УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 5-17

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СОКРЫТИЯ ИНФОРМАЦИИ ДЛЯ СИСТЕМ С ЗАШУМЛЕННЫМИ КАНАЛАМИ СВЯЗИ

И.И. Маракова[1], **А.А. Яковенко**[2]

[1] Telecom Bretagne,
Technopôle Brest-Iroise, CS 83818, 29238 Brest Cedex 3, France; e-mail: marakova.irina@gmail.com
[2] Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: iakovenko.oleksandr@gmail.com

Рассматривается система передачи сокрытой информации по зашумленным каналам связи и сценарий, при котором атакующая сторона не имеет другого доступа к стеганосигналу, кроме как в гауссовом канале. При таком подходе требуется обеспечить практически недостижимую на практике величину отношения сигнал/шум, особенно с учетом того, что покрывающее сообщение может быть известно атакующей стороне. Для решения этой проблемы предлагается использовать стеганосистему с разнесением по времени (СРВ). Доказана возможность построения СРВ с заданным уровнем секретности и надежности восприятия сокрытого сигнала. Рассмотрены вопросы оптимизации параметров на основе использования кодов коррекции ошибок. Представлены результаты моделирования при помощи реализации СРВ для покрывающих сообщений в виде цифровых звуковых файлов формата WAV.

Ключевые слова: стеганосистема, покрывающее сообщение, коды коррекции ошибок, гауссовский канал с шумами, относительная энтропия

Введение

Стеганография – это техника сокрытия информации, позволяющая добавить скрытую информацию в не вызывающее подозрения покрывающее сообщение (аудио-, видеоинформация и т.д.) при условии, что покрывающее сообщение (ПС) не искажается до такой степени, что может сделать заметным наличие в стеганосигнале дополнительной информации.

Для обеспечения устойчивости к статистическим атакам необходимо обеспечить идентичность вероятностных мер ПС и стегосигнала на некотором временном дискрете. Но для реализации этого принципа разработчик стегосистемы должен, по меньшей мере, владеть информацией о статистике ПС, т.е. реального аудио или видеосигнала, что само по себе является довольно сложной задачей. С целью решения этой проблемы и было предложено построение стегосистемы на основе каналов с зашумлением [1].

Известно направление развития методов передачи конфиденциальной информации по незащищенным каналам связи с шумом при достаточно низкой сложности реализации и малых финансовых затрат, гарантирующее сколь угодно малую вероятность успешного перехвата и сколь угодно малую вероятность ошибки в канале легитимных пользователей [2]. Применение данного подхода в стеганографии может быть оправдано только при наличии естественного зашумленного канала и только в том случае, когда атакующая сторона не имеет другого доступа к стегосигналу, кроме как в зашумленном канале. Суть атаки заключается в выявлении сокрытого сообщения на

основе анализа вероятностных мер перехваченного сигнала. Необходимо отметить, что такая модель является более жесткой, чем стандартная стеганосистема, для которой ПС в большинстве случаев является известным. Таким образом, проблема стеганоанализа сводится к выделению из канального шума внедренного скрытого сообщения. Так как распределение шума в канале, как правило, известно намного лучше, чем статистика ПС, проблема разработки стегосистемы упрощается.

В статье рассматривается только гауссовский канал [1]. Если для стегосистемы информационную ценность представляют как ПС, так и скрываемая информация, т.е. внедряемая информация является цифровым водяным знаком (ЦВЗ), то внедрение бита информации может быть реализовано как:

$$\forall n = 1,\ldots,N : C_W(n) = C(n) + (-1)^b \sigma_W \pi(n), \tag{1}$$

где

$C = (C(n))_{n=1}^N$ – ПС;

$\pi = (\pi(n))_{n=1}^N$ – независимые одинаково распределенные по закону Гаусса псевдослучайные величины с нулевым средним значением и единичной дисперсией;

N – длина обеих последовательностей;

σ_W – дисперсия ЦВЗ.

На выходе гауссовского канала получим:

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

где $\varepsilon = (\varepsilon(n))_{n=1}^N$ – независимый одинаково распределенный по закону Гаусса шум с нулевым средним значением и дисперсией σ_ε^2.

Как было показано, относительная энтропия для данной модели стегосистемы даже в случае известного ПС может быть представлена [1], [3] как:

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

где $\eta_W = \sigma_\varepsilon^2 / \sigma_W^2$ – отношение дисперсий гауссовского шума и ЦВЗ.

