Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 204–210*

Application of Error Control codes in Steganography [1]

Hristo Kostadinov hristo@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
Nikolai L. Manev nlmanev@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, and
University of Structural Engineering & Architecture

Abstract. In this paper we describe two methods of applying error control codes to steganography.

1 Introduction

Steganography and digital watermarking are concerned with embedding information in digital media such as images, audio signals and video. The purpose of steganographic techniques is to alter the cover digital object in undetectable manner, that is, no one but the intended recipient to be able to detect the altering of the cover work. Both steganography and digital watermarking are subject of a strong interest and research activity especially in the last decades. 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], [5],

The application of error correcting codes to steganography and watermarking started with so called matrix embedding introduced by Grandall [3]. Since that time it has been popularized, developed, and carefully analyzed by many authors. Here are a few of them: [9], [10], [11].

In this paper we discuss two methods of information embedding in spatial domain: the aforesaid matrix embedding by q-ary codes and a method based on pseudo-noise patterns that explodes the erasure capability of error correcting codes.

2 Preliminaries

The process of hiding information can be described in general as a mapping (***embedding process***)

[1]This research is partially supported by ...

$$\mathcal{E}: \left| \begin{array}{lcl} (\mathfrak{P}, \mathfrak{T}, \mathfrak{K}) & \rightarrow & \mathfrak{P} \\ (\mathbf{c}_0, \mathbf{m}, \mathbf{k}) & \rightarrow & \mathbf{c}_m = \mathcal{E}(\mathbf{c}_0, \mathbf{m}, \mathbf{k}) \end{array} \right. ,$$

where $\mathbf{c}_0$, the *cover object*, is an element of the set $\mathfrak{P}$ of possible digital objects (e.g., images), $\mathbf{m} \in \mathfrak{T}$ is the message intended for embedding, and $\mathbf{k}$ is a key randomly taken from the space of keys $\mathfrak{K}$.

Respectively, the process of revealing the hidden text consists of applying a ***decision function*** (which is based on the chosen ***detection metric***) to the received eventually distorted copy $\mathbf{c}_{mn}$ of the sent work $\mathbf{c}_m$:

$$\mathbf{m}' = \mathcal{D}(\mathbf{c}_{mn}), \qquad \text{or} \quad \mathbf{m}' = \mathcal{D}(\mathbf{c}_{mn}, \mathbf{c}_0), \quad \text{if } \mathcal{D} \text{ needs the original.}$$

In many cases the distortion can be considered as an additive noise $\mathbf{n}$, i.e, $\mathbf{c}_{mn} = \mathbf{c}_m + \mathbf{n}$. Very often in practice $\mathbf{c}_{mn} = \mathbf{c}_m$.

In the described considerations and experiments the embedding process is a composition of two mappings. The first one, $\mathcal{M}$, transforms the cover image into a matrix over Z_q, the ring of integers modulo q, or into the finite field $GF(q)$ of q elements. We shall denote the set of such matrices by $\mathfrak{M}$, that is,

$$\mathcal{M}: \ (\mathfrak{P}, \mathfrak{T}, \mathfrak{K}) \ \rightarrow \ \mathfrak{M}.$$

The transformation $\mathcal{M}$ depends on the cover object and the chosen key. After careful analysis of the image some pixels are market as "wet" pixels which are not used. The order of the embedding into the rest ("dry") pixels is also determined according to the chosen key. The second transformation realizes the embedding algorithm based on the use of error control codes. Usually it is referred to as ***embedding function*** and we shall keep the notation $\mathcal{E}()$ for it.

Herein we discuss two methods of concealing data into images and both are realized by embedding into the spatial domain: A) the aforesaid syndrome (matrix) embedding using q-ary codes, and B) a method based on pseudo-noise patterns.

