**УДК 004.056.5** **DOI:10.30837/rt.2020.4.203.04**

*А.А. КУЗНЕЦОВ, д-р техн. наук, А.А. СМИРНОВ, д-р техн. наук, А.С. КИЯН, Т.Ю. КУЗНЕЦОВА*

# СОКРЫТИЕ ДАННЫХ НА ОСНОВЕ АДРЕСАЦИИ ШУМОПОДОБНЫХ СИГНАЛОВ

## Введение

Для передачи секретных сообщений используются различные вычислительные методы [1 – 4]. Например, криптографические методы скрывают смысловое содержание передаваемых сообщений, представляя их в виде шумоподобных бессмысленных данных [1, 5]. Стеганографические методы скрывают сам факт существования информационных сообщений [3, 6]. Для этого сообщения скрываются внутри контейнеров (cover files) – избыточных данных, которые передаются открытым способом и не вызывают ни у кого подозрений [2, 3]. Сторонний наблюдатель может перехватывать cover files, анализировать и исследовать их, однако детектировать сокрытые данные и, тем более, их восстанавливать, для него очень сложно или вообще невозможно.

Сегодня стеганографические методы развиты очень хорошо. В литературе описаны различные способы сокрытия информационных сообщений избыточных cover files [7 – 10]: в изображениях, звуке, текстовых документах, видео и пр. Наиболее распространенные примеры описаны для контейнеров-изображений (cover images). При этом используются различные вычислительные приемы.

Наиболее перспективным направлением в сокрытии данных является стеганография на основе расширения спектра (Spread Spectrum Steganographic) [6, 11 – 14]. Эти методы используют достижения теории сложных дискретных сигналов для организации широкополосной высокоскоростной цифровой связи. Например, современные системы мобильной связи 4G и 5G используют широкополосные шумоподобные сигналы (специальным образом сформированные псевдослучайные последовательности), обеспечивая высокую помехоустойчивость, безопасность и экологичность связи [15 – 17]. Эти положительные свойства можно использовать и для сокрытия данных внутри cover files, например в изображениях [18 – 24].

В данной работе обсуждаются методы сокрытия данных в cover images с использованием технологии прямого расширения спектра. Мы показываем, что некоторые базовые предположения и гипотезы, принимаемые для организации широкополосной высокоскоростной цифровой связи, могут не выполняться при сокрытии данных внутри cover files. Это приводит к негативным эффектам:

- cover files сильно искажаются;
- интенсивность ошибок в восстановленных сообщениях очень высока.

В статье предлагается новый метод, который заключается в прямой адресации расширяющей последовательности. С одной стороны, это значительно уменьшает искажение cover file. С другой стороны, интенсивность ошибок в восстановленных сообщениях не увеличивается. Приводятся наглядные примеры и показываются преимущества предложенного метода. Также приводятся результаты экспериментов, оценивается качество изображений по различным показателям.

## Обзор литературы

В первых работах по стеганографии на основе расширенного спектра (Spread Spectrum Steganographic) введены базовые понятия и определения, показана принципиальная возможность сокрытия данных в cover files с использованием сложных шумоподобных дискретных сигналов и прямого расширения спектра [18 – 20, 25]. В то же время рассмотренные методы имеют определенные недостатки:

• битовая интенсивность ошибок (bit error rate – BER) восстановленных сообщений очень высокая. Например, в [18, с. 12, табл. 2] показано, что в большинстве случаев BER принимает значения 15 – 30 %. Даже при очень высокой «энергии» сокрытого сообщения BER не удается уменьшить ниже 10 %;

• искажения cover images очень высоки. Например, в [18] показано, что, увеличивая «энергию» сокрытого сообщения, удается снизить BER до 12 – 15 %, однако качество cover image при этом значительно снижается.

Таким образом, основная проблема рассмотренных стеганографических методов состоит в необходимости существенного снижения BER при сохранении приемлемого качества cover image. Например, в [18, с. 22] указано: «The BER is always higher than the desired value of 12 %. A power of 150 has an error rate of 16 %+ and the picture quality is becoming unacceptable. Increasing the stego power results in smaller improvements of the BER, approaching a limit of just under 16 %».

Дальнейшие исследования были направлены на снижение BER и повышение качества cover image. Для этого использовались различные методы [23, 26]: помехоустойчивое кодирование, фильтрация и пр. В работах [22, 27] исследуются варианты Spread Spectrum Steganographic при использовании аудио- и видео- cover files. В [28 – 31] сокрытие сообщение реализуется в DCT-области. Эти методы позволяют реализовать сокрытие сообщений, устойчивое к атакам сжатия. Например, наиболее распространенный способ сжатия JPEG использует DCT. Сокрытие данных в DCT-области снижает BER, т.е. число ошибок восстановленных сообщений уменьшается.

