*Bartosz CZAPLEWSKI**

DOI: 10.15199/59.2017.10.3

Current trends in the field of steganalysis and guidelines for constructions of new steganalysis schemes

Aktualne trendy w dziedzinie steganalizy oraz zalecenia dla konstrukcji nowych systemów steganalitycznych

Artykuł dotyczy niekoherentnych technik steganalizy w scenariuszu pasywnej steganalizy przeznaczonych do detekcji systemów steganograficznych stosujących metodę modyfikacji obrazów cover. Celem jest zbadanie aktualnego stanu wiedzy w dziedzinie steganalizy, a przede wszystkim rozpoznanie aktualnych kierunków w tej dziedzinie i ustalenie wytycznych dla konstrukcji nowych systemów steganalitycznych. Zamierzonymi efektami są zbadanie możliwości rozwoju wiedzy w dziedzinie steganografii i wyznaczenie celów dla przyszłych badań.
Słowa kluczowe: steganaliza, stan wiedzy, wytyczne, bogaty model, splotowe sieci neuronowe.

The paper concerns blind steganalysis techniques in the passive steganalysis scenario designed to detect the steganographic cover modification schemes. The goal is to investigate the state-of-art in the field of steganalysis, and, above all, to recognize current trends existing in this field and determine guidelines for constructions of new steganalysis schemes. The intended effects are to examine the possibilities for the development of knowledge in the field of steganography and to set directions for future research.
Key words: steganalysis, state-of-art, guidelines, rich model, convolutional neural networks.

1. INTRODUCTION

Steganography is a field of science of concealing communications by hiding secret messages within other data, e.g. images. At the sender side, the aim of steganography scheme is to embed a secret message into innocent-looking image called cover image. An image containing hidden message is called stego image and is usually transmitted through public channel. At the receiver side, the aim of steganography scheme is to extract the hidden message from the received stego image. Thus, a steganography scheme includes two parts: the embedding algorithm and the extraction algorithm.

There are three steganographic architectures [1]: steganography by cover selection, steganography by cover synthesis and steganography by cover modification. In steganography by cover selection, the sender communicates the secret message by choosing a cover image that has hidden meaning. In steganography by cover synthesis, the sender creates his own cover image which carry the secret message. In steganography by cover modification, the sender introduces modifications to a cover image in order to hide the secret message. This article concerns the steganography by cover modification.

Steganalysis is a field of science of detecting secret communications carried by steganography schemes. The aim of steganalysis is to detect the presence of a hidden message in test image by distinguishing between stego and cover images. If a stego image is detected then the secret communication is revealed and the steganography scheme is broken. It is not necessary to discover the content of the secret message to break the steganography scheme, since determining the presence of the message is sufficient. Steganalysis schemes are the focus of this article.

*** Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics, Department of Teleinformation Networks,**
e-mail: bartosz.czaplewski@eti.pg.edu.pl

There are three steganalysis scenarios [1]: passive steganalysis, active steganalysis, and malicious steganalysis. In passive steganalysis, the communication is observed and analyzed, but not interfered, in order to detect secret messages. In active steganalysis, the communication is intentionally disrupted in order to make steganography impossible. In malicious steganalysis, the communication is infiltrated by impersonating one of the users of steganography scheme. This article concerns the passive steganalysis scenario.

Another classification of steganalysis methods is based on their targets. We can distinguish targeted steganalysis and blind steganalysis. Targeted steganalysis schemes are designed to detect only particular steganographic schemes. This kind of steganalysis is very accurate against the targeted algorithm but it's usually ineffective against other steganographic schemes, thus it has very limited use. Blind steganalysis schemes are designed to detect any steganographic scheme regardless of their embedding algorithms. This kind of steganalysis is more universal, because it can be used even against the unknown embedding algorithms. This article concerns blind steganalysis techniques.

