Journal scientific and applied research, vol. 8, 2015
Association Scientific and Applied Research
International Journal

Original Contribution

ISSN 1314-6289

GRAPHIC INTERPRETATION OF DIGITAL PRODUCTS AND APPLICATIONS IN STEGANOGRAPHY

Emanuil Stoyanov, Bozhidar Stoyanov*

SHUMEN UNIVERSITY "BISHOP KONSTANTIN OF PRESLAV"
E-mail: emanuil_stoyanov@yahoo.com

**SHUMEN UNIVERSITY "BISHOP KONSTANTIN OF PRESLAV"*
E-mail: bojidar_stoyanow@yahoo.com

ABSTRACT. *Today, the generation of digital data is easier than it has ever been. These are the so-called digitally born products – documents, images, audio and video recordings, software, e-books, digital models, maps, etc. They are more and more widely employed nowadays in a variety of fields, such as business, science, art, education, digital communications, national security, intelligence service, military science, etc. Their global application has brought forth the need for their being reliably protected and has made it an issue of paramount importance in the modern world of information. This necessity has imposed the fast development of two contemporary sciences - cryptography and steganography. The present report treats one of the recent variations in the development of steganography - digital steganography, suggesting a universal idea for its application to all types of digital products.*

KEY WORDS: *Steganography, Watermark, Fingerprint, Secret Image, Stego Object, Cover Image, Embedding*

Steganography is an ancient art [1] and a science for communicating hidden data in such a way that nobody else except for their receiver should be able to recognize their existence. A special interest for us are the up-to-date steganographic methods, which are systemized in the field of digital steganography. The latter explores the possibilities of hiding one piece of information into another, analyzing the characteristics of digital data presentation as well as the weaknesses of human perception [6]. One of the most popular contemporary methods for steganographic protection is LSB (Least Significant Bit), based on the usage of the least significant bit [3] for the presentation of hidden information.

The methods for steganographic hiding, which are used in this report, are subject to authorship and their description is not an objective of this article. They have been discussed in [6]. This report suggests an approach which allows for them to be applied in every sphere of modern life, where digitally presented information is stored and used in electronic form.

1. A Method for hiding a random digital product into an image

The steganographic methods in this report operate entirely with images. This imposes the necessity for all sources to be turned into images.

The digital products can be presented as separate files of a size of K bytes. In the cases when they are multi-componential (e.g. software packages), it is possible to reduce them to a single file by way of archiving them.

The suggested approach is underlined by the concept [4] that all files, regardless of their purpose, structure or type, are stored in electronic form as a sequence of bytes. In the cases when their sizes fulfil the requirement of formula [1], they can be interpreted as raster images with sizes MxN pixels, via changing their type into RAW - format, uncompressed (8-bits, Grayscale).

In the context of digital steganography, these images are suitable to be used as objects to hide, therefore they can be labeled as Secret Images. The process of hiding requires the availability of one more image, functioning as a Cover Image. Let it be PxQ pixels in size. In order for the Secret Image to be successfully “interwoven” into the Cover Image, it is obligatory that the condition (2) is fulfilled. The result from this operation is an image which is indistinguishable from the cover one and is called a steganographic image or Stego Object.

(1) $$K = MN$$

(2) $$M \leq P,\ N \leq Q$$

That way, the hiding of any digital product is reduced to the method of interweaving one image into another. By a reverse process an equivalent copy of the interwoven RAW image is extracted. Then, by another reversal of its file format to the original one before the process of hiding the image, the original file format, as well as the initial format and structure are restored, which ensures its accurate interpretation and makes it an exact copy of the hidden digital product (Secret Image). Fig.1 shows [4] the approach for hiding and extracting any kind of digital product by using an image, described above.

The interpretation of any file as a Grayscale image allows for it to be hidden in only one of the RGB-channels of a color image. This actually means that in one full-color image can be hidden up to 3 different files, which meet the conditions (1) and (2).