Для того чтобы надежно спрятать секретную информацию в шуме канала, отношение η_W должно быть большим [3]. Следовательно, относительная энтропия (2) приближенно равна

$$D \approx 0.36\frac{N}{\eta_W^2}. \tag{3}$$

Из теории информации известно, что инвариантно к методу статистического анализа должно выполняться неравенство:

$$P_{ЛД}\ln\frac{P_{ЛД}}{1-P_{ПС}} + (1-P_{ЛД})\ln\frac{1-P_{ЛД}}{P_{ПС}} \le D, \tag{4}$$

где

$P_{ЛД}$ – вероятность ложного детектирования стегосигнала,

$P_{ПС}$ – вероятность пропуска стегосигнала.

Допустим для простоты изложения, что $P_{ЛД} = P_{ПС} = P$. Тогда из (4) получаем

$$(2P-1)\ln\frac{P}{1-P} \le D.$$

Из (3) следует, что:

$$\eta_W = 0.6\sqrt{\frac{N}{D}}. \tag{5}$$

Оптимальным правилом принятия решения о наличии/отсутствии сокрытого бита b для гауссовского канала и информированного декодера, т.е. такого декодера, которому известно ПС, является:

$$\Lambda = \sum_{n=1}^{N}\left(C'(n)-C(n)\right)\pi(n) \Rightarrow \widetilde{b} = \begin{cases} 0, \text{ если } \Lambda \ge 0 \\ 1, \text{ в противном случае} \end{cases}. \tag{6}$$

Нетрудно показать, что для гауссовской последовательности $\pi = (\pi(n))_{n=1}^{N}$ вероятность принятия неправильного решения (6) имеет следующий вид:

$$P_{ош} = \Phi\left(\sqrt{\frac{N}{\eta_W + 2}}\right) \le \exp\left(-\frac{N}{2(\eta_W+2)}\right), \tag{7}$$

где $\Phi : x \mapsto \Phi(x) = \frac{1}{\sqrt{2\pi}}\int_x^{+\infty} e^{-\frac{u^2}{2}}du$.

Если $\eta_W >> 1$, что является довольно обычным для стеганосистем, то требование к секретности сводится к следующему выражению:

$$P_{ош} = \Phi\left(\sqrt{\frac{N}{\eta_W + 2}}\right) \le \exp\left(-0.83(ND)^{\frac{1}{2}}\right). \tag{8}$$

Из (8) следует важный вывод, что для любого уровня надежности восприятия и значения D может быть выбрано значение N, обеспечивающее требуемый уровень секретности, т.е. заданное значение $P_{ош}$.

При практической реализации данного подхода очевидно следующее противоречие. Для уменьшения вероятности ошибки извлечения ЦВЗ легальным пользователем, необходимо увеличить параметр η_W, что неизбежно ведет к увеличению искажений стегосигнала, т.е. уменьшению надежности восприятия. Для устранения данного противоречия и применяется так называемая стеганосистема с разнесением по времени.

Далее будет приведено ее описание и рассмотрены возможности оптимизации ее параметров на основе применения кодов коррекции ошибок, а также представлены результаты симуляции для цифрового звукового сигнала формата WAV в качестве ПС.

Описание стеганосистемы и оценка ее эффективности

Для стегосистемы с разнесением по времени без кодирования (рис. 1) правило (1) внедрения секретных бит преобразуется к виду:

$$\Pr[C_W(n) = C(n) + (-1)^b \sigma_W \pi(n)] = P_0,$$
$$\Pr[C_W(n) = C(n)] = 1 - P_0. \quad (9)$$

Для практической реализации модифицированного правила внедрения (9) используемая псевдослучайная последовательность отсчетов может быть непосредственно секретным ключом (СК) или может быть связана с СК по некоторому закону. Пусть $(n_m)_{m=1}^{N_s}$ – последовательность увеличивающихся индексов $(N_s \le N)$, определяющая номера отсчетов, в которые будет производиться внедрение стегосигнала (рис. 1). Для большого значения N, с учетом центральной предельной теоремы, $P_0 = N_s / N$. При отсутствии кодирования для внедрения секретного бита b используется N_0 последовательно выбранных дискретов для погружения ЦВЗ. Отсюда следует, что общее количество секретных бит составит $N_t = N_s / N_0$. Каждый легальный пользователь должен знать стеганоключ K, другими словами – номера отсчетов с внедренным ЦВЗ, и способен выделить по одному все N_t секретных бит, используя правило принятия решений (6). Вероятность ошибки может быть найдена из (7) путем подстановки в формулу текущего значения N_0 вместо N.

