Watermarking, Steganography, and ErrorControl Codes

S. Boumova, H. Kostadinov, and N. L. Manev

Citation: AIP Conf. Proc. **1404**, 193 (2011); doi: 10.1063/1.3659920
View online: http://dx.doi.org/10.1063/1.3659920
View Table of Contents: http://proceedings.aip.org/dbt/dbt.jsp?KEY=APCPCS&Volume=1404&Issue=1
Published by the American Institute of Physics.

Watermarking, Steganography, and Error-Control Codes

S. Boumova*, H. Kostadinov† and N. L. Manev†

*Higher School of Civil Engineering "Lyuben Karavelov", Sofia, Bulgaria
†Institute of Mathematics and Informatics, BAS, Sofia, Bulgaria

Abstract. An algorithm for embedding binary messages in spatial domain of images is proposed. The algorithm exploits erasure capability of error-control codes that results in improving the robustness and increasing the size of the embedded message. This enables the described algorithm to be used for steganographic purposes, too.

Keywords: Watermarking, steganography, erasure codes, images, spatial domain
PACS: 89.70.Kn; 89.20.Ff;

INTRODUCTION

Steganography and Digital Watermarking are concerned with embedding information in digital media such as images, audio signals and video. Both scientific disciplines develop methods for conceal message (a sequence of bits) by modifying the host (cover) digital object but their goals are slightly different. The purpose of steganographic techniques is to alter the cover object in undetectable manner, that is, no one but the intended recipient to be able to detect the altering of the cover work. The goal of watermarking is to prevent piracy or to prove the ownerships by imperceptibly altering the digital media object. Both digital watermarking and steganography are subject of a strong interest and research activity especially in the last decade. A lot of techniques as well as commercial realization of some of them have been proposed. A comprehensive overview of the mathematical methods and the core techniques can be found, *e.g.*, in [1], [3], [5], [6].

In this talk we propose an algorithm for embedding binary sequences in spatial domain of images. Our method exploits erasure capability of error-control codes that results in improving the robustness. The algorithm enables the relatively larger number of bits to be embedded. Thus it can be used for steganographic purposes, too.

The next section is a very brief introduction to watermarking, steganography, and error control codes. The algorithm is described in the third section. The forth section demonstrates the algorithm by an example.

PRELIMINARIES

Definitions and notations

Here is the list of basic terms.

- **Cover work (object)** is the term used for referring to the digital object that presents a media product: a song, picture, video, or a specific copy of them;
- **Media** refers to the means of representing, transmitting, and recording cover works;
- **Watermarking** is any practice of imperceptibly altering a cover work to embed a message about that work.
- **Steganography** is the term used for techniques of altering the cover object in undetectable manner, that is, no one but the intended recipient to be able to detect this altering.
- **Watermark** is usually used with two different meanings: the reference (noisy) pattern added to a cover work, and the message embedded by that pattern. The right meaning is cleared by the context.

Figure 1 presents a general description of digital watermarking (and steganographic techniques). The source message is optionally encrypted and/or encoded and added to the cover work. The sign $\oplus$ in the figure should be understood as a symbol for a function $\mathbf{c}_w = \mathscr{E}(\mathbf{c}_0, \mathbf{m}, \mathbf{k})$ of the cover work, message, and key, although it is often

Application of Mathematics in Technical and Natural Sciences
AIP Conf. Proc. 1404, 193-199 (2011); doi: 10.1063/1.3659920