Guidelines for constructions of steganographic schemes have been determined [1]. The first guideline is to preserve a model of the cover. With this approach, the steganographic scheme will be undetectable within the chosen model. However, it's usually possible to implement a steganalysis scheme based on a statistic which is not preserved within the model. The second guideline is to make the embedding mimic a natural image processing. The assumption is that stego images will stay compatible with the distribution of cover images if the effects of embedding were indistinguishable from some natural processing. The third guideline is to design the steganographic scheme to resist known steganalysis attacks. In steganalysis-aware steganography, the effects of embedding are designed to be undetectable using existing steganalysis schemes. This approach led to development of such stego schemes as ±1

embedding [1] and F5 algorithm [2]. The fourth guideline is to minimize the impact of embedding. In this approach, each cover element has an assigned factor which means the impact of embedding at this element. The algorithm embeds messages in cover elements with the lowest factors to minimize the total embedding impact. Good examples are matrix embedding [3] and wet paper codes [4].

Despite the well-defined guidelines for construction of steganographic schemes, the guidelines for steganalysis schemes are not determined. The goal of the article is to investigate the current state-of-art in the field of steganalysis, to review existing steganalysis schemes, and, above all, to recognize current trends existing in this field and determine guidelines for constructions of new steganalysis schemes. The intended effects are to examine the possibilities for the development of knowledge in the field of steganography and to set directions for future research. The structure of this article is as follows. Brief review on steganalysis trends is provided in Section 2. Guidelines for new steganalysis schemes are presented in Section 3. Section 4 contains conclusions.

2. CURRENT TRENDS IN STEGANALYSIS

The classical methodology for blind steganalysis schemes consists of two steps: feature extraction and classification. The goal of the feature extraction is to obtain a set of features, usually a vector, describing an image. These features should capture the maximum of information from the image and, at the same time, their values should be different for a cover image and a stego image. In other words, the feature vector should be diverse and complete. The goal of the classification is to distinguish between cover images and stego images on the basis of the feature vector.

This section provides a brief review on the state-of-art of the last 8 years. The goal is to verify that the above methodology is still valid or it has been changed according to new trends. Due to the very large number of publications in the field of steganalysis, the brief review was realized in two steps. Firstly, publications have been categorized due to the utilized trends, i.e. domains of operation, approaches, concepts, models, metrics, etc. This overall categorization was presented in Table 1. Then, the selected works, that have had the greatest influence on the current trends, have been further described.

Table 1. Categorization of the trends in the field of steganalysis

	Trends (domains, approaches, concepts, models, metrics, etc.)	Publications
Features extraction	Spatial domain	[5,6,7,8,9,10,11]
	Discrete cosine transform (DCT) domain	[5,12,13,14,7,15,16,17,18,19,11]
	Discrete wavelet transform (DWT) domain	[20,21,14,22,23,24,25,18,19,11]
	Discrete Fourier transform (DFT) domain	[6,8,19]
	Wavelet Packet Decomposition (WPD) domain	[26]
	Rich model of the noise residuals	[10,27]
	High-dimensional feature space	[10,27,28,28,30,31]
	Markov chain model, Markov empirical transition matrices, Markov features	[26,13,22,15,21]
	Characteristic function moments of wavelet subbands	[21,25]
	Genetic algorithms (GA)	[32,33,34,23]
	Higher-order statistics	[32,33,34]
	Forward difference image in three directions: horizontal, vertical and diagonal	[6,8]
	Co-occurrence matrices	[23,35]
	Differential image histograms in pixel, DCT, DWT, and DFT domains	[9,18,6,8]
	Histogram characteristic function (HCF)	[7,23]
	The center of mass (COM)	[5,7,23]
	Huffman code statistics (HCS)	[36]
	File size to Resolution ratio (FR) index	[36,17]
	Huffman Bit Code Length (HBCL)	[17]
	Analysis of Variance (ANOVA)	[35]
	Euclidean distance	[21,9]
	Manhattan distance	[9]
	Bhattacharyya distance	[37]
Classification	Support vector machine (SVM)	[5,20,12,13,14,6,7,8,24,35,9,16,17,25]
	Neural network (NN) with back propagation (BP)	[21,15,38,37,19,11]
	Ensemble classifier (EC)	[10,27]
	Convolutional neural network (CNN)	[28,29,30,31]
	K-nearest neighbor classifier (KNN)	[20,23]
	Naïve Bayes classifier (NB), Gaussian naïve Bayes (GNB)	[20,23]
	Bayesian network model	[33,34]
	Logistic regression model	[32,33]
	Fisher linear discriminator (FLD)	[10,27]
	Decision tree classifier (DT)	[20]

