$$R_{MAP} = \arg\max_{R_j \in R} p(R_j) \prod_{i=1}^{n} p(F_i \mid R_j) \quad (9)$$

В соответствии с выбранным подходом каждая составляющая выражения (3), заключенная в угловые скобки считается независимым событием. Относительные частоты появления таких событий для роли R_j являются оценками условных вероятностей $p(F_i|R_j)$. В случае, если проверяется транзакция, состоящая из нескольких команд, верхний предел n в выражении (9) равен количеству независимых событий вида (3), составляющих транзакцию.

Принцип обнаружения аномального поведения следующий – если на основании модели и текущего поведения пользователя классификатор определяет, что пользователь принадлежит к роли R_j и он действительно включен в эту роль, то поведение пользователя считается нормальным, в противном случае оно считается аномальным.

Литература: **1.** *Carter and Katz. Computer crime: an emerging challenge for law enforcement. FBI Law Enforcement Bulletin, 1-8, December 1996.* **2.** *Y. Hu and B. Panda. Identification of malicious transactions in database systems. In Proceedings of the nternational Database Engineering and Applications Symposium (IDEAS), 2003.* **3.** *A. Kamra, E. Bertino, and E. Terzi. Detecting anomalous access patterns in relational databases. The International Journal on Very Large Data Bases (VLDB), 2008.* **4.** *C. Chung, M. Gertz, and K. Levitt. Demids: a misuse detection system for database systems. In Proceedings of Integrity and Internal Control in Information Systems: Strategic Views on the Need for Control. IFIP TC11 WG11.5 Third Working Conference, 2000.* **5.** *V. Lee, J. Stankovic, and S. Son. Intrusion detection in realtime databases via time signatures. In Proceedings of the Sixth IEEE Real-Time Technology and Applications Symposium (RTAS), 2000.* **6.** *T. M. Mitchell. Machine Learning. McGraw-Hill, 1997.*

УДК 004.056.5+003.26

АНАЛИЗ СТОЙКОСТИ МЕТОДА КОХА-ЖАО СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ ИНФОРМАЦИИ В СТАТИЧЕСКИЕ ИЗОБРАЖЕНИЯ

Дмитрий Андрущенко, Галина Козина
Запорожский национальный технический университет

Аннотация: **Рассмотрен метод стеганографического встраивания информации Коха-Жао. В статье проведен анализ стойкости данного метода к JPEG-компрессии изображений со встроенным сообщением. Разработаны рекомендации по выбору параметров алгоритма.**
Summary: **The steganographic Koch and Zhao method is considered. The robustness of this method to the JPEG-compression of images with embedded data is analyzed. The robust algorithm settings are recommended.**
Ключевые слова: **Стеганоанализ, статическое изображение, метод Коха-Жао, алгоритм сжатия JPEG.**

I Введение

В связи с широким распространением мультимедийных технологий в последние годы появился значительный интерес к стеганографии. За это время было опубликовано немало качественных алгоритмов стеганографического скрытия данных в изображениях, как в зарубежной, так и отечественной литературе [1–4]. Однако значительно меньше публикаций посвящено анализу стойкости предложенных алгоритмов к различным атакам. Стеганографических методов, одинаково стойких ко всем видам атак, на сегодняшний день не существует. Поэтому при выборе стеганоалгоритма важно иметь в наличии как можно более подробный анализ стойкости этих алгоритмов к различным видам атак.

Другим важным требованием к стеганосистемам является «незаметность» встроенного сообщения, для обеспечения которого искажения, вносимые в контейнер во время скрытия в нем информации, должны быть минимальными, но обеспечивать при этом необходимую стойкость к определенным видам атак. В данной работе исследована стойкость стеганографического метода Коха-Жао к атаке сжатия JPEG в зависимости от различных параметров реализации алгоритма [1].

II Постановка задачи

Алгоритм Коха-Жао для скрытия данных использует частотную область контейнера и заключается в относительной замене величин коэффициентов дискретного косинусного преобразования (ДКП). Изображение разбивается на блоки размерностью 8×8 пикселей и к каждому блоку применяется ДКП. Каждый блок пригоден для записи одного бита информации. При организации секретного канала выбираются два коэффициента ДКП из полосы средних частот, которые задаются координатами (υ_1, ν_1) и (υ_2, ν_2). Для передачи бита «0» эти коэффициента изменяются так, чтобы разница между ними стала не ниже некоторой фиксированной величины P $(\geq P)$. Для передачи бита «1» эта разница должна стать не выше, чем $(-P)$ $(\leq -P)$. После этого производится обратное ДКП. От выбора параметров $\upsilon_1, \nu_1, \upsilon_2, \nu_2$ и P зависит величина вносимых изменений при встраивании информации в контейнер и стойкость стеганосистемы.

