doi: 10.36724/2409-5419-2020-12-6-38-47

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТЕГОСИСТЕМ С ВЛОЖЕНИЕМ В НАИМЕНЬШИЕ ЗНАЧАЩИЕ БИТЫ С СОГЛАСОВАНИЕМ И С ЗАМЕЩЕНИЕМ

**АХРАМЕЕВА**
**Ксения Андреевна**[1]

**ГЕРЛИНГ**
**Екатерина Юрьевна**[2]

АННОТАЦИЯ

В работе представлены результаты сравнительного анализа стегосистем с алгоритмами вложения в наименьший значащий бит с согласованием и с замещением на предмет различия процедуры вложения дополнительной информации в покрывающий объект и стойкости полученных стеганограмм к различным методам стегоанализа. При использовании стегосистем с алгоритмами вложения в наименьший значащий бит с согласованием и с замещением получены выборки стеганограмм с различными долями вложения по взятой выборке из 200 покрывающих объектов. Проанализированы результаты стегоанализа на данные стеганограммы, произведено сравнение полученных выборок стеганограмм к обнаружению наличия вложения дополнительной информации, при помощи трех методов стегоанализа: визуальной атаки, статистической атаки первого порядка (атака хи-квадрат) и статистической атаки второго порядка (атака парно-выборочного анализа). Представленный пример изображений до и после визуальной атаки, для выборок стеганограм с вложениями в наименьший значащий бит с замещением и с согласованием, при долях вложения в 10%, 50% и 100%, позволяет наглядно продемонстрировать результативность визуального метода стегаонализа. Графическая форма представления результатов по атакам первого и второго порядков позволяет оценить эффективность исследуемых методов стегоанализа для стегосистем с алгоритмами вложения в наименьший значащий бит с согласованием и с замещением. Показано, что стегосистема с алгоритмом вложения в наименее значащие биты с согласованием является более устойчивой к атакам обнаружения, использующим современные методы стегоанализа. Сделаны выводы о возможности применения рассмотренных методов стегоанализа к представленным методам стегосистем.

**Сведения об авторах:**

[1]к.т.н., доцент Санкт-Петербургского государственного университета телекоммуникации им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, oklaba@mail.ru

[2]к.т.н., доцент Санкт-Петербургско гогосударственного университета телекоммуникации им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, gerlingeu@gmail.com

КЛЮЧЕВЫЕ СЛОВА: стеганография; вложение в наименьшие значащие биты; стегоанализ; покрывающий объект; стеганограмма.

**Для цитирования:** *Ахрамеева К.А., Герлинг Е.Ю.* Сравнительный анализ стегосистем с вложением в наименьшие значащие биты с согласованием и с замещением // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 6. С. 38–47. doi: 10.36724/2409-5419-2020-12-6-38-47

**Введение**

Защита частной информации является основной задачей стеганографии. Это один из наиболее древних и распространённых методов сокрытия информации, суть которого заключается в маскировке защищаемой информации внутри других, безобидных невинных данных (покрывающий объект) [1]. После вложения скрываемой информации в покрывающий объект получается стеганограмма (либо стегообъект). Стеганография определяется как наука сокрытия информации таким образом, чтобы существование вложенной информации не обнаруживалось посторонним наблюдателем или программным обеспечением[1].

В современном мире активно развивается цифровая стеганография, позволяющая скрывать информацию в покрывающих объектах, которые представляют собой оцифрованную информацию, например, в компьютерных файлах различных форматов, в заголовках пакетов различных протоколов и т.д. [2] Компьютеры и компьютерные сети передачи данных прочно вошли в нашу жизнь. Объемы информации в цифровом виде, в том числе конфиденциальной, личного характера, представляющей коммерческую тайну и т.д., хранящейся и передающейся по современным сетям, растут каждый день. Защита этих данных от несанкционированного прочтения, удаления или использования сегодня является актуальной и остро стоящей задачей. Для построения надежной и безопасной информационной системы с хранением и передачей информации необходимо неуклонно соблюдать три принципа — конфиденциальность, целостность и доступность[2]. Для обеспечения конфиденциальности, т.е. для защиты личных данных, коммерческой тайны и т.д. все чаще применяются методы цифровой стеганографии. Поэтому на сегодняшний день развитие, исследование, сравнения и разработка новых методов стеганографии также является актуальной задачей. Но при этом методы стеганографии могут быть использованы и для незаконного обмена информацией, например, для распространения нелегального контента, для общения террористическими группировками и т.д. Поэтому остро также стоит и вопрос выявления скрытой информации в невинных объектах. Для выявления скрытой информации активно разрабатываются методы стегоанализа.

В данной работе далее речь пойдет именно о цифровой стеганографии, для краткости будем называть ее просто «стеганография».

Наиболее распространенным и одним из самых простых методов построения стегосистем является метод вложения в наименьшие значащие биты отсчетов покрывающего объекта. На сегодняшний момент наиболее распространенными являются два метода стегосистем с вложением в наименьшие значащие биты: стегосистемы с вложением в наименьшие значащие биты с замещением (СГ-НЗБ) и стегосистемы с вложением в наименьшие значащие биты с согласованием (СГ-±1-НЗБ). Согласно ранее проведенным исследованиям [3] именно эти два метода чаще всего встречаются в современном программном обеспечении, использующем методы стеганографии.

Также согласно все там же исследованиям в качестве покрывающих объектов, как правило, используются медиафайлы с неподвижными изображениями [4]. Поэтому далее в данной работе в качестве объектов исследования использованы файлы с неподвижными изображениями [5].

**Описание стегосистемы с вложением в наименьшие значащие биты с замещением**

Рассмотрим метод вложения в наименьшие значащие биты с замещением (СГ-НЗБ) на примере неподвижного растрового изображения[3].

