УДК 004.94 **doi: 10.20998/2522-9052.2017.1.10**

V. Oleshchenko, V. Pevnev

National Aerospace University – Kharkiv Aviation Institute, Kharkiv, Ukraine

DEVELOPMENT OF DIGITAL STEGANOGRAPHY TECHNIQUES FOR COPYRIGHT PROTECTION, BASED ON THE WATERMARK

The increasing value of information protection is an important question in our fast-paced world. Especially acute is the question of copyright protection, which is against the backdrop of increasing the number of generated content, has become a real problem. The unauthorized use of foreign Intellectual Property of liability leads to great economic author`s losses. In order to minimize cases of data theft, steganography requires a large number of ways to conceal the fact of the information transfer (in contrast to cryptography, where you actually encrypted the message itself). Steganography is changing the image in a way that only the sender and the intended recipient is able to detect the message sent through it. It is invisible, and thus the detection is not easy. It is a better way of sending secret messages than encoded messages or cryptography as it does not attract attention to itself. Among the already proposed, existing steganography methods, such as: Digital prints (DP), steganography watermark (SW), hidden data (HD), in this work, attention is paid to watermarks (SW). SW implies the presence of the same labels for each container copy. In particular, the SW can be used to confirm the copyright. For example, when you recording video, you can intersperse information about recording time, in each frame, or the camcorder model, or name of your camcorder or the information about operator. If the footage gets into the hands of a rival company, you can try to use the watermark to confirm authorship of the record. If the key is kept secretly by the owner of the camera, then you can use the SW as a confirmation the authenticity of the photo and / or video images. Digital watermarks are used to protect the copyright or proprietary rights to the digital images, digitized photographs or other artwork. The main requirements that apply to this integrated data, are reliability and resistance to distortion. In modern systems, the formation of the digital watermark embedding the principle of label being a narrowband signal over a wide frequency range of the image to be marked. Digital watermarks have a small amount, however, subject to the above requirements for their integration using more sophisticated methods than to embed a message or header. This report is examined the possibility of using methods of steganography, which is based on the use of watermarks to protect and hide information to protect copyright.

Keywords: steganography, cryptography, watermarks, copyrights.

Introduction

Steganography - a method of transmitting or storing information in view of the secrecy the fact of transfer itself. Unlike cryptography, where the enemy can accurately determine whether the transmitted message is encrypted text, steganographic techniques allow embedding secret messages in innocuous message so that it was impossible to suspect the existence of the embedded secret message. Steganography takes its place in security: it does not replace, but rather complements cryptography. Hiding messages by steganography techniques greatly reduces the probability of detection of the fact of transmission of messages. And if message also encrypted, it would have another layer of protection. When combined, steganography and cryptography can provide two levels of security. Computer programs exist which encrypt a message using cryptography, and hide the encryption within an image using steganography. As a rule, a message will appear as something else, such as an image, an article, a shopping list, or a letter Sudoku. [1, 3].

Steganography usually used in conjunction with cryptography techniques, thereby completing it. The advantage of steganography over “clear” cryptography is that messages do not attract attention. Messages which encryption fact is not hidden, is suspicious and may be themselves incriminating in countries where prohibited cryptography [6].

1. Steganographic method`s overview

Currently, due to the rapid development of computer technology and new information channels, new steganographic methods appear, which are based on characteristics of information in computer files. Digital steganography is the most interesting, in terms of information security, it`s a most promising direction of steganography.

Let`s look closer than. The main provisions of steganography are:

- methods of concealment must ensure the authenticity and integrity of the file;
- it is assumed that cryptographer is fully aware of the possible methods of steganography;
- security methods based on the preservation of steganography transformation of the basic properties of open file transfer, when incorporated in it a secret message and some unknown to enemy information – some sort of key. Even if the fact of concealment message has become known to the enemy, the extraction of the secret message is a complex computational task [2].