Цель данной работы – исследование стойкости стеганографической системы к JPEG-компрессии с различными коэффициентами сжатия α и разработка рекомендаций по выбору параметров алгоритма Коха-Жао при организации секретного канала передачи информации.

III Решение задачи

Для количественной оценки величины искажения использовалось пиковое отношение сигнал/шум, вычисляемое в децибелах [2]:

$$\mathrm{PSNR} = 10\log_2 \frac{n \cdot 255^2}{\sum_{i=1}^{n} \left(x_i - \overline{x}_i\right)^2}, \tag{1}$$

где n – число пикселей в изображении, $x_i, \overline{x}_i$ – значения пикселей исходного изображения и изображения со встроенным сообщением, 255 – максимальное значение яркости полутонового изображения (т.е. 8 бит/пиксель). Такая модель хоть и не является точной, поскольку плохо согласовывается со зрительной системой человека, но она очень популярна в связи с трудностью математического описанию последней [1]. Если в среднем *PSNR* ≥ 28 дБ, то величину вносимых искажений можно считать приемлемой [2]. В некоторых случаях могут быть более жесткие требования к вносимым искажениям.

Для проведения исследований было отобрано 10 фотографий размером 200x150 пикселей. В канал синего цвета каждой из них внедрено сообщение длиной 300 бит, представляющее собой битовое изображение размером 20x15 пикселей. Встраивание производилось в коэффициенты с координатами (4,5), (5,4) и (3,2), (2,3) при различных значениях параметра P, которое изменялось от 5 до 55 с шагом 5. Таким образом, было получено 220 изображений, каждое из которых в дальнейшем было подвергнуто компрессии с различным коэффициентом сжатия α, изменяющемся от 12 до 2 с шагом 1. Чем меньше α, тем большему сжатию подвергаются изображения. Из всех сжатых изображений (2420 шт.) извлекалось сообщение, которое сравнивалось с оригиналом. Для оценки совпадения сообщений вычислялся коэффициент корреляции [2]:

$$\rho = \frac{\sum_{i=1}^{N} w_i \widehat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2} \sqrt{\sum_{i=1}^{N} \widehat{w}_i^2}}, \tag{2}$$

где $w_i, \widehat{w}_i$ – элементы оригинального и извлеченного сообщения; N – количество бит сообщения.

Различные варианты извлеченного сообщения и соответствующие коэффициенты корреляции представлены в таблице 1.

Таблица 1 – Примеры оригинального сообщения и искаженных сообщений после извлечения и соответствующие коэффициенты корреляции

Графическое сообщение 1					

Коэффициент корреляции, ρ	1,00 (оригинал)	0,82	0,79	0,67	0,55
Графическое сообщение 2					
Коэффициент корреляции, ρ	1,00 (оригинал)	0,99	0,94	0,89	0,72

IV Полученные результаты

Результаты исследований представлены на рис. 1 и рис. 2. Анализ характера изменения кривых на рис. 1 показывает, что при увеличении параметра P, значение коэффициента корреляции ρ из зоны полного разрушения сообщения (заштрихованная область) переходит в зону частичного разрушения, после чего достигает уровня полного соответствия извлеченного и оригинального сообщений ($\rho = 1$), и в дальнейшем не изменяется.

Анализ характера изменения кривых на рис. 2 показывает, что при компрессии контейнера с коэффициентом сжатия $\alpha \le 5$, величина параметра P практически не влияет на пиковое отношение сигнал/шум *PSNR* (кривые сливаются на этом участке), что означает разрушение внедренного сообщения. Это подтверждается тем, что кривые на рис. 1 при $\alpha \le 5$ находятся в зоне полного разрушения сообщения. Конечно, при увеличении параметра P кривые перейдут в зону частичного разрушения, однако в данной работе было установлено, что при значениях $P > 55$ могут появляться видимые изменения контейнера при встраивании информации, что является крайне нежелательным при построении стеганосистемы. Поэтому был сделан вывод, что метод Коха-Жао пригоден, если не требуется стойкость стеганосистемы к компрессии с коэффициентом сжатия $\alpha \le 5$.

