European Journal of Science and Theology, December 2015, Vol.11, No.6, 201-210

STEGANOGRAPHY USED FOR COPYRIGHT PROTECTION IN BMP AND JPG FILE FORMAT

Robert Halenár*

University of Ss. Cyril and Methodius, Faculty of Mass Media Communication, Nám. J. Herdu 2, 91701 Trnava, Slovak Republic

(Received 16 July 2015, revised 20 August 2015)

Abstract

Copyright protection is derived from the specific needs of a particular type of subject matter and the environment. Protection solution of author's work in electronic (or digital) form in the online environment requires a specific approach and specific methods. In general, it is true that 100% protection against abuse is not possible. Therefore, it is necessary to seek out ways of protecting copyright, which would have a preventive effect and their application costs would be minimal. This paper does not address the issue of protecting digital photos in the online environment. However, once the copyright infringement has occurred, it offers a solution how to prove authorship and thus also contributes to the prevention prior to the abuse and it is applied for different data formats of images.

Keywords: copyright, protection, steganography, extension

1. Introduction

Nowadays, much attention is paid to the issue of copyright. The Slovak Act strictly defines who the author is, what the work is, and how the work and the author are protected. On the other hand, literature provides an example from practice, saying that in a case of dispute, the burden of proof is almost always on the author [K. Babiaková, *Practical advice on how to protect copyright*, http://www.ephoto.sk/photopointy/photopointy-cz/vysocina/prakticke-rady-ako-chranit-autorske-prava/, accessed on 20 March 2015]: „Photographer drafted and passed a number of photos for the client, which, however, did not pay for ordered photos. Photographer applied to the court for payment of the amount owed, and over the course of the proceedings, mentioned that some photos did his son, while the court did not submit slides of those pictures. Therefore, the court in this case held that in view of the fact that the photographer during the procedure did not demonstrate that the author of all photos, procedurally not eligible for filing and the court rejected his proposal. Court decision that the burden of proof as a procedural responsibility of the participant for the outcome of the case means the party who has failed to adduce evidence necessary to

*E-mail: robert.halenar@ucm.sk

support his statements carries a possible adverse effects such as a court decision, which will be based on the facts ascertained on the basis of other evidence transferred."

There are several ways to protect the rights of the author, but their implementation is largely dependent on the form of the work. Act 618/2003 from the Slovak Collection of Laws, section 7, provides a definition of what can be considered a work: „is subject to copyright and other literary work of art and scientific work, which is the result of his own intellectual creation of the author, especially

a) literary works and computer program;
b) oral, submitted or otherwise made literary work, especially speech and lecture;
c) theatrical works, especially the dramatic work as musical works, choreographic and pantomime work and other work created for publication;
d) musical work with text or without text;
e) audiovisual work, in particular cinematographic work;
f) painting, drawing, sketch, illustration, sculpture and other works of visual art;
g) photographic work;
h) architectural work, especially work of building architecture and urban planning, work of garden architecture and interior design and construction work;
i) works of applied art;
j) cartographic work in analog or in another form." [*Autorský zákon č. 618/2003 Z.z. zo 24. januára 2014*, http://www.vyvlastnenie.sk/predpisy/autorsky-zakon/, accessed on 17 March 2015].

Authors must accept that the online environment has some security principles [1].

2. Protection

A photo represents the author's own intellectual creation and is therefore considered a photographic work. The author of such a photographic work comes with a photo copyrights which consist of personality and equity components. Copyright to the photograph arises by its creation and to prove copyright to the photograph there is no registration needed, as the copyright arises by operation of law. Although the creation of copyright to the photo arises automatically and the author does not need registration, there are of course certain advantages as well because without registering it is not clearly and easily demonstrable, to whom the copyright of the photo belongs. This feature supports plagiarism. To prove their rights to the photograph, the authors must use all legal and technical means, to make the authorship of the picture clear and demonstrable. One of the basic things every author should do, is to realize their basic right to a royalty by checking their name or a pseudonym. Marking the photo can be done by inserting the author's name directly on the photo or under the photo, while the

character © (copyright) and date of creation of the work can be inserted in the menu. Indication of authorship can also be put under the photo, or next to it. To indicate the name of the author of the photo in electronic form, there are several technical methods, which should act as a preventive means of authorship [K. Babiaková, *Practical advice on how to protect copyright*, p. 4]:

1. Keep the original photos with precise and original EXIF (Exchangeable image file format – information set, which are attached to each image that the camera will shoot). EXIF can carry information about:

- the author,
- date and time of design or date of the last modification of the picture,
- data on the camera and lens (brand, exact model),
- exposure data (exposure time and aperture values but also other camera settings).