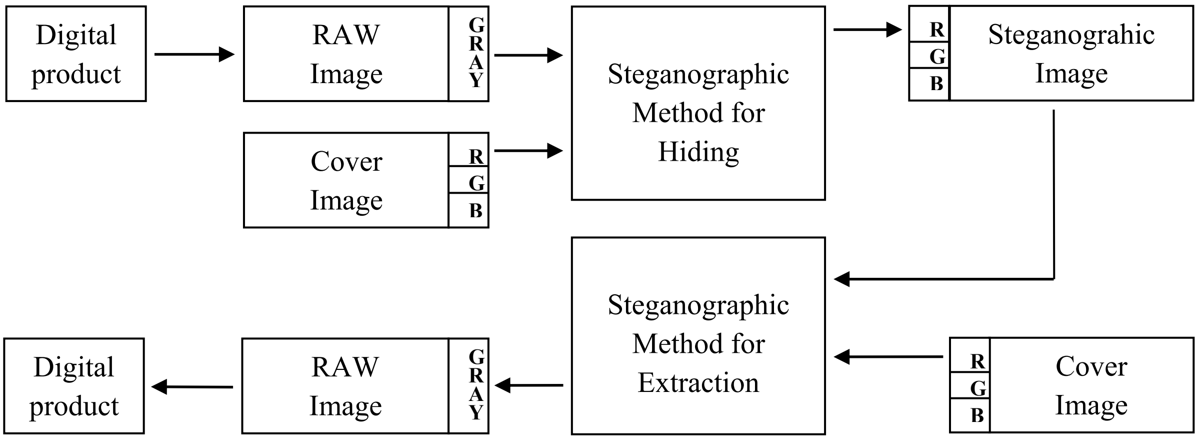


Fig. 1 - A model scheme for the application of steganographic methods to digital

There are many and varied requirements for the qualities of the developed steganographic methods, the most important of which are:

- *preservation of the structure of the cover image file;*
- *hiding the fact that another piece of information is present;*
- *stability in relation to attempts to delete or damage the hidden information;*

Taking into consideration the requirements just mentioned, we can conclude that, for cover sources, we can use files, which do not contain a header in their structure. Examples of such formats are – RAW (for images), WAV (for audio files), TXT (for text documents). Apart from this, the content of the cover images should be closely connected with the imperfections of human senses in relation to hearing, sight, touch and smell. Despite the fact that text documents are created in a suitable text format (TXT), they cannot be used as cover images for hidden information. That is so, because the second requirement cannot be met - hiding the fact that another piece of information is present.

The following conclusions [4] can be drawn from what has just been said:

☞ Unsuitable cover images are those, which contain a header, or those, in which the information is presented by a limited number of values. An example of this are text files, where the separate symbols are represented only by values from 0 to 255.

☞ Every digital source is possible to be hidden (Secret), provided that the conditions (1) and (2) are met, which allows transforming it into a single-channel RAW- image.

On the basis of the suggested approach for hiding unspecified digital products into images, and the developed original steganographic method described in [6], the following experiments, described in Table 1, have been successfully carried out. For all the investigated cases, complete hiding and a 100 per-cent restoration of the hidden information have been ascertained.

Table 1 - Experiments

Areas of application	**A description of the experiment**	
	A secret object	**A cover object**
Photogrammetry	A secret image	A censored image
	A stereo pair	A single aerial photograph
Geodesy	DEM with high resolution	DEM with low resolution
	digital watermark, fingerprinting	DEM
	Heterogeneous information	Digital maps
Audio processing	An audio file	An image
	An audio file	An audio file
	An image	An audio file
	A text file	An audio file
	An executable program	An audio file
Raster processing	An image	An image
	An audio file	An image
	An executable program	An image
	A text file	An image

2. Applications in steganography

Digital steganography was born as a science literally in the last few years and has been developed as a science in a variety of disciplines. This report describes just a few of them, in which the approach for raster interpretation of any digital products, presented in **1**, can be applied. Here are some of them:

- *copyright and intellectual property*
- *secretive delivery of information (secret communications)*
- *development of new file formats and standards*

2.1. Copyright and intellectual property

In the world of modern communications with rapidly developing multimedia technologies, the problem of copyright and intellectual property of digital products is sharply posed. The question is particularly relevant when we start talking about the digital industry. It comprises, for example, the software, photographic, audio recording and film industries. Apart from this, copyright protection is a priority in a variety of other areas, which are only users of digital products. Examples of these are automobile engineering, aircraft engineering, geodesy, architecture and building works, scientific and military organizations, etc.

The advantages of presenting and conveying digital data can be easily outweighed by the possibility of stealing and modifying this information. For that reason, various methods for its protection are being developed. One of the most efficient technical means of protection of digital information is the embedding of an invisible signature-label into the protected object, which is called a digital watermark. This term was first used in [7].

