CRYPTOGRAPHY AND SECURITY

AN OVERVIEW OF STEGANOGRAPHIC TECHNIQUES AND METHODS APPLIED ON JPEG IMAGES USING DIFFERENT TRANSFORMATION TECHNIQUES

Dejan Uljarević[1],
Vladan Pantović[2],
Aleksandar Mišković[1],
Nataša Aleksić[3]

[1]Singidunum University,
Belgrade, Serbia
[2]Faculty of Business Economics and Entrepreneurship,
Belgrade, Serbia
[3]University of Kragujevac,
Faculty of Engineering,
Kragujevac, Serbia

Abstract:
Since steganography is a science that hasn't been fully researched, this paper gives an overview and analysis of current stenographic techniques and methods applied on different multimedia files. The emphasis is on applying steganography on JPEG images, where secret message encoding is done through various transformational techniques. Therefore, the paper gives an overview of the methods for detecting secret content through steganalysis.

Key words:
steganography, steganalysis, JPEG compression standards, DCT.

1. INTRODUCTION

Today, there is hardly no aspect of human activities where computers do not play a significant role. With that, human activities are made significantly faster and easier. Nevertheless, problems with information security often occur, as information is transferred through various channels and mediums in digital form. Business Information Systems and human communication functioning through a computer network increase codependence between the information and communication channels. Therefore, pieces of information become the target for many malicious users. This certainly leads to the necessity to protect the data in a business environment. To protect such data, besides applying such software as RSA, DES, AES, *etc.*, it is also possible to apply stenographic techniques that enable data protection by hiding behind harmless looking objects. Steganography is the practice of concealing messages in other data, so that the existence of ciphertext is hidden in the information carrier. The word steganography combines two words of Greek origin, στεγανοσ (steganos) and γραφο (grapho), which translates to concealed writing. The goal of steganography is to transfer the information from sender to receiver by imprinting the message in the information carrier, which needs to be intelligible and comprehensible to the target destination.

Unlike cryptography where the malicious user intercepting the encoded message is aware of the secret communication, with steganography the secret communication can remain undetected, since it is not possible to detect the differences indicating the presence of steganography [1].

Correspondence:
Dejan Uljarević

e-mail:
duljarevi@gmail.com

DOI: 10.15308/Sinteza-2016-165-172

As the digital world doesn't have perfect and impenetrable data protection systems, it should be noted that steganography carries risks that can endanger this security approach, because in the process of modifying *i.e.* encrypting the secret message, some of the parameters in the structure of the file – stego object, can be altered and disturbed compared to the original stego medium[1]. By monitoring and comparing the occurring changes, there is a possibility of an attack on these systems, which will be described in detail in this paper through various methods and techniques used in Steganography and steganalysis. The rest of this paper will deal with describing steganography systems applied on JPEG images where the secret message is hidden through various transformation techniques.

2. STEGANOGRAPHY

Steganography is a scientific discipline whose goal is to protect certain confidential messages in the best way by skillfully hiding them [2]. The main principle of steganography is based on using the mediums that are available to a wide range of people. Nowadays, modern steganography is most commonly applied in the world of digital technology, within the contents of a multimedia file that can be an image, an audio or a video recording, *etc*. The secrecy of the message is tied to the steganographic system[2] and a secret key under which the secret message is hidden. Modifying the stego medium creates the stego object which is sent through one of the known communication channels. When the stego object arrives to a certain destination it is unpacked using a previously defined secret key and the steganographic system, and the secret message is revealed. A model of how a steganographic system functions is shown in Figure 1.

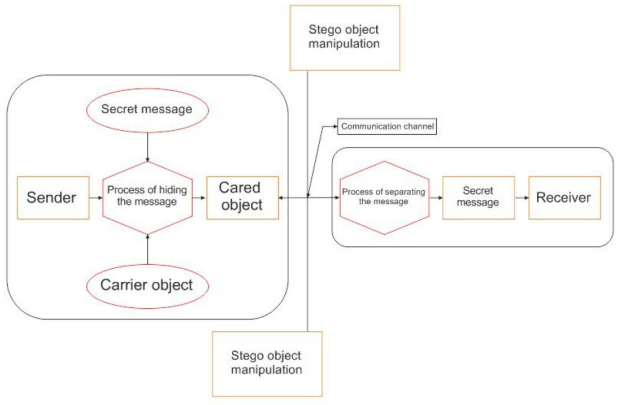

Figure 1. Schematic diagram of how a steganographic system functions

1 The original object in which the secret message is inserted
2 Algorithm for hiding the secret message in the stego medium

