примітивного елементу мультиплікативної групи відповідного скінченого поля та інших обчислень, в яких примітивний елемент використовується.

V Висновки

У даній роботі отримано критерій степеневості елемента скінченого поля та наведено прості рекурентні алгоритми обчислення кубічного кореня та коренів більш високого степеню з елементу поля, який є відповідним лишком. Алгоритми розпізнавання степеневості та добування кореня за складеним модулем (наприклад, за модулем $n=pq$) повністю визначаються відповідними алгоритмами за простим модулем, за умови, що відомий розклад числа n на прості множники та це число є вільним від квадратів.

Цікаво також зазначити, що задача розкладу на прості множники та задача добування кореня є поліноміально еквівалентними відносно імовірнісного алгоритму.

Дані алгоритми є, перш за все, цікавими з математичної точки зору, а їх поодинокий випадок – алгоритми добування кубічного кореня – можуть бути використані при побудові криптосистем на еліптичних кривих над кільцями лишків. Так, з використанням вказаних алгоритмів, замість імовірнісних алгоритмів обчислення базової точки кривої та алгоритмів "вкладання" відкритого тексту у точку кривої можна побудувати детерміновані алгоритми.

*Література: **1.** Коблиц Н. Курс теории чисел и криптографии. // Пер. с англ. – М.: Научное изд-во ТВП, 2001. – 254 с. **2.** О. Вербицький, "Вступ до криптології" // Л.: Вид-во науково-технічної літератури, 1998р., 247с. **3.** А. Бессалов, А. Тележенко, "Криптосистеммы на эллиптических кривых", Киев, 2004, 223 с. **4.** Н. Бабенко, "Методы и алгоритмы вычисления структур на ЭК с параллелизмом машинных операций" // Автореф. на соискание степени к.ф.-м.н., Ставрополь, 2011, 19с. **5.** А. Нестеренко, "Об одном варианте метода Ленстры факторизации целых чисел" // Материалы 3-ей международной конференции "Математика и безопасность информации" (МаБИТ-07), МГУ, 25-27 октября 2007 года, М.: МЦМНО, 2008, с. 234-240. **6.** М. Самохина. "Эллиптические кривые" // Доклад на семинаре кафедры радиотехники МФТИ, radio.fiztex.ru//infsec/f_3kdhla/f_3erfbr/seminar_6.pdf. **7.** М. Глухов. И. Круглов. А. Пичкур, А. Черёмушкин, "Введение в теоретико-числовые методы криптографии" // СПб.: Изд-во "Лань", 2011, 400с. **8**. Лидл Р., Нидеррайтер Г. Конечные поля: В 2-х т. / Пер. с англ. – М.: Мир, 1988. – 822 с.*

УДК 004.056.5

РАЗРАБОТКА НОВОГО ПОДХОДА К ВЫЯВЛЕНИЮ ЗАМЕЩАЮЩЕЙ ОБЛАСТИ В ЦИФРОВОМ ИЗОБРАЖЕНИИ

Алла Кобозева, Елена Лебедева

Одесский национальный политехнический университет

Анотація: ***Стаття присвячена подальшій розробці нового підходу до рішення задачі виявлення і локалізації заміщуючої області в цифровому зображенні, що був запропонований одним з авторів раніше, реалізацією якого став новий метод, який є інваріантним відносно формату збереження зображення.***

Summary: ***The article is devoted to the further development of a new approach to solving the problem of detection and localization of substitution region in a digital image that was proposed by one of the authors earlier, the implementation of which was a new method that is invariant relative to the storage format of the image.***

Ключові слова: ***Цифрове зображення, заміщуюча область, фальсифікація, сингулярне число, сингулярний вектор, матриця.***

I Введение

Неотъемлемой составной частью функционирования и жизнеобеспечения современного общества является анализ и обработка цифровых сигналов, преследующая разные цели. Несанкционированные изменения информационных контентов могут привести к невосполнимым пагубным последствиям как для отдельных лиц, так и для организаций и даже государства.

