STEGANOGRAPHIC CAPACITY OF LOCALLY UNIFORM MARKOV COVERS

Valeriy Voloshko
Research Institute for Applied Problems of Mathematics and Informatics
Minsk, BELARUS
e-mail: ValeraVoloshko@yandex.ru

Abstract

Proposed a new correction algorithm for the standard steganographic model of binary message embedding into binary cover. Embedding is known to be influential on cover's statistical characteristics and, thus, to be statistically detectable. The proposed correction algorithm does not affects the embedded message and under certain model assumptions restores the cover's histogram of n-subwords frequencies. The key condition for the n-subwords histogram restorability limits the ratio of message to cover: it should not exceed some value called n-capacity of cover. Some capacities found theoretically for locally uniform Markov covers.

Keywords: steganographic capacity, histogram correction, embedding

1 Introduction

Such tools for multimedia copyright protection, as digital watermarking or digital signature, use steganographic methods of covert embedding. The standard embedding model is very simple [1, 2]. We have three binary sequences of $\{0,1\}$ values: *cover* $\mathbf{c} = (\mathbf{c}_i)_{i=1}^N$, *selector* $\mathbf{s} = (\mathbf{s}_i)_{i=1}^N$ and *message* $\mathbf{m} = (\mathbf{m}_i)_{i=1}^{N_1}$, where N_1 is the number of ones in selector $\mathbf{s}$. Cover values $\mathbf{c}_i$ corresponding to N_1-subset of indices $\{i : \mathbf{s}_i = 1\}$ are then being replaced with N_1 message values. Cover sequence $\mathbf{c}$ with embedded message $\mathbf{m}$ we call *stego* and denote $\mathbf{c}^* = (\mathbf{c}_i^*)_{i=1}^N$. After message embedding we may want to correct stego $\mathbf{c}^*$ for some goal. Of course, correction should not affect the embedded message values $\{\mathbf{c}_i^* : \mathbf{s}_i = 1\}$. Corrected stego sequence we denote $\mathbf{c}^{**} = (\mathbf{c}_i^{**})_{i=1}^N$.

The goal of correction is usually to somehow restore certain features of cover $\mathbf{c}$, distorted by message embedding. Obviously, we are not talking about restoration of the cover $\mathbf{c}$ itself, because stego $\mathbf{c}^*$ can not even be moved closer to it in Hamming metric d by correction:

$$d(\mathbf{c}, \mathbf{c}^*) \leq d(\mathbf{c}, \mathbf{c}^{**}).$$

Nevertheless, the cover's statistical characteristics turn quite repairable. Here we aim to approximately restore the histogram of frequencies of cover's n-subwords:

$$\|\mathbf{H}_n(\mathbf{c}) - \mathbf{H}_n(\mathbf{c}^{**})\| \to \min, \tag{1}$$

where

$$\mathbf{H}_n(x) ::= \left(\frac{\#\{0 \leq i \leq N-n : (x_{i+1}, \dots, x_{i+n}) = q\}}{N+1-n} \right)_{q \in \{0,1\}^n}, \ x \in \{0,1\}^N. \tag{2}$$

In its formulation the problem (1) looks rather combinatorial, but it appears to be effectively treatable by probabilistic and statistical methods based on few model assumptions. The following probabilistic model assumptions are used to be standard in literature [1, 2]:

A1: cover $\mathbf{c}$, selector $\mathbf{s}$ and message $\mathbf{m}$ are mutually independent random binary sequences;

A2: selector $\mathbf{s}$ is a Bernoulli process with success probability $0 < \varepsilon < 1$;

A3: message $\mathbf{m}$ is a uniformly distributed sequence (Bernoulli process with parity of successes and failures);

A4: cover $\mathbf{c}$ is a Markov chain.

Based on [1], we use extended versions of **A2** and **A4**:

XA2: selector $\mathbf{s}$ is a stationary n-ergodic process;

XA4: cover $\mathbf{c}$ is a stationary n-ergodic process.

