Преглед НЦД 19 (2011), 1–6

Vesna Vučković
Faculty of Mathematics, Belgrade

DIGITAL WATERMARK IN DIGITAL IMAGES AND E-BOOKS

Abstract: In the Internet and digital copies era, there is a problem of copyright protection for intellectual property in digital format. Digital watermarking is recognized as one solution of this problem. Here is given brief description of results for images and e-books digital watermarking, that I obtained, working on cultural and scientific heritage digitization project.

Keywords: Digital watermark, white Gaussian noise, digital images, e-books

1. Introduction

This paper resulted from my participation in Serbian scientific and cultural heritage digitization project. This project participants (first of all from Faculty of Mathematics Belgrade and Mathematical Institute SASA), during the previous decade, put into the public's reach many digital works (images and e-books) by means of compact disks or Internet. For example,

- Compact disc which contains e-book dedicated to Serbia and Belgrade photos from the second half of the 19th Century (precisely, from the time of Serbian–Turkish wars, 1876–1878), whose author was I.V. Groman, Russian military photographer. These photos are mainly in ownership of Belgrade City Museum and Belgrade Military Museum ([1], [2], [3])
- Nikola Tesla's press-clippings collection (ownership of Nikola Tesla Museum in Belgrade) ([4])
- Virtual library – e-books library (old worthy books, doctoral dissertations, scientific papers, for now mainly from mathematics and related sciences – and recently also from other sciences) ([5], [6])

In order to copyright those images and e-books, we decided to label them by digital watermark embedding.

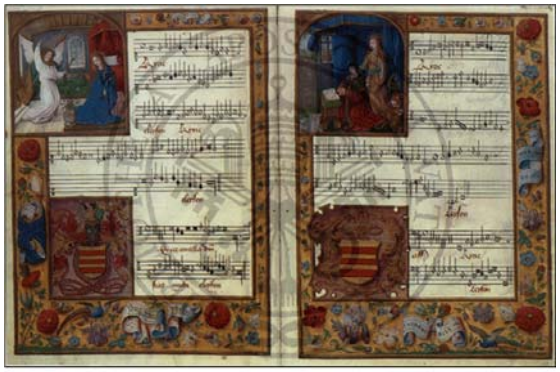
This paper deals with obtained results in searching for good watermarking procedure for our needs. Actually, here it is not proposed any new watermarking algorithm. Here is used well-known AWGN watermark, and for it I search for optimal embedding conditions.

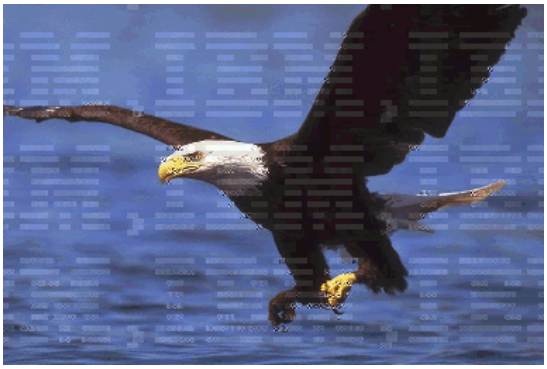
In Section 2 is given a brief view of fundamental concepts related to digital watermarking. Digital watermark for grayscale images is theme of Section 3. Obtained results are then passed to color images (4), black-white images (5) and e-books (6).

2. Digital watermark – basic concepts

(Digital) watermark is bit pattern which is embedded into digital image, e-book, video or audio clip, or another digital work, and which contains some information about this work (usually about its author or owner). This information is written together with file's data (in the case of image, for example, in a way some pixels will be changed). The purpose of digital watermark is to provide copyright protection for intellectual property in digital format.

Although perceptible exist also (see images!), in copyright protection imperceptible watermarks attract much bigger attention.





In digital watermarking there are “two sides of the coin”. In some moment, the watermark is embedded; later, it will be detected. This will be done by two computer programs – *embedder* and *detector*.