Последние успехи в создании, развитии и общедоступности редактирующего цифровые сигналы программного обеспечения требуют обязательного включения в комплексную систему защиты информации методов проверки целостности цифровых изображений (ЦИ), видео, аудио, отнесенных в [1] к пассивным методам информационной безопасности.

Настоящая работа посвящена вопросам детектирования и локализации фальсификации ЦИ, под которой понимается замещение части (частей) одного изображения, называемого основным (ОИ), частью (частями) другого (этого же) изображения, называемой замещающей областью (ЗО). Такой вид несанкционированного изменения изображения является одним из наиболее распространенных в случае преднамеренного нарушения его целостности [2 – 5].

Решению упомянутых вопросов сегодня уделяется много внимания, однако методы, информация о которых доступна в открытой печати, не лишены недостатков, наиболее значимыми из которых являются ориентированность на конкретные форматы хранения изображений, отсутствие возможности детектирования фальсификаций малых размеров [6 – 8], что делает актуальным поиск новых методов решения рассматриваемых задач.

В [9] были разработаны основы нового подхода к решению проблемы обнаружения и локализации ЗО в ЦИ произвольного формата, который без труда адаптируется для решения аналогичной задачи в цифровом видео, представляющем последовательность кадров, т. е. формализуемом в виде конечного множества матриц. Основой подхода явился анализ изменения поведения максимальных сингулярных чисел (СНЧ) σ_1 стандартных блоков тестируемого ЦИ, получаемых при последовательных сдвигах начального блока на 1 пиксель. В [9] на основании общего подхода к анализу состояния и технологии функционирования информационных систем (ОПАИС) [10] выдвинута и подтверждена в ходе вычислительного эксперимента следующая гипотеза: нарушение целостности ЦИ должно проявиться в виде скачка (разрыва первого рода) функции зависимости значения σ_1 от номера блока (при сдвигах на 1 пиксель), отделяющего СНЧ одного ЦИ от СНЧ другого, локализуя тем самым область фальсификации. Предложенный подход дает принципиальную возможность определения и локализации малой ЗО, например, размеры которой равны 1×8 пикселей [9]. Однако, при анализе поведения максимальных СНЧ блоков матрицы ЦИ возможна ситуация, когда разделение блоков, принадлежащих различным изображениям или различным частям одного изображения при выявлении фальсификации не будет явным. Такая проблема возникает в случае, когда энергии блоков ЦИ, задействованных в фотомонтаже, окажутся близкими по значению в области соединения изображений: скачок функции изменения максимального СНЧ хотя и будет иметь место, но будет трудно детектируемым. Это приводит к необходимости дополнительных исследований с привлечением анализа формальных параметров, определяющих ЦИ (блок ЦИ), отличных от СНЧ.

II Цель исследования и постановка задачи

Целью настоящей работы является дальнейшая разработка нового подхода к выявлению ЗО ЦИ, хранимых в произвольных форматах, предложенного в [9].

В соответствии с ОПАИС, положенному в основу разрабатываемого подхода, состояние ЦИ описывается состоянием совокупности СНЧ и сингулярных векторов (СНВ) матрицы (матриц), отвечающей ЦИ, составляющих полный набор формальных параметров. Это приводит к целесообразности привлечения анализа СНВ для организации дополнительных исследований изображения с целью выявления его фальсификации.

Таким образом, для достижения поставленной цели в работе необходимо решить следующие *задачи*:

1. Среди СНВ, входящих в полный набор формальных параметров, определяющих ЦИ в соответствии с ОПАИС, выделить наименее чувствительные к произвольным возмущающим воздействиям, в том числе, значительным, независимо от формата хранения изображения. Отличие характера поведения таких параметров для различных ЦИ даст возможность для выделения ЗО.
2. Разработать основные шаги метода выявления ЗО, учитывающего особенности изменения формальных параметров в оригинальных и фальсифицированных изображениях, инвариантного относительно форматов хранения ЦИ.