Remark. Compared to **XA4**, extension **XA2** is more exotic and analytically harder to work with, but it may sufficiently increase the capacity of stegosystem [1].

Remark. Under ergodicity we mean almost sure convergence of frequencies to probabilities. Namely, let $x : \mathbb{Z} \to \{0,1\}$ be a stationary random binary process. Then we call it n-ergodic, if in (2):

$$\mathbf{H}_n(x) \xrightarrow[N\to+\infty]{\text{a.s.}} [x]^n = \left([x]^n_q\right)_{q\in\{0,1\}^n}, \; [x]^n_q ::= \mathbb{P}\{(x_1,\dots,x_n) = q\}. \tag{3}$$

Remark. We call $[x]^n$ in (3) an *n-projection* of x's probability measure $[x] ::= [x]^\infty$.

Thus the distance (1) between histograms almost surely vanishes at $N \to +\infty$, if the following two conditions hold for cover $\mathbf{c}$ and corrected stego $\mathbf{c}^{**}$:

- they are both n-ergodic;
- they have the same n-projections of probability measures: $[\mathbf{c}]^n = [\mathbf{c}^{**}]^n$.

The correction algorithm proposed in [1] provide these conditions.

Remark. Under n-ergodicity the restoration of n-projection $[\mathbf{c}]^n$ of cover's measure guarantees the asymptotic restoration of cover's n-subwords histogram $\mathbf{H}_n(\mathbf{c})$. So further under histogram restoration we understand the asymptotic one.

2 Correction algorithm

Thus the embedding leads to deformation of the cover's probability measure $[\mathbf{c}]$, and we want to restore it (at least up to probabilities of n-subwords) by correction. It is shown in [1] that under assumptions **A1**, **XA2**, **A3** and **XA4** the considered deformation of $[\mathbf{c}]$ turns out to be a convolution with the specially transformed selector's measure. Namely, with the measure $[\mathbf{su}]$ of selector $\mathbf{s}$ multiplied by independent from it uniformly distributed random binary sequence $\mathbf{u}$ (in the standard **A2** case $[\mathbf{su}]$ is Bernoulli measure with success probability $\varepsilon/2$). So the idea of correction algorithm is clear now: we just have to replace cover $\mathbf{c}$ with another stationary n-ergodic random binary sequence $\mathbf{k}$ (let us call it *corrector*), whose measure (n-projection, to be precise) $[\mathbf{k}]^n$ convoluted with $[\mathbf{su}]^n$ gives n-projection $[\mathbf{c}]^n$ of the cover's measure.

From the computational point of view, we need an inverse convolution. To obtain it, one may use Fourier transform $\mathbf{F}$, which provides correspondence between convolution and multiplication. Without going into technical details, the object of our interest, n-projection $[\mathbf{k}]^n$ of the corrector's measure, has the form [1]:

$$[\mathbf{k}]^n = 2^{-n}\mathbf{F}\left(\frac{\mathbf{F}[\mathbf{c}]^n}{\mathbf{F}[\mathbf{su}]^n}\right),\ (\mathbf{F}f)_q = \sum_{q' \in \{0,1\}^n} f_{q'}(-1)^{|qq'|},\ q \in \{0,1\}^n, \tag{4}$$

reducing in the standard **A2** case to:

$$[\mathbf{k}]^n_q = \left(\frac{1-\varepsilon/2}{1-\varepsilon}\right)^n \sum_{q' \in \{0,1\}^n} [\mathbf{c}]^n_{q\oplus q'} \left(\frac{\varepsilon}{\varepsilon-2}\right)^{|q'|},\ q \in \{0,1\}^n, \tag{5}$$

where $|q'|$ means Hamming weight of q' and $\oplus$ means elementwise XOR. The uniqueness of $[\mathbf{k}]^n$ is guaranteed by strict positiveness of $[\mathbf{s}]^n$ (every binary n-word $q \in \{0,1\}^n$ has nonzero probability to appear as a subword in selector $\mathbf{s}$, holds for **A2**). The existence of n-ergodic corrector itself is guaranteed by strict positiveness of $[\mathbf{k}]^n$ in (4) (or (5) for **A2**). The last thing we should say about the algorithm is that we have to use histogram $\mathbf{H}_n(\mathbf{c})$ instead of n-projection $[\mathbf{c}]^n$, which is unknown on practice.