One of the most influential research in recent years was the publication on spatial-domain Rich Model (**RM**) with ensemble classifiers [10]. Feature extraction in this approach is based on assembling a rich model of the noise residuals in spatial domain. A rich model consists of submodels of various types of relationships among neighboring samples of noise residuals obtained by linear and nonlinear high-pass filters. Models are rich in the sense that they maximize the diversity of submodels while keeping all their elements well populated and thus statistically significant. The combination of all the proposed submodels has a total dimension of 34671. Model dimensionality is reduced based on various feature selection strategies, e.g. the best rich model has a dimension of 3300. Ensemble classifiers are used to assemble the model as well as the final steganalyzer due to their low computational complexity and ability to efficiently work with high-dimensional feature spaces. Moreover, this approach combines a feature selection with a classification feedback. The proposed steganalysis scheme was tested against HUGO, edge-adaptive algorithm, and optimally coded ternary ±1 embedding steganographic schemes. For each steganographic scheme, a submodel-selection technique was applied to obtain a good tradeoff between model dimensionality and detection accuracy. BOSSbase database of images was utilized.

Another use of ensemble classifiers in steganalysis was presented in CS-RS method [27]. In this method during, the chi-square statistic is employed to calculate the weight of each feature in the original feature space. Weights correspond to the correlation between the feature and the class (cover or stego). Next, the feature space is sorted according to weights, and then divided into two parts according to a dividing threshold. Final feature subset is formed by selecting features randomly from each part. In this way, informative features are included in each subspace and at the same time the diversity them is preserved due to the random selection of features in each part. Ensemble classifier built as random forest with the FLD as a base

learner were utilized. The original 12753-dimensional feature set was extracted according to RM models [10]. The dimension of the subspaces was from 100 to 5000. The proposed steganalysis scheme was tested against HUGO algorithm and the obtained results outperformed the results for Bagging, AdaBoost, and L-SVM schemes. BOSSbase database of images was utilized.

Very innovative point of view was presented in the first research utilizing deep learning for the purpose of steganalysis [28]. This research suggests that RM framework has a similar architecture to Convolutional Neural Network (**CNN**). The assumption was that the steganalysis performance of a well-trained CNN should be comparable to or even better than the well-known RM. The strategy is innovative because this approach is not the classic two-part scenario with feature extraction and subsequent classification. In this approach, raw images are accepted as the input and the output is the binary classification results which can be used to distinguish stego images from cover images. In this research [28], a steganalyzer in a form of a nine-layer, three-stage CNN was presented. At the input of the first layer, there are images in size of 512×512. At the input of the last layer, there are four thousand 8×8 feature maps, which means that a dimension of the feature space is 25600. At the output of the last layer, which is fully connected neural network, there is a binary classification result. The proposed steganalysis scheme was tested against HUGO algorithm. BOSSbase database of images was utilized. Unfortunately, the experimental results for the proposed CNN, with a trained stack of convolutional auto-encoders and feature pooling layers, are not comparable with the results obtained for the RM scheme. Nevertheless, the concept is inspiring.

