International Science Journal of Engineering & Agriculture
2022; 1(3): 133-142
https://isg-journal.com/international-science-journal-of-engineering-agriculture/
doi: 10.46299/j.isjea.20220103.11
ISSN: 2720-6319

INTERNATIONAL
SCIENCE GROUP

UNIVERSAL APPROACH TO THE IDENTIFICATION OF STEGANOGRAPHIC TRANSFORMATION OF THE SPATIAL DOMAIN OF DIGITAL IMAGES

Hanna Akhmametieva[1]
[1]Faculty of Cyber Security and Information Technology, National University "Odesa Law Academy", Odesa, Ukraine
ORCID 0000-0002-0567-902X
Email address:anna.odessitka@gmail.com

To cite this article:
Hanna Akhmametieva. Universal approach to the identification of steganographic transformation of the spatial domain of digital images. International Science Journal of Engineering & Agriculture. Vol. 1, No. 3, 2022, pp. 133-142. doi: 10.46299/j.isjea.20220103.11.
Received: 06 21, 2022; **Accepted**: 07 27, 2022; **Published**: 08 01, 2022

Abstract: The article proposes a universal approach to detect the presence of additional information attachments in the spatial domain of digital images. The approach is based on the use of the steganalytic method developed by the author earlier and based on the analysis of sequential triads of triplets in the matrix of unique colors of image. The steganoanalytic method Color Triads allows to detect with high accuracy the additional information attachments embedded by various steganographic methods into the spatial domain of images. The perturbations in the matrix of unique colors of images as a result of steganographic transformation are illustrated which concludes about the sensitivity of the blue color component even to small modifications of the brightness values of this matrix. The efficiency of detecting stegoes formed at small values of payload (0.4 bpp and less) based on LSB, S-UNIWARD, MiPOD and WOW steganographic methods is shown. The obtained results of computational experiments allow detect the filled color components of digital images with high accuracy even at payload of 0.1 and 0.05 bpp that is much higher than the results of modern analogues. The steganalytic method analyzes the spatial domain of images, which avoids the accumulation of computational errors that affect the detection result.

Keywords: Steganalysis, Digital Image, Spatial Domain

1. Introduction

Wide use of digital technologies and the computer equipment in any sphere of human activity leads to the need to protect information from leakage or unauthorized use and copying. Due to restrictions on the use of cryptographic tools developments in the field of

steganography has become widespread which allows organizing a hidden channel for transmitting confidential data that can be used by attackers to steal valuable information. Therefore, an important task is development of steganalysis aimed at detecting any additional information in the analyzed digital content [1]. The most convenient container in steganography is a digital image due to the presence of redundant information in it and the possibility of concealing a considerable amount of data.

One of the most widespread steganographic methods is the method of replacing the least significant bit (LSB) thanks to its simplicity of implementation and ensuring high payload. However, this method is absolutely unstable to compression and different modifications, for example, to affine transformations or imposing of noise.

Despite the existing shortcomings of application of steganographic transformation of spatial domain of images new methods such as PVD [2], HUGO [3], WOW [4], MVG [5], S-UNIWARD [6], Hill [7], MiPOD [8] are developed. These methods are often applied for testing of new steganalytic developments including in the conditions of small payload that considerably complicates process of identification such stego – result of embedding of additional information to the container.

Most of the steganalytic methods aimed at detecting of additional information attachments in digital images carry out an analysis of the transformations domain of digital image. However, it leads to an accumulation of computational error which greatly affects the efficiency of stego detection especially in the case of small payload (0.5 bpp or less).

A wide class of steganalytic methods is devoted to the construction of neural networks and their training with the subsequent classification of stego and unfilled containers [9-16]. Among recent developments can be distinguished [9] where detection errors for the 0.2 bpp payload on average 11.8% for the WOW method and 17.5% for HUGO. In work [10] when detecting stego formed by the WOW method with a payload of 0.2 bpp the errors are 24%. Somewhat fewer classification errors for stego and empty containers for the same method in [11] – here they make up 16.7%.

The situation is even worse for a payload of 0.1 bpp. In [11] percent of incorrectly classified digital contents makes 24.4% and 32.2% respectively for the WOW and S-UNIWARD methods. In work [12] detection errors belong to the range from 23 to 42% for the S-UNIWARD and MiPOD methods.