III Анализ поведения сингулярных векторов блоков матрицы цифрового изображения

Качественные и количественные характеристики многих параметров изображения зависят от формата его хранения, в частности, от того, предусматривает ли выбранный формат потери или является беспотерийным. Например, значения минимальных СНЧ в подавляющем большинстве блоков ЦИ, хранимого в формате с потерями, сравнимы друг с другом и мало отличаются от нуля, что не свойственно СНЧ блоков изображения, хранимого без потерь [10]. В связи с этим для решения задачи 1 необходимо проверить, существует ли среди СНВ блоков такие, поведение которых не зависит от формата изображения (потерийного или беспотерийного). С учетом того, что сжатие с потерями является одним из частных

случаев возмущающего воздействия, очевидно, что такие СНВ должны быть наименее чувствительными из всех к любому возмущающему воздействию. Характер изменения поведения таких векторов будет уникальным для конкретного ЦИ, а различия в поведении позволит отделить части разных ЦИ — ОИ от ЗО.

Пусть B - произвольный блок, полученный в результате стандартного разбиения матрицы ЦИ. Чувствительность СНВ u_i любой матрицы, в том числе и матрицы B, различна, и в соответствии с соотношением [11]

$$\frac{1}{2}\sin 2\theta_i \le \frac{\|\Delta B\|_2}{svdgap(i,B)},\ svdgap(i,B) \ne 0,$$

где $svdgap(i,B) = \min_{i \ne j} |\sigma_j - \sigma_i|$ — отделенность СНЧ $\sigma_i, i = \overline{1,8}$, матрицы B, θ_i — угол между соответствующими исходным и возмущенным сингулярными векторами u_i и $\bar{u}_i$, $i = \overline{1,8}$, мерой этой чувствительности является отделенность соответствующего сингулярному вектору сингулярного числа. Наибольшую отделенность в пределах любого блока ЦИ имеет максимальное СНЧ σ_1. Таким образом, наименее чувствительными к возмущающим воздействиям является левый и правый СНВ, далее обозначаемые u_1, v_1 соответственно, отвечающие σ_1. Выясним, зависит ли чувствительность этих векторов от формата хранения ЦИ.

По теореме Фробениуса [12] любая неразложимая неотрицательная матрица M всегда имеет положительное собственное значение $\bar{\lambda}(M)$, являющееся простым корнем характеристического уравнения. Модули всех других собственных значений не превосходят $\bar{\lambda}(M)$. Собственному значению $\bar{\lambda}(M)$ соответствует собственный вектор $\bar{\varphi}(M)$ с положительными координатами. В общем случае матрица блока B — это матрица общего вида, для которой имеет место нормальное сингулярное разложение [10]:

$$B = U_B \Sigma_B V_B^T, \tag{1}$$

где U_B, V_B — ортогональные матрицы левых и правых СНВ B соответственно, столбцы U_B лексикографически положительные [10], а Σ_B — диагональная матрица СНЧ $\sigma_1 \ge ... \ge \sigma_8 \ge 0$.

Для произвольного блока B симметричными неотрицательными неразложимыми матрицами являются BB^T и $B^T B$. Действительно:

$$\left(BB^T\right)^T = BB^T,\ \left(B^T B\right)^T = B^T B,$$

а неотрицательность и неразложимость вытекает из того, что B — блок матрицы яркости ЦИ, значения которой лежит в пределах от 0 до 255.

