

показателями алгоритма AES. Продемонстрировано, что алгоритм ДСТУ ГОСТ 28147-89 в сравнении с AES имеет значительно меньшие требования к размеру кода при сопоставимой производительности.

Ключевые слова: ГОСТ 28147-89, AES, AVR, MSP430, ARM7TDMI, микроконтроллеры, встраиваемые системы, lightweight-криптография.

In the article the estimation of the performance and code size of the symmetric-key cipher algorithm of DSTU GOST 28147-89 during realization on 8/16/32-bit microcontrollers of AVR, MSP430, ARM7TDMI. Comparing of the obtained results with the results of the algorithm AES. It is shown that the algorithm DSTU GOST 28147-89 in comparison from AES has significantly less requirements to the code size at the comparable performance.

Keywords: GOST 28147-89, AES, AVR, MSP430, ARM7TDMI, microcontrollers, embedded systems, lightweight-cryptography.

Рецензент: д.т.н., проф. Дудикевич В.Б.
Надійшла 31.01.2011

УДК 004.056.5

Бобок И.И.

(Одеський національний політехнічний університет)

СТЕГАНОАНАЛИТИЧЕСКИЙ МЕТОД ДЛЯ ЦИФРОВОГО СИГНАЛА-КОНТЕЙНЕРА, ХРАНЯЩЕГОСЯ В ФОРМАТЕ С ПОТЕРЯМИ

Активизация научной деятельности в области стеганографии, где скрывается сам факт существования тайного сообщения, связанная с запретом шифрования на законодательном уровне во многих странах мира, привела в настоящий момент к чрезвычайно негативному последствию - росту частоты использования получаемых новых разработок различными террористическими структурами [1-5]. В силу этого в настоящий момент трудно переоценить актуальность решения вопросов, связанных с повышением эффективности стеганоанализа (СА) [1-5]. Общей чертой стеганографических методов является то, что скрываемое сообщение, или дополнительная информация (ДИ), встраивается в некоторый непривлекательный для внимания объект - основное сообщение (ОС), или контейнер (неограничивая общности рассуждений [7], в качестве ОС рассматривается цифровое изображение (ЦИ) в градациях серого). Процесс погружения ДИ в контейнер будем называть стеганообразованием (СП), а результат этого погружения - стеганообщением (СС). После встраивания информации СС открыто транспортируется адресату по каналу связи или хранится в таком виде.

Под СА будем понимать процесс выявления или констатации отсутствия определенных характерных признаков в анализируемом информационном контенте, позволяющих делать вывод о факте внедрения секретной информации или об отсутствии такового.

В настоящее время хранение и передача цифровых сигналов, в частности, ЦИ по каналам телекоммуникаций в связи со значительным увеличением объемов информации осуществляется в сжатом состоянии. Этот немаловажный факт не может не учитываться при разработке подхода к решению задачи СА. Одним из самых популярных форматов хранения ЦИ сегодня является формат JPEG (с потерями), который и будет рассматриваться ниже как формат хранения ОС (для определенности рассматривается JPEG, основанный на дискретном косинусном преобразовании (ДКП)).

При организации стеганографического канала связи на сегодняшний день очень широко используется метод модификации наименьшего значащего бита (LSB) [2,6], что явилось побуждающим фактором для автора работы, в первую очередь, рассмотреть характерные особенности и найти способы выявления последствий работы этого метода.

Целью настоящей работы является разработка стеганоаналитического алгоритма (САА) детектирования наличия секретного сообщения, погруженного в JPEG-контейнер с использованием LSB-метода.

Как известно, метод модификации наименьшего значащего бита является неустойчивым к любого рода возмущающим воздействиям, в частности, к операции сжатия [2]. Следовательно, СС, сформированное LSB-методом на основе JPEG-контейнера, может быть сохранено только в формате без потерь (например, TIF, BMP). С учетом этого для достижения поставленной цели необходимо решить следующие задачи:

1. Выделить математические объекты, характеризующие ОС, СС, анализ которых позволит отделить ЦИ, подвергнутое операции СП, от неизмененного ЦИ;
2. Выявить характерные признаки (качественные, количественные) для выделенных математических объектов, которые позволят отличить JPEG-ЦИ, пересохраненное в формате без потерь (TIF, BMP), от ЦИ, которое первоначально хранится в формате TIF или BMP;
3. Выявить характерные признаки (качественные, количественные) для выделенных математических объектов, которые позволят отличить сформированное LSB-методом на основе JPEG-контейнера и сохраненное в формате без потерь (TIF, BMP) СС от ЦИ, которое хранилось первоначально в формате JPEG и, не подвергаясь процессу СП, было пересохранено в формате без потерь;
4. На основе результатов решения задач 2 и 3, необходимо выявить характерные признаки (качественные, количественные) для выделенных математических объектов, которые позволят отличить сформированное LSB-методом на основе JPEG-контейнера и сохраненное в формате без потерь (TIF, BMP) СС от ЦИ, которое первоначально хранится в формате TIF или BMP;
5. Исходя из результатов решения предыдущих задач, разработать САА для выявления СС, построенных методом LSB на основе JPEG-контейнера.

Везде ниже для определенности в качестве формата хранения без потерь ЦИ рассматривается TIF.