Information protection can this way exist in the form of a visible digital watermark and in the form of digital steganographic techniques which include three very important aspects in its functioning [3]:

- Capacity – the amount of information that can be hidden in a stego medium
- Security – the degree of inability of a detection device to uncover the secret
- Robustness – the amount of modifications that a stego medium can endure

Visible Digital watermark system is mostly used for protecting digital media copyrights and its goal is to achieve a high level of robustness – *i.e.* to disable removing the certificate without reducing the quality of the object data, while other steganographic techniques have a wider application, are invisible to the naked eye, and can be applied through the following categories [4]:

- Substitution techniques: Excess parts of the message carrier (medium) are used to insert the secret information. The most prominent technique in this category is LSB (Least Significant Bit) which makes the least significant bits the carriers of the hidden message.
- Transform domain techniques: Modification is performed in a transformed domain. The techniques most commonly used are Discrete Cosine Transformation, DCT and Discrete Fourier Transformation, DFT.
- Spread Spectrum, SS techniques: Narrowband information signal is hidden within the medium. The secret message is modified by a noise signal and added to the medium: only by knowing the key can the seemingly random signal produce the hidden message. There are two spread spectrum methods used in digital steganography - Direct Sequence Spread Spectrum, DSSS and Frequency Hopping Spread Spectrum, FHSS. These methods are typically used for transferring data in wireless systems, they increase resistance to jamming and enable multiple users to transmit simultaneously in the same frequency band.
- Statistical methods: The carrier is divided into the number of blocks corresponding to the size of the message. Each block is used to hide one bit of the secret message. If the bit of the message equals 1, the block is modified so that the message receiver can determine if the block has been changed by statistically analyzing the hypothesis. If the bit of the message is 0, the block remains unchanged.

- Reshaping Techniques: The secret message isn't hidden directly in the medium, it is reshaped to convey the secret message. The receiver is required to know the original version of the medium in which the message is hidden, which is the key to revealing the secret content.
- Creating the hidden information medium techniques: The secret message is not hidden in the medium, but the corresponding medium is created based on it.

3. JPEG FORMAT

Although steganography is applicable to a variety of multimedia content, this paper will focus on analyzing hiding data in JPEG images (steganography and steganalysis techniques and methods) [5]. Steganographic systems for JPEG format are particularly interesting because the systems function in a transformed space and are not affected by visual attacks.

JPEG format is one of the most popular and most commonly used image formats on the Internet, because it is convenient and practical when it comes to compression. This standard provides very good, or even excellent, both black & white and color image quality. It is simple to implement, and its software algorithms are at an acceptable level of computational complexity. JPEG belongs to the class of transform coding techniques, meaning that the compression isn't performed directly on the signal, but on its transformation. When it comes to image editing, most commonly used transformation is Discrete Cosine Transform (DCT). The main characteristics of DCT are a high degree of data "packaging", as well as availability of fast algorithms for its computation. The rest of this paper will deal with the methods and techniques for applying these systems.

4. JPEG COMPRESSION STANDARD

JPEG standard is the first standard in the area of image compression which applies to black & white and color image compression and it is a common standard for three international organizations: ISO, IEC and ITU [6]. The popular name JPEG is an abbreviation for the name of the working group that worked on its creation for many years (Joint Photographic Experts Group). The main goals achieved by adopting JPEG standards are [7], [8]:

- Standard enables compression of any digital image, greyscale or color, with or without loss.
- Standard is applicable to a digital image regardless of its resolution. If the number of pixels of any dimension is indivisible by 8, the image is internally expanded by an adequate number of pixels.

For compression with loss the number of bits per pixel of a black & white image (or per color component) can be either 8 or 12, while for a lossless compression the number of bits per pixel can range from 2 to 16.

The standard imposes the methods that provide a high level of compression, ensuring very good or excellent quality of the reconstructed image. The standard enables setting a parameter in order to reach a compromise between the degree of compression and the quality of a compressed image.

