Data Embedding Based on Linear Hash Functions

Boris Ryabko
Andrey Fionov
Institute of Computational Technologies of SB RAS
Novosibirsk state university
Novosibirsk

Introduction-What is steganography?

The classical problem of steganography is transmitting messages so that the *very fact of transmission be concealed* from any observer.

To achieve this goal, the messages are embedded in various innocuous objects (digital photos, audio, video, etc.), called cover objects or covertexts, whose transmission cannot raise any suspicion.

The observer who examines transmitted objects tries to detect the presence of hidden data, which is the problem of *steganalysis*.

Nowadays there are a lot of applications to IT and a lot of papers and books devoted to staganography.

watermarks, fingerprints

spying business

Cryptography or not cryptography ?

anyway, it belongs to data protection

Introduction- II

We assume that there are two communicating parties — the sender (Alice) and the receiver (Bob). Alice embeds a secret message in a cover object and transmits it to Bob over an open communications channel. Bob is able to extract the message from the cover object. There is also an eavesdropper (Eve) who observes all transmissions and carries out steganalysis to detect the fact of transmitting hidden data.

We also assume that the secret messages are encrypted prior to their embedding and thus are *indistinguishable from uniformly distributed random sequences.*

comment

If a memory of cover object is a finite (like Bernoulli or Markov chain) the problem is solved

B. Ryabko, D.Ryabko. Asymptotically Optimal Perfect Steganographic Systems. Problems of Information Transmission, 2009, Vol. 45, No. 2, pp. 184-190.

B. Ryabko, D. Ryabko. Information–Theoretic Approach to Steganographic Systems. IEEE International Symposium on Information Theory, Proceedings. 2007, Nice, France, pp. 2461-2464.

Introduction- III

Embedding hidden data is usually performed by introducing some distortions (errors) in cover objects.

In the simplest case, it may be the number of bits changed divided by the total number of bits in least significant bit (LSB) replacement or matching algorithms.

The progress in steganalysis shows that if the distortions exceed a certain bound, the presence of hidden data can be detected, and the bound tends to be smaller and smaller.

The main example

Let Alice be able to transmit N-bit messages in which she can change no more than n bits. (It is supposed that Eve can detect the fact of introducing distortion and, hence, the fact of hidden data transmission, if $n + 1$ bits or more have been changed). One of the possible strategies for Alice is to select n positions (agreed with Bob) and replace them with the bits of a secret message. The size of the set of all possible secret messages is 2^n.

The main result

But Alice may select any n positions in the covertext to make changes, she has the set of possible messages of a rather greater size $\sum_{i=0}^{n} \binom{N}{i}$ Consequently, Alice can potentially transmit secret messages of $\log \sum_{i=0}^{n} \binom{N}{i}$ bits which asymptotically, equals $N\, h(n/N)\,(1 + o(1))$, where $h(x) = -(x \log x + (1-x)\log(1-x))$ is the binary Shannon entropy.

If $n = 1$, then $\log N$ instead of 1, if $n = 2$, $(2 \log N - 1)$ instead 2, etc.
So, even for small embedding rates n/N, the length of embedded message, asymptotically, can be much greater than n.

We suggest the method which is asymptotically close to this bound!

Example

Let there be given a stegosystem with the set of covertexts $\hat{C}$ and the set of admissible distortions $\hat{D}$. For instance, $\hat{C}$ may be a set of digital photos in full-color BMP format with resolution 1280×800 pixels where each pixel is encoded by three bytes, representing the intensities of red, green and blue color components (RGB). A set of admissible distortions $\hat{D}$ may be composed of elements represented as three matrices (maps) of zeros and ones, each of size 1280×800, where ones indicate the positions which must be changed by LSB replacement or LSB matching, the share of ones being not greater than some threshold (say, 1%) in each matrix.

Example-2

But what is important, our approach is suitable for more complicated distortion models. An alternative demand may admit distortions of not more than 1% of LSB, as previously, but distortions in adjacent pixels are prohibited.
In the third case, the distortions are admitted if in any 10×10 square (or a circle with a diameter of 10 pixels) there is not more than 1 bit changed.
And so on.

The capacity

A natural question is related to estimation of the amount of information which can be transmitted in the system $\hat{C}$, $\hat{D}$.
We call this value the capacity of the system and denote by γ.
Then, evidently,

$$\gamma \leq \log |\hat{D}| \, ,$$

Indeed, each distortion corresponds to one hidden message, so the number of words of length γ (which is 2^{γ}) cannot be greater than the number of admissible distortions $|\hat{D}|$, hence $2^{\gamma} \leq |\hat{D}|$.