Алгоритм вложения СГ-НЗБ очень прост, если необходимо вложить бит информации, равный 1, то наименее значащий бит пикселя меняется на 1 (вне зависимости от того, какой именно бит там был в покрывающем объекте). Если необходимо вложить бит информации, равный 0, то наименее значащий бит пикселя меняется на 0 [6].

Покрывающий объект можно представить в виде последовательности L-битовых отсчетов

$$C(n) = \sum_{i=0}^{L-1} C_i(n)2^i,$$

где $C(n)$ — это отсчеты покрывающего объекта;

$n$ — количество отсчетов в покрывающем объекте;

$L = 2^t$ — количество уровней;

$t$ — количество биты на пиксель (поскольку в работе рассматривается пример с неподвижным растровым изображением);

$C_i(n) = 0,1$ — двоичные коэффициенты.

После вложения дополнительной информации гистограмма изображения примет вид:

$$C_w(n) = \sum_{i=1}^{L-1} c_i(n) \cdot 2^i + b(n),$$

где $C_w(n)$ — это отсчеты стеганограммы;

$b(n)$ — погружаемый в $n$-ый отсчет бит информации $b \in (0,1)$.

[1]Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: СОЛОН-ПРЕСС, 2016. 262 с.

[2]Рябко В.Я., Фионов А.Н. Основы современной криптографии и стеганографии. М.: Горячая линия, Телеком, 2010. 232 с.

[3]Fridrich J. Steganography in Digital Media Principles, Algorithms, and Applications. Cambridge UnivP, 2010. 462 p.

*Пример:* Имеется изображение с градациями яркости $L = 256$, $t = 8$ (8 бит на пиксель).

$C(n) = 00101101 = 45$ (пиксель имеет яркость 45).

Если вкладываемый бит $b(n) = 0$, то в стеганограмме получаем уровень яркости $C_w(n) = 00101100 = 44$.

Если вкладываемый бит $b(n) = 1$, то в стеганограмме получаем уровень яркости $C_w(n) = 00101101 = 45$.

Таким образом, последний бит при вложении 1 заменяется на 1, а при вложении 0 — на 0. В примере, в каждый пиксель можно вложить один бит информации.

Процесс извлечения вложенных бит можно представить следующим выражением:

$$\begin{aligned}&\tilde{b}(n) = 0, \text{ если } C_w(n) - \text{четное число, т. е. НЗБ } \left(C_w(n)\right) = 0;\\ &\tilde{b}(n) = 1, \text{ если } C_w(n) - \text{нечетное число, т. е. НЗБ } \left(C_w(n)\right) = 1.\end{aligned} \quad (1)$$

Как следует из формулы (1), если наименьший значащий бит в пикселе стеганограммы равен 1, то извлекается 1, если 0 — то 0.

**Описание стегосистемы с вложением в наименьшие значащие биты с согласованием**

Процедура вложения для стегосистемы с вложением в наименьшие значащие биты с согласованием (СГ-±1-НЗБ) имеет следующий вид[4]:

$$C_w(n) = \begin{cases} C(n), \text{ если НЗБ } (C(n)) = b(n);\\ \left.\begin{matrix} C(n)+1, \text{ с вероятностью } 1/2\\ C(n)-1, \text{ с вероятностью } 1/2 \end{matrix}\right\}, \text{ если НЗБ } (C(n)) \neq b(n). \end{cases} \quad (2)$$

Из выражения (2) видно, что вложение представляет собой рандомизированный алгоритм.

*Пример.* Допустим, имеется цифровое изображение, в котором $x_5 = 228$, $x_6 = 202$, $x_7 = 202$. Что в двоичном представлении соответствует $x_5 = 11100100$, $x_6 = 11001010$, $x_7 = 11001010$. Например, необходимо передать сообщение, представленное битами 011. Тогда встраиваемая последовательность бит будет, соответственно, $m_5=0$, $m_6=1$, $m_7=1$. Следовательно, соответствующие яркости пикселов стеганограммы будут: $x_5 = 11100100$ ($x_5 = 228$), $x_6 = 11001001$ ($x_6 = 201$), $x_7 = 11001011$ ($x_7 = 203$).

Таким образом, в СГ-±1-НЗБ в процессе вложения дополнительной информации младший (наименьший значащий) бит, также как и в предыдущем методе, изменяется в зависимости от соответствующего бита встраиваемого сообщения, но при этом происходит «сглаживание» новой, полученной после вложения, гистограммы. «Сглаживание» достигается за счет того факта, что при вложении битов информации со значением 1, яркость будет увеличиваться и уменьшаться с равной вероятностью, и перераспределение значений количества пикселей будет происходить не между двумя соседними отчетами, как в СГ-НЗБ, а между 3 следующими друг за другом отчетами.

**Описание методов стегоанализа**

В данной работе рассмотрим 3 основных метода стегоанализа на стегосистемы с вложением в наименьшие значащие биты, основанные на статистических свойствах исследуемого объекта [8,9]:

1. визуальная атака;
2. статистическая атака первого порядка;
3. статистическая атака второго порядка

Для проведения сравнительного анализа применим приведенные выше атаки и к СГ-НЗБ и к СГ-±1-НЗБ.

Для проведения визуального стегоанализа необходимо привести исследуемое изображения (цветное или в градациях серого) к черно-белому. Для перевода изображения к черно-белому необходимо воспользоваться следующим алгоритмом:

$$\text{если } C_0(n) = 1, \text{то } \tilde{C}(n) - \text{белое};$$
$$\text{если } C_0(n) = 0, \text{то } \tilde{C}(n) - \text{черное},$$

где $C_0(n)$ — значение наименьшего значащего бита $n$-го пикселя;

$\tilde{C}(n)$ — значение пикселя в новом черно-белом изображении.

