Proceedings of the International Multiconference on
Computer Science and Information Technology pp. 723–728

ISBN 978-83-60810-27-9
ISSN 1896-7094

Undetectable Spread-time Stegosystem Based on Noisy Channels

Valery Korzhik (Member, IEEE)
State University
of Telecommunications
St. Petersburg, Russia
Email: korzhik@spb.lanck.net

Guillermo Morales-Luna
Computer Science
CINVESTAV-IPN
Mexico City, Mexico
gmorales@cs.cinvestav.mx

Ksenia Loban
State University
of Telecommunications
St. Petersburg, Russia

Irina Marakova-Begoc
Bretagne Telecom, France
marakova.irina@gmail.com

***Abstract*—We consider a scenario where an attacker is able to receive a stegosignal only over a Gaussian channel. But in order to provide security of this channel noise–based stegosystem under the very strong condition that an attacker may know even the cover message, it is necessary to establish a very low signal-to-noise ratio in the channel. The last requirement is very hard to be implemented in practice. Therefore we propose to use spread-time stegosystem (STS). We show that both security and reliability of such STS can be guaranteed and their parameters can be optimized with the use of error correcting codes. We show some simulation results with an own STS implementation for digital audio cover messages presented in WAV format.**

***Index Terms*—Digital audio signal, error correcting codes, noisy Gaussian channel, relative entropy, stegosystems.**

I. Introduction

Steganography (SG) is the information hiding technique that embeds the hidden information into an innocent *cover message* (CM) under the conditions that the CM is not corrupted significantly and that the presence of the additional information into the CM may not be detected.

In order to prevent statistical detecting attacks on SG systems, it should be guaranteed the following principle: the statistics of the CM and the SG signal have to be indistinguishable for the time limited analysis.

But in order to implement this principle, the designer of the SG system should know at least the statistics of the CM. At the same time, it is a rather hard problem to study completely the CM distribution. In order to be successful within this risky situation (which is, indeed, a bottleneck of any SG system), it has been proposed in [1] to move into another concept of SG system setting, namely to SG system *based on noisy channels*.

This setting can be justified only if there exists in a natural manner a noisy channel and the attacker is able to receive the stegosignal just over this channel, and nothing else. Then the attacker's problem consists in statistically distinguishing the CM after its passing over the noisy channel and the SG signal passing over the same noisy channel. It should be emphasized that such model is even stronger than conventional SG systems since CM can be publicized. Thus the steganalysis problem reduces to channel noise recognition within the sum of the channel noise and the embedded signal. Since the channel noise distribution is, as a rule, known much better than the CM distribution, the problem to design SG systems which are resistant to their detection is simplified.

In the current paper we adopt only a Gaussian channel from the two models given in [1]. The embedding of an information bit b can be provided as

$$\forall n = 1, \dots, N: \quad C_W(n) = C(n) + (-1)^b \sigma_W \pi(n) \qquad (1)$$

where $C = (C(n))_{n=1}^N$ is the CM, $\pi = (\pi(n))_{n=1}^N$ is a zero-mean Gaussian pseudorandom i.i.d. reference sequence with variance 1, N is the length of both sequences and σ_W is the depth of embedding. After a passing of the watermarked signal through the Gaussian channel we get

$$\forall n = 1, \dots, N: \quad C'_W(n) = C_W(n) + \varepsilon(n)$$

where $\varepsilon = (\varepsilon(n))_{n=1}^N$ is a zero-mean Gaussian i.i.d. noise sequence with variance σ_ε^2. It has been proved in [1] that, under the condition that an attacker knows even the CM, the *relative entropy* D (introduced in [2]) can be expressed, for the current SG-system model, as

$$D = 0.72\ N \left[\ln\left(1 + \frac{1}{\eta_W}\right) - \frac{1}{1+\eta_W} \right] \qquad (2)$$

with $\eta_W = \frac{\sigma_\varepsilon^2}{\sigma_W^2}$. In order to provide a good hiding of secret information into the channel noise, η_W should be taken large. Hence, the relative entropy given by (2) is approximated as

$$D = 0.36\ \frac{N}{\eta_W^2}. \qquad (3)$$

We recall that in line with Information Theory [2], for any hypothesis testing rule, the following inequality should hold:

$$P_{fa} \ln \frac{P_{fa}}{1-P_m} + (1-P_{fa}) \ln \frac{1-P_{fa}}{P_m} \le D, \qquad (4)$$

where P_{fa} is the probability of *SG signal false alarm* and P_m is the probability of *SG signal missing*. Let us assume, for simplicity, $P_{fa} = P_m = P$. Then, by (4), we get $(2P-1) \ln \frac{P}{1-P} \le D$. From eq. (3) it follows that

$$\eta_W = 0.6 \sqrt{\frac{N}{D}}. \qquad (5)$$

The optimal decision rule for the embedded bit b, in the case of a Gaussian channel and decoder's CM knowledge (*informed decoder*), is

$$\Lambda = \sum_{n=1}^{N} (C'(n) - C(n))\,\pi(n) \;\Rightarrow\; \tilde{b} = \begin{cases} 0 & \text{if } \Lambda \geq 0 \\ 1 & \text{otherwise} \end{cases} \quad (6)$$

It is easy to show that for a Gaussian reference sequence $\pi = (\pi(n))_{n=1}^{N}$ the error probability of the decision rule (6) is

$$P_e = Q\left(\sqrt{\frac{N}{\eta_W + 2}}\right) \leq \exp\left(-\frac{N}{2(\eta_W + 2)}\right) \quad (7)$$

where $Q : x \mapsto Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} e^{-\frac{u^2}{2}}\, du$. If $\eta_W >> 1$ (which is a rather common situation in SG systems) both security and reliability can be pooled together in one expression:

$$P_e = Q\left(1.29\,(ND)^{\frac{1}{4}}\right) \leq \exp\left(-0.83\,(ND)^{\frac{1}{2}}\right). \quad (8)$$

From (8) there follows that for any security level D there can be chosen an appropriate N such that the SG system provides any given reliability P_e.

But this apparent good design of the SG system has one defect. Namely, if one wants to embed many secret bits into the CM in such a way that they can be reliably decoded by a legal user, it is necessary to increase the parameter η_W and this may not be possible in practical implementation. In order to see sharply this negative property, let us consider the following:

Example 1: Let $D = 0.1$ (that provides an acceptable level of security) and let $m = 10$ be the number of secure embedded bits. For multiple bit embedding, (8) should be posed as

$$P_e \leq \exp\left(-0.83\,\frac{(ND)^{\frac{1}{2}}}{m}\right). \quad (9)$$

Let us choose then $N = 10^5$. From (9), the probability of error is bounded as $P_e \leq 2.5 \times 10^{-4}$ which is acceptable. But $\eta_W = 600$, by (5). Now, if the CM signal-to-noise ratio has been taken also within an acceptable, say $\frac{\sigma_C^2}{\sigma_\varepsilon^2} = 10^2$, where $\sigma_C^2 = \mathrm{Var}\left((C(n))_{n=1}^{N}\right)$, then $\frac{\sigma_\varepsilon^2}{\sigma_W^2} = 6 \times 10^4$ which is indeed unacceptable for the most practical digital applications.

In order to overskip this unfortunate situation, we propose in section 2 the so called *spread-time stegosystem* (STS). The security and reliability of STS are proved in that section jointly with an optimization of parameters. An improvement of the cost of using error correcting codes is also given there. Section 3 presents the results of STS simulation for digital audio signal with a CM in the WAV format. Section 4 consists of some conclusions and open problems in this direction.

II. Description of STS and its performance evaluation

Let us consider initially an uncoded stegosystem. Let us embed secret bits b as a random modification of the embedding rule (1), namely, $\forall n = 1, \ldots, N$:

$$\begin{array}{rcl} \Pr\left[C_W(n) = C(n) + (-1)^b \sigma_W \pi(n)\right] & = & P_0 \\ \Pr\left[C_W(n) = C(n)\right] & = & 1 - P_0 \end{array} \quad (10)$$

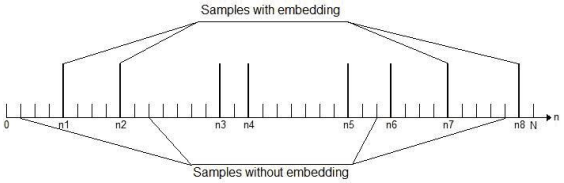

Fig. 1. Pseudorandom samples for STS system embedding, with $N_s = 8$, $N = 38$, $P_0 = 8/38 = 4/19$.