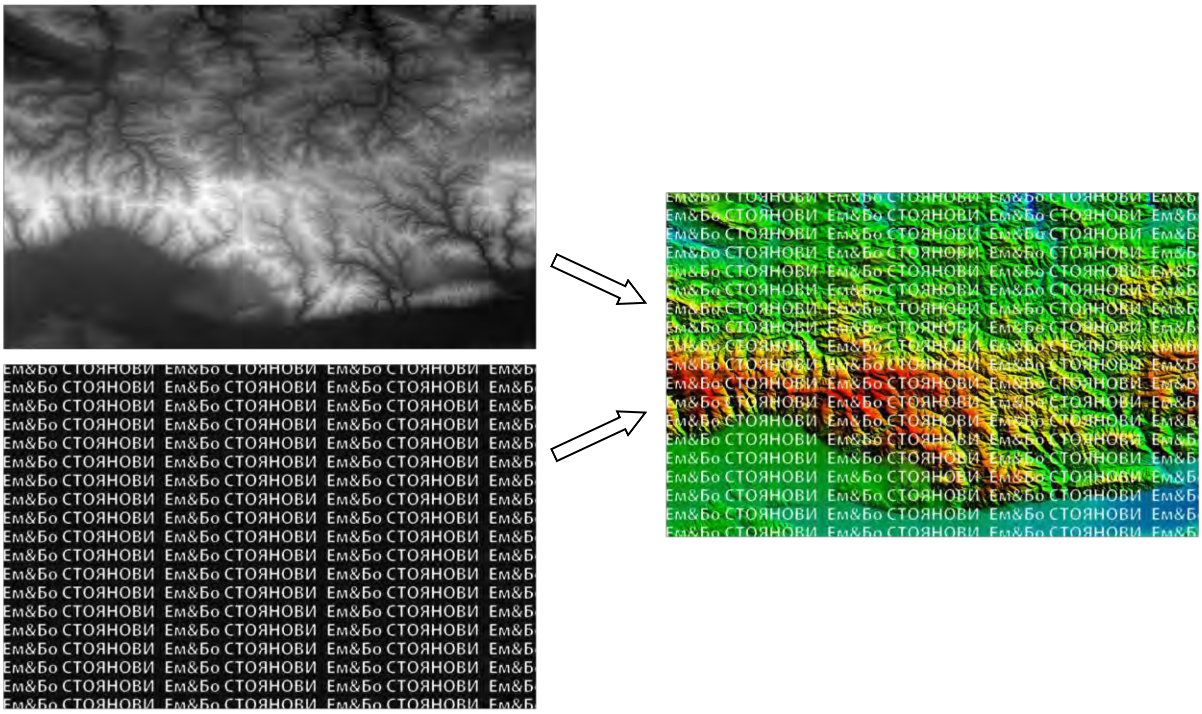


Fig. 2 - Embedding a watermark-grid in DEM

In contrast with the ordinary watermarks, DWMs (Digital Water Marks) can be not only visible, but also (as a rule) invisible. The invisible DWMs are analyzed by special decoders, which assess their authenticity. A DWM can contain an authentic code, information about the owner, as well as controlling information [5]. The objects which are most suitable to be protected with a DWM are still images and audio and video files. With regard to this, all digital products, which can be reduced to digital images, can also be protected with an invisible DWM, indicating their author.

Fig.2 shows a general scheme for hiding <a digital watermark> in a DEM. A **D**igital **E**levation **M**odel is a digital model of a part of the Earth’s surface, which depicts the altitude information in shades of grey [8]. In it, lower altitudes are visualized in darker shades, whereas higher altitudes are lighter.

In the example below the watermark is a black and white raster in the shape of a dense grid with repetitive information, which covers the whole DEM. This makes it possible to embed information about the owner of the model, so that, if only a small local area of it is taken, it will still contain all or at least part of the information about the owner. (Fig.3)

When applying this original steganographic method, we observed shifts in the elevation model only of about 6 mm, which is considered insignificant in geodesy.