Steganalysis in the domain of singular decomposition of matrices represented by works [17, 18] is less common. However, in these methods we can see low efficiency of detecting stego at small values of payload. For example, steganalysis by SAVV [18] method gives 20% of errors in case of the 0.2 bpp payload while the KBG method [17] considers cases of payload of 0.5 bpp and above.

Thus, the analysis of the transformation domain of digital images does not provide a high efficiency of detecting stegoes formed at small payload. Solution to this problem is the analysis of the spatial domain of digital images which will avoid the accumulation of computational errors and improve the detection of hidden messages embedded in the spatial domain of digital images with low payload.

In view of a wide choice of the steganographic methods modifying spatial domain of

images the universal approach to detecting stegoes and empty containers is offered in work based on the steganalytic method for digital images developed by the author earlier.

2. Theoretical basis of the steganalytic method based on the analysis of sequential triads of color triplets

In [19] a steganalytic method for digital images and video was proposed. The method is based on the analysis of sequential triads of color triplets in a matrix of unique colors of image and showed high efficiency in detecting stegoes formed by LSB method with low values of payload. The essence of a method consists in the following.

As containers for a steganographic transformation we will consider color digital images in a format with losses presented according to the color scheme RGB where each pixel of the image is described as a triple of values (r_{mn}, g_{mn}, b_{mn}), r_{mn}, g_{mn}, b_{mn} - brightness values of the (m,n)-th pixel of the red, green and blue color matrixes respectively. All unique triplet's values of the digital image we will call unique colors, their number is denoted by U.

The steganalytic method is based on calculation of quantity of sequential Red-, Green-and Blue-triads in the matrix of unique colors UCT containing U ordered unique triplets (r_k, g_k, b_k), $k \in [1,U]$.

We will understand as sequential Red-, Green-and Blue-triads:

$$(r_k, g_k, b_k) \in UCT \ \& \ (r_{k-1}, g_k, b_k) \in UCT \ \& \ \& \ (r_{k+1}, g_k, b_k) \in UCT \quad (1)$$

$$(r_k, g_k, b_k) \in UCT \ \& \ (r_k, g_{k-1}, b_k) \in UCT \ \& \ \& \ (r_k, g_{k+1}, b_k) \in UCT \quad (2)$$

$$(r_k, g_k, b_k) \in UCT \ \& \ (r_k, g_k, b_{k-1}) \in UCT \ \& \ \& \ (r_k, g_k, b_{k+1}) \in UCT \quad (3)$$

respectively. When counting the sequential triads of triplets we will associate sequential triad with $(r_k, g_k, b_k) \in UCT$ for which execution of the conditions (1), (2) or (3) depending on the type of triad is carried out. Triplet $(r_k, g_k, b_k) \in UCT$ we will call middle if there is a sequential triad for him.

The empty container in a format with losses contains no more than 2.5% of middle triplets corresponding to Red-, Green- and Blue-triads. At embedding of additional information their quantity considerably increases and in case of one filled color component indicates the color matrix of the image used in the process of a steganographic transformation.

The main steps of the earlier developed method are given in [19].

3. Evaluation of the efficiency of the steganalytic method using various methods of embedding secret information

Taking into account the fact that the method based on the analysis of sequential triads of triplets in a matrix of unique colors is initially directed against LSB steganography, we will consider its possibilities for identifying stegoes formed by other methods modifying the spatial domain of digital images.

To evaluate the efficiency of the proposed steganalytic method a computational experiment based on 418 color digital images from [20] and photos taken by nonprofessional cameras in JPG format was conducted. Use of color images in a format with losses as containers is caused by their availability: it is easy to receive such containers by means of any devices (digital cameras, smart phones, tablets, etc.) or to take them from image database. And although in most studies computational experiments are carried out on the basis of grayscale images they are quite rare in modern world. As a rule, it is professional art photos which there are not (or very few) in open access. Therefore in this work into the analysis the efficiency of the steganalytic method we will understand the correctness of detecting the filled and empty color components of a color image.

The embedding of additional information into digital images is carried out into one arbitrarily selected color component with payload of 0.4, 0.2, 0.1 and 0.05 bpp by S-UNIWARD, MiPOD and WOW steganographic methods.

