УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 3, pp. 221-230

ИСПОЛЬЗОВАНИЕ МЕТОДА АНАЛИЗА ROC-КРИВЫХ ДЛЯ КОМПЛЕКСНОЙ ОЦЕНКИ ЭФФЕКТИВНОСТИ СТЕГАНОАНАЛИТИЧЕСКОГО МЕТОДА

И.И. Бобок

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: onu_metal@ukr.net

Представлены результаты анализа эффективности и сравнения работы нового стеганоаналитического метода детектирования стеганографических вложений, осуществленных методом модификации наименьшего значащего бита, в цифровое изображение, хранимое в формате с потерями, разработанного автором ранее, с наиболее эффективными существующими аналогами. Оценка работы методов производится при помощи ROC-анализа. Представлены результаты вычислительных экспериментов

Ключевые слова: стеганоанализ, метод модификации наименьшего значащего бита, ROC-анализ, точка отсечения

Введение

Стеганография, один из древнейших способов сокрытия и защиты информации, переживает в настоящий момент очередной виток в своем развитии, результатом чего является активизация работы в области стеганоанализа (СА) [1-6]. Стеганография и СА – два взаимосвязанных и взаимозависимых звена одной цепи: развитие одного звена приводят к адекватному ответу в другом, хотя цели и задачи их различны. Так общим для стеганографирования является организация тайного канала связи внутри открытого канала: в непривлекающий внимание объект – контейнер (или основное сообщение (ОС)) погружается секретная, или дополнительная, информация (ДИ) таким образом, что ее наличие в составе ОС остается незамеченным. Результатом такого погружения, или стеганопреобразования (СП), является стеганосообщение (СС), которое открыто пересылается адресату по каналам связи. Задачей стеганоанализа является детектирование наличия и, возможно, декодирование ДИ в «подозрительном» информационном контенте, или доказательство отсутствия секретного сообщения [1, 2].

Одним из наиболее широко используемых стеганографических методов был и остается до настоящего момента метод модификации наименьшего значащего бита (LSB) [1, 2]. В силу этого значительная часть стеганоаналитических исследований посвящена именно этому методу [7-10]. Но несмотря на то, что разработки здесь ведутся достаточно активно, все они, учитывая главное достоинство LSB – большую скрытую пропускную способность (СПС) [1], разрабатывают стеганоаналитические методы с учетом СПС, как правило, 0.5-1 бит/пиксель и более и даже не рассматривают возможность детектирования секретного вложения при СПС менее 0.25 бит/пиксель в силу сложности получаемой задачи, т.к. возмущения здесь оказываются настолько малыми, что их выявление вызывает значительные затруднения. Однако такая задача является реальной, а применение LSB при малой СПС, значительно повышающее стойкость стеганографической системы, часто используемым, оставляя задачу детектирования малых вложений *актуальной*.

Автором настоящей работы был предложен принципиально новый стеганоаналитический метод *SAVV* детектирования LSB – метод выявления *малых* возмущений матрицы контейнера, в качестве которого рассматривается цифровое изображение (ЦИ), хранимое в формате с потерями, происходящих при стеганопреобразовании, за счет анализа скорости изменения наименьших сингулярных чисел (СНЧ) блоков матрицы, полученных при ее стандартном разбиении [11], дающий принципиальную возможность выявления наличия ДИ даже при малой СПС.

Цель статьи и постановка исследований

Целью настоящей работы является оценка эффективности разработанного автором ранее стеганоаналитического метода *SAVV*.

Для достижения поставленной цели в разделе решаются следующие задачи:

1) Выбора метода для оценки эффективности *SAVV*;

2) Оценка эффективности разработанного стеганоаналитического метода по детектированию результатов вложения секретной информации методом LSB;

3) Сравнение эффективности разработанного стеганоаналитического метода с результатами работы современных методов по детектированию результатов вложения секретной информации методом модификации наименьшего значащего бита.

