PASSIVE STEGANALYSIS OF MULTIDOMAIN EMBEDDING METHODS

Dmytro Progonov, Serhii Kushch

Abstract: *The paper is devoted to analysis of effectiveness the usage of modern statistical model of digital image for revealing the stego images with data, embedded in transformation domain of cover images. It is considered the case of applying of standard Subtractive Pixel Adjacency Matrix model for detection the presence of stegodata, hidden with usage of various type the cover image transformation – Discrete Cosine Transform, Discrete Wavelets Transform, Singular Value Decomposition. It is established that accuracy of stego image detection by usage of the model rises by increasing the amount of stage the cover image processing and significantly depends on type of embedded stegodata.*

Keywords: *passive steganalysis, multistage embedding methods, digital images.*

ACM Classification Keywords: *D.4 Operating Systems – Security and protection – Information flow controls.*

Introduction

During the last days of computer systems widespread usage of high speed communication systems (CS), integration of government agencies and private corporations computers systems into global network, usage of various types the communication services led to corresponding revision of methodology the attacks of malefactors and terrorists [Tallinn, 2013]. Significant part of success these attacks depends on the reliable communication between the intruders for data transmission and coordination of actions. In most cases such communication channels are embedded in existed information flows in various types the communication services, such as social networks, multimedia files sharing, Voice-over-IP services, with usage of steganographic systems (SS) [The Cisco, 2014]. Therefore, the early detection and counteraction the hidden messages (stegodata) transferring in communication services are important task today.

As cover media for stegodata are widely used difference types of multimedia files, in particular digital images (DIs), which is explained by high redundancy of theirs representation in digital form [Fridrich, 2010]. Existed methods of image steganography can be divided in two groups – embedding in spatial domain (LSB-methods) and in the transformation domain (TD) [Katzenbeisser, 2000]. LSB methods allow minimizing the distortion of cover image parameters by stego images forming, but has relatively low robustness to any alteration of stego image by DIs transferring in CS. Message hiding in TD is

based on usage the different types transformations of cover images by stegodata embedding. It allows considerably increasing the robustness of obtained stego images to active steganalysis by preservation the fixed distortion of cover image's parameters.

For revealing the stego images with data, embedded in spatial and transformation domains of cover images, were proposed effective approaches, based on statistical [Pevny, 2008; Fridrich, 2012], multifractal [Progonov, 2014a, 2014b, 2014d], variogram [Progonov 2014c] and spectral [Doroshenko, 2014] analysis. In spite of "universality" the statistical methods, in most cases they are used for revealing the stego images with data, embedded only in spatial domain or JPEG domain of cover images. Therefore it is represented the interest to investigate the effectiveness of applying statistical steganalysis for discerning the stego images with data, hidden in TD.

In the paper we investigated the effectiveness of usage the statistical model of images, based on Markov features the DIs, for detection the presence of stegodata, hidden in various TD. Obtained results can be used by creation of universal stegodetectors for revealing the stego image with data, embedded in spatial as well as difference transformation domains of digital images.

Related Works

For revealing the stego images with data, embedded in spatial domain of DIs, there were proposed structural analysis method [Dumitrescu, 2002] and approaches, based on applying the statistical models (SMs) of DI [Pevny, 2010b; Kodovsky, 2009]. In most cases SM are created for realization the targeting attack on specified SS, which limits further usage of proposed SM for revealing the another methods of stegodata embedding. For overcome mentioned limitation it was proposed [Fridrich, 2012] to merge the separate SMs into the rich models (RMs) of DI. It allows successfully attack the modern highly undetectable embedding algorithms (for instance, HUGO algorithm [Pevny, 2010a]), which has been impossible with usage of simple SMs. Limitation of practical usage the RMs is high dimensionality of features space (for example, 34671 features for SRM model [Fridrich, 2012]), which leads to complication of stegodetector tuning procedure. Due to this, further improvements of RM are carried out by optimization the used feature space or development the alternative statistical models of DIs [Holub, 2013b, 2015].

Alternative approach to create the highly undetectable embedding algorithms (HUEA) is message hiding in TD of cover image, in particular in spectral domain of DI (for instance, WOW algorithm [Holub, 2012], UNIWARD method [Holub, 2013a]). Rich models, proposed for revealing of such HUEA, are based on assumption the stegodata hiding in JPEG-domain of DIs [Kodovsky, 2009, 2012b], which led to narrowing of application domain for these models. Therefore it is represented the interest to investigate the effectiveness of applying the standard spatial domain-based RMs for revealing the stegodata, embedding with usage both spectral (Discrete Cosine Transform (DCT), Two-Dimensional Discrete

Wavelets Transform (2D-DWT)) and special (Singular Value Decomposition, SVD) transformation of the cover images.