The standard recommends compression methods that are computing efficient and convenient for software implementation on different processors and operating systems, or for hardware implementation in the VLSI technology with moderate production costs.

Standard enables performing a luma component reconstruction from a compressed color image, with no need for decoding the chroma components.

JPEG standard enables four methods for compressing an image:

1. Sequential coding: the image is coded from left to right, top to bottom.
2. Progressive coding: the image is coded in several waves, so that in applications with long data transfer time the user gradually receives the more detailed structure of the image.
3. Lossless coding: the reconstructed image is identical to the original, although the degree of compression is lower.
4. Hierarchical coding: the image is coded in different resolutions, where reconstructing a lower resolution image doesn't require knowing the data about coding a higher resolution image.

Figure 2 shows links between four methods of compression specified by the JPEG standard.

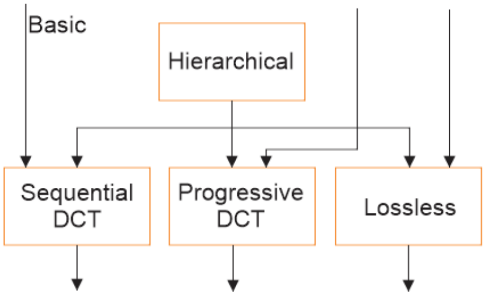

Figure 2. Scheme of four methods of compression specified by the JPEG

JPEG sequential coding

The basis for the JPEG standard (except Lossless coding) is consists of the process of transform coding the image with Discreet Cosine Transform [9]. Based on the subjective analysis and computing efficiency, a division of the image to blocks of 8×8 pixels was adopted. Since the pixel values are 8-bit positive numbers, 128 is subtracted from the value of every pixel before entering the coder, so that the value of input pixels f (x, y) lies in the range [-128, 127].

By using the Discreet Cosine Transform, every block of pixels is transformed to a group of 64 DCT coefficients representing amplitudes of orthogonal basis functions, *i.e.* a "two dimensional spectrum" of the input signal.

Unlike black & white images, color images require a more complex way of applying this system, and it is done by first performing the RGB→YCbCr transformation, and then dividing every luma component Y into blocks of 8×8 pixels. Images of chroma components Cb and Cr are first divided into blocks of 16×16 pixels, which are then divided into 2, and thus reduced to the size of 8×8 pixels. So, on every four blocks of the Y component there is one block of chroma components Cb and Cr. Then all three components of the image Y, Cb and Cr are independently transformed by applying DCT.

In order to achieve data compression, output data from each DCT block i. e. 64 DCT coefficient, must again be quantified and coded. Quantifying is done by dividing each DCT coefficient by an adequate element of the quantization matrix which can be seen in Fig. 3. and by rounding to the nearest number according to the following equation (1):

$$Fq(k,l) = int\frac{F(k,l)}{Q(k,l)} + 0{,}5 \qquad (1)$$

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Figure 3. Quantization matrix for 8×8 pixel block.

The last step in compressing the image according to JPEG standard is entropy coding. In this way, the DC coefficients F (0,0) are treated in a different way than AC coefficients. Namely, since DC coefficients of nearby blocks are very similar, the difference between DC coefficients of two nearby blocks in a block sequence is subjected to entropy coding. The order of processing DCT AC coefficients is in the shape of a zigzag sequence which is shown in Fig. 4.

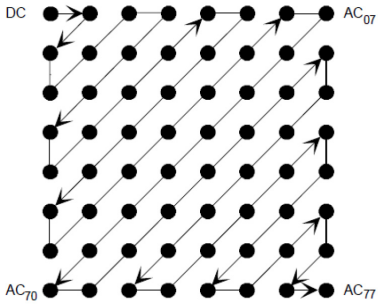

Figure 4. The order of processing DCT coefficients in 8×8 block.

This pattern facilitates entropy coding because the higher value coefficients are at the beginning of the sequence. Entropy coding is compact coding of DCT coefficients based on their statistical features. Huffman code is used for entropy coding in JPEG sequential method. The first step in entropy coding is converting the zigzag sequence of quantized coefficients into a sequence of symbols. The second step is converting symbols into a sequence of data where it is no longer possible to identify the ends of those symbols. To apply the Huffman coding, it is necessary to specify one or more coding tables used on both input and output side. JPEG standard does not provide a single coding table, this is done by the system user, but Huffman tables used while testing in the process of developing the standard are provided in addition. Block diagrams of JPEG coder and decoder for sequential coding of a black & white image and individual components of a color image are shown in Figure 5.