Another research on the use of deep learning for the purpose of steganalysis was presented in [29]. This article showed that a well parameterized Convolutional Neural Network (**CNN**) gives better results than the RM-based feature extraction with an ensemble classifier. However, the authors considered the scenario where the steganograph always uses the same embedding key for different images. The best examined CNN consists of two convolutional layers, followed by a three layer fully connected network. The pooling step in CNN was considered as not important or even interfering in the context of the steganalysis scenario, and thus, it was removed from the CNN resulting in 8% increase in classification results. The cost of this decision was an increase in the computational cost and an increase in GPU memory consumption. The experimental results show ~16% reduction in the classification error for the CNN over the results for the RM+EC method. The proposed steganalysis scheme was tested against S-UNIWARD algorithm. BOSSbase database of images was utilized. Additionally, the authors have created and used their own database of cover and stego images called LIRMMBase.

Another promising concept was presented in the article on ensemble of convolutional neural networks for steganalysis [30]. The authors pointed out that CNNs are suitable to form ensembles which in turn can give a better classification results. In the research, multiple CNNs were employed as base learners and multiple ensemble strategies were tested. Each of base CNNs was trained on a random subsample of the training dataset. The second-level classifiers of the ensemble were trained on the feature vectors obtained from: the direct output probabilities generated from the trained CNNs, the output probabilities generated from the CNNs with offsets in the spatial subsampling steps of pooling layers, and the output vectors of the convolutional modules in CNNs. The proposed steganalysis scheme was tested against S-UNIWARD algorithm. BOSSbase database of images was utilized.

The next work exploring the trend of deep learning in steganalysis was presented in [31]. In this paper, a CNN-based steganalyzer was designed to further improve the performance of the previous works. This work contributes to the field in two ways. Firstly, the structure of the proposed CNN is simplified. The convolution part has only two convolutional layers with hyperbolic tangent function as activation function. The final fully connected part is a classical neural network with a single output layer of two softmax neurons. The pooling operations are skipped. Secondly, the proposed CNN is more general because it's able to process larger images, it can detect steganographic schemes which embed messages in the spatial and the frequency domain, and with lower payload values. Utilized larger filters are more suited for complex images. Utilized filters depend on the input dataset and the expected data correlations. The proposed steganalysis scheme was tested against WOW, HUGO and J-UNIWARD algorithms. BOSSbase database of images was utilized.

Summarizing, current trends in steganalysis research are as follows. In the context of the domain of operation, steganalysis schemes extract features from both the spatial domain and the frequency domain. In the latter case, DCT and DWT transforms are utilized. In the context of methodology, Until 2012, steganalysis schemes utilized various concepts and metrics (see Table 1) for feature extraction and mostly SVM for classification. Later, until 2016, the most common trend was to use Rich Model (RM) of noise residuals for feature extraction and Ensemble Classifier (**EC**) for classification. Nowadays, the dominant trend is the use of Convolutional Neural Networks (CNN). This approach not only gives better steganalysis results than the previous solutions, but also combines two parts of the classic steganalysis scenario, i.e. feature extraction and classification, into a single algorithm. Currently presented research are in the form of empirical experiments aimed at adjusting the structure and the shape of CNNs, i.e. the number, the size, and the connectivity of the layers, adjusting the kernels or activation functions, etc. Lastly, in the context of testing, the selection of steganographic schemes, which have been attacked by new steganalysis schemes, has changed. At the beginning of this decade, for purpose of testing, researchers were choosing such algorithms as: e.g. LSB, Steghide, F5, Outguess, or JP Hide&Seek. Nowadays, validation of recent studies is based on attacks on HUGO, WOW, S-UNIWARD or J-UNIWARD algorithms.