Еще один из возможных способов снижения BER – это подбор расширяющих шумоподобных последовательностей [32, 33]. Например, в работе [32] предложено формировать расширяющие последовательности с учетом статистических свойств cover files. Это позволило существенно снизить BER. В отдельных случаях удается добиться BER≈0, однако при этом время формирования расширяющих последовательностей очень велико. Кроме того, приемной стороне для восстановления сообщения нужен список расширяющих последовательностей (или компактное правило их формирования). Качество изображений остается на прежнем уровне. При увеличении объема сокрытого сообщения качество изображений неизбежно снижается.

В данной работе предлагается новый способ сокрытия данных в cover files. Этот подход позволяет минимизировать искажения cover files даже при большом объеме одновременно скрываемых сообщений. В работе показаны примеры изображений с различными способами сокрытия. Предлагаемый способ действительно выигрывает по качеству cover image. Однако вычислительная сложность предлагаемого способа существенно выше – сложность восстановления сообщений растет экспоненциально по мере повышения пропускной способности. Это основной недостаток предлагаемого способа. Однако всегда можно найти компромисс между вычислительной сложностью и качеством cover files.

**Известные методы сокрытия данных**

Известные примеры Spread Spectrum Steganography используют псевдослучайные последовательности для сокрытия сообщений. При этом в качестве cover files могут использоваться различные данные: изображения, аудио, видео и пр. Кроме того, сокрытие может реализовываться как в пространственной области, так и в области DCT. Мы не будем акцентировать на этом внимание, поскольку предлагаемый ниже способ также может применяться в различных вариантах. Для описания базовой технологии будем следовать публикациям [18 – 20], предлагая, тем не менее, некоторые собственные интерпретации.

Обозначим информационное сообщение как последовательность $m_0, m_1, ..., m_{k-1}$ бит, записанных в полярном виде:

$$\forall i \in \{0,1,...,k-1\} : m_i \in \{-1,1\}.$$

Для реализации технологии прямого расширения спектра используются дискретные сигналы [18 – 20]:

$$\Phi_i \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{N-1}\},\ k \le N,$$

причем каждый сигнал представляет собой псевдослучайную последовательность (ПСП):

$$\forall i \in \{0,1,...,N-1\} : \Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}}\right),\ \forall j \in \{0,1,...,n-1\} : \varphi_{i_j} \in \{-1,1\}.$$

Предполагается, что различные сигналы из множества $\Phi$ слабокоррелированы, т.е. коэффициент их взаимной корреляции примерно равен нулю:

$$\forall i \ne j : \rho\left(\Phi_i, \Phi_j\right) = \sum_{u=0}^{n-1} \varphi_{i_u} \varphi_{j_u} \approx 0.$$

Стегано-контейнер (cover) $S$ формируется посредством прибавления к исходному cover file $C$ усиленного модулированного сигнала $E$ [18 – 20]:

$$E = G \cdot \sum_{i=0}^{k-1} m_i \Phi_i,$$

т.е.

$$S = C + G \cdot E = C + G \cdot \sum_{i=0}^{k-1} m_i \Phi_i, \tag{1}$$

где $G > 0$ – коэффициент усиления, который задает «энергию» модулированного сигнала $E$.

Восстановление информационного сообщения на приемной стороне осуществляется с помощью корреляционного приема. При этом предполагается, что каждый сигнал из множества $\Phi$ не коррелирован с исходным cover file $C$:

$$\forall i : \rho\left(\Phi_i, C\right) \approx 0. \tag{2}$$

Тогда значение коэффициента корреляции определяется как

$$\rho\left(\Phi_i, S\right) = \rho\left(\Phi_i, C + G \cdot E\right) =$$
$$= \rho\left(\Phi_i, C\right) + G \cdot \rho\left(\Phi_i, E\right) \approx G \cdot \sum_{j=0}^{k-1} m_j \sum_{u=0}^{n} \varphi_{i_u} \varphi_{j_u}.$$

Принимая предположение

$$\forall j \ne i :\ \rho\left(\Phi_i, \Phi_j\right) = \sum_{u=0}^{n} \varphi_{i_u} \varphi_{j_u} \approx 0,$$