Steganographic system or stegosystem - a set of tools and techniques that are used to form a secret channel of information transfer.

Stegosystem generalized model shown in Fig. 1.

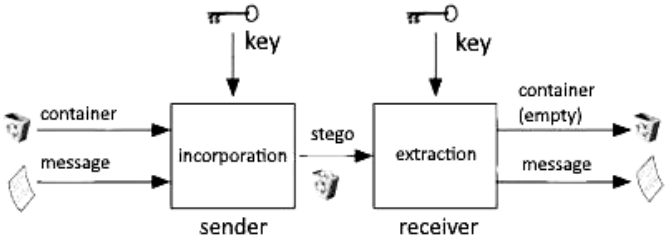

Fig. 1. Stegosystem model

Any information can be used as a data: text, message, image, and so on. In the general case, it is advisable to use the word "message" as the message can be either text or image, and, for example, audio data.

Next to describe hidden information, we'll use the term “message” [2].

There are many algorithms to embed hidden information. All of them can be divided into several subgroups:

- working with the digital signal itself. For example, LSB method;
- “soldering” of hidden information. In this case, there is an imposing concealed of image (sound, sometimes text) over the original. Often used for embedding digital watermarks (DW);
- using the features of the file formats. This includes recording information in metadata or in various other non-reserved fields file.

By way of embedding information stegoalgorithm`s can be divided into linear (additive), and other non-linear. Algorithms of additive introduction of information are concluded in a linear modification of the original image, and its extraction is carried out in the decoder correlation methods. Below is a brief list of stegoalgorithm:

LSB-method (Least Significant Bit) — the essence of this method is to replace the least significant bits in the container (image, audio or video) to the beats of hide messages. The difference between the empty and filled containers should not be perceptible to the human organs of perception.

Echo-methods used in digital audio steganography with irregular intervals and inter-echo sequence to encode values. In imposing a number of restrictions enforced stealth condition for the human perception.

Phase coding — it is also used in digital audio steganography. There is a replacement of the original audio element on the relative phase, which is the secret message.

Method of embedding messages is that a special random sequence is integrated into the container, and then, using a matched filter, the sequence is detected. This method allows to build a large number of messages in a container, and they will not interfere with each other, provided orthogonal sequences used.

Also became popular methods when hidden information transmitted via computer networks using the features of the data transmission protocol. These techniques are called "network steganography." Typical methods of network steganography include changing the properties of one of the network protocols. Furthermore, the relationship can be used between two or more different protocols with a view to better conceal the secret message transmission. Network steganography covers a wide range of techniques, including:

WLAN - Steganography is based on methods that are used to transmit steganogram in wireless networks (Wireless Local Area Networks). A practical example of WLAN steganography - hiccups System (Hidden Communication System for Corrupted Networks).

LACK - steganography - hiding messages during calls using IP-telephony. For example: the use of packages that are delayed or deliberately damaged and ignored by the receiver (this method is referred to as LACK - Lost Audio Packets Steganography) or concealment of information in the header fields that are not used [3, 4].

2. The use of digital watermarking

Hiding information in the media space is usually produced using steganography algorithms. There are several problems, solutions for that use such algorithms, for example:

- ensuring the confidentiality of correspondence (postal privacy);
- communication remote subscribers exchanging digital data arrays;
- communication remote users in an open network structures;
- achieving stealth stored large amounts of information.

One of the most effective methods of protecting multimedia information is embedding the protected object with invisible labels - digital watermark (DW). The name of this method has the known method of protection of securities including money from forgery.

The most important use of a digital watermark found in the copy protection system that seek to prevent or kept from unauthorized copying of digital data. Steganography uses DW when parties exchange secret messages are embedded into a digital signal. It used as tool of protection the documents with a photo - passports, driving licenses, credit cards with photos. Comments to the digital photos with descriptive information - another example of invisible DW. Although some formats of digital data can also carry the additional information, called metadata, DW characterized in that the information is "sewn up" directly in the signal. Multimedia objects in this case will constitute the containers (carriers) of the data. The main advantage is that there is a conditional relationship between the event of substitution of object identification and the presence of the security element - the hidden watermark [7].