According to the results of steganalysis of formed stego errors of the first (False Negative *FN*) and the second type (False Positive *FP*) are obtained (see Table 1) where errors of the first type indicate a stego omission, errors of the second type indicate the definition of an empty container as stego.

Table 1. The efficiency of detecting the presence/absence of additional information in digital images, %

	S-UNIWARD				**MiPOD**				**WOW**			
Payload, bpp	0.4	0.2	0.1	0.05	0.4	0.2	0.1	0.05	0.4	0.2	0.1	0.05
FN	0.16	0.66	4.11	14.45	0.33	1.32	8.70	14.12	0	0.82	3.78	11.33
FP	0.49											

An example of the quantity of sequential triads of triplets in the matrix of unique colors relative to the total number of unique colors of image with payload of 0.1 bpp for different steganographic methods is shown in Fig.1.

As can be seen from Fig.1 the number of basic triads exceeds the number of concomitant triads and unambiguously indicates the color component used in the process of steganographic transformation. Here the basic triad is a sequential triad corresponding to color component of the container into which embedding of additional information was carried out and concomitant triads are those that correspond to unfilled color components of the container.

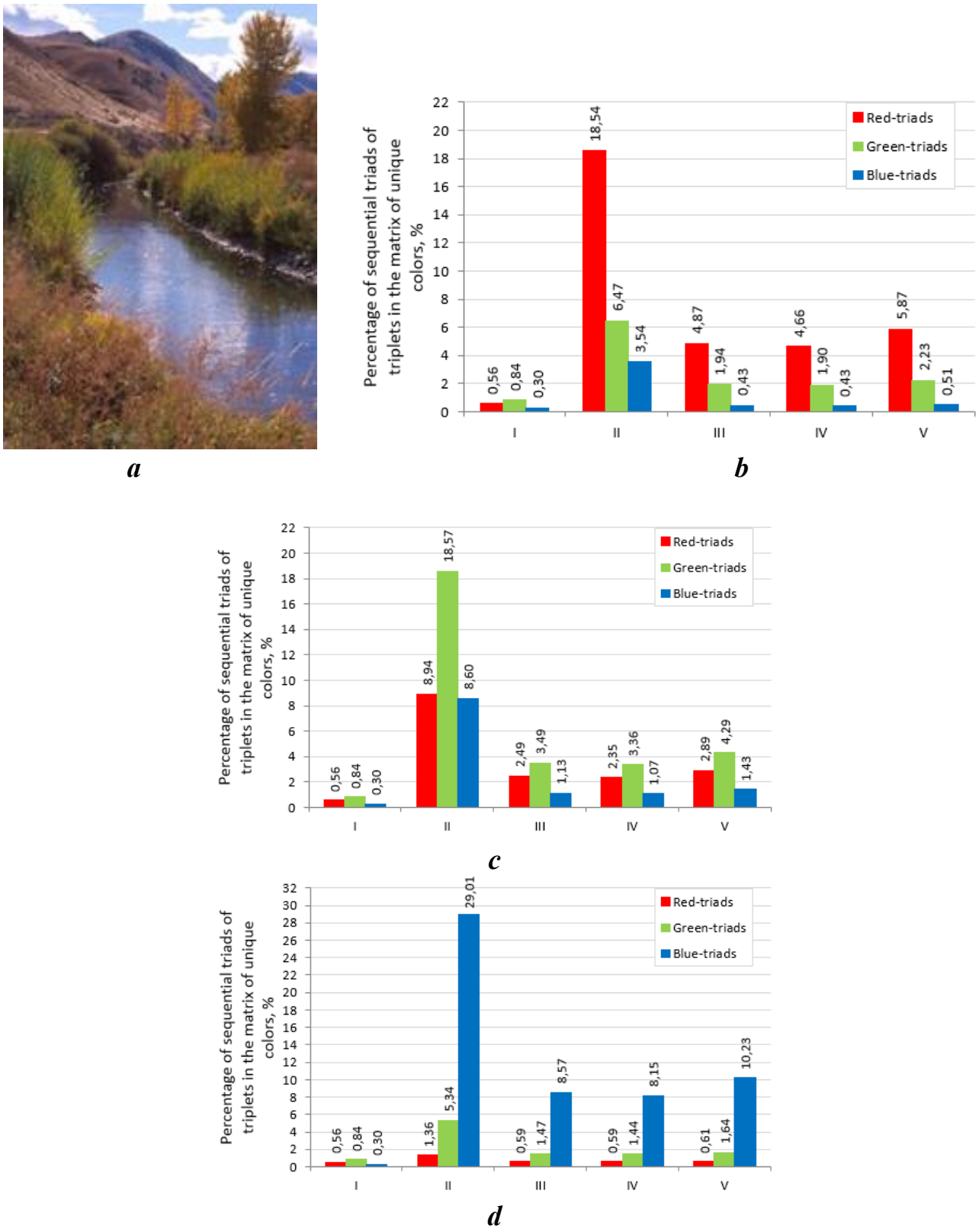

Figure 1. The percentage of sequential triads of triplets in the matrix of unique colors of container (a) and stego formed by embedding of additional information into red color component (b), into green color component (c), into blue color component (d) by various methods: I - container; II - LSB method; III - S-UNIWARD method; IV - MiPOD method; V - WOW method

Although the perturbations in the matrix of unique colors of stego formed by S-UNIWARD, MiPOD and WOW methods are noticeably less than in case when additional information was embedded by the LSB method it is still possible to determine the filled color component even at payload of 0.1 bpp. In addition, based on the conducted experiments the following feature is characteristic of the majority of digital images. The most sensitive to perturbations caused by the steganographic transformation is the blue color component (Fig.1, d), despite the fact that its use is due to the insensitivity of the human vision to blue color. The green color component of image is the least sensitive to perturbations (Fig.1, c).