Далее, как правило, необходимо присутствие человека, который визуально рассмотрит полученное черно-белое изображение. Если на полученном черно-белом изображении видны контуры оригинального изображения, то следует сделать вывод, что вложения нет. Если вместо контуров исходного изображения виден шум — делается вывод, что дополнительное вложение есть. Основным недостатком данного метода является сложный механизм автоматизации (пример автоматизации визуального метода рассмотрен, например, в [10]) и, как следствие, необходимость присутствия человека-оператора, для принятия окончательного решения о наличии или отсутствии вложения в исследуемом объекте.

Статистическая атака первого порядка — атака хи-квадрат сводится к расчету параметра $\chi^2$:

$$\chi^2 = \sum_{j=0}^{\left[(L-1)/2\right]} \frac{\left(n_{2j} - n_{2j+1}\right)^2}{2\left(n_{2j} + n_{2j+1}\right)},$$

где $n_{2j}$ — это количество пикселей оттенка $2j$;

$n_{2j+1}$ — это количество пикселей оттенка $2j+1$;

[4]Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография: монография. СПб.: СПбГУТ, 2016. 226 с.

$L$ — это общее количество пикселей в исследуемом изображении.

Критерий обнаружения стегосистем с вложением в наименьшие значащие биты будет иметь следующий вид:

$$H_0 : \chi^2 \geq \chi_0^2;$$
$$H_1 : \chi^2 < \chi_0^2,$$

где $H_0$ — гипотеза, при которой вложение дополнительной информации отсутствует;

$H_1$ — гипотеза, при которой вложение дополнительной информации присутствует;

$\chi_0^2$ — это некоторое пороговое значение, которое необходимо выбрать заранее.

Стегоанализ на основе статистики второго порядка был впервые предложен в работе [3]. Данный метод стегоанализа разрабатывался для обнаружения вложений, выполненных методом СГ-НЗБ. Еще одно название данного метода sample pair analysis — парно-выборочный анализ.

Для атаки методом парно-выборочного анализа критерий обнаружения имеет следующий вид:

$$H_0 : \tilde{P} \leq \tilde{P}_0;$$
$$H_1 : \tilde{P} > \tilde{P}_0,$$

где $\tilde{P}_0$ — это пороговое значение, в [12] рекомендуется в качестве порогового значения использовать «0»; а параметр $\tilde{P}$ рассчитывается по следующему правилу:

$$\tilde{P} = \frac{\frac{2D_0 + 2Y_1 - D_2 - 2X_1}{2}}{\frac{2C_0 - C_1}{2}} - \frac{\sqrt{\left(-\frac{2D_0 + 2Y_1 - D_2 - 2X_1}{2}\right)^2 - 4\frac{2C_0 - C_1}{4}(Y_1 - X_1)}}{\frac{2C_0 - C_1}{2}},$$

где $C_0$ — это количество пар, которые совпадают в первых семи битах;

$C_1$ — количество пар, которые отличаются на 1 в первых семи битах;

$D_0$ — это количество пар, которые совпадают во всех битах;

$D_2$ — это количество пар, которые отличаются на 2;

X — это количество пар вида ($2k$, $2k$-1), где $k$ — целое число;

Y — это количество пар вида ($2k$+1, $2k$), где $k$ — целое число.

Особенность метода парно-выборочного анализа заключается еще и в том, что при малых (менее 10%) долях вложенной информации значение $\tilde{P}$ показывает оценку доли вложенной информации. Данное значения позволяет оценить количество скрываемой информации, которая передается в исследуемой стеганограмме.

**Практические результаты**

Исследование проводилось на выборке из 200 изображений, которые являются покрывающими объектами. В изображения из выборки было произведено вложение по методам СГ-НЗБ и СГ-±1-НЗБ. Результаты экспериментов по стойкости данных методов к различным методам стегоанализа приведены ниже.

Так, результаты визуального стегоанализа для СГ-НЗБ и СГ-±1-НЗБ при различных долях вложения приведены на рис. 1 и 2, соответственно.

Как видно из рис. 1–2, визуальная атака практически во всех случаях определяет наличие вложенного сообщения при доле вложения более 10%. Как известно [13], визуальная атака не является достоверной и эффективной, и если стегоаналитик наблюдает шумовое поле — такое изображение требует дальнейшего анализа, поскольку нельзя однозначно сказать, что данное изображения имеет вложение, а не является, например, изображением с сильным шумом.