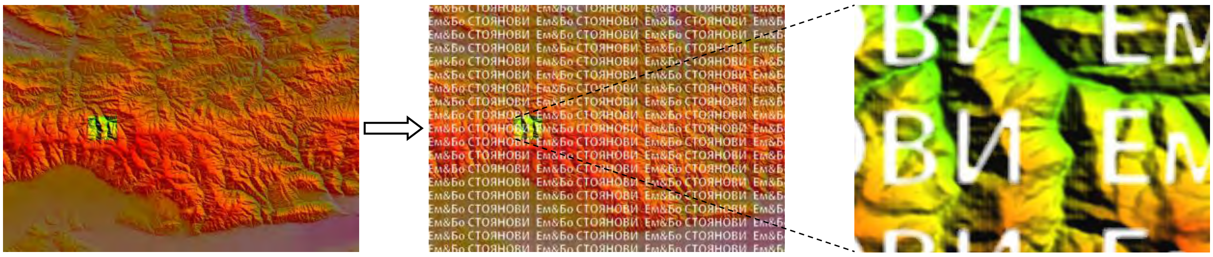


Fig. 3 - Covering a local area of a DEM with a watermark grid

Another technique, which can be applied and has a lot in common with the one of the digital watermark, employs embedding an identification number of the manufacturer of the digital product. The difference lies in the fact that in <fingerprinting> every protected copy possesses a unique identification number, which is where the term comes from – literally “a fingerprint”. These numbers allow manufacturers to track the future life of their products, in case any of the buyers is illegally copying or spreading the product. If that is the case, the <fingerprint> will quickly point to the culprit.

These methods are applicable in all the fields which deal with creating and commercial distribution of finished digital products. The application of the method, described in paragraph **1**, makes it possible to use a variety of types of sources – texts, audio files, images, short video messages, etc. – for the purpose of protection with digital watermarks and fingerprints.

2.2. Application in secret communications

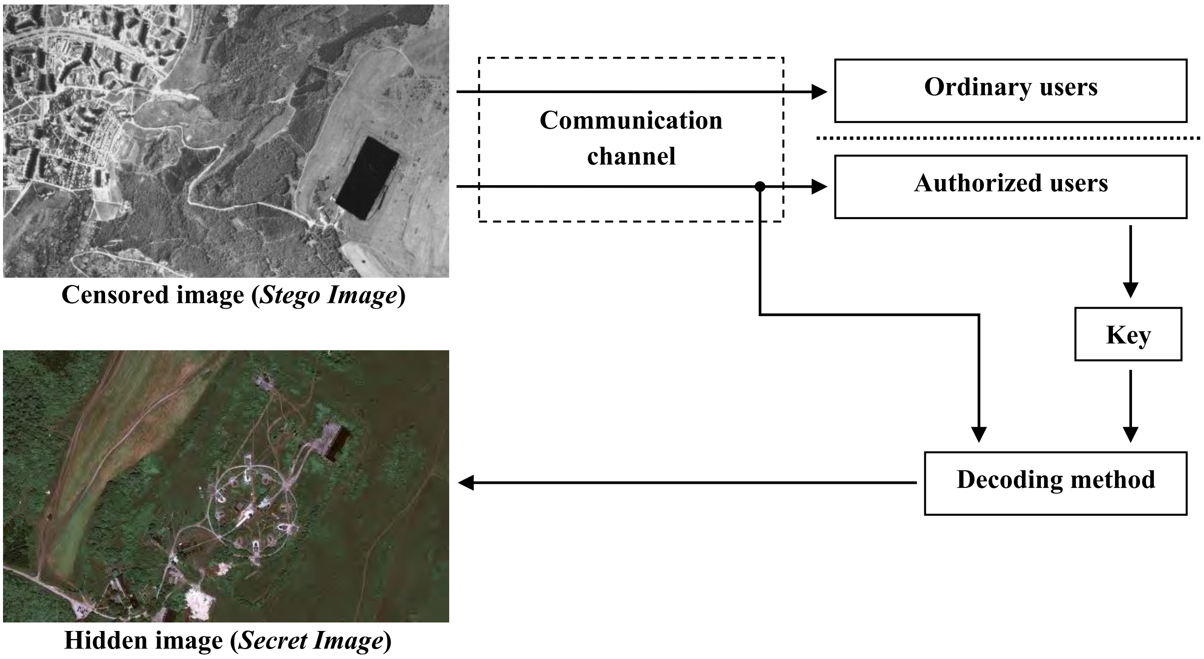
Hidden communications are used by military, spy and intelligence organizations, as well as by various state institutions like the Presidency, the Ministries of domestic and foreign affairs, diplomacy, etc. They are also often used by businessmen or boards of public and private companies as a means of guarding corporate secrets, know-how, inventions, etc.

Secret communication can be carried out, on the one hand, by encrypting the transferred information, and, on the other, by securing the secrecy of the traffic itself. A propitious method for providing the secrecy of communication is the possibility to hide the very fact of the existence of the secret communication. This idea is part of the essence of steganography – hiding the message in a way which does not allow anyone to see it [2].