To determine the detection errors of the steganalytic method (hereinafter "Color Triads") and the subsequent comparison of its efficiency with modern analogues a computing experiment was conducted on the basis of images including both unfilled containers and stegoes formed at different values of payload. The results of the comparison are presented in Tables 2, 3, 4 respectively for the S-UNIWARD, MiPOD and WOW steganographic methods.

Table 2. Comparison of detection errors for various steganalytic methods of S-UNIWARD-steganography identification under various payload values

Payload, bpp	SRM +EC from [12]	CNN from [12]	CNN + SRM + EC from [12]	SCA-TLU-CNN from [11]	FLD from [13]	LSMR from [14]	LASSO from [15]	Color Triads
0.4	0.2205	0.0905	0.1587	0.1281	–	–	–	**0.0033**
0.2	–	–	–	0.2224	0.3364	0.3342	0.3671	**0.0057**
0.1	0.41	0.2336	0.3888	0.322	–	–	–	**0.0230**
0.05	–	–	–	0.4	–	–	–	**0.0747**

Table 3. Comparison of detection errors for various steganalytic methods of MiPOD-steganography identification under various payload values

Payload, bpp	SRM + EC from [12]	CNN from [12]	CNN + SRM+EC from [12]	FLD from [13]	LSMR from [14]	LASSO from [15]	Color Triads
0.4	0.2389	0.0926	0.1565	–	–	–	**0.0041**
0.2	–	–	–	0.3321	0.3307	0.3669	**0.0091**
0.1	0.4213	0.2188	0.4024	–	–	–	**0.0459**
0.05	–	–	–	–	–	–	**0.0731**

Table 4. Comparison of detection errors for various steganalytic methods of WOW-steganography identification under various payload values

Payload, bpp	[10]	SCA-TLU-CNN from [11]	FLD from [13]	LSMR from [14]	LASSO from [15]	[16]	Color Triads
0.4	0.1658	0.0959	–	–	–	0.0272	**0.0049**
0.2	0.2472	0.1691	0.3289	0.3267	0.3694	–	**0.0065**
0.1	–	0.2442	–	–	–	0.2226	**0.0213**
0.05	–	0.345	–	–	–	–	**0.0591**

As can be seen from Tables 2-4 a steganalysis of the spatial domain of color digital images allows to significantly improve results of detecting the fact of presence of additional information in the analyzed contents on condition of small payload values. In the case of a 0.2 bpp payload detection errors were reduced from 0.2224 to 0.0057

(S-UNIWARD), from 0.3321 to 0.0091 (MiPOD) and from 0.1691 to 0.0065 (WOW) compared to the best analogues. In the case of a 0.1 bpp payload detection errors were reduced from 0.2336 to 0.0230 (S-UNIWARD), from 0.2188 to 0.0459 (MiPOD) and from 0.2226 to 0.0213 (WOW) in comparison with the best analogues.

