Kozin Alexander Borisovich

National University "Odessa Law Academy,"

associate Professor of the Department of Information Technologies,

candidate of sciences (Physics and Mathematics), associate Professor

ANALYSIS OF MODERN METHODS OF CHECKING THE IMAGE INTEGRITY

Today, one of the areas of practical application of steganographic algorithms is the protection of copyright or property rights for multimedia products using digital watermarks (DW). DWs contain information that unequivocally confirms authorship or the rights to commercial use of the protected digital object, which can be read to resolve disputable legal situations. DW embedded in the protected image with the help of stegoalgorithms and solving the problem of copyright protection should have increase resistance to external influences or attacks on the protected digital object.

Thus, in our opinion, today the question of analyzing new modern integrated methods for checking the integrity of digital images is very urgent. In the open Internet, scientific articles of this direction were found.

In open press, effective stegomethods were found using small blocks [1-5].

Thus, in work [1] the authors proposed a method of photomontage detection based on the analysis of singular values of matrix blocks for digital images. Authors check the application of photomontage detection area method based on analysis of singular values of matrix blocks for digital images in the absence of restrictions on the degree of their compression. The basis of proposed method is the detection of the differences between the images when they have different degrees of compression. We distinguish this area on the background of the main image, that allows to detect falsification.

The authors of [2, 3], through searches in the field of steganography, suggest an algorithm for checking integrity, color digital images, analyzing potential

unauthorized changes additional information, which was embedded, made by third parties, with the intention of changing or destroying these digital objects and/or attachments.

In the scientific work [4], a steganographic method is proposed, which is based on the structure of confidential information in the frequency domain of the container, which is a digital image in the gray scale. The transition from spatial to frequency domain and vice versa occurs using the discrete Hartley transform. The matrix of frequency coefficients is constructed for blocks of partitioning the initial matrix of a digital image by a size 2×2. Due to the choice of the block of this size, not only the capacity of the communication channel was increased, in comparison with the standard breakdown, but also the zero imaginary part of the frequency coefficients was obtained.

In the analyzed works [2-4], modifications of digital images in the field of transformation, and justification of the area of DFT.

In work [5], an algorithm was developed for verifying the integrity violation of a digital color container image by unauthorized changes occurring in the frequency domain, taking into account the possibility of exceeding the range of the luminance of the pixel of the image matrix at the encoding step. In the presented scientific work, in order to achieve the set goal, the area of transformation of the DCT was chosen.

The division of the image matrix into blocks of different sizes and the calculation of the frequency coefficients of the discrete cosine transform for the blocks of the obtained sizes are analyzed. It is obtained that for the DCT and DFT units have the same frequency coefficient formation.

To check the integrity of the digital color container image from unauthorized changes, an algorithm was developed and the software product that realize it. The algorithm takes into account the possibility of exceeding the range of the brightness value of the pixel of the image matrix at the encoding step. The software implementation of the algorithm detects unauthorized changes even in one pixel.

In [6] sufficient conditions were obtained for the stability of stegomethods and stegoalgorithms for compression, including those with significant coefficients, independent of which area of the digital image container-the spatial or transformation domain-used to immerse additional information. The obtaining of these conditions was the result of the further development of a general approach to the analysis of the state and technology of the functioning of information systems based on matrix analysis and perturbation theory and its adaptation to the solution of steganography problems.

Conclusions

The analysis of modern methods of checking the integrity of images is carried out. The use of stegomethods and stegoalgorithms, implemented as software packages, can solve the problem of illegal use of digital information, which is intellectual property. Unfortunately, in Ukraine today, there is not a clear legal basis for using steganography methods to confirm copyrights or property rights for multimedia products using digital watermarks. And this problem must be solved as soon as possible, using the experience of our european and american partners.

References:

1. Zorilo, V. V. Method of photomontage detection under conditions of limitations absence for photos falsification / V.V. Zorilo, Ye. Yu. Lebedeva, M.O.Kozina, D. S. Belush // Пр. Одес. політехн. ун-ту. - Одеса,2016. - Вип.2 (49). - P.84-87.

2. Кобозева, А.А. Стеганографический метод, обеспечивающий проверку целостности и аутентичности передаваемых данных / А.А. Кобозева, М.А. Козина // Проблемы региональной энергетики. Электронный журнал Академии наук Республики Молдова. – 2014. – №3 (26). – С. 93-106.

3. Козина, М.А. Стеганографический метод организации скрытого канала связи, осуществляющий проверку целостности передаваемой

информации / М.А. Козина // Сучасна спеціальна техніка. – 2014. – №4 (39). – С. 98-106.

4. Kozin A. Steganography method using Hartley transform / A. Kozin, O. Papkovskaya, M. Kozina // Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії: матеріали XIII Міжнар. конф., 23.02–26.02.2016 р., Львів, Славське, Україна / Нац. ун-т "Львів. політехніка". – Л. : Вид-во Львів. політехніки, 2016. – С. 473-475.

5. Козіна М.О. Алгоритм перевірки цілісності цифрового зображення / М.О.Козіна, В.Ю.Кремінський, О.Б.Козін, С.-М.Нджикє Амугу / Сучасний захист інформації – 2016. – №4. – С.41-46.

6. Кобозева, А.А. Формальные условия обеспечения устойчивости стеганометода к сжатию /А.А.Кобозева, М.А. Мельник // Сучасна спеціальна техніка. – 2012. – № 4(31). – С. 60–69.