Атакующая сторона, при условии известного ПС, но при неизвестном СК, для принятия решения о наличии или отсутствии сокрытого сообщения должна выполнить статистический анализ и протестировать две гипотезы:

$$H_0 : [C''(n) \in N(0, \sigma_\varepsilon^2) \text{ и является ППС}], \quad (10)$$

$$H_1 : \begin{cases} \Pr[C''(n) \in N(0, \sigma_s^2) \text{ и является ППС}] = P_0, \\ \Pr[C''(n) \in N(0, \sigma_\varepsilon^2) \text{ и является ППС}] = 1 - P_0, \end{cases} \quad (11)$$

где

$C''(n) = (C'_W(n) - C(n))_{n=1}^{N}$;

$\sigma_s^2 = \sigma_\varepsilon^2 + \sigma_W^2$;

ППС – псевдослучайная последовательность некоррелированных чисел.

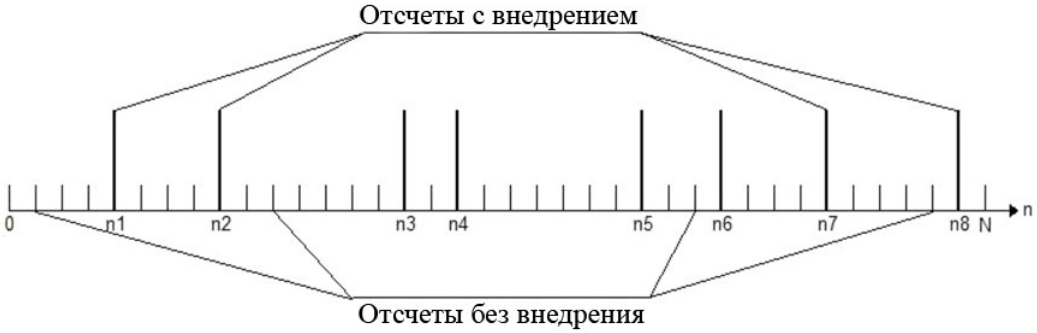

Рис. 1. Псевдослучайные отсчеты для СРВ, $N_s = 8,\ N = 38,\ P_0 = 4/19$

Проверка гипотез может осуществляться путем вычисления отношения максимального правдоподобия:

$$\Lambda\left(\Lambda_1|\Lambda_0\right)=\frac{P\left(C''(n)|H_1\right)}{P\left(C''(n)|H_0\right)}, \tag{12}$$

где $P\left(C''(n)|H_j\right)$ – вероятность распределения случайной величины $C''(n)$ для каждой из гипотез H_j, $j=0,1$. Проверка оптимальной гипотезы, основанной на отношении максимального правдоподобия (12), выглядит следующим образом:

$$\begin{aligned}&\Lambda\left(\Lambda_1|\Lambda_0\right)\geq\lambda\Rightarrow H_1,\\&\Lambda\left(\Lambda_1|\Lambda_0\right)<\lambda\Rightarrow H_0,\end{aligned} \tag{13}$$

где λ – некоторый фиксированный порог. Подставив в (13) распределения вероятности (10), (11), получим после простых преобразований:

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

или для логарифмического масштаба

$$\Lambda_L\left(\Lambda_1|\Lambda_0\right)=\log\Lambda\left(\Lambda_1|\Lambda_0\right)=\sum_{n=1}^{N}\log\left[P_0\sqrt{\frac{\sigma_\varepsilon^2}{\sigma_s^2}}\exp\left(\frac{\sigma_W^2}{2\sigma_s^2\sigma_\varepsilon^2}\left(C''(n)\right)^2\right)+\left(1-P_0\right)\right]. \tag{14}$$

Применение на практике полученного правила принятия решений (14) довольно сложно. Рассмотрим подоптимальное правило принятия решений в случае выполнения условия $\sigma_W^2<<\sigma_\varepsilon^2$. При этом (14) преобразуется к виду

$$\frac{1}{N}\sum_{n=1}^{N}\log\left[P_0\exp\left(\frac{1}{2\eta_W^2\sigma_\varepsilon^2}\left(C''(n)\right)^2\right)+\left(1-P_0\right)\right]. \tag{15}$$

При $x\mapsto\log(1+x)$ получим:

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

и правило принятия решений:

$$[\widetilde{\Lambda}\geq\widetilde{\lambda}\Rightarrow H_1];\qquad[\widetilde{\Lambda}<\widetilde{\lambda}\Rightarrow H_0], \tag{16}$$

где

$\widetilde{\Lambda}=\frac{1}{\mathrm{N}}\sum_{n=1}^{N}\left(C''(n)\right)^2$;

$\widetilde{\lambda}$ – некий новый порог.

Правило принятия решений (16) достаточно обосновано, поскольку, как будет показано далее $M[(C''(n))^2|H_1] > M[(C''(n))^2|H_0]$, где M – математическое ожидание.

