УДК 519.111: 621.391 DOI: 10.26565/2519-2310-2020-1-01

СОКРЫТИЕ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ С ИСПОЛЬЗОВАНИЕМ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Алексей Смирнов[1], Людмила Горбачова[2], Александр Кузнецов[2]

[1] Центральный украинский национальный технический университет, пр. Университетский 8, Кропивницкий, 25006, Украина
[2] Харьковский национальный университет им. В.Н. Каразина, пл. Свободы, 4, Харьков, 61022, Украина

dr.smirnovoa@gmail.com, kuznetsov@karazin.ua

Рецензент: Николай Карпинский, д.т.н., проф., Университет Бельско-Бяла, ул. Виллова 2, 43-309 Бельско-Бяла, Польша
mkarpinski@ath.bielsko.pl

Поступила: Январь 2020

Аннотация. *В работе рассматриваются техники сокрытия информационных сообщений в контейнерах-изображениях с использованием технологии прямого расширения спектра. В основе этой технологии лежит использование слабокоррелированных псевдослучайных (шумовых) последовательностей. Модулируя информационные данные такими сигналами, сообщение представляется в шумоподобном виде, что существенно затрудняет его обнаружение. Сокрытие состоит в добавлении модулированного сообщения к контейнеру-изображению. Если интерпретировать это изображение как шум в канале связи, тогда задача сокрытия пользовательских данных эквивалентна передаче шумоподобного модулированного сообщения по каналу связи с шумом. При этом предполагается, что шумоподобные сигналы слабокоррелированы, как друг с другом, так и с контейнером-изображением (или его фрагментом). Однако последнее предположение может не выполняться, т.к. реалистичное изображение не является реализацией случайного процесса, его пиксели имеют сильную корреляцию. Очевидно, что выбор псевдослучайных расширяющих сигналов должен учитывать эту особенность. В работе исследованы различные способы формирования расширяющих последовательностей. Выполнена оценка интенсивности битовых ошибок (Bit Error Rate, BER) информационных данных, а также искажений контейнера-изображения по среднеквадратической ошибке (Mean Squared Error, MSE) и пиковому отношению сигнал/шум (Peak signal-to-noise ratio, PSNR). Полученные экспериментальные зависимости наглядно подтверждают преимущество использования последовательностей Уолша. В ходе исследований получены наименьшие значения BER. Даже при небольших значениях мощности сигналов расширяющих последовательностей ($P \approx 5$) величина BER в большинстве случаев не превышала 0,01. Это представляет собой лучший результат из всех рассмотренных в работе вариантов расширяющих последовательностей. Значения PSNR при использовании ортогональных последовательностей Уолша, в большинстве случаев, сопоставимо с другими рассмотренными вариантами. Однако для фиксированного значения PSNR использование преобразования Уолша приводит к значительно меньшим величинам BER. Отмечено, что перспективным направлением является использование адаптивно формируемых дискретных последовательностей. Так, например, если правило формирования расширяющих сигналов будет учитывать статистические свойства контейнера, то можно существенно снизить BER. Также, другим полезным результатом может быть повышение PSNR при фиксированном (заданном) значении BER. Основной целью работы является обоснование выбора расширяющих последовательностей для снижения BER и MSE (увеличения PSNR).*

Ключевые слова: *стеганография; технология прямого расширения спектра; псевдослучайная последовательность, расширяющие сигналы.*

1 Введение

Для сокрытия факта передачи и самого существования информационного сообщения традиционно используют различные стеганографические техники [1-4]. С развитием компьютерных наук и цифровых методов обработки информации стеганографическое сокрытие сообщений стало очень распространенным, его используют при обработке изображений, аудио, текстовых документов и пр. Это довольно эффективный и надежный способ организации скрытых каналов передачи данных. Для стороннего наблюдателя передаваемые (*например, посредством электронной почты*) контейнеры, содержащие сокрытые в них информационные сообщения, ничем не отличаются от обычных пользовательских файлов. Это дает возможность организовать скрытый канал связи (КС), не вызывая подозрения о своих намерениях, причем детектировать такие каналы чрезвычайно сложно [1, 2].

Одним из перспективных направлений в развитии современной стеганографии являются

техники встраивания данных в контейнеры-изображения на основе технологи прямого расширения спектра [5-17]. Эта технология традиционно используется в системах связи для повышения скрытности передачи данных по КС с шумами [12-17]. Информационные данные модулируются расширяющей спектр псевдослучайной (*шумовой*) последовательностью. При передаче полученные сигналы в статистическом смысле неотличимы от естественного шума, что повышает скрытность связи. Кроме того, реализуемые методы корреляционного приема позволяют обеспечить исправление произошедших ошибок, что повышает помехоустойчивость связи. Эти и многие другие преимущества технологии прямого расширения спектра позволяют строить надежные и безопасные системы связи. Например, можно организовать связь со значительно меньшей мощностью передатчика, что обеспечивает экологичность связи; применение больших ансамблей (*множеств*) расширяющих последовательностей позволяет повысить абонентскую емкость множественного доступа и т.д. [18-21]. Подобный подход можно применять и в компьютерной обработке цифровых изображений. Интерпретируя изображение, как шум в КС и используя технологию прямого расширения спектра можно организовать сокрытие информационных сообщений без видимого (*демаскирующего*) искажения контейнера. Такие техники и составляют предмет исследований данной статьи.