имеем

$$\rho\left(\Phi_i, S\right) \approx G \cdot m_i \cdot n,$$

т.е. знак $\rho\left(\Phi_i, S\right)$ совпадает со значением $m_i$ [18 – 20]:

$$m_i = sign\left(\rho\left(S, \Phi_i\right)\right) = \begin{cases} -1,\ \rho\left(S, \Phi_i\right) < 0; \\ +1,\ \rho\left(S, \Phi_i\right) > 0. \end{cases} \tag{3}$$

Очевидно, что число $k$ сокрытых информационных бит не может быть велико. Действительно, если $k = 1$, тогда cover file будет искажен незначительно. Как следует из (1), к значениям cover file $C$ будет прибавлено $G \cdot m_0 \Phi_0$, т.е. искажения cover file будут в диапазоне $-G...G$. Если $G$ невелико, тогда $S \approx C$. Например, для cover images искажения визуально

будут незаметны. Однако при увеличении $k>1$ искажения cover file будут возрастать пропорционально и находиться в диапазоне $-Gk...Gk$. Например, для $k=10$ искажения возрастут в 10 раз, и это невозможно изменить.

Напомним, что в реальных ситуациях для уменьшения BER значение $G$ также приходится увеличивать. Например, в [18] даже для больших значений $G$ значение BER не удалось уменьшить ниже 12 %. И это основное противоречие: снижение BER и сохранение качества cover file возможны только при небольшой пропускной способности, т.е. при малых $k$.

Мы предлагаем новый метод сокрытия данных, основанный на других правилах, отличных от (1) и (3).

**Предлагаемый метод сокрытия данных**

Обозначим информационное сообщение как последовательность $m_0, m_1, ..., m_{(k-1)K}$ бит:

$$\forall i \in \{0,1,...,(k-1)K\} : m_i \in \{0,1\}.$$

Сокрытие сообщения осуществляется блоками по $k$ бит. Для удобства представим информационное сообщение в виде последовательности неотрицательных целых чисел:

$$M_1, M_2, ..., M_K,$$

где

$$\forall i \in \{1,2,...,K\} : M_i = \sum_{j=0}^{k-1} 2^j m_{k(i-1)+j}.$$

Эти числа $M_i \in \{0,1,...,N-1\}$, $N=2^k$, $i \in \{1,2,...,K\}$ будем интерпретировать как адреса (порядковые номера) псевдослучайных последовательностей

$$\Phi_{M_i} \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{N-1}\},$$

где, как и прежде:

$$\forall i \in \{0,1,...,N-1\} : \Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}}\right),\ \forall j \in \{0,1,...,n-1\} : \varphi_{i_j} \in \{-1,1\}.$$

Для снижения искажений cover file мы предлагаем скрывать информационные сообщения на основе адресации расширяющих последовательностей. Правило кодирования расширяющей последовательностью предлагается реализовать следующим образом:

$$E_i = \Phi_{M_i} = \left(\varphi_{M_{i_0}}, \varphi_{M_{i_1}}, ..., \varphi_{M_{i_{n-1}}}\right),$$

т. е. есть модуляция осуществляется через адресацию этого сигнала в множестве $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{N-1}\}$.

Предлагаемый подход минимизирует вносимые искажения используемых контейнеров. Действительно, стегано-контейнер формируется, как и прежде, поэлементным сложением модулированного сигнала и данных контейнера, т.е. вместо (1) теперь имеем:

$$S_i = C_i + G \cdot E_i = C_i + G \cdot \Phi_{M_i}, \quad (4)$$

что приведет к внесению вносимых искажений в диапазоне $-G...G$ (при любом значении $k$).

Таким образом, предлагаемый метод за счет использования правила (4) позволяет одновременно сокрыть блок из $k \geq 1$ сокрытых информационных бит, а искажения cover file будут такие же, как и в известном способе (1) для $k=1$. В общем случае величина вносимых искажений в предлагаемом методе будет определяться только величиной коэффициента

усиления $G$, и не будет зависеть от $k$, т.е. от пропускной способности стеганосистемы. Это основное преимущество предлагаемого способа.

Для восстановления каждого блока $M_i \in \{0,1,...,N-1\}$ информационного сообщения на приемной стороне необходимо определить номер расширяющей последовательности

$$\Phi_{M_i} \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{N-1}\}.$$

Для этого предлагается поочередно вычислять коэффициенты корреляции $\rho(\Phi_\ell, S)$ для всех $\forall \ell \in \{0,1,...,N-1\}$. Адрес (порядковый номер) $\ell$ того дискретного сигнала $\Phi_\ell$, для которого вычисленный коэффициент корреляции $\rho(\Phi_\ell, S)$ будет максимальным (по всем $\ell$), задает десятичное значение блока информационного сообщения $M_i = \ell$, которое было сокрыто на передающей стороне.