Good imperceptible digital watermark is not easy to produce. It needs to satisfy two opposite requests:

- *Detectability* – in any case it needs to be detectable
- *Fidelity* – digital watermark needs to be imperceptible for casual observer.

These two demands are mutually confronted. If watermark is embedded stronger, then it will be more confident that it will be detectable. On the other hand, if watermark is strongly embedded, it will be more noticeable. Detectability is surely more important condition – “essential requirement”. Thus, the problem is: determine *optimal embedding strength – minimal one which guarantees detectability.*

In some situations it may be expected that watermarked work will be subjected to some modification (from embedding to detection moment). In the case of image, modification examples are lossy compression, sharpening, blurring, brightness/contrast changing, cropping, dimension changing, rotation... Under these circumstances it is also useful to know optimal strength – minimal one which ensures watermark detectability after this (expected) modification.

Two concepts are close related to watermark detectability: effective and robust embedding. Watermark is embedded *effectively* if it is detectable immediately after embedding. If a message is detectable in digital work which is after embedding subjected to some modification, we say the watermark is *robust* against undergone modification.

3. Digital watermark for grayscale images

Basic steps in my search for adequate digital watermark for grayscale images were:

- Algorithm decision
- Determining optimal strength for effective embedding
- Determining optimal strength for watermark robust against expected modification

3.1 Algorithm decision. In two decades long digital watermarking history, there are proposed many different robust watermark algorithms for grayscale images. Most of them use one of spread spectrum techniques: message bit is embedded over whole image or over its big part.

During the search for a watermark which will be used in our digitization project, I decided to use one technique, based on embedding white Gaussian noise pattern. Precisely, one bit information we embed by addition of image matrix with one matrix whose elements ale liable to normal (Gaussian) distribution of zero mean. Detection will be preformed by exam-

ining of correlation between image matrix and matrix with normal distribution, for which we examine if it is embedded.

It follows brief outline of embedding and detection algorithms that will be used here. Detailed description can be found in [7].

3.1.1 One-bit message embedding. Each grayscale image of $m \times n$ pixels is presented in computer memory by one $m \times n$ matrix or (same in essence) by vector of dimension $m \cdot n$. Image matrix (vector) components contain pixels values – integers from the set $\{0,1,2,...,255\}$. Grayscale pixels nuances from black to white are presented by numbers from 0 to 255.
We embed into the image one bit information (binary one or binary zero) as follows:

$c_{w1} = [c_0 + \alpha \cdot r_w]_8$, $\quad c_{w0} = [c_0 - \alpha \cdot r_w]_8$

c_0 is original image (before embedding) matrix, c_{w1} and c_{w0} are images matrices after binary one (binary zero) embedding, α is embedding strength coefficient ($\alpha > 0$), and r_w is reference pattern. *Reference pattern* is one matrix of the same dimension as in original image, with elements from standard normal distribution ($N(0,1)$). From practical reasons, program – embedder does not use as input data the whole reference pattern. It rather uses one secret number, *watermark key*, from which the reference pattern will be generated.

During saving on disk as image, all of matrix elements need to be "squeezed" into only possible – 8-bit values – integers from the set $\{0,1,2,...,255\}$. In quoted formulas, $[\ ]_8$ denotes this "squeezing".

3.1.2 Detection. Detector, beginning with watermark key (the same as in embedder) generates reference pattern r_w (the same as in embedder). Then, it calculates linear correlation

$$\boldsymbol{lc}(\boldsymbol{c},\boldsymbol{r}_w) = \frac{\boldsymbol{c} \bullet \boldsymbol{r}_w}{\|\boldsymbol{r}_w\| \cdot \|\boldsymbol{r}_w\|}$$

between the image and the reference pattern. Then, it compares the obtained value with in advance set threshold value τ. Detector reports:

It is embedded binary one	if	$\boldsymbol{lc}(\boldsymbol{c},\boldsymbol{r}_w) \geq \tau$
It is embedded binary zero	if	$\boldsymbol{lc}(\boldsymbol{c},\boldsymbol{r}_w) \leq -\tau$
It is embedded nothing	if	$\lvert\boldsymbol{lc}(\boldsymbol{c},\boldsymbol{r}_w)\rvert < \tau$

3.1.3. Longer message embedding. We embed a k bits message into the image by embedding repeatedly (k times) one bit message: beginning with watermark key it will be calculated k reference patterns, which will be embedded into the image.