3. GUIDELINES FOR NEW STEGANALYSIS SCHEMES

In this Section, guidelines for constructions of new steganalysis schemes or rather directions for future research have been presented. The first guideline is to build a blind steganalysis scheme, and not a targeted scheme. The reason for this choice is quite clear. Although, targeted steganalysis methods are able to effectively detect targeted steganographic systems and they can directly lead to the development of steganography, but they cease to be effective when new effective steganographic schemes are developed. In the meantime, blind steganalysis methods could be used potentially to detect even steganalysis schemes which don't exist yet. This means that blind steganalysis techniques provide much more value from a practical point of view, as well as, from a research point of view, because the same blind steganalysis scheme could be used as a testing tool for a comparison of multiple steganographic schemes. Furthermore, if a training dataset for a classifier of steganalysis scheme comes from a single steganographic scheme, then a blind method can be considered as a targeted method.

The major trend in steganalysis is to, firstly, obtain a high dimensional feature vector and, secondly, to use a classifier, which is trained on the basis of that feature vector. In order to get better and better classification results, the dimensionality of feature vectors continues to grow. However, with increasing dimensionality of feature sets, the classification task becomes harder and the number of labeled samples required for training process grows larger. Consequently, there is a challenge of finding better classifiers to work with high dimensional features. In the first half of

this decade, the most popular classification tool was SVM, which has great complexity in case of high dimensionality of features vectors. Later, various studies have shown that ensemble classifier gives better results than SVM, so EC-based steganalysis schemes have been developed, e.g. RM+EC. In recent years, it has been shown that stacked auto-encoders (SAE) and convolutional neural networks (CNN) gives much better results than SVM and better or comparable results than EC. Not only that but CNN-based steganalyzer allows to unify feature extraction and classification in one uniform algorithm. Therefore, the second guideline is to use the deep learning architecture both for feature extraction and classification, e.g. Convolutional Neural Networks (CNN), Stacked Auto-Encoders (**SAE**), or Deep Belief Networks (**DBN**). Deep learning architectures are used with a great success for solving problems of recognition and classification of images or videos. Therefore, the introduction of deep learning should be beneficial to blind steganalysis since the goal of steganalysis is actually image classification. Existing studies indicate that the best approach is to use CNN which is composed of multiple convolutional layers and some fully connected layers of neurons, similar to classical neural networks. The task of the convolutional layers is to learn how to extract feature maps from input images so that the final map, which is used as an input for the fully connected part of CNN, gives the most accurate representation of the input image, and consequently the best classification results. This approach reduces of the input's dimensionality and automatically finds the most suitable feature sets.

The next aspect of steganalysis scheme is a domain of operation. In theory, the best results should be obtained if the steganalysis scheme operates, i.e. extracts features, in the same domain as the most popular steganographic schemes, i.e. in spatial domain and DCT domain, or in the same domain which is most often used to store and transfer images, i.e. DCT domain because of JPEG format. On the other hand, embedding changes introduced by steganographic scheme could be difficult to detect in the domain of operation of the embedding algorithm, but noticeable in other domains, e.g. DWT domain. Besides, as mentioned above, blind steganalysis schemes can be used to detect unknown steganographic schemes in which case the domain is unknown. Consequently, the third guideline is to build multi-domain steganalysis schemes to ensure that the method will be truly universal.

Majority of steganalysis studies consider only greyscale images assuming that steganographic schemes embed secret messages only in the luminance of image and stating that the case of steganalysis of color images can be realized by duplicating algorithm for other components of a color image, i.e. chrominance or other in case of e.g. RGB representation. Naturally, this approach is not ideal because it leads to linear increase in computational requirements in case of steganalysis of color images, where the coefficient of linear increase is equal to the number of color channels. The fourth guideline is to use an algebra supporting calculations in all components of color images simultaneously, e.g. quaternion algebra [39,40]. Three color channels (or one luminance channel and two chrominance channels) of the image can be considered as a 3D space and each element of the image, e.g. pixel, can be represented as a point in this 3D space. Currently, quaternions are used in graphical APIs (DirectX, OpenGL) because 3D movement using quaternions is calculated faster and easier than using other algebra. Quaternions can represent many 3D transformations, such as reflections, scaling, translations and more. To solve these problems we can model 3D transformations in a 4D space using quaternions. Quaternions have already been used successfully to process color images for the purpose of encryption [41,42] and digital fingerprinting [43,44] but not yet for steganalysis.

