ISSN 0032-9460, Problems of Information Transmission, 2009, Vol. 45, No. 2, pp. 184–190. © Pleiades Publishing, Inc., 2009.
Original Russian Text © B.Ya. Ryabko, D.B. Ryabko, 2009, published in Problemy Peredachi Informatsii, 2009, Vol. 45, No. 2, pp. 119–126.

INFORMATION PROTECTION

Asymptotically Optimal Perfect Steganographic Systems[1]

B. Ya. Ryabko[a] and D. B. Ryabko[b]

[a] *Siberian State University of Telecommunication and Information Science*
Institute of Computational Technologies, Siberian Branch of the RAS, Novosibirsk
boris@ryabko.net
[b] *INRIA Lille - Nord Europe, France*
daniil@ryabko.net

Received February 9, 2006; in final form, February 23, 2009

Abstract—In 1998 C. Cachin proposed an information-theoretic approach to steganography. In particular, in the framework of this approach, so-called perfectly secure stegosystems were defined, where messages that carry and do not carry hidden information are statistically indistinguishable. There was also described a universal steganographic system, for which this property holds only asymptotically, as the message length grows, while encoding and decoding complexity increases exponentially. (By definition, a system is universal if it is also applicable in the case where probabilistic characteristics of messages used to transmit hidden information are not known completely.)
In the present paper we propose a universal steganographic system where messages that carry and do not carry hidden information are statistically indistinguishable, while transmission rate of "hidden" information approaches the limit, the Shannon entropy of the source used to "embed" the hidden information.

DOI: 10.1134/S0032946009020094

1. INTRODUCTION

Steganographic data transmission systems are designed to "secretly" transmit messages "hidden" in openly transmitted data (such as e-mail messages, digital photos, films, etc.). In other words, the aim of steganography is to transmit data protected from unauthorized access (e.g., encrypted) in such a way that the very fact of transmission is hidden. This condition is formulated as follows: messages that carry and do not carry hidden information should be subject to the same probability distribution, being therefore statistically indistinguishable [1].

In many cases of using stegosystems, the probability distribution law of messages in which the hidden information is "embedded" is not known precisely; in the case where these messages are digital photos, films, music, electronic correspondence, SMS or ICQ messages, etc., the distribution law, apparently, cannot be known precisely. Therefore, the problem (considered in [1]) of constructing so-called universal stegosystems—where the probability distribution law of messages in which hidden information is "embedded" is not known, but symbols generated by the source are a priori known to be identically distributed and independent—seems quite natural.

Here is some notation used in what follows. We assume that there is a source of *cover messages* μ, which generates i.i.d. random variables that take values in some (possibly, infinite) alphabet A. There are two parties, Alice and Bob, and Alice wants to use this source to secretly transmit messages that are sequences of symbols in the alphabet $B = \{0, 1\}$ generated independently and

[1] Supported in part by the Russian Foundation for Basic Research, project no. 06-07-89025.

equiprobably. We denote the latter source by ω and hereafter refer to it as a *source of secret messages*. This model of a source of secret messages is in fact standard since usually it is assumed that secret messages are already encrypted by Alice using a key that is known to her and to Bob only. If Alice uses the Vernam cipher, then the encrypted message consists of equiprobable and independent symbols; if modern block or stream secret-key ciphers are used, then the encrypted sequence must "resemble" a chain of equiprobable and independent binary symbols (the "resemblance" may mean indistinguishability in polynomial time or may be justified by experimental statistical data, which are available for all modern ciphers; for details, see, e.g., [2,3]). Besides Alice and Bob, there is one more party, Eve, who reads all messages transmitted from Alice to Bob and tries to find whether the messages contain any hidden information. We note that if messages that contain and do not contain embedded secret information are subject to the same probability distribution law, then Eve (as well as anybody else) is unable to distinguish between such messages. Due to this property, such systems were called perfectly secure in [1].

For the described model, [1] proposed a construction of a universal stegosystem where a sequence of symbols generated by a source of secret messages is divided into subwords (blocks) of some length m, and to each block there is assigned a certain word of a fixed length $n(m)$ in the alphabet A in such a way that the sequence of obtained symbols is subject to a probability distribution that approaches the (unknown) distribution μ (recall that μ is the distribution of messages that contain no hidden secret information). It is important to note that, first, though the probability distribution of messages of the stegosystem converges to μ as the message length n grows, this convergence is not uniform (with respect to the set of all probability distributions μ for a fixed alphabet A), and second, the encoder and decoder memory of this stegosystem grows exponentially with n. These two reasons make the stegosystem from [1] practically inapplicable. In [4, 5] the approach and results of [1] were used to construct and analyze stegosystems that are in this or that sense close to but not perfectly secure.