3.2 Effective embedding optimal strength. Results sketched in (3.2) and (3.3) are derived in [8] and [9]. It is derived mathematical formula for effective embedding optimal strength for one bit message. Formula is based on normal distribution properties. Thus, optimal embedding strength α for image given by matrix c_0 and reference pattern r_w is

$\alpha = \max(\tau - l, 0)$ if we embed binary one

$\alpha = \max(\tau + l, 0)$ in the case of binary zero embedding

(where $l = lc(c_0, r_w)$). For message of k bits, which will be embedded with strengths $\alpha_1, \alpha_2, ..., \alpha_k$, it is derived formula for total embedding strength: $\beta = \sqrt{\alpha_1^2 + \alpha_2^2 + ... + \alpha_k^2}$ (em-

bedding of k reference patterns with strengths $\alpha_1, \alpha_2, ..., \alpha_k$ respectively, will be realized as embedding of one reference pattern with strength β).

3.3 Optimal strength for image which will be subjected to expected modification. It is proposed algorithm for determining the minimal embedding strength, which guaranties watermark detectability after expected modification. Special attention is paid to lossy compression. The reason for this is: Almost all images and e-books which can be found on Internet are in some lossy compressed format. Under such circumstances, one part of watermark will be destroyed after embedding, during saving on the disk. For example, if watermarked image we save in JPG format, it automatically will be subjected to JPEG compression, and a part of watermark data will be destroyed.

4. Digital watermark and color image

Each color image can be regarded as three grayscale images combination (one for each of red/ green/ blue components). Therefore, it is not too complicated to generate results for grayscale images to use for color images. However, for better results we need to take care of human visual system (HVS) characteristics:

- Human eye notices changes in green color nuances best, something worse it discerns changes in red, and changes in blue it discerns worst. That's why some authors recommend watermark embedding mostly in blue color channel.
- Human eye better notices changes in brightness than in color nuances. Hence, JPEG standard use different compression intensity for those components. For good watermark algorithm, we should take care about this fact.

Until now, I didn't investigate particularly watermarking for color images. This is one of research themes for subsequent period.

5. Digital watermark and black-white images

Proposed algorithm is not suitable for simple black-white images (as book pages usually are). First of all, in big white image regions (for example, page margins) a large part of embedded data will be destroyed by "squeezing" operation: values which, after adding white noise to image matrix becomes greater than 255, after "squeezing" return to 255. Also, it is very easy to erase watermark data from these image regions (for example, with eraser in Photoshop).
Particular class of such images form black-white text pages. These images are especially inconvenient for watermark embedding, because the watermark can be removed from them simply by text retyping.

6. Watermark for e-books

Electronic book (e-book) is the digital equivalent of a printed book. In our Virtual library e-books are in PDF format. On Internet, DjVu format is often used as well.
PDF books in our Virtual library, from the viewpoint of digital watermark embedding, may be classified as:

- E-books produced by *scanning***;** theirs pages are images (book pages scans). Watermark may be embedded into them in the same manner as in other images.
- E-books originated *from DOC or TeX files*; these image pages are not bitmapped images. Hence before embedding, they need to be converted to bitmaps.

6.1 PDF e-books produced by scanning. In order to make PDF watermarked e-book:

1. We scan book pages – result are bitmapped (e.g., TIFF) images.
2. In each book page (TIFF file) we will embed watermark – result will be watermarked TIFF page.
3. We will combine watermarked TIFF pages, into one PDF file – watermarked e-book.