2 Технология прямого расширения спектра для сокрытия сообщений в изображениях

В первых работах по использованию технологии прямого расширения спектра в цифровой стеганографии выдвигалась идея использования псевдослучайных (*шумовых*) последовательностей в качестве «носителя» информационных сообщений [5-11]. Например, для двоичного случая модулированное сообщение S получают умножением отдельных информационных бит b_i (*представляемых в полярном виде* $b_i \in \{-1,1\}$) на расширяющий шумовой сигнал φ_i:

$$S = \sum_i b_i \varphi_i \qquad (1)$$

причем φ_i принадлежит ансамблю (множеству) слабокоррелированных друг с другом псевдослучайных последовательностей (ПСП):

$$\forall \varphi_i \in \varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}.$$

Это означает, что коэффициент корреляции двух разных сигналов (*вычисляемый как скалярное произведение последовательностей*) примерно равен нулю:

$$\forall i \neq j : \rho(\varphi_i, \varphi_j) \approx 0.$$

Выражение (1), которое описывает процесс модуляции информационных бит $b_i \in \{-1,1\}$ расширяющими сигналами φ_i, традиционно используется в широкополосной системе связи с прямым расширением спектра. Поскольку расширяющий сигнал φ_i по своим статистическим свойствам подобен шуму, то полученное модулированное сообщение S слабоотличимо от шумов в канале связи, что и позволяет осуществить скрытую передачу. Действительно, передаваемые сообщения приобретают вид шумоподобных последовательностей, а за счет большой мощности множества φ и прямого расширения частотного спектра обеспечивается высокая скрытность и имитостойкость организовываемых каналов связи [18-21]. В системах с кодовым разделением каналов CDMA (*Code Division Multiple Access*) каждый сигнал φ_i назначается отдельной паре абонентов, т.е. увеличение мощности M множества $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$ позволяет повысить абонентскую емкость систем связи, т.е. существенно удешевить передачу данных [18,19].

Стеганография с использованием прямого расширения спектра использует эти техники в различных файлах-контейнерах. Например, интерпретируя контейнер-изображение I, как естественный шум в канале связи можно организовать передачу информационных сообще-

ний «внутри» изображения [5-17]. В работах [5-11] в качестве сигналов φ_i предлагалось использовать формируемые генераторами ПСП последовательности, после чего сформированный по правилу (1) сигнал S поэлементно суммируется с контейнером-изображением I:

$$N = I + S \tag{2}$$

Таким образом, полученное изображение-стеганоконтейнер N формируется посредством добавления к исходному изображению I модулированного сообщения (1). Это аналогично тому, как в системах связи передаваемое модулированное информационное сообщение S «складывалось» с естественным фоновым шумом (*помехой*).

На приемной стороне, как и в системах связи, информационное сообщение восстанавливается с использованием корреляционного приема. Для двоичного случая для извлечения j-ого бита вычисляют коэффициент корреляции между сигналом φ_j и принятым N:

$$\rho\left(N,\varphi_j\right) = I\varphi_j + \varphi_j \sum_i b_i \varphi_i \tag{3}$$

В системах связи естественный шум и шумовой сигнал φ_i статистически независимы (*некоррелированы*). Следуя подобным интерпретациям логично предположить, что аналог шума – контейнер-изображение I также некоррелирован с расширяющими сигналами, т.е. $\rho\left(I,\varphi_j\right) = I\varphi_j \approx 0$. Различные шумовые сигналы также некоррелированы друг с другом, т.е. $\forall j \neq i : \varphi_j\varphi_i \approx 0$. В этом случае $\rho\left(N,\varphi_j\right) \approx b_j\varphi_j\varphi_j$, т.е. значение b_j можно определить по знаку $\rho\left(N,\varphi_j\right)$:

$$b_j = sign\left[\rho\left(N,\varphi_j\right)\right] \tag{4}$$

К сожалению, для стеганографических приложений, когда используется контейнер-изображение I, предположение $\rho\left(I,\varphi_j\right) = I\varphi_j \approx 0$ в (3) может не выполняться. Действительно, если для сокрытия информационного сообщения используется реалистичное изображение (*т.е. не являющееся реализацией некоторого датчика случайных величин*), то тогда может наблюдаться существенная корреляция I и φ_i. В этом случае восстановление информационных бит в соответствии с выражением (4) может быть ошибочным.

В данной работе исследуются различные способы формирования множества $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$ и проведена оценка интенсивности битовых ошибок (*BER - Bit Error Rate*) при извлечении сообщения из изображений-контейнеров (*N*). В частности, исследован предложенный в работах [7,8,10,11] нелинейный способ формирования последовательностей с нормальным гауссовым распределением, а также ортогональные последовательности Уолша [22] и псевдослучайные последовательности, с равномерно распределенными на интервале (-1, 1) элементами. Также, в рамках работы проведена оценка искажения изображения-контейнера по среднеквадратической ошибке (СКО) и пиковому отношению сигнал/шум (*Peak signal-to-noise ratio, PSNR*). Эти две характеристики (*BER* и *PSNR*) наглядно демонстрируют возможности по достоверной (*безошибочной*) и скрытной (*без демаскирующих искажений изображения-контейнера*) передачи информационных сообщений с использованием технологии прямого расширения спектра.

