Provably Secure Universal Steganographic Systems

Boris Ryabko, Daniil Ryabko
{boris, daniil}@ ryabko.net

Abstract

We propose a simple universal (that is, distribution–free) steganographic system in which covertexts with and without hidden texts are statistically indistinguishable. Moreover, the proposed steganographic system has two important properties. First, the rate of transmission of hidden information approaches the Shannon entropy of the covertext source as the size of blocks used for hidden text encoding tends to infinity. Second, if the size of the alphabet of the covertext source and its minentropy tend to infinity then the the number of bits of hidden text per letter of covertext tends to $\log(n!)/n$ where n is the (fixed) size of blocks used for hidden text encoding. The proposed stegosystem uses randomization.

1 Introduction

The goal of steganography is as follows. Alice and Bob can exchange messages of a certain kind (called covertexts) over a public channel which is open to Eve. The covertexts can be, for example, photographic images, videos, text emails and so on. Alice wants to pass some secret information to Bob so that Eve can not notice that any hidden information was passed. Thus, Alice should use the covertexts to hide the secret text. It is supposed that Alice and Bob share a secret key. A classical illustration from [2] states the problem in terms of communication in a prison: Alice and Bob are prisoners who want to concoct an escape plan passing each other messages which can be read by a ward.

Perhaps the first formal approach to steganography was taken by Cachin [1] who proposed a steganographic protocol in which, relying on the fact that the probability distribution of covertexts is known, covertexts with and without hidden information are statistically indistinguishable. In the same work a universal (distribution-free) steganographic system was proposed, in which this property holds only asymptotically with the size of the messages going to infinity, and which has exponential complexity of coding and decoding. Distribution-free stegosystems are of particular practical importance, since in reality covertexts can be graphical images, ICQ or email messages, that is, sources for which the distribution is not only unknown but perhaps can not be reasonably approximated. Later a complexity–theoretic approach for (distribution-free) steganography was developed in [3, 4], where stegosystems were proposed in which covertexts with and without hidden information are indistinguishable in polynomial time.

We use the following model for steganography, mainly following [1]. It is assumed that Alice has an access to an oracle which generates independent and identically distributed covertexts according to some fixed but unknown distribution μ. Covertexts belong to some (possibly infinite) alphabet A. Alice wants to use this source for transmitting hidden messages. A hidden message is a sequence of letters from $B = \{0, 1\}$ generated independently with equal probabilities of 0 and 1. We denote the source of hidden messages by ω. This is a commonly used model for the source of secret messages since it is assumed that secret messages are encrypted by Alice using a key shared only with Bob. If Alice uses the ideal Vernam cipher then the encrypted messages are indeed generated according to the Bernoulli 1/2 distribution, whereas if Alice uses modern block or stream ciphers then the encrypted sequence "looks like" a sequence of random Bernoulli 1/2 trials. Here to "look like" means to be indistinguishable in polynomial time or that the likeness is confirmed experimentally by statistical data, known for all widely used cyphers; see, e.g. [6, 7]. The third party, Eve, is reading all messages passed from Alice to Bob and is trying to determine whether secret messages are being passed in the covertexts or not. Observe that if covertexts with and without hidden information have the same probability distribution (μ) then it is impossible to distinguish them.

In the universal system proposed in [1] the hiddentext sequence is divided into blocks of a certain size m each of which corresponds to a block of length $n(m)$ of covertexts letters from A. The distribution of resulting covertexts letters tends to the (unknown) distribution μ (of covertexts without hidden information) as n tends to infinity. It is important to note that the convergence is not uniform (on the set of all possible distributions μ with A fixed), and also the memory size of coder and decoder grows exponentially with n. Thus such stegosystems are not practical.

We propose a simple universal stegosystem for which covertexts with and without hidden information have the same distribution (and hence are statistically indistinguishable) for any size of the message. Moreover, the proposed system has two important properties. First, the rate of transmission of hidden information approaches the Shannon entropy of the covertext source as the size n of blocks used for hidden text encoding tends to infinity. Second, if the size of the alphabet of the covertext source and its minentropy tend to infinity then the the number of bits of hidden text per letter of covertext tends to $\log(n!)/n$ where n is the (fixed) size of blocks used for hidden text encoding. The latter property is, in particular, an advantage as compared to the complexity–theory based stegosystems proposed in [3, 4, 5] for which the rate of hidden text transmission is no more than a constant per covertext letter. We note that it is also possible to use the proposed stegosystems for open-key steganography in a standard way.

