УДК 004.056.55

А. В. СИДОРЕНКО, И. В. ШАКИНКО, Ю. В. СИДОРЕНКО

АЛГОРИТМ ШИФРОВАНИЯ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ДВУМЕРНЫХ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ

Белорусский государственный университет

Предложен новый алгоритм шифрования изображений на основе динамического хаоса. При этом для шифрования используется модифицированная процедура перестановки элементов. Процедура же изменения значений элементов производится с учетом проведенной перестановки. Модифицированная процедура перестановки включает в себя следующие этапы: (1) формирование таблицы перестановки, (2) перестановку блоков изображения, (3) перестановку внутри областей изображения. Процедура «перестановка блоков – перестановка элементов внутри областей» проводится определенное количество раз ***q****. В данной работе использовалось значение* ***q*** *= 3. При проведении второй процедуры изменения значений к элементам изображения добавляется псевдослучайная последовательность* ***G****, для формирования которой предлагается следующий алгоритм. Он заключается в: (1) формировании распределения элементов гаммы* ***G*** *по значениям яркостей; (2) инициализации элементов гаммы* ***G****; (3) перестановке элементов гаммы* ***G****. Модифицированная процедура перестановки, как показали расчеты, позволяет уменьшить количество вычислений новых позиций элементов с использованием хаотических отображений в* ***a*** *раз. В данной работе использовались значения* ***a****, равные 16 и 64. Для осуществления предлагаемой процедуры изменения значений элементов требуется формирование* ***d*** *псевдослучайных значений из интервала [0, 1) с равномерным законом распределения. При этом для большинства практических задач достаточным является значение* ***d*** *= 256. Проведено тестирование предлагаемого алгоритма, которое заключается в следующем. Вычислены значения коэффициентов корреляции между исходным и зашифрованным изображениями, между соседними элементами (пикселями) зашифрованного изображения в вертикальном, горизонтальном, диагональном направлениях. Проведена оценка ключевой чувствительности алгоритма шифрования. Также определяются: нормированное среднее изменение интенсивности (UACI) и отношение количества различающихся бит к общему количеству бит изображения. Результаты тестирования предлагаемого алгоритма свидетельствуют о его работоспособности и возможности применения в задачах защиты информации в виде изображений.*

Ключевые слова: *динамический хаос, хаотическое отображение, шифрование, изображение, информационная безопасность.*

Введение

На современном этапе развития телекоммуникационных технологий изображения широко используются при работе различных веб-приложений. При этом для большинства приложений остро стоит вопрос защиты передаваемой информации. С учетом того, что размер изображений достаточно большой, а некоторым приложениям необходимо работать в режиме реального времени, процесс шифрования должен осуществляться достаточно быстро. Традиционные алгоритмы шифрования, например, такие как AES и DES, разрабатывались без учета этих требований и не являются подходящими для данных целей [1]. Поэтому возникает необходимость в создании новых алгоритмов шифрования.

Алгоритмы шифрования изображений на основе динамического хаоса

Новым подходом, используемым при шифровании изображений, является применение явления динамического хаоса. В частности, в схемах на основе данного явления используются две независимые процедуры [2]: перестановки и изменения значений элементов (пикселей) изображения. Проведение процедуры перестановки, во-первых, позволяет снизить корреляцию между значениями соседних элементов изображения, а во-вторых, делает визуальную

информацию изображения более устойчивой к потере фрагментов зашифрованного изображения из-за ошибок в канале связи [3]. Перестановка элементов должна осуществляться способом, похожим на случайный, и быть обратимой [4]. Данным условиям удовлетворяют двумерные хаотические отображения. Однако поскольку данная процедура не меняет сами значения элементов, то гистограмма распределения элементов по яркостям сохраняется и содержит информацию об исходном изображении. Возникает необходимость в проведении процедуры изменения значений элементов изображения.

Для снижения вычислительных затрат на осуществление процесса шифрования в данной работе используется модифицированная процедура перестановки элементов и процедура изменения значений элементов с учетом перестановки.