Рассмотрим более подробно BB^T. Для нее с учетом (1) имеет место соотношение:

$$BB^T = \left(U_B \Sigma_B V_B^T\right)\left(U_B \Sigma_B V_B^T\right)^T = U_B \Sigma_B^2 U_B^T, \tag{2}$$

которое в силу ортогональности матрицы U_B и лексикографической положительности ее столбцов, а также диагональности матрицы Σ_B^2 представляет собой нормальное спектральное разложение BB^T [10], определяемое однозначно, при этом собственные значения матрицы BB^T — диагональные элементы Σ_B^2, равные квадратам СНЧ B, в частности,

$$\overline{\lambda}(BB^T) = \sigma_1{}^2,$$

а левые СНВ B — ортонормированные лексикографически положительные собственные векторы BB^T. По теореме Фробениуса собственному значению $\overline{\lambda}(BB^T)$ отвечает собственный вектор $\overline{\varphi}(BB^T)$ с положительными координатами, являющийся одновременно левым СНВ u_1 блока B, отвечающим максимальному СНЧ σ_1.

Аналогичное утверждение будет следовать для правого СНВ v_1 блока, отвечающего σ_1, поскольку для симметричной матрицы $B^T B$ имеет место равенство, по смыслу аналогичное (2):

$$B^T B = \left(U_B \Sigma_B V_B{}^T\right)^T \left(U_B \Sigma_B V_B{}^T\right) = V_B \Sigma_B{}^2 V_B{}^T.$$

Таким образом, в любой неразложимой неотрицательной матрице, какой и является B, левый и правый СНВ, отвечающие максимальному СНЧ, имеют положительные координаты, т. е. находятся в первом координатном ортанте пространства R^8. Важно, что независимо от возмущающего воздействия, которое претерпевает ЦИ, матрицы его блоков остаются неразложимыми неотрицательными, а значит и обсуждаемые СНВ должны после любого возмущения (даже сильного), в том числе, после сжатия, иметь все положительные координаты, поэтому эти векторы являются не только нечувствительными, но и sign-нечувствительными к любому возмущающему воздействию [10], причем это свойство им присуще как до, так и после возмущающего воздействия, которое оставляет матрицу блока неразложимой неотрицательной. Очевидно, что это возможно лишь в том случае, когда обсуждаемые СНВ для подавляющего большинства блоков изображения будут близки к *n*-оптимальному [13].

Полученные результаты влекут за собой следующие выводы:

- результатом решения задачи 1 являются левый и правый СНВ блока ЦИ, отвечающие максимальному СНЧ;
- для блоков ЦИ независимо от формата хранения, а также от конкретики и величины возмущающего воздействия, которое претерпевает ЦИ, незначительными будут углы между векторами u_1 и *n*-оптимальным, v_1 и *n*-оптимальным и, как следствие, углы между u_1 и v_1;
- в силу коррелированности значений яркости соседних пикселей в ЦИ функция изменения угла между векторами u_1 и v_1 при переходе от блока к блоку со сдвигом в 1 пиксель в пределах одного ЦИ будет гладкой, а ее скачки — показателем наличия ЗО, что даст возможность для выявления ЗО.

Последовательный и совокупный учет изменений характера поведения максимальных СНЧ и соответствующих им СНВ в блоках тестируемого ЦИ даст возможность повышения эффективности анализа целостности ЦИ по сравнению с анализом лишь максимальных СНЧ блоков.

IV Метод обнаружения замещающей области в цифровом изображении

В результате полученных теоретических заключений разработан новый метод обнаружения замещающей области в цифровом изображении, эффективный независимо от того, с потерями или без потерь осуществляется его хранение. Формальным представлением ЦИ являются три матрицы, соответствующие цветовому пространству RGB.

Основные шаги предложенного метода следующие.

Шаг 1. В тестируемом ЦИ выделяется горизонтальная (вертикальная) блоковая полоса, высота (ширина) которой равна l пикселей (с учетом характеристик стандартного разбиения матрицы изображения возможно положить $l = 8$, что и делается ниже). В случае предполагаемой области фальсификации полоса выделяется так, чтобы захватывать подозрительную область. В противном случае выделение полосы происходит последовательно, начиная с крайней верхней (нижней) с последующим сдвигом на 1 пиксель вниз (вверх) в случае горизонтальной; начиная с крайней левой (правой) с последующим сдвигом на 1 пиксель вправо (влево) в случае вертикальной. Полоса проходится в одном направлении 8×8 – блоками со сдвигом в 1 пиксель, например, слева направо (в случае вертикальной полосы – сверху вниз).