A. Syndrome Embedding

Syndrome embedding (also known as matrix embedding) is a method in which the parties agree on a parity-check matrix $\mathbf{H}$ of a linear code and the secrete message is extracted as a sequence of syndromes (with respect to $\mathbf{H}$) from the cover digital object. With a few exceptions ([10], [8]) the codes used in the proposed algorithms are mainly binary codes, e.g., BCH, Reed-Solomon, random codes, etc.. In these case $\mathcal{M}$ transform the digital object which is in fact a matrix of 8, 16, or 12 (for CD audio) bits long unsigned integers (i.e., elements of $\mathbb{Z}_{2^b}, b = 8, 12, 16$) into a binary matrix $\mathbf{D}$. All these algorithms are based on looking among the elements of a given coset for a vector that minimize distortion in the image. The covering radius of the code is also very important characteristic. More detailed description of this method in the form used by us is given in Section 3.

B. Noise patterns embedding

In most general form this embedding algorithm can be described as

$$\mathbf{c}_m = \mathcal{E}(\mathbf{c}_0, \mathbf{m}) = \mathbf{c}_0 + \alpha \mathbf{w}_m, \tag{1}$$

where $\mathbf{w}_m$ called ***message pattern*** is a function of the message and the set of predefined reference patterns (and eventually of $\mathbf{c}_0$). The scale constant α controls the tradeoff between visibility and robustness of the embedded data. The set of predefined reference patterns $\mathbf{W} = \{\mathbf{w}_{r1}, \mathbf{w}_{r2}, \ldots, \mathbf{w}_{rk}\}$ consists of matrices whose entries have a given probability distribution, most often normal or uniform distribution. These patterns are pair-wise orthonormal according to the chosen detection metric $\delta(\ ,\ ) : \mathfrak{M} \times \mathfrak{M} \to \mathbb{R}$. In fact it is enough $\delta(\mathbf{w}_{ri}, \mathbf{w}_{rj})$ to be relatively small, not necessarily exact zero.

Assume that the message is a binary vector $\mathbf{m} = (m_1, m_2, \ldots, m_k)$. Then

$$\mathbf{w}_m = \gamma\left(\epsilon_1 \mathbf{w}_{r1} + \epsilon_2 \mathbf{w}_{r2} + \cdots + \epsilon_k \mathbf{w}_{rk}\right), \text{ where } \epsilon_i = \begin{cases} 1, & m_i = 1 \\ -1, & m_i = 0 \end{cases}.$$

The coefficient γ, when it differs from 1 is used for a kind of normalization of $\mathbf{w}_m$, for example, $\gamma = \frac{1}{\sqrt{k}}$ normalizes the variance to 1.

The process of revealing message is also based on the detection metric. For $i = 1, 2, \ldots, k$ the receiver calculates $\delta(\mathbf{c}_{mn}, \mathbf{w}_{ri})$ and according to the sign of its value decides what is the i-th bit m_i. Here are the most used detection metrics:

- ***Linear correlation***: $lc(\mathbf{x}, \mathbf{y}) = \frac{1}{N}\,\mathbf{x} \cdot \mathbf{y} = \frac{1}{N}\sum_{i=1}^{N} x_i y_i,$
- ***Normalized correlation***: $nc(\mathbf{x}, \mathbf{y}) = \frac{\mathbf{x} \cdot \mathbf{y}}{|\mathbf{x}| \cdot |\mathbf{y}|}.$
- ***correlation coefficient***: $cc(\mathbf{x}, \mathbf{y}) = \frac{\hat{\mathbf{x}} \cdot \hat{\mathbf{y}}}{|\hat{\mathbf{x}}| \cdot |\hat{\mathbf{y}}|}$, $\hat{\mathbf{x}} = \mathbf{x} - \mathrm{E}[\mathbf{x}]$, $\hat{\mathbf{y}} = \mathbf{y} - \mathrm{E}[\mathbf{y}]$

3 Syndrome embedding and q-ary codes

In this section we describe in short our approach to syndrome embedding underling the differences with the usual one. Assume $\mathbf{c}_0$ is a matrix of elements of $\mathbb{Z}_{256}$. We will skip descriptions of $\mathcal{M}$ in concern of the use of the key and determination of the "dry" pixels, and will consider only the part that concerns embedding function. The aforesaid feature of $\mathcal{M}$ are implemented in the developed software, but in most of experiments we skip $\mathcal{M}$ and realize only what follows. For information about the case when "wet" pixels are involved in the syndrome embedding algorithm can be found in [6].

