CZASOPISMO TECHNICZNE M
WYDAWNICTWO POLITECHNIKI KRAKOWSKIEJ

z. 3-M/2008
ISSN 0011-4561
ISSN 1897-6328

MARIUSZ KRAWCZYK*

DIGITAL MARKING AND HIDING OF INFORMATION IN CAD SYSTEMS

ZNAKOWANIE I UKRYWANIE INFORMACJI W SYSTEMACH CAD

A b s t r a c t

Although the copyrights are more and more protected by law they will soon be a dead law. In the digital age, there is no difference between the original and the copy, which makes them undistinguishable. A solution that may help in protecting copyrights is technique of hiding information, which in case of doubt may identify the owner of the project. Such techniques are watermarks, which are used very often in music and movie industry. The paper presents a technique of marking documents in CAD system. It allows efficient identification of the authors of drawings.

Keywords: *steganography*, *CAD system*, *hiding information*

S t r e s z c z e n i e

Aktualne przepisy chroniące prawa autorskie, mimo że są coraz bardziej szczegółowe, tak naprawdę nie chronią własności. W dobie powszechnej informatyzacji nie ma różnicy między oryginałem i kopią. Pomocą służą techniki ukrywania informacji umieszczające dane o twórcy projektu i w sytuacjach spornych rozstrzygających o prawach własności. Techniki znakowania plików są stosowane w przemyśle muzycznym i filmowym. W artykule opisano metody ukrywania informacji w plikach CAD, które pomogą w identyfikacji autora pliku.

Słowa kluczowe: *steganografia*, *systemy CAD*, *ukrywanie informacji*

*Mariusz Krawczyk, MSc, Institute of Applied Informatics, Cracow University of Technology.

1. Introduction

There is a need to electronically mark documents in the process of designing. The race to hold the market often leads producers to abuses or even to plagiarism in the process of designing. The espionage and copying ideas of the competition are very difficult to prove in the electronic age due to the fact that while copying the quality of the file does not deteriorate. Marking one's own documents, i.e. adding some information about the owner, might be a way of securing the file against unauthorised copying.

There are available methods of marking graphic and sound files with "watermark technology"; however, marking text files is very difficult. It seems that steganography (the field of science that deals with hiding information), might be useful for such purposes.

2. Analysis of marking methods

Watermarking technology and steganography are based on a fundamental function: hiding additional representative information in the original signal (OS), using socalled watermark (WM). This additional information is imperceptible depending on the application type: for the voice system (HAS – Human Auditory System) for vision system (HVS – Human Visual System). Combining OS with WM technology we receive a genuine signal marked with watermark (OWM) which sounds or looks like (almost identical) OS. In Figure 1 the basic structure of marking systems has been shown according to R. Popa [1].

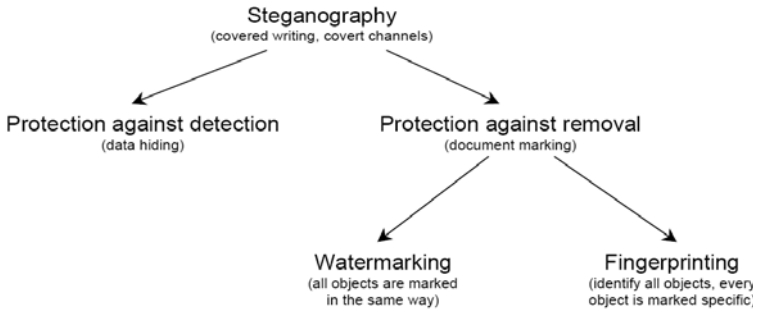


Fig. 1. Direction within steganography [1]

Rys. 1. Podział steganografii [1]

2.1. Requirements for hiding information

A steganographic system is a system of hiding additional information which will have the information hidden below the layer of the original signal.

There are many ways of hiding information in the original signal; however, the way that can be used in a steganographic system has to fulfil the following requirements [2]:

– Integrity of the hidden information after placing it in the stego object (the original signal together with the hidden message) must be kept. The hidden information can not be changed at any moment by adding, removing or modifying the existing one.

– Changes in the stego object should not be visible, or almost invisible, with a naked eye. If changes are visible, they can be changed or destroyed by the third party.
– The watermark itself should not be affected during the marking (watermarking) operations on the stego object. For example, when we have an illegal copy of some image which we want to transform, change size, or rotate. The watermark must be resistant to such manipulations, otherwise a third party can easily remove the watermark and the principles of marking are lost.
– We always assume that the third party knows about the hidden information in the stego object.