The Goal and Contribution

The goal of paper is investigation of effectiveness the application of Subtractive Pixels Adjacency Matrix (SPAM) model for revealing the stego image with data, embedded with usage of one-stage and multi-stage methods in the spectral and singular value domains of the cover images.

Multidomain Data Embedding Methods

Historically, the first methods, proposed for message embedding in spatial domain, were based on substitution the least significant bits of pixels by stegodata [Fridrich, 2010]. These methods allows embedding the message with volume up to 1/8 of cover image's size, but result in specific distortion of image parameters – changing the statistics of bit value distribution (chi-square attack [Westfeld, 1999]) or local correlation among neighboring pixels (Sample Pairs Analysis [Dumitrescu, 2002], RS Analysis [Fridrich, 2004]). Modern approaches to message hiding with applying of LSB-methods based on adaptive selection of image context for stegodata embedding and usage the encoding systems for minimization the amount of changed pixels [Fridrich, 2010].

For increase the robustness of the stego images to possible alteration or intentional changes by image transmission in CS, Zhao and Koch proposed to use the peculiarities of DCT [Zhao, 1995]. Based on this work, the separate class of methods for stegodata embedding in DIs with usage of classical spectral as well as special transformations was developed.

Choice the type of cover image transformation depends on requirements to SS – usage of spectral transformation (for instance, Discrete Wavelets or Cosine Transforms) allows increase the endurance of formed stego images to applying the standard transformation, such as lossy compressions, while special types of transformation (for example, Singular Value Decomposition) gives opportunity to decrease the distortion of cover image parameters.

In the work we analyzed the methods, which are based on usage both groups of cover image transformations, as well as the case of one-stage and multistage message embedding, when several transformation are used simultaneously.

The list and parameters of investigated embedding methods are represented in table 1. Message embedding was provided by weighted summation of transformation coefficient the cover image K_{cover} and stegodata K_{data} in specified transformation domain:

$$K_{stego} = K_{cover} + G \times K_{data}, \quad (1)$$

where G – weighted coefficient, which is used for variation the energy of stegodata. Values of the coefficient G were changed from $G_{\min}$ (lower bound of stegodata reconstruction on receiver's side the SS) to $G_{\max}$ (appearance the visual distortion of cover image by message hiding) with step Δ_G (Table 1). Cover image payload is determined as fraction of changed coefficients by message hiding to total amount of the transformation coefficients. By stego images forming each color channels of cover image and stegodata were processed independently.

Table 1. Analyzed methods the message embedding in transformation domain of digital images

Authors	Cover image processing			Stegodata processing	Weighted coefficient G		
	1st stage	2nd stage	3rd stage		$G_{\min}$	$G_{\max}$	Δ_G
Dey (2011)	2D-DWT	–	–	2D-DWT	0.02	0.08	0.02
Agarwal (2006)	SVD	–	–	SVD	0.02	0.08	0.02
Joseph (2013)	2D-DWT	SVD	–	SVD	0.1	2	0.5
Khan (2013)	2D-DWT	DCT	SVD	SVD	0.5	4	1

Approximation W_φ and detailed W_ψ coefficients of 2D-DWT transform of grayscale image $I_{x,y}$ with size $M \times N$ (pixels) were calculated according to further formulae [Gonzalez, 2008]:

$$W_\varphi(j,m,n) = \frac{1}{\sqrt{MN}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} I_{x,y} \times \varphi_{j_0,m,n}(\mathrm{x},y),$$

$$W_\psi^i(j,m,n) = \frac{1}{\sqrt{MN}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} I_{x,y} \times \psi_{j,m,n}^i(\mathrm{x},y) i \in \{H,V,D\},$$

where

$$\varphi_{j,m,n}(\mathrm{x},y) = 2^{j/2} \times \varphi\left(2^j x - m\right) \otimes \varphi\left(2^j y - n\right),\ \psi_{j,m,n}^H(\mathrm{x},y) = 2^{j/2} \times \psi\left(2^j x - m\right) \otimes \varphi\left(2^j y - n\right),$$

$$\psi_{j,m,n}^V(\mathrm{x},y) = 2^{j/2} \times \varphi\left(2^j x - m\right) \otimes \psi\left(2^j y - n\right),\ \psi_{j,m,n}^D(\mathrm{x},y) = 2^{j/2} \times \psi\left(2^j x - m\right) \otimes \psi\left(2^j y - n\right),$$

correspondingly, two-dimensional scaling function $\varphi_{j,m,n}(\mathrm{x},y)$ and wavelets $\psi_{j,m,n}^i(\mathrm{x},y)$; $\varphi(x), \psi(x)$ – one-dimensional scaling and wavelet functions; $\otimes$ – Cartesian product; j_0, j – initial and

current decomposition levels; m,n – spatial shift parameters for two-dimensional scaling and wavelet functions.