Матрицы одного ЦИ в форматах TIF и JPEG (обозначим эти матрицы F_{TIF} и F_{JPEG} соответственно) отличаются друг от друга. В процессе сохранения ЦИ в JPEG (с потерями) происходит обнуление высокочастотных (и, возможно, некоторых среднечастотных) коэффициентов ДКП 8×8 -блоков, полученных после стандартного разбиения матрицы исходного изображения. Исключение высоких (и возможно средних) частот в JPEG-ЦИ никак не восполнится при его пересохранении в формате TIF, поэтому матрица изображения, сохраненного в TIF первоначально и сохраненного в TIF после JPEG-сжатия (обозначим последнюю $F_{JPEG \rightarrow TIF}$) должны качественно отличаться друг от друга по своим характеристикам, в частности, они кардинально по-разному должны отреагировать на пересохранение ЦИ в формате JPEG (для определенности и однозначности везде ниже пересохранение в формате JPEG проводится в FOTOSHOP с качеством $Q=10$). Действительно, ведь F_{TIF} отвечает представлению сигнала, у которого все частотные коэффициенты в «первозданном» невозмущенном виде, в то время, как $F_{JPEG \rightarrow TIF}$ соответствует представлению сигнала, у которого уже «отсутствуют» высокочастотные (возможно, среднечастотные) составляющие - коэффициенты при них если ненулевые, то малые (сравнимы с погрешностями округлений). Сжатие для F_{TIF} - первое (матрицу результата обозначим $F_{TIF \rightarrow JPEG}$), его качественные результаты описаны выше, а свойства $F_{TIF \rightarrow JPEG}$ аналогичны F_{JPEG} . С учетом того, что сжатие происходит с достаточно высоким качеством, ожидаемым результатом является незначительное возмущение значений яркости большинства пикселей изображения. Для $F_{JPEG \rightarrow TIF}$ очередное сжатие является вторым (матрицу результата обозначим $F_{JPEG \rightarrow TIF \rightarrow JPEG}$), причем матрица квантования для повторного сжатия с большой вероятностью не будет совпадать с матрицей квантования для первого сжатия, в силу чего, несмотря на высокое качество второго сжатия, результат возмущений

значений яркости пикселей $F_{JPEG \rightarrow TIF}$ при переходе к $F_{JPEG \rightarrow TIF \rightarrow JPEG}$ в общем случае принципиально предсказать невозможно. Ясно лишь, что эти возмущения должны быть значительнее, чем при переходе от F_{TIF} к $F_{TIF \rightarrow JPEG}$. Обозначим:

$$R = abs(F_{TIF} - F_{TIF \rightarrow JPEG}) \quad (\bar{R} = abs(F_{JPEG \rightarrow TIF} - F_{JPEG \rightarrow TIF \rightarrow JPEG}))$$

— матрицу абсолютных значений разностей элементов F_{TIF} и $F_{TIF \rightarrow JPEG}$ ($F_{JPEG \rightarrow TIF}$, $F_{JPEG \rightarrow TIF \rightarrow JPEG}$). Пусть $M(A)$ - значение, которое встречается среди элементов произвольной матрицы A с максимальной частотой, $\max(A)$ - максимальное значение среди элементов матрицы A .

На основании проведенных рассуждений выдвинем следующую гипотезу:

$$\max(R) < \max(\bar{R}); M(R) < M(\bar{R}).$$

Для проверки выдвинутой гипотезы в среде MATLAB был проведен вычислительный эксперимент, в котором участвовало около 800 ЦИ размером 1024×1024 пикселей. С учетом поставленных задач в качестве предмета исследования были выбраны гистограммы значений матриц R , \bar{R} .

На первом этапе эксперимента устанавливались характерные особенности возмущения элементов матрицы изображения при переходе от F_{TIF} к $F_{TIF \rightarrow JPEG}$. В результате вычислительного эксперимента было получено, что для различных ЦИ

$$\max(R) \in \{7, 8, 9, \dots, 32\}, \tag{1}$$

причем для подавляющего большинства изображений $\max(R) \in \{18, 19, \dots, 24\}$, при этом гистограммы значений R имеют «правильную» и определенную форму, типичные виды которой представлены на рис.1 (лишь 1.5% исследованных ЦИ дали гистограммы II-типа (рис.1(б))). Для всех ЦИ с гистограммой I-типа глобальный максимум - мода, который одновременно является единственным локальным максимумом, достигается в 1, а для гистограмм II-типа - в 0. Таким образом:

$$M(R) \leq 1. \tag{2}$$

Большинство пикселей ЦИ при переходе от F_{TIF} к $F_{TIF \rightarrow JPEG}$, как и предполагалось, претерпевают незначительные возмущения или не возмущаются вовсе.

Во второй части вычислительного эксперимента устанавливались характерные особенности возмущений элементов матрицы изображения при переходе от $F_{JPEG \rightarrow TIF}$ к $F_{JPEG \rightarrow TIF \rightarrow JPEG}$. В результате вычислительного эксперимента было установлено, что

$$\max(\bar{R}) \in \{36, 37, \dots, 47\} \tag{3}$$

для разных ЦИ, причем для подавляющего большинства изображений $\max(\bar{R}) \in \{40, \dots, 44\}$, что в совокупности с (1) экспериментально подтверждает первую часть выдвинутой гипотезы. При этом гистограммы значений \bar{R} качественно отличаются от гистограмм R (рис.2), в большинстве случаев наблюдается наличие нескольких локальных максимумов - полимодальное распределение; для всех протестированных ЦИ $M(\bar{R}) > 1$ (причем для абсолютного большинства изображений $M(\bar{R}) \gg 1$), что в совокупности с (2) подтверждает

вторую часть выдвинутой гипотезы и, с учетом соотношений (1) и (3) позволяет различить ЦИ, первоначально сохраненные в формате TIF, и ЦИ, пересохраненные в TIF после JPEG-сжатия.