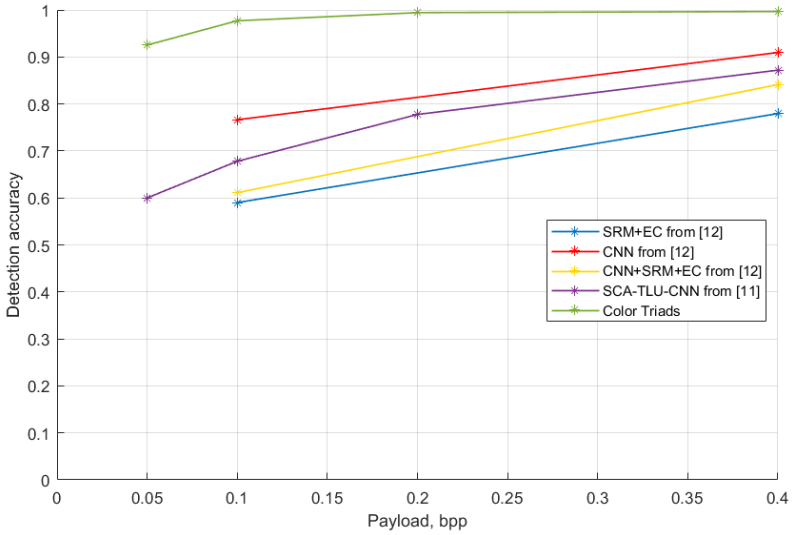

Figure 2. Detection accuracy of S-UNIWARD-steganography

At identifying of additional information attachments with payload of 0.05 bpp detection errors are 0.0747 and 0.0591 for the S-UNIWARD and WOW steganographic methods respectively which are significantly less than data provided by the only analogues. For the MiPOD method detection errors are 0.0731.

Figures 2-4 show a graphical representation of the results of detecting of additional information attachments in images using various steganoanalytic methods. Detection accuracy refers to the proportion of correctly defined stegos and empty containers among the entire set of images, including both filled and unfilled images.