Основная часть

В соответствии с общим подходом к анализу состояния и технологии функционирования информационных систем (ОПАИС) [12], на основе которого был разработан *SAVV*, произвольная информационная система, в том числе, стеганографическая система (или отдельно рассматриваемые контейнер, СС), формализуется в виде двумерной матрицы (конечного множества двумерных матриц). Результат преобразования информационной системы, ее свойства определяются характерными особенностями совокупности возмущений однозначно определяющих ее формальных параметров – СНЧ и сингулярных векторов (СНВ) соответствующей матрицы (матриц) [12]. Анализ состояния контейнера, формальным представлением которого является матрица F, или анализ СС, в частности, стеганоанализ, в [11] сводится к анализу только СНЧ соответствующей матрицы (матриц), являющихся в соответствии с соотношением [12] $\max\limits_{1\le j\le n}\left|\sigma_j(F)-\sigma_j(F+\Delta F)\right|\le\left\|\Delta F\right\|_2$, где $\sigma_j(F)$, $\sigma_j(F+\Delta F)$ – СНЧ матриц F, $F+\Delta F$ соответственно, $\left\|\Delta F\right\|_2$ – спектральная норма матрицы возмущения ΔF, нечувствительными к возмущающим воздействиям, или хорошо обусловленными, поскольку реакция СНВ на возмущения различна, а в некоторых случаях – непредсказуема [12]. Хорошая обусловленность СНЧ приводит к тому, что величина их возмущений качественно отвечает величине возмущающего воздействия, характеризуя «силу» этого воздействия, в отличие от СНВ.

В соответствии с ОПАИС, СП, осуществляемое методом LSB, представляется в виде аддитивного погружения некоторой информации в пространственной области: $\overline{F}=F+\Delta F$, где $\overline{F}$ – матрица СС, ΔF – матрица возмущения ОС вследствие СП, ΔF сформирована случайным образом, ее элементы принадлежат множеству $\{-1,0,1\}$. Сформированное СС сохраняется в формате без потерь (хотя это принципиально не важно. Важно только чтобы *после* СП не происходило квантование коэффициентов ДКП). Везде ниже для определенности в качестве формата хранения без потерь ЦИ рассматривается TIFF.

Матрицы одного ЦИ до СП (формат JPEG) и после СП отличаются друг от друга. Выявление этого различия в методе *SAVV* происходит при анализе значения скорости изменения минимальных СНЧ 8×8-блоков, полученных после стандартного разбиения матрицы исходного изображения. В [13] были получены основные качественные отличия сингулярных спектров блоков СС с разными СПС от сингулярных спектров блоков JPEG-контейнеров: с увеличением СПС характер поведения СНЧ блоков СС все больше соответствует характеру СНЧ для ЦИ, хранимого без потерь, в частности, происходит увеличение скорости изменения наименьших СНЧ с ростом СПС. В [11] эмпирическим путем было получено пороговое значение $K = 4$ числового параметра $ih1$, непосредственно связанного с наиболее часто встречаемым значением скорости изменения наименьших СНЧ для совокупности блоков матрицы анализируемого ЦИ, позволяющего отделить СС от ОС по следующему принципу: если $ih1 < K$, то анализируемое ЦИ относится к контейнерам, иначе – к СС. В связи с этим ключевым моментом эффективной работы *SAVV* является определение порогового значения K; желаемым является подтверждение значения этого параметра, полученного ранее эмпирическим путем, при помощи математически обоснованных методов.

Учитывая все вышесказанное, основным инструментов для анализа эффективности работы метода *SAVV* выбран метод, основанный на анализе так называемых операционных характеристических кривых – ROC-анализе (*ROC – Receiver Operating Characteristic*) [14], и обладающий следующими свойствами:

- он позволяет оценить эффективность анализируемого метода (алгоритма) в целом, с учетом как ошибок первого, так и ошибок второго рода;
- он позволяет формализовать процесс получения порогового значения анализируемого параметра – так называемой точки отсечения (в нашем случае – это значение K), которое даст возможность отделить СС от ОС;
- значение точки отсечения является своеобразным «рычагом» управления чувствительностью исследуемого алгоритма, т.к. позволяет менять соотношение между ошибками первого и второго рода в зависимости от специфики решаемой задачи.