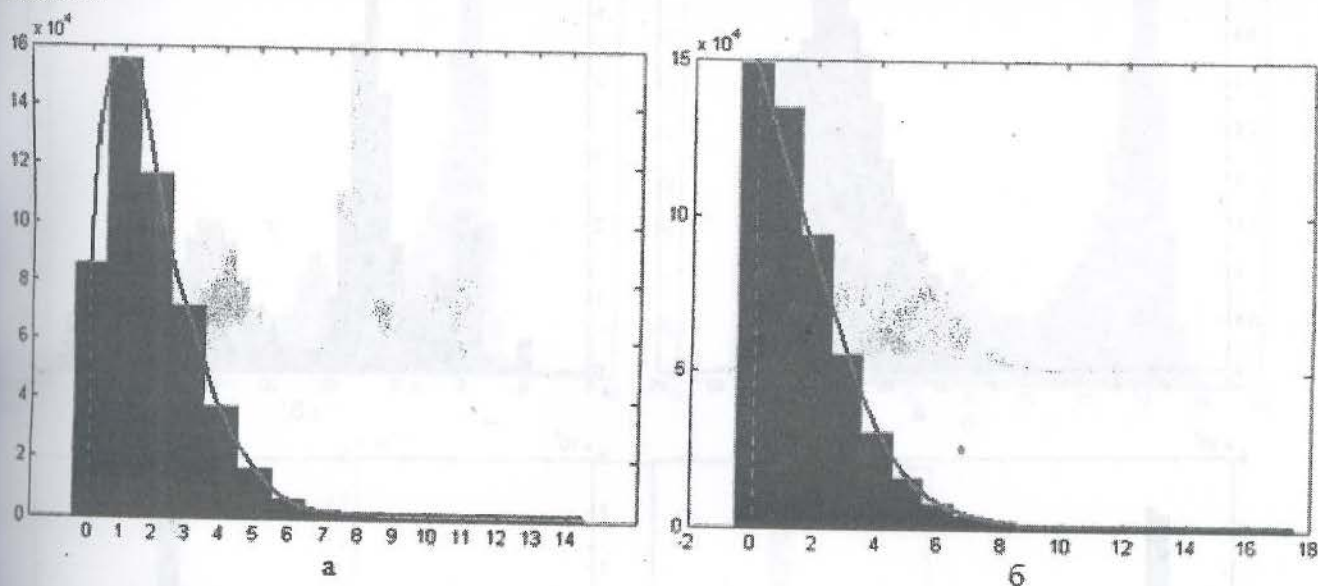


Рис.1. Гистограммы значений матриц абсолютных возмущений яркости пикселей в процессе пересохранения ЦИ из формата TIF в формат JPEG: а - гистограмма I-типа; б - гистограмма II-типа

Пусть JPEG-контейнер подвергается СП методом наименьшего значащего бита, при этом стеганопуть [2] формируется случайным образом. Результат работы LSB-метода в соответствии с [7] в матричном виде будем представлять как возмущение ΔF матрицы контейнера F_{JPEG} , т.е.

$$\bar{F}_{JPEG} = F_{JPEG} + \Delta F, \quad (4)$$

где \bar{F}_{JPEG} - матрица СС, при этом матрица возмущения ΔF имеет элементы, значения которых принадлежат множеству $\{-1,0,1\}$. При погружении ДИ в дальнейшем будем учитывать лишь те ее биты, которые вызывают возмущение соответствующих пикселей ОС. Так, будем говорить, что объем погруженной информации (ОПИ) составляет, например, 10%, если при погружении этой ДИ десятая часть общего числа пикселей контейнера претерпела возмущения. СС сохраняется в формате TIF (результатирующая матрица - $\bar{F}_{JPEG \rightarrow TIF}$). Как показывает проведенный вычислительный эксперимент, в котором ОПИ изменялся от 10% до 50% с шагом 10%, полученные СС $\bar{F}_{JPEG \rightarrow TIF}$ ведут себя аналогично $F_{JPEG \rightarrow TIF}$, т.е. аналогично ЦИ, которое не подвергалось СП: после последующего пересохранения СС в формат JPEG (результатирующую матрицу обозначим $\bar{F}_{JPEG \rightarrow TIF \rightarrow JPEG}$), гистограммы значений элементов матриц

$$\bar{R} = abs(\bar{F}_{JPEG \rightarrow TIF} - \bar{F}_{JPEG \rightarrow TIF \rightarrow JPEG})$$