3 Порядок исследований

Для проведения исследований различных способов сокрытия информации в контейнерах-изображениях используют несколько показателей эффективности.

Для оценки правильности восстановленных данных (*их достоверности, безошибочности*) используют *BER* [23]. *BER* - количество битовых ошибок N_{error}, деленное на общее количество переданных бит N_{total}:

$$BER = \frac{N_{error}}{N_{total}} \tag{5}$$

BER - это единичный показатель производительности, часто выражаемый в процентах[23]. Мы оценивали *BER* в абсолютных величинах, т.е. непосредственно по (5). Для оценки искажений контейнера-изображения используют *MSE* и *PSNR* [23-25].

Для монохромного $m \times n$ изображения *I* и его искаженного ошибками приближения (*Noisy Approximation*) *N* значение *MSE* определяют выражением:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I_{i,j} - N_{i,j}]^2 \tag{6}$$

PSNR характеризует отношение между максимально возможной мощностью сигнала и мощностью искажающего шума. *PSNR* обычно выражается в логарифмической шкале (*dB*):

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{I_{\max}^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{I_{\max}}{\sqrt{MSE}}\right) = \\ &= 20 \cdot \log_{10}(I_{\max}) - 10 \cdot \log_{10}(MSE). \end{aligned} \tag{7}$$

где $I_{\max}$ есть максимально возможное значение пикселя изображения.

Если пиксели кодируются m-ми битными величинами, тогда $I_{\max} = 2^m - 1$. Например, для наиболее простого случая с $m = 8$ имеем $I_{\max} = 255$ и значение *PSNR* рассчитывается по (8):

$$PSNR = 20 \cdot \log_{10}(255) - 10 \cdot \log_{10}(MSE) \tag{8}$$

При проведении экспериментов были использованы различные изображения (*размером 256×256 эл.*) при кодировании каждого монохромного пикселя одним байтом [7,8,10,11]. Так в частности, в рамках экспериментов обработке подвергалось стандартное тестовое изображение *Lenna* размером 256×256 пикселей. Приводимые далее результаты, представляют собой усредненные значения, полученные для нескольких различных изображений. Для усреднения результатов использовались формулы квадратичной регрессии с интерполяцией полученных результатов (*встроенная функция regress и interp системы MathCad*).

Следует отметить, что приводимые здесь результаты соответствуют использованию различных расширяющих последовательностей, но без применения помехоустойчивого кодирования. Например, в работе [8] для снижения *BER* применяются блоковые коды в режиме прямого исправления ошибок. В данной работе приводятся оценки *BER* без использования помехоустойчивых кодов. В этом смысле полученные результаты могут быть сопоставлены с уже имеющимися, известными данными.

4 Результаты исследований

При проведении исследований мы реализовали несколько вариантов формирования множества расширяющих сигналов $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$. Для каждого способа формирования расширяющих последовательностей осуществлялась вставка информации в различные контейнеры-изображения и выполнялась оценка значений *BER*, *MSE* и *PSNR* (*как в (5-8)*). Основное внимание было акцентировано на сравнении полученных результатов, с целью определения лучшего способа формирования последовательностей φ_i.

4.1 Использование нелинейной модуляции

В работах *Lisa M. Marvel* и др. [7, 8, 10, 11] для использования технологии прямого расширения спектра предлагалось использовать нелинейное правило формирования множества $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$:

$$(\varphi_i)_j = \begin{cases} \Phi^{-1}((u_i)_j), b_i = -1; \\ \Phi^{-1}((u'_i)_j), b_i = 1, \end{cases} \quad (9) \qquad \text{где} \qquad (u'_i)_j = \begin{cases} (u_i)_j + 0.5, u_i < 0.5; \\ (u_i)_j - 0.5, u_i \geq 0.5, \end{cases} \quad (10)$$

$(u_i)_j$ - равномерно распределенная на интервале (0,1) случайная величина, а Φ^{-1} представляет собой обратную кумулятивную функцию распределения для стандартной гауссовой случайной величины.

Таким образом, расширяющие спектр последовательности из $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$ представляют собой реализацию случайной величины, распределенной по нормальному закону с нулевым средним и единичным среднеквадратичным отклонением. Эта случайная реализация вычисляется в соответствии с (9), т.е. с использованием метода обратного преобразования (*The Inverse Transformation Method*) [26].

Для практической реализации нелинейного правила (9) и (10) были использованы встроенные в *MathCad* функции $rnd(x)$ и $dnorm(p, \mu, \sigma)$: $\Phi^{-1}(x) = dnorm(x, 0, 1)$; $(u_i)_j = rnd(1)$.