Формализуем описанный выше процесс. Для восстановления блока $M_i$ сокрытого сообщения используем корреляционный приемник, правило работы которого состоит в вычислении коэффициента корреляции:

$$\rho(\Phi_\ell, S) = \rho(\Phi_\ell, C + G \cdot E) = \rho(\Phi_\ell, C) + G \cdot \rho(\Phi_\ell, E).$$

Принимая предположение (2) имеем:

$$\rho(\Phi_\ell, S) \approx G \cdot \rho(\Phi_\ell, E) = G \cdot \Phi_\ell \cdot \Phi_{M_i} = G \cdot \sum_{u=0}^{n} \varphi_{\ell_u} \varphi_{M_{i_u}}.$$

Принимая предположение

$$\forall \ell \neq M_i : \ \rho(\Phi_\ell, \Phi_{M_i}) = \sum_{u=0}^{n} \varphi_{\ell_u} \varphi_{M_{i_u}} \approx 0$$

имеем возможные значения:

$$\rho(\Phi_\ell, S) \approx \begin{cases} 0, \ell \neq M_i; \\ G, \ell = M_i. \end{cases}$$

Тогда значение блока $M_i$ информационного сообщения определим по правилу

$$M_i = \ell : \rho(\Phi_{M_i}, S) = \max_{\ell} \rho(\Phi_\ell, S). \quad (5)$$

Таким образом, для восстановления каждого блока $M_i$ информационного сообщения необходимо вычислить не более $N = 2^k$ коэффициентов корреляции $\rho(\Phi_\ell, S)$ и выбрать максимальное значение. Индекс (номер, адрес) $\ell$ такого ПСП $\Phi_\ell$ и задает значение блока $M_i = \ell$.

Очевидно, что с увеличением размерности блока $k$ вычислительная сложность восстановления сообщения быстро (экспоненциально) возрастает. Это основной недостаток нашего способа. Например, для $k = 10$ необходимо вычислить не более $2^{10} \approx 10^3$ коэффициентов $\rho(\Phi_\ell, S)$, а для $k = 20$ уже $2^{20} \approx 10^6$. В то же время для каждого такого случая качество cover file будет снижаться минимально (так же, как и для способа из раздела 3 при $k = 1$). Рациональным, на наш взгляд, является поиск компромисса между ожидаемой вычислительной сложностью и пропускной способностью стеганосистемы.

Следует отметить, что суть предложенного способа сокрытия данных использует несколько базовых предположений:

• предположение (2) о том, что каждый сигнал из множества $\Phi$ не коррелирован с исходным cover file $C$. В реальных случаях это предположение может не выполняться, однако в работе [32] предложен эффективный способ гарантированного выполнения условия (2) за счет адаптивной (учитывающей статистические свойства cover file) генерации множества $\Phi$;

• предположение о том, что различные сигналы из множества $\Phi$ слабокоррелированы, т.е. коэффициент их взаимной корреляции примерно равен нулю: $\forall i \neq j : \rho\left(\Phi_i, \Phi_j\right) \approx 0$. Выполнение этого предположения также обеспечивается на этапе генерации множества $\Phi$.

**Экспериментальные исследования**

Для оценки качества cover files обычно используют отношения сигнал/шум [34]. Например, пиковое отношение сигнал/шум (Peak signal-to-noise ratio, PSNR), которое характеризует отношение между максимально возможной мощностью сигнала и мощностью искажающего шума. Для удобства PSNR обычно выражается в логарифмической шкале, т.е. в децибелах.

Для монохромного изображения PSNR рассчитывают по среднеквадратической ошибке (mean squared error – MSE) [34]. Например, для монохромного изображения $C$ размером $N_1 \times N_2$ пикселей и его искаженного ошибками приближения $S$ значение MSE определяют по формуле

$$C_{MSE} = \frac{1}{N_1 N_2} \sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} [C(i, j) - S(i, j)]^2 ,$$

где $C(i, j)$ и $S(i, j)$ – значения яркости пикселей с координатами $i, j$.

Значение PSNR, выраженное в логарифмической шкале (т.е. в децибелах), определяют как

$$PSNR = 10 \cdot \log_{10}\left(\frac{C_{\max}^2}{C_{MSE}}\right) = 20 \cdot \log_{10}\left(\frac{C_{\max}}{\sqrt{C_{MSE}}}\right) =$$
$$= 20 \cdot \log_{10}\left(C_{\max}\right) - 10 \cdot \log_{10}\left(C_{MSE}\right),$$

где $C_{\max}$ – максимально возможное значение пикселя изображения.