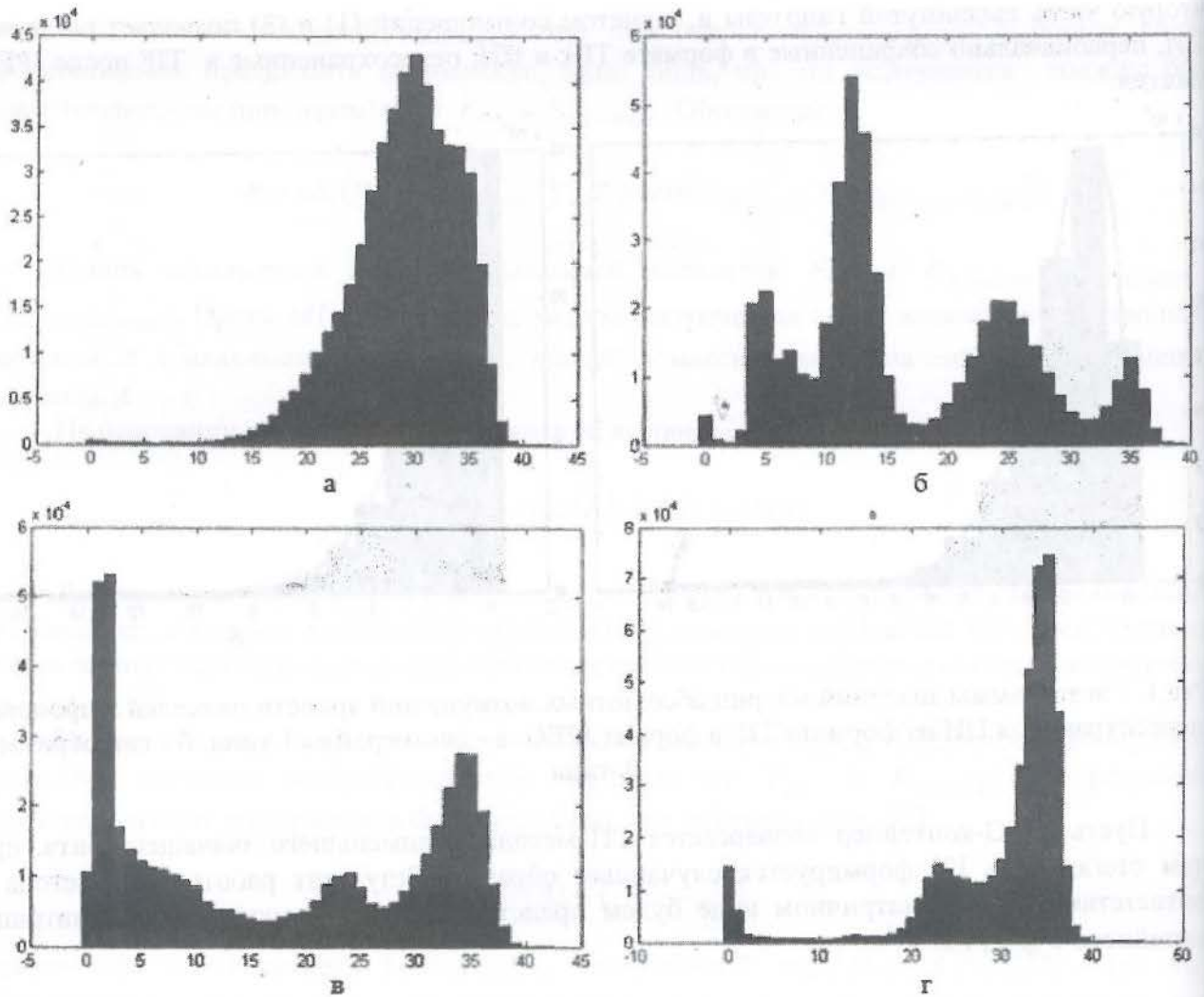


Рис.2. Гистограммы значений матрицы \bar{R}

качественно практически не отличаются от гистограмм матриц \bar{R} , а также между собой, несмотря на различие в ОПИ. Типичный пример для иллюстрации сказанного представлен на рис.3. Теоретически такой результат был ожидаемым: возмущение матрицы ОС F_{JPEG} за счет СП, которое изменит значения яркости определенной части пикселей лишь на 1, является незначительным. В представлении сигнала ОС F_{JPEG} коэффициенты при высоких (и возможно некоторых средних) частотах 8×8 -блоков матрицы были малы (сравнимы с нулем), что, учитывая связь между частотным спектром произвольной матрицы и ее сингулярными тройками [8], приводит к сравнимости с нулем наименьших сингулярных чисел блоков матрицы. СНЧ произвольной матрицы являются нечувствительными к возмущающим воздействиям, или хорошо обусловленными [9], что приведет к их незначительному возмущению при СП, т.е. оставит их значения сравнимыми с нулем, что, в свою очередь, оставит сравнимыми с нулем коэффициенты при высоких (и возможно некоторых средних) частотах блоков матрицы \bar{F}_{JPEG} , а значит и $\bar{F}_{JPEG \rightarrow TIF}$. Потому при пересохранении в формат JPEG $\bar{F}_{JPEG \rightarrow TIF}$ качественно ведет себя практически также, как ЦИ, представлением которого является матрица $F_{JPEG \rightarrow TIF}$.