In practical implementation of the modified embedding rule (10), we can simply use a pseudorandom subsequence of samples. Let $(n_m)_{m=1}^{N_s}$ be an increasing sequence of indexes, $N_s \leq N$, generated also as a secret stegokey K, determining the samples in which the WM's are to be embedded (see Fig. 1). Then for a large value of N we may assume that $P_0 = N_s/N$. For uncoded SG, the same secret bit b is used at N_0 consecutive chosen samples for embedding. Hence the total number of secret bits embedded into N_0 samples for STS is $N_t = N_s/N_0$. Any legal user should know the stegokey K, hence he knows exactly the samples with embedding, and is able to extract one-by-one all the N_t secret bits using the decision rule (6). The error probability can be found by (7) (by considering the N appearing there as the current N_0).

An attacker A ignores the stegokey and hence the samples with the WM embedding. In order to take a decision about presence or absence of the SG system under the condition of a known $C = (C(n))_{n=1}^{N}$, the attacker A has to perform a testing of two hypothesis. Let

$$\delta = (\delta(n) = C'_W(n) - C(n))_{n=1}^{N} \quad (11)$$

and $\sigma_s^2 = \sigma_\varepsilon^2 + \sigma_W^2$. Then the two hypothesis to be tested are:

$$H_0 : \left[\delta \in \mathrm{N}(0, \sigma_\varepsilon^2) \text{ and is an i.i.d}\right] \quad (12)$$

$$H_1 : \begin{cases} \Pr\left(\delta \in \mathrm{N}(0, \sigma_s^2) \text{ and is an i.i.d}\right) = P_0 \\ \Pr\left(\delta \in \mathrm{N}(0, \sigma_\varepsilon^2) \text{ and is an i.i.d}\right) = 1 - P_0 \end{cases} \quad (13)$$

The hypothesis testing can be done using the *maximum likelihood ratio*

$$\Lambda\left(\Lambda_1 | \Lambda_0\right) = \frac{P\left(\delta | H_1\right)}{P\left(\delta | H_0\right)}$$

where $P\left(\delta | H_j\right)$ is the probability distribution of the random variables $(\delta(n))_{n=1}^{N}$ under the condition that hypothesis H_j is valid, $j = 0, 1$. Namely, the *optimal hypothesis testing* based on maximum likelihood ratio [3] is

$$\begin{array}{rcl} \Lambda\left(\Lambda_1 | \Lambda_0\right) \geq \lambda & \Longrightarrow & H_1 \\ \Lambda\left(\Lambda_1 | \Lambda_0\right) < \lambda & \Longrightarrow & H_0 \end{array} \quad (14)$$

where λ is some fixed threshold. By substituting into (14) the probability distributions (12)-(13) we get after simple transforms

$$\Lambda\left(\Lambda_1 | \Lambda_0\right) = \prod_{n=1}^{N} \left[P_0 \sqrt{\frac{\sigma_\varepsilon^2}{\sigma_s^2}} \exp\left(\frac{\sigma_W^2}{2\sigma_s^2 \sigma_\varepsilon^2} \delta(n)^2\right) + (1 - P_0)\right]$$

By changing λ in (14), it is possible to pass to the logarithmic likelihood ratio, $\Lambda_L(\Lambda_1|\Lambda_0) = \log\Lambda(\Lambda_1|\Lambda_0)$, and it equals

$$\sum_{n=1}^{N}\log\left[P_0\sqrt{\frac{\sigma_\varepsilon^2}{\sigma_s^2}}\exp\left(\frac{\sigma_W^2}{2\sigma_s^2\sigma_\varepsilon^2}\delta(n)^2\right)+(1-P_0)\right] \quad (15)$$

The application of the transformed decision rule based on $\Lambda_L(\Lambda_1|\Lambda_0)$ using (15) is rather hard. We will consider it again something later.