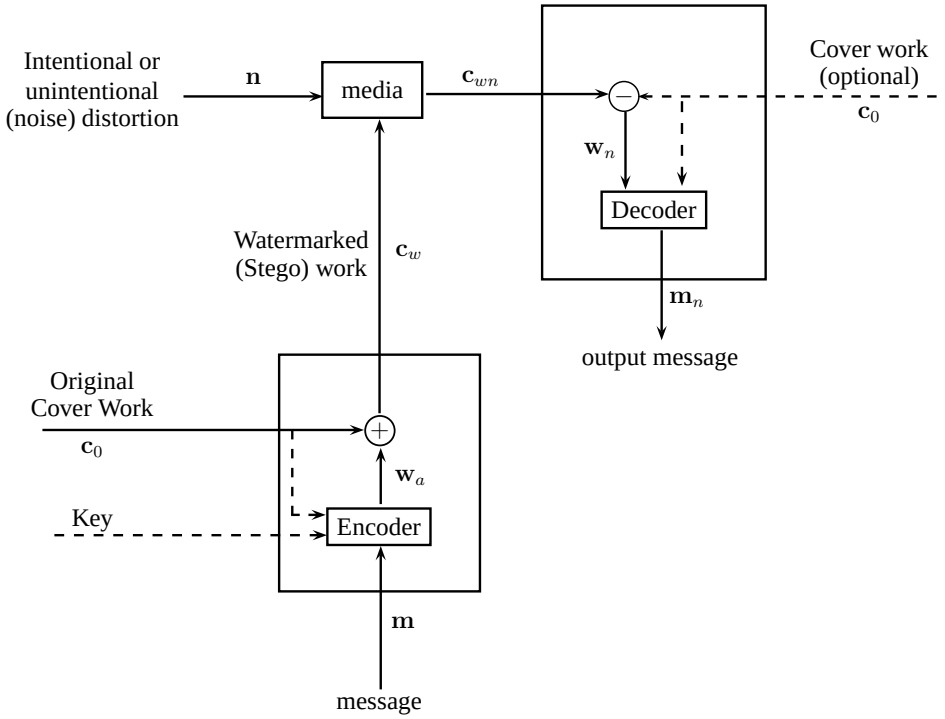

FIGURE 1. Watermarking (steganography) block diagram

the simple addition. The watermarked digital object passes through media where it is a subject of intentional or unintentional distortions. In spite of these distortions the recipient has to derive and decode and/or decrypt the message.

The possible applications of watermarking are:

- **Broadcast monitoring**: Identifying when and where works are broadcast by recognizing watermarks embedded in them.
- **Owner identification**: Embedding the identity of a work's copyright holder as a watermark.
- **Proof of ownership**: Using watermarks to provide evidence in ownership disputes.
- **Transaction tracking**: Using watermarks to identify people who obtain content legally but illegally redistribute it.
- **Content authentication**: Embedding signature information in content that can be later checked to verify it has not been tampered with.
- **Copy control**: Using watermarks to tell recording equipment what content may not be recorded.

In many practical situations we **do not need to provide strong security against removing or modification of the hidden message but it is very important to conceal its existence**. Such situations form the area of application of steganography.

The most important characteristics of the digital watermarking systems are given below.

- **Capacity (Payload)** refers to the number of bits a watermark embeds within a unit of time or within a Work. For a photograph, the data payload would refer to the number of bits encoded within the image. For audio, data payload refers to the number of embedded bits per second that are transmitted.
- **Imperceptibility** - The watermark is imperceptible if a normal human being is unable to distinguish (optically or acoustically) the original from the watermarked work.
- **Robustness** refers to the ability to detect the watermark after common signal processing operations like spatial filtering, lossy compression, printing and scanning, and geometric distortions (rotation, translation, scaling, and

so on). Robustness does not include intentional attacks based on the knowledge of the algorithms or on availability of the detector functions.

- **Security of a watermark** refers to its ability to resist hostile attacks, such as unauthorized removal, embedding (forgery), and detection. In many watermarking systems, the method by which messages are embedded in cover works depends on a key, and a matching key must be used to detect those marks.

The requirements to steganographic techniques are similar but they are considered from the view point of steganography goals.

- **Capacity**:
  - ***Embedding capacity*** is the maximum number of bits that can be hidden in a given cover work.
  - ***Steganographic capacity*** is the maximum number of bits that can be hidden in a given cover work, such that the probability of detection by an adversary is negligible.
- **Embedding efficiency** is defined as the number of secret message bits embedded per unit distortion.
- **Statistical undetectability** is the probability of detecting a stego work based on the assumed distributions of cover and stego works.
- **Security refers** to the situation in which the warden is active or malicious, rather than passive.
- **False alarm rate** is the probability that a steganalysis algorithm will report the presence of a covert message when none is present.

Watermarks can be embedded by altering the cover works either in spatial domain, or in frequency domain.