Рассмотрим аналитическую оценку вероятностей ошибок первого и второго рода, $P_{ПС}$ и $P_{ЛД}$ соответственно, для гипотезы H_1 (наличие стегосигнала) и гипотезы H_0 (отсутствие стегосигнала) при использовании правила принятия решений (16).

Для достаточно больших N, согласно центральной предельной теореме [3], $\tilde{\Lambda} \in N(\mu_j, \sigma_j^2)$ для H_j, где $\mu_j = M[\tilde{\Lambda}|H_j]$, и $\sigma_j^2 = Var(\tilde{\Lambda}|H_j)$, для $j = 0,1$. Так как $\sigma_1^2 > \sigma_0^2$, получим:

$$P_{ПС} \geq \frac{1}{\sqrt{2\pi\sigma_0^2}} \int_{-\infty}^{\tilde{\lambda}} \exp\left(-\frac{(x-\mu_1)^2}{2\sigma_0^2}\right) dx, \tag{17}$$

$$P_{ЛД} \geq \frac{1}{\sqrt{2\pi\sigma_0^2}} \int_{\tilde{\lambda}}^{+\infty} \exp\left(-\frac{(x-\mu_1)^2}{2\sigma_0^2}\right) dx. \tag{18}$$

Выберем порог $\tilde{\lambda}$ таким образом, чтобы выполнялось условие $P_{ПС} = P_{ЛД} = P$. После простых преобразований выражений (17) и (18), можно получить неравенство:

$$P \geq \Phi\left(\frac{\mu_1 - \mu_0}{2\sigma_0}\right) \tag{19}$$

при выполнении условий

$$\mu_0 = \sigma_\varepsilon^2; \quad \mu_1 = \sigma_\varepsilon^2 + P_0\sigma_W^2; \quad \sigma_0^2 = \frac{2}{N}\sigma_\varepsilon^4. \tag{20}$$

Подставив (20) в (19), получим:

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

или

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

Следовательно, если асимптотически $N_s \sim \sqrt{N}$, то $P \sim 1/2$, что приводит к невозможности обнаружения стегосигнала нелегитимным пользователем.

Для внедрения m секретных бит в N_s отсчетов необходимо выбрать $N_0 = \frac{N_s}{m}$ отсчетов для каждого бита секретного сообщения. В таком случае вероятность ошибки $P_{ош}$ после извлечения одного бита легальным информированным декодером определяется по (7) (с подстановкой N_0 вместо N). Необходимо заметить, что для того, чтобы выделить секретные биты, декодер легитимного пользователя должен быть синхронизирован как с последовательностью π в (1), так и с псевдослучайной

последовательностью, определяющей номера отсчетов, в которые производилось внедрение, т.е. СК.

В табл. 1 показаны результаты вычисления для некоторых значений параметров N_s, N_0, m и P_0, позволяющие достигнуть $P_{ош} \le 10^{-3}$ и $P \ge 0.4$, с заданными значениями N и η_W, отвечающими требованиям надежного восприятия. Для достаточно больших N становятся возможными высокая скрытность ($P \ge 0.4$) и устойчивость ($P_{ош} \le 10^{-3}$) СРВ при погружении до 232 бит защищенной информации.

Таблица 1.

Наборы параметров для СРВ, обеспечивающие $P_0 \ge 0.4$ и $P_{ош} \le 10^{-3}$ при разных значениях N и η_W

N	η_W	N_0	N_s	m	P_0
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

Для улучшения эффективности СРВ можно использовать СРВ с кодированием. Тогда процедура внедрения (9) должна быть модифицирована следующим образом. Для заданного ПС $C = (C(n))_{n=1}^{N}$ пусть $C_w = (C_W(n))_{n=1}^{N}$ и для каждого индекса n_j при внедрении стегосигнала будет выполняться

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

$$\Pr\left[C_W(n_j) = C(n_j)\right] = 1 - P_0,$$

где

b_{ij} – это *j*-й бит в *i*-ом кодовом слове длины $N_0 = N_s / \ell$,

ℓ – положительное целое число.

Для простоты изложения ограничимся рассмотрением бинарных линейных систематических (N_0, k, d)-кодов, изменяя i в интервале $\{1,2,\cdots,2^k - 1, 2^k\}$, где d – минимальное кодовое расстояние. Информированный декодер принимает решение о внедрении *i*-го кодового слова стеганосообщения, вычисляя

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

Полное количество внедренных бит $m = kl$, и вероятность ошибочного блока $P_{ОБ}$, основываясь на хорошо известной границе неравенства Буля [5], может быть выражена следующим образом:

$$P_{ОБ} \le \left(2^k - 1\right)\Phi\left(\sqrt{\frac{d}{2+\eta_W}}\right) \le \exp\left(-\frac{d}{2\left(2+\eta_W\right)} + RN_0 \ln 2\right).$$