Модифицированная процедура перестановки элементов изображения

Модифицированная процедура перестановки включает в себя следующие этапы: 1) формирование таблицы T; 2) перестановку блоков изображения; 3) перестановку элементов внутри областей изображения.

На первом этапе формируется таблица T, содержащая m строк и n столбцов. При этом значением каждого элемента таблицы T является упорядоченная пара чисел, равных индексам соответствующего элемента:

$$t_{ij} = (i, j), \qquad (1)$$

где t_{ij} – ij-ый элемент таблицы T, $i = 1 \ldots m$, $j = 1 \ldots n$.

После этого к элементам таблицы T применяется процедура перестановки w раз с использованием выбранных хаотических отображений. При этом значения параметров данных хаотических отображений выступают в роли ключа шифрования. При выборе m и n меньших, чем размеры исходного изображения m_u и n_u, количество элементов в таблице в a раз меньше, чем в исходном изображении. Таким образом, при проведении перестановки требуется в a раз меньше вычислений с использованием хаотических отображений для определения новых позиций элементов. На втором этапе изображение разбивается на равные прямоугольные блоки. При этом размеры блоков выбираются таким образом, чтобы количество блоков по горизонтали было равно m, а по вертикали – n. Выбор именно таких размеров блоков позволяет использовать сформированную на предыдущем этапе таблицу T при проведении процедуры перестановки. На следующем этапе осуществляется перестановка сформированных блоков. Проведение данного этапа позволяет равномерно распределить по всему изображению его элементы. Однако взаимное положение элементов внутри каждого блока сохраняется. Для изменения взаимного положения элементов внутри блоков на изображении выделяются области размером m на n элементов. После этого осуществляется перестановка элементов внутри данных областей. Пара процедур «перестановка блоков – перестановка элементов внутри областей» проводится некоторое количество раз q. В данной работе использовалось значение $q = 3$.

Процедура изменения значений элементов изображения

Поскольку перестановка элементов изображения не изменяет значения самих элементов, то гистограмма распределения элементов по яркостям не изменяется после проведение перестановки и содержит информацию об исходном изображении. Таким образом, возникает необходимость в проведении дополнительной процедуры изменения значений элементов. Для уменьшения вычислительных затрат на осуществление процесса шифрования в данной работе предлагается схема процедуры изменения значений элементов на основе перестановки.

При проведении предлагаемой процедуры к элементам изображения добавляется псевдослучайная последовательность (гамма). При использовании гаммы для расшифровки символа исходного сообщения требуется знание только соответствующего символа зашифрованного сообщения и соответствующего элемента гаммы. Таким образом, если зашифрованное сообщение передается по каналу связи с помехами, то количество неверно расшифрованных символов исходного сообщения равно количеству символов зашифрованного сообщения, значения которых были изменены в рас-

сматриваемом канале связи вследствие помех. Следует отметить, что при использовании блочных алгоритмов шифрования с использованием некоторых режимов шифрования, изменение значения одного символа зашифрованного сообщения может привести к неверному расшифрованию половины символов исходного сообщения.

Для формирования псевдослучайной последовательности $\{g_i\}_{i=1}^{N} = G$ предлагается выполнение следующих этапов: 1) формирование распределе ния элементов гаммы по значениям яркостей; 2) инициализация элементов гаммы G; 3) перестановка элементов гаммы G.

На первом этапе вычисляются значения элементов последовательности $\{z_k\}_{k=1}^{d}$, где z_k имеет смысл количества элементов гаммы G со значением, равным b_k, $k = 1\ldots d$, d – количество возможных значений элементов изображения.

При формировании i-го значения элемента последовательности $\{z_k\}_{k=1}^{d}$ возможно использование биномиального распределения с математическим ожиданием ν_i и дисперсией μ_i равными:

$$\nu_i = N_i p_i , \tag{2}$$

$$\mu_i = N_i p_i (1 - p_i) , \tag{3}$$

где

$$N_i = \begin{cases} N, & i = 1 \\ N_{i-1} - z_{i-1}, & i > 1 \end{cases}, \tag{4}$$

$$p_i = 1(d - i + 1) , \tag{5}$$

N – количество элементов гаммы G, $i = 1\ldots d$.