These are the basic information that a file can contain metadata. The advantage is that inside EXIF in some programs, you can write the name or other information about authorship. Some programs can even lock this information. The disadvantage, however, is that many programs allow you to change information in the EXIF, even those that are locked. Basically, every software and digital lock is attacked by hackers.

2. Buy a more expensive software tool (around hundreds of euros) called Authorization software which connects a unique code to every photo and registers photos in the database.
3. With images that we want to potentially sell or protect our authorship of them, watermark can be used. Watermark (semi-transparent or translucent character that allows picture view and evaluation of the content and quality, but given that it overlaps with the picture, it is not allowed to be used for commercial purposes or other unlawful use). However, watermark can be removed using a variety of software. The more complex and clearer the watermark, the harder it is to remove.

All of these methods have a number of disadvantages. Unfortunately, these methods are generally known or protecting authorship marks can be readily removable, or the protecting methods are relatively expensive.

Photographers who shoot on film have a simpler demonstration of authorship in that they have more negatives, which should demonstrate that the person, who owns negative, is also the author of the photographs. In the case of digital photography, proving of the origin is much more complex – this is the more so if the photo is stored on a publicly accessible digital repository or on the Internet.

If the photos are placed online, the author can be sure that the protection of his rights is insufficient. Scripts 'right-click' can circumvent direct source view, drop-down images can be circumvented in the same way, the watermark can be removed (sometimes with difficulty). Even if the photo is inserted into the Flash object, it can easily create a screenshot [J. Kirnini, *How to Protect Your Digital Photos from Being Copied*, accessed on 17 March 2015, http://webdesign.about.com/od/graphics/a/aa102406.htm].

In this case the author must find an alternative method of protection. A suitable alternative is the location information directly to the user's profile photo (not the notorious metadata). Author also must have an acknowledgement, what is under protection [G. Kessler, *Steganography: Hiding Data Within Data*, http://www.garykessler.net/library/steganography.html, accessed on 17 March 2015].

3. Steganography

The following formula provides a very generic description of the pieces of the steganographic process:

cover_medium + hidden_data + stego_key = stego_medium

In this context, the *cover_medium* is the file in which we will hide the *hidden_data*, which may also be encrypted using the *stego_key*. The resultant file is the *stego_medium* (which will, of course, be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files. This article focuses on image files and will, therefore, refer to the *cover_image* and *stego_image*.

The simplest approach to hiding data within an image file is called *least significant bit (LSB) insertion*. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. If we are using 24-bit colour, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

Now suppose we want to 'hide' the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed):

10010101 0000110**0** 11001001
10010111 0000111**0** 1100101**1**
10011111 00010000 11001011

Note that we have successfully hidden 9 bits but at a cost of only changing 4, or roughly 50%, of the LSBs.

This description is meant only as a high-level overview. Similar methods can be applied to 8-bit colour but the changes are more dramatic. Gray-scale images, too, are very useful for steganographic purposes. One potential problem with any of these methods is that they can be found by an adversary who is looking. In addition, there are other methods besides LSB insertion used to insert hidden information.

Without being too detailed, it is worth remembering that there is *steganalysis*, the art of detecting and breaking steganography. One form of this analysis is to examine the colour palette of a graphical image. In most images,

there will be a unique binary encoding of each individual colour. If the image contains hidden data, however, many colours in the palette will have duplicate binary encodings since, for all practical purposes, we cannot count the LSB. If the analysis of the colour palette of a given file yields many duplicates, we might safely conclude that the file has hidden information.

But what files should be analyzed? Suppose we decide to post a hidden message by hiding it in an image file that I post at an auction site on the Internet. The item auctioned is real so a lot of people may access the site and download the file; only a few people know that the image has special information that only they can read. Needless to say, audio files may cover hidden data, too. Indeed, the quantity of potential cover files makes steganalysis a Herculean task [2].

We must also have an effective tool to apply the protection (for steganography) and also for steganalyse, e.g. Matlab. Matlab and its use were described in literature [3].