Шаг 2. Для каждой из трех цветовых составляющих каждого 8×8 – блока B, которые обозначаются B_R, B_G, B_B, находятся: максимальное СНЧ σ_1, левый и правый СНВ - u_1, v_1, отвечающие максимальному СНЧ.

Шаг 3 *(локализация области фальсификации)*.

3.1. По результатам шага 2 строятся графики зависимости $\cos(u_1, v_1)$ - косинуса угла между u_1, v_1 от номера блока, которому они отвечают, по каждой цветовой компоненте для каждой блоковой полосы. Как область S_1, подозрительная на фальсификацию, на данном шаге рассматривается область блоков между глобальным минимумом графика и локальным минимумом, значение которого второе по модулю после модуля значения глобального минимума (рассматривается график для той цветовой составляющей, глобальный минимум в которой по модулю имеет максимальное значение).

3.2. По результатам шага 2 строятся графики зависимости R_σ - скорости изменения значения максимального СНЧ блока при переходе к следующему блоку от номера блока, по каждой цветовой компоненте. Как область, подозрительная на фальсификацию, на данном шаге рассматривается область S_2, состоящая из блоков, отвечающих части графика между глобальным максимумом графика и локальным максимумом, значение которого второе после значения глобального максимума (рассматривается график для той цветовой составляющей, глобальный максимум в которой имеет максимальное значение).

3.3. Область S_G, подозрительная на фальсификацию в рассматриваемой блоковой полосе, на данном шаге состоит из блоков тестируемого изображения, определяемых как

$$S_G = S_1 \cap S_2 .$$

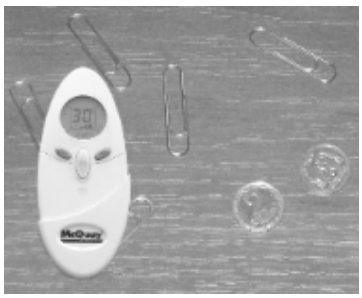
Шаг 4. Для блоков из S_G аналогичные шагам 3.1 – 3.3 действия проводятся для выделяемых вертикальных (горизонтальных) блоковых полос, пересекающих S_G. Пусть S_V - область блоков, подозрительная на фальсификацию в рассматриваемой вертикальной (горизонтальной) блоковой полосе на данном шаге.

Шаг 5. Границу области фальсификации содержит блоки из

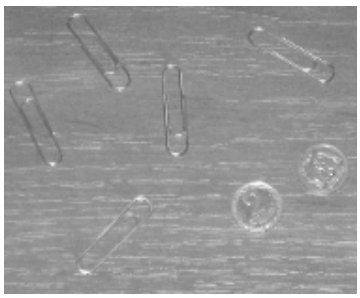
$$S = S_G \cap S_V ,$$

причем каждый из блоков, входящих в S, содержит в себе часть границы ЗО.

Работу предложенного метода рассмотрим на примере. Пусть тестируемое ЦИ изображено на рис. 1(а), при этом для наглядности расположения ЗО на рис. 1(б) приведено оригинальное изображение.



а



б

Рисунок 1 – Фальсифицированное ЦИ (а); оригинальное ЦИ (б)

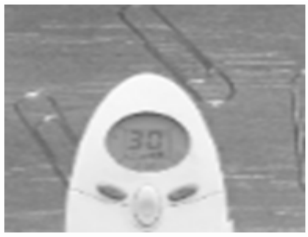


Рисунок 2 – Тестируемое ЦИ

Для наглядности и упрощения процедуры демонстрации результатов рассмотрим лишь часть фальсифицированного изображения, содержащего ЗО (рис. 2), которое и будем считать исходным.