In this paper we propose a novel construction of a universal stegosystem free of drawbacks of the method of [1]: in our construction messages that carry and do not carry hidden information are statistically indistinguishable for any message length; i.e., the system is perfectly secure. Furthermore, we show that the transmission rate of hidden information is bounded by a limit value, the Shannon entropy of the source μ, and find constructions of stegosystems where this rate approaches the limit. It is important to note that we propose a simple encoding and decoding algorithm, whose complexity grows polynomially as the transmission rate of hidden information tends to its limit, the Shannon entropy.

2. A SIMPLE UNIVERSAL STEGOSYSTEM

To explain the main idea of the proposed construction, we start describing the system with the simplest case where not only the source ω of secret messages is binary but also the source μ of cover messages generates a sequence of independent symbols of the binary alphabet $A = \{a, b\}$. Assume that Alice has to transmit a (secret) sequence $y^* = y_1y_2y_3\ldots$ of symbols generated by a source ω of independent and equiprobable binary symbols, and let a sequence $x^* = x_1x_2x_3\ldots$ of symbols generated by μ be given. For instance, let

$$y^* = 0110\ldots, \qquad x^* = aababaaaabbaaaaabb\ldots. \tag{1}$$

The sequences x^* and y^* are encoded into a new sequence X, transmitted to Bob, such that, first, Bob can uniquely reconstruct the (secret) sequence y^* given X, and second, the probability distribution of symbols in X is the same as in x^* (in other words, X and x^* are statistically indistinguishable). We divide the construction of X given x^* and y^* into stages. First we divide

all symbols of X^* into pairs and for convenience denote all possible pairs as follows:

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

For instance, the sequence in (1) can be represented as

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

(spaces are put for the convenience of reading only). Then we form the sequence X as follows: all pairs that correspond to u are left unchanged, and all pairs that correspond to v_k are successively changed into pairs corresponding to $v_{y_1}v_{y_2}v_{y_3}\ldots$. In the considered example (1), we obtain the following sequence X:

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

Decoding is obvious: Bob cuts the received sequence of symbols X into pairs and replaces the pairs ab and ba with 0 and 1, respectively, simply skipping other pairs of symbols.

Properties of this method, which we denote by St_2, are characterized by the following almost obvious fact.

Claim. *Let us be given a source μ generating i.i.d. random variables that take values in the alphabet $A = \{a, b\}$. Let this source be used for secret transmission of messages that consist of independent and equiprobable binary symbols according to the described method St_2. Then the probability distribution of messages output by the stegosystem is the same as for the source μ.*

We do not present a quite obvious proof of this claim since it is a particular case of Theorem 1 given below.

It is interesting to note that a similar construction was used by von Neumann when constructing a sequence of equiprobable binary symbols (see [6, 7]). His method, as well as the described stegosystem, was based on the fact that occurrence probabilities of ab and ba are the same.

The above-described construction can easily be extended to the case of an arbitrary alphabet A. Indeed, define any order on the set of symbols of A. (Here it should be noted that A may consist of graphics files or photographic images, but in any case these or similar objects are represented in data transmission systems as binary words and therefore can be ordered, say, lexicographically.) As above, to transmit a (secret) sequence $y^* = y_1y_2y_3\ldots$ of symbols generated by a source ω of independent and equiprobable binary symbols, a given sequence $x^* = x_1x_2x_3\ldots$ of symbols generated by a source μ of independent symbols, $x_i \in A$, is divided into blocks of length 2. If a block $x_{2i-1}x_{2i}$ consists of identical symbols, it is not used for encoding and is transmitted unchanged; if a block $x_{2i-1}x_{2i}$ consists of different symbols, say α and β, then it is used to encode the current symbol, which we denote by y_k. Without loss of generality, assume that $\alpha < \beta$ for a given ordering; then the transmitted sequence contains the word $\alpha\beta$ if $y_k = 0$ and the word $\beta\alpha$ if $y_k = 1$. Decoding is obvious: if a pair of symbols $X_{2i-1}X_{2i}$ in the encoded sequence consists of identical symbols, it does not encode a symbol of $y^* = y_1y_2y_3\ldots$. If $X_{2i-1}X_{2i}$ are different and $X_{2i-1} < X_{2i}$ (for a given ordering), then the current secretly transmitted symbol y_k is 0; otherwise, $y_k = 1$. We denote this stegosystem by $\mathrm{St}_2(A)$.