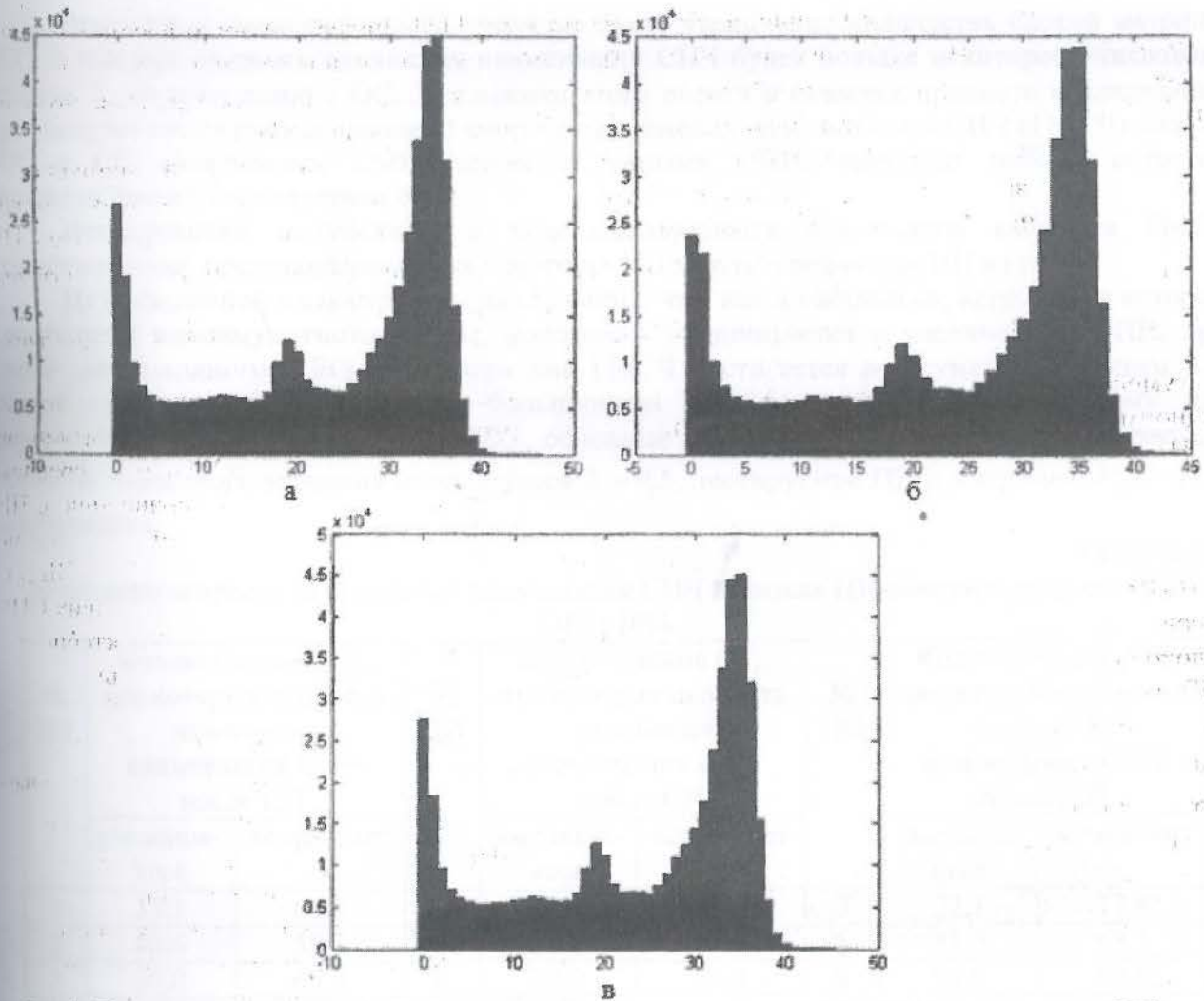


Рис.3. Гистограммы возмущений значений яркости пикселей, отвечающие одному ЦИ при различных преобразованиях: а – гистограмма значений элементов \bar{R} при СП с ОПИ 10%; б – гистограмма \bar{R} при СП с ОПИ 50%; в – гистограмма значений элементов \bar{R} (СП отсутствует)

Таким образом, в результате анализа определенных выше гистограмм становится возможным автоматизация отделения ЦИ, сохраненных в TIF первоначально, от ЦИ, которые были пересохранены в TIF из JPEG. Однако выявить наличие (отсутствие) ДИ, внедренной LSB-методом, т.е. отделить СС, построенное на основе JPEG-контейнера и сохраненного в формате TIF, от JPEG-ЦИ, которое не подвергалось СП, а было просто пересохранено в TIF, по анализируемым гистограммам оказывается крайне затруднительным.

В соответствии с общим математическим подходом к анализу состояния и технологии функционирования информационных систем (ОПАИС), в частности, систем защиты информации, основанным на теории возмущений и матричном анализе, разработанным в [7,10], о состоянии и изменении состояния JPEG-изображения в связи с его СП можно судить по характерным свойствам сингулярных чисел (СНЧ) и сингулярных векторов (СНВ) соответствующей матрицы ЦИ. В связи с тем, что реакция СНВ на возмущающие воздействия различна, а в некоторых случаях – непредсказуема [9,10], анализ состояния контейнера (или СС) целесообразности свести к анализу только СНЧ.

Рассмотрим более подробно схему сжатия (с потерями) для ЦИ, состоящую из трех основных шагов: отображение в частотную область, квантование полученных в частотной области коэффициентов, энтропийное кодирование. Восстановление включает в себя шаги,

Результатом вищесказанного очевидно будет увеличение количества блоков матрицы СС, в которых скорость изменения наименьших СНЧ будет больше некоторого числового порога k , по сравнению с ОС. Для оценки этого порога в качестве предмета исследования рассмотрим гистограммы значений скорости изменения минимальных СНЧ (ГМСЧ) блоков ОС и СС, полученных LSB-методом с разными ОПИ, результат работы которого представляется в соответствии с (4).