Let q' be an integer less than 255. Consider $\mathbf{D}' = \mathbf{c}_0 \pmod{q'}$. This is the target matrix of the embedding. If q' is a power of 2 the action is equivalent to embedding in the several less significant bits. In this case binary codes can also be used.

Algorithm:

Let $\mathbf{H}$ be a $r \times n$ parity-check matrix of a linear code over $\mathbb{Z}_q$, or a finite field $\mathbb{F}_q$ of $q \le q'$ elements. Let $\mathbf{D}$ be a $n \times N$ matrix over $\mathbb{F}_q$ or $\mathbb{Z}_q$ obtained from the target image by the transformation $\mathcal{M}$. Let the message (randomized and eventually encrypted) be also transformed into a $r \times N$ matrix $\mathbf{m}$ over $\mathbb{F}_q$.

1. Compute $\mathbf{S} = \mathbf{m} - \mathbf{HD}$, i.e., $\mathbf{m} = \mathbf{S} + \mathbf{HD}$
2. Find $n \times N$ matrix $\mathbf{E}$ such that $\mathbf{S} = \mathbf{HE}$
3. Compute $\mathbf{V} = \mathbf{D} + \mathbf{E}$
4. Construct an image $\mathbf{c}_m$ such that $\mathcal{M}(\mathbf{c}_m, \mathbf{k}) = \mathbf{V}$ and send $\mathbf{c}_m$.

The receiver

1. Determines $\mathbf{V} = \mathcal{M}(\mathbf{c}_w, \mathbf{k})$
2. computes $\mathbf{HV} = \mathbf{HD} + \mathbf{HE} = \mathbf{HD} + \mathbf{S} = \mathbf{m}$

Embedding efficiency in the case of syndrome encoding using a code with $r \times n$ parity check matrix is

$$E_f = \frac{r \log_2 q'}{n} \quad \text{bits/pixel}$$

Note that the embedding efficiency does not depend on which field (ring) the code is defined over. The number of its elements is usually $q = q'$, but it can be in partial $q = 2$ when q' is a power of 2.

We apply codes over $\mathbb{Z}_q$ that correct errors of type $\pm e$ for small integer e. The authors have used such codes for coded modulation [7]. These codes have simple decoding algorithms. Soft decoding (trellis) can also be applied to them. Our approach simplifies the process of determining the matrix $\mathbf{E}$. The representative of the coset that corresponds to a given syndrome is chosen to be with the minimum Lee weight and its entries to be with minimum absolute value. For example, between the $\mathbb{Z}_4$-vectors $(0, 3, 3)$ and $(2, 0, 0)$ the first vector is preferable ($3 = -1$ in $\mathbb{Z}_4$).

4 Pseudo-noise patterns and erasure codes

4.1 Algorithm

Embedding

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

A-2. Starting with a given state (used as password) of the random number generator generate t reference patterns of size $a \times b$: $\mathbf{W} = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_t\}$.

A-3. Divide (in some way) the cover work 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 $\mathbf{c}_1, \ldots, \mathbf{c}_N$.

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

$$\mathbf{c}_{jw} = \mathbf{c}_j + \frac{\alpha_j}{\sqrt{t}} \left(\epsilon_1 \mathbf{w}_1 + \epsilon_2 \mathbf{w}_2 + \cdots + \epsilon_t \mathbf{w}_t\right), \text{ where } \epsilon_i = \begin{cases} 1, & m_{ji} = 1 \\ -1, & m_{ji} = 0 \end{cases}.$$

The scale constant α_j controls the trade-off between visibility and robustness of the hiding data.