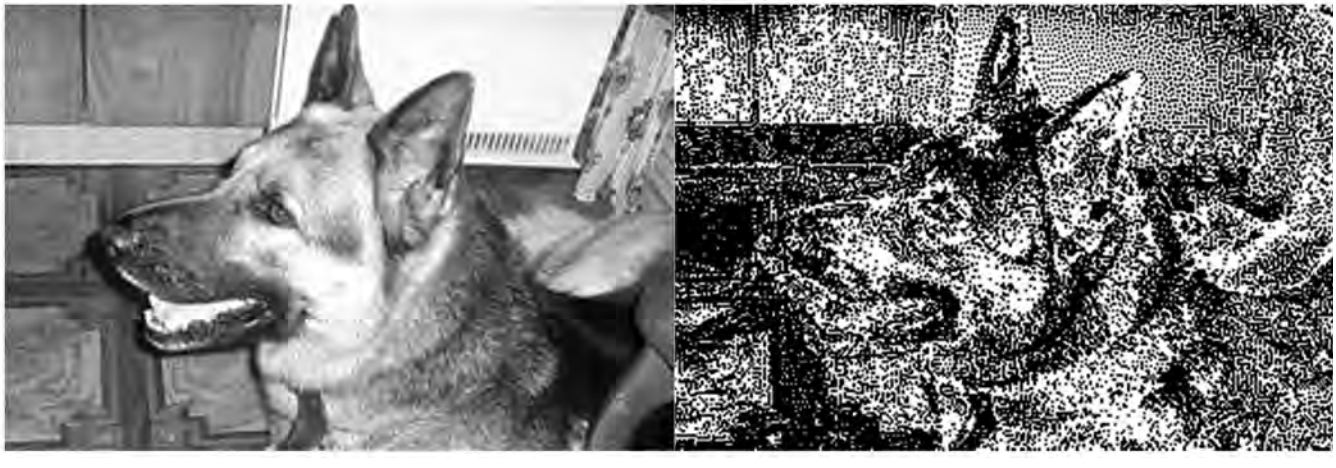


**Рис. 1.** Изображения с вложением по методу СГ-НЗБ до и после атаки, при долях вложения а) 0%, б) 10%, в) 50%, г) 100%

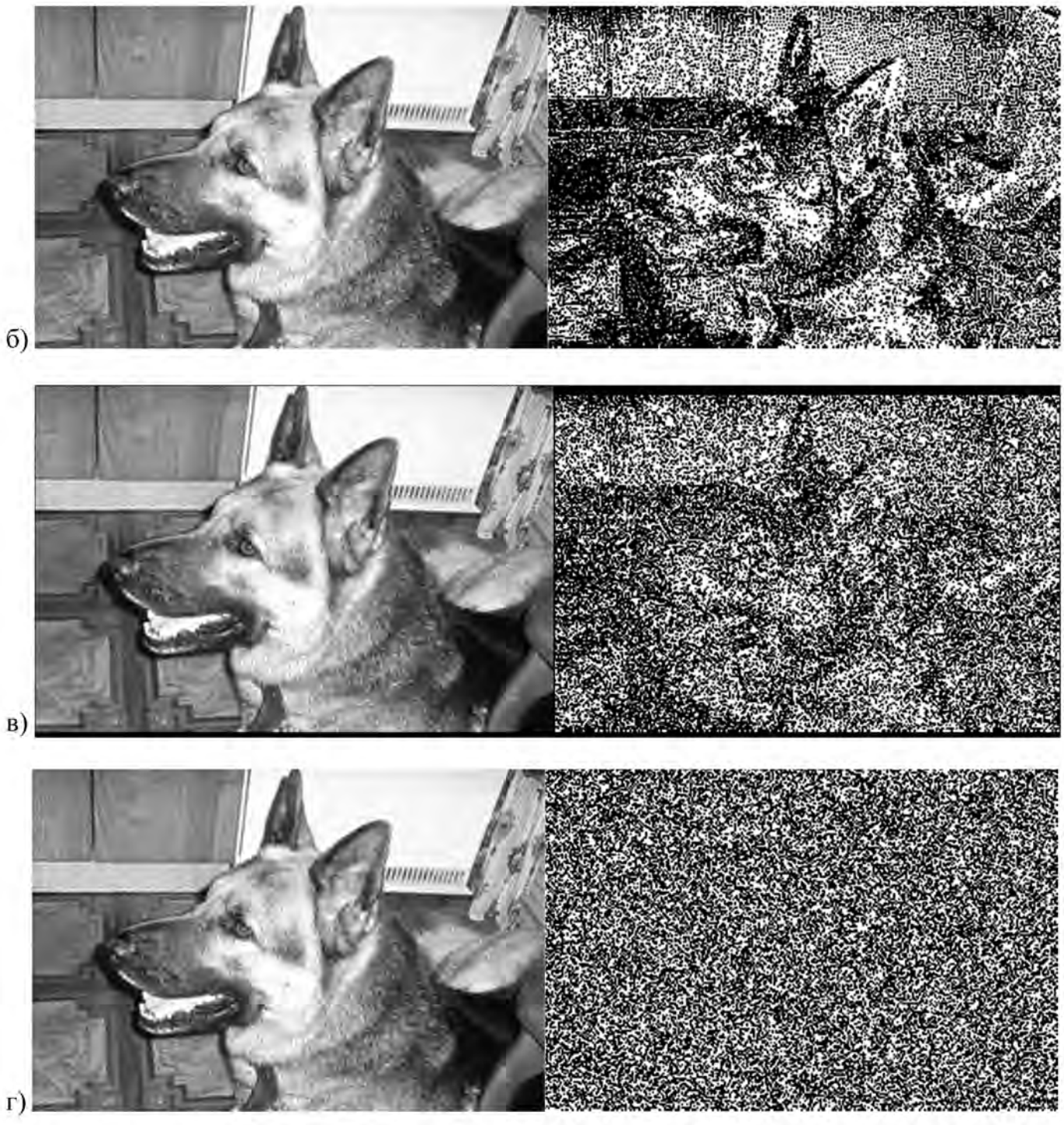


**Рис. 1.** Изображения с вложением по методу СГ-НЗБ до и после атаки, при долях вложения а) 0%, б) 10%, в) 50%, г) 100%

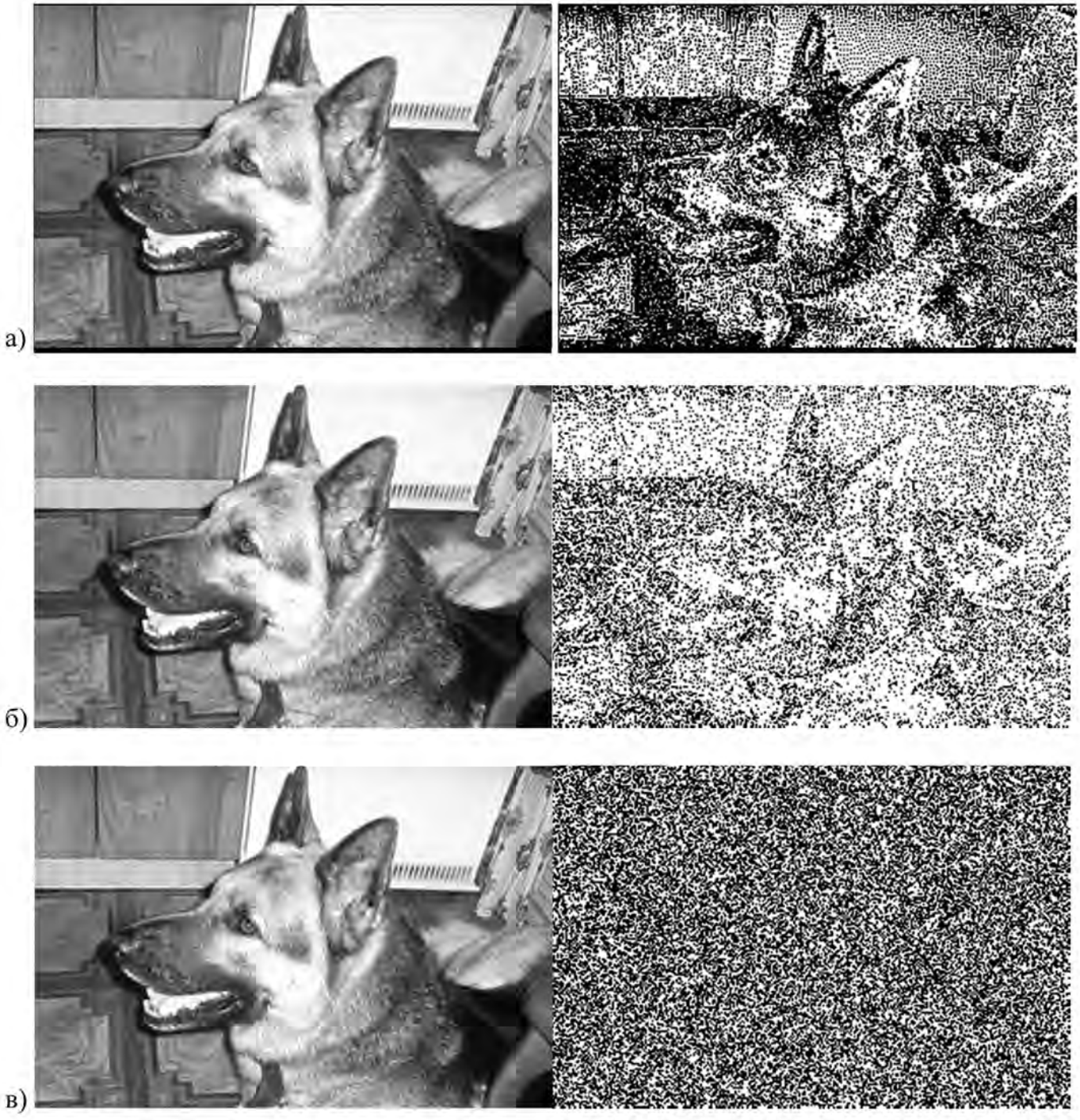


**Рис. 2.** Изображения с вложением по методу СГ-НЗБ+-1 до и после атаки, при доле вложения а) 10%, б) 50%, в) 100%

И в то же самое время четкость контуров исходного изображения позволяет сделать вывод об отсутствии в данном образце вложения. Так рис. 1б) и 2б), с долей вложения 10%, имеют четкие контуры исходного изображения, и следовательно, логичнее сделать вывод, что в данных исследуемых объектах нет вложения.

Гораздо эффективнее и надежнее выявляют скрытые вложения методы статистического стегоанализа, два из которых будут рассмотрены далее. Для наглядности результаты исследований статистического стегоанализа приведены на графиках, изображенных на рис. 3–8.

Так на рис. 3–5 отображены значения $\chi^2$ покрывающих объектов, а также стеганограмм, созданных с помощью методов СГ-НЗБ и СГ-±1-НЗБ при долях вложения 10%, 50% и 100%, соответственно.

Из графиков, представленных на рис. 3–5 можно сделать вывод, что для СГ-±1-НЗБ данный метод стегоанализа менее эффективный, чем для метода СГ-НЗБ, поскольку во всех 3 случаях график, отображающий распределение СГ-±1-НЗБ, расположен ближе к графику покрывающего объекта, чем график СГ-НЗБ. Также заметим, что для выборок однотипных изображений (с одинаковыми размерами, качеством изображения) возможно выбрать пороговое значение для обнаружения СГ-НЗБ. Для стегосистем с вложением по методу СГ-±1-НЗБ так же возможно выбрать пороговое значение, однако в данном случае эффективность обнаружения будет ниже, чем в случае с СГ-НЗБ, либо неэффективной, что обуславливается симметричным характером вложения СГ-±1-НЗБ.