Основная идея метода анализа ROC-кривых в приложении к решению задачи СА заключается в следующем. Необходимо выявить СС (класс V_1) в группе ЦИ, где есть и незаполненные контейнеры (класс V_2). Для выявления СС используется стеганоаналитическим метод (САМ), который принимает одно из двух решений: положительное $\delta = 1$ (СС) или отрицательное $\delta = 0$ (ОС). Для оценки эффективности САМ проводится его тестирование на группе ЦИ, для которых известно, какое из них является СС, а какое ОС. Результаты такого тестирования в общем случае можно представить в виде таблицы 1, где приняты следующие обозначения: *TP* – число правильно выявленных СС; *TN* – число правильно выявленных ОС; *FP* – число ОС, ошибочно принятых за СС (ошибка второго рода); *FN* – число СС, ошибочно признанных ОС (ошибка первого рода).

Таблица 1.

Результаты тестирования репрезентативной группы ЦИ

Истинное состояние ЦИ	Результат тестирования	
	$\delta = 1$ – СС	$\delta = 0$ – ОС
Класс V_1 – СС	TP	FN
Класс V_2 – ОС	FP	TN

По данным табл. 1 результаты тестирования САМ возможно представить точками в двумерном ROC-пространстве, где по оси ординат откладывается значение, несущее в себе информацию об ошибках первого рода (чувствительность): $S_E = TP/(TP + FN)$, а

по оси абсцисс – значение $1-S_P$, характеризующее ошибки второго рода, где S_P (специфичность [14]) вычисляется в соответствии с формулой: $S_P = TN/(TN+FP)$. ROC-пространство дает наглядное графическое представление об эффективности алгоритма и позволяет сравнивать эффективность различных алгоритмов.

Наиболее распространенным способом построения ROC-кривых является разбиение возможных значений анализируемого параметра (в нашем случае – $ih1$) на группы. Группы могут формироваться по-разному, различным может быть их количество в зависимости от специфики решаемой задачи. В случае небольшого количества различных значений для анализируемого параметра рекомендуется разбиение на группы по значению параметра [14], что и делается в настоящей работе. В этом случае появляется возможность оценить чувствительность и специфичность алгоритма при различных значениях параметра, что будет соответствовать последовательности точек в ROC-пространстве [14].

Количественной оценкой эффективности исследуемого при помощи ROC-анализа алгоритма (метода) является значение интегральной характеристики ρ, определяемой в соответствии с формулой [14]: $\rho = 2A-1$, где A – площадь под ROC-кривой. Чем больше A, тем выше эффективность исследуемого алгоритма (метода).

Таким образом, очевидна целесообразность выбора в качестве метода для оценки эффективности *SAVV* метода анализа ROC-кривых.

Вычислительный эксперимент для проверки эффективности разработанного САМ по детектированию результатов вложения LSB-методом проводился в среде *MathWorks* MATLAB на множестве Q из 500 ЦИ, хранимых в формате JPEG, основанном на ДКП, взятых из базы NRCS [15], которая является традиционной при тестировании стеганографических и стеганоаналитических алгоритмов. В ходе эксперимента в каждое из изображений производилось внедрение ДИ одной из современных вариаций LSB – алгоритмом *LSB-matching* [7-10], при этом СПС составляла 0.05, 0.1, 0.2, 0.25, 0.3, 0.4, 0.5, 0.75, 1 бит/пиксель.