Для моделирования случайной величины с биномиальным законом распределения существует ряд подходов [5]. При выполнении условий

$$Np(1 - p) > 5 , \tag{6}$$

для $p \in [0.1,0.9]$, и

$$Np(1 - p) > 25 , \tag{7}$$

для любого p, биноминальное распределение может быть аппроксимировано нормальным распределением. При этом для вычисления значений элементов последовательности $g_i = b_k$ потребуется формирование d псевдослучайных значений из интервала [0, 1) с равномерным законом распределения. Стоит отметить, что на практике значение d обычно равно 256, а условия (6) и (7) выполняются для изображений с количеством элементов большим, чем $N = 90 \cdot 90 = 8100$.

На следующем шаге каждому элементу гаммы G присваивается значение

$$g_i = b_k , \tag{8}$$

где индексы i и k связаны соотношением

$$\sum_{j=1}^{k-1} z_j < i \le \sum_{j=1}^{k-1} z_j + z_k , \tag{9}$$

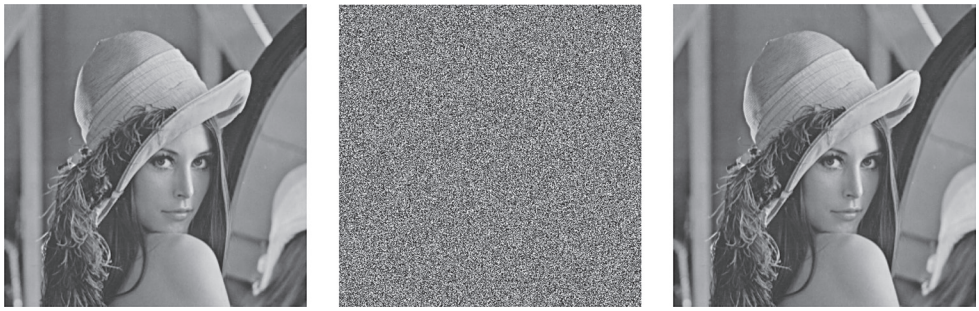
где $i = 1\ldots N$, $k = 1\ldots d$.

После этого проводится перестановка элементов последовательности G с использованием таблицы T, сформированной при проведении процедуры перестановки элементов изображения.

Предлагаемый алгоритм шифрования

Предлагаемый алгоритм шифрования сводится к следующей последовательности действий: 1) формирование таблицы перестановки T; 2) инициализация элементов гаммы G; 3) применение к элементам изображения I выбранное количество раз q пары процедур «перестановка блоков – перестановка элементов внутри областей» с использованием таблицы T; 4) добавление к изображению I_T, полученному на шаге (3), посредством операции «сложение по модулю 2» элементов гаммы G; 5) применение к элементам изображения I_G, полученного на шаге (4), выбранное количество раз q пары процедур «перестановка блоков – перестановка элементов внутри областей» с использованием таблицы T.

Для расшифровки полученного изображения требуется выполнение операций: 1) формирование таблицы перестановки T_{Inv}, обратной T; 2) инициализация элементов гаммы G; 3) применение к элементам зашифрованного изображения I_C выбранное количество раз q пары процедур «перестановка блоков – перестановка элементов внутри областей» с использованием таблицы T_{Inv}; 4) добавление к полученному изображению I_G, полученному на шаге (3), посредством операции «сложение по модулю 2» элементов гаммы G; 5) применение к элементам изображения I_T, полученного на шаге (4), выбранное количество раз q пары процедур «перестановка блоков – перестановка эле-



а *б* *в*

Результаты применения предлагаемого алгоритма шифрования к тестовому изображению «Lena.bmp»: *а* – исходное, *б* – зашифрованное и *в* – расшифрованное изображения

Таблица 1. **Значения коэффициентов корреляции**

Изображение	Алгоритм	$R_c \cdot 10^3$	$R_h \cdot 10^3$	$R_v \cdot 10^3$	$R_d \cdot 10^3$
«Lena.bmp»	предлагаемый	2,04	1,82	–3,97	9,20
	AES	–1,91	–7,80	9,23	2,34
«Baboon.bmp»	предлагаемый	–1,27	6,74	2,00	–2,83
	AES	2,55	7,86	4,81	–1,59
«Peppers.bmp»	предлагаемый	0,88	–5,99	2,26	–6,67
	AES	3,65	3,97	–10,00	1,81

ментов внутри областей» с использованием таблицы T_{Inv}.