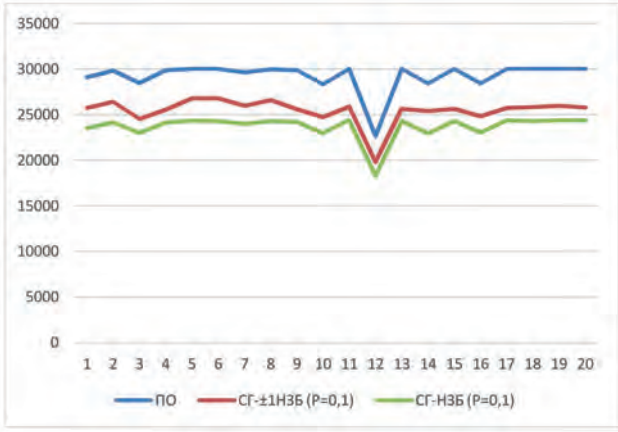


**Рис. 3.** График распределения значений $\chi^2$ для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 10%

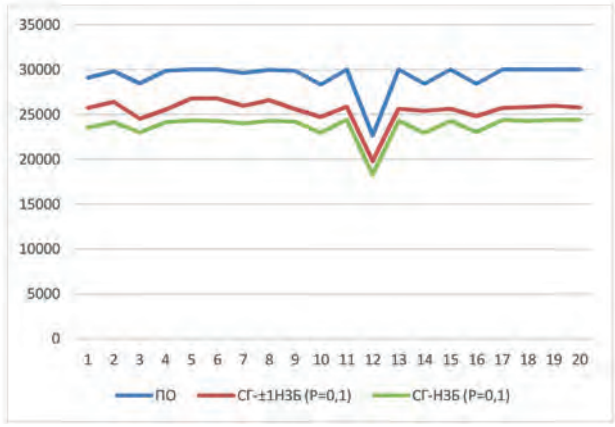


**Рис. 5.** График распределения значений $\chi^2$ для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 100%

Результаты исследований по методу парно-выборочного анализа выборок покрывающих объектов и соответствующим им стеганограмм, созданным с помощью СГ-НЗБ и СГ-±1-НЗБ представлены на рис. 6–8.

Как видно из графиков, представленных на рис. 6–8, с помощью стегоанализа по методу парно-выборочного

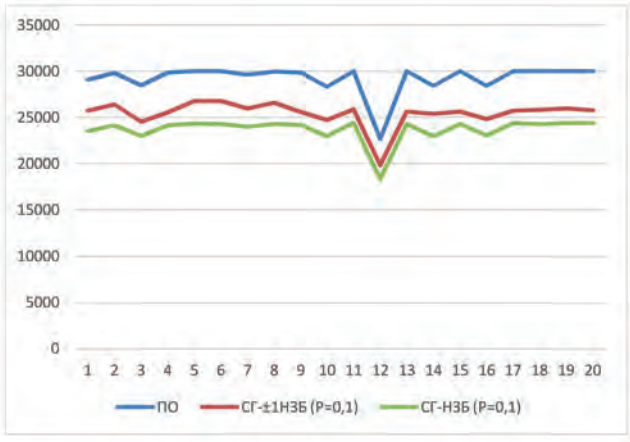


**Рис. 4.** График распределения значений $\chi^2$ для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 50%

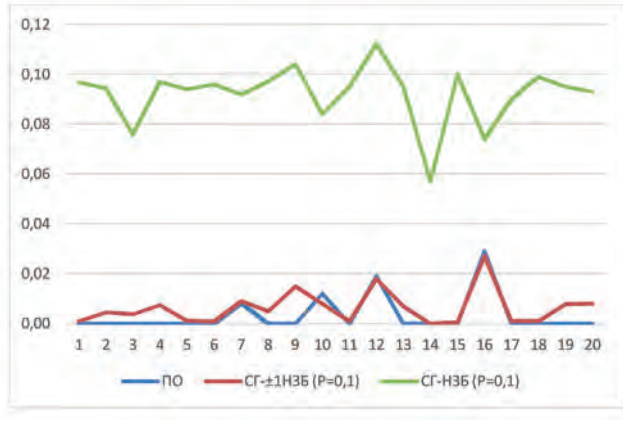


**Рис. 6.** График распределения значений $P'$ для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 10%

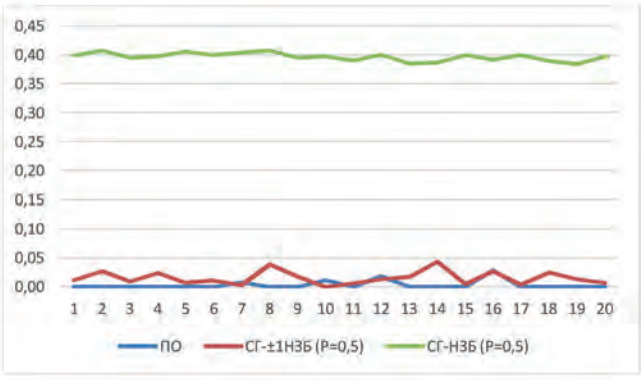


**Рис. 7.** График распределения значений *P*' для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 50%

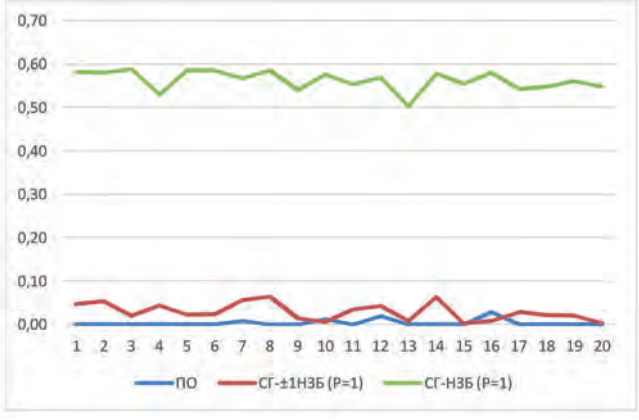


**Рис. 8.** График распределения значений *P*' для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 100%

анализа не только возможно определить наличие вложения, выполненного по методу СГ-НЗБ, но и выбрать универсальный порог для всех исследуемых объектов, оптимальным пороговым значением по мнению авторов метода является значение 0. Также отметим, что парно-выборочный метод анализа позволяет оценить долю вложенное информации, если доле вложения не более 10%.

При этом, для метода вложения СГ-±1-НЗБ данный вид стегоанализа оказывается неэффективным, поскольку графики покрывающего объекта и СГ-±1-НЗБ, если и не сливаются в одну линию, то пересекаются и идут очень близко на всех 3 графиках. Следовательно, в данном случае рекомендованное авторами метода пороговое значение окажется неэффективным, а самостоятельно выбрать данный порог крайне сложно.