Unlike conventional DW watermark can be not only visible, but (usually) invisible. Invisible DW analyzes special decoder, which brings about the correctness of their decision. Stegosystem DW, in particular, should have the task of protection of copyright and property rights for the e-mails with different active intruder attempts distortion or erase the authentication information embedded in them. Formally speaking, the DW system must provide authentication of senders of electronic messages.

Such a problem can be assigned to cryptographic system of electronic digital signature (EDS) data, but unlike stegosystems DW known system electronic signature does not provide protection of authorship is not only digital, but also analog alarms in an environment where the active violator distorts protected message and authentication information.

Other security requirements for stegosystem designed to hide the fact that the transmission of confidential communications from passive offender. It also has its own characteristics to ensure imitoprotection

stegosystems to be put into a hidden channel of transmission of false information [8]. Life cycle of DW can be described like that, on fig. 2:

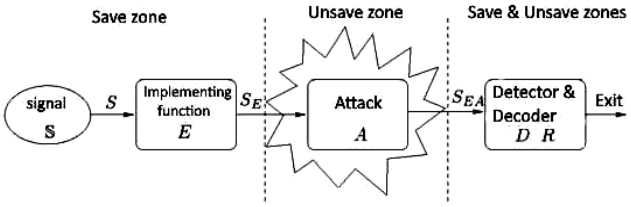

Fig. 2. Stegosystem life cicle

First, in a signal source **S** in a trusted environment embedded watermarks by using the tool **E**. The result is a signal . The next stage - the spread of through a network or any other means. While distributing the signal system can be attacked. In the resulting signal watermarks can potentially be eliminated or changed. The next step is the detection function ***D***. ***D*** tries to detect the watermark ***w***, and pull out of the function ***R*** signal embedded message. This process has the potential to make the attacker. For steganographic systems adopted to determine non-detectability - the probability of missing (ie the lack of detection stegosystem when it was presented for the analysis), and the probability of false detection (when stegosystem falsely detected when its actual absence) [6].

Practical ways stegosystems resistance evaluation based on their resistance to the detection means developed to date steganalysis algorithms.

They are all built on the fact that all the algorithms embedded somehow contribute to distortion relative stegograms used containers.

3. Attack's on stegosystem

By attack on stegosystem mean an attempt to detect, remove, change hidden steganographic message. Such attacks are called steganalysis by analogy with the cryptanalysis cryptography. The following types of attacks:

Subjective attack. Analyst carefully examines the image (listening to audio) in an attempt to determine the "eye", is there a hidden message in it. It is clear that such an attack may be carried out only against the totally unprotected stegosystems. Nevertheless, it is probably the most common in practice, at least at the initial stage of opening stegosystem.

The attack based of the known filled container. In this case the offender has one or more stego. In the latter case, it is assumed that embedding hidden information carried by the sender in the same manner. The analyst's task may consist in detecting the existence stegochanel (basic), as well as in the removal or determination key. Knowing the key, the offender will be able to analyze other stegomessage.

Attack based of the known embedded messages. This type of attack is more characteristic of the intellectual property protection systems, when used in a well-known company logo as a watermark. The objective of the analysis is to obtain a key. If the corresponding hidden messages filled container is unknown, the task is extremely difficult to be solved.

Attack based of the selected hidden message. In this case, the analyst is able to offer the sender to transmit their message and to analyze the resulting stego.

Adaptive attack based on the selected hidden message. This attack is a special case of the previous one. In this case, the analyst has the ability to select messages in order to impose the sender adaptively, depending on the results of previous analysis stego.