Finally, the fifth guideline is to define testing scenarios which enable fair comparison with other studies. Currently, most recent steganalysis schemes were tested against HUGO, WOW, S-UNIWARD and J-UNIWARD steganographic schemes. Moreover, every recent steganalysis scheme utilized cover and stego images from the BOSSbase or the LIRMMBase. In order to compare the performance of a newly designed steganalysis scheme with the existing ones, the new scheme should be tested in similar scenarios, i.e. using the same steganographic algorithms, similar parameters and common databases of images.

4. CONCLUSIONS

This paper concerns blind steganalysis techniques in the passive steganalysis scenario designed to detect the steganographic cover modification schemes. The current state-of-art has been investigated and the current trends have been identified. Firstly, publications have been categorized due to the utilized trends, i.e. domains of operation, approaches, concepts, models, metrics, etc. Then, the selected works, that have had the greatest influence on the current trends, have been further described. In the last Section, guidelines for constructions of new steganalysis schemes have been presented.

The first guideline is to build a blind steganalysis scheme, and not a targeted scheme. The second guideline is to use the deep learning architecture both for feature extraction and classification, e.g. Convolutional Neural Networks (CNN), Stacked Auto-Encoders (SAE), or Deep Belief Networks (DBN). The third guideline is to build multi-domain steganalysis schemes to ensure that the method will be truly universal. The fourth guideline is to use an algebra supporting calculations in all components of color images simultaneously, e.g. quaternion algebra. The fifth guideline is to define testing scenarios based on well-known steganographic schemes, which enable fair comparison with other studies. The determined guidelines provide directions for future research for the author of the paper.

REFERENCES

[1] Fridrich J., "Steganography in Digital Media: Principles, Algorithms, and Applications", Cambridge, UK: *Cambridge University Press*, ISBN: 978-0-521-19019-0, 2010.

[2] Westfeld A., *High capacity despite better steganalysis (F5 – a steganographic algorithm), Information Hiding*, 4th Int. Workshop, vol. 2137 of Lecture Notes in Computer Science, pp. 289-302, 2001.

[3] Kodovský J., J. Fridrich, *Influence of embedding strategies on security of steganographic methods in the JPEG domain*, Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, vol. 6819, pp. 02-1-02-13, 2008.

[4] Fridrich J., M. Goljan, D. Soukal, *Efficient Wet Paper Codes, Information Hiding.* 7th International Workshop, LNCS vol. 3727, pp. 204-218, 2005.

[5] Li Z., K. Lu, X. Zeng, X. Pan, *Feature-Based Steganalysis for JPEG Images*, Int. Conf. Digital Image Processing, pp. 76-80, 2009.

[6] Deng Q.L., J.J. Lin, *A Universal Steganalysis Using Features Derived from the Differential Image Histogram in Frequency Domain*, CISP '09. 2nd Int. Congress on Image and Signal Processing, pp. 1-4, 2009.

[7] Yu W., Z. Li, L. Ping, *Blind detection for JPEG steganography*, Int. Conf. on Networking and Information Technology (ICNIT), pp. 128-132, 2010.

[8] Deng Q.L., *The blind detection of information hiding in color image*, 2nd Int. Conf. on Computer Engineering and Technology (ICCET), vol. 7, pp. V7-346-V7-348, 2010.

[9] Joo J.C., T.W. Oh, J.H. Choi, H.K. Lee, *Steganalysis Scheme Using the Difference Image of Calibrated Sub-sampling*, 6th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, pp. 51-54, 2010.

[10] Fridrich J., "Rich Models for Steganalysis of Digital Images", *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, 2012.

[11] Ge H., H. Liu and Z. Jin, *Key Technical Analysis on Steganography and Steganalysis*, 3rd Int. Conf. Multimedia Technology ICMT, 2013.