Embedding efficiency in this case is $E_f = \dfrac{(n-r)tN}{nab}$ bits/pixel.

Detection and Decoding

A-6. The recipient divides the received image into N blocks $\{\tilde{\mathbf{c}}_j\}$ and knowing the reference patterns (or the key to generate them) calculates

$$\delta(\tilde{\mathbf{c}}_j, \mathbf{w}_i) = \delta(\mathbf{c}_j, \mathbf{w}_i) + \frac{\alpha_j}{\sqrt{t}}\delta(\mathbf{w}_i, \mathbf{w}_i)\,\epsilon_i,\ \ j = 1, 2, \ldots, N,\ \ i = 1, \ldots, t,$$

where $\delta(,)$ is the chosen detection measure. (Indeed $\tilde{\mathbf{c}}_j$ are noise versions of $\mathbf{c}_{jw}$) Then recover the message:

$$\tilde{\mathbf{m}}_{ji} = \begin{cases} 1, & \text{if} \quad \delta(\tilde{\mathbf{c}}_j, \mathbf{w}_i) > \tau \\ 0, & \text{if} \quad \delta(\tilde{\mathbf{c}}_j, \mathbf{w}_i) < -\tau \\ \text{an erasure} & \text{if} \quad -\tau \le \delta(\tilde{\mathbf{c}}_j, \mathbf{w}_i) \le \tau \end{cases},$$

A-7. The error control code decoder corrects errors and erasures. Its output can be

- "there is no watermarking or hidden message", when the number of erasures is $> N/2$;
- a decoded message (a sequence of bits);
- a decoded message with warning "errors are possible".

We introduced also a new non-additive embedding:

$$\mathbf{c}_{jw} = \mathbf{c}_j \cos\varphi + \epsilon\frac{|\mathbf{c}_j|}{|\mathbf{h}_i|}\mathbf{h}_i \sin\varphi, \tag{2}$$

where $\epsilon = +1$ or -1, when the embedded bit m_i is 1 or 0, respectively. The parameter φ controls the trade-off between visibility and robustness of embedding. This embedding gives the best results if it is applied with normalized correlation as detection measure.

4.2 Error analysis

The expected value of $\delta(,)$ is $\mu_1 = \mu = \frac{\alpha}{\sqrt{t}}$, when $m_i = 1$, and $\mu_0 = -\mu = -\frac{\alpha}{\sqrt{t}}$, when $m_i = 0$ is embedded, respectively (see A-5 and A-6). Let us assume that $\delta(,)$ is normal distributed. Then the variance is $\sigma^2 = \sigma^2_{\boldsymbol{w}_i}(\sigma^2_{\boldsymbol{c}} + \sigma^2_{\boldsymbol{n}})$, where $\sigma^2_{\boldsymbol{w}_i} = 1$, and $\sigma^2_{\boldsymbol{c}}$ and $\sigma^2_{\boldsymbol{n}}$ are the variance of the cover work and the channel noise, respectively. Usually $\sigma^2_{\boldsymbol{c}} \approx (60/255)^2$. Let $p_c,\ p_{er}$ and p_{es} be the probability of correct detection, of error, and of an erasure, respectively. Then in both cases, when $m_i = 1$ and $m_i = 0$ is embedded:

$$p_c = \frac{1}{2}\operatorname{erfc}\left(\frac{\tau - \mu}{\sigma\sqrt{2}}\right); \qquad p_{er} = \frac{1}{2}\operatorname{erfc}\left(\frac{\tau + \mu}{\sigma\sqrt{2}}\right); \qquad p_{es} = 1 - p_c - p_{er}$$