Очевидно, что правило (1) для вычисления модулированного сигнала S при таком способе формирования множества $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$, следует записать в следующем виде:

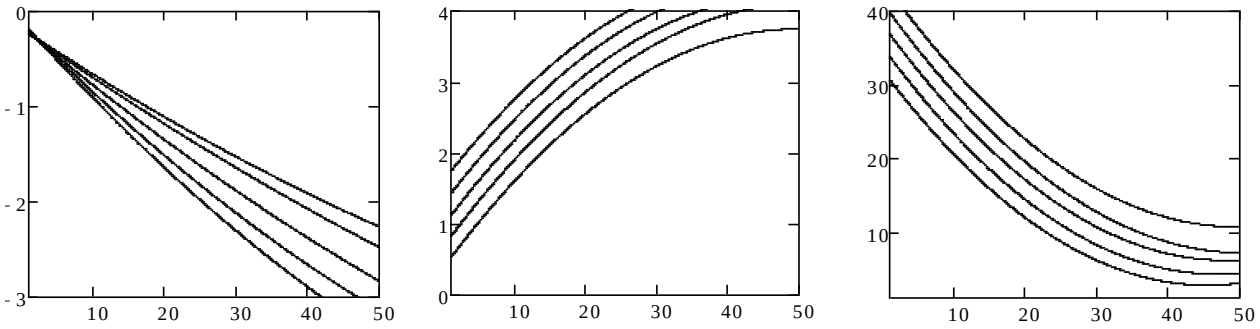
$$S = \sum_i \varphi_i \quad (11)$$

Как известно [7-8,10-11], непосредственное использование расширяющих последовательностей для сокрытия информации в изображениях-контейнерах, приводит к значительным битовым ошибкам в извлеченных данных. Для этого предлагалось повышать мощность расширяющих сигналов. Таким образом, выражение (11) запишем как

$$S = \sum_i P\varphi_i \quad (12)$$

где P - положительное значение, кратно увеличивающее мощность (*power*) расширяющих сигналов последовательностей φ_i.

В серии проведенных экспериментов авторами реализовано сокрытие данных в изображениях-контейнерах с использованием выражений (9), (10), (12). Полученные результаты для различных значений P представлены на рис. 1, где приведены различные случаи для $k = 1, 2, 4, 8, 16$ и $P = 2^i, i = 0, 1, ..., 6$. Число слагаемых в (1) и (12) определяется числом k информационных бит, скрываемых в одном изображении-контейнере.



a) BER (P) *b) MSE (P)* *c) PSNR (P)*

Рис. 1 - Результаты моделирования с использованием выражений (9), (10), (12)

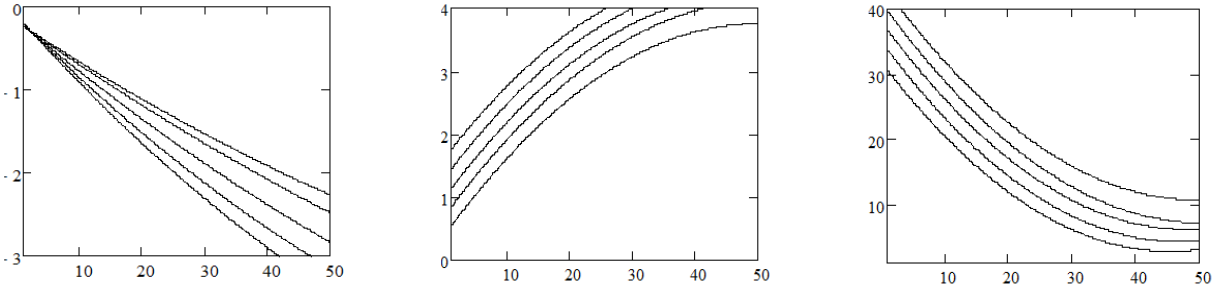
Если множество сигналов $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$ формировать по упрощенной схеме (13):

$$(\varphi_i)_j = \Phi^{-1}((u'_i)_j), (u'_i)_j = \begin{cases} (u_i)_j + 0.5, u_i < 0.5; \\ (u_i)_j - 0.5, u_i \geq 0.5, \end{cases} \quad (13)$$

то для сокрытия данных можем использовать аналог выражения (1) в следующем виде:

$$S = \sum_i Pb_i\varphi_i \quad (14)$$

Данный способ формирования расширяющих сигналов нами также был исследован, а полученные результаты представлены на рис 2.



a) BER (P) *b) MSE (P)* *c) PSNR (P)*

Рис. 2 – Результаты моделирования с использованием выражений (13) и (14)

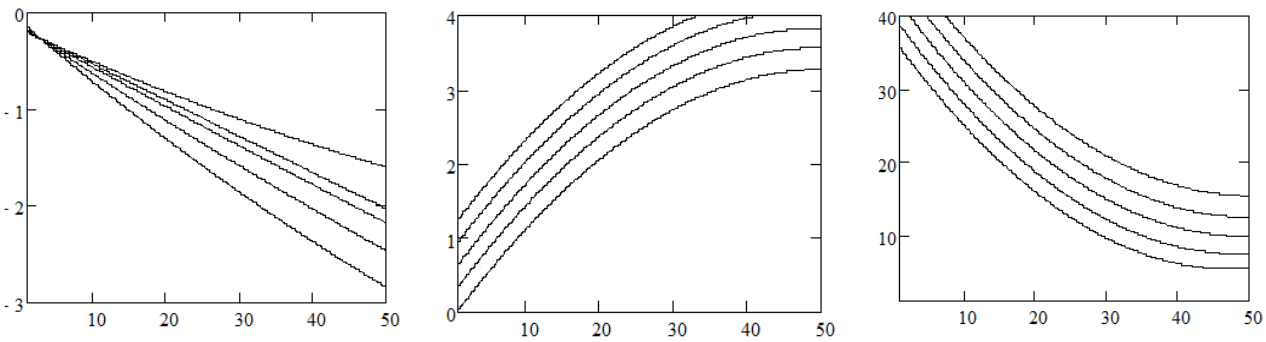
Анализ представленных данных позволяет утверждать, что оба способа формирования расширяющих последовательностей дают практически одинаковые результаты. В сери проведенных экспериментов правило (9), (10) было лишь немногим лучше по значению *PSNR* (*из-за логарифмической шкалы это различие практически не заметно*). Также следует отметить высокое значение *BER*, например, уже при «мощности» расширяющих сигналов $P \approx 20$ это значения, в большинстве случаев, находится в диапазоне 0,1 ... 0,01 (*практически граничное значение целесообразности использования помехоустойчивого кодирования*).