Соответствующие ROC-кривые представлены на рис. 1. Значения интегрального параметра ρ в совокупности с непосредственными значениями площади A под ROC-кривой (формула (10)) представлены в табл. 2.

Полученные значения интегрального параметра ρ (табл.2) являются высокими [14], но для окончательной оценки эффективности *SAVV* необходимо провести сравнение с результатами ROC-анализа для современных аналогов, что делается ниже.

ROC-анализ, как уже было отмечено, используется для нахождения оптимального порогового значения K, или точки отсечения (*cut-off value*). В общем случае, оптимальное значение порога зависит от предъявляемых к алгоритму требований, т.е. от выбранного критерия оптимальности [14]. В настоящей работе в качестве оптимальной рассматривается точка на ROC-кривой, которая имеет наибольшее значение чувствительности. Эта точка может быть найдена с помощью индекса Йодена J [16]: $J = \max(S_E + S_p - 1)$. Для ее нахождения воспользуемся результатами проведенных вычислительных экспериментов. Полученные значения J приведены в табл. 3. Для каждой СПС находится максимальное значение J – $J_{\max}$ (в табл. 3 эти значения выделены жирным шрифтом), для каждого $J_{\max}$ определяется соответствующее значение $ih1$; из полученных значений $ih1$ – 4, 5, 6 выбирается минимальное: $K = 4$, что подтверждает правильность порогового значения, полученного автором ранее эмпирическим путем.

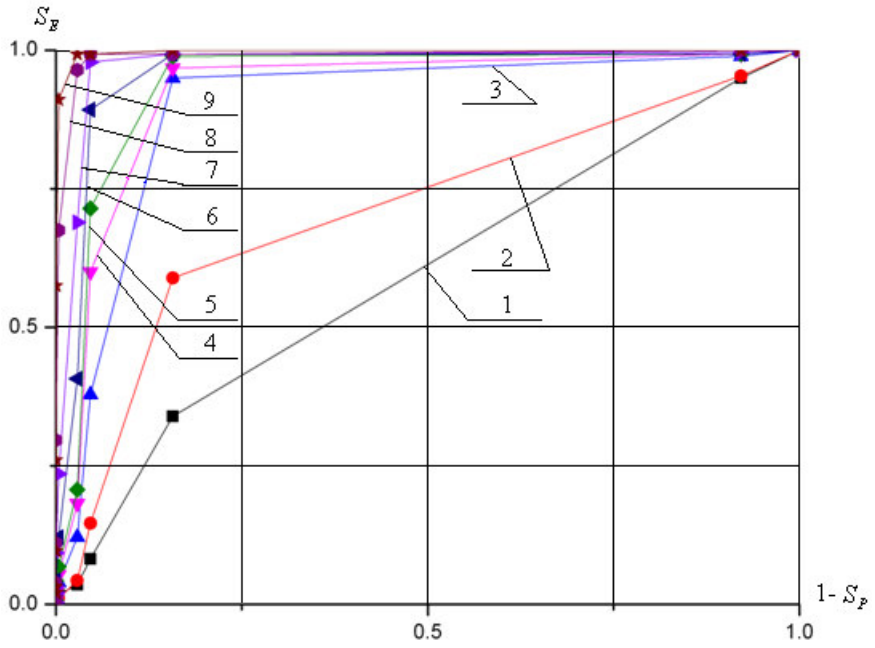

Рис. 1. ROC-кривые, характеризующие работу метода *SAVV* при детектировании результатов *LSB-matching* для различных значений СПС: 1 – 0.05; 2 – 0.1; 3 – 0.2; 4 – 0.25; 5 – 0.3; 6 – 0.4; 7 – 0.5; 8 – 0.75; 9 – 1 бит/пиксель

Таблица 2.