- **Spatial domain** is the term used for the standard form of a digital object that represents the media product. For example, a gray-scale image is represented by a matrix whose entries are integers in [0, 255]. Watermarks are embedded by either altering the least significant bit (LSB) or adding a proper noisy pattern.
- **Frequency domain** is the term used for the object obtained after applying to the cover work discrete cosine, discrete Fourier, Hadamard, wavelet, or such other transformations. The message is embedded by altering the components of that transformed object, and then by applying the reverse transformation.

Detection metrics

The majority of watermarking systems proposed in the literature fall into the class of so called ***correlation-based watermarking systems***. Here is the list of the most used such detection metrics:

Linear correlation

$$lc(\mathbf{x},\mathbf{y}) = \frac{1}{N}\mathbf{x}\cdot\mathbf{y} = \frac{1}{N}\sum_{i=1}^{N} x_i y_i,$$

where N is the length of the vectors. Linear correlation method of detecting is optimal in the presence of additive, white Gaussian noise.

Normalized correlation.

$$nc(\mathbf{x},\mathbf{y}) = \frac{\mathbf{x}\cdot\mathbf{y}}{|\mathbf{x}|\cdot|\mathbf{y}|} = \frac{\sum_{i=1}^{N} x_i y_i}{\sqrt{\sum_{i=1}^{N} x_i^2}\sqrt{\sum_{i=1}^{N} y_i^2}}.$$

Correlation coefficient.

$$cc(\mathbf{x},\mathbf{y}) = \frac{\hat{\mathbf{x}}\cdot\hat{\mathbf{y}}}{|\hat{\mathbf{x}}|\cdot|\hat{\mathbf{y}}|} = \frac{\sum_{i=1}^{N} \hat{x}_i \hat{y}_i}{\sqrt{\sum_{i=1}^{N} \hat{x}_i^2}\sqrt{\sum_{i=1}^{N} \hat{y}_i^2}},$$

where $\hat{\mathbf{x}} = \mathbf{x} - E[\mathbf{x}]$ and $\hat{\mathbf{y}} = \mathbf{y} - E[\mathbf{y}]$.

Error control codes

Let $\mathbb{F} = GF(q)$ be a finite field of q elements. Any linear subspace C of dimension k of the n-dimensional vector space $\mathbb{F}^n$ is called a ***linear*** $[n,k]$ ***code***.

The ***Hamming weight*** of $\mathbf{v} \in \mathbb{F}$ is $\mathrm{wt}(\mathbf{v}) \stackrel{\text{def}}{=} |\{i \mid v_i \neq 0\}|$. The ***Hamming distance*** between $\mathbf{u}$ and $\mathbf{v}$ is

$$d(\mathbf{u},\mathbf{v}) \stackrel{\text{def}}{=} \mathrm{wt}(\mathbf{u}-\mathbf{v}) = |\{i \mid u_i \neq v_i\}|.$$

The smallest distance, $d(C)$, between two codewords of C is called ***minimum distance*** of the code.
A linear code of block length n, dimension k, and minimum distance d is refereed to as $[n,k,d]$ code.

Let a codeword $\mathbf{c} \in C$ is sent trough the channel. The received vector $\mathbf{v}$ can be considered as

$$\mathbf{v} = \mathbf{c} + \mathbf{e}.$$

If $\mathbf{e}$ is a nonzero vector with $\mathrm{wt}(\mathbf{e}) = w$ we say that w ***errors are occurred***.

Error control codes are used for detecting or correcting errors, or/and for correcting *erasures*. A position of the received vector $\mathbf{v}$, which is expected to be erroneously received is referred to as an ***erasure***.

Proposition 1 *Let C be a code over a finite field $\mathbb{F}$. The code C can simultaneously correct t errors and s erasures if and only if it has minimum distance $d(C) \geq 2t+s+1$.*

Hence, if the code is used only for correcting erasures it can restore the right values in up to $d(C)-1$ positions.

For more information about error control codes see [4].

AN ALGORITHM FOR EMBEDDING IN SPATIAL DOMAIN

Description of the algorithm

A-1. Let C be a binary $[n,k,d]$ linear code. Encode the source message into a binary sequence $\mathbf{m}$.

A-2. Starting with a given state of the random number generator generate r watermarks of size $a \times b$: $\mathbf{W} = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_r\}$.