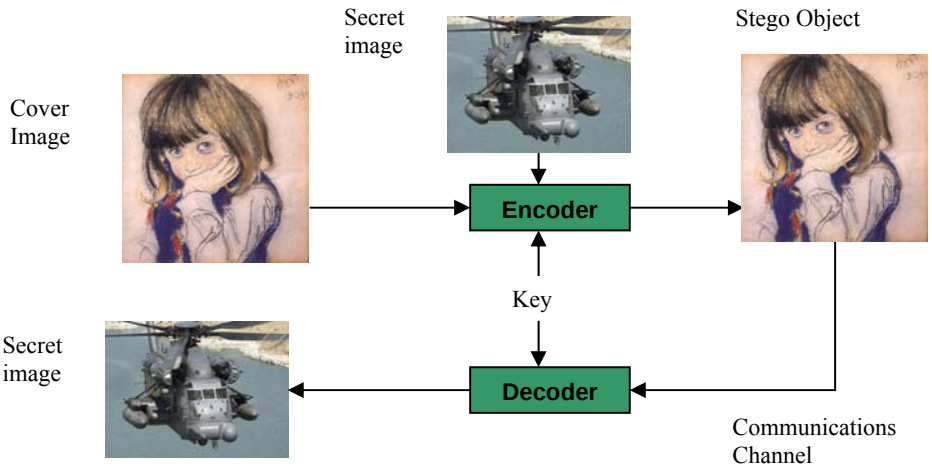


Fig. 2. Generic process of encoding and decoding hidden information

Rys. 2. Proces kodowania i dekodowania ukrytej informacji

In the presented example the protected image will be encoded in the covering image, which will result in a stego object.

On account of performed functions, marking technologies can be divided into:

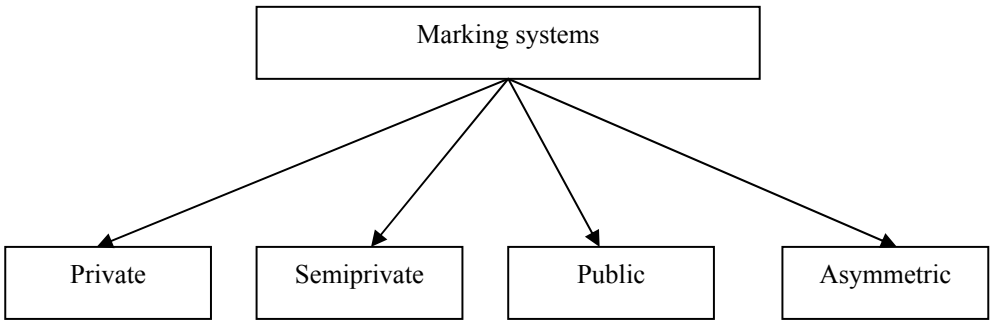


Fig. 3. Marking systems

Rys. 3. Systemy znakujące

Equation (1) shows how the function is transformed into a three-element set [1]

$$I \times K \times M = I' \tag{1}$$

where:

I – object,
K – key,
M – hidden information,
I' – stego object.

Private Marking Systems require genuine signals during detection

I type: $$I' \times I => \{0, 1\} \tag{2}$$

II type: $$I' \times I \times K \times M => \{0, 1\} \tag{3}$$

Semi-Private Systems do not require the genuine signal during detection

$$I' \times K \times M => \{0, 1\} \tag{4}$$

Public Marking Systems (Blind Marking) – do not require the genuine signal during detection

$$I' \times K => M \tag{5}$$

Asymmetric Marking Systems allow only reading WM, but not removing it.
In the process of designing technical drawings are saved in universal file formats, for example for 2D graphics DXF format is used.

However, there are some restrictions for hiding information in text files:
– amount of hidden information is limited,
– detecting hidden information in an open text is an easy task, even without any software,
– hidden information is easy to damage or completely destroy.
– Stego algorithms based on text containers can be divided into two groups:
– algorithms setting the information in such a way as to make it possible to keep the stego object in a non-digital form (e.g. as a printed sheet of paper),
– algorithms are exclusively digital.

The group of mechanisms proposed by J. Brassil is related to the first category, and they are determined as *line-shift-coding*, *word-shift-coding*, *feature coding*, a semantic and syntactic method. The algorithm of white signs ranks among the second category.