The main result-short

We suggest a stegosystem construction that allows to transmit secret information of the amount asymptotically close to the maximum possible $\log |\hat{D}|$.
In a case where n bits from N this amount is close to

$$\log \sum_{i=0}^{n} \binom{N}{i}.$$

The construction is based on linear hash functions.
Definition. A hash function λ is linear if for any x, y

$$\lambda(x \oplus y) = \lambda(x) \oplus \lambda(y).$$

($\oplus$ = bitwise addition modulo 2).

The algorithm

In many cases, both covertexts and distortions may be represented as binary words of equal length and the process of applying the distortion d to the covertext c may be reduced to bitwise addition modulo 2, the covertext with introduced distortion may be represented as $w = c \oplus d$.

Let λ be a mixing linear hash function defined over the set of words w and taking values in the set of binary words of a certain length γ_λ.

The stegosystem Λ:

Let Alice have a covertext $c \in \hat{C}$ and wish to send it with embedded secret message $s \in \{0,1\}^{\gamma_\lambda}$. To do that she computes $u = \lambda(c)$, $v = u \oplus s$, and finds the distortion $d \in \hat{D}$ satisfying the identity $\lambda(d) = v$. Alice forms the stegotext $w = c \oplus d$ and sends it to Bob.

Bob extracts the message by computing $s = \lambda(w)$.

Theorem about Λ

Theorem

Let the stegosystem Λ be used. If for every word $v \in \{0,1\}^{\gamma_\lambda}$ there exists $d \in \hat{D}$ for which $\lambda(d) = v$, then $\lambda(w) = s$ and the system capacity equals γ_λ.

Remark

In order to fulfill the condition that $d \in \hat{D}$ for which $\lambda(d) = v$ exists, it is sufficient to require that the values of hash function λ cover entirely the set of γ_λ-bit words, the identity must hold $\{\lambda(d) : d \in D\} = \{0,1\}^{\gamma_\lambda}$. Then, evidently, for any $v \in \{0,1\}^{\gamma_\lambda}$ such $d \in \hat{D}$ can be found that $\lambda(d) = v$. Notice also that the system capacity equals γ_λ in this case.

Example of linear hash function

Hash functions defined over binary fields. Every word

$$w = w_{N-1} w_{N-2} \dots w_1 w_0 \in \{0,1\}^N$$

may be seen as the polynomial

$$w(x) = w_{N-1} x^{N-1} + w_{N-2} x^{N-2} + \cdots + w_1 x + w_0 \ .$$

Let m be an integer and

$$g(x) = x^m + g_{m-1} x^{m-1} + g_{m-2} x^{m-2} + \cdots + g_1 x + g_0$$

be a degree m polynomial. We define the hash function $\lambda_G(w)$ $w(x)$ by $g(x)$:

$$\lambda_G(w) = w(x) \bmod g(x) \ ,$$

$\lambda_G(w_1 \oplus w_2) = \lambda_G(w_1) \oplus \lambda_G(w_2)$, λ_G is a linear hash function. It is known that if $g(x)$ is an irreducible polynomial then the set of all possible polynomials $\lambda_G(w)$ constitutes a binary field $\mathbb{F}_{2^m}$

Example of stegosystem

Consider an implementation of the described protocol using the hash function $\lambda_G(w)$ defined over a binary field $\mathbb{F}_{2^m}$. Denote by Λ_G the described above stegosystem Λ in the case when the hash function λ_G is employed.
Let the covertexts be binary words of length $N = 2^m - 1$, $m \geq 1$, and the admissible distortion be 1 bit (in other words, the sender gets an N-bit word w in which she may change not more than 1 bit for hidden data transmission).
Formally, the set of admissible distortions $\hat{D}$ may be represented as $\hat{D} = \{s_0, s_1, \ldots, s_N\}$, where s_i is a word having a single 1 at the i-th position and zeros at the remaining positions (s_0 consisting of zeros only).

Example of stegosystem-2

To construct the stegosystem Λ_G choose a primitive polynomial $g(x)$ of degree m that constitutes a binary field $\mathbb{F}_{2^m}$ and let for a word $w \in \{0,1\}^N$ hash function $\lambda_G(w)$ be defined . (Note that the length of hash values is m bits.)

Proposition

The capacity of the stegosystem Λ_G equals m bits which is the maximum possible value.

Asymptotic Capacity of Stegosystems Based on Hash Functions

It occurs that, asymptotically, under any arbitrarily small $\delta > 0$ the capacity γ_λ is close to the maximum possible. More formally, the following holds:

Theorem

Let the stegosystem Λ be defined on the set of covertexts $\hat{C}$, the set of randomly selected admissible distortions $\hat{D}$ and uses a hash function λ which possesses the mixing property. Then for large $|\hat{D}|$ and any $\delta > 0$ the inequality

$$\gamma_\lambda \geq \log |\hat{D}| - \log \ln(|\hat{D}|/\delta)$$

holds with probability $1 - \delta$ (here log *denotes binary and* ln *natural logarithms).*

Thank you for attention!