Иллюстрацией полученных в ходе эксперимента результатов являются ГМСЧ типичного вида, представленные для одного из 450 протестированных ЦИ на рис. 5.

Из приведенной иллюстрации (рис.5) видно, что, как и ожидалось, аргумент, в котором достигается максимум гистограммы, монотонно увеличивается с увеличением ОПИ, при этом для исходного JPEG-контейнера пик ГМСЧ достигается в аргументе, меньшем 0.5. Такая картина наблюдается для большинства протестированных ЦИ, поэтому для предлагаемого САА SA_LSB_OSJPEG, основные шаги которого представлены на рис.6, в качестве порогового значения используется $k = 0.5$, тестируемое ЦИ с матрицей F_{test} - TIF-изображение.

Таблица 1 –

Изменение скорости возрастания наименьших СНЧ в блоках ЦИ-контейнера после СП с ОПИ 10%

| № ЦИ | Кол-во блоков (%), для которых скорость изменения наименьших СНЧ после СП | | № ЦИ | Кол-во блоков (%), для которых скорость изменения наименьших СНЧ после СП | | № ЦИ | Кол-во блоков (%), для которых скорость изменения наименьших СНЧ после СП | |
|---|---|------------|------|---|--|------|---|------------|
| | уменьшается | возрастает | | уменьшается | возрастает | | уменьшается | возрастает |
| 1 | 35.3 | 64.7 | 4 | 28.8 | 71.1 | 7 | 22.1 | 77.9 |
| 2 | 40.6 | 59.3 | 5 | 24.7 | 75.2 | 8 | 31.5 | 68.5 |
| 3 | 30.0 | 69.9 | 6 | 24.0 | 76.0 | 9 | 38.0 | 62.0 |
| Среднее значение (тестировались более 230 ЦИ) | | | | | | | | |
| Кол-во блоков (%), для которых скорость изменения наименьших СНЧ после СП уменьшается | | | | | Кол-во блоков (%), для которых скорость изменения наименьших СНЧ после СП возрастает | | | |
| 32 | | | | | 68 | | | |