Значения интегрального параметра для оценки эффективности *SAVV* при детектировании результатов *LSB-matching*

СПС, бит/пиксель	A	ρ
0.05	0.594	0.188
0.1	0.710	0.420
0.2	0.89936	0.79872
0.25	0.92442	0.84884
0.3	0.942	0.884
0.4	0.960	0.920
0.5	0.9748	0.9496
0.75	0.98975	0.9795
1	0.99735	0.9947

Необходимо отметить, что часто при использовании ROC-анализа при определении точки отсечения в качестве критерия оптимальности используется требование баланса между чувствительностью и специфичностью, т.е. требование $S_E \approx S_P$ [14]. В этом случае порог есть точка пересечения двух кривых, когда по оси X откладываются значения анализируемого параметра, а по оси $Y-$ S_E и S_P. Проведение такой операции для результатов тестирования метода *SAVV* при СПС 0.05 бит/пиксель представлено на рис. 2. Как видно, определенное выше значение $K = 4$ для *SAVV* является не только оптимальным в смысле чувствительности, но и близко к оптимальному в смысле баланса между чувствительность и специфичностью.

Важной составляющей ROC-анализа является то, что изменение значения точки отсечения позволяет управлять чувствительностью тестируемого метода в зависимости от требований, выдвигаемых к решению задачи в данный конкретный момент, за счет изменения соотношения между ошибками первого и второго рода.

Таблица 3.

Определение точки отсечения с использованием индекса Йодена

	J								
СПС / *ih*1	5	10	20	25	30	40	50	75	100
1	0	0	0	0	0	0	0	0	0
2	0.028571	0.032143	0.067857	0.071429	0.071429	0.071429	0.075	0.078571	0.078571
3	0.028571	0.032143	0.067857	0.071429	0.071429	0.071429	0.075	0.078571	0.078571
4	**0.182143**	**0.432143**	**0.792857**	**0.810714**	**0.832143**	0.835714	0.835714	0.835714	0.842857
5	0.035714	0.1	0.332143	0.553571	0.667857	**0.846429**	**0.932143**	**0.946429**	0.946429
6	0.007143	0.014286	0.092857	0.153571	0.178571	0.378571	0.660714	0.935714	**0.964286**
7	0.014286	0.007143	0.035714	0.05	0.064286	0.117857	0.232143	0.671429	0.907143
8	0	0	0.017857	0.021429	0.042857	0.042857	0.092857	0.296429	0.575
9	0	0	0.010714	0.003571	0.007143	0.014286	0.032143	0.110714	0.260714
10	0	0	0	0.003571	0	0.007143	0.021429	0.039286	0.096429
11	0	0	0	0	0	0	0.017857	0.010714	0.032143
12	0	0	0	0	0	0	0.003571	0.003571	0.021429

Для сравнительной оценки работы *SAVV* были выбраны современные стеганоаналитические аналоги, детектирующие LSB-метод: методы Керра, Лю и т.д. [7-10].

Результаты сравнения представлены на рис. 3, в таблице 4.