Так как отношение сигнал/шум η_W^{-1} обычно мало, ограничимся лишь двумя классами линейных кодов коррекции ошибок: симплексными кодами (СК) и кодами Рида-Маллера (КРМ) [5]. Для первого класса основные параметры – $N_0 = 2^\nu - 1$, $k = \nu$, $d = 2^{\nu-1}$, $R = \frac{\nu}{N_0}$, где ν – некоторое целое число; для второго класса – $N_0 = 2^\nu$, $k = \sum_{i=1}^{r}\binom{\nu}{i}$, $d = 2^{\nu-r}$, где $\nu \ge 3$ и r – целое число, т.н. порядок КРМ.

Теперь можно зафиксировать полное количество отсчетов N, уровень защищенности P, вероятность ошибки в блоке $P_{ОБ}$, параметр η_W, а затем оптимизировать параметры кода N_0, ν и r с целью увеличения числа защищенных и достоверных бит.

Например, если задаться значениями $N = 10^7$, $P \ge 0.4$, $P_{ОБ} \le 10^{-3}$, $\eta_W = 20$, то оптимальными параметрами СК будут $\nu = 10$, $k = 10$, а общее число внедряемых секретных бит $m = k\frac{N_s}{N_0} = 442$.

Если требуется усилить надежность системы, можно использовать КРМ с оптимальными параметрами $\nu = 14$, $r = 2$, $k = 105$ и с теми же ограничениями $P \ge 0.4$, $\eta_W = 20$. В таком случае общее число внедренных секретных бит будет близко к 290 при $P_{ОБ} \le 10^{-9}$.

Таким образом, использование кодов коррекции ошибок позволяет увеличить число внедряемых защищенных бит и/или повысить секретность системы.

Определим, может ли правило принятия оптимального решения (14) обеспечить значительные улучшения при детектировании в СРВ по сравнению с субоптимальным правилом принятия решений (15).

Так как N значительно больше, можно применить центральную предельную теорему к сумме из (15). Тогда, аналогично доказательству выражения (19), можно получить такой критерий выбора порога λ, который позволяет достичь для $P_{ПС} = P_{ЛД} = P$ следующей верхней границы:

$$P \ge \Phi\left(\frac{\widetilde{\mu}_1 - \widetilde{\mu}_0}{2\widetilde{\sigma}_0}\right), \qquad (21)$$

где для $j = 0,1$

$$\widetilde{\mu}_j = M\left[\left(\log\left(P_0 \exp\left(\frac{\left(C''(n)\right)^2}{2\eta_W\sigma_\varepsilon^2}\right) + \left(1 - P_0\right)\right)\right)_{n=1}^{N} \middle| H_j\right]$$

и

$$\widetilde{\sigma}_0 = \frac{1}{N} Var\left(\left(s(n)\right)_{n=1}^{N} \middle| H_j\right) = \frac{1}{N}\left(M\left[\left(s^2(n)\right)_{n=1}^{N} \middle| H_j\right] - \widetilde{\mu}_0^2\right),$$

где $s(n) = \log\left(P_0 \exp\left(\frac{\left(C''(n)\right)^2}{2\eta_W \sigma_\varepsilon^2}\right) + \left(1 - P_0\right)\right)$, и случайные значения $C''(n)$ имеют вероятность распределения, приведенную в (10). Так как крайне сложно определить значения $\widetilde{\mu}_0$, $\widetilde{\mu}_1$ и $\widetilde{\sigma}_0$ аналитически, они будут оценены в результате симуляции описанной выше процедуры.

В табл. 2 представлены результаты симуляции для $\widetilde{\mu}_0$, $\widetilde{\mu}_1$ и $\widetilde{\sigma}_0$, а также результаты вычисления P из (21) для типичных значений σ_ε^2, η_W и P_0. Очевидно, что использование правила оптимального решения не нарушает секретность СРВ (P), следовательно, последняя может считаться защищенной стеганосистемой.

Таблица 2.

Результаты симуляции значений $\widetilde{\mu}_0$, $\widetilde{\mu}_1$ и $\widetilde{\sigma}_0$ в зависимости от типичных значений σ_ε^2, η_W и P_0

N	σ_ε^2	η_W	$P_0 = N_s / N$	$\widetilde{\mu}_0$	$\widetilde{\mu}_1$	$\widetilde{\sigma}_0$	$P = Q\left(\frac{\widetilde{\mu}_1 - \widetilde{\mu}_0}{2\widetilde{\sigma}_0}\right)$
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

Моделирование стеганосистемы с разнесением по времени для звукового покрывающего сообщения

Используется музыкальный аудиофайл в формате WAV с частотой дискретизации 44100 Гц длительностью около 29 секунд. Отношение ПС/шум η_c выбрано 10 дБ, в то время как отношение ЦВЗ/шум η_W^{-1} выбрано 20 дБ. Используется правило погружения (9), причем $P_0 = 0.1$. Зависимость интенсивности I аудио-сигнала от времени t представлена на рис. 2, где стрелками показаны отсчеты с внедрением. На основе сравнительного анализа видно, что шум слегка искажает аудиосигнал, также это заметно на слух, в то время как результат процедуры внедрения не заметен.