Если для кодирования яркости каждого пикселя используется $m$ бит, тогда $C_{\max} = 2^m - 1$. Например, для $m = 8$ имеем $C_{\max} = 255$ и PSNR рассчитывается по формуле

$$PSNR = 20 \cdot \log_{10}\left(255\right) - 10 \cdot \log_{10}\left(C_{MSE}\right).$$

Для проведения экспериментов мы использовали стандартное тестовое изображение (standard test image) Lenna, размером $256 \times 256$ пикселей, при кодировании каждого монохромного полутонового пикселя одним байтом (см. рис. 1). На рис. 2 – 5 приведены примеры соответствующих cover images при сокрытии информационных сообщений с использованием правила (1) с $G = 4$:

- рис. 2 соответствует случаю $k = 1$;
- рис. 3 соответствует случаю $k = 2$;
- рис. 4 соответствует случаю $k = 4$;
- рис. 5 соответствует случаю $k = 8$.

На рис. 6 приведен пример cover image при сокрытии информационных сообщений с использованием правила (5) с $k = 8$ и $G = 4$.

Рис. 1. Стандартное тестовое изображение Lenna

Рис. 2. Cover image, правило сокрытия (1), $k = 1,\ G = 4$

Рис. 3. Cover image, правило сокрытия (1), $k = 2,\ G = 4$

Рис. 4. Cover image, правило сокрытия (1), $k=4$, $G=4$

Рис. 5. Cover image, правило сокрытия (1), $k=8$, $G=4$

Рис. 6. Cover image, правило сокрытия (5), $k=8$, $G=4$

Сокрытие информационных сообщений было реализовано программно с использованием системы компьютерной алгебры MathCad. Для формирования множества $\text{ПСП}\,\Phi=\{\Phi_0,\Phi_1,...,\Phi_{N-1}\}$ использован встроенный в MathCad генератор случайных чисел,

длина ПСП была выбрана $n = 256$. Для снижения BER дополнительно осуществлялась отбраковка ПСП по критерию

$$\forall i : \left|\rho\left(\Phi_i, C\right)\right| \le \rho_{\max} = 1000,$$

так как это было реализовано в [32].

Сокрытие $k$ информационных бит последовательно осуществлялось в каждую из 256 строк изображения. Таким образом, в качестве $C$ использовалась одна из строк контейнера-изображения $256 \times 256$ пикселей.

Для таких параметров и при $G = 4$ имеем

$$\rho_{\max} = 1000 < G \cdot n = 1024.$$

Практически достигается безошибочное (BER≈0) восстановление информационных сообщений [32].

На рис. 7 и 8 представлены зависимости MSE и PSNR от $k$ для различных значений $G$. Сплошные линии соответствуют правилу сокрытия информации (1), пунктирные линии – правилу (2).