Будем выделять на тестируемом изображении горизонтальные блоковые полосы, одна из которых высотой 8 пикселей, шириной 120 пикселей. представлена на рис. 3. Результат шага 3.1 для рассматриваемой полосы представлен на рис. 4. Подозрительной на фальсификацию на этом шаге является область, содержащая блоки, номера которых, соответствуют глобальному минимуму и локальному, модуль значения которого следующий за глобальным минимумом в кривой, отвечающей синей составляющей. Первый минимум соответствует блоку 68, второй – 11. Между этими блоками лежит фрагмент, представленный на рис. 5 (который действительно содержит фальсифицированную область).

Результат шага 3.2 представлен на рис. 6.

Рисунок 3 – Одна из блоковых горизонтальных полос тестируемого ЦИ

Максимальная скорость изменения максимального СНЧ блока соответствует блоку 40, а второе по величине значение отвечает блоку 68. Таким образом, S_G, а в конечном итоге и S включают блоки между 40 и 68. Окончательный результат работы предложенного метода представлен на рис. 7, что действительно отвечает части ЗО на блоковой полосе (рис. 3).

Замечание. В ходе дальнейшей разработки предложенного метода предполагается уточнение области, подозрительной на фальсификацию, что даст возможность выявления малых ЗО. Для этого необходим совокупный учет скорости изменения максимальных СНЧ и изменения характера поведения соответствующих им СНВ в блоках тестируемого ЦИ. Предполагается, что такой учет будет эффективным при следующей реализации:

Для блоков, вошедших в S в ЦИ выделяются вертикальные и горизонтальные блоковые полосы. Полоса проходится в одном направлении $8\times 8-$блоками со сдвигом в 1 пиксель слева направо (в случае вертикальной полосы – сверху вниз), повторяя при этом шаг 3.2 предложенного метода, после действий которого для каждого блока для совокупного учета нехарактерных для оригинальных изображений изменений угла между СНВ, отвечающими максимальному СНЧ блока, и значений скорости изменения максимальных СНЧ рассчитывается коэффициент

$$K=\frac{V\cdot\cos(u_1,v_1)}{W\cdot R_\sigma},$$

где V и W - весовые коэффициенты.

- По результатам предыдущего шага строится график зависимости K от номера блока для каждой горизонтальной (вертикальной) блоковой полосы. Для каждой кривой определяется номер блока, соответствующего глобальному минимуму кривой-графика.
- Блок из S, отвечающий глобальному минимуму построенного графика как для горизонтальной, так и для вертикальной блоковой полосы содержит в себе часть границы области фальсификации.

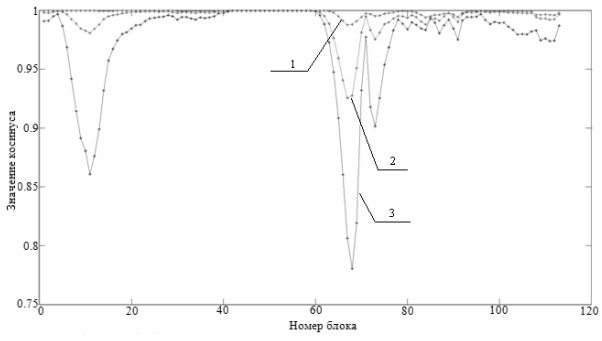


Рисунок 4 – График зависимости косинуса угла между правым и левым СНВ блока, отвечающими максимальному СНЧ, от номера блока: 1 – красная; 2 – зеленая; 3 – синяя составляющая