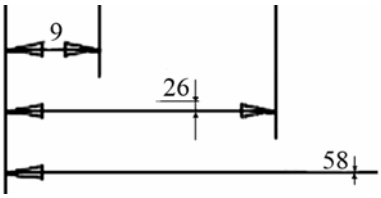
Line-shift-coding

The *line-shift-coding* algorithm is based on precise manipulating of location of the line of the text with respect to lines above and under it. The shift should have a fixed value, which usually is 1/300 inch. The advantage of this algorithm is that the hidden information will not be destroyed even after document was printed. The research shows that it is possible to separate out the hidden information even after ten Xerox copies of the original document have been made.

An advantage of this algorithm is that the information will not be destroyed even after printing the document. Examinations showed that correct distinguishing the hidden information was possible even after 10 generations of photocopy of the original. However, the disadvantage of this method is the probability of detection of hidden information by a third party.

Fig. 4. An example of coding technical documentation: change in the height of the dimensions above the dimension line

Rys. 4. Przykładowe kodowanie informacji poprzez zmianę odległości liczby wymiarowej od linii



Feature coding

This algorithm is based on changes of idiosyncrasies, e.g. change in height of letters belonging to letters L = {b,d,k,l,h.t}

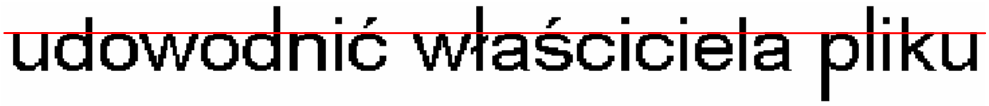


Fig. 5. Feature coding

Rys. 5. Funkcja kodowania

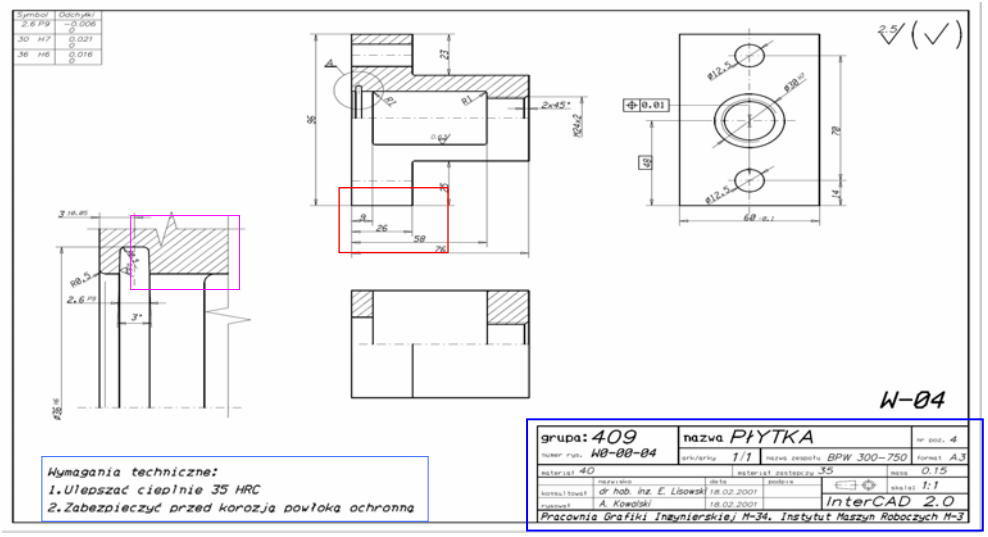


Fig. 6. Figure 2D with hidden information

Rys. 6. Ukrywanie informacji w rysunku 2D

In this way with a few algorithms of hiding the information we can hide the additional information in the 2D drawing. In drawings consisting of three views, text, dimensions and table it is possible to hide ca. 20 bits of information. It allows to encode 2 bytes and 4 bits of the "check sum"

3. Conclusions

Due to the standardisation of technical drawings, what is the most important problem for hiding information is to find an appropriate information container. Hiding information in 2D vector files is difficult due to the ease of their removal. Therefore it is most favourable to include hidden information on a printout.

References

[1] Popa R., *An Analysis of Steganographic Techniques,* Politechnica University of Timisoara 1998 http://ad.informatik.unifreiburg.de/mitarbeiter/will/dlib_bookmarks/digital-watermarking/popa/popa.pdf.

[2] Cummins J., Diskin P., Lau S., Parlett R., *Steganography and Digital Watermarking* School of Computer Science, The University of Birmingham, 2004.