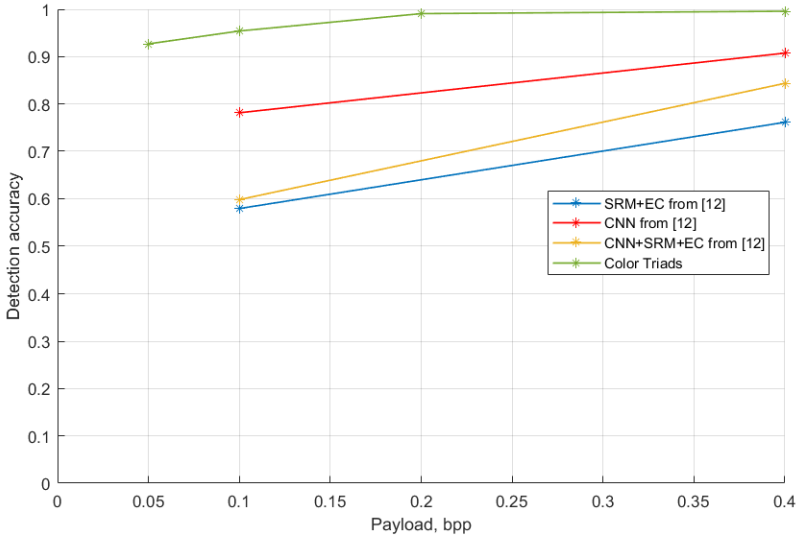

Figure 3. Detection accuracy of MiPOD-steganography

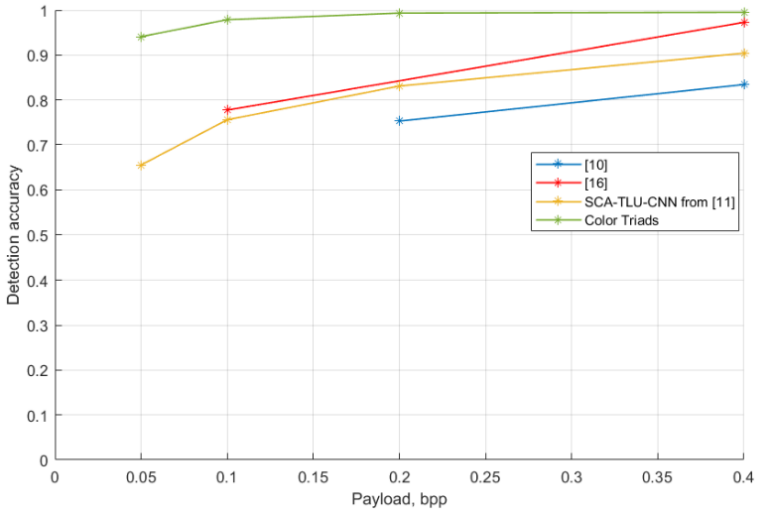

Figure 4. Detection accuracy of WOW-steganography

Table 5 provides a comparison of the integral parameter ρ defined in the ROC-analysis as

$$\rho=2A-1,$$

where A is the area under the ROC-curve, with analogues in case when additional information embeds by LSB steganography.

Thus, based on the obtained results of computational experiments the steganalytic method "Color Triads" makes it possible to effectively detect attachments of additional information in digital images when using different steganographic methods modifying spatial domain of containers in a format with losses.

Table 5. Comparison of integral parameter ρ for various steganalytic methods of LSB-steganography identification under various payload values

Payload, bpp	Ker's [21]	Liu's [22]	HGE [23]	NDH COM [23]	RLH COM [23]	Fused feature [23]	Joint feature set [23]	SAVV [18]	KBG [17]	Color Triads
1	0.938	0.993	0.564	0.924	0.851	0.938	0.973	0.995	0.981	**1**
0.75	0.905	0.988	0.462	0.765	0.847	0.914	0.964	0.980	0.962	**1**
0.5	0.585	0.961	0.290	0.521	0.830	0.732	0.944	0.950	0.930	**1**
0.4	–	–	–	–	–	–	–	0.920	–	**1**
0.3	–	–	–	–	–	–	–	0.884	–	**1**
0.25	0.135	0.802	0.063	0.263	0.732	0.373	0.886	0.849	–	**1**
0.2	–	–	–	–	–	–	–	0.799	–	**1**
0.1	–	–	–	–	–	–	–	0.420	–	**0.990**
0.05	–	–	–	–	–	–	–	0.188	–	**0.959**

Respectively the analysis of sequential triads of triplets in the matrix of unique colors of digital images is universal approach to identification of steganographic transformation of the spatial domain of containers.

4. Conclusion

The paper presents the results of computational experiments for the developed earlier steganalytic method “Color Triads” aimed at detecting the attachments of additional information embedded by various steganographic methods in the spatial domain of digital images.

Comparison of the “Color Triads” method with other modern analogues showed that the analysis of spatial domain of digital contents based on accounting the quantity of color triads in the matrix of unique colors is universal and provides an effective identification of stegoes created at small values of payload (0.1 and 0.05 bpp).

At present researches are being carried out on the possibility of determining the filled color components of digital images in cases when additional information embeds into two and three color components which will allow expand a “Color Triads” method’s scope of application.