4. BMP and JPG file extension

Data of which a photography consists can be enriched by information (cipher) which is not directly visible but can help in proving copyright. Pixels that the picture displays are used for the location of the information. It is therefore a process which is similar to a watermark, but it is not directly visible (even in many cases indistinguishable to the human eye).

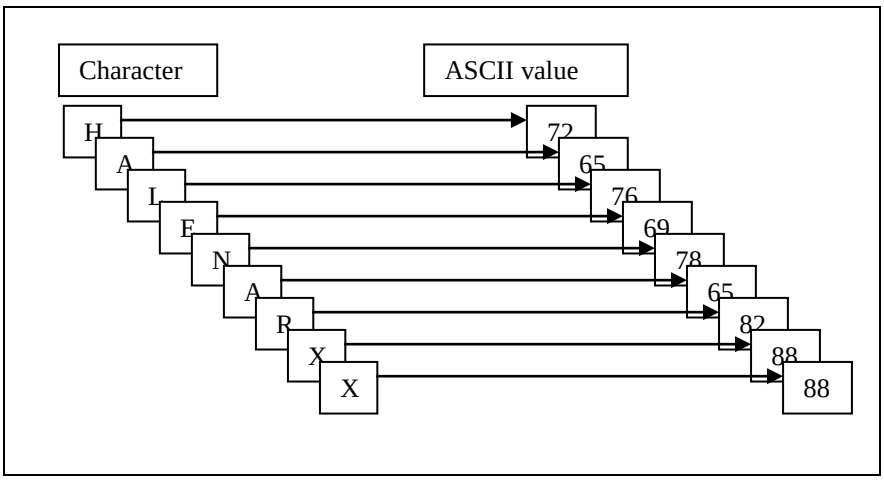

Figure 1. Decimal character codes identifier according to the ASCII table.

The principle is in the code - simple password consisting of several characters (first name, last name, or other identifier), which is translated using the ASCII table numbers in decimal, which are converted into binary form.

Let us identify ‘HALENARXX’ that uses ASCII translate table as shown in Figure 1 (to automate the translation, the MATLAB environment was used).

Each character is expressed as a numerical representation. Then it is converted into the binary form as shown in Figure 2.

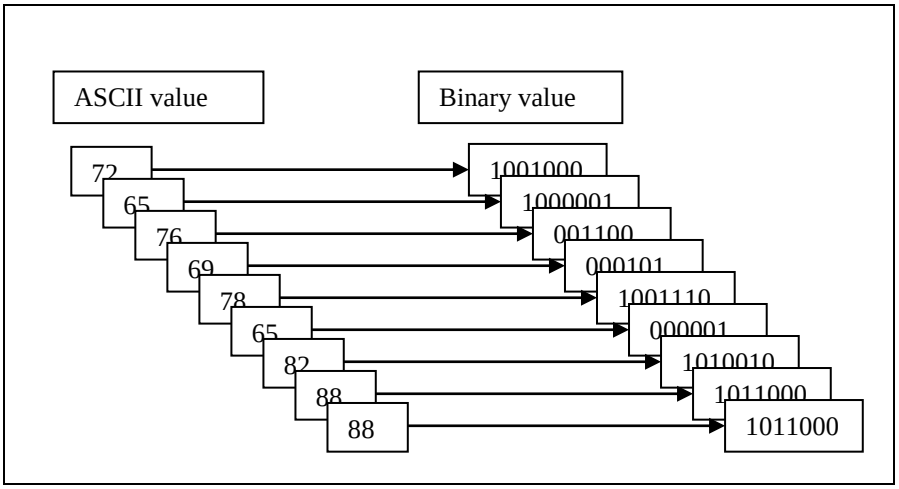

Figure 2. Binary character codes identifier according to the ASCII table.

Figure 3. Steganography infiltration applied at 5th bit of the Blue component of RGB, BMP file extension, C. Monet, *Snow at Argenteuil – 1875*, http://grafika.sk/clanok/vianocny-pozdrav-od-grafika-sk/, accessed 19 March 2015.

If we use only one bit, and not the least one, but for example the fifth bit, and not for all components of RGB representation, but only for one, for example Blue, quality impact is completely different. Figure 3 shows an image with steganography infiltration applied on 5th bit of the Blue component of RGB model representation.

To proof the infiltration in it we applied modified settings of Hue/Saturation in Adobe Photoshop, as we can see in Figure 4.