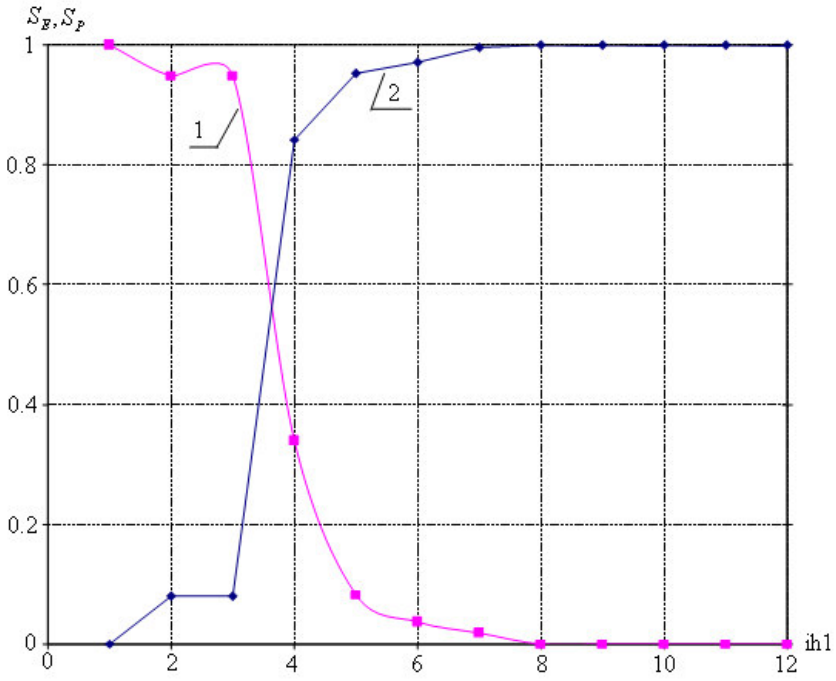

Рис. 2. Построение точки отсечения при требовании баланса между чувствительность и специфичностью: 1 – кривая чувствительности, 2 –кривая специфичности

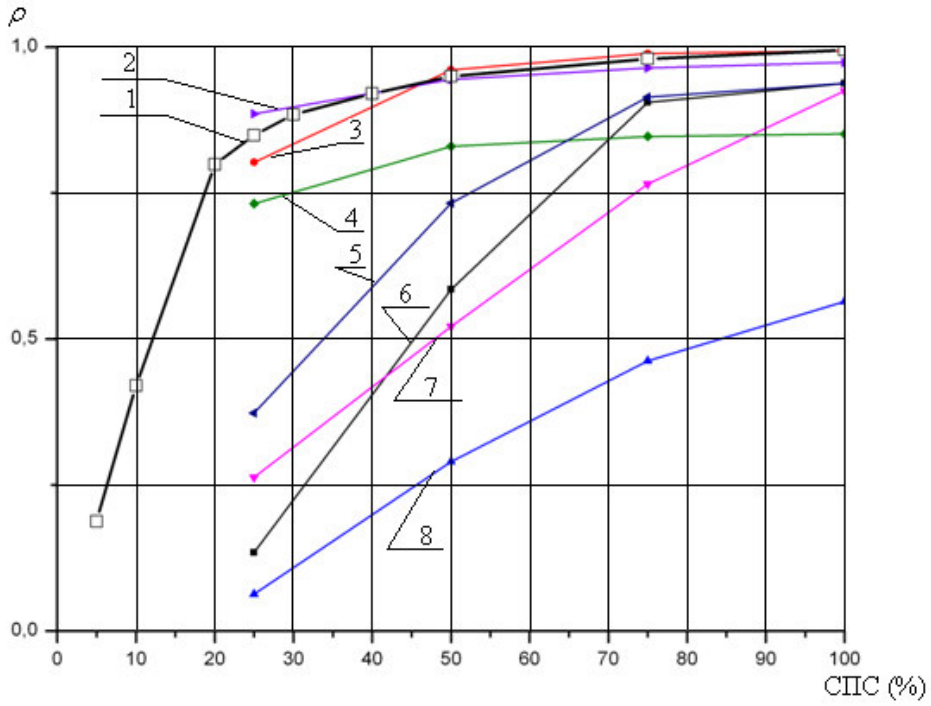

Рис. 3. Результаты сравнения эффективности работы *SAVV* с существующими аналогами: 1 — *SAVV*; 2 — Joint feature set; 3 — Liu's; 4 — RLH COM; 5 — Fused feature; 6 — Ker's; 7 — NDH COM; 8 — HGE