The probability of **a false positive decision** ($\mu = 0$) is given by

$$P_{fp} = \sum_{i=0}^{\lfloor \frac{N}{2} \rfloor} \binom{N}{i} p^{N-i}(1-p)^i, \text{ where } p = \operatorname{erfc}\left(\frac{\tau}{\sigma\sqrt{2}}\right) \tag{3}$$

The embedded n bits can be correctly decoded with a probability

$$P_{corr} = P_1 + P_2 + P_3, \qquad \text{where}$$

$$P_1 = \sum_{s=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{s} p_{es}^s \left(\sum_{t=0}^{\lfloor \frac{d-1-s}{2} \rfloor} \binom{n-s}{t} p_{er}^t p_c^{n-t-s} \right),$$

$$P_2 = \sum_{s=\lfloor \frac{d-1-s}{2} \rfloor + 1}^{d-1} \binom{n}{s} p_c^{n-s} p_{es}^s, \qquad P_3 = \sum_{s=d}^{n} \binom{n}{s} p_c^{n-s}(q-p_c)^s,$$

where d is the minimum distance of the code and $q = \frac{1}{2}\operatorname{erfc}\left(\frac{-\mu}{\sigma\sqrt{2}}\right)$ (this is p_c with $\tau = 0$) is the probability of positive (resp. negative) value of $\delta(\tilde{\mathbf{c}}_{wn}, \mathbf{w}_i)$.

If more than $N/2$ erasures are marked for a given watermark pattern $\mathbf{w}_i$ then the detector outputs "there is no watermark", that is, it makes **false negative decision**. The probability, P_{fn}, for such an output is given by

$$P_{fn} = \sum_{i=0}^{\lfloor \frac{N}{2} \rfloor} \binom{N}{i} p_{es}^{N-i}(1-p_{es})^i. \tag{4}$$

5 Experiments and conclusions

We have made numerous experiments with picture from several galleries (with grey-scale and color images) and many error control codes for both type of algorithms. Also, we have tested the cover images with the available in the internet software for stego-analysis. Although the channel is assumed noiseless and detection blind (i. e., the receiver and the opponent don't have the original), we have compered the results of stego-analysis on both original and cover objects.

Our observations show that q-ary codes are good choice in the case of syndrome embedding. For both algorithms it is better to use not very long codes with simple decoding and leave security issues to $\mathcal{M}$.

References

[1] I.J. Cox et al., *Digital Watermarking and Steganography*, Morgan Kaufmann Publ., 2008.

[2] F. Galand and G. Kabatiansky, Information hiding by coverings, in *Proc. IEEE Inf. Theory Workshop, 2003*, 151–154.

[3] R. Grandal, Some notes on stegsnography, avilable from http://os.inf.tu-dresden.de/ westfeld/crandall.pdf

[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, Data-hiding codes, *Proceedings of IEEE,* **93**, 2083–2126, 2005.

[6] C. Munuera, and M. Barbier, Wet paper codes and the dual distance in steganography, *Advances in Mathematics of Communications* **6**, 1,

[7] H. Kostadinov, H. Morita, N. Manev, Integer codes correcting single errors of specific types $(\pm e1, \pm e2, \ldots, \pm es)$, *IEICE Trans. Fundamentals*, **E86-A**, (7), 1843–1849, 2003.

[8] H. Rifa, J. Rifa, and L. Ronquillo, Perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes in steganography, *Adv. Math. Commun.*, **5**, (3), 425–433, 2011.

[9] A. Westfeld, High capacity despite better steganalysis (F5 - A steganographic algorithm), *Lecture Notes in Computer Science*, **2137**, Springer-Verlag, 289–302, 2001.

[10] F. M. J. Willems and M. van Dijk, Capacity and codes for embedding information in grayscale signals, *IEEE Trans. on Inf. Theory*, **51**, (3), 1209–1214, March 2005.

[11] W. Zhang, X. Zhang, Sh. Wang, Near-optimal codes for information embedding in gray-scale signals, *IEEE Trans. on Inf. Theory*, vol. 56, (3), 1262–1270, March 2010.