Thus the correction algorithm is of the form:

step 1: compute cover's histogram of n-subwords frequencies $\mathbf{H}_n(\mathbf{c})$;

step 2: using $\mathbf{H}_n(\mathbf{c})$ instead of $[\mathbf{c}]^n$ in (4) (or (5) for **A2**), compute n-projection $[\mathbf{k}]^n$ of the corrector's measure;

step 3: generate the corrector $\mathbf{k}$ by pseudorandom stationary Markov chain of order $n-1$ with transfer probabilities, providing computed $[\mathbf{k}]^n$, or state the fail of correction, if $[\mathbf{k}]^n$ is not strictly positive;

step 4: correct the values of stego $\mathbf{c}^*$: replace $\mathbf{c}^*_i$ with $\mathbf{k}_i$ at the positions i, not occupied by message ($\mathbf{s}_i = 0$).

3 Capacity of cover

The assumption **XA2** means, in particular, that the portion of ones N_1/N in selector $\mathbf{s}$ almost surely tends to $[\mathbf{s}]_1 = \mathbb{P}\{\mathbf{s}_i = 1\}$ when the cover's volume N grows. For this reason under **XA2** the value $[\mathbf{s}]_1$ can be thought of as a data transfer rate (DTR for brevity) of stegosystem. Maximization of DTR seems rather natural objective, next after cover's histogram restoration. Hence the idea of capacity [1, 3] as a steganographic characteristic of cover. Informally, capacity is a maximum achievable DTR among stegosystems providing histogram restorability for some particular cover. More precisely, in considered model capacity characterizes cover's distribution $[\mathbf{c}]$.

Following [1], consider two cases. If selector $\mathbf{s}$ is an arbitrary one (**XA2** case), providing restoration of cover's n-subwords histogram, then maximum DTR is called *absolute n-capacity* of cover's measure $[\mathbf{c}]$ and denoted by $\varepsilon_n^*[\mathbf{c}]$. And it is called *plain n-capacity* and denoted by $\varepsilon_n[\mathbf{c}]$, if selector is chosen among Bernoulli processes (**A2** case). Obviously, both absolute and plain capacities of a fixed cover's probability measure $[\mathbf{c}]$ do not increase in n and $\varepsilon_n[\mathbf{c}] \leq \varepsilon_n^*[\mathbf{c}]$.