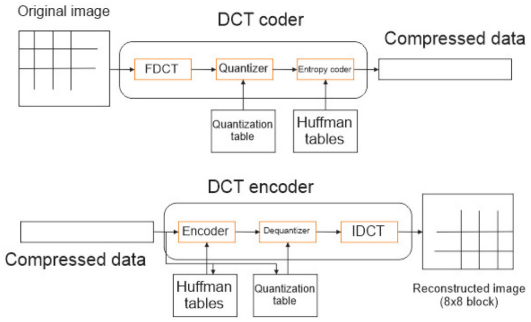

Figure 5. Block diagram of JPEG sequence system for compressing a component of a color image: (a) coder, (b) decoder.

JPEG progressive coding

Progressive coding of an image differs from sequential coding in the fact that the coding of DCT coefficient is done in several wavelets, with every wavelet transferring only a part of quantified DCT coefficients. In progressive coding, there are two procedures for dividing DCT coefficients.

- Spectral selectivity
- successive approximation method

Organization of DCT coefficients and division of DCT coefficients in both ways is shown in Figure 6.

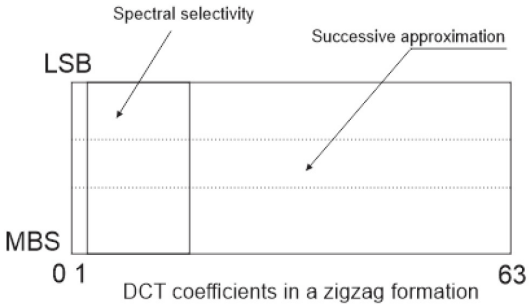

Figure 6. Editing DCT coefficients for progressive coding

In order to carry out progressive coding of an image, it is necessary to add a buffer memory behind the quantizer and before entering the entropy coder for all DCT coefficients. Minimum required capacity of this memory for compressing a black & white image is given in the following equation,

$$C = MN(b + 3) \quad (2)$$

where M and N are image dimensions, and b is the number of bits per pixel in the original greyscale image. Increasing the number of bits per pixel by 3 is the result of energy compression, which is why some of the DCT coefficients have significantly bigger values than the original pixels. In the case of color images, minimum required memory capacity is 50 % bigger.

In the process of Spectral Selectivity DCT coefficients are grouped into spectral ranges. First, the DC DCT coefficient is transmitted, then two most significant AC DCT coefficients, and then in the following wavelets groups of three AC DCT coefficients are transmitted. On the receiving side, the image initially has a block structure which is gradually lost during transmission. For an acceptable image quality, it is usually enough to transmit DC and the first five AC DCT coefficients. When all of the DCT coefficients are transmitted, it results in getting the same image as with the application of the sequence algorithm. With successive approximation methods, DC DCT coefficients are transmitted in full accuracy. Then, in the second wavelet, four of the most important bits of all AC DCT coefficients are transmitted. In the following wavelets, image quality is improved by transmitting the rest less important bits. Successive approximation method provides a better quality image with smaller bit rate. It is interesting that the spectral selectivity method and the successive approximation method can be successfully combined.

JPEG lossless coding

For lossless coding of an image, JPEG standard uses simple predictive methods of compression[3]. The standard specifies seven methods of prediction, which are defined by the equations (3) and (4).

$$f^{\wedge}(m,n) = A \quad (3)$$

$$f^{\wedge}(m,n) = B \quad (4)$$

What is used for the first line of the image is the prediction method (3), and after subtracting the estimated values from the actual values of the pixels, the result image of the difference is entropically coded by applying the Huffman or an arithmetic coder. Even though the standard supposes that each pixel of the innitial image can be represented by 2 to 16 bits, JPEG standard is practically used to decompress images represented by at least 4-5 bits per pixel, when getting a degree of compression of around 2. If the number of bits per pixel is smaller, better results can be produced by applying other lossless image compression methods.

JPEG hierarchical coding

Hierarchical coding method is intended for progressive image transmission, because it is performed in several wavelets. However, unlike regular progressive coding, here, with every wavelet, spatial resolution of the image is altered by the factor of 2 on both dimensions. This provides a hierarchical representation of the image in the shape of a pyramid, which is shown in Figure 7.