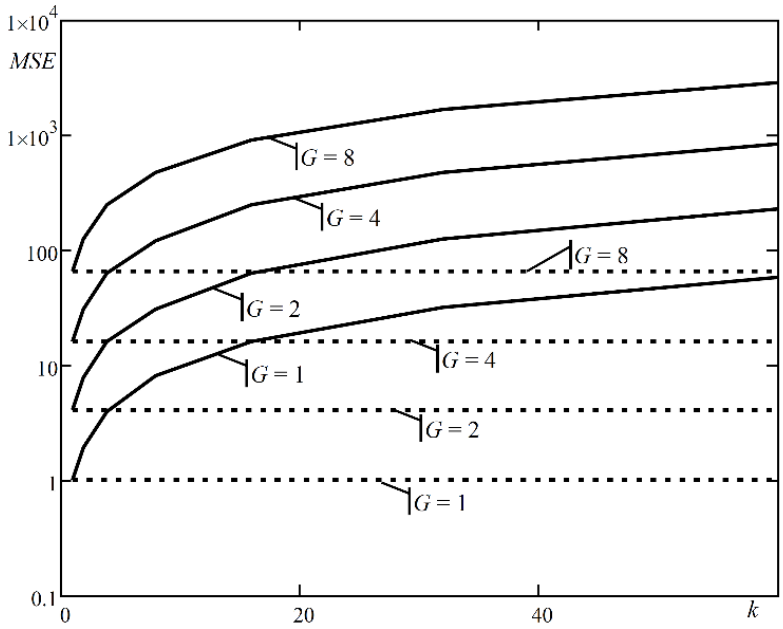


Рис. 7. Зависимости MSE от $k$

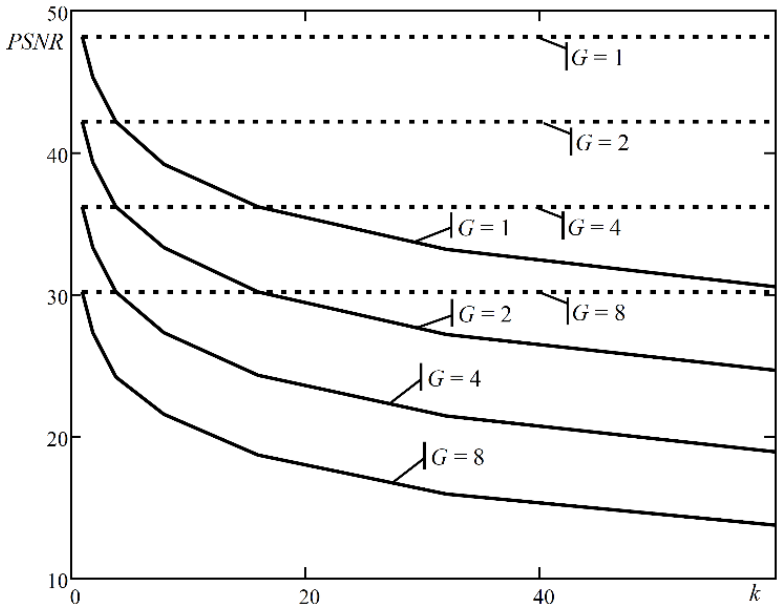


Рис. 8. Зависимости PSNR от $k$

Как видно из приведенных результатов, предлагаемый способ действительно позволяет существенно снизить искажения cover file. Например, качество изображения на рис. 6 сопоставимо с качеством рис. 2. Однако число сокрытых бит данных при использовании правила (4) увеличено в $k=8$ раз. Дальнейшее увеличение значения $k$ не приводит к снижению качества cover images и рис. 7, 8 наглядно это подтверждают. Напротив, повышение числа $k$ при использовании известного правила (1) приводит к неизбежному снижению качества изображения.

**Выводы**

Технология прямого расширения спектра успешно применяется в стеганографических задачах. С использованием расширяющих ПСП удается надежно скрывать информационные сообщения в cover files. Однако при этом возникают естественные противоречия:

- повышение объема сокрытых данных приводит к снижению качества cover files, например изображений;
- для снижения интенсивности ошибок (BER) в восстановленных сообщениях приходится усиливать ПСП, что еще больше искажает cover files.

В нашей предыдущей работе [32] мы показали, что, используя специальные способы формирования ПСП, можно существенно снизить BER (при выполнении ряда ограничений добиться практически безошибочного восстановления сообщений, т.е. BER≈0). Однако качество cover files при сокрытии все равно снижается.

В данной работе мы предложили новый метод сокрытия информации на основе адресации ПСП. Этот способ ведет к резкому увеличению вычислительной сложности (для восстановления сообщений необходимо многократно вычислять коэффициенты корреляции со всеми возможными ПСП). Однако качество cover files при этом практически не снижается. Наши эксперименты наглядно это подтверждают.

Перспективным направлением дальнейших исследований является использование ПСП с особыми корреляционными свойствами, например из [35 – 37]. Это направление представляется особенно актуальным для одновременного снижения BER и MSE. Кроме того, важным является также обоснование рекомендаций по выбору компромисса между величиной $k$ и ожидаемой вычислительной сложностью при реализации правила (5).