Inverse DWT was calculated according to formula [Gonzalez, 2008]:

$$I(x,y)=\frac{1}{\sqrt{MN}}\times\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left[W_{\varphi}(j_0,m,n)\times\varphi_{j_0,m,n}(\mathrm{x},y)+\sum_{i\in\{H,V,D\}}\sum_{j=j_0}^{+\infty}W_{\psi}^{i}(j,m,n)\right].$$

According to Dey, Joseph and Khan methods the detailed coefficient were used for message hiding in cover image, which is explained by features of human vision – relatively low sensitivity to slight changes of fine details the images. As basic functions of 2D-DWT were used the Haar wavelet and corresponding scaling function.

Direct and inverse DCT of grayscale image $I_{x,y}$ with size $M\times N$ (pixels) were calculated according to further formula [Oppengeim, 2010]:

$$T(u,v)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}I_{x,y}\times r(x,y,u,v);I_{x,y}=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}T(u,v)\times s(x,y,u,v),$$

$$r(x,y,u,v)=s(x,y,u,v)=\beta(u)\times\beta(v)\times\cos\left[\frac{(2x+1)u\pi}{2M}\right]\times\cos\left[\frac{(2y+1)v\pi}{2N}\right],$$

$$\beta(u)=\begin{cases}\sqrt{1/M},u=0;\\ \sqrt{2/M},u=1,2\ldots(M-1);\end{cases}\quad\beta(v)=\begin{cases}\sqrt{1/N},\mathrm{v}=0;\\ \sqrt{2/N},\mathrm{v}=1,2\ldots(N-1);\end{cases}$$

where $r(x,y,u,v),s(x,y,u,v)$ – correspondingly, kernels of direct and inverse DCT, $\beta(u),\beta(v)$ – normalization multipliers.

SVD of grayscale image $I_{x,y}$ with size $M\times N$ (pixels) were provided according to formula [Murphy, 2012]:

$$I_{x,y}=U_{M\times M}\times S_{M\times N}\times V_{N\times N}^{T},$$

where U,V – orthonormal matrix of left and right eigenvectors; S – diagonal matrix, which contains the singular values of matrix $I_{x,y}\times I_{x,y}^{T}$. Stegodata embedding was provided with usage of eigenvalues due to ambiguous the eigenvector reconstruction (up to theirs permutation) on the receiver's side of SS.

SPAM Model of Digital Images

Consequence of embedding stegodata in cover images with usage of any steganographic methods is alteration of cover parameters. Due to this, significant part of modern steganalysis methods is based on analysis the changing of cover image parameters and further creation the cluster of image's characteristics, which changes at most by stego image forming. It should be mentioned that in most

cases providing of targeting steganalysis is impossible due to absence or scantiness the priory information about the embedding domain or hiding algorithm. Therefore modern approach for stego image detection is usage of cover RMs (CRMs) – consolidation of several simple SM of cover images, which is based on peculiarities of DI (for instance, Markov features) or specific of image parameters alteration by message hiding.

Existed CRMs can be divided into two groups – spatial-domain and JPEG-domain based models. These models were developed for targeting steganalysis of modern embedding methods (for instance, CC-PEV model for attack the YASS algorithm [Kodovsky, 2009]) or creation the universal (blinf) stegodetectors for revealing the stego images in case of absence the a priory information about the embedding method (for example, [Kodovsky, 2012b]). Limitation of known JPEG-domain based models is theirs ability for detection only the specific types of hiding algorithm, while spatial-domain based models (SDBMs) also give opportunity to provide the blind steganalysis. Therefore it is represented the interest to use the SDBMs for revealing the steganograms with data, embedding in various TD.

In the work we investigated the efficiency of well-known Subtractive Pixel Adjacency Matrix (SPAM) model [Pevny, 2010b]. SPAM model is based on usage the first and second order Markov chains (MCs) for modeling the dependencies between difference $D_{x,y}$ of adjacency pixels in grayscale image $I_{x,y}$. For instance, difference between brightness of horizontally adjacent pixels can be represented as:

$$D^{\rightarrow}_{x,y} = I_{x,y} - I_{x+1,y}.$$

Then parameters $M^{\rightarrow}_{u,v}$ ($M^{\rightarrow}_{u,v,w}$) of first (second) order of MC were calculated according to further formulae [Pevny, 2010b]:

$$M^{\rightarrow}_{u,v} = \Pr\left(D^{\rightarrow}_{x+1,y} = u \mid D^{\rightarrow}_{x,y} = v\right), M^{\rightarrow}_{u,v,w} = \Pr\left(D^{\rightarrow}_{x+2,y} = u \mid D^{\rightarrow}_{x+1,y} = v \mid D^{\rightarrow}_{x,y} = w\right), u,v,w \in \{-T,...T\},$$

where $\Pr(A)$ – probability of event A; T – specified threshold, which is used for limit the variability of $D_{x,y}$ values. Consolidate the parameters of MC, we can write the whole SPAM model as:

$$\begin{cases} F_{1,2...k} = \frac{1}{4} \times \left[M^{\rightarrow}_{*} + M^{\leftarrow}_{*} + M^{\uparrow}_{*} + M^{\downarrow}_{*} \right]; \\ F_{k+1,k+2...2k} = \frac{1}{4} \times \left[M^{\searrow}_{*} + M^{\nwarrow}_{*} + M^{\swarrow}_{*} + M^{\nearrow}_{*} \right]. \end{cases}$$

where $k = (2T+1)^2$ and $k = (2T+1)^3$ for first and second order MC correspondingly.

For increasing the performance of SPAM model, according to recommendation [Pevny, 2010b], in the work were used the second-order MC for modelling the difference between adjacent pixels with threshold $T = 3$. Therefor the dimensionality of features space for grayscale cover image was equal to $2 \times (2T+1)^3 = 2 \times 7^3 = 686$.

Results

Analysis of effectiveness the SPAM model for revealing the stego images with data, embedded in TD, were provided with usage of cover images (JPEG, True Color) packet MIRFlickr-25k [Huiskes, 2008]. For training and testing of stegodetector were used the subset of 2,500 pseudo randomly selected and scaled DI from packet. As stegodata were used three DI – engine's draft, map and portrait. Characteristics of the stegodata are represented in Table 2:

Table 2. Characteristics of used test digital images and stegodata

Characteristics	Engine's draft	Map	Portrait
Resolution, pixels	567×463	800×800	565×850
Color system	RGB		
Format	BMP		

By investigation, cover image payloads were changed from 5% to 25% with step 5% and from 25% to 95% with step 10%. Weighted coefficients G, for each investigated embedding method, were changed from $G_{\min}$ up to $G_{\max}$ with step Δ_G (Table 1).

The stegodetector was training with usage of half the test packet. Testing the tuned stegodetector was provided on the remained half of test packet. Recognition of stego images by stegodetector was provided with usage of ensemble classifier [Kodovsky, 2012a]. As base classifier was used the Fisher's Linear Discriminant (FLD), which was tuned for minimization of total detection error P_E on training subset the test packet:

$$P_E = \min_{P_{FA}} \frac{1}{2}\left[P_{FA} + P_{MD}\left(P_{FA}\right)\right],$$

where P_{FA}, P_{MD} denote the probabilities of false alarm and missed detection respectively. Assessment of P_{FA} and P_{MD} was provided according to bootstrap estimation algorithm [Kodovsky, 2012a] by training each base classifier B_l on pseudo random selected subset of training set

$$\mathrm{X}_l = \left\{x_m^{(D_l)}, \overline{x}_m^{(D_l)}\right\}_{m\in\mathfrak{M}_l^b},$$

where $x_m, \bar{x}_m$ – training samples; $D_l, l \in \{1,2...d\}$ – pseudo randomly selected subset of features from general feature space with dimensionality d; $\mathfrak{M}_l^b$ – bootstrap sample of $\{1,2...N^{trn}\}$; N^{trn} – amount of test cover images at training stage.

The total detection error P_E (out-of-bag (OOB) error) for stegodetector after training phase was computed according to formula:

$$P_{E-OOB}^{(n)} = \frac{1}{2N^{trn}} \sum_{m=1}^{N^{trn}} \left[B^{(n)}(x_m) + 1 - B^{(n)}(\bar{x}_m) \right].$$

Analysis of accuracy the stego image detection was provided with usage of SPAM model was provided for two cases – with usage of all or separate stegodata for stegodetector training and testing. Investigation was provided for grayscale (separate color channels of test DIs) and true color images. Estimation of mean value and variance of the OOB-error P_E was provided by repeating the training and testing stage 10 times.

Results of testing the performance of stegodetector, tuned with usage of SPAM model, by message hiding in TD are represented at Figure 1 and Table 3.

It should be mentioned the unexpected results for the Dey, Joseph and Khan methods – total detection error P_E depends only on weighted coefficient G, in other words on stegodata energy (Figures 1b - 1d). It can be explained by ability of 2D-DWT to separate the details on DI depends on theirs orientation. Due to this it is possible to minimize the distortion of Markov features by selection of detailed coefficient (direction of fine details) for message hiding.