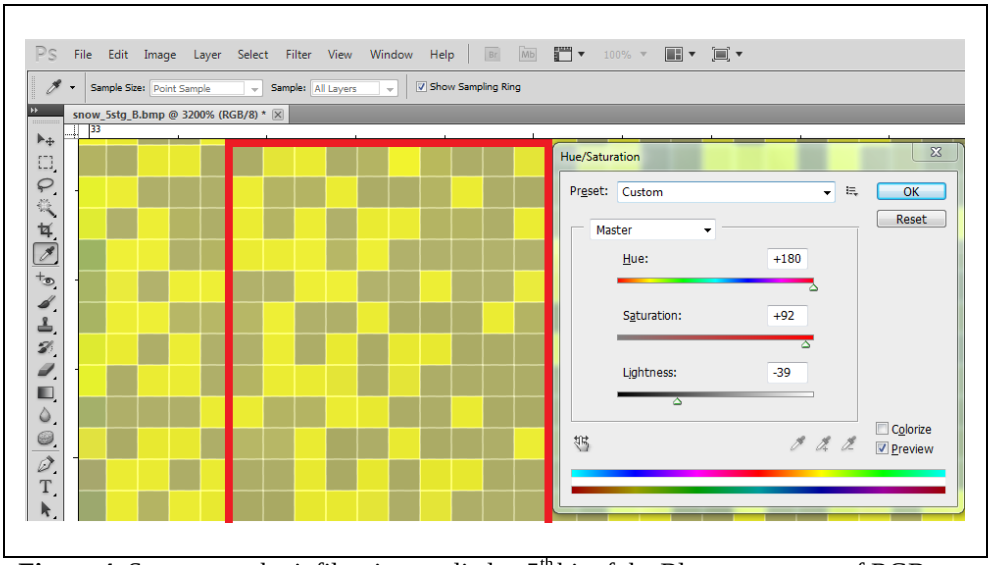

Figure 4. Steganography infiltration applied at 5th bit of the Blue component of RGB after modification of Hue/Saturation settings in the Photoshop.

Figure 5. 24 bit BMP file extension saved as 256 colours BMP file.

Next we saved 24 bit BMP file extension to 256 colours BMP file extension, see Figure5, and then we saved this image as JPG file extension, see Figure 6.

Figure 6. 256 colours BMP file extension saved as JPG.

Figure 7. Area with untouched steganography infiltration – it can be clearly recognizable in detail.

After several modifications, the image may look different. These modifications can be done selflessly or can be purpose-made. However, steganography infiltration can be lost in some parts of the image. That is why it is necessary to look for areas, where infiltration is still untouched, as we can see in Figure 7. Sometimes it is necessary to analyze a huge amount of data [4].

To proof the infiltration in the image, we zoomed a part of the image, as we can see in Figure 8. After comparison with the pattern in Figure 5, there is

still compliance. This research can be considered to be used as case study and as a research method [5].

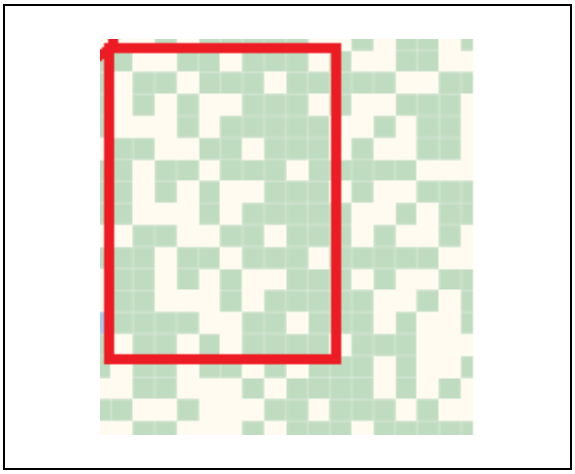

Figure 8. JPG extension with steganography infiltration zoomed.