But so far let us consider a suboptimal decision rule based on some further reasonable conditions. First of all let us assume, in line with a good security guarantee, $\sigma_W^2 << \sigma_\varepsilon^2$. Then, a normalization of (15) expresses $\Lambda_L(\Lambda_1|\Lambda_0)$ as

$$\frac{1}{N}\sum_{n=1}^{N}\log\left[P_0\exp\left(\frac{1}{2\eta_W^2\sigma_\varepsilon^2}\delta(n)^2\right)+(1-P_0)\right] \quad (16)$$

The series expansion of $x\mapsto\log(1+x)$ up to its linear term produces

$$\Lambda_L(\Lambda_1|\Lambda_0) = P_0\left[\sum_{n=1}^{N}\exp\left(\frac{1}{2\eta_W^2\sigma_\varepsilon^2}\delta(n)^2\right)-N\right].$$

The series expansion of $x\mapsto\exp(x)$ up to its linear term renders the following decision rule:

$$\left[\tilde{\Lambda}\geq\tilde{\lambda}\implies H_1\right] \quad ; \quad \left[\tilde{\Lambda}<\tilde{\lambda}\implies H_0\right] \quad (17)$$

where $\tilde{\Lambda} = \frac{1}{N}\sum_{n=1}^{N}\delta(n)^2$ and $\tilde{\lambda}$ is some new threshold. The decision rule (17) is sufficiently reasonable because $E[\delta^2|H_1] > E[\delta^2|H_0]$ as we will show later.

Let us estimate the missing and false alarm probabilities, P_m and P_{fa} respectively, for the hypothesis H_1 (presence of the SG system) against hypothesis H_0 (absence of the SG system) under the decision rule given by (17).

For enough large N, by the Central Limit Theorem [4], $\tilde{\Lambda}\in\mathrm{N}(\mu_j,\sigma_j^2)$ for H_j, where $\mu_j = E[\tilde{\Lambda}|H_j]$ and $\sigma_j^2 = \mathrm{Var}\left(\tilde{\Lambda}|H_j\right)$, for $j=0,1$. Since $\sigma_1^2>\sigma_0^2$ we get:

$$P_m \geq \frac{1}{\sqrt{2\pi\sigma_0^2}}\int_{-\infty}^{\tilde{\lambda}}\exp\left(-\frac{(x-\mu_1)^2}{2\sigma_0^2}\right)dx \quad (18)$$

$$P_{fa} \geq \frac{1}{\sqrt{2\pi\sigma_0^2}}\int_{\tilde{\lambda}}^{+\infty}\exp\left(-\frac{(x-\mu_0)^2}{2\sigma_0^2}\right)dx \quad (19)$$

Let us select the threshold $\tilde{\lambda}$ in such a way that the condition $P_m = P_{fa} = P$ is fulfilled. After simple transforms of eq's (18)-(19) it is obtained

$$P\geq Q\left(\frac{\mu_1-\mu_0}{2\sigma_0}\right). \quad (20)$$

Necessarily the following identities should hold:

$$\mu_0=\sigma_\varepsilon^2\ ;\ \mu_1=\sigma_\varepsilon^2+P_0\sigma_W^2\ ;\ \sigma_0^2=\frac{2}{N}\sigma_\varepsilon^4. \quad (21)$$

By substituting (21) into (20), we get

$$P\geq Q\left(\sqrt{\frac{N}{2}}\frac{P_0}{2\eta_W}\right),$$

N	η_W	N_0	N_s	m	$P_0=\frac{N_s}{N}$
10^4	20	210	1431	6	0.1431
	50	496	3578	7	0.3578
	100	973	7156	7	0.7156
10^5	20	210	4526	21	0.04526
	50	496	11310	22	0.1131
	100	973	22630	23	0.2263
10^6	20	210	14310	68	0.01431
	50	496	35780	72	0.03578
	100	973	71560	73	0.07156
10^7	20	210	45260	215	0.004526
	50	496	113100	228	0.01131
	100	973	226300	232	0.02263

TABLE I
SETS OF PARAMETERS FOR STS PROVIDING $P_0\geq 0.4$ AND $P_e\leq 10^{-3}$ GIVEN DIFFERENT VALUES OF N AND η_W.

or equivalently,

$$P\geq Q\left(\frac{N_s}{2\sqrt{2N}\eta_W}\right),$$

where, as introduced at the beginning of the current section, N_s is the number of samples with embedding. Consequently if asymptotically $N_s\sim\sqrt{N}$, then $P\sim\frac{1}{2}$ and an undetectable stegosystem results.