Secondly, usage of SVD (Figure 1a) allows considerably decrease the precision of stego image detection in comparison with 2D-DWT cases (Figures 1b - 1d). Also, the high level of OOB for Agarwal method preserved for wide range of cover image payloads and weighted parameter G values, which indicates about the relatively low effectiveness of usage the SPAM model it this case. Obtained results are explained with usage statistical interpretation of SVD transform – opportunity to decompose the DI on components with maximum variance [Murphy, 2012].

Usage of cover image's components with higher variance for message embedding allows decrease the changes of difference the brightness of adjacent pixels and, correspondingly, alteration the parameters of MC and SPAM model.

Results, represented at Figure 1, allow us estimating the minimum OOB error for SPAM model due to usage of all color channels and types of stegodata at training phase of stegodetector tuning. So, let see the results for more "realistic" situation, when only part of available information can be used for stegodetector adjustment (Table 3):

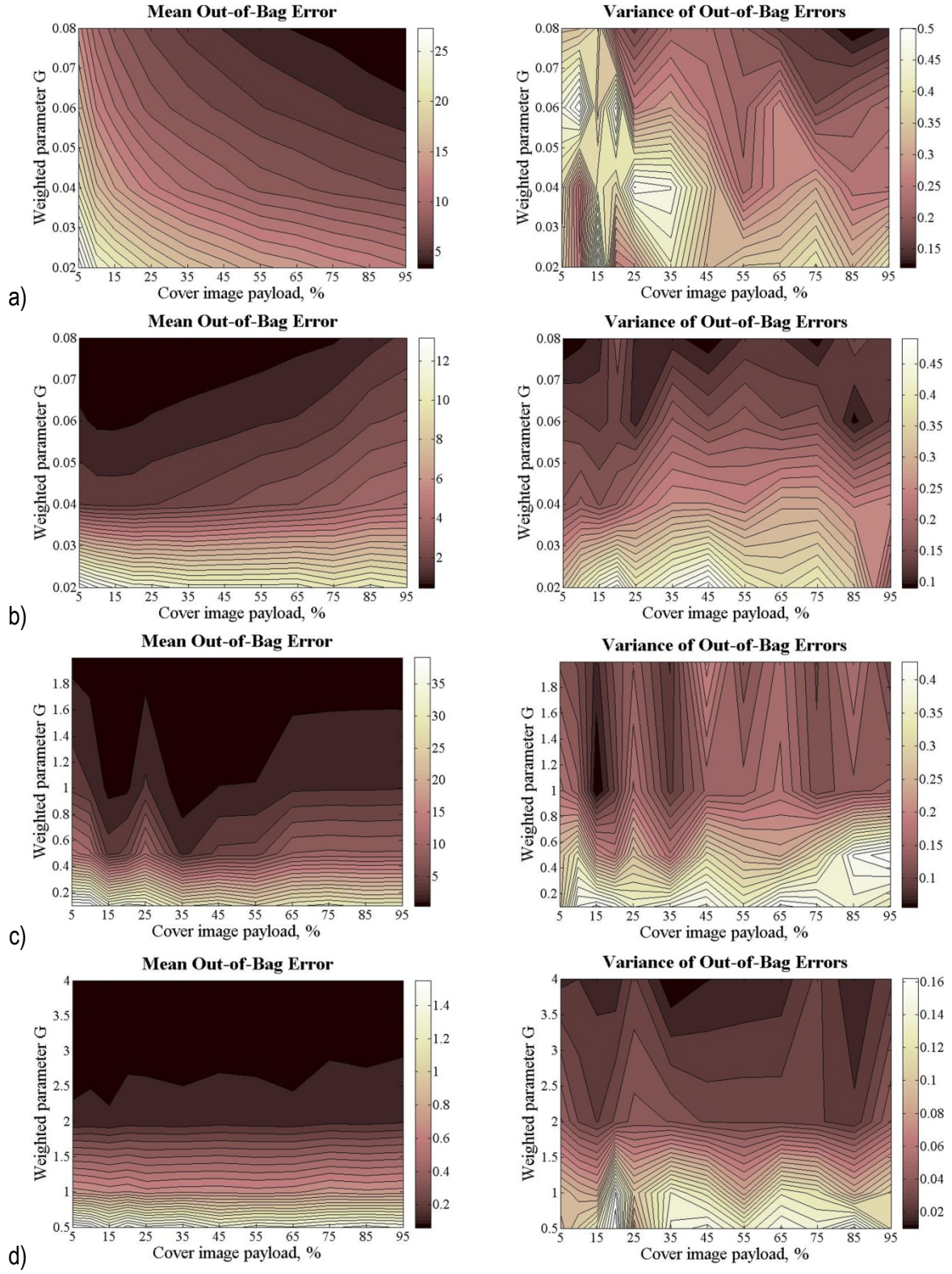

Figure 1. Mean value and variation of total detection error P_E for stegodetector by usage of SPAM model and all cover image color channels and stegodata type. Message was embedded according to: (a) – Agarwal method; (b) – Dey method; (c) – Joseph method; (d) – Khan method