The paper is organized as follows. In Section 2 a simple stegosystem which does not use randomization is proposed; for this system the number of bits of hidden text per letter of covertext tends to 1/2 if the size of the alphabet of the covertext source and its minentropy tend to infinity. This system also illustrates the main ideas used in Section 3, where the general (randomized) stegosystem is proposed which has the mentioned asymptotic properties of the rates of hidden text transmission. In Section 4 we discuss possible extensions of the proposed steganographic systems and outline some potentially interesting open problems. In particular, we discuss issues concerning stegosystems based on a common set of data and open–key steganography.

2 A simple non-randomized universal stegosystem

In this section we present a very simple stegosystem which demonstrates the main ideas used in the general stegosystem which we develop in the next section and also does not use randomization.

The notation is as follows. The source μ draws i.i.d. (covertext) letters from an alphabet A. The source ω draws i.i.d. (hidden, or secret) equiprobable letters from the alphabet $B = \{0, 1\}$. Finite groups of (covertext, hidden, secret) letters are sometimes called (covertext, hidden, secret) words. Elements of A (B) are usually denoted by x (y).

First consider an example. Consider a situation in which not only the secret letters are drawn (using ω) from a binary alphabet, but also the source of covertexts μ generates symbols from the alphabet $A = \{a, b\}$ (not necessarily with equal probabilities). Suppose that Alice has to transmit the sequence $y^* = y_1 y_2 \ldots$ generated according to ω and let there be given a covertext sequence $x^* = x_1 x_2 \ldots$ generated by μ. For example, let

$$y^* = 01100\ldots, \quad x^* = aababaaaabbaaaaabb\ldots. \tag{1}$$

The sequences x^* and y^* are encoded in a new sequence X (to be transmitted to Bob) such that y^* is uniquely determined by X and the distribution of X is the same as the distribution of x^* (that is, μ; in other words, X and x^* are statistically indistinguishable).

The encoding is carried out in two steps. First let us group all symbols of x^* into pairs, and denote

$$aa = u,\ bb = u,\ ab = v_0,\ ba = v_1.$$

In our example, the sequence (1) can be represented as

$$x^* = aa\,ba\,ba\,aa\,ab\,ba\,aa\,aa\,bb \cdots = uv_1v_1uv_0v_1uuu\ldots$$

Then X is acquired from x^* as follows: all pairs corresponding to u are left unchanged, while all pairs corresponding to v_k are transformed to pairs corresponding to $v_{y_1}v_{y_2}v_{y_3}\ldots$; in our example

$$X = aa\,ab\,ba\,aa\,ba\,ab\,aa\,aa\,bb....$$

Decoding is obvious: Bob groups the symbols of X into pairs, ignores all occurrences of aa and bb and changes ab to 0 and ba to 1.

The properties of the described stegosystem, which we call St_2, are summarized in the following (nearly obvious) statement.

Claim 1. *Let a source μ be given, which draws i.i.d. random variables taking values in $A = \{a, b\}$ and let this source be used for encoding secret messages consisting of a sequence of i.i.d. equiprobable binary symbols using the method St_2. Then the sequence of symbols output by the stegosystem obeys the same distribution μ as the input sequence.*

We will not give the (obvious) proof of this claim since it is a simple corollary of Theorem 1 below.

It is interesting to note that a similar construction was used by von Neumann in his method for extracting a sequence of equiprobable binary symbols (see [8, 9]). His method, as well as the just described stegosystem, was based on the fact that the probabilities of ab and ba are equal.