**Список литературы:**


1. Menezes A.J., Oorschot P.C. van Vanstone S.A., Oorschot P.C. van Vanstone S.A. Handbook of Applied Cryptography. CRC Press (2018). https://doi.org/10.1201/9780429466335.
2. Cox I., Miller M., Bloom J., Fridrich J., Kalker T. Digital Watermarking and Steganography. 2nd Ed. Morgan Kaufmann, Amsterdam; Boston (2007).
3. Fridrich J. Steganography in Digital Media Principles, Algorithms, and Applications. Cambridge University Press, Cambridge; New York (2009).
4. Rubinstein-Salzedo S. Cryptography. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-94818-8.
5. Delfs H., Knebl H. Introduction to Cryptography. Springer Berlin Heidelberg, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47974-2.
6. Singh A.K., Kumar B., Singh G., Mohan A. Secure Spread Spectrum Based Multiple Watermarking Technique for Medical Images // Singh A.K., Kumar B., Singh G. and Mohan A. (eds.) Medical Image Watermarking: Techniques and Applications. pp. 125–157. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-57699-2_6.
7. Menon N., Vaithiyanathan A survey on image steganography // 2017 International Conference on Technological Advancements in Power and Energy ( TAP Energy). pp. 1–5 (2017). https://doi.org/10.1109/TAPENERGY.2017.8397274.
8. Qin J., Luo Y., Xiang X., Tan Y., Huang H. Coverless Image Steganography: A Survey // IEEE Access. 7, 171372–171394 (2019). https://doi.org/10.1109/ACCESS.2019.2955452.
9. Schöttle P., Böhme R.: Game Theory and Adaptive Steganography // IEEE Transactions on Information Forensics and Security. 11, 760–773 (2016). https://doi.org/10.1109/TIFS.2015.2509941.
10. Yahya A. Introduction to Steganography // Yahya, A. (ed.) Steganography Techniques for Digital Images. pp. 1–7. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-78597-4_1.

11. Li M., Guo Y., Wang B., Kong X. Secure spread-spectrum data embedding with PN-sequence masking // Signal Processing: Image Communication. 39, 17–25 (2015). https://doi.org/10.1016/j.image.2015.07.014.

12. Pomponiu V., Cavagnino D., Botta M. SS-SVD: Spread spectrum data hiding scheme based on Singular Value Decomposition // 2015 International Symposium on Consumer Electronics (ISCE). pp. 1–2 (2015). https://doi.org/10.1109/ISCE.2015.7177769.

13. Hua G. Over-Complete-Dictionary-Based Improved Spread Spectrum Watermarking Security // IEEE Signal Processing Letters. 27, 770–774 (2020). https://doi.org/10.1109/LSP.2020.2986154.

14. Kokui N., Kang H., Iwamura K., Echizen I. Best embedding direction for spread spectrum-based video watermarking // 2016 IEEE 5th Global Conference on Consumer Electronics. pp. 1–3 (2016). https://doi.org/10.1109/GCCE.2016.7800389.

15. Torrieri D.: Principles of Spread-Spectrum Communication Systems // Springer International Publishing (2018). https://doi.org/10.1007/978-3-319-70569-9.

16. Ipatov V.P. Spread Spectrum and CDMA: Principles and Applications. John Wiley & Sons, Ltd, Chichester, UK (2005). https://doi.org/10.1002/0470091800.

17. Sklar B. Digital Communications: Fundamentals and Applications. Prentice Hall, Upper Saddle River, NJ (2017).

18. Marvel L.M., Boncelet C.G., Retter C.T. Spread spectrum image steganography // IEEE Transactions on Image Processing. 8, 1075–1083 (1999). https://doi.org/10.1109/83.777088.

19. Marvel L.M., Boncelet C.G., Retter C.T. Methodology of Spread-Spectrum Image Steganography. ARMY RESEARCH LAB ABERDEEN PROVING GROUND MD (1998).

20. Brundick F.S., Marvel L.M. Implementation of Spread Spectrum Image Steganography: Defense Technical Information Center, Fort Belvoir, VA (2001). https://doi.org/10.21236/ADA392155.

21. Eze P.U., Parampalli U., Evans R.J., Liu D. Spread Spectrum Steganographic Capacity Improvement for Medical Image Security in Teleradiology* // 2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). pp. 1–4 (2018). https://doi.org/10.1109/EMBC.2018.8512344.

22. Nugraha R.M. Implementation of Direct Sequence Spread Spectrum steganography on audio data // Proceedings of the 2011 International Conference on Electrical Engineering and Informatics. pp. 1–6 (2011). https://doi.org/10.1109/ICEEI.2011.6021662.

23. Youail R.S., Samawi V.W., Kadhim A.-K.A.-R. Combining a spread spectrum technique with error-correction code to design an immune stegosystem // Security and Identification 2008 2nd International Conference on Anti-counterfeiting. pp. 245–248 (2008). https://doi.org/10.1109/IWASID.2008.4688395.

24. Yadav, P., Dutta, M.: 3-Level security based spread spectrum image steganography with enhanced peak signal to noise ratio. In: 2017 Fourth International Conference on Image Information Processing (ICIIP). pp. 1–5 (2017). https://doi.org/10.1109/ICIIP.2017.8313696.

25. Smith J.R., Comiskey B.O. Modulation and information hiding in images // Anderson, R. (ed.) Information Hiding. pp. 207–226. Springer, Berlin, Heidelberg (1996). https://doi.org/10.1007/3-540-61996-8_42.