Detection:

1. Book page in which we search for watermark we will extract from PDF file and save (e.g.,) as TIFF image.
2. We detect the watermark message in this image.

6.2 PDF e-books originated from DOC and TeX files. PDF file pages need at first to be converted to bitmaps; this can be done by conversion of PDF pages into (e.g.,) TIFF images. After that we may proceed with described procedure.

However, by converting pages into images, we lose possibility of text retrieving in the file. This problem can be overcome by using some OCR procedure.

6.3 Problems in e-books watermarking. Although e-books watermarking is possible, in its realization arise serious problems. One of them exists with each big book (with a lot of pages) – huge spatial and temporal resources are needed for its watermarking (if we embed such watermark in each e-book page). Until now, we have not found a way for this problem overcoming, and this is one of the tasks whose solution we need to search for.

Another problem is related to those e-books which contain black text on white background. Problem is first of all emphasized with second mentioned e-books class. Watermarking makes sense only if these books aren't purely textual files (see chapter 5), but they contain some amount of pictures, in which watermark would be embedded. Pages in e-books produced by scanning usually aren't black-white, but grayscale (or color) images. Even theirs margins are not completely white, and watermarking is possible for them.

Conclusion and future activities

Here presented text is a brief description of former activities in digital images watermarking, within cultural heritage digitization project. Here are presented achieved results concerning digital watermarking for electronic documents.

Segment concerning grayscale images is practically completed (results may be seen in detail, in [8] and [9]).

As regards color and black-white images watermarking, although some results that enable digital watermark embedding exist, additional effort is needed to achieve better results. Watermark embedding into e-books is in a certain degree investigated, but real embedding into big books follows. Watermarking for black-white textual books is not suitable because the ease of watermark removing.

References

[1] Žarko Mijajlović et al. *Groman's photo album 1876-1878*. (compact disk), 2003. Published by TheBelgrade City Museum, The Faculty of Mathematics in Belgrade, The MathematicalInstitute of SANU. The CD is catalogued as ISBN 86-7589-0370-0.

[2] Žarko Mijajlović et al. Web page. *Groman's photo album 1876-1878*. http://www.ncd.matf.bg.ac.rs/projects/en/groman.html, 2003.

[3] Saša Malkov: *On photograph library design – Groman library,* NCD Review 13 (2008), 27–36

[4] Saša Malkov, Nenad Mitić, Žarko Mijajlović: *Nikola Tesla online clipping library prototype*, NCD Review 12 (2008), 75–81

[5] Web page *Virtual library eLibrary*, http://elibrary.matf.bg.ac.rs/
[6] Mirjana Borisavljević: *Doctoral dissertations in logic from Virtual library of the Faculty of Mathematics in Belgrade*, NCD Review 16 (2010), 1-17
[7] I J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, T. Kalker: *Digital Watermarking and Steganography*, Morgan Kaufmann Publishers, 2008
[8] Vesna Vučković: *Embedding strength criteria for AWGN watermark, robust against expected distortion*, Computing and Informatics, Vol. 29, no.3 (2010), p. 357–387
[9] Vesna Vučković: *AWGN watermark optimal strength* (doctoral dissertation), Faculty of Mathematics, Belgrade, 2010

Сажетак: У ери Интернета и дигиталних копија, тешко је заштитити ауторска права аутора и власника дигиталних радова (слика, аудио и видео клипова). Као једно решење проблема препозната је уградња дигиталних жигова у ове радове. Овде се даје кратак приказ резултата у вези са праксом уградње жигова у слике и електронске књиге, до којих смо дошли у току рада на пројекту дигитализације културне и научне баштине.

Кључне речи: Дигитални водени жиг, бели Гаусов шум, дигиталне слике, електронске књиге

vesnav@matf.bg.ac.rs