Next we consider the generalisation of the described stegosystem to the case of any alphabet A (such that $|A| > 1$). To do this we fix some total ordering on the set A. As before, Alice has to transmit a sequence $y^* = y_1 y_2 \dots$ generated by the source ω of i.i.d. equiprobable binary letters and let there be given a sequence $x^* = x_1 x_2 \dots$ of covertext letters generated i.i.d. according to a distribution μ on A. Again we transform the sequences y^* and x^* into a new sequence X which obeys the same distribution as x^*. As before we break x^* into blocks of length 2. If a block $x_{2i-1}x_{2i}$ has the form aa for some $a \in A$ then it is left unchanged. Otherwise let the block $x_{2i-1}x_{2i}$ be ab for $a, b \in A$ and suppose $a < b$; if the current symbol y_k is 0 then the block ab is included in X, and if $y_k = 1$ then ba is included in X. Denote this stegosystem by $St_2(A)$.

Theorem 1. *Let a source μ be given, which generates i.i.d. random variables taking values in some alphabet A. Let this source be used for encoding secret messages consisting in a consisting sequence of i.i.d. equiprobable binary symbols, using the method $St_2(A)$. Then the sequence of symbols output by the stegosystem obeys the same distribution μ as the input sequence and the number of letters of hidden text transmitted per letter of covertext is $\frac{1}{2}(1 - \sum_{a \in A} \mu(a)^2)$.*

Proof. Fix some $\alpha, \beta \in A$ and $k \in \mathbb{N}$. We will show that

$$p(X_{2k-1}X_{2k} = \alpha\beta) \;=\; \mu(\alpha\beta),$$

where p is the probability distribution of the output sequence. Suppose $\alpha < \beta$. Decomposing the probability on the left we get

$$\begin{aligned} p(X_{2k-1}X_{2k} = \alpha\beta) = \omega(y_k = 0)(\mu(\alpha\beta) + \mu(\beta\alpha)) \\ = \frac{1}{2}(\mu(\alpha\beta) + \mu(\alpha\beta)) = \mu(\alpha\beta). \end{aligned}$$

The case $\beta < \alpha$ is analogous, and the case $\beta = \alpha$ is trivial. The second statement is obtained by calculating the probability of that letters in the block coincide. $\square$

Note that in practice when the covertexts are, for example, graphical files, each covertext is practically unique (the alphabet A is potentially infinite) so that the number of covertext letters (files) per one hidden bit is approximately 2.

3 The general construction of a universal stegosystem

In this section we consider the general construction of universal stegosystem which has the desired asymptotic properties. As before, Alice needs to transmit a sequence $y^* = y_1 y_2 \dots$ of secret binary messages drawn by an i.i.d. source ω with equal probabilities of 0 and 1, and let there be given a sequence of covertexts $x^* = x_1 x_2 \dots$ drawn i.i.d. by a source μ from an alphabet A. First we break the sequence x^* into blocks of n symbols each, where $n > 1$ is a parameter. Each block will be used to transmit several symbols from y^* (for example, in the previously constructed stegosystem $St_2(A)$ each block was used to transmit 1 or 0 symbols). However, in the general case a problem arises which was not present in the construction of $St_2(A)$. Namely, we have to align the lengths of the blocks of symbols from x^* and from y^*, and for this we will need randomization. The problem is that the probabilities of blocks from y^* are divisible by powers of 2, which is not necessarily the case with blocks from x^*.

We now present a formal description. Let u denote the first n symbols of x^*: $u = x_1 \dots x_n$, and let $\nu_u(a)$ be the number of occurrences of the symbol a in u. Define the set S_u as consisting of all words of length n in which the frequency of each letter $a \in A$ is the same as in u:

$$S_u = \{v \in A^n : \forall a \in A \ \nu_v(a) = \nu_u(a)\}.$$

Observe that the μ-probabilities of all members of S_u are equal. Let there be given some ordering on the set S_u (for example, lexicographical) which is known to both Alice and Bob (and to anyone else) and let $S_u = \{s_1, s_2, \dots, s_{|s|-1}\}$ with this ordering.