[12] Lin J.Q.; S.P. Zhong, *JPEG image steganalysis method based on binary similarity measures,* Int. Conf. on Machine Learning and Cybernetics, vol. 4, pp. 2238-2243, 2009.

[13] Yang G., H. Zhang, *Using Higher Order DCT Difference to Effective Improve Markov Process Based JPEG Steganalysis Detection Rate*, Asia-Pacific Conf. Information Processing, vol. 2, pp. 47-50, 2009.

[14] Liu S., L. Ma, H. Yao, D. Zhao*, Universal Steganalysis Based on Statistical Models Using Reorganization of Block- based DCT Coefficients*, 5th Int. Conf. Information Assurance and Security IAS '09, vol. 1, pp. 778-781, 2009.

[15] He Z.M.; W.W.Y. Ng, P.P.K. Chan, D.S. Yeung, *Steganography detection using localized generalization error model*, IEEE Int. Conf. Systems Man and Cybernetics (SMC), pp. 1544-1549, 2010.

[16] Chen Q., S. Zhong, *Universal Steganographic Detection Algorithmin in JPEG Image Using the Data-Dependent Kernel*, 3th Int. Symposium on Electronic Commerce and Security (ISECS), pp. 232-236, 2010.

[17] Bhat V.H., S. Krishna, P.D. Shenoy, K.R. Venugopal, L.M. Patnaik*, HUBFIRE – A multi-class SVM based JPEG steganalysis using HBCL statistics and Fr Index*, Int. Conf. Security and Cryptography, pp. 1-6, 2010.

[18] Ping Q., C. Li-ya, W. Meng, *A universal steganalysis to steganographic images on frequency domain*, Int. Conference E-Business and E -Government (ICEE), pp. 1-5, 2011.

[19] Anitha P. T., M. Rajaram, S. N. Sivanandham, "Neural Network Based Steganalysis Framework to Detect Stego-Contents in Corporate Emails", *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, issue 3, 2012.

[20] Geetha S., S.S. Sindhu, N. Ishwarya, A. Mohan, P. Amuthayazhini, N. Kamaraj, *Intelligent detection of LSB stego anomalies in images using soft computing paradigms*; Int. Conf. Methods and Models in Computer Science, pp. 1-5, 2009.

[21] Sun Z., H. Li, Z. Wu, Z. Zhou, *An Image Steganalysis Method Based on Characteristic Function Moments of Wavelet Subbands*, Int. Conf. Artificial Intelligence and Computational Intelligence, vol. 1, pp. 291-295, 2009.

[22] Yang X., S. Wang, J. Liu, *Universal Steganalysis to Images with WBMC Model*, 5th Int. Conf. Information Assurance and Security, vol. 2, pp 627–630, 2009.

[23] Ramezani M., S. Ghaemmaghami, *Towards Genetic Feature Selection in Image Steganalysis,* 7th IEEE Consumer Communications and Networking Conference, pp. 1-4, 2010.

[24] Gireesh Kumar T., R. Jithin, D.D. Shankar, Int.Conf. Feature Based Steganalysis Using Wavelet Decomposition and Magnitude Statistics Advances in Computer Engineering, pp. 298-300.

[25] Li H.; Z. Sun, Z. Zhou*, An image steganalysis method based on characteristic function moments and PCA,* 30th Chinese Control Conference (CCC), pp. 3005-3008, 2011.

[26] Yang X., Y. Lei, X. Pan, J. Liu, *Universal Image Steganalysis Based on Wavelet Packet Decomposition and Empirical Transition Matrix in Wavelet Domain*; Int. Forum on Computer Science, Technology and Applications IFCSTA '09, vol. 2 pp. 179-182, 2009.

[27] He F., S. Zhong, K. Chen. "An Effective Ensemble-based Classification Algorithm for High-Dimensional Steganalysis", *Journal of Software,* vol. 9, no. 7, 2014.