26. US-6557103-B1 – Spread Spectrum Image Steganography | Unified Patents, https://portal.unifiedpatents.com/patents/patent/US-6557103-B1, last accessed 2020/09/14.

27. Zarmehi N., Akhaee M.A. Video steganalysis of multiplicative spread spectrum steganography // 2014 22nd European Signal Processing Conference (EUSIPCO). pp. 2440–2444 (2014).

28. Ustubioglu A., Ulutas G., Ulutas M. DCT based image watermarking method with dynamic gain // 2015 38th International Conference on Telecommunications and Signal Processing (TSP). pp. 550–554 (2015). https://doi.org/10.1109/TSP.2015.7296323.

29. Agrawal N., Gupta A. DCT Domain Message Embedding in Spread-Spectrum Steganography System // 2009 Data Compression Conference. pp. 433–433 (2009). https://doi.org/10.1109/DCC.2009.86.

30. Weihua X., Yongbing W., Shuiyuan Y. H.264 Video Watermark Algorithm Using DCT Spread Spectrum // 2015 3rd International Conference on Applied Computing and Information Technology/2nd International Conference on Computational Science and Intelligence. pp. 447–450 (2015). https://doi.org/10.1109/ACIT-CSI.2015.84.

31. Ling Lu, Xinde Sun, Leiting Cai. A robust image watermarking based on DCT by Arnold transform and spread spectrum // 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). pp. V1-198-V1-201 (2010). https://doi.org/10.1109/ICACTE.2010.5579033.

32. Kuznetsov A., Smirnov O., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. Adaptive Pseudo-Random Sequence Generation for Spread Spectrum Image Steganography // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). pp. 161–165 (2020). https://doi.org/10.1109/DESSERT50317.2020.9125032.

33. Kuznetsov A., Smirnov A., Gorbacheva L., Babenko V. Hiding data in cover images using a pseudo-random sequences // Subbotin S. (ed.) Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, April 27-May 1, 2020. pp. 646–660. CEUR-WS.org (2020).

34. Korhonen J., You J. Peak signal-to-noise ratio revisited: Is simple beautiful? // 2012 Fourth International Workshop on Quality of Multimedia Experience. pp. 37–38 (2012). https://doi.org/10.1109/QoMEX.2012.6263880.

35. Kuznetsov A., Smirnov O., Kovalchuk D., Pastukhov M., Kuznetsova K., Prokopovych-Tkachenko D. Discrete Signals with Special Correlation Properties // Luengo D., Subbotin S., Arras P., Bodyanskiy Y., Henke K., Izonin

I., Levashenko V.G., Lytvynenko V., Parkhomenko A., Pester A., Shakhovska N., Sharpanskykh A., Tabunshchyk G., Wolff C., Wuttke H.-D., and Zaitseva E. (eds.) Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), Zaporizhzhia, Ukraine, April 15-19, 2019. pp. 618–629. CEUR-WS.org (2019).

36. Kuznetsov A., Smirnov O., Reshetniak O., Ivko T., Kuznetsova T., Katkova T. Generators of Pseudorandom Sequence with Multilevel Function of Correlation // 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S T). pp. 517–522 (2019). https://doi.org/10.1109/PICST47496.2019.9061530.

37. Kuznetsov A., Kiian A., Kuznetsova K., Zub M., Zaburmekha Y., Lyshchenko E. Pseudorandom Sequences with Multi-Level Correlation Function for Direct Spectrum Spreading // 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). pp. 232–237 (2019). https://doi.org/10.1109/ATIT49449.2019.9030436.

*Поступила в редколлегию 23.09.2020*

*Сведения об авторах:*

**Кузнецов Александр Александрович** – д-р техн. наук, профессор, профессор кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: kuznetsov@karazin.ua, ORCID: https://orcid.org/0000-0003-2331-6326

**Смирнов Алексей Анатольевич –** д-р техн. наук, профессор, заведующий кафедрой кибербезопасности и программного обеспечения, Центральноукраинский национальный технический университет, м. Кропивницкий, Украина; e-mail: dr.smirnovoa@gmail.com, ORCID: https://orcid.org/0000-0001-9543-874X

**Киян Анастасия Сергеевна –** здобувач кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: nastyak931@gmail.com, ORCID: https://orcid.org/0000-0003-2110-010X

**Кузнецова Татьяна Юрьевна** – научный сотрудник научно-исследовательской части, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: kuznetsova.tatiana17@gmail.com, ORCID: https://orcid.org/0000-0001-6154-7139