Рисунок 5 – Область, подозрительная на фальсификацию

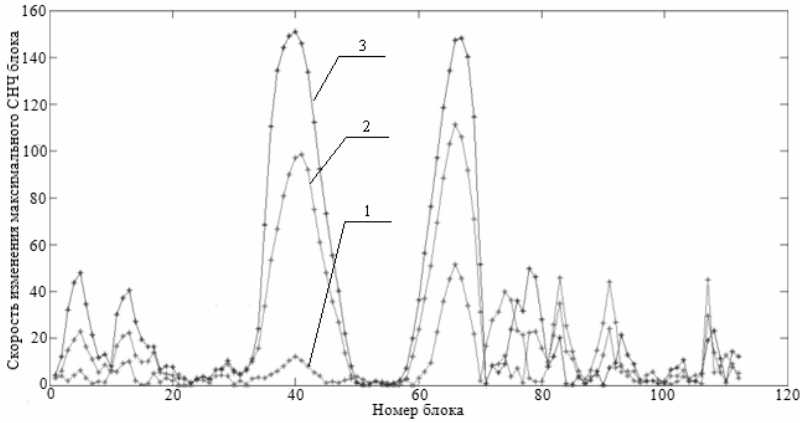


Рисунок 6 – График зависимости скорости изменения максимального сингулярного числа блока от номера блока: 1 – красная; 2 – зеленая; 3 – синяя составляющая

Рисунок 7 – Результат работы метода выявления ЗО

V Выводы

В настоящей работе осуществлена дальнейшая разработка нового подхода к выявлению ЗО ЦИ, предложенного в [9]. Показана целесообразность привлечения для обнаружения области фальсификации изображения анализа СНВ блоков соответствующей матрицы, отвечающих наибольшим СНЧ. В статье разработаны основные шаги нового метода, основанного на анализе поведения кривых, отражающих скорость изменения максимального СНЧ блока и изменение угла между соответствующими ему левым и правым СНВ при последовательном сдвиге блока на 1 пиксель в пределах горизонтальной (вертикальной) блоковой полосы. Предложенный метод может быть использован для решения задачи выявления ЗО в цифровом видео путем применения его к ключевым кадрам. Основным преимуществом предлагаемого метода является его инвариантность относительно формата хранения как ОИ, так и ЗО. Эта инвариантность вытекает из независимости используемых при построении метода свойств максимальных СНЧ и отвечающих им СНВ блоков матрицы от формата ЦИ.

*Литература:**1**. Нариманова Е. В. Проверка целостности цифрового сигнала. – Донецк: Изд. Цифровая типография, 2011. – 180 с. **2**. Кобозєва А. А. Аналіз захищеності інформаційних систем / А. А. Кобозєва, І. О. Мачалін, В. О. Хорошко. — К.: Вид. ДУІКТ, 2010. — 316 с. **3.** Журавель В. В. К развитию теории выявления следов цифровой обработки сигналограмм / В. В. Журавель, О. В. Рыбальский // Захист інформації. — 2007. — №1(32). — С. 83—85. **4.** Рыбальский О. В. Анализ тенденций разработки современных методов и аппаратуры экспертизы материалов и средств видео и звукозаписи / О. В. Рыбальский // Інформатика та математичні методи в моделюванні. — 2011. — Т.1, №1. — С.12—16. **5.** Кобозева А. А. Разработка общей теории выявления следов цифровой обработки сигналограмм и ее реализация аппаратно-программным комплексом «Теорема-М» / А.А.Кобозева, О. В. Рыбальский, В. И. Соловьев // Сучасна спеціальна техніка. — 2010. — №1(20). — С.5—14. **6.** Popescu A. C. Exposing digital forgeries by detecting traces of re-sampling / A. C. Popescu, H.Farid // IEEE Trans. Signal Process. — 2005. — Vol. 53(2). — P. 758—767. **7.** Bayram S. Image manipulation detection / S.Bayram, B.Sankur, N.Memon // Journal of Electronic Imaging. — 2006. — Vol. 15(4). —*