Denote $m = \lfloor \log_2 |S_u| \rfloor$, where $\lfloor y \rfloor$ stands for the largest integer not greater than y. Consider the binary expansion of $|S_u|$:

$$|S_u| = (\alpha_m, \alpha_{m-1}, \dots, \alpha_0),$$

where $\alpha_m = 1$, $\alpha_j \in \{0,1\}$, $m > j \geq 0$. In other words,

$$|S_u| = 2^m + \alpha_{m-1}2^{m-1} + \alpha_{m-2}2^{m-2} + ... + \alpha_0.$$

Define a random variable Δ as taking each value $i \in \{0, 1, \dots, m\}$ with probability $\alpha_i 2^{m-i}/|S_u|$:

$$p(\Delta = i) = \alpha_i 2^{m-i}/|S_u|. \tag{2}$$

Alice, having read u, generates a value of the random variable Δ, say d, and then reads $m-d$ symbols from y^*. Consider the word r^* represented by these symbols as an integer which we denote by r. Then we encode the word r^* (that is, $m-d$ bits of y^*) by the word s_τ from the set S_u, where

$$\tau = \sum_{l=m-d+1}^{m} \alpha_l 2^l + r.$$

(In other words, the word s_τ is being output by the coder.)

Then Alice reads the next n–bit word, and so on. Denote the constructed stegosystem by $St_n(A)$.

To decode the received sequence Bob breaks it into blocks of length n and repeats all the steps in the reversed order: by the current word u he obtains S_u and τ, then d (clearly d is uniquely defined by τ) and then r and r^*; that is, he finds $|r^*|$ next symbols of the secret sequence y^*.

Consider an example which illustrates all the steps of the calculation. Let $A = \{a, b, c\}$, $n = 3$, $u = bac$. Then $S_u = \{abc, acb, bac, bca, cab, cba\}$, $|S_u| = 6, m = 2, \alpha_2 = 1, \alpha_1 = 1, \alpha_0 = 0$. Let the sequence of secret messages be 0110..., that is, $y^* = 0110...$. Suppose the value of Δ generated by Alice is 1. Then she reads one symbol of y^* (in this case 0) and calculates $r = 0, r^* = 0, \tau = 2^2 + 0 = 4$ and finds the codeblock $s_4 = cab$. To decode the message, Bob from the block cab calculates $\tau = 4, r = 0, r^* = 0$ and finds the next symbol of the secret sequence — 0.

Theorem 2. *Let a source μ be given, which generates i.i.d. random variables taking values in some alphabet A. Let this source be used for encoding secret messages consisting of a sequence of i.i.d. equiprobable binary symbols using the described method $St_n(A)$ with $n > 1$. Then*

(i) the sequence of symbols output by the stegosystem obeys the same distribution μ as the input sequence,

(ii) the average number of secret symbols per covertext (L_n) satisfies the following inequality

$$L_n \geq \frac{1}{n}\left(\sum_{u\in A^n} \mu(u)\log\frac{n!}{\prod_{a\in A}\nu_u(a)!} - 2\right), \tag{3}$$

where $\mu(u)$ is the μ-probability of the word u and $\nu_u(a)$ is the number of occurrences of the letter a in the word u.

Proof. To prove the first statement it is sufficient to show that for any covertext word u of length n its probability of occurrence in the output sequence is $1/|S_u|$. This follows from (2) and the fact that letters in y^* are independent and equiprobable.

The second statement can be obtained by direct calculation of the average number of symbols from y^* encoded by one block. $\square$

Let us now consider the asymptotic behaviour of L_n when $n \to \infty$.

Corollary 1. *If the alphabet A is finite then the average number of hidden symbols per letter L_n goes to the Shannon entropy $h(\mu)$ of the source μ as n goes to infinity; here by definition $h(\mu) = -\sum_{a\in A}\mu(a)\log\mu(a)$.*

Proof. This statement follows from a well-known fact of Information Theory which states that for each $\delta > 0$ and $n \to \infty$ the following inequality holds with probability 1

$$h(\mu) - \delta < \log|S_u|/n < h(\mu) + \delta,$$

see, e.g. [10]. $\square$

In many real stegosystems the alphabet A is huge (it can consist, for example, of all possible digital photographs of given file format, or of all possible e-mail messages). In such a case it is interesting to consider the asymptotic behaviour of L_n with fixed n when the alphabet size $|A|$ goes to infinity. For this we need to define so-called the min-entropy of the source μ:

$$H_\infty(\mu) = \min_{a\in A}\{-\log\mu(a)\}. \tag{4}$$

Corollary 2. *Assume the conditions of Theorem 2 and fix the block length $n > 1$. If $|A| \to \infty$ so that $H_\infty(\mu) \to \infty$ then L_n tends to $(log(n!)+O(1))/n$.*

This statement can be easily derived from the fact that the number of different permutations of n elements in $n!$.