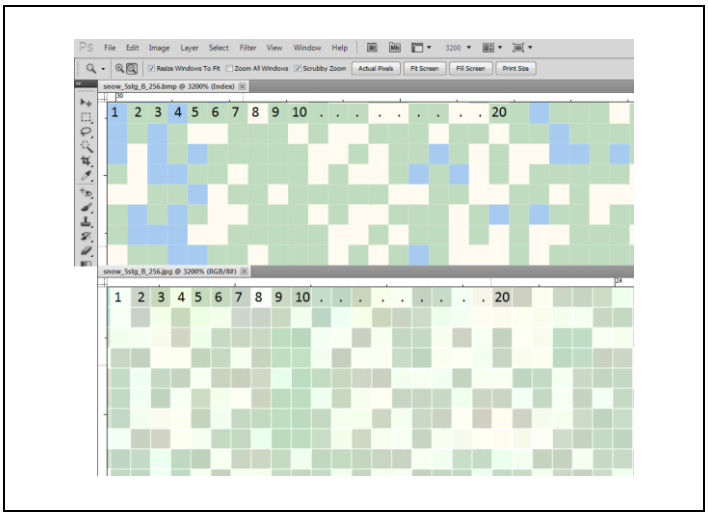

Figure 9. Original BMP extension (top) and JPG extension (bottom) file with steganography infiltration zoomed.

If we compare a part of the image saved as 24 bit BMP file extension, with the image degraded on 256 colour BMP file and the part of the same image saved as JPG file extension, the same pattern can still be recognized, see Figure 9. In Figure 10 we can see directly which pixels represent characters from the identifier. There is also a match.

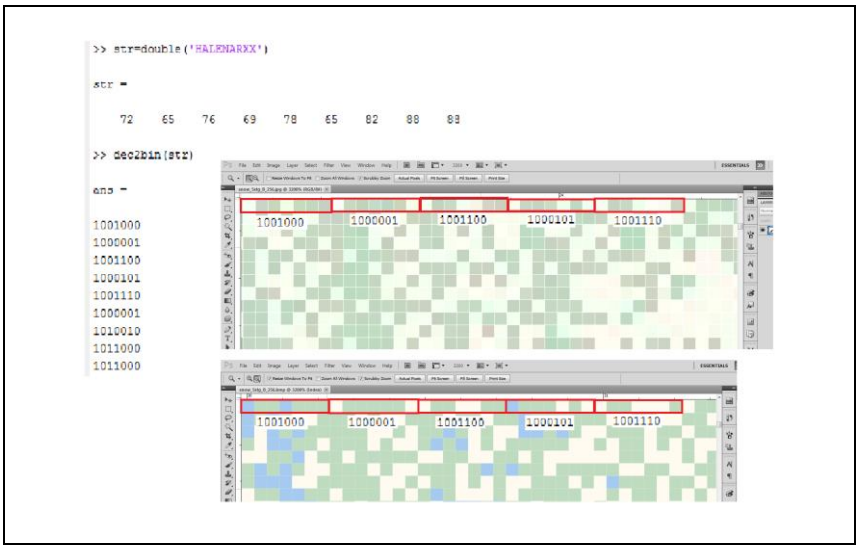

Figure 10. JPG (top) and BMP (bottom) file extension with steganography infiltration zoomed and directly explored.

5. Conclusion

There are many ways how to apply copyright protection. In this paper we use steganography, for which there are several possibilities how to infiltrate information into an image in digital form. In this article we selected the 5th bit of Blue channel of RGB colour representation because we assumed that the steganography infiltration stored in such a high bit can resist a huge impact on the quality of original photography. As we can see, human eye is not able to recognize it in original. We converted 24 bit BMP file extension to 256 colours BMP and then to JPG file extension. After several file extension conversions and colour depth change, the steganography infiltration is still 100% readable and recoverable. This may be seen as a proof of resistance.

References

[1] P. Murár, *On-line bezpečnosť,* in *Mediálna výchova: pre učiteľov stredných škôl*, Centrum mediálnej gramotnosti, Trnava, 2011, 106-107.

[2] M. Solík, *Issues of Applications of Law*, in *Otázky zvyšovania právneho vedomia v neprávnických študijných odboroch - Megatrendy a médiá 2014*, Fakulta masmediálnej komunikácie UCM v Trnave, Trnava, 2014, 153-163.

[3] R. Halenar, Eur. J. Sci. Theol., **10(suppl. 1)** (2014) 253-262.

[4] A. Trnka, Eur. J. Sci. Theol., **10(suppl. 1)** (2014) 143-148.

[5] A. Hurajová, *Case study as a research method: features, design and methodology*, in *Mapping and Applying: Research in Foreign Language Education*, Pedagogická fakulta UKF v Nitre, Nitra, 2013, 70-88.