References

1) Bohme, R.: Advanced statistical steganalysis. Springer, Berlin (2010).
2) Wu, D.C., Tsai, W.H.: A Steganographic method for images by pixel-value differencing. Pattern Recognition Letters, vol.24, 1613-1626 (2003).
3) Filler, T., Fridrich, J.: Gibbs Construction in Steganography. IEEE Transactions on Information Forensics and Security, vol.4, iss.5, 705-720 (2010).
4) Holub, V., Fridrich, J.: Designing Steganographic Distortion Using Directional Filters. In: 2012 IEEE International Workshop on Information Forensics and Security (WIFS 2012), pp. 1-6. IEEE, Tenerife, Canary Islands (2012).
5) Fridrich, J., Kodovsky, J.: Multivariate Gaussian model for designing additive distortion for steganography. In Proc. IEEE, International Conference on Acoustics, Speech and Signal Processing (ICASSP 2013), pp. 1-5. IEEE, Vancouver, Canada (2013).
6) Holub, V., Fridrich, J., Denemark, T.: Universal Distortion Function for Steganography in an Arbitrary Domain. EURASIP Journal on Information Security (Section: SI: Revised Selected Papers of ACM IH and MMS 2013), 1-13 (2014).
7) Shuliang Sun, Yongning Guo: A Novel Image Steganography Based on Contourlet Transform and Hill Cipher. Journal of Information Hiding and Multimedia Signal Processing, vol.6, no.5, 889-897 (2015).
8) Sedighi, V., Cogranne, R., Fridrich, J.: Content-Adaptive Steganography by Minimizing Statistical Detectability. IEEE Transactions on Information Forensics and Security, vol.11, iss.2, 221-234 (2016).
9) Lerch-Hostalot, D. Meg´ıas, D.: Unsupervised steganalysis based on artificial training sets. Engineering Applications of Artificial Intelligence, vol.50, 45-59 (2016).
10) Denemark, T., Fridrich, J., Comesaña, P.: Improving Selection-Channel-Aware Steganalysis Features. Media Watermarking, Security, and Forensics, 1-8 (2016).

11) Jian Ye, Jiangqun Ni, Yang Yi: Deep Learning Hierarchical Representations for Image Steganalysis. IEEE Transactions on Information Forensics and Security, vol.12, iss.11, 2545-2557 (2017).
12) Couchot, J.-F., Couturier, R., Salomon, M.: Improving Blind Steganalysis in Spatial Domain Using a Criterion to Choose the Appropriate Steganalyzer Between CNN and SRM+EC. In IFIP International Conference on ICT Systems Security and Privacy Protection, pp. 327-340. Springer, Rome, Italy (2017).
13) Kodovsky, J., Fridrich, J., Holub, V.: Ensemble classifiers for steganalysis of digital media. Information Forensics and Security, IEEE Transactions, vol.7, no.2, 432-444 (2012).
14) Fong, D.C.-L., Saunders, M.: LSMR: An iterative algorithm for sparse least-squares problems. SIAM Journal on Scientific Computing, vol. 33, no. 5, 2950-2971 (2011).
15) Cogranne, R., Sedighi, V., Fridrich, J., Pevný, T.: Is Ensemble Classifier Needed for Steganalysis in High-Dimensional Feature Spaces? IEEE International Workshop on Information Forensics and Security (WIFS 2015), pp.1-6. IEEE, Rome, Italy (2015).
16) Salomon, M., Couturier, R., Guyeux, C., Couchot, J.-F., Bahi, J.M.: Steganalysis via a convolutional neural network using large convolution filters for embedding process with same stego key: A deep learning approach for telemedicine. European Research in Telemedicine / La Recherche Européenne en Télémédecine 6, 79-92 (2017).
17) Kobozeva, A.A., Bobok, I.I., Garbuz, A.I.: General Principles of Integrity Checking of Digital Images and Application for Steganalysis. Transport and Telecommunication, vol.17, no.2, 128-137 (2016).
18) Bobok, I.I.: Application of ROC-analysis for integrated assessment of steganalysis method's efficiency. Informatics and Mathematical Methods in Simulation, vol. 2, no. 3, 221-230 (2012).
19) Akhmametieva, A.: Steganalysis of digital contents, based on the analysis of unique color triplets. Annales Mathematicae et Informaticae, no. 47, 3-18 (2017).
20) NRCS Photo Gallery, http://photogallery.nrcs.usda.gov, last accessed 2016/03/14.
21) Ker, A.D.: Steganalysis of LSB matching in grayscale images. IEEE Signal Processing Letters, vol. 12, no. 6, 441-444 (2005).
22) Liu, Q.Z., Sung A.H.: Image complexity and feature mining for steganalysis of least significant bit matching steganography. Information Sciences, vol. 178, no. 1, 21-36 (2008).
23) Zhihua Xia, Lincong Yang: A Learning-Based Steganalytic Method against LSB Matching Steganography. Radioengineering, vol. 20, no. 1, 102-109 (2011).