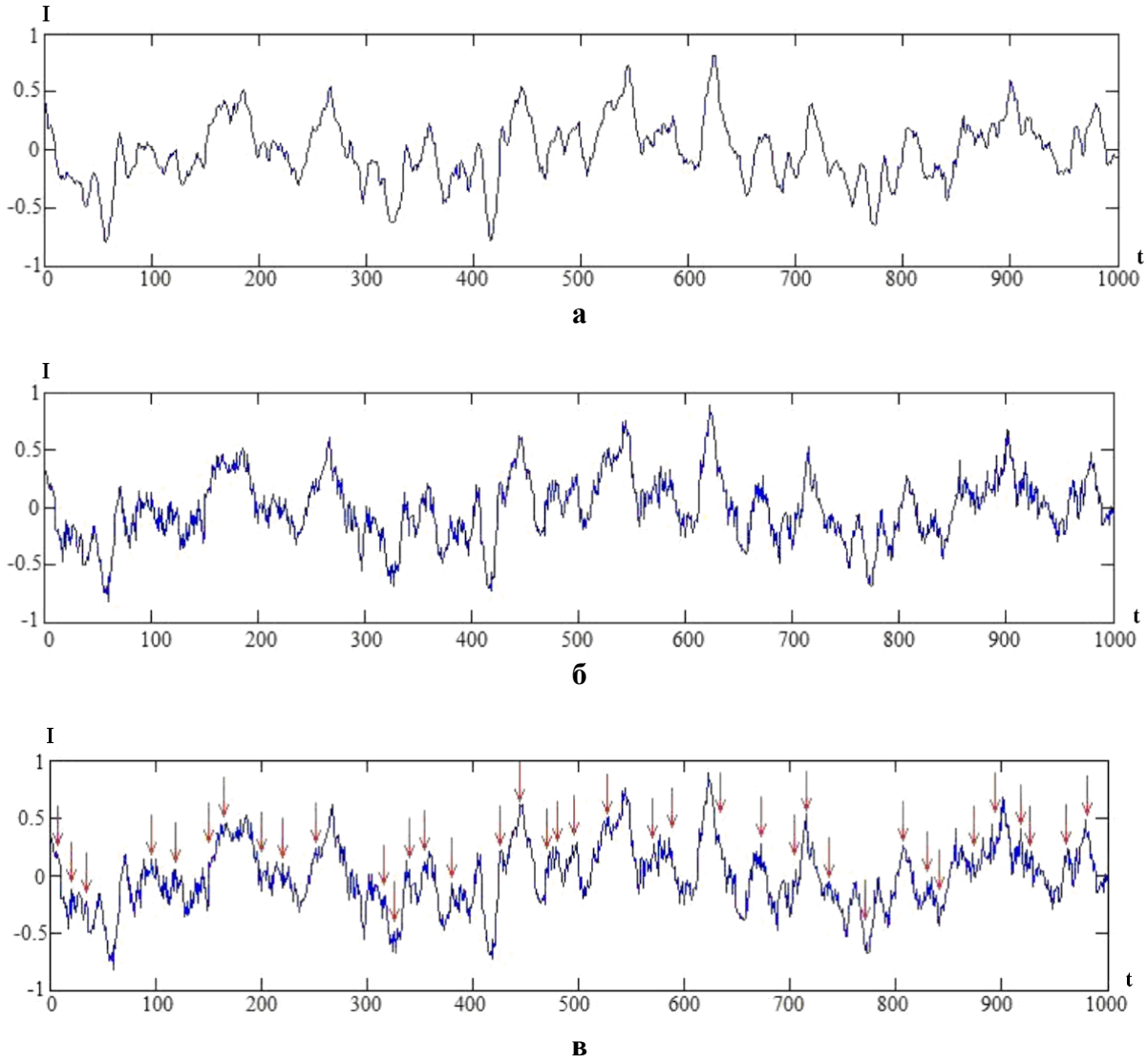

Рис. 2. Синограммы тестового аудиофайла: а – исходного; б –после прохождения по зашумленному каналу; в – после внедрения скрытого сообщения

На рис. 3 показаны синограммы шума в канале до и после внедрения стегано-сигнала. Конечно незаметность внедрения стегосигнала на слух, также как и на глаз, никоим образом не доказывает невозможность его обнаружить статистическим методом. Факт невозможности обнаружения лучшим статистическим методом был доказан в предыдущем разделе.