Р. 1—17. ***8.*** *Нариманова Е.В. Исследование эффекта двойного квантования и его использование при обнаружении фальсификации ЦИ / Е.В. Нариманова // Вісник Східноукр-го нац-го ун-ту ім. В. Даля. — 2008. — №8(126), ч.1. — С.47—55.* ***9.*** *Информационные технологии и системы в управлении, образовании, науке: Монография / Под ред. проф. В. С. Пономаренко. – Х.: Цифрова друкарня №1, 2013. – 278 с.* ***10.*** *Кобозева А. А. Анализ информационной безопасности / А. А. Кобозева, В .А. Хорошко. — К.: Изд.ГУИКТ, 2009. — 251 с.* ***11.*** *Деммель Дж. Вычислительная линейная алгебра / Дж.Деммель; пер.с англ. Х. Д. Икрамова. — М.: Мир, 2001. — 430 с.* ***12****. Гантмахер Ф. Р. Теория матриц / Ф. Р. Гантмахер. — М.: Наука, 1988. — 552 с.* ***13.*** *Кобозева А. А. Векторная SIGN-чувствительность как основа геометрической модели системы защиты информации / А. А. Кобозева, В. А. Хорошко // Захист інформації. — 2008. — №3. — С. 49—57.*

УДК 004.056.55:519.2

МЕТОДИКА ОБГРУНТУВАННЯ СТІЙКОСТІ НЕМАРКОВСЬКИХ СИМЕТРИЧНИХ БЛОЧНИХ ШИФРІВ ДО ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ

Сергій Яковлєв

Фізико-технічний інститут, НТУУ «КПІ»

Анотація: ***Запропонована методика оцінювання стійкості немарковських блочних шифрів до диференціального аналізу. Ґрунтуючись на даній методиці, був проведений аналіз низки узагальнених схем Фейстеля.***

Summary: ***We propose a procedure of provable security evaluation of non-Markov ciphers against differential cryptanalysis. Security of some generalized Feistel networks is estimated according to proposed procedure.***

Ключові слова: ***Симетрична криптографія, блочні шифри, диференціальний криптоаналіз, доказова стійкість, узагальнені схеми Фейстеля.***

I Вступ

Задача доказової стійкості блочних шифрів до диференціального аналізу була поставлена Ніберг та Кнудсеном у 1994 році [3]; ними була виведена теоретична верхня межа імовірності існування диференціалів у схемі Фейстеля, виражена через відповідні імовірності раундових функцій. Цей параметр дозволяє оцінити знизу складність проведення диференціальної атаки на довільний шифр, побудований на основі схеми Фейстеля. В подальшому подібні результати були одержані для низки інших ітеративних схем блочного шифрування. Зауважимо, однак, що переважна більшість отриманих оцінок стосувалась марковських шифрів, тобто шифрів, диференціальні імовірності яких були незалежними на кожному раунді. Дослідження доказової стійкості немарковських шифрів до диференціального аналізу вперше було зроблене Ковальчук [6]; нею одержані оцінки стійкості для немарковських схеми Фейстеля та MISTY-схеми.

В даній роботі пропонується загальна методика побудови аналітичної оцінки верхньої межі імовірності існування диференціалів через відповідні параметри раундових функцій. Ця методика базується на принципах, які використовувались при доведенні результатів попередніх дослідників, однак вона дозволяє оцінювати немарковські шифри та будувати аналітичні оцінки автоматично, що виявляється дуже корисним для оцінки стійкості складних схем шифрування, для яких традиційний математичний підхід вимагав би розглядання великої кількості різних випадків. Наприкінці ми покажемо застосування методики, що пропонується, для оцінювання стійкості деяких узагальнених схем Фейстеля до диференціального аналізу.

Зауважимо, що при аналізі марковських шифрів наведена методика може бути майже покроково перенесена для побудови оцінки теоретичної стійкості до лінійного криптоаналізу.

II Необхідні теоретичні відомості

Нехай M – множина відкритих текстів, C – множина шифртекстів, K – множина ключів.

Шифруюче перетворення – це функція вигляду

$$F : M \times K \to C,$$

яка задовольняє такій умові: для кожного фіксованого значення $k \in K$ перетворення $y = F(x,k) = F_k(x)$ є бієктивним. Надалі ми розглядаємо лише той випадок, коли множини M та C є просторами V_q двійкових векторів довжини q. Зауважимо, що це справедливо для переважної більшості сучасних алгоритмів шифрування.