Theorem 1. *Let us be given a source μ generating i.i.d. random variables that take values in an alphabet A, and let this source be used for hidden transmission of messages consisting of independent and equiprobable binary symbols with the help of the stegosystem $\mathrm{St}_2(A)$. Then the probability distribution of messages output by the stegosystem is the same as for the source μ, and the average number of transmitted symbols per secretly transmitted bit is $2/\Big(1 - \sum\limits_{a\in A}\mu(a)^2\Big)$.*

Proof. Take arbitrary $\alpha, \beta \in A$ and i. Let us show that

$$P(X_{2i-1}X_{2i} = \alpha\beta) = \mu(\alpha\beta).$$

If $\alpha = \beta$, then $P(X_{2i-1}X_{2i}) = P(x_{2i-1}x_{2i})$; i.e., the probabilities in the sequence that contains hidden information and in the original sequence coincide. Now let $\alpha < \beta$. Then

$$\begin{aligned} P(X_{2i-1}X_{2i} = \alpha\beta) &= P(y_k = 0)P(x_{2i}x_{2i+1} = \alpha\beta) + P(y_k = 0)P(x_{2i}x_{2i+1} = \beta\alpha) \\ &= 1/2\mu(\alpha)\mu(\beta) + 1/2\mu(\beta)\mu(\alpha) = \mu(\alpha)\mu(\beta). \end{aligned}$$

The case $\beta > \alpha$ is considered similarly. The second claim is obtained by direct computation of the probability that two symbols in a block are identical. $\triangle$

Note that in practice, when openly transmitted symbols of A are, e.g., graphics files and each file is practically unique, the alphabet A is enormous, so the average number of transmitted symbols (graphics files) per secretly transmitted bit is approximately 2.

3. GENERAL CONSTRUCTION OF A UNIVERSAL STEGOSYSTEM

Now we describe the general method. Assume, as above, that it is required to transmit a (secret) sequence $y^* = y_1y_2y_3\ldots$ of symbols generated by a source ω of independent and equiprobable binary symbols, and let us have a sequence $x^* = x_1x_2x_3\ldots$ of symbols generated by a source μ of independent symbols, where each symbol x_i belongs to A. In the proposed stegosystem, we divide the sequence x^* into blocks of length n, where $n > 1$ is a parameter of the method.

Each block is used to encode several symbols of y^* (for example, in the stegosystem $\mathrm{St}_2(A)$ described above, each block of two symbols encodes either one symbol of y^* or no symbols). However, in the general case there arises a problem that does not occur in the case of a two-symbol block. Namely, this is the problem of coordination of probabilities of blocks in x^* and y^*. The point is that probabilities of words generated by the source of secret symbols are multiples of powers of 2, whereas the number of equiprobable blocks need not satisfy this condition.

Here is a precise description. Denote by u the first n symbols of x^*, $u = x_1\ldots x_n$, and let $\nu_u(a)$ be the number of occurrences of a symbol a in u. By definition, the set S_u consists of all words of length n in which the occurrence frequency of each symbol of the alphabet A is the same as in the word u; i.e., S_u consists of words of the frequency class of u. (To clarify the meaning of this set, note that probabilities of all of its elements are the same, since μ is a source of i.i.d. random variables.) Let on S_u there be defined an ordering (say lexicographic) known to Alice and Bob, and let $S_u = \{s_0, s_1, \ldots, s_{|S_u|-1}\}$ for this ordering.

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

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

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

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

Denote by $\delta(u)$ the order number of u (for a given ordering on S_u), and let $(\lambda_m, \lambda_{m-1}, \ldots, \lambda_0)$ be the binary representation of $\delta(u)$. Let $j(u)$ be the largest of numbers with $\alpha_j \neq \lambda_j$. Alice, having found $j(u)$, reads $j(u)$ symbols of the sequence of secretly transmitted symbols y^*; let these symbols viewed as a binary representation define a number τ. Alice finds in S_u a word v whose number in S_u is $\sum\limits_{j(u)<s\leq m} \alpha_s 2^s + \tau$ and transmits v to Bob (or, in other words, v is put into the output sequence of the encoder).

In decoding, Bob, having received the word v, determines the set S_v (which coincides with S_u); in the same way as in encoding, finds $j(v)$ (for u and v they coincide: $j(u) = j(v)$) and τ; and then, from τ, obtains the $j(v)$ encoded symbols. All subsequent n-tuples are encoded by Alice and decoded by Bob in the same way. We denote this system by $\mathrm{St}_n(A)$.