A-3. Divide the cover work (in some way) into N blocks, $\mathbf{c}_1, \ldots, \mathbf{c}_N$, each of size $a \times b$.

A-4. (optional) Replace the set $\mathbf{W}$ by the set of patterns $\{\mathbf{h}_i\}$ which are orthogonal to all blocks $\mathbf{c}_1, \ldots, \mathbf{c}_N$. The vector $\mathbf{h}_i$ is constructed as a perpendicular from $\mathbf{w}_i$ on the space generated by all blocks $\mathbf{c}_j,\ j = 1, \ldots, N$.

A-5. In each block $\mathbf{c}_j,\ j = 1,2,\ldots,N$, embed r bits of the message sequence $\mathbf{m}$ by

$$\mathbf{c}_{jw} = \mathbf{c}_j + \alpha_j \left(\varepsilon_1 \mathbf{w}_1 + \varepsilon_2 \mathbf{w}_2 + \cdots + \varepsilon_r \mathbf{w}_r\right),$$

where $\varepsilon_i = \begin{cases} 1, & m_i = 1 \\ -1, & m_i = 0 \end{cases}$.

The scale constant α_j controls the tradeoff between visibility and robustness of the watermark.
Then make up the watermarked work gathering back all (now watermarked) blocks.

A-6. (optional) Add a noise pattern $\mathbf{n}_0$ to watermarked work, that is,

$$\mathbf{c}_{wn} = \mathbf{c}_w + \mathbf{n}_0.$$

A-7. The recipient divides $\mathbf{c}_{wn}$ into N blocks $\{\mathbf{c}_{jn}\}$ and knowing the reference patterns (or the key to generate them) calculate

$$l(\mathbf{c}_{jn}, \mathbf{w}_i),\ j = 1,2,\ldots,N,\ i = 1,\ldots,r,$$

where $l(,)$ is the chosen detection measure.

A-8. For a fixed in advance threshold τ set

$$\mathbf{m}_{\boldsymbol{ni}} = \begin{cases} 1, & \text{if} \quad l(\mathbf{c}_{wn}, \mathbf{w}_{ri}) > \tau \\ 0, & \text{if} \quad l(\mathbf{c}_{wn}, \mathbf{w}_{ri}) < -\tau \\ \text{an erasure}, & \text{if} \quad -\tau \leq l(\mathbf{c}_{wn}, \mathbf{w}_{ri}) \leq \tau \end{cases},$$

A-9. The error control code decoder corrects errors and erasures. Its output can be

- a decoded message (a sequence of bits);
- "there is no watermarking or hidden message";
- a decoded message with warning "errors are possible".

Normalize correlation and correlation coefficients are more robust to some transformation of the image like rotation and scaling. But $nc(\mathbf{c}_{jn}, \mathbf{w}_i)$ usually is very small that makes difficult to fix the threshold τ. To avoid this situation we recommend the following embedding to be used in this case:

A-5*

$$\mathbf{c}_{jw} = \mathbf{c}_j \cos\varphi + \varepsilon \frac{|\mathbf{c}_j|}{|\mathbf{h}_i|} \mathbf{h}_i \sin\varphi, \tag{1}$$

where $\varepsilon = +1$ or -1, when the embedded bit m_i is 1 or 0, respectively. The parameter φ controls the tradeoff between visibility and robustness of the watermark.

Since $\mathbf{c}_j$ and $\mathbf{h}_i$ are orthogonal and $|\mathbf{c}_{jw}| = |\mathbf{c}_j|$

$$nc(\mathbf{c}_{jw}, \mathbf{h}_i) = \frac{\varepsilon |\mathbf{c}_j||\mathbf{h}_i| \sin\varphi}{|\mathbf{c}_{jw}||\mathbf{h}_i|} = \varepsilon \sin\varphi.$$

The advantage of this embedding algorithm is that the expectation for $nc(\mathbf{c}_{jw}, \mathbf{h}_i)$ is fixed: $\sin\varphi$. On the contrary, in the case of a simple adding $\mathbf{h}_i$

$$nc(\mathbf{c}_j + \mathbf{h}_i, \mathbf{h}_i) = \frac{|\mathbf{h}_i|}{|\mathbf{c}_j + \mathbf{h}_i|} < \frac{|\mathbf{h}_i|}{|\mathbf{c}_j|} \ll \sin\varphi.$$

Therefore, using (1), we can choose a fixed and larger value for the threshold τ (usually $|\mathbf{c}_j|$ is about 10^4).