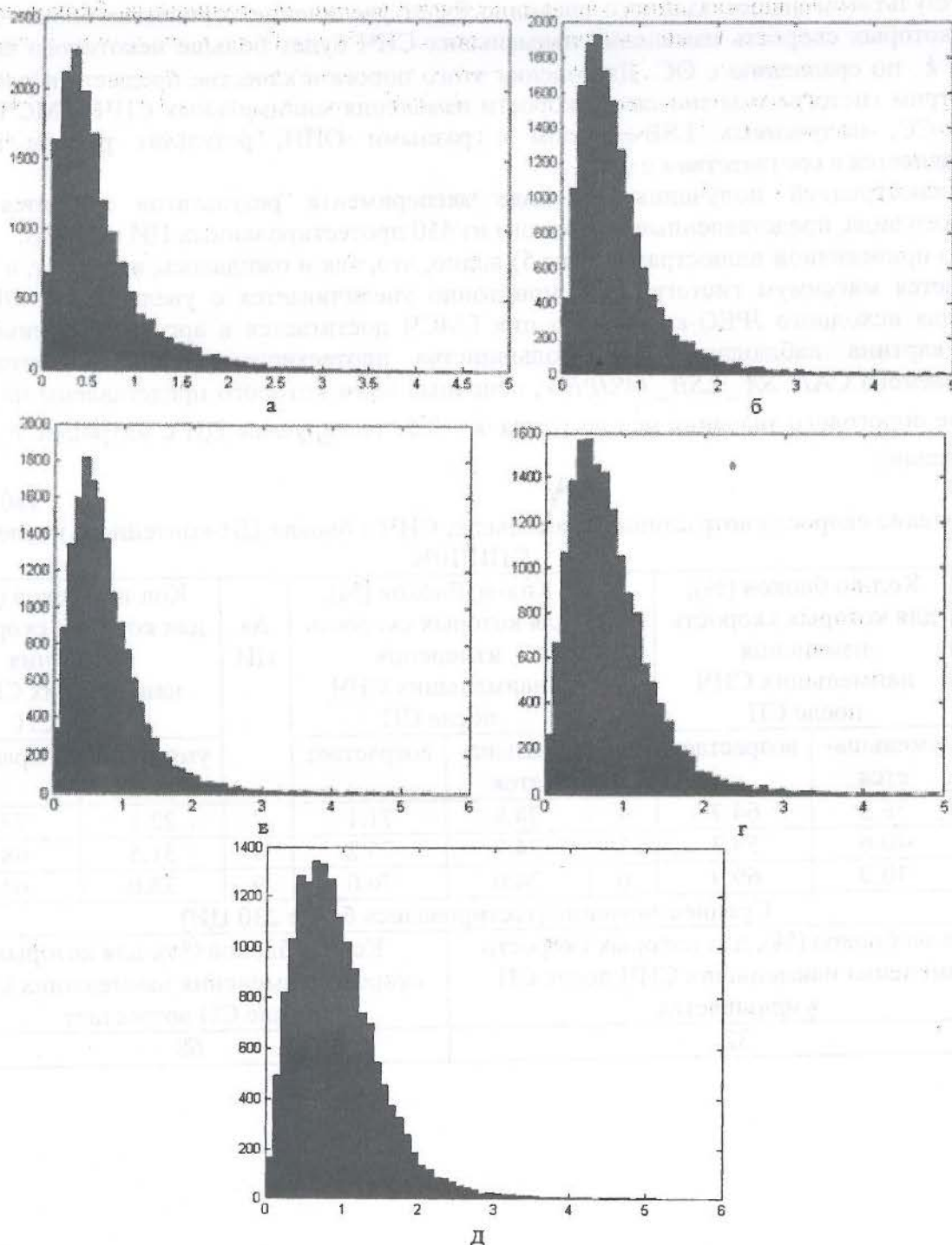


Рис.5. Гистограммы значений скорости изменения наименьших СНЧ блоков матриц с шагом 0.1: а - ОС, б – СС с ОПИ 10%, в – СС с ОПИ 20%, г – СС с ОПИ 35%, д – СС с ОПИ 65 %

Для апробации разработанного алгоритма *SA_LSB_OSJPEG* в среде MATLAB был проведен вычислительный эксперимент для более 500 различных JPEG-изображений, каждое из которых в процессе эксперимента пересохранялось в формате TIF. Перед пересохранением часть ЦИ подвергались СП с различными ОПИ. При работе алгоритма со СС с ОПИ 50%, 100% в 98% случаев наличие ДИ детектировалось верно. Ошибки первого рода для предложенного САА, когда ЦИ, не подвергавшееся СП, было ошибочно принято за СС, составили лишь 3%.

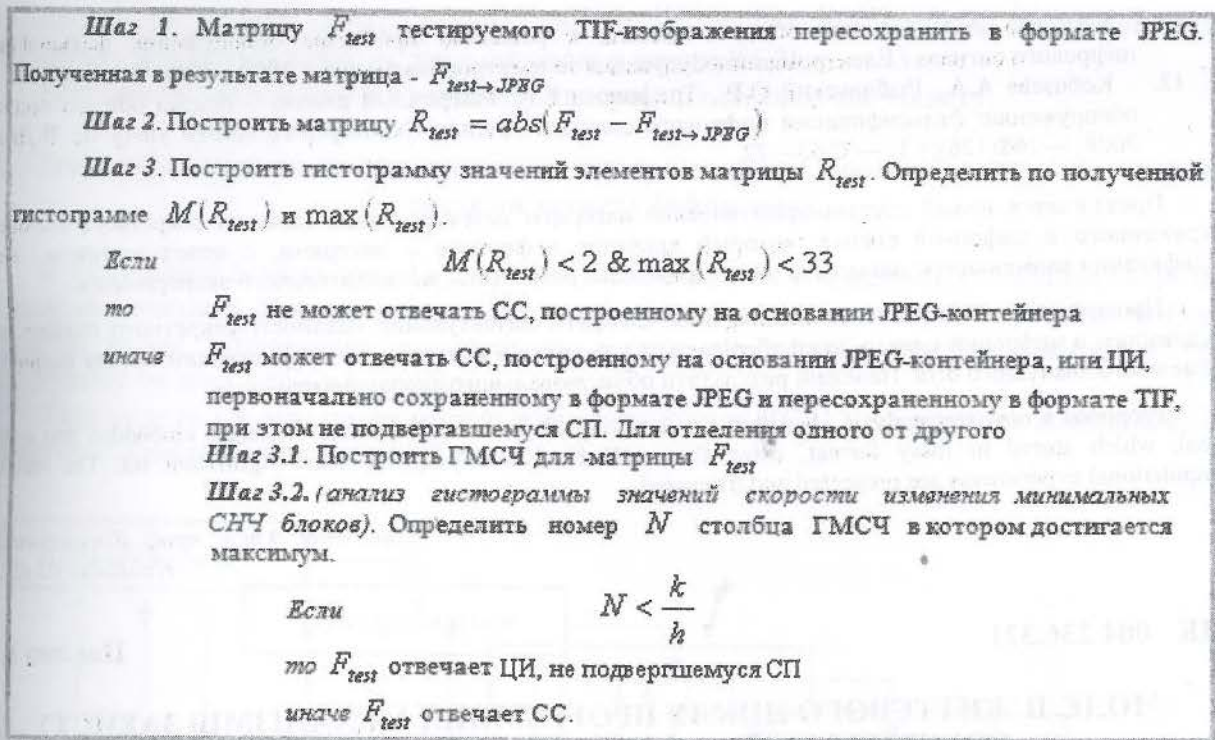


Рис.6. Стеганоаналитический алгоритм SA_LSB_OSJPEG детектирования секретного сообщения, погруженного LSB-методом

Таким образом, на основе проделанных в работе исследований разработан эффективный в условиях применения LSB-метода САА детектирования наличия секретного сообщения, погруженного с использованием метода модификации наименьшего значащего бита в JPEG-контейнер. В настоящий момент усилия автора направлены на поиск возможностей повышения эффективности разработанного метода при малом ОПИ.