Consider an example illustrating all stages of computation. Let $A = \{a, b, c\}$, $n = 3$, and $u = bac$. Then $S_u = \{abc, acb, bac, bca, cab, cba\}$, $|S_u| = 6$, $m = 2$, $\alpha_2 = 1$, $\alpha_1 = 1$, $\alpha_0 = 0$, $\delta(u) = 2$, $\lambda_2\lambda_1\lambda_0 = 010$, and $j(u) = 2$. Having computed these values, Alice reads $j(u)$ $(= 2)$ secretly transmitted symbols of y^*. Let, for definiteness, these symbols be 11. After that, Alice finds $j(v) = 2$ and the number of the word v in S_v $(= S_u)$, which in this case is $\sum\limits_{2<s\le 2} \alpha_s 2^s + \tau = 0 + 3 = 3$. The corresponding word is $v = bca$. Bob, having received this word, finds S_v $(= S_u)$ and $\tau = 3$, and obtains from the value of τ the transmitted secret symbols 11.

Theorem 2. *Let us be given a source μ generating i.i.d. random variables that take values in an alphabet A, and let this source be used for secret transmission of messages that consist of independent and equiprobable binary symbols according to the above-described method $\mathrm{St}_n(A)$ with block length n, $n \ge 2$. Then we have the following statements*:

(i) *Output messages of the stegosystem are subject to the distribution μ (i.e., distributions of the input and output sequence of the encoder are the same, and therefore the system is perfectly secure*);

(ii) *The average number of hidden symbols per source symbol L_n satisfies the inequality*

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

where $\mu(u)$ is the probability that μ generates a word u, and $\nu_u(a)$ is the number of occurrences of a symbol a in u;

(iii) *If the alphabet A is finite and the block length n tends to infinity, then the average number L_n of hidden symbols per source symbol tends to the Shannon entropy $h(\mu) = -\sum\limits_{a\in A} \mu(a) \log \mu(a)$ of the message source.*

Proof. To prove (i), it suffices to show that for each n-tuple u in the input (original) sequence, the occurrence probability of any word $v \in S_u$ in the encoding sequence equals $1/|S_u|$. The proof is based on the total probability formula. As is seen from the description, the probability that j, $j = 0, \dots, m$, is read from the sequence of secretly transmitted symbols equals $2^j/|S_u|$ if $\alpha_j = 1$ (since the number of the word u in S_u must satisfy the inequality $\sum\limits_{j(u)<s\le m} \alpha_s 2^s \le \delta(u) < \sum\limits_{j(u)\le s\le m} \alpha_s 2^s$). For definiteness, let u and v be the first words in the original and encoded sequences. Then

$$P(X_1 \dots X_n = v) = P(u \in S_v \text{ and } j(v) = j(u)) 2^{-j(v)}.$$

Here the last factor is the probability to read, from the sequence y^* of secretly transmitted symbols, a binary word of length $j(v)$ that encodes v. This implies

$$\begin{aligned} P(X_1 \dots X_n = v) &= P(u \in S_v) P(j(v) = j(u) \,|\, u \in S_v) 2^{-j(v)} \\ &= |S_v| \mu(u) (2^{j(v)}/|S_v|) 2^{-j(v)} = \mu(u). \end{aligned}$$

Since u and v belong to the same frequency class, this equality shows that $P(X_1 \dots X_n = v) = \mu(v)$.

To prove (ii), define the quantity $\phi = 2^m/|S_u|$ and denote by $L(S_u)$ the average number of secretly transmitted symbols per word of S_u:

$$L(S_u) = \frac{1}{|S_u|} \sum_{i=0}^{m} \alpha_i i 2^i.$$

We have

$$L(S_u) = \frac{1}{|S_u|}\sum_{i=0}^{m}\alpha_i i 2^i = \frac{1}{|S_u|}\left(m\sum_{i=0}^{m}\alpha_i 2^i - \sum_{i=0}^{m}\alpha_i 2^i(m-i)\right)$$
$$= m - \left(2^m\sum_{k=0}^{m}k\alpha_{m-k}2^{-k}\right) > m - 2^{m+1}/|S_u| = m - 2/\phi = \log|S_u| - \log\phi - 2/\phi.$$

One can check by directly finding the maximum that $\log\phi + 2/\phi \le 2$ for $\phi \in [1,2]$. Hence, $L(S_u) > \log|S_u| - 2$. This, together with the equality $|S_u| = \dfrac{n!}{\prod\limits_{a\in A}\nu_u(a)!}$, implies statement (ii) of the theorem.