4.2 Использование случайных чисел, равномерно распределенных на интервале (-1,1)

Другой способ формирования множества $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$, который мы исследовали, состоял в использовании равномерно распределенных на интервале (-1,1) случайных чисел. Для моделирования данного варианта использована встроенная функция $rnd(x)$ системы *MathCad*, а правило формирования последовательностей имело вид:

$$(\varphi_i)_j = rnd(2) - 1 \quad (15)$$

Результаты исследований эффективности сокрытия информации в соответствии с правилом (13) для различных соотношений k и P приведены на рис. 3.



a) BER (P) *b) MSE (P)* *c) PSNR (P)*

Рис. 3 – Результаты моделирования с использованием выражений (15) и (14)

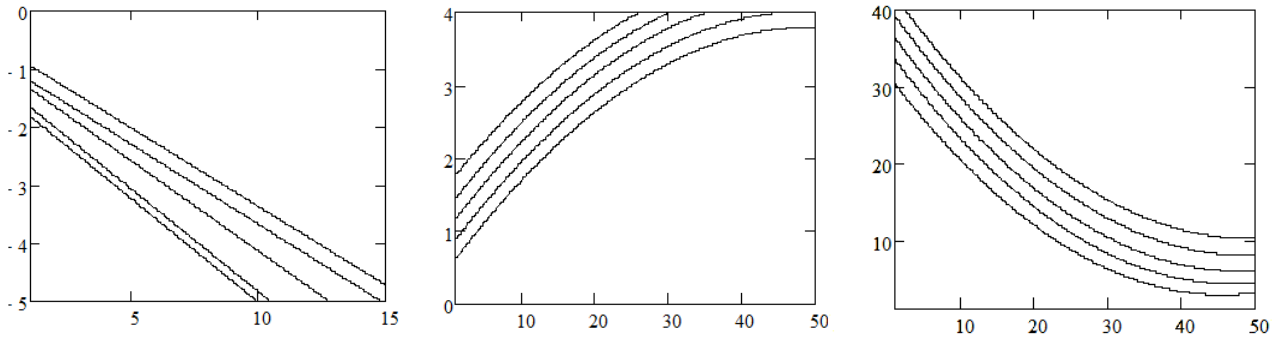
Приведенные на рис. 3 результаты практически сопоставимы с данными, полученными для случая нелинейной модуляции (9), (10), а также для упрощенного варианта (13). В данном случае наблюдается, лишь незначительное повышение *BER*, однако *PSNR* при этом также увеличилось. В целом, можно утверждать, что выявленные отличия невелики и эти способы формирования расширяющих последовательностей практически равноценны.

4.3 Использование ортогональных последовательностей Уолша

В своих исследованиях мы также использовали ортогональные дискретные последовательности Уолша (*Walsh*). Такие сигналы образуются из строк матрицы Адамара (*Hadamard matrix*) H_{2^i}, формируемой по рекуррентному правилу:

$$H_{2^i} = \begin{bmatrix} H_{2^{i-1}} & H_{2^{i-1}} \\ H_{2^{i-1}} & -H_{2^{i-1}} \end{bmatrix}, \; H_1 = [1]. \tag{16}$$

Итеративное повторение правила (16) позволяет сформировать любую матрицу Адамара H_{2^i} порядка 2^i, $i = 1, 2, \ldots$. Строки (или столбцы) сформированных матриц взаимно ортогональны, т.е. их скалярное произведение равно нулю. В ходе проведенного моделирования было использовано правило (16), а строки матрицы H_{2^i} интерпретировались, как элементы множества $\varphi = \{\varphi_0, \varphi_1, \ldots, \varphi_{M-1}\}$. Полученные результаты приведены на рис. 4.



a) BER (P) *b) MSE (P)* *c) PSNR (P)*

Рис. 4 – Результаты моделирования с использованием ортогональных последовательностей Уолша и выражения (14)

Зависимости на рис. 4 наглядно подтверждают преимущество использования последовательностей Уолша. Так, в ходе исследований получены наименьшие значения *BER*. Даже при небольших значениях $P \approx 5$ величина *BER*, в большинстве случаев, не превышала 0,01, что представляет собой наилучший результат из всех рассмотренных вариантов расширяющих последовательностей.