In order to embed m secret bits into N_s samples, $N_0=\frac{N_s}{m}$ samples should be selected for embedding each bit. Then the error probability P_e after extraction of one bit by a legal informed decoder is expressed by (7) (with N_0 playing the role of N). It is necessary to note that in order to extract the secret bits, the legal decoder has to be synchronized with both the reference sequence π, appearing in relation (1), and the pseudorandom sequence determining the samples with embedding.

In Table I we show the calculation results for some values of parameters N_s, N_0, m, P_0 providing $P_e\leq 10^{-3}$ and $P\geq 0.4$, given some values of N and η_W. For enough large N, it is possible to provide a good undetectability ($P_0\geq 0.4$) and reliability ($P_e\leq 10^{-3}$) of the STS and embed up to 232 secure bits.

In order to improve the STS efficiency it is possible to use *coded STS*. Then an embedding procedure such as (10) has to be replaced as follows: Given a CM $C=(C(n))_{n=1}^N$, let $C_W=(C_W(n))_{n=1}^N$ be such that for each sample index n_j with embedding

$$\begin{aligned}\Pr\left[C_W(n_j)=C(n_j)+(-1)^{b_{ij}}\sigma_W\pi(n_j)\right] &= P_0\\ \Pr\left[C_W(n_j)=C(n_j)\right] &= 1-P_0\end{aligned}$$

where b_{ij} is the j-th bit in the i-th codeword of length $N_0=N_s/\ell$, with ℓ a positive integer value.

We will restrict our attention to binary linear systematic (N_0,k,d)-codes, varying i in the interval $\{1,2,\cdots,2^k-1,2^k\}$, with d the minimal code distance. In this setting the informed decoder takes a decision about the

embedding of the i-th codeword by making

$$i = \arg\max_{1\le i'\le 2^k} \sum_{j=1}^{N_0} \left(C'_W(n_j) - C(n_j)\right)(-1)^{b_{i'j}}\pi(n)$$

The total number of secure embedded bits is $m = k\ell$ and the block-error probability P_{be}, based on well known union bound [5], can be expressed as

$$\begin{aligned} P_{be} &\le (2^k - 1)\, Q\left(\sqrt{\frac{d}{2+\eta_W}}\right) \\ &\le \exp\left(-\frac{d}{2(2+\eta_W)} + R\, N_0 \ln 2\right) \end{aligned}$$

Since signal-to-noise ratio η_W^{-1} is typically small, we will restrict our consideration only to two classes of linear error correcting codes: the simplex codes (SC) and the Reed-Muller codes (RMC) [5]. For the first class the main parameters are $N_0 = 2^\nu - 1$, $k = \nu$, $d = 2^{\nu-1}$, $R = \frac{\nu}{N_0}$, where ν is some integer; whereas for the second class: $N_0 = 2^\nu$, $k = \sum_{i=1}^{r}\binom{\nu}{i}$, $d = 2^{\nu-r}$, where $\nu \ge 3$ and r is an integer, the so called *order of the* RMC.

Now we can fix the total number of samples N, the security level P, the block-error probability P_{be}, the parameter η_W and then to optimize the code parameters N_0, ν and r in order to provide the maximum possible number m of secure and reliable embedded bits.

Example 2: Let us take $N = 10^7$, $P \ge 0.4$, $P_{be} \le 10^{-3}$, $\eta_W = 20$. Then we get for the class of SC the optimal parameters $\nu = 10$, $k = 10$, the total number of secret bits $m = k\frac{N_s}{N_0} = 442$. If we require more reliable extraction then we get, for the class of RM codes, the optimal parameters $\nu = 14$, $r = 2$, $k = 105$ and for the same restrictions $P \ge 0.4$, $\eta_W = 20$, the total number m of embedded secret bits is about 290 with $P_{be} \le 10^{-9}$. So, we can conclude that the use of error correcting codes results in either an increment in the number of secure embedded bits or in an improvement of reliability.

Let us find out whether the use of the optimal decision rule (16) can provide an appreciable improvement of STS detecting in comparison with the suboptimal decision rule (17).