Statement (iii) follows from the fact widely known in information theory that the inequality $h(\mu) - \delta < \log|S_u|/n < h(\mu) + \delta$ holds for any $\delta > 0$ with probability tending to 1 (see, e.g., [8,9]). $\triangle$

In many real-world stegosystems, the alphabet A is enormous (say consists of all possible digital photos of a given image format or all e-mail messages). In this case, asymptotic behavior of L_n for a fixed n and $|A| \to \infty$ is of interest. To treat this case precisely, we use the notion of minimum entropy (or minentropy), which is defined as

$$H_\infty(\mu) = \min_{a\in A}\{-\log\mu(a)\}. \tag{3}$$

Corollary. *If the conditions of Theorem 2 are fulfilled, the block length n is finite, and the number of symbols of A tends to infinity in such a way that $H_\infty(\mu) \to \infty$, then L_n satisfies*

$$\log(n!)/n \ge L_n \ge (\log(n!) - 2)/n,$$

which is equivalent for large n to the asymptotic equality

$$L_n = \log n(1 + o(n)).$$

This is easily deduced from the fact that the number of permutations of n elements is $n!$ and from statement (ii) of Theorem 2.

Now let us briefly discuss the complexity of the stegosystem $\mathrm{St}_n(A)$. Storing all words of the set S_u would require of the order of $2^n\log|A|$ memory bits, which of course cannot be practically realized for large n. In [10], a fast enumeration algorithm is proposed, which makes it possible to find the number of a block of any word u in S_u in the encoding and to perform the inverse operation in the decoding with $O(\log^{\mathrm{const}} n)$ operations per symbol and with memory size of $O(n\log^3 n)$ bits.

It should be noted that the main idea exploited in the construction of the stegosystem $\mathrm{St}_n(A)$ can be applied to more general sources of cover messages than sources that generate i.i.d. messages. Indeed, the only property of such sources that we use consists in the fact that all blocks of messages obtained from each other by permutations are equiprobable. If the source of cover messages has the property that at some step some messages have the same (conditional) probability, then, if the source generates one of these messages, we can transmit secret information by replacing it with one of the equiprobable messages. Messages that do not belong to any group of equiprobable messages are not used for encoding secret information. Sources that generate i.i.d. messages is only a simple and significant example of encoding of this type.

The authors are deeply grateful to G.A. Kabatiansky, who suggested a considerable simplification of the method described in the paper and a simple proof of the estimate in Theorem 2.

REFERENCES

1. Cachin, C., An Information-Theoretic Model for Steganography, *Proc. 2nd Int. Workshop on Information Hiding, Portland, USA, 1998*, Aucsmith, D., Ed., Lect. Notes Comp. Sci., vol. 1525, Berlin: Springer, 1998, pp. 306–318.
2. Ryabko, B.Ya. and Fionov, A.N., *Kriptograficheskie metody zashchity informatsii* (Cryptographic Data Protection Methods), Moscow: Telekom, 2005.
3. Menezes, A.J., van Oorschot, P.C., and Vanstone, S.A., *Handbook of Applied Cryptography*, Boca Raton: CRC Press, 1997.
4. Sallee, P., Model-Based Steganography, *Proc. 2nd Int. Workshop on Digital Watermarking (IWDW'03), Seoul, Korea*, Kalker, T., Cox, I.J., and Ro, Y.M., Eds., Lect. Notes Comp. Sci., vol. 2939, Berlin: Springer, 2004, pp. 154–167.
5. Mittelholzer, T., An Information-Theoretic Approach to Steganography and Watermarking, *Proc. 3rd Int. Workshop on Information Hiding (IH'99), Dresden, Germany*, Pfitzmann, A., Ed., Lect. Notes Comp. Sci., vol. 1768, Berlin: Springer, 2000, pp. 1–16.
6. von Neumann, J., Various Techniques Used in Connection with Random Digits, in *Monte Carlo Method (Proc. Sympos. Held in Los Angeles, California, 1949)*, Appl. Math. Ser., vol. 12, Washington: U.S. Govt. Print. Off., 1951, pp. 36–38.
7. Elias, P., The Efficient Construction of an Unbiased Random Sequence, *Ann. Math. Stat.*, 1972, vol. 43, no. 3, pp. 864–870.
8. Csiszár, I., The Method of Types. Information Theory: 1948–1998, *IEEE Trans. Inform. Theory*, 1998, vol. 44, no. 6, pp. 2505–2523.
9. Gallager, R.G., *Information Theory and Reliable Communication*, New York: Wiley, 1968. Translated under the title *Teoriya informatsii i nadezhnaya svyaz'*, Moscow: Sov. Radio, 1974.
10. Ryabko, B.Ya., Fast Enumeration of Combinatorial Objects, *Diskret. Mat.*, 1998, vol. 10, no. 2, pp. 101–119 [*Discrete Math. Appl.* (Engl. Transl.), 2998, vol. 8, no. 2, pp. 163–182].