В табл. 3 представлены результаты симуляции вероятности ошибки $P_{ош}$ в зависимости от длины блока N_0 и отношения η_W, вероятность ошибки $\widetilde{P}_{ош}$, рассчитанная в соответствии с (7). Из таблицы видно, что защищенность СРВ, полученная в результате симуляции, показывает лучшие результаты, чем теоретическая ожидаемая граница.

Таблица 3.

Результаты вычислений вероятности ошибки $P_{ош}$, полученной после декодирования по правилу (6) и теоретической вероятности ошибки $\widetilde{P}_{ош}$, вычисленной в (7) при $N = N_0$, для разных значений параметров η_W и N_0

η_W	N_0	$P_{ош}$	$\widetilde{P}_{ош}$
20	210	5.0×10^{-4}	0.001
50	496	6.0×10^{-4}	0.001
100	973	5.5×10^{-4}	0.001

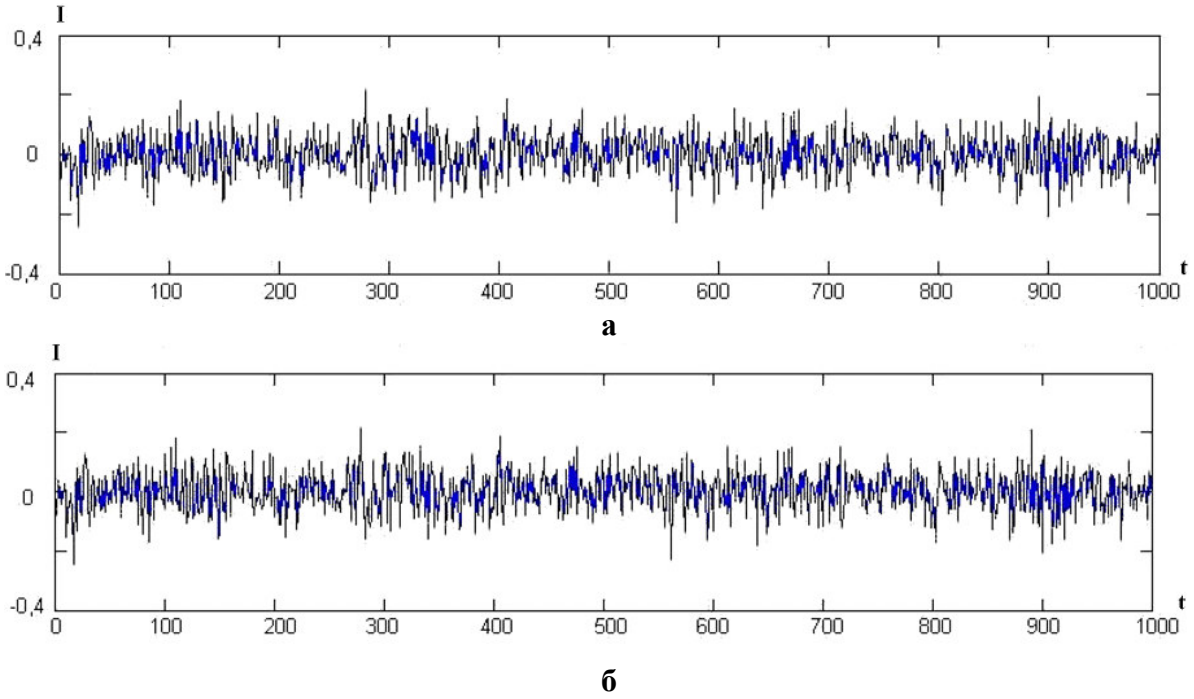

Рис. 3. Синограммы шума в канале: a – до внедрения скрытого сообщения; b –после внедрения скрытого сообщения по правилу (9)

Выводы

В данной работе представлена стеганографическая система для зашумленного канала – стеганографическая система с разнесением по времени, способная обеспечить необходимые уровни секретности и надежности восприятия сокрытого сообщения при реализуемом на практике значении отношения сигнал/шум. Доказано, что секретность и надежность восприятия такой системы могут быть обеспечены одновременно при правильном выборе ее параметров. Основным недостатком предложенной системы является низкая скорость внедрения, которая влечет за собой увеличение времени формирования стегосигнала одновременно с ограничением объема скрытой информации. Коды коррекции ошибок способны улучшить эту ситуацию, но лишь незначи-

тельно. Тем не менее, это свойство является своеобразной платой за невозможность обнаружения внедренного сообщения, даже при условии, что атакующая сторона обладает знанием покрывающего сообщения.