Attack based on the selected error filled container. This type of attack is more typical for DWM systems. Steganalyst has stegosystems detector in the form of a "black box" and several stegosystems. Analyzing the detected hidden messages, the intruder tries to open the key. Also steganalyst can apply three attacks, which have no analogues in cryptography.

The attack based of the known empty container. If analyst known about it, he comparing it with the expected stego he can always establish the fact of the stego-channel. Despite the triviality of this case, in many works is its information-theoretical basis. Much more interesting scenario, when the container is known approximately, with some error (as may be the case when you add to it the noise).

Attack based on the selected empty container. In this case, the analyst is able to force the sender to use it proposed container. For example, proposed container may have large homogeneous areas (monochrome image), and then it will be difficult to ensure privacy implementation.

The attack on the based on the known mathematical model of container or part thereof. In this case the attacker attempts to determine the difference between a suspicious message from known model. For example, assume that the bits within the image frame are correlated. Then the lack of such a correlation may be a signal about the existing of hidden message. Message an implementing task is not to break of container statistics. Implement and the attacker may have different patterns of signals, whereas in the information-win confrontation conceals having a better model. [3 , 6].

Conclusions

Currently, computer steganography continues to develop: formed the theoretical basis, is developing new, more persistent messaging integration methods. Among the main reasons observed a surge of interest in steganography can be identified in a number of countries adopted restrictions on the use of strong cryptography, as well as the problem of protecting copyright in artistic works in the digital global networks. For example, for graphics in terms of protection of copyright in their files fundamentally necessary to implement the automatic signing files for the publication of information about the author. It can be a text or other graphic information placed in any (eg, the bottom) of the image, clearly an association with a person by the authors copyright owner. These "tags" are an irrefutable link to the source, provides a particular image file. The introduction of the digital image watermarking, allowing to confirm and verify the developer rights to the media file, is also an effective protective measure for the enforcement of intellectual

property rights. Such tags can be variously positioned as a multimedia file and serve opposition to such unlawful acts, such as the substitution of attribution and repudiation.

REFERENCES

1. Ingemar J., Cox, Matthew L., Miller, Jeffrey A., Bloom, Jessica, Fridrich and Ton, Kalker(2008), *Digital Watermarking and Steganography*, Elsevier Inc., 502 p.
2. Konakhovych, H.F. and Puzyrenko, A.Yu (2006), *Kompyuternaya Stehanohrafyya. Teoryya y Praktyka* [Computer Steganography. Theory and Practice], MK-Press, Kyiv, 288 p., ISBN 966-8806-06-9.
3. Stehanohrafyya [Steganography], available at: https://ru.wikipedia.org/wiki/Стеганография (last accessed January 30, 2017).
4. Osnovy steganografii i tsifrovyye vodyanyye znaki [The Basics of Steganography and Digital Watermarks], available at : http://citforum.ck.ua/internet/securities/stegano.shtml (last accessed January 30, 2017).
5. Steganography and Digital Watermarking, available at : www.lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti98/Fortini/ intro.html (last accessed January 30, 2017).
6. Sunchugashev I/ (2008) Stehanohrafyya [Steganography], Dolgoprudnyy, MIFI, available at : http://re.mipt.ru/infsec/2008/ essay/2008_Steganography_Sunchugashev.pdf (last accessed January 30, 2017).
7. Steganography And Digital Watermarking», available at : http://https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.pdf (last accessed January 30, 2017).
8. Tsifrovyye vodyanyye znaki [Digital Watermarks], available at: https://ru.wikipedia.org/wiki/Цифровой_водяной_знак (last accessed January 30, 2017).

