld A., F5, <http://wwwrn.inf.tu-dresden.de/ westfeld/F5.html> (2001).

[16] Johnson N. F., Jajodia S., *Steganalysis of Images Created Using Current Steganography Software*, Centre for Secure Information Systems, George Mason University, Fairfax, Virginia, Information Hiding, Second International Workshop, IH'98 Portland, Oregon, USA, April (1998) 273.

[17] Westfield A., Pfitzmann A., *Attacks on Steganographic Systems - Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools - and Some Lessons Learned*, Lecture Notes in Computer Science (2000).

[18] Fridrich J., Goljan M., *Practical Steganalysis: State of the Art*, SPIE Vol. 4675, EI2002 (2002) 1.

[19] Dygnarowicz R., *Steganografia*, ENIGMA 2000 - IV Krajowa Konferencja Zastosowań Kryptografii, Warszawa (2000).

[20] Jackson J. T., Gunsch G. H., Claypoole Jr. R.L., Gary B. Lamont G. B., *Wavelet-based steganalysis using a computational immune system approach*, VCIP (2003) 1884.

[21] Farid H., *Detecting hidden messages using higher-order ststistical models*, International Conference of Image Processing, Rochester, New York (2002).

[22] Upham D., Jpeg-Jsteg, <ftp://ftp.funet.fi/pub/crypt/steganography/> (1997).

[23] Provos N., Outguess, <http://www.outguess.org>.

[24] Fisher R., *The use of multiple measures in taxonomic problems.* Annals of Eugenics, 7 (1936) 179.

[25] Shah I., KalkerA., *Theory and Design of Multidimensional QMF Subband Filters From 1-D Filters Using Transforms*, in Proceedings of the 4th International Conference on Image Processing and Applications (Maastricht) (1992) 474.

[26] Divakaran A., Pearlman W.A., *Information-theoretic performance of quadrature mirror filters*, IEEE Transactions on Information Theory 41 (1995) 2094.

[27] FreeFoto, <www.freefoto.com>.