Значения *PSNR* при использовании ортогональных последовательностей Уолша, в большинстве случаев, сопоставимо с рассмотренными ранее вариантами. Однако для фиксированного значения *PSNR* использование преобразования Уолша приводит к значительно меньшим величинам *BER*.

5 Выводы

Полученные в ходе моделирования зависимости показывают, что использование технологии прямого расширения спектра действительно может являться перспективным решением задачи сокрытия информационных сообщений в изображениях-контейнерах (стеганографии).

Интерпретируя изображение, как шум в КС можно организовать скрытный канал передачи данных, причем искажения изображения могут быть не велики. В тоже время, основное предположение о некоррелированности расширяющих последовательностей с контейнером-переносчиком информации (*или его отдельной частью/фрагментом*), может быть ошибочным. В этом случае при восстановлении информационных (*скрытых*) данных будет получен

высокий уровень ошибок. Следовательно, важным элементом такой стеганосистемы является корректный выбор расширяющих последовательностей.

В данной работе были проанализированы несколько вариантов построения расширяющих последовательностей для целей синтеза стеганосистемы. В частности, рассмотрен один из известных алгоритмов [11] с нелинейной модуляцией по правилу (9), (10), на примере которого исследована эффективность подобной стегановставки по показателям *BER*, *MSE* и *PSNR*. Полученные данные частично совпадают с известными результатами из [7,8,10,11], что косвенно подтверждает адекватность представленных результатов.

Также исследованиям были подвергнуты и другие способы формирования расширяющих последовательностей (*для целей сокрытия данных в контейнерах-изображениях*). Моделирование показало, что применение упрощенного правила (13), равно как и использование последовательностей с равновероятными на интервале (-1,1) значениями, не приводит к существенному ухудшению результатов *(показатели BER и PSNR отличаются не значительно)*.

В ходе экспериментов изучено применение расширяющих последовательностей Уолша. Анализ данных результатов свидетельствует, что этот вариант наиболее удачный, поскольку при сопоставимых значениях *PSNR* достигается значительно меньшая величина ошибок. Действительно, как следует из представленных результатов, величина *BER* значительно ниже, чем для других вариантов использованных расширяющих последовательностей.

Подчеркнуто, что потенциально интересным направлением дальнейших исследований является использование адаптивно формируемых дискретных последовательностей. Так, например, если правило формирования расширяющих сигналов будет учитывать статистические свойства изображения-контейнера, то можно существенно снизить *BER*, либо вовсе получить практически безошибочную передачу. Также, другим полезным эффектом может быть повышение *PSNR* при фиксированном (*например, наперед заданным*) значении *BER*.

В рамках дальнейших исследованиях будут представлены результаты моделирования ряда других способов формирования расширяющих последовательностей, рассмотренных в наших предыдущих работах [27-31].

Ссылки

[1] “Digital Watermarking and Steganography,” 2008. doi:10.1016/b978-0-12-372585-1.x5001-3.

[2] F. Y. Shin, “Digital Watermarking and Steganography,” Dec. 2017. doi:10.1201/9781315219783.

[3] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," in Computer, vol. 31, no. 2, pp. 26-34, Feb. 1998. doi: 10.1109/MC.1998.4655281.

[4] I. V. S. Manoj, “Cryptography and Steganography,” International Journal of Computer Applications, vol. 1, no. 12, pp. 63–68, Feb. 2010. doi:10.5120/257-414.

[5] A. Z. Tirkel, C. F. Osborne and R. G. Van Schyndel, "Image watermarking-a spread spectrum application," Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications, Mainz, Germany, 1996, pp. 785-789 vol.2. doi: 10.1109/ISSSTA.1996.563231.

[6] J. R. Smith and B. O. Comiskey, “Modulation and information hiding in images,” Lecture Notes in Computer Science, pp. 207–226, 1996. doi:10.1007/3-540-61996-8_42.

[7] L. M. Marvel, C. G. Boncelet, R. Jr., and Charles T., “Methodology of Spread-Spectrum Image Steganography,” Jun. 1998. doi:10.21236/ada349102.

[8] L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread spectrum image steganography," in IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075-1083, Aug. 1999. doi: 10.1109/83.777088.

[9] M. Kutter, “Performance Improvement of Spread Spectrum Based Image Watermarking Schemes through M-ary Modulation,” Lecture Notes in Computer Science, pp. 237–252, 2000. doi:10.1007/10719724_17.

[10] F. S. Brundick and L. M. Marvel, “Implementation of Spread Spectrum Image Steganography,” Mar. 2001. doi:10.21236/ada392155.

[11] Patent No.: US 6,557,103 B1, Int.Cl. G06F 11/30. Charles G. Boncelet, Jr., Lisa M. Marvel, Charles T. Retter. Spread Spectrum Image Steganography. Patent No.: US 6,557,103 B1, Int.Cl. G06F 11/30. – № 09/257,136; Filed Feb. 11, 1999; Date of Patent Apr. 29, 2003

[12] Fan Zhang, Bin Xu and Xinhong Zhang, "Digital image watermarking algorithm based on CDMA spread spectrum," 2006 12th International Multi-Media Modelling Conference, Beijing, 2006, pp. 4 pp.-. doi: 10.1109/MMMC.2006.1651359.