Since N is sufficiently large, we can apply the Central Limit Theorem to the sum in (16). Then similar to the proof of (20) we get for such a choice of the threshold λ, which provides $P_m = P_{fa} = P$ the following upper bound

$$P \ge Q\left(\frac{\tilde\mu_1 - \tilde\mu_0}{2\tilde\sigma_0}\right) \tag{22}$$

where, for $j = 0, 1$,

$$\tilde\mu_j = E\left[\left(\log\left(P_0 \exp\left(\frac{\delta(n)^2}{2\eta_W\sigma_\varepsilon^2}\right) + (1 - P_0)\right)\right)_{n=1}^{N}\middle| H_j\right]$$

and

$$\begin{aligned} \tilde\sigma_0 &= \frac{1}{N}\mathrm{Var}\left((s(n))_{n=1}^{N}\middle| H_j\right) \\ &= \frac{1}{N}\left(E\left[\left((s(n))^2\right)_{n=1}^{N}\middle| H_j\right] - \tilde\mu_0^2\right) \end{aligned}$$

η_W	N_0	P_e	$\tilde P_e$
20	210	$5.0\cdot 10^{-4}$	0.001
50	496	$6.0\cdot 10^{-4}$	0.001
100	973	$5.5\cdot 10^{-4}$	0.001

TABLE III
THE RESULTS OF CALCULATIONS FOR THE ERROR PROBABILITY P_e OBTAINED AFTER DECODING BY RULE (6) AND THE THEORETICAL ERROR PROBABILITY $\tilde P_e$ CALCULATED BY EQ. (7), WITH $N = N_0$ FOR DIFFERENT PARAMETERS η_W AND N_0.

where

$$s(n) = \log\left(P_0 \exp\left(\frac{\delta(n)^2}{2\eta_W\sigma_\varepsilon^2}\right) + (1 - P_0)\right)$$

and the random values $\delta(n)$ have the probability distributions given by (11). Since it is very hard to find analytically the values $\tilde\mu_0$, $\tilde\mu_1$ and $\tilde\sigma_0$, we will estimate them just by the simulation of the above described procedure.

In Table II there are presented the simulation results for $\tilde\mu_0$, $\tilde\mu_1$ and $\tilde\sigma_0$ and the calculation of P by (22) for typical values of σ_ε^2, η_W and P_0. It can be seen that the use of the optimal decision rule does not break undetectability of STS, hence it can be declared as a secure SG system indeed.

III. SIMULATION OF STS FOR AUDIO COVER MESSAGES

We use an audio music file in format WAV where the sample frequency is 44.1 kHz with duration about 29 sec. The CM signal-to-noise ratio η_c has been taken as 10 dB, whereas watermark-to-noise ratio (WNR) η_W^{-1} was 20 dB. The embedding rule was taken as (10), where $P_0 = 0.1$. In Fig. 2 the wave forms of the original audio signal, audio signal after passing over a noisy channel and after secret message embedding are presented at the same time interval. One can see that the noise corrupts slightly the audio signal and this fact can also be appreciated by human ear, whilst, at the same time, the embedding procedure is not observable.

Moreover, in Fig. 3 the waveforms of channel noise are shown, as well as this noise after embedding with straining in time confirming this fact. (Of course we do not claim that the impossibility to detect the SG system either by ear or by eye, is enough to prove its security by the best statistical methods. We have proved indeed this fact in the previous section).

In Table III we present the results of simulation for the error probability P_e versus the block length N_0 and η_W. The error probability $\tilde P_e$ calculated by eq. (7) is also presented in this Table. There, we can see that the reliability of STS obtained by simulation is even better than the theoretical estimated bound.

IV. CONCLUSIONS

In the current paper we proposed some modification of the stegosystem based on noisy channel called spread-time stegosystem (STS). The goal of the STS is to provide such a WNR able to be implemented in practice, especially with digital cover messages. We prove that both STS security