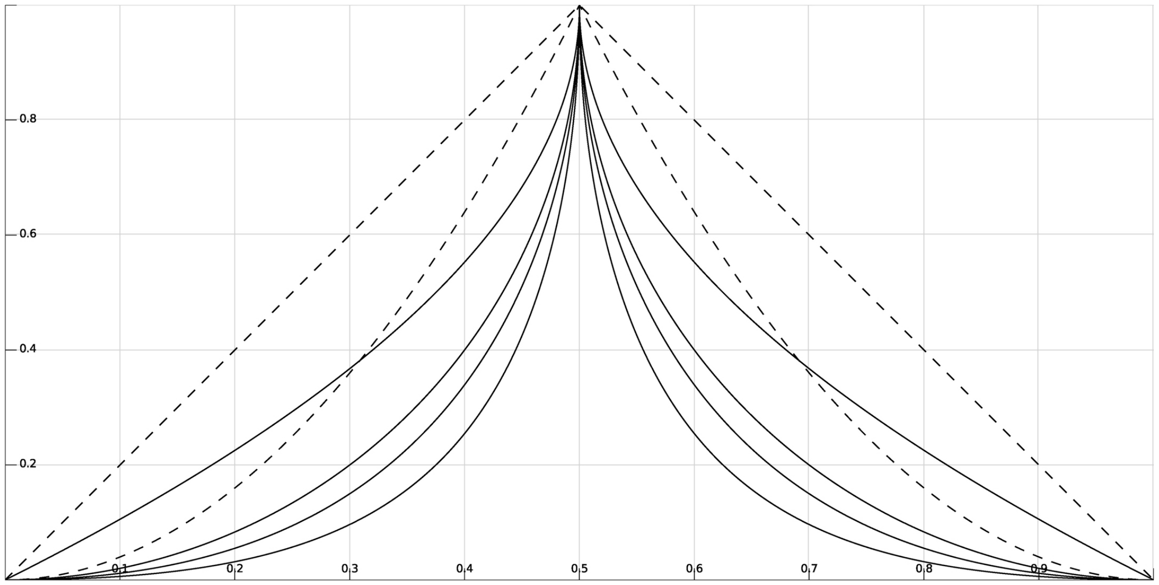

Figure 1: Capacities of $\mathrm{MC}_{\mathrm{U}}^1(p)$ against p: plain $\varepsilon_2 > \varepsilon_3 > \varepsilon_4 > \varepsilon_\infty$ (solid lines) and absolute $\varepsilon_2^* > \varepsilon_3^*$ (dashed lines).

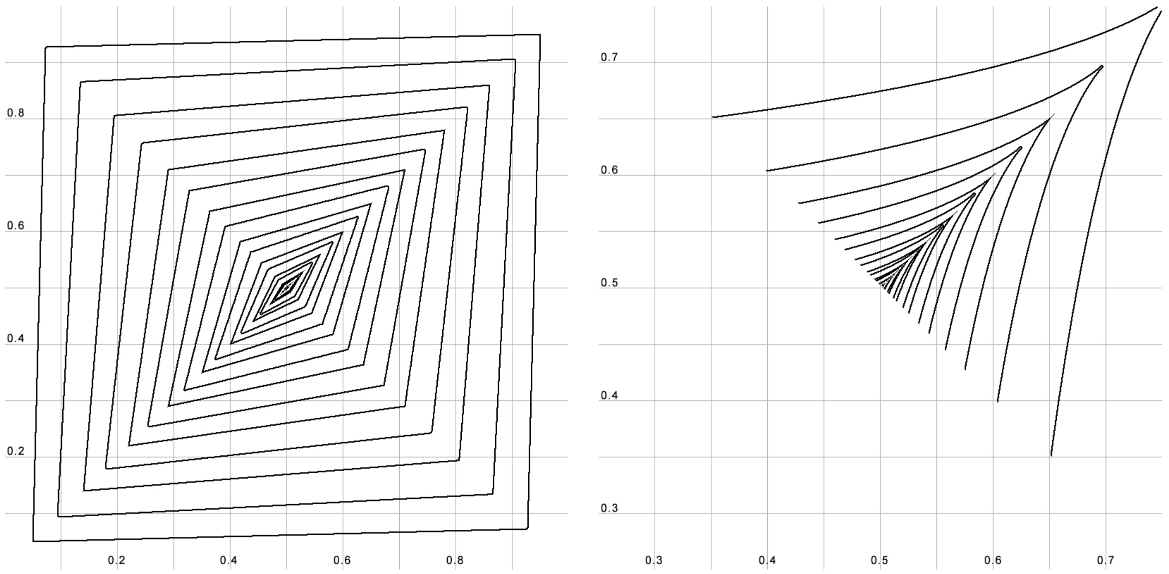

Figure 2: Contour maps for plain capacities of $\mathrm{MC}_{\mathrm{U}}^2(p, s)$ on the (p, s) plane: ε_3 on the left and ε_∞ (only for $p + s > 1$) on the right. Lines correspond to multiples of 0.05.