Полученные результаты также показали, что при встраивании сообщения в коэффициенты с координатами (3,2), (2,3) стойкость к сжатию, а, соответственно, и искажения контейнера оказались больше, чем при встраивании в коэффициенты с координатами (4,5), (5,4). Кроме того, сообщение не разрушается, когда искажения, вносимые компрессией изображений, не превышают искажений, вносимых внедрением сообщения.

Интересно проследить за характером изменения значения пикового отношения сигнал/шум *PSNR* при $P = 55$ (рис. 2). На участке $8 < \alpha < 12$ значение *PSNR* убывает, а извлеченное сообщение полностью совпадает с оригиналом (рис. 1), следовательно, преобладают искажения, вносимые при встраивании информации. На участке $6 < \alpha < 8$ значение *PSNR* возрастает, а извлеченное сообщение частично разрушено, значит, величина вносимых искажений при сжатии контейнера приближена к величине искажений, вносимых при встраивании информации. На участке $1 < \alpha < 6$ значение *PSNR* снова убывает, а извлеченное сообщение полностью разрушено, значит, преобладают искажения, вносимые при сжатии контейнера.

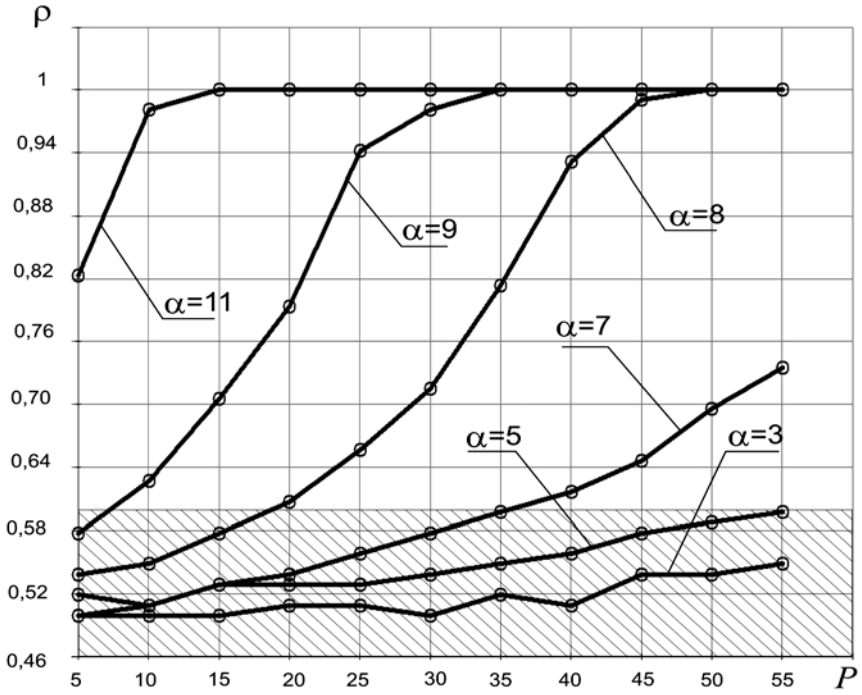

Рис. 1 – Изменение коэффициента корреляции для извлеченного и оригинального сообщений в зависимости от параметра P при различных коэффициентах сжатия контейнера α (для встраивания выбраны коэффициенты (4,5) и (5,4))

В зависимости от целей, предъявляемых к стеганосистеме, может требоваться различная стойкость к компрессии контейнера. Например, это может быть требование частичного соответствия извлеченного и оригинального сообщений с коэффициентом корреляции $\rho = 0{,}8$ при компрессии контейнера с коэффициентом сжатия $\alpha \geq 9$. На основании результатов исследований, полученных в данной работе, были разработаны рекомендации по выбору параметра P при встраивании сообщения по алгоритму Коха-Жао в зависимости от предъявляемых требований к стойкости стеганосистемы (табл. 2).

В случае требования частичного соответствия извлеченного и оригинального сообщений с коэффициентом корреляции $\rho = 0{,}8$ при компрессии контейнера с коэффициентом сжатия $\alpha \geq 9$ рекомендуется значение $P = 25$. Если требуется полное соответствие извлеченного и оригинального сообщений ($\rho = 1$) при компрессии контейнера с коэффициентом сжатия $\alpha \geq 8$ рекомендуется значение $P = 50$.