Table 3. Mean values and variance of total detection error P_E for investigated methods (Maximum OOB-error / Variance of OOB-error / Minimum OOB-error)

	All color channel	Separate color channel		
		Red color	Green color	Blue color
Agarwal method				
All stegodata	28.78 / 0.52 / 3.37	31.97 / 0.53 / 5.51	33.45 / 0.54 / 4.93	35.07 / 0.44 / 5.36
Stegodata type "Draft"	30.67 / 0.81 / 3.17	32.86 / 1.07 / 4.36	34.06 / 0.96 / 3.82	36.53 / 1.07 / 4.62
Stegodata type "Map"	30.77 / 1.06 / 3.28	33.08 / 0.94 / 5.13	34.64 / 0.85 / 4.16	36.73 / 0.997 / 4.85
Stegodata type "Portrait"	30.46 / 0.87 / 4.52	32.88 / 0.90 / 7.35	34.66 / 0.86 / 6.14	35.99 / 0.92 / 7.03
Dey method				
All stegodata	13.70 / 0.51 / 0.50	26.90 / 0.96 / 1.70	20.80 / 0.71 / 1.20	27.00 / 0.85 / 1.30
Stegodata type "Draft"	17.00 / 0.88 / 1.20	26.40 / 0.76 / 2.00	19.70 / 0.78 / 1.40	26.00 / 0.72 / 1.70
Stegodata type "Map"	17.70 / 0.88 / 0.80	26.80 / 0.80 / 1.70	20.90 / 0.87 / 1.30	27.10 / 1.03 / 1.40
Stegodata type "Portrait"	18.20 / 1.02 / 1.30	27.60 / 1.01 / 2.10	20.90 / 0.71 / 1.50	27.30 / 1.05 / 1.80
Joseph method				
All stegodata	40.67 / 0.43 / 0.49	43.19 / 0.40 / 0.64	43.14 / 0.61 / 0.82	44.09 / 0.45 / 0.63
Stegodata type "Draft"	38.86 / 1.08 / 0.37	40.64 / 0.78 / 0.22	40.00 / 0.91 / 0.40	41.80 / 0.81 / 0.31
Stegodata type "Map"	46.28 / 0.83 / 0.26	47.92 / 0.66 / 0.28	47.23 / 0.90 / 0.23	46.94 / 0.96 / 0.34
Stegodata type "Portrait"	46.84 / 0.87 / 0.83	47.50 / 0.62 / 1.16	47.15 / 0.75 / 1.09	47.27 / 0.81 / 0.59

	All color channel	Separate color channel		
		Red color	Green color	Blue color
Khan method				
All stegodata	1.61 / 0.17 / 0.07	2.10 / 0.19 / 0.08	1.83 / 0.13 / 0.06	1.94 / 0.12 / 0.07
Stegodata type "Draft"	1.67 / 0.18 / 0.00	2.17 / 0.27 / 0.00	1.78 / 0.25 / 0.00	1.96 / 0.21 / 0.00
Stegodata type "Map"	1.83 / 0.24 / 0.00	2.58 / 0.24 / 0.01	2.26 / 0.26 / 0.00	1.99 / 0.17 / 0.01
Stegodata type "Portrait"	2.21 / 0.29 / 0.11	2.73 / 0.34 / 0.08	2.69 / 0.25 / 0.10	2.77 / 0.38 / 0.11

First of all, it should be mentioned that values of OOB errors are significantly variance for various color channels (Table 3) – OOB error is minimal for green channel and maximum for blue channel (Agarwal, Dey and Joseph methods) or red channel (Khan method). Obtained results are explained by procedure of DI acquisition in digital camera or scanners – presence of demosaicing (debayering) stage, when the equalization of energy the DI spectral components according to peculiarities the human vision is carried out [Fridrich, 2010]. It is realized by averaging the values for adjacent green subpixels, which leads to corresponding suppression of noise. Message hiding leads to distortion of statistics parameters for green color channel, which is registered by corresponding change of results for SPAM model.

Also, the values of OOB errors for stegodata type "Portrait" are higher for all considered methods in comparison with other types of stegodata (Table 3). Such "imbalance" in obtained results is explained by substantially lesser amount of fine details for Portrait-stegodata, which leads to corresponding decreasing the number of changed pixels by stego image forming.