Результаты и их обсуждение

Приводятся результаты применения предлагаемого алгоритма шифрования к изображениям «Lena.bmp», «Peppers.bmp» (512×512 пикселей) и «Baboon.bmp» (300×300 пикселей). Для формирования таблицы перестановки T использовались хаотические отображения «Кот Арнольда» и отображение Чирикова. Размеры таблицы T выбирались равными 64×64 и 75×75 для изображений с размерами 512×512 и 300×300, соответственно. Количество пар процедур «перестановка блоков – перестановка элементов внутри областей» q было выбрано равным 3. Результаты применения предлагаемого алгоритма шифрования к тестовому изображению «Lena.bmp» представлены на рисунке.

Визуально исходное и зашифрованное изображения существенно различаются, у зашифрованного изображения отсутствует структурированность. В качестве количественного параметра, характеризующего, насколько схожи изображения, использовался коэффициент корреляции R_c между элементами исходного и зашифрованного изображений. Также для зашифрованного изображения были вычислены значения коэффициентов корреляции между соседними элементами в горизонтальном R_h, вертикальном R_v и диагональном R_d направлениях (табл. 1). Для оценки равномерности распределения элементов изображения по значениям яркости использовалась дисперсия D гистограммы данного распределения.

Для сравнения приводятся результаты, полученные при использовании известного алгоритма AES. Как следует из приведенных данных, значения коэффициентов корреляции и дисперсии D, полученные при использовании предлагаемого алгоритма и алгоритма AES, схожи по величине.

Одним из параметров, характеризующих стойкость алгоритма шифрования, является чувствительность к изменениям секретного ключа. Для оценки данного параметра для двух зашифрованных изображений, полученных при использовании одного и того же исходного изображения и ключей шифрования, различающихся одним битом, были вычислены: количество пикселей, изменивших значение (Number of Pixel Changing Rate, NPCR); нормированное среднее изменение интенсивности (Unified Average Change Intensity, UACI); а также отношение количества различающихся бит к общему количеству бит изображения, выраженное в про-

Таблица 2. **Значения дисперсии гистограммы распределения элементов изображения по яркостям и значения параметров для оценки чувствительности алгоритма к изменениям ключа**

Изображение	Алгоритм	$D \cdot 10^{-3}$	A, %	UACI	NPCR·10^2
«Lena.bmp»	предлагаемый	1,19	49,98	0,335	99,60
	AES	1,10	50,03	0,335	99,62
«Baboon.bmp»	предлагаемый	0,29	50,01	0,336	99,60
	AES	0,34	49,98	0,334	99,57
«Peppers.bmp»	предлагаемый	0,93	49,98	0,335	99,61
	AES	1,16	49,99	0,335	99,61

центах (A) (табл. 2). Из полученных значений следует, что предлагаемый алгоритм проявляет чувствительность к изменениям ключа шифрования, сравнимую с чувствительностью алгоритма AES.

Заключение

Предложен новый алгоритм шифрования изображений на основе динамического хаоса. Отличительной особенностью данного алгоритма является уменьшение количества вычислений с использованием хаотических отображений. Модифицированная процедура перестановки позволяет уменьшить необходимое количество вычислений новых позиций элементов с использованием хаотических отображений в a раз. В данной работе использовалось значения a, равные 16 и 64. Для осуществления предлагаемой процедуры изменения значений элементов требуется формирование d псевдослучайных значений из интервала [0,1) с равномерным законом распределения. При этом для большинства практических задач $d = 256$.

Результаты тестирования предлагаемого алгоритма свидетельствуют о его работоспособности и возможности применения в реальных задачах защиты изображений в каналах передачи информации.