The reference patterns generation

Each of the watermark patterns $\mathbf{w}_j$ is obtained by generating an $a \times b$ matrix of real entries that are normal gaussian distributed or uniformly distributed on [0,1). Then the matrix is transform into a matrix with zero mean and variance 1. In our experiments good results are observed with watermarks which are a Kronecker product of matrices with uniformly and gaussian distributed entries. We also involved ***Hadamard matrices*** in the process of generation reference patterns.

Hadamard matrix is a square $m \times m$ matrix $\mathbf{H}_m$ whose entries are either +1 or -1 and

$$\mathbf{H}_m \mathbf{H}_m^{\tau} = m\mathbf{I}_m,$$

where $\mathbf{I}_m$ is the $m \times m$ identity matrix.

Hadamard matrices (normalized to variance 1) themselves are mathematically very suitable for reference patterns, but due to their regular structure the perceptibility of their adding is high. Nevertheless, the involving of Hadamard matrices is fruitful.

The following method demonstrate very good results in our experiments.

1. Generate a small block $\mathbf{v}$ with gaussian distribution of its entries.
2. Take the Kronecker product of an Hadamard matrix of a suitable size with $\mathbf{v}$: $\mathbf{w} = \mathbf{H}_m \otimes \mathbf{v}$.
3. Applied several times random permutations to rows and to columns of $\mathbf{w}$.

All above operations depend only on the pseudo-random generator. Hence the described procedure can be repeated many times giving the same patterns as the output if each time the initial state of generator is one and the same. Therefore this state can be used as a key.

a) b)

FIGURE 2. a) The original; b) The text "The house in Botswana where I will move in soon" is embedded

AN EXAMPLE

Both pictures, the original and the one with hidden message, presented in Figure 2 are in ".png" format with 256 pixels in width and 208 pixels in height. Each of the picture is determined by three 208×256 matrices (a matrix per color) whose entries are integers in [0, 255]. We divide each matrix associated with the original picture in $13 \cdot 16 = 208$ blocks of size 16×16. The obtained blocks are $3 \cdot 208 = 624$ in total. Thus, we can embed 624 bits with only one reference (noisy) pastern w.

Our text consists of 47 ASCII symbols, that is, each symbol is presented by 7 bits. We use a $[12,7,4]$ code C. Therefore, our text is encoded in $47 \cdot 12 = 564$ bits. We add 60 zeros and embed these 624 bits using only one reference pastern w according to A-5. The chosen constants $\alpha_j = 2$. The decoding procedure has been tested with $\tau = 0.5$ and $\tau = 0.3$.

CONCLUSIONS

We can summarize the contributions of our research as follows:

- A modified method of embedding that enlarges the payload of watermarking.
- A new method of embedding in the case of normalized correlation.
- The use of error control codes in erasure mode. This significantly increases the payload and robustness.
- A new method of generating the reference patterns.

ACKNOWLEDGMENTS

This work was partially supported by the Bulgarian National Science Fund under Contracts DO02-146/2008 and Supper CA^{++}.

REFERENCES

1. I.J. Cox *et al*, *Digital Watermarking and Steganography*, Morgan Kaufmann Publ., 2008.
2. R. Grandal, "Some notes on stegsnography", avilable at `http://os.inf.tu-dresden.de/~westfeld/crandall.pdf`.
3. H. Li, G. Liu, Y. Dai, and Z.Wang (2010) "Secure Multimedia Distribution Based on Watermarking and Encryption", *Journal of Convergence Information Technology* **5**(9), 279–286.
4. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.

5. P. Moulin and R. Koetter (2005) “Data-hiding codes”, *Proceedings of IEEE* **93**, 2083–2126.
6. F.M.J. Willems and M. van Dijk (2005) “Capacity and codes for embedding information in grayscale signals”, *IEEE Trans. on Inf. Theory*, **51**(3) 1209–1214.