Conclusion

On the basis on conducted analysis of OOB errors by usage the SPAM model for detection the stego images with data, embedded with applying of various transforms, it is established that:

1. Effectiveness of SPAM model significantly depends on amount of stage the cover image processing by stegodata hiding – the lowest OOB-errors are achieved in case of usage the multistage embedding methods. Increase the OOB error took place by applying of SVD for message hiding (Agarwal and Joseph embedding methods), which explained by usage the image components with the higher variance for stegodata hiding;

2. Range of OOB errors value in case of 2D-DWT usage for stego images forming depends only on weighted parameter G. Due to this it is impossible to provide the quantitative steganalysis with usage of tuned stegodetector – estimation of cover image payload by analysis of variation of changes the parameters of SPAM model;

3. Considerable influence on level the OOB error has type of used stegodata and color channel of cover image by message hiding. Therefore it is recommended to provide the adjustment of stegodetectors with usage as much as possible testing message and usage both grayscale as well as true color images for increase the accuracy of steganogram discerning.

Acknowledgements

The paper is published with partial support by the project ITHEA XXI of the ITHEA ISS (www.ithea.org) and the ADUIS (www.aduis.com.ua).

Bibliography

[Agarwal, 2008] Agarwal R., Santhanam M.S. Digital watermarking in the singular vector domain. International Journal of Image and Graphics, 2008. Vol. 8. pp. 351-362.

[Dey, 2011] Dey N., Roy A.B., Dey S. A novel approach of color image hiding using RGB color planes and DWT. International journal of computer application, 2011. Vol. 36, No.5. pp.19-24.

[Doroshenko, 2014] Doroshenko A., Kushch S., Progonov D. Spectral characteristics of steganograms. Proceedings of VII International conference "Suchasni problemy i dosyagnennya v galuzi radiotechniky, telekomunikatiy ta informaciynuh tehnologiy". pp. 327-328 (in Ukrainian).

[Dumitrescu, 2002] Dumitrescu S., Wu X., Memon N.D. On steganalysis of random LSB embedding in continuous-tone images. Proceedings IEEE, International Conference on Image Processing, ICIP 2002. Rochester, NY, USA, September22-25 2002. pp. 324-339.

[Fridrich, 2004] Fridrich J., Goljan M., Du R. Detection LSB steganography in color and grayscale images. IEEE Multimedia, Special Issue on Security, 2001. Volume 8, Issue 4. pp. 22-28.

[Fridrich, 2010] Fridrich J. Steganography in Digital Media: Principles, Algorithms and Applications. Cambridge University Press, New York, USA. 2010. 437 p.

[Fridrich, 2012] Fridrich J., Kodovsky J. Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 2012. Vol. 7, Issue 3. pp. 868-882.

[Gonzalez, 2008] Gonzalez R., Woods R. Digital Image Processing. International version 3rd edition. Pearson Education Press, 2008. 1103 p.

[Holub, 2012] Holub V., Fridrich, J. Designing steganographic distortion using directional filters. In Fourth IEEE International Workshop on Information Forensics and Security, December 2–5, 2012.

[Holub, 2013a] Holub V., Fridrich, J. Digital image steganography using universal distortion. Puech, W., Chaumont, M., Dittmann, J., and Campisi, P., eds. In 1st ACM IH&MMSec. Workshop, June 17–19, 2013.

[Holub, 2013b] Holub V., Fridrich J. Random Projections of Residuals for Digital Image Steganalysis. IEEE Transactions on Information Forensics and Security, 2013. Vol. 8, Issue 12. pp. 1996-2006.

[Holub, 2015] Holub V., Fridrich J. Phase-Aware Projection Model for Steganalysis of JPEG Images. Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XVII, San Francisco, CA, February 8–12, 2015.

[Huiskes, 2008] Mark J. Huiskes, Michael S. Lew. The MIR Flickr Retrieval Evaluation. Proceedings of the 2008 ACM International Conference on Multimedia Information Retrieval, Vancouver, Canada. ACM Press, New York, NY, USA. DOI 10.1145/1460096.1460104.

[Joseph, 2013] Joseph A., Anusudha K. Robust Watermarking Based on DWT-SVD. International Journal on Signal & Image Security, 2013. Issue 1, Vol. 1.

[Katzenbeisser, 2000] Katzenbeisser S., Petitcolas P. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Boston, USA. 2000. 237 p.

[Khan, 2013] Khan M.I., Rahman M., Sarker I.H. Digital Watermarking for image Authentication Based on Combined DCT, DWT and SVD Transformation. International Journal of Computer Science Issues, IJCSI, 2013. Volume 10, Issue 3, No. 1. pp. 223-230.