Результаты вычислительного эксперимента показывают, что разработанный САМ *SAVV* имеет высокую эффективность детектирования, в частности, даже при СПС меньше 0.25 бит/пиксель, которая вообще не рассматривается аналогами. Так ρ=0.79872 для *SAVV* при СПС 0.2 бит/пиксель, что выше, чем ρ для всех сравниваемых САМ при СПС 0.25 бит/пиксель, за исключением единственного САМ: Joint feature set (эффективность которого для СПС меньшей 0.25 бит/пиксель также неизвестна, однако отсутствие таких данных в результатах эксперимента косвенно указывает на то, что соответствующая эффективность является малой, и по этой причине авторы ее не приводят), кроме того, при СПС 0.5, 0.75, 1 бит/пиксель эффективность Joint feature set уступает *SAVV*. При СПС 0.5, 0.75 бит/пиксель *SAVV* несколько уступает САМ Liu's, но для малой СПС САМ Liu's значительно хуже *SAVV*: его эффективность для СПС 0.25 меньше, чем для разработанного метода при СПС 0.2 бит/пиксель.

Таким образом, исходя из результатов вычислительного эксперимента, можно утверждать, что разработанный САМ *SAVV* является эффективнее своих аналогов, что особенно явно проявляется при малой СПС.

Для полученной выше точки отсечения $K = 4$ результаты работы *SAVV* с явным указанием ошибок I и II рода представлены в табл. 5.

Таблица 4.

Значение интегрального параметра ρ для различных САМ детектирования результатов *LSB-matching* при различной СПС

САМ / СПС, (%)	Ker's	Liu's	HGE	NDH COM	RLH COM	Fused feature	Joint feature set	*SAVV*
5	–	–	–	–	–	–	–	**0.188**
10	–	–	–	–	–	–	–	**0.42**
20	–	–	–	–	–	–	–	**0.79872**
25	0.1346	0.7922	0.063	0.2628	0.7316	0.3732	0.8855	**0.84884**
30	–	–	–	–	–	–	–	**0.884**
40	–	–	–	–	–	–	–	**0.92**
50	0.5846	0.9608	0.2898	0.5212	0.8298	0.7324	0.9441	**0.9496**
75	0.9052	0.9885	0.4622	0.765	0.8468	0.9138	0.9637	**0.9795**
100	0.9376	0.9931	0.5642	0.9244	0.851	0.9376	0.9732	**0.9947**

Таблица 5.

Результаты детектирования *LSB-matching* стеганоаналитеческим методом *SAVV*

СПС (бит/пиксель)	0.05	0.1	0.2	0.25	0.3	0.4	0.5	0.75	1
Ошибки 1-го рода (%)	33.12	27.87	5	3.21	1.07	0.71	0.71	0.71	0
Ошибки 2-го рода (%)	7.5								

Количество ошибок первого и второго рода (табл. 5), их соотношение объясняется сделанным выше выбором критерия оптимальности для определения точки отсечения: максимизация чувствительности разрабатываемого САМ.

Выводы

В настоящей работе обоснована целесообразность выбора для оценки эффективности разработанного САМ метода анализа ROC-кривых, использование которого позволило получить комплексную оценку *SAVV* с одновременным учетом ошибок первого и второго рода, а также провести формальную проверку правильности установленного ранее эмпирически порогового значения скорости изменения наименьших СНЧ блоков матрицы ЦИ, позволяющего в *SAVV* отделить СС от ОС; установлено, что разработанный САМ *SAVV* является эффективнее своих аналогов по детектированию результатов вложения секретной информации методом модификации наименьшего значащего бита, что особенно явно проявляется при малой СПС.