Consider now two Markov models of locally uniform covers: the first order Markov chain with uniformly distributed 1-subwords and the second order one with uniformly distributed 2-subwords. We call them $\mathrm{MC}_{\mathrm{U}}^{1}$ and $\mathrm{MC}_{\mathrm{U}}^{2}$ respectively. The first one appears one-parametric with parameter:

$$p = \mathbb{P}\{0 \to 1\} = \mathbb{P}\{1 \to 0\}.$$

The second one is two-parametric with parameters:

$$\begin{aligned} p &= \mathbb{P}\{00 \to 1\} = \mathbb{P}\{10 \to 0\}, \\ s &= \mathbb{P}\{11 \to 0\} = \mathbb{P}\{01 \to 1\}. \end{aligned}$$

The arrows mean transfers within the cover's sequence $\mathbf{c}_i$.

Theorem 1. *[1] Absolute and plain capacities of* $\mathrm{MC}_{\mathrm{U}}^{1}(p)$*-distributed cover are:*

$$\varepsilon_2^* = 2\hbar, \ \varepsilon_3^* = 4\hbar^2,$$

$$\varepsilon_2 = 1 - \sqrt{1-2\hbar}, \ \varepsilon_3 = 1 - \sqrt{1-4\hbar^2}, \ \varepsilon_4 = 1 - \sqrt{\kappa+\kappa^2-\kappa^3}, \ \varepsilon_\infty = 1 - \frac{\sqrt{1-2\hbar}}{1-\hbar},$$

where $\hbar = \min\{p, 1-p\}$, $\kappa = \hbar + \sqrt{1+\hbar^2}$.

Theorem 2. *Third and limiting (for* $p+s > 1$*) plain capacities of* $\mathrm{MC}_{\mathrm{U}}^{2}(p,s)$*-distributed cover are:*

$$\varepsilon_3 = \begin{cases} 1 - \sum_{\pm} \sqrt[3]{\hbar_- \pm \sqrt{\hbar_-^2 - \hbar_+^3}}, & \hbar_-^2 \geq \hbar_+^3, \\ 1 - 2\sqrt{\hbar_+} T_{\frac{1}{3}}(\hbar_- \hbar_+^{-\frac{3}{2}}), & \hbar_-^2 < \hbar_+^3, \end{cases}, \ \varepsilon_\infty = 1 - \frac{\sinh^3\Phi - \tanh^3\Psi}{\sinh^2\Phi - \tanh^2\Psi} \cdot \frac{1}{\cosh\Phi},$$

where $\hbar_+ = \frac{1}{3}|1-p-s|$, $\hbar_- = \frac{1}{2}|p-s|$, $T_\nu(x) = \cos(\nu \arccos x)$ *is a fractional analogue of Chebyshev polynomial,*

$$\Psi = \operatorname{arcsinh} \sqrt[3]{\frac{|p-s|}{p+s-2ps}}, \ \Phi = \operatorname{arccosh}\left(\frac{p+s-2ps}{(1-p)(1-s)} \cdot \frac{7+\cosh(4\Psi)}{16\cosh\Psi}\right).$$

Remark. Both limiting plain capacities ε_∞ for the considered cover models were obtained based on some unproven hypotheses, confirmed by numerical experiments.

Remark. Comparison of absolute and plain capacities (Figure 1) shows that more sophisticated choice of positions for embedding may sufficiently increase the data transfer rate of stegosystem.

References

[1] Voloshko V.A. (2016). Steganographic Capacity for One-dimensional Markov Cover. *Diskretnaya Matematika*. Vol. **28**(1), pp. 19–43 (in Russian).

[2] Kharin Yu.S., Vecherko E.V. (2016). Detection of Embeddings in Binary Markov Chains. *Discrete Mathematics and Applications*. Vol. **26**(1), pp. 13–29.

[3] Harmsen J.J., Pearlman W.A. (2009). Capacity of Steganographic Channels. *IEEE Transactions on Information Theory*. Vol. **55**, pp. 1775–1792.