[Kodovsky, 2009] Kodovsky J., Fridrich J. Calibration revisited. In J. Dittmann,S. Craver, and J. Fridrich editors. Proceedings of the 11th ACM Multimedia and Security Workshop, Princeton, NJ, September 7–8, 2009.

[Kodovský, 2012a] Kodovský J., Fridrich J., Holub V. Ensemble Classifiers for Steganalysis of Digital Media. IEEE Transactions on Information Forensics and Security, 2012. Vol. 7, No. 2. pp. 432-444.

[Kodovsky, 2012b] Kodovsky J., Fridrich J. Steganalysis of JPEG Images Using Rich Models. Electronic Imaging, Media Watermarking, Security, and Forensics. Proceedings of 14th SPIE conference. San Francisco, California, USA. January 23–25, 2012. Vol. 8303. pp. 1-12.

[Murphy, 2012] Murphy Kevin P. Machine Learning: A Probabilistic Perspective. Massachusetts Institute of Technology Press, 2012. 1071 p.

[Oppenheim, 2010] Oppenheim Alan V., Shaffer Ronald W. Discrete-Time Signal Processing. 3rd edition. Pearson Education Press, 2010. 1046 p.

[Pevny, 2010a] Pevný T., Filler T., Bas P. Using high-dimensional image models to perform highly undetectable steganography. In R. Böhme and R. Safavi-Naini, editors. Information Hiding, 12th International Workshop, Calgary, Canada, June 28–30, 2010. Springer-Verlag, New York. Volume 6387 of Lecture Notes in Computer Science, pages 161–177,

[Pevny, 2010b] Pevny T., Bas P., Fridrich J. Steganalysis by Subtractive Pixel Adjacency Matrix. IEEE Trans. on Information Forensics and Security, 2010. Vol. 5, Issue 2. pp. 215-224.

[Progonov 2014c] Progonov D., Kushch S. Variogram Analysis of Steganograms. Proceeding of 3rd International Conference "Zahyst informatii I bezpeka informatiynuh system", 05-06 Juni, 2014, Lviv, Ukraine. pp. 84-85. (in Ukrainian).

[Progonov 2014d] Progonov D., Kushch S. On the Multifractal Analysis of the Steganograms. Proceeding of the 4th International conference "Theoretical and Applied Aspects of Cybernetics", November 24-28, 2014, Kyiv, Ukraine pp. 32-38.

[Progonov, 2014a] Progonov D. O., Kushch S. M. Revealing of steganograms with data, which are hidden in transformation domain of digital images. Visn. NTUU KPI, Ser. Radioteh. radioaparatobuduv., 2014. No. 57, pp. 128-142. (in Ukrainian).

[Progonov, 2014b] Progonov D., Kushch S. Identification the type of transformations, used by message hiding in digital images. Proceeding of 16th International conference "System Analysis and information Technologies", My 26-30, 2014, Kyiv, Ukraine. pp. 435-436. (in Russian).

[Tallinn, 2013] Tallinn Manual On the International Law Applicable to Cyber Warfare. Ed. Michael N. Schmitt. Cambridge University Press, 2013, 302 p.

[The Cisco, 2014] The Cisco 2014 Annual Security Report. San Jose, California, USA. January, 2014.

[Westfeld, 1999] Westfeld A., Pfitzmann A. Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned. Proceedings of Third International Workshop, IH`99. Dresden, Germany, 1999. pp. 61-71.

[Zhao, 1995] Zhao J., Koch E. Embedding Robust Labels into Images for Copyright Protection. Proceedings of the Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and Techniques. Munich-Vienna, 1995. Verlag. pp.242-251.

Authors' Information

Dmytro Progonov *– the 2nd year postgraduate student, the Assistant, Faculty of Information Security, Institute of Physics and Technology, National Technical University of Ukraine "Kyiv Polytechnic Institute"; Postal Code 03056, Prospect Peremohy, 37, Kyiv, Ukraine; e-mail: progonov@gmail.com.*

Major Fields of Scientific Research: Digital Media Steganography, Advanced Signal Processing, Machine Learning.

Serhii Kushch *– Ph.D. in Electronics, ISOC Member, Associated Professor, Faculty of Information Security, Institute of Physics and Technology, National Technical University of Ukraine "Kyiv Polytechnic Institute"; Postal Code 03056, Prospect Peremohy, 37, Kyiv, Ukraine; e-mail: skushch1@gmail.com.*

Major Fields of Scientific Research: Wireless Communication System, Ultra High Frequency Communication Systems, Advanced Signal Processing.