Как показано, метод с замещением достаточно легко обнаруживается с помощью рассмотренных выше методов стегоанализа, поскольку вложение методом СГ-НЗБ носит асимметричный характер. При этом рассмотренные выше методы стегоанализа оказались неэффективны для СГ-±1-НЗБ.

**Заключение**

Основная идея использования СГ-±1-НЗБ вместо обычного НЗБ-замещения заключается в том, что обычное СГ-НЗБ обладает некоторой несимметрией. Что, в свою очередь, приводит к появлению характерных статистических признаков, позволяющих сделать процедуру обнаружения более надежной. Рандомизация отчетов в процессе вложении дополнительных бит информации позволяет уменьшить изменения статистических свойств гистограммы стеганограммы, и приблизить их к статистический свойствам покрывающего объекта, таким образом данный метод вложения становится более устойчивым к статистическим методам стегоанализа.

Сравнительный анализ стегоатак относительно стегосистем СГ-НЗБ и СГ-±1-НЗБ показал, что:

- СГ-НЗБ не стойка к визуальной атаке с долей вложения более 50%. Модифицированная СГ-НЗБ — СГ-±1-НЗБ так же подвержена визуальной атаке, хотя и более секретна по отношению с СГ-НЗБ за счет симметричного вложения;
- эффективность применения стегоанализа на основе статистики первого порядка относительно СГ-НЗБ выше, чем для СГ-±1-НЗБ.
- СГ-±1-НЗБ стойко к стегоанализу на основе статистики второго порядка, в отличие от СГ-НЗБ, для которого данный вид атаки позволяет не только определить наличие вложения, но и оценить долю вложения, из которой можно рассчитать погруженное количество бит.

На основе материалов, представленных выше, можно сделать вывод, что СГ-±1-НЗБ обеспечивает большую секретность, чем СГ-НЗБ, вследствие чего, если стоит выбор из двух стегосистем, для хранения и передачи дополнительной информации рекомендуется использовать стегосистемы с вложением в наименьший значащий бит с согласованием.

При этом, в дальнейшей работе стоит рассмотреть возможные модификации вложения в наименьшие значащие биты, для повышения стойкости к известным методам стегоанализа. Для стегоаналитиков необходимо модифицировать известные и разработать новые методы стегоанализа для рассмотренных выше стегосистем, для улучшения методов обнаружения.

**Литература**

1. *Годлевский А. К., Коржик В. И.* Стегосистемы повышенной секретности для вложения информации в неподвижные изображения // Сборник научных статей V международной научно-технической и научно-методической конференции «Актуальные

проблемы инфотелекоммуникаций в науке и образовании». 2016. С. 320–323.

2. *Shterenberg S.I., Krasov A.V., Ushakov I.A.* Analysis of using equivalent instructions at the hidden embedding of information into the executable files // Journal of Theoretical and Applied Information Technology. 2015. Vol. 80. No. 1. С. 28–34.

3. *Герлинг Е.Ю., Ахрамеева К.А.* Обзор современного программного обеспечения, использующего методы стеганографии // Экономика и качество систем связи. 2019. № 3 (13). С. 51–58.

4. *Nie S.A., Abel A., Sulong G., Ali R.* The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image // International Journal of Electrical and Computer Engineering. 2019. Vol. 9. No. 6. Pp. 5218–5226.

5. *Ker A.* Steganalysis of LSB Matching in Grayscale Images // Signal Processing Letters. 2005. Vol. 12. Pp. 441–444.

6. *Luo W., Huang F., Huang Luo J.* Edge Adaptive Image Steganography Based on LSB Matching Revisited // Transactions on Information Forensics and Security. 2010. Vol. 5. Pp. 201–214.

7. *Lee Y.-K., Bell G., Huang S.-Y., Wang R.-Z., Shyu S.-J.* An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding // Lecture Notes in Computer Science. 2009. Vol. 5414. Pp. 349-360.

8. *Korzhik V., Nguyen C., Fedyanin I., Morales-Luna G.* Side attacks on stegosystems executing message encryption previous to embedding // Journal of Information Hiding and Multimedia Signal Processing. 2020. Vol. 11. No. 1. Pp. 44–57.

9. *Korzhik V., Fedyanin I., Godlewski A., Morales-Luna G.* Steganalysis Based on Statistical Properties of the Encrypted Messages // In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. LNCS10446. 2017. Pp. 288–298. DOI: 10.1007/978–3–319–65127–9_23

10. *Ахрамеева К.А., Герлинг Е.Ю., Радынская В.Е.* Автоматизация визуального метода на НЗБ // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1. Естественные и технические науки. 2020. № 1. С. 42–45.

11. *Dumitrescu S., Wu X., Wang Z.* Detection of LSB Steganography via Sample Pair Analysis // IEEE Transactions on Signal Processing. 2003. Vol. 51. No. 7. Pp. 1995–2007. doi: 10.1109/TSP.2003.812753

12. *Dumitrescu S., Wu X., Wang Z.,* Detection of LSB Steganography via Sample Pair Analysis // Information Hiding. IH 2002. Lecture Notes in Computer Science / Petitcolas F.A.P. (eds). Springer, Berlin, Heidelberg, 2003. Vol. 2578. Pp. 355–372.

13. *Герлинг Е.Ю.* Исследование эффективности методов обнаружения стегосистем, использующих вложение в наименее значащие биты // Информационные системы и технологии. 2011. № 4. С. 137–144.