In cryptography the reverse principle is to be followed – the message is rearranged in such a way that it becomes unintelligible. However, a basic shortcoming of cryptography is the fact that the transfer of secret information is accessible (visible) for unauthorized users and they can easily intercept, duplicate and attack it.

Considering the advantages and the disadvantages of the two methods (cryptology and steganography), a useful approach is to combine them in order to achieve maximum security and protection.

Fig. 4 shows hidden transfer of classified information by accessing public data in a common communication channel. For example, when photographing parts of the Earth’s surface for the purpose of placing the images at the public’s disposal (e.g. Google Earth), some of them may happen to contain sites, which are subject to military or state secrecy. What is usually done in such cases is to censor (mask) those parts of the photographs, which reveal the secret information.



Censored image (*Stego Image*)

Hidden image (*Secret Image*)

Fig. 4 - Public access to a censored image containing hidden information

The example demonstrates how, in a censored image, which is generally accessible, the original (uncensored) variant of the photograph or another photograph, containing hidden information, can be hidden. Thus only authorized users will have access to this information, all the rest – only to the censored variant. (Fig.4).

2.3. Application of the steganographic methods for the purpose of developing new file formats and standards

The approach, described in **1**, can be applied to all types of digital data. This universality may give rise to ideas for applying the technique, described above, in the development of new file formats and standards. Here are some of them:

- ***hiding an audio file in an image***

On Fig.5 there is a general scheme for embedding an audio file into an image. Apart from the hidden transfer of audio data, another interesting application of this idea is that, in the future, a new graphic format (container) will be established, allowing for the digital image to be accompanied by an audio commentary, music or information about its author, interwoven in it.

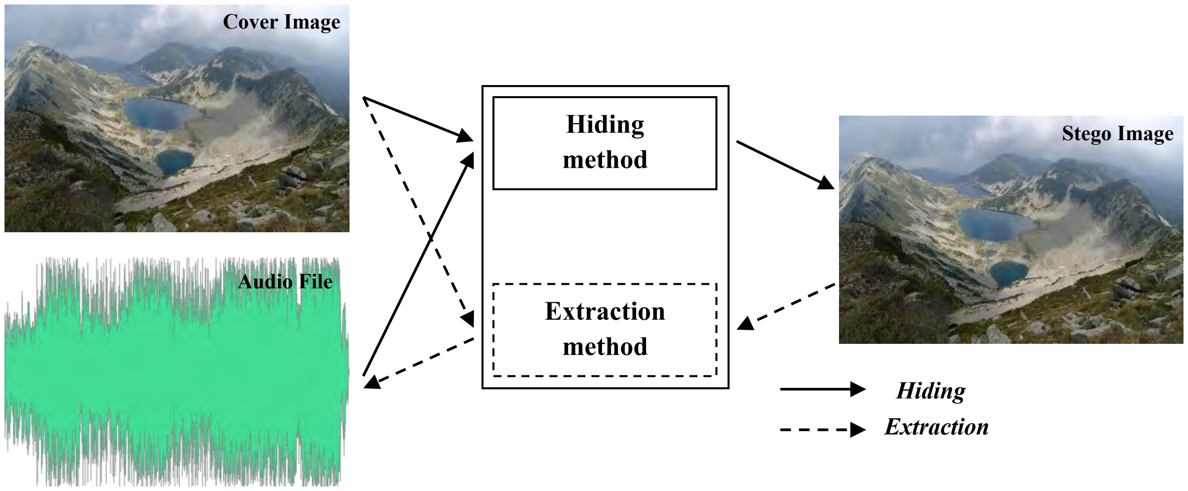


Fig. 5 - A general scheme for hiding audio data into an image

From Table-1 it is obvious that the method allows us to swap the places of the source and the recipient, i.e., to perform a reverse process of hiding an image into an audio file. The only restriction for the container is to comply with the conditions, described in **1**.

- ***hiding information in digital maps***

Modern digital cartography is a process [8], in which a certain amount of data is accumulated and formatted into a virtual image. Digital maps are a product of digital photography. A digital map can result either from an analogue source by digitalizing it or be “digitally born” (i.e., without having an analogue duplicate). Regardless of their origins, digital maps can be presented (exported) as raster images. Generally, if they are full-colour, the RGB system is to be used for the representation of the raster. That is so because this system is the most appropriate for computer screen visualization, because, structurally, every pixel from the surface is composed of three sub-pixels – for the colours red, green and blue.