[28] Tan S., B. Li, "Stacked Convolutional Auto-Encoders for Steganalysis of Digital Images", Asia-Pacific Signal and Information Processing Association", 2014 *A*nnual Summit and Conference (APSIPA), 2014.

[29] Pibre L., J. Pasquet, D. Ienco, M. Chaumont, *Deep learning is a good steganalysis tool when embedding key is reused for different images*, even if there is a cover sourcemismatch, IS&T. Media Watermarking, Security and Forensics, Part of IS&T Int. Symp. On Electronic Imaging, 2016.

[30] Xu G., H. Wu, Y.Q. Shi, "Ensemble of CNNs for Steganalysis: An Empirical Study", *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*, pp. 103-107, 2016.

[31] Couchot J., R. Couturier, C. Guyeux, M. Salomon, *Steganalysis via a Convolutional Neural Network using Large Convolution Filters,* CoRR abs/1605.0794, 2016.

[32] Yu X.Y., A. Wang, *An Investigation of Genetic Algorithm on Steganalysis Techniques,* 5th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing, pp. 1118-1121, 2009.

[33] Yu X.Y., A. Wang*, Steganalysis Based on Regression Model and Bayesion Network*, Int. Conf. Multimedia Information Networking and Security, vol. 1, pp. 41-44, 2009.

[34] Yu X.Y., A. Wang, *Steganalysis Based on Bayesion Network and Genetic Algorithm,* 2nd Int. Congress on Image and Signal Processing CISP '09, pp. 1-4, 2009.

[35] Sheikhan M., M.S. Moin, M. Pezhmanpour*, Blind image steganalysis via joint co-occurrence matrix and statistical moments of contourlet transform*; 10th Int. Conf. Intelligent Systems Design and Applications (ISDA), pp. 368-372, 2010.

[36] Veena H.B., S. Krishna, P.D. Shenoy, *SURF: Steganalysis using random forests*, 10th Int. Conf. Intelligent Systems Design and Applications (ISDA), pp. 373-378, 2010.

[37] Ke K., T. Zhao, O. Li, *Bhattacharyya Distance for Blind Image Steganalysis*; Int. Conf. Multimedia Information Networking and Security (MINES), pp. 658-661, 2010.

[38] Holoska J., Z. Oplatkova, I. Zelinka, R. Senkerik, *Comparison between Neural Network Steganalysis and Linear Classification Method Stegdetect*, 2nd Int. Conf. Computational Intelligence, Modelling and Simulation, pp. 15 – 20, 2010.

[39] Zhang F., *Quaternion and Matrices of Quaternions*, *Linear Algebra and its Applications*, Elsevier Science Inc., pp. 21-57, 1997.

[40] Baker M.J.*, Maths - Quaternions*, http://www.euclideanspace.com/maths/algebra/realNormedAlgebra/quaternions/index.htm, date: 18.06.2014.

[41] Dzwonkowski M., M. Papaj, R. Rykaczewski, "A New Quaternion--Based Encryption Method for DICOM Images", IEEE Transactions on Image Processing, vol. 24, issue 11, pp. 4614-4622, 2015.

[42] Dzwonkowski M., R. Rykaczewski, "Quaternion Feistel Cipher with an infinite key space based on quaternion Julia sets", *Journal of Telecommunications and Information Technology,* vol. 4, pp. 15-21, 2015.

[43] Czaplewski B., R. Rykaczewski, "Receiver-side fingerprinting method for color images based on a series of quaternion rotations"*, Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne / Telecommunication Review + Telecommunication News*, vol. 8-9, pp. 1127-1134, 2015.

[44] Czaplewski B.,"Joint fingerprinting and decryption method for color images based on quaternion rotation with cipher quaternion chaining"*, Journal of Visual Communication and Image Representation*, vol. 40, part A, pp. 1-13, 2016.