N	σ_ε^2	η_W	$P_0 = \frac{N_s}{N}$	$\tilde{\mu}_0$	$\tilde{\mu}_1$	$\tilde{\sigma}_0$	$P = Q\left(\frac{\tilde{\mu}_1 - \tilde{\mu}_0}{2\tilde{\sigma}_0}\right)$
10^4	1	20	0.1431	0.00161414	0.00162667	0.00240398	0.401753
		50	0.3578	0.00157674	0.00158801	0.00229017	0.401759
		100	0.7156	0.00156462	0.00157585	0.00225445	0.401737
	5	20	0.1431	0.00161414	0.00162590	0.00240398	0.401754
		50	0.3578	0.00157675	0.00158821	0.00229017	0.401745
		100	0.7156	0.00156462	0.00157583	0.00225445	0.401726
10^5	1	20	0.04526	0.000512618	0.000513737	0.000767001	0.401741
		50	0.1131	0.000500332	0.000501449	0.000729712	0.401809
		100	0.2263	0.000496672	0.000497830	0.000718483	0.401737
	5	20	0.04526	0.000512618	0.000513854	0.000767001	0.401772
		50	0.1131	0.000499062	0.000500277	0.000727769	0.401806
		100	0.2263	0.000496672	0.000497795	0.000718483	0.401745
10^6	1	20	0.01431	0.000162288	0.000162393	0.000243341	0.401835
		50	0.03578	0.000158479	0.000158585	0.000231440	0.401862
		100	0.07156	0.000157686	0.000157808	0.000228397	0.401548
	5	20	0.01431	0.000162288	0.000162435	0.000243187	0.401752
		50	0.03578	0.000158479	0.000158598	0.00023144	0.401711
		100	0.07156	0.000157686	0.000157797	0.000228397	0.401461
10^7	1	20	0.004526	$5.13502 \cdot 10^{-5}$	$5.13615 \cdot 10^{-5}$	$7.69844 \cdot 10^{-5}$	0.401964
		50	0.01131	$5.01145 \cdot 10^{-5}$	$5.01246 \cdot 10^{-5}$	$7.32173 \cdot 10^{-5}$	0.401900
		100	0.02263	$4.97464 \cdot 10^{-5}$	$4.97587 \cdot 10^{-5}$	$7.20836 \cdot 10^{-5}$	0.401777
	5	20	0.004526	$5.13502 \cdot 10^{-5}$	$5.13626 \cdot 10^{-5}$	$7.69844 \cdot 10^{-5}$	0.401812
		50	0.01131	$5.01145 \cdot 10^{-5}$	$5.01245 \cdot 10^{-5}$	$7.32173 \cdot 10^{-5}$	0.401969
		100	0.02263	$4.97464 \cdot 10^{-5}$	$4.97569 \cdot 10^{-5}$	$7.20836 \cdot 10^{-5}$	0.401686

TABLE II
RESULTS OF SIMULATIONS FOR VALUES OF $\tilde{\mu}_0$, $\tilde{\mu}_1$ AND $\tilde{\sigma}_0$ VERSUS TYPICAL VALUES OF σ_ε^2, η_W AND P_0.