Treating the maps as raster images allows hiding information in them. What is more, different sets of data can be concealed in each of the three colour channels. Examples of these are Digital elevation models (DEM), extremely precise coordinates (rank 1 and rank 2), a black and white photo of an area, various layers of GIS and others.

Fig.6 presents a scheme for embedding three various images in the R, G and B channels of a digital map. However, the three of them should be monochromatic (i.e. represented in the grayscale).

In the example shown here, the digital map can be seen as a type of container, which stores the extra information. This suggests the idea of developing new file formats, which will pack heterogeneous, yet reciprocally connected information into one digital source.

Although the ideas, described above, contrast the basic principle of steganography - hiding the fact of the existence of other data, this technique can be used to control the access of users to various levels of information in publically accessible sources, depending on the rights they have been entitled to.

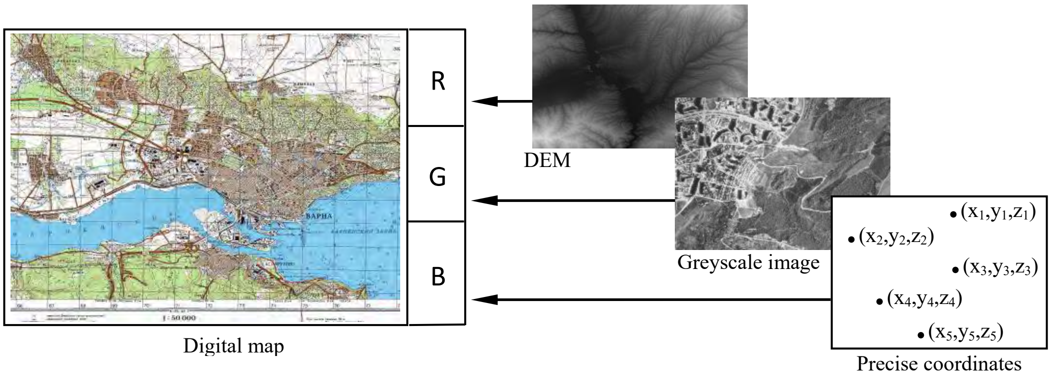


Fig. 6 - Simultaneous hiding of heterogeneous information into the RGB channels of a digital map

3. Conclusion

The life of modern society is unthinkable without the development and the advancement of new digital technologies. The huge challenges lie mostly in the issues about protection of information, copyright and confidentiality of communication. The approach, which was presented in this report, is based on the contemporary steganographic methods and represents a step towards the handling of these challenges.

References:

[1]. Neil F. Johnson, Sushil Jajodia. Exploring Steganography: Seeing the Unseen. Computing Practices. //IEEE Press, February 1998, pp.26-34.

[2]. T. Aura, Invisible Communication. // EET 1995, technical report, Helsinki Univ. of Technology, Finland, Nov.1995; URL: http://deadlock.hut.fi/ste/ste_html.html.

[3]. W. Brown and B.J. Shepherd, Graphics File Formats: Reference and Guide. // Manning Publications, Greenwich, Conn., 1995.

[4]. Stoyanov E., Stoyanov B., An Approach to Steganographic Protection of Digital Products. //Anniversary Scientific International Conference 45 Years Computer Sciences and Engineering Department, 30 Years Computer Systems and Technologies Speciality, 27-28 September, 2013, TU Varna, Bulgaria, COMPUTER SCIENCE AND TECHNOLOGIES Journal, Year XI, Number 1/2013, p.176-181.

[5]. Gribunin V. G., Okov I. N., Turincev I. V. Cifrovaja Steganografija [Digital Steganography]. //Moscow, Solon-Press Publ, 2009. 272 p. (in Russian).

[6]. Stoyanov B., Stoyanov E., Convertible Raster Transformations and Their Application in Steganography. // International Scientific Conference at "Angel Kanchev" University of Ruse, 31 October - 01 November, 2008, Bulgaria, Vol. 47, Ser. 3.2, 2008, p. 84-91.

[7]. Osborne C., van Schyndel R., Tirkel A., A Digital Watermark. // IEEE Intern. Conf. on Image Processing, 1994. P. 86-90.

[8]. Stoyanov E., Stoyanov B., The application of steganography in the fields of geodesy and photogrammetry. //Proceedings of the international conference, University of Shumen “Bishop Konstantin Preslavsky”, MATTEX 2012, 22-24 November, 2012, Bulgaria, 2009, Vol. 2, p. 176 – 183.