Список литературы

1. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: Солон-Пресс, 2002. — 272 с.
2. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
3. Gul, G. SVD-Based Universal Spatial Domain Image Steganalysis / G. Gul, F. Kurugollu // IEEE Transactions on Information Forensics and Security. — 2010. — Vol.5, No.2. — PP. 349–353.
4. Gul, G. Steganalytic Features for JPEG Compression-Based Perturbed Quantization / G. Gul, A.E. Dirik, I. Avcibas // IEEE Signal Processing Letters. — 2007. — Vol.14, Iss.3. — PP. 205–208.
5. Lyu, S. Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines / S. Lyu, H. Farid // Lecture Notes in Computer Science. — New York: Springer-Verlag, 2002. — Vol.2578. — PP. 340–354.
6. Avcibas, I. Image Steganalysis with Binary Similarity Measures / I. Avcibas, M. Kharrazi, *et al.* // EURASIP Journal on Applied Signal Processing. – 2005. – Vol.17. – PP. 2749–2757.
7. Ker, A.D. Steganalysis of LSB matching in grayscale images // IEEE Signal Processing Letters. – 2005. — Vol.12, No.6. — PP. 441–444.
8. Liu, Q.Z. Image complexity and feature mining for steganalysis of least significant bit matching steganography / Q.Z. Liu, A.H. Sung, *et al.* // Information Sciences. — 2008. — Vol.178, No.1. — PP. 21–36.
9. Zhihua Xia. A Learning-Based Steganalytic Method against LSB Matching Steganography / Zhihua Xia, Lincong Yang, *et al.* // Radioengineering. — 2011. — Vol.20, No.1. — PP. 102–109.
10. Natarajan, V. Blind Image Steganalysis Based on Contourlet Transform / V. Natarajan, R. Anitha // International Journal on Cryptography & Information Security. — 2012. — Vol.2, Iss.3. — PP. 77–87.
11. Бобок, И.И. Детектирование наличия возмущений матрицы цифрового изображения как составная часть стеганоанализа / И.И. Бобок // Вісник Східноукраїнського національного університету ім. В. Даля. — 2011. — №7(161). — С.32–41.
12. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. — К.: ГУИКТ, 2009. — 251 с.
13. Бобок, И.И. Стеганоанализ как частный случай анализа информационной системы / И.И. Бобок, А.А. Кобозева // Сучасна спеціальна техніка. — 2011. — №2. — С. 21–34.
14. Файнзильберг, Л.С. Гарантированная оценка эффективности диагностических тестов на основе усиленного ROC-анализа / Л.С. Файнзильберг, Т.Н. Жук // Управляющие системы и машины. — 2009. — №5. — С.3–13.
15. NRCS Photo Gallery: *[Електронний ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступу: http://photogallery.nrcs.usda.gov (Дата звернення: 26.07.2012).
16. Schlisterman, E.F. Optimal cut-point and its corresponding Youden index to discriminate individuals using pooled blood samples / E.F. Schlisterman, N.J. Perkins, *et al.* // Epidemiology. — 2005. — Vol.16, Iss.1. — PP. 73–81.

ВИКОРИСТАННЯ МЕТОДУ АНАЛІЗУ ROC-КРИВИХ ДЛЯ КОМПЛЕКСНОЇ ОЦІНКИ ЕФЕКТИВНОСТІ СТЕГАНОАНАЛІТИЧНОГО МЕТОДУ

І.І. Бобок

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: onu_metal@ukr.net

Представлено результати аналізу ефективності й порівняння роботи нового стеганоаналітичного методу детектування стеганографічних вкладень, здійснених методом модифікації найменшого значущого біта, у цифрове зображення, збережене у форматі із втратами, розробленого автором раніше, з найбільш ефективними існуючими аналогами. Оцінка роботи методів проводиться за допомогою ROC-аналізу. Представлено результати обчислювальних експериментів.
Ключові слова: стеганоаналіз, метод модифікації найменшого значущого біта, ROC-аналіз, точка відсікання

APPLICATION OF ROC-ANALYSIS FOR INTEGRATED ASSESSMENT OF STEGANALYSIS METHOD'S EFFICIENCY

Ivan I. Bobok

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: onu_metal@ukr.net

Results of the analysis of the new LSB-steganalysis method for digital images stored in a lossy format and comparison its efficiency with the best existing analogues. Evaluation of analyzed method is done by ROC-analysis. The results of computational experiments are presented.
Keywords: steganalysis, Least Significant Bit, ROC-analysis, cut-off value