3 Lossles methods for compressing JPEG image

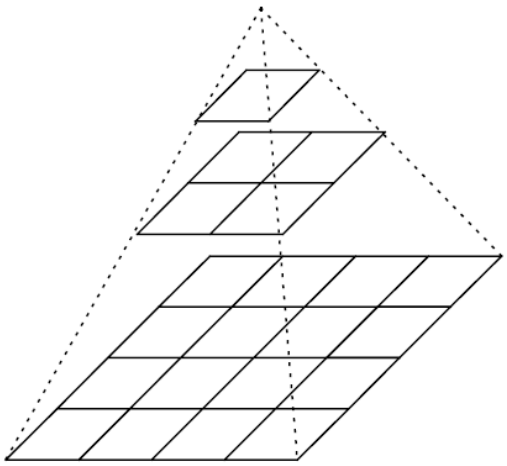

Figure 7. Hierarchical representation of an image.

The procedure of hierarchical coding can be divided into the following phases:

- The original image is filtered by a low frequency filter and is decimated by a factor of 2 on each dimension.
- Reduced image is coded using the previously described sequential DCT method, progressive DCT method, or using predictive lossless coding.
- The reduced image is decoded and interpolated by a factor on both dimensions, using the same interpolation filter used on the receiving end.
- The difference between the interpolated image (serving as an estimate) and the original image in the same resolution is formed, and the difference image is coded using the previously described sequential DCT method, progressive DCT method, or using predictive lossless coding.
- This process is repeated until the image is coded in full resolution.

Hierarchical coding is very useful in instances where a very high resolution image must be shown in a low resolution. This scenario occurs when an image is scanned and compressed in very high resolution for printing on a high-quality printer, and it needs to be shown on a video monitor of a computer with a significantly lower resolution.

Of the three JPEG coding methods based on using DCT, hierarchical coding provides the best quality of the image with extremely small bit rate. However, when excellent image quality is required, progressive transmission demands a somewhat bigger bit rate than sequential or hierarchical methods.

5. STEGANALYSIS

Steganalysis or third party steganography detection, is a relatively young research discipline with the first articles on the subject published in 1990s. The main task of steganalysis is to solve three main tasks: detecting, defining and decoding a hidden message.

To detect hidden messages, steganalysis uses methods of spotting changes: visual detection (files with jpeg, bmp and gif extensions), audio detection (files with wav, mpeg extension), static detection (change in the pixel pattern or LSB) or histogram analysis and structure detection or unusual structure detection (content review of the file, its length, change in date and time, content modification and checksum – limit number of bits).

Attacks on hidden information can have several forms: detection, separation or destruction or decoding the hidden information. System is already unsafe if the attacker is merely able to prove the existence of the hidden information. The initial assumption is that the attacker has unlimited computer resources and is able to apply a variety of attack algorithms. Attacks on steganography systems can theoretically be divided into three types, based on the end goal of the attacker: passive, active and intentional.

Passive attacks include techniques that merely detect the existence of a hidden message, for example, static testing of a hypothesis in which there are two possibilities of error: I-type error occurs when existence of a secret message in the carrier is detected, and it doesn't actually exist, and II-type error occurs when the secret message is undetected, and it actually does exist.

Active attackers are able to modify a stego carrier during transmission, but not too much, because in that case perceptual and semantic properties would be altered. Active attacker, often unable to detect the existence of a secret message, can add a random signal to the stego carrier and destroy the secret information. Attackers can be accidental and intentional. An example of an accidental attacker can be an accidental noise accumulated during a signal emission through one of the outside connections. That is why one of the more significant demands a steganographic system must meet is robustness, so that the imprinted secret information cannot be damaged without drastically altering the stego carrier. It is important to emphasize that there is a compromise between security (secrecy) and robustness. Security requires that the secret information is hidden in the areas

which are perceptually conspicuous because that way it will be more difficult to damage the information without significantly degrading the quality of the carrier. There are generally two principles to make a robust steganographic system. The first system predicts possible attacks and then projects a procedure for implementing the secret message that is robust to that kind of modifications, so that the modification doesn't completely destroy the information. The second strategy is to apply inverse modifications from those used in an attack in order to reconstruct the original secret information. Intentional attackers try to falsify a message or start a steganographic protocol by impersonating a communication partner. In an intentional attack robustness is not enough. In cases when implementation process doesn't depend on a secret information only known to the sender and the receiver, the intentional attacker can falsify the message, considering that the receiver isn't able to verify authenticity of the sender's identity. In order to anticipate this, the implementation algorithm must be robust and secure. This is why a secure steganographic system is presented with four main demands it must meet:

- Messages must be implemented in the carriers using public algorithms and secret keys.
- Only the holder of the right key can detect, separate and prove the existence of a secret message.
- Even though the attacker manages to select the contents of a secret message, they cannot detect other messages
- From an informatics standpoint it is impossible to detect a secret message.

6. CONCLUSION

As it can be seen from this synoptic paper, steganography has at its disposal very efficient and powerful solutions, which can be of great significance to quality security and protecting confidential information. Steganographic techniques are very simple to use, extremely difficult to detect, and very reliable. Steganography's main goal is to keep the existence of a secret message undetected. The secrecy of the message is tied to the steganographic system (algorithm) and the secret key under which the secret message is hidden. Apart from the positive side, steganographic methods can be used for illegal purposes, which is why, in recent years, steganography has been the main subject of many discussions about its misuse. The main argument in its defense and disclosure is steganalysis which is a younger scientific discipline than steganography. Various steganalysis methods listed in this synoptic paper can very successfully uncover and prevent any illicit actions.

This synoptic paper analyses existing steganographic systems which can use JPEG images as stego mediums. Applying discrete cosine transform, the first step in JPEG algorithm is compression of the original where successive blocks of pixels are turned into individual DCT coefficients in which the confidential data is inserted. The paper also shows recent research on detecting them through statistical steganalysis. Other analyses focus on the general use of hiding and protecting information and give an overview of detection algorithms.

Considering all of the listed methods and techniques, steganographic or steganalysis, there is a lot of space for further development and improvement, and therefore, for use of these systems in everyday human activities.

REFERENCES

[1] Jeremy Callinan, Donald Kemick, Detecting Steganographic Content in Images found on the Internet, Department of Business Management, University of Pitsburgh at Bradford, aug. 2001, http://www.chromesplash.com/jcallinan.com/publications/steg.pdf

[2] Julijana Mirčevski, Biljana Djokić, Nikola Popović, Moderne softverske tehnike u prepoznavanju proskribovanih kompjuterskih sadržaja, II Konferencija ZITEH, Tara, novembar 2006.

[3] D.Uljarević, M.Veinović, G.Kunjadić, D.Tepšić: ''A new way of covert communication by steganography via JPEG images within a Microsoft Word document'', accepted for publishing in Springer – Multimedia Systems ISSN: 0942-4962, DOI: 10.1007/s00530-015-0492-3, 2015

[4] Katzenbeisser S., Petitcolas F.: Information Hiding Techniques for Steganography and Digital Watermarking, Artech house, Boston Kipper G., Investigator's Guide to Steganography, Auerbach Publications, London

[5] D.Uljarević, M.Veinović: ''Digitalna steganografija JPEG slika primenom DCT transformacije'', Konferencija: Infotech 2014, Aranđelovac, Srbija

[6] ISO/IEC-10918/ITU-T Recommendation T.81 (JPEG), Information Technology - Digital Compression and Coding of Continuous-Tone Still Images, Sept. 1992.

[7] Wallace, G.K., "The JPEG still picture compression standard", Communications of the ACM, Vol. 34, No. 4, pp. 30-44, April 1991.

[8] Pennebaker, W.B., and J.L. Mitchell, JPEG: Still Image Data Compression Standard, Van Nostrand Reinhold,New York, 1993.

[9] Cvetković, Z., and M.V. Popović, "New fast recursive algorithms for the computation of discrete cosine and sine transforms", IEEE Trans. Signal Processing, Vol. 23, No. 8, pp. 2083-2086, August 1992.

[10] Fridrich J. Goljan M., Practical Steganalysis of Digital Images – State of the Art, Proc.SPIE, Svezak 4675, Str. 1-13, Security and Watermarking of Multimedia ContentsIV, Dostupnona:http://www.ws.binghamton.edu/fridrich/Research/steganalysis01.pdf,Pristupano: Travanj 2010.