Полученные результаты относятся к встраиванию сообщения, представляющего собой битовое изображение. Однако, если встраивается «обычный» текст, требуется полное соответствие извлеченного и оригинального сообщения. В этом случае можно пойти по следующему пути. Перед встраиванием сообщения воспользоваться одним из методов помехоустойчивого кодирования [5] для преобразования

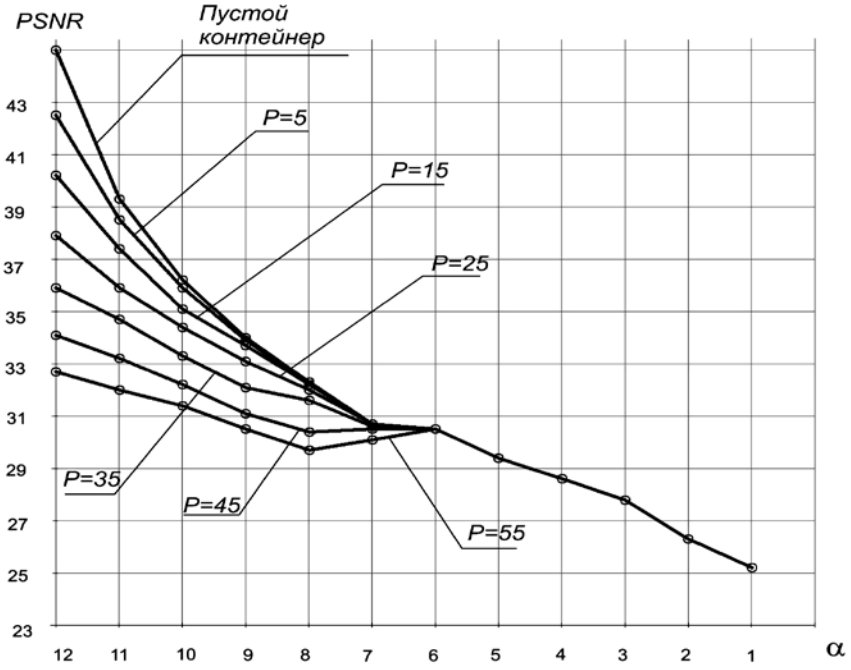

Рис. 2 – Изменение пикового отношения сигнал/шум в зависимости от параметра *P* при различных коэффициентах сжатия контейнера α (для встраивания выбраны коэффициенты (4,5) и (5,4))

текстового сообщения в помехоустойчивый код, предварительно сжав информацию. Это позволит с одной стороны избавиться от избыточности, которая всегда присуща в текстовой информации, а с другой – добавить специфическую избыточность, которая позволит восстановить сообщение после частичного разрушения.

Таблица 2 – Оптимальное значение параметра алгоритма *P* в зависимости от требований, предъявляемых к стойкости стеганосистемы

$\rho \backslash \alpha$	**12**	**11**	**10**	**9**	**8**	**7**	**6**
0,6	5	5	5	10	20	30	40
0,7	5	5	10	15	30	35	–
0,8	5	5	15	25	35	–	–
0,9	5	10	15	30	40	–	–
1	10	15	25	35	50	–	–

V Заключение

Полученные результаты позволяют при организации секретного канала передачи информации обоснованно выбирать параметры алгоритма Коха-Жао, обеспечивающие необходимый уровень стойкости одновременно с максимально возможной «незаметностью» встроенного сообщения.

Приемлемое значение параметра P алгоритма Коха-Жао находится в диапазоне $5 \le P \le 55$. Если $P < 5$, сообщение разрушается при малейшем сжатии контейнера. Если $P > 55$, видимые искажения, вносимые при встраивании информации в контейнер, чрезмерно велики. В случае приемлемых значений параметра P алгоритм Коха-Жао может обеспечить стойкость к компрессии контейнера с коэффициентом сжатия $\alpha \ge 6$ при полном соответствии извлеченного сообщения либо частичном его разрушении. Если требуется стойкость к компрессии контейнера с коэффициентом сжатия $\alpha \le 5$, то алгоритм Коха-Жао не пригоден.

В дальнейшем планируется создать систему стегоанализа для исследования стойкости других методов стеганографического встраивания информации к атакам, направленным на разрушение данных, встроенных в контейнер.