[13] T. T. Nguyen and D. Taubman, "Optimal linear detector for spread spectrum based multidimensional signal watermarking," 2009 16th IEEE International Conference on Image Processing (ICIP), Cairo, 2009, pp. 113-116. doi: 10.1109/ICIP.2009.5414121.

[14] E. Nezhadarya, Z. J. Wang and R. K. Ward, "Image quality monitoring using spread spectrum watermarking," 2009 16th IEEE International Conference on Image Processing (ICIP), Cairo, 2009, pp. 2233-2236. doi: 10.1109/ICIP.2009.5413955.

[15] S. Ghosh, P. Ray, S. P. Maity and H. Rahaman, "Spread Spectrum Image Watermarking with Digital Design," 2009 IEEE International Advance Computing Conference, Patiala, 2009, pp. 868-873. doi: 10.1109/IADCC.2009.4809129.
[16] H. O. Altun, A. Orsdemir, G. Sharma and M. F. Bocko, "Optimal Spread Spectrum Watermark Embedding via a Multistep Feasibility Formulation," in IEEE Transactions on Image Processing, vol. 18, no. 2, pp. 371-387, Feb. 2009. doi: 10.1109/TIP.2008.2008222.
[17] A. Samčović and M. Milovanović, "Robust digital image watermarking based on wavelet transform and spread spectrum techniques," 2015 23rd Telecommunications Forum Telfor (TELFOR), Belgrade, 2015, pp. 811-814. doi: 10.1109/TELFOR.2015.7377589.
[18] V. P. Ipatov, "Spread Spectrum and CDMA," Mar. 2005. doi:10.1002/0470091800.
[19] "Introduction to CDMA Wireless Communications," 2007. doi:10.1016/b978-0-7506-5252-0.x5001-7.
[20] "The Generalized CDMA," CDMA: Access and Switching, pp. 1–28. doi:10.1002/0470841699.
[21] S. Hara and R. Prasad, "DS-CDMA, MC-CDMA and MT-CDMA for mobile multi-media communications," Proceedings of Vehicular Technology Conference - VTC, Atlanta, GA, USA, 1996, pp. 1106-1110 vol.2. doi: 10.1109/VETEC.1996.501483.
[22] S. S. Agaian, H. G. Sarukhanyan, K. O. Egiazarian, and J. Astola, "Hadamard Transforms," Aug. 2011. doi:10.1117/3.890094.
[23] "Probability Theory of Bit Error Rate," Optical Bit Error Rate, 2009. doi:10.1109/9780470545430.ch7.
[24] J. Korhonen and J. You, "Peak signal-to-noise ratio revisited: Is simple beautiful?," 2012 Fourth International Workshop on Quality of Multimedia Experience, Yarra Valley, VIC, 2012, pp. 37-38. doi: 10.1109/QoMEX.2012.6263880
[25] "Data Compression," 2007. doi:10.1007/978-1-84628-603-2.
[26] L. Devroye, "Non-Uniform Random Variate Generation," 1986. doi:10.1007/978-1-4613-8643-8.
[27] Yu.V. Stasev, A.A. Kuznetsov, A.M. Nosik. "Formation of pseudorandom sequences with improved autocorrelation properties." Cybernetics and Systems Analysis, vol. 43, Issue 1, pp. 1-11, January 2007. DOI: 10.1007/s10559-007-0021-2
[28] N.I.Naumenko, Yu.V.Stasev, A.A.Kuznetsov. "Methods of synthesis of signals with prescribed properties." Cybernetics and Systems Analysis, vol. 43, Issue 3, pp. 321-326, May 2007. DOI: 10.1007/s10559-007-0052-8
[29] O.Karpenko, A.Kuznetsov, V.Sai, Yu.Stasev. "Discrete Signals with Multi-Level Correlation Function." Telecommunications and Radio Engineering, vol. 71, 2012 Issue 1. pp 91-98. DOI: 10.1615/TelecomRadEng.v71.i1.100
[30] A. Kuznetsov, S. Kavun, V. Panchenko, D. Prokopovych-Tkachenko, F. Kurinniy and V. Shoiko, "Periodic Properties of Cryptographically Strong Pseudorandom Sequences," 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 129-134. doi: 10.1109/INFOCOMMST.2018.8632021
[31] A. Kuznetsov, O. Smirnov, D. Kovalchuk, A. Averchev, M. Pastukhov and K. Kuznetsova, "Formation of Pseudorandom Sequences with Special Correlation Properties," 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2019, pp. 395-399. doi: 10.1109/AIACT.2019.8847861

Reviewer: Mikołaj Karpiński, Dr. of Sciences (Eng.), Full Prof., University of Bielsko-Biala, Bielsko-Biala, Poland.
E-mail: mkarpinski@ath.bielsko.pl

Received: January 2020.

Authors:
Oleksii Smirnov, Central Ukrainian National Technical University, avenue University, 8, 25006, Kropivnitskiy.
E-mail: dr.smirnovoa@gmail.com
Ludmila Gorbacheva, student of CSD, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
Alexandr Kuznetsov, Doctor of Sciences (Eng.), Full Prof., V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: kuznetsov@karazin.ua

Hiding information in images using pseudo-random sequences.