Received (надійшла) 07.02.2017
Accepted for publication (прийнята до друку) 16.05.2017

Розробка методів цифрової стеганографії для захисту авторських прав, на основі водяних знаків

В.В. Олещенко, В.Я. Пєвнєв

Все більшого значення в нашому швидко змінюваному світі набуває захист інформації. Особливо гостро стоїть питання захисту авторського права, який на тлі збільшення кількості створюваного контенту, став справжньою проблемою. Несанкціоноване використання чужої інтелектуальної власності призводить до великих економічних втрат автора. Для того що б мінімізувати випадки крадіжки даних, стеганографія передбачає наявність великої кількості способів приховування самого факту передачі даних (на відміну від криптографії, де шифрується саме повідомлення). Серед уже запропонованих, існуючих способів стеганографії таких як: Цифрові відбитки (ЦО), стеганографічні водяні знаки (СВЗ), прихована передача даних (СПД), в даній роботі увага приділена водяним знакам (СВЗ). СВЗ має на увазі наявність однакових міток для кожної копії контейнера. Зокрема СВЗ можна використовувати для підтвердження авторського права. Наприклад, під час запису на відеокамеру можна в кожен кадр вкраплять інформацію про час запису, моделі відеокамери і / або імені оператора відеокамери. У разі якщо відзнятий матеріал потрапить в руки конкуруючої компанії, ви можете спробувати використовувати СВЗ для підтвердження авторства записи. Якщо ключ тримати в секреті від власника камери, то за допомогою СВЗ можна підтверджувати справжність фото та / або відео знімків. Цифрові водяні знаки використовуються для захисту авторських або майнових прав на цифрові зображення, фотографії або інші оцифровані твори мистецтва. Основними вимогами, які пред'являються до таких вбудованим даними, є надійність і стійкість до спотворень. Цифрові водяні знаки мають невеликий обсяг, проте, з урахуванням зазначених вище вимог, для їх вбудовування використовуються більш складні методи, ніж для вбудовування просто повідомлень або заголовків. У цій доповіді розглянута можливість застосування методів стеганографії, заснованих на використанні водяних знаків, для захисту і приховування інформації, для захисту авторського права.

Ключові слова: стеганографія, криптографія, водяні знаки, авторські права.

Разработка методов цифровой стеганографии для защиты авторских прав, на основе водяных знаков

В.В. Олещенко, В.Я. Певнев

Все большее значение в нашем быстро изменяющемся мире приобретает защита информации. Особенно остро стоит вопрос защиты авторского права, который на фоне увеличения количества создаваемого контента, стал настоящей проблемой. Несанкционированное использование чужой интеллектуальной собственности приводит к большим экономическим потерям автора. Для того что бы минимизировать случаи воровства данных, стеганография предполагает наличие большого количества способов сокрытия самого факта передачи данных (в отличии от криптографии, где шифруется само сообщение). Среди уже предложенных, существующих способов стеганографии таких как: Цифровые отпечатки (ЦО), стеганографические водяные знаки (СВЗ), скрытая передача данных (СПД), в данной работе внимание уделено водяным знакам (СВЗ). СВЗ подразумевает наличие одинаковых меток для каждой копии контейнера. В частности СВЗ можно использовать для подтверждения авторского права. Например, при записи на видеокамеру можно в каждый кадр вкраплять информацию о времени записи, модели видеокамеры и/или имени оператора видеокамеры. В случае если отснятый материал попадет в руки конкурирующей компании, вы можете попытаться использовать СВЗ для подтверждения авторства записи. Если ключ держать в секрете от владельца камеры, то с помощью СВЗ можно подтверждать подлинность фото и/или видео снимков. Цифровые водяные знаки используются для защиты авторских или имущественных прав на цифровые изображения, фотографии или другие оцифрованные произведения искусства. Основными требованиями, которые предъявляются к таким встроенным данным, являются надежность и устойчивость к искажениям. Цифровые водяные знаки имеют небольшой объем, однако, с учетом указанных выше требований, для их встраивания используются более сложные методы, чем для встраивания просто сообщений или заголовков. В данном докладе рассмотрена возможность применения методов стеганографии, основанных на использовании водяных знаков, для защиты и скрытия информации, для защиты авторского права.

Ключевые слова: стеганография, криптография, водяные знаки, авторские права.