*Литература: **1**. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. –*

К.: МК-Пресс, 2006. – 288 с. ***2.*** *Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 272 с.* ***3.*** *Аграновский А.В., Девянин П.Н., Хади Р.А. и др. Основы компьютерной стеганографии. – М.: Радио и связь, 2003. – 151 с.* ***4.*** *Eyadat M., Vasikarla S. Performance evaluation of an incorporated DCT Block-Based Watermarking algorithm with Human Visual system Model // Pattern Recognition Journal. – 2005. – V. 26. – P. 1405-1411.* ***5.*** *Золотарев В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник / Под ред. чл.-кор. РАН Ю.Б. Зубарева. – М.: Горячая линия-Телеком, 2004. – 126 с.*

УДК 681.3.06

МЕТОД ПОБУДОВИ ВИСОКОШВИДКІСНОГО ПРОГРАМНО-ОРІЄНТОВАНОГО ПОТОКОВОГО ШИФРУ

Олександр Дирда

Державна служба спеціального зв'язку та захисту інформації України

Анотація: **Запропонована криптографічна схема нового программно-орієнтованого потокового шифру гамування з умовною назвою WSC, який базується на лінійному рекурентному регістрі довжини 32 над скінченним полем $GF(2^{32})$ та схемі ускладнення на основі чотирьох нелінійних регістрів зсуву над скінченним полем $GF(2^8)$. У схемі ускладнення пропонується використати 8×8 S-блоки з властивістю кореляційної імунності всіх координатних функцій.**

Summary: **This article proposes description of cryptographic scheme of new software-oriented stream cipher called WSC. It based on two items: linear feedback shift register length of 16 over the Galois field GF(2^{32}) and complication scheme which based on four nonlinear shift registers over the Galois field GF(2^8). 8x8 S-boxes with correlation immunity property of all coordinate functions are proposed to be used in this complication scheme.**

Ключові слова: **Потоковий шифр, генератор гами, лінійний рекурентний регістр, скінченне поле, S-блок, кореляційна імунність.**

I Вступ

Одним із важливих класів симетричних криптографічних алгоритмів є потокові шифри гамування. Вони містять у своєму складі генератор гами (ключової послідовності), що виробляє псевдовипадкову послідовність бітів, яка додається за модулем два до послідовності бітів відкритого тексту. Секретний ключ, як правило, використовується для ініціалізації початкового стану генератора гами.

До недавнього часу на практиці використовувались переважно біт-орієнтовані потокові шифри гамування, які містили один або декілька лінійних рекурентних регістрів (ЛРР) над скінченним полем $GF(2)$ та фільтруючі або комбінуючі булеві функції. Принципи синтезу та аналізу таких схем досить докладно наведені в монографії [1]. Математичні основи синтезу ЛРР над полем $GF(2)$ викладені в [2].

Прикладом біт-орієнтованого потокового шифру гамування є шифр A5, який був запропонований у 1987 році і використовується для криптографічного захисту інформації в стандарті GSM [3]. Ряд прикладів потокових шифрів наведені в монографії [4]. Біт-орієнтовані потокові шифри мають швидку апаратну реалізацію, однак, їх реалізація на сучасних процесорах є повільною. Такі шифри можна вважати апаратно-орієнтованими, хоча вони мають досить ефективну реалізацію на інтегральних логічних матрицях, що програмуються.

Першим широко відомим байт-орієнтовним потоковим шифром є шифр RC4, який був розроблений Рівестом у 1987 році [5]. В останнє десятиріччя криптографами розроблені низка високошвидкісних слово-орієнтованих потокових шифрів, найбільш відомими з яких є алгоритми SEAL, WAKE, SNOW 2.0, Sober-t32. Як байт-, так і слово-орієнтовані шифри є програмно-орієнтованими, що означає можливість їх ефективної реалізації саме на універсальних процесорах.

Взагалі, слід відзначити, що розробка високошвидкісних програмно-орієнтованих потокових шифрів є актуальною задачею сучасної прикладної криптографії. Це пояснюється, по-перше, поступовим витискуванням апаратних реалізацій складних електронних схем програмно-апаратними, по-друге, постійно зростаючою швидкістю передачі інформації у сучасних телекомунікаційних мережах передачі даних, що диктує необхідність розробки високошвидкісних алгоритмів шифрування. Про це свідчать ряд міжнародних