Литература

1. G.Gul, F.Kurugollu. SVD-Based Universal Spatial Domain Image Steganalysis / IEEE Transactions on Information Forensics and Security. – 2010. - Vol. 5, NO.2. – PP. 349-353.
2. Грибунин В.Г. Цифровая стеганография / В.Г.Грибунин, И.Н.Оков, И.В.Туринцев. — М.: Солон-Пресс, 2002. — 272с.
3. G. Gul, A. E. Dirik, and I. Avcibas. Steganalytic features for JPEG compression based perturbed quantization. - IEEE Signal Process.Lett., vol. 14, no. 3, pp. 205–208, Mar. 2007.
4. S. Lyu and H. Farid. Detecting hidden messages using higher-order statistics and support vector machines / Lecture Notes in Computer Science. New York: Springer-Verlag, 2002, vol. 2578, pp. 340–354.
5. I. Avcibas, M. Kharrazi, N. Memon, and B. Sankur. Image steganalysis with binary similarity measures / EURASIP J. Appl. Signal Process., vol. 17, pp. 2749–2757, 2005.
6. Ленков С.В. Методы и средства защиты информации: в 2 т. / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко. — К.: Арий, 2008. — 344 с.
7. Кобозева А.А. Анализ защищеності інформаційних систем / А.А.Кобозева, І.О.Мачалін, В.О.Хорошко. - К.: Вид. ДУІКТ, 2010. – 316 с.
8. Кобозева А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации / Искусственный интеллект. — 2007. — №4. — С. 531-538.
9. Деммель Дж. Вычислительная линейная алгебра / Дж.Деммель; пер.с англ. Х.Д.Икрамова. — М.: Мир, 2001. — 430 с.
10. Кобозева А.А. Анализ информационной безопасности / А.А.Кобозева, В.А.Хорошко. - К.: Изд.ГУИКТ, 2009. – 251 с.
11. Гонсалес Р. Цифровая обработка изображений / Р.Гонсалес, Р.Вудс; пер. с англ. под ред. П.А.Чочиа. — М.: Техносфера, 2005. — 1072 с.

12. Кобозева А.А. Основы общего подхода к решению проблемы обнаружения фальсификации цифрового сигнала / *Електромашинобудування та електрообладнання*. - 2009. - Вип.72. - С.35-41.
13. Кобозева А.А., Рыбальский О.В., Трифонова Е.А. Матричный анализ – основа общего подхода к обнаружению фальсификации цифрового сигнала / *Вісник Східноукр-го нац-го ун-ту ім. В.Даля*. - 2008. — №8(126),ч.1. — С.62—72.

Предлагается новый стеганоаналитический алгоритм детектирования наличия секретного сообщения погруженного в цифровой сигнал, который хранится в формате с потерями, с использованием метода модификации наименьшего значащего бита. Приведены результаты вычислительного эксперимента.

Пропонується новий стеганоаналітичний алгоритм детектування наявності секретного повідомлення вбудованого в цифровий сигнал, який зберігається у форматі з втратами, з використанням методу модифікації найменшого значущого біта. Наведені результати обчислювального експерименту

Proposed a new steganalysis algorithm for detecting the presence of secret messages embedded into a digital signal, which stored in lossy format, using the method of modifying the least significant bit. The results of computational experiments are presented and discussed.

Рецензент: д.т.н., проф. Козловський В.
Надійшла 02.02.2011

УДК 004.236.321

Павлов І.М.

МОДЕЛІ ЖИТТЄВОГО ЦИКЛУ ПРОГРАМНИХ МЕХАНІЗМІВ ЗАХИСТУ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

З розвитком методів, технологій створення і експлуатації засобів захисту інформації з одного боку, відбувається все більша деталізація етапів життєвих циклів (конструювання), з другого – відбувається розширення життєвого циклу, набір все більших об'ємів інформації, знань, даних про розробку, виготовлення та функціонування засобів захисту.

Поняття моделі життєвого циклу виникло у зв'язку з необхідністю інтеграції процесів проектування, виготовлення і використання складних технічних систем, з одного боку, розвитком системного підходу як методологічної основи аналізу і синтезу систем – з другого боку. Метою введення цього поняття можна рахувати об'єднання різних технологій пов'язаних з процесом існування об'єкта дослідження, в єдину технологію, в якій визначені закони перетворення ролевих функцій компонентів локальних технологій.

Ця інтеграційна мета поділяється на наступні підцілі:

- розподіл загального процесу на основні етапи (фази);
- забезпечення безперервності фаз в рамках загального процесу;
- визначення основних характеристик фаз процесу;
- дослідження взаємного впливу етапів;
- використання інтегрального критерію ефективності життєвого циклу (функціоналу від часткових критеріїв фаз);
- забезпечення управління процесом реалізації фаз життєвого циклу;

Стосовно поняття проектування модель життєвого циклу визначається як упорядкована сукупність змін між початковим і кінцевим станом системи. При цьому початковий стан системи починається з моменту виникнення задуму (ідеї) або початку фінансування процесу її створення. А кінцевий стан починається з моменту закінчення діяльності у зв'язку з фізичним або моральним старінням, заміною або переобладнання в якісно новий об'єкт.

В [1] були розглянуті порядок аналізу та моделювання життєвого циклу комплексної системи захисту інформації (КСЗІ) на основі існуючих моделей інформаційних систем. Крім того показані приклади моделей життєвого циклу КСЗІ, які повинні бути проаналізовані розробниками на етапах проектування та розробки КСЗІ. В подальшому під час аналізу структури КСЗІ розробники, на основі розглянутих моделей життєвого циклу КСЗІ повинні проаналізувати та змоделювати порядок роботи механізмів захисту КСЗІ, які мають свої