Также показано, что субоптимальное детектирование стеганосистемы (16) практически настолько же эффективно, как и оптимальное (основанное на отношении максимального подобия). Симуляция СРВ с использованием в качестве ПС аудиофайла показывает, что обнаружение внедренной информации на слух или на глаз невозможно, при том, что внедренные биты могут быть уверенно извлечены.

В дальнейшем представляется интересным продолжить исследование СРВ для ПС в цифровом формате, а также методы извлечения стеганосообщения при использовании неинформированного декодера, т.е. при неизвестном ПС на приемной части. Это возможно, например, на основе применения методов, рассмотренных в [6].

Список литературы

1. Korjik V.I., Lee M.H., Morales-Luna G. Stegosystems based on noisy channels // Proceeding of IX Spanish Meeting on Cryptology and Information Security. – Barcelona: Universidad Autonoma de Barcelona, 2006. – PP. 379-387.
2. Иванов В.А. Об искусственном зашумлении каналов передачи данных // Труды по дискретной математике. – 2004. – Том 8. – С. 99-115.
3. Cachin C. An information-theoretic model for steganography / C. Cachin // Proceeding of 2nd Workshop on Information Hiding, Lecture Notes in Computer Science. – USA: Springer, 1998. – Vol.1525. – PP. 306-318.
4. Van der Waerden B.L. Mathematische Statistik. – Berlin: Springer-Verlag, 1957; English transl. of 2nd (1965) ed. Springer-Verlag, Berlin and New York, 1969. – 367 p.
5. MacWilliams F.J. The Theory of Error-Correcting Codes / F.J. MacWilliams, N.J.A. Sloane. – Ney York : North Holland Publishing Co., 1977. – 762 p.
6. Malvar H.S. Improved spread spectrum: A new modulation technique for robust watermarking / H.S. Malvar, D.A.F. Florencio // IEEE Transaction on Signal Processing. – 2001. – Vol.51, Iss.4. – PP. 898-905.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРИХОВУВАННЯ ІНФОРМАЦІЇ ДЛЯ СИСТЕМ З ЗАШУМЛЕННИМИ КАНАЛАМИ ЗВ'ЯЗКУ

І.І. Маракова[1], О.О. Яковенко[2]

[1] Telecom Bretagne,
Technopôle Brest-Iroise, CS 83818, 29238 Brest Cedex 3, France; e-mail: marakova.irina@gmail.com
[2] Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна: e-mail: iakovenko.oleksandr@gmail.com

Розглядається система передачі прихованої інформації по зашумленних каналах зв'язку і сценарій, при якому атакуюча сторона не має іншого доступу до стеганосигналу, окрім як в ґаусовому каналі. При такому підході потрібно забезпечити практично недосяжну на практиці величину відношення сигнал/шум, особливо з урахуванням того, що покриваюче повідомлення може бути відомо стороні, що атакує. Для вирішення цієї проблеми запропоновано використовувати стеганосистему з рознесенням за часом (СРЧ). Доведена можливість побудови СРЧ із заданим рівнем секретності і надійності сприйняття прихованого сигналу. Розглянуто питання оптимізації параметрів на основі використання кодів корекції помилок. Представлені результати моделювання за допомогою реалізації СРЧ для покриваючих повідомлень у вигляді цифрових звукових файлів формату WAV.
Ключові слова: стеганосистема, покриваюче повідомлення, коди корекції помилок, ґаусовий канал з шумами, відносна ентропія

INFORMATION HIDING EFFICIENCY IMPROVEMENT FOR NOISY CHANNEL COMMUNICATION SYSTEMS

Irina I. Marakova[1], Alexander A. Iakovenko[2]

[1] Telecom Bretagne,
Technopôle Brest-Iroise, CS 83818, 29238 Brest Cedex 3, France; e-mail: marakova.irina@gmail.com
[2] Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: iakovenko.oleksandr@gmail.com

A system of hidden information transmission through a noisy communication channels, and a scenario where an attacker has no other access to steganographic signal, except in the Gaussian channel, are considered. With such an approach, it is required to provide virtually unattainable in practice magnitude of the signal/noise ratio, especially considering the fact that the covering message may be known to attackers. The steganographic systems with time spread (STS) are offered to solve this problem. STS constructions with a given level of privacy and perception fidelity are proved possible. The means of parameter optimization using error correcting codes is also considered. Results of simulation for STS over a WAV digital audio file format are presented.
Keywords: steganographic systems, covering message, error correction codes, Gaussian channel with noise, relative entropy