## COMPARATIVE ANALYSIS OF STEGOSYSTEMS WITH EMBEDDING IN THE LEAST SIGNIFICANT BITS WITH MATCHING AND SUBSTITUTION

**KSENIYA A. AKHRAMEEVA**

St-Petersburg, Russia, oklaba@mail.ru

**EKATERINA U. GERLING**

St-Petersburg, Russia, gerlingeu@gmail.com

**KEYWORDS:** steganography; embedding in the smallest significant bits; steganalysis; covering object; steganogram.

**ABSTRACT**

The work presents the results of a comparative analysis of stegosystems with algorithms for embedding in the least significant bit with matching and substitution for differences in the procedure for embedding additional information in the covering object and the resistance of the obtained steganograms to various methods of steganalysis. When using stegosystems with embedding algorithms in the least significant bit with matching and substitution, samples of steganograms with different embedding fractions were obtained for a sample of 200 covering objects. The results of the steganogram analysis on the steganogram data were analyzed, the obtained steganogram samples were compared to the detection of the presence of an additional information attachment using three steganalysis methods: visual attack, first-order statistical attack (chi-square attack) and second-order statistical attack (pairwise selective analysis

attack). The presented example of images before and after a visual attack, for samples steganograms with attachments in the least significant bit with substitution and matching, with an investment fraction of 10%, 50% and 100%, allows to demonstrate the performance of the visual method steganalysis. The graphical representation of the results for first-and second-order attacks allows us to evaluate the effectiveness of the studied methods of stegoanalysis for stegosystems with algorithms for embedding in the least significant bit with matching and substitution. It is shown that a stegosystem with an algorithm for embedding in the least significant bits with matching is more resistant to detection attacks using modern methods of stegoanalysis. Conclusions are made about the possibility of applying the considered methods of stegoanalysis to the presented methods of stegosystems.

**REFERENCES**

1. Godlevskiy A., Korzhik V. Stegosystem with Improved Security for Embedding of Information Into Digital Motionless Images. *V sborni-ke: Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii sbornik nauchnyh statej V mezhdunarodnoj nauchno-tehnicheskoj i nauchno-metodicheskoj konferencii* [In the collection: Actual problems of infotelecommunications in science and education collection of scientific articles of the V international scientific-technical and scientific-methodical conference] 2016. Pp. 320–323.

2. Shterenberg S.I., Krasov A.V., Ushakov I.A. Analysis of using equivalent instructions at the hidden embedding of information into the executable files. *Journal of Theoretical and Applied Information Technology.* 2015. Vol. 80. No. 1. C. 28–34.

3. Gerling E.U., Ahrameeva K.A. The review of the modern software using sreganography methods. *Jekonomika i kachestvo sistem svjazi* [Economy and quality of communication systems] 2019. No. 3 (13). Pp. 51–58. (In Rus)

4. Nie S.A., Abel A., Sulong G., Ali R. The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image. *International Journal of Electrical and Computer Engineering*. 2019. Vol. 9. No. 6. Pp. 5218–5226.

5. Ker A. Steganalysis of LSB Matching in Grayscale Images. *Signal Processing Letters.* 2005. Vol. 12. Pp. 441–444.

6. Luo W., Huang F., Huang Luo J. Edge Adaptive Image Steganography Based on LSB Matching Revisited. *Transactions on Information Forensics and Security.* 2010. Vol. 5. Pp. 201–214.

7. Lee Y.-K., Bell G., Huang S.-Y., Wang R.-Z., Shyu S.-J. An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding. *Lecture Notes in Computer Science*. 2009. Vol. 5414. Pp. 349-360.

8. Korzhik V., Nguyen C., Fedyanin I., Morales-Luna G. Side attacks on stegosystems executing message encryption previous to embedding. *Journal of Information Hiding and Multimedia Signal Processing.* 2020. Vol. 11. No. 1. Pp. 44–57.

9. Korzhik V., Fedyanin I., Godlewski A., Morales-Luna G. Steganalysis Based on Statistical Properties of the Encrypted Messages. *In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security.* LNCS10446. 2017. Pp. 288–298. DOI: 10.1007/978–3–319–65127–9_23

10. Ahrameeva K.A. Gerling E.U., Radynskaya V.E. Automatization for visual steganalysis of LSB. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tehnologii i dizajna. Serija 1. Estestvennye i tehnicheskie nauki* [Vestnik of St. Petersburg State University of Technology and Design. Series 1. Natural and technical sciences] 2020. No. 1. Pp. 42–45.

11. Dumitrescu S., Wu X., Wang Z. Detection of LSB Steganography via Sample Pair Analysis. *IEEE Transactions on Signal Processing.* 2003. Vol. 51. No. 7. Pp. 1995–2007. doi: 10.1109/TSP.2003.812753

12. Dumitrescu S., Wu X., Wang Z., Detection of LSB Steganography via Sample Pair Analysis. *Information Hiding. IH 2002. Lecture Notes in Computer Science.* By ed. Petitcolas F.A.P. Springer, Berlin, Heidelberg, 2003. Vol. 2578. Pp. 355–372.

13. Gerling, E.U. Investigation of the effectiveness of detection methods stegosystems, which use an embedding to the least significant bits. *Informacionnye sistemy i tehnologii* [Information systems and technologies.] 2011. No. 4. Pp. 137–144. (In Rus)

**INFORMATION ABOUT AUTHORS:**

Akhrameeva K.A., PhD, Associate Professor at the Department of Secure Communication Systems, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications;

Gerling E.U., PhD, Associate Professor at the Department of Secure Communication Systems, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications.

**For citation:** Akhrameeva K.A., Gerling E.U. Comparative analysis of stegosystems with embedding in the least significant bits with matching and substitution. *H&ES Research*. 2020. Vol. 12. No. 6. Pp. 38–47. doi: 10.36724/2409-5419-2020-12-6-38-47 (In Rus)