Abstract. In this article are discussed techniques of hiding information messages in cover image using direct spectrum spreading technology. This technology is based on the use of poorly correlated pseudorandom (noise) sequences. Modulating the information data with such signals, the message is presented as a noise-like form, which makes it very difficult to detect. Hiding means adding a modulated message to the cover image. If this image is interpreted as noise on the communication channel, then the task of hiding user's data is equivalent to transmitting a noise-like modulated message on the noise communication channel. At the same it is supposed that noise-like signals are poorly correlated both with each other and with the cover image (or its fragment). However, the latter assumption may not be fulfilled because a realistic image is not an implementation of a random process; its pixels have a strong correlation. Obviously, the selection of pseudo-random spreading signals must take this feature into account. We are investigating various ways of formation spreading sequences while assessing Bit Error Rate (*BER*) of information data as well as cover image distortion by mean squared error (*MSE*) and by Peak signal-to-noise ratio (*PSNR*). The obtained experimental dependencies clearly confirm the advantage of using Walsh sequences. During the research, the lowest *BER* values were obtained. Even at low values of the signal power of the spreading sequences ($P \approx 5$), the *BER* value, in most cases, did not exceed 0,01. This is the best result of all the sequences under consideration in this work. The values of *PSNR* when using orthogonal Walsh sequences are, in most cases, comparable to other considered options. However, for a fixed value of *PSNR*, using the Walsh transform results in significantly lower *BER* values. It is noted that a promising direction is the use of adaptively generated discrete sequences. So, for example, if the rule for generating expanding signals takes into account the statistical properties of the container, then you can significantly reduce the value of *BER*. Also, another useful result could be increasing *PSNR* at a fixed (given) value of *BER*. The purpose of our work is to justify the choice of extending sequences to reduce *BE*R and *MSE* (*increase PSNR*).

Keywords: Steganography; Direct spectrum Spreading technology; Pseudorandom sequence; Spreading signals.

Рецензент: Микола Карпінський, д.т.н., проф., університет Бельсько-Бяла, Бельсько-Бяла, Польща.
E-mail: mkarpinski@ath.bielsko.pl

Надійшло: Січень 2020.

Автори:
Олексій Смірнов, Центральній український національний технічний університет, проспект Університетський, 8, Кропивницький, 25006, Україна.
E-mail: dr.smirnovoa@gmail.com

Людмила Горбачова, студентка факультету комп'ютерних наук, Харківський національний університет імені В. Н. Каразіна, Харків, 61022, Україна.

Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, 61022, Україна.
E-mail: kuznetsov@karazin.ua

Приховування інформації в зображеннях з використанням псевдовипадкових послідовностей.

Анотація. У статті розглядаються техніки приховування інформаційних повідомлень в контейнерах-зображеннях з використанням технології прямого розширення спектра. В основі цієї технології лежить використання слабокорельованих між собою псевдовипадкових (шумових) послідовностей. Модулюючи інформаційні дані такими сигналами, повідомлення видається в шумоподібному вигляді, що суттєво ускладнює його виявлення. Приховування полягає в додаванні модульованого повідомлення до контейнера-зображення. Якщо інтерпретувати це зображення як шум у каналі зв'язку, тоді завдання приховування призначених для користувача даних еквівалентна передачі шумоподібного модульованого повідомлення по каналу зв'язку з шумом. При цьому передбачається, що шумоподібні сигнали слабокорельовані як один з одним, так і з контейнером-зображенням (або його фрагментом). Однак останнє припущення може не виконуватися, тому що реалістичне зображення не є реалізацією випадкового процесу, його пікселі мають сильну кореляцію. Очевидно, що вибір псевдовипадкових розширюючих сигналів повинен враховувати цю особливість. В роботі досліджено різні способи формування розширюючих послідовностей. Виконана оцінка інтенсивності бітових помилок (*Bit Error Rate, BER*) інформаційних даних, а також спотворення зображення - контейнера за середньоквадратичною помилкою *(mean squared error, MSE*) та піковому відношенню сигнал/шум (*Peak signal -to-noise ratio, PSNR*). Отримані експериментальні залежності наочно підтверджують перевагу користування послідовностей Уолша. В ході досліджень отримані найменші значення *BER*. Навіть при невеликих значеннях потужності сигналів розширюючих послідовностей ($P \approx 5$) величина *BER*, в більшості випадків, не перевищувала 0,01. Це являє собою кращий результат з усіх розглянутих в роботі варіантів розширюючих послідовностей. Значення *PSNR* при використанні ортогональних послідовностей Уолша, в більшості випадків, можна порівняти з іншими розглянутими варіантами. Однак для фіксованого значення *PSNR* використання перетворення Уолша призводить до значно менших величинам *BER*. Відзначено, що перспективним напрямком є використання дискретних послідовностей, які адаптивно формуються. Так, наприклад, якщо правило формування розширюючих сигналів буде враховувати статистичні властивості контейнера, то можна істотно знизити *BER*. Також, іншим корисним результатом може бути підвищення *PSNR* при фіксованому (заздалегідь заданому) значенні *BER*. Головною метою роботи є обгрунтування вибору розширюючих послідовностей для зниження *BER* і *MSE* (*збільшення PSNR*).

Ключові слова: стеганографія; технологія прямого розширення спектра; псевдовипадкова послідовність; сигнали розширення.