Next we briefly consider the resource complexity of the stegosystem $St_n(A)$. To store all possible words from the set S_u would require memory of order $2^n \log|A|$ bits, which is practically unacceptable for large n. However, if we use the algorithm for fast enumeration from [11], then we can find the index of a block s_τ given τ (encoding) and vice versa (decoding) using $O(\log^{const} n)$ operations per symbol and $O(n \log^3 n)$ bits of memory.

4 Discussion

We have proposed two stegosystems (with and without randomization) for which the output sequence of covertexts with hidden information is statistically indistinguishable from a sequence of covertexts without hidden information. The main idea that was used is that for any block of covertexts it is possible to find several other blocks which have the same probability as the original one; then hidden information can be encoded in the number of a block in this group. This idea has several possible extensions which we discuss here.

First of all, observe that the proposed stegosystems rely heavily on the assumption that the oracle generates independent and identically distributed covertexts. This is perhaps a reasonable assumptions if covertexts are graphical images of a certain kind, but if, for example, we want to use just one image to transmit (a large portion of) a secret text then our covertexts are parts of the image, which are clearly not i.i.d. How to extend the ideas developed in this work to the case of non-i.i.d. covertexts is perhaps the main open question.

The idea to use the number of a covertext in a known group to encode information can also be used in the following situation. Suppose that Alice and Bob share a database of covertexts (say, graphical images or list of mottos). Then by sending one covertext from the database (or a reference to it) to Bob, Alice can transmit $\log N$ bits of information, where N is the size of the database. If the database was generated using an oracle generating i.i.d. covertexts then the fact of secret communication is not statistically recognisable. Similar ideas can also be used if the database is any public collection of objects available for indexing.

References

[1] *Cachin C.* An information-theoretic model for steganography. In: Proc. 2nd Information Hiding Workshop, v. 1525 of LNCS, pp. 306-318, Springer Verlag, 1998.

[2] *Simmons G.J.* The Prisoner's Problem and the Subliminal Channel. In: Proceedings of CRYPTO'83, 1984.

[3] *Hopper N., Langford J., von Ahn L.* Provably secure steganography. Technical Report 2002/137, Cryptology e-print archive, http://eprint.iacr.org , 2002.

[4] *Tre Van Le.* Efficient provably secure public key steganography. Technical Report 2003/156, Cryptology e-print archive, http://eprint.iacr.org , 2003.

[5] *von Ahn L., Hopper N.* Public-key steganography. In: Advances in Cryptology - EUROCRYPT 2004, v. 3027 of LNCS, p. 323-341

[6] *B.Ryabko, A. Fionov.* Basics of Contemporary Cryptography for IT Practitioners. World Scientific Publishing Co., 2005.

[7] *Menzes A., van Oorschot P., Vanstone S.* Handbook of Applied Cryptography. CRC Press, 1996.

[8] *von Neumann J.* Various Techniques Used in Connection with Random Digits. // Monte Carlo Method, Applied Mathematics Series, 12, U.S. National Bureau of Standarts, Washington D.C., P. 36-38.

[9] *Elias P.* The Efficient Construction of an Unbiased Random Sequence. // The Annals Math. Statist. 1972. V. 43 (3), P. 864-870.

[10] *Gallager R.G.* Information Theory and Reliable Communication. John Wiley & Sons, New York, 1968.

[11] *Ryabko B.Ya.* The fast enumeration of combinatorial objects. //Discrete Math.and Applications, v.10, n2, 1998.

(see also http://arxiv.org/abs/cs.CC/0601069).