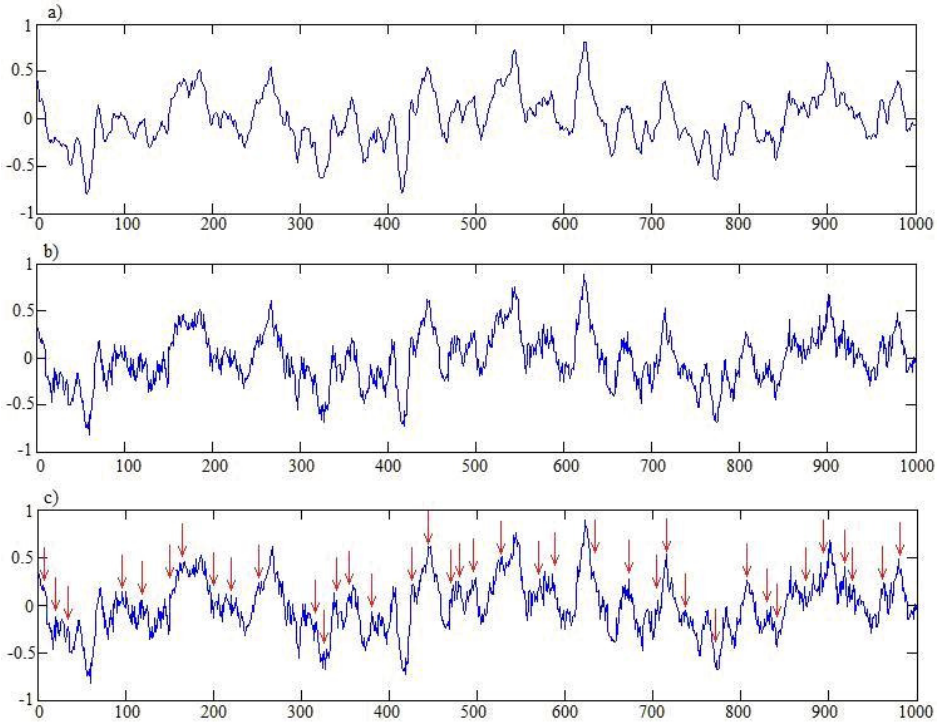

Fig. 2. (a) The waveforms of audio signal, (b) audio signal after its passing over noisy channel with CM signal-to-noise ratio $\eta_c = 10$dB, and (c) after embedding by STS algorithm with $WNR = 20$dB. The arrows show the samples with embedding.

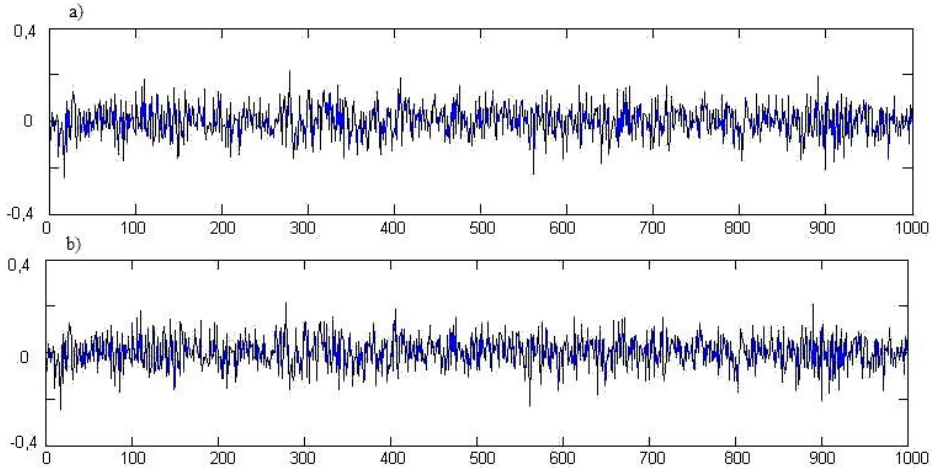

Fig. 3. (a) The waveform of channel noise and (b) the same channel noise after embedding according to rule (10).

and reliability of secure bit extraction can be provided by an appropriate selection of the system parameters. The main defect of the proposed stegosystem is its low embedding rate which entails longer times for the embedding of a limited number of secret bits. The used error correcting codes improve this situation but only slightly. However this is a generic property "sacrificed on the altar of undetectability" and an attacker's knowledge of the CM.

We show that the suboptimal SG system detection (see eq. (17) is practically as much efficient as the optimal (based on the maximum likelihood ratio). Simulation of the STS with audio CM shows that its detection by ear and eye is impossible, whereas the embedded bits can be extracted reliably.

The first of open problems which we are going to consider in the near future is to specify security of STS for digital CM and after saving the stegosignal in digital formats. The second problem considers an extraction of secret bits by a blind decoder (in particular using the improved spread spectrum modulation [6]) while keeping a good undetectability of STS.

ACKNOWLEDGMENT

Dr. Morales-Luna acknowledges the support of Mexican Conacyt.

REFERENCES

[1] V. Korjik, M. H. Lee, and G. Morales-Luna, "Stegosystems based on noisy channels," in *Proc. IX Spanish Meeting on Cryptology and Information Security*. Univ. Aut. Barcelona, 2006, pp. 379–387.

[2] C. Cachin, "An information-theoretic model for steganography," in *International Workshop on Information Hiding 1998*. Springer LNCS, 1998, pp. 306–318.

[3] B. van der Waerden, *Mathematische Statistik*. Springer, 1957.

[4] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. Mc-Graw Hill, 1984.

[5] F. J. Macwilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, ser. North-Holland Mathematical Library. North Holland, January 1983. [Online]. Available: http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20&path=ASIN/0444851933

[6] H. S. Malvar and D. Florêncio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. on Signal Processing*, vol. 51, no. 4, pp. 898–905, 2001.