Литература

1. **Cheng, P.** A fast image encryption algorithm based on chaotic map and lookup table / P. Cheng [et al.] // Nonlinear Dynamics. – 2015. – Vol. 79, Issue 3. – P. 2121–2131.

2. **Hanchinamani, G.** Image encryption based on 2-D Zaslavskii chaotic map and pseudo Hadmard transform / G. Hanchinamani, L. Kulakami // Int. J. of Hybrid Information Technology. – 2014. – Vol. 7, Issue 4. – P. 185–200.

3. **Gschwandtner, M.** Transmission error and compression robustness of 2D chaotic map image encryption schemes / M. Gschwandtner, A. Uhl, P. Wild // EURASIP J. on Information Security [Electronic resource]. – 2007. – Mode of access: http:// jis. eurasipjournals. com/content/2007/1/048179. – Date of access: 08.04.2015.

4. **Wong, K.** Image encryption using chaotic maps / K. Wong // Intelligent computing based on chaos / L. Kocarev [et al.]. – Berlin, 2009. – Ch. 16. – P. 333–354.

5. **Харин Ю. С.** Математические и компьютерные основы статистического анализа данных и моделирования: учеб. пособие / Ю. С. Харин, В. И. Малюгин, М. С. Абрамович. – Минск: БГУ, 2008. – 455 с.

References

1. **Cheng, P.** A fast image encryption algorithm based on chaotic map and lookup table / P. Cheng [et al.] // Nonlinear Dynamics. – 2015. – Vol. 79, Issue 3. – P. 2121–2131.

2. **Hanchinamani, G.** Image encryption based on 2-D Zaslavskii chaotic map and pseudo Hadmard transform / G. Hanchinamani, L. Kulakami // Int. J. of Hybrid Information Technology. – 2014. – Vol. 7, Issue 4. – P. 185–200.

3. **Gschwandtner, M.** Transmission error and compression robustness of 2D chaotic map image encryption schemes / M. Gschwandtner, A. Uhl, P. Wild // EURASIP J. on Information Security [Electronic resource]. – 2007. – Mode of access: http://jis.eurasipjournals.com/content/2007/1/048179. – Date of access: 08.04.2015.

4. **Wong, K.** Image encryption using chaotic maps / K. Wong // Intelligent computing based on chaos / L. Kocarev [et al.]. – Berlin, 2009. – Ch. 16. – P. 333–354.

5. **Kharin Yu. S.** Mathematical and computer basics of statistical data analysis and modeling: textbook / Yu. S. Kharin, V. I. Malugin, M. S. Abramovich. – Minsk: BSU, 2008. – 455 p.

Поступила *25.03.2016* | *После доработки* *15.04.2016* | *Принята к печати* *10.05.2016*

Sidorenko A. V., Shakinko I. V., Sidorenko Yu. V.

IMAGE ENCRYPTION ALGORITHM USING TWO-DIMENSIONAL CHAOTIC MAPS

Belarusian State University

A new image encryption algorithm based on dynamic chaos is proposed. The encryption is performed using the modified element permutation procedure. The element value changing procedure is carried with regard to the performed permutation. The modified permutation procedure includes the following steps: (1) permutation table creation; (2) permutation of image blocks, (3) element permutation in the image regions. The procedure «block permutations – permutation in the image regions» is performed ***q*** *times – for this study* ***q*** *= 3. The second element value changing procedure is realized with the use of the pseudorandom sequence* ***G*** *that is added to the image elements. The following algorithm is proposed for the formation of this pseudorandom sequence: (1) the formation of the sequence* ***G*** *element distribution by brightness; (2) sequence* ***G*** *element initialization; (3) permutation of the sequence* ***G*** *elements. It is shown that, owing to the modified permutation procedure, the amount of calculations for new positions of the elements using chaotic maps is reduced by a factor of* ***a*** *– in this study* ***a*** *is equal to 16 and 64. The implementation of the proposed element value changing procedure necessitates the formation of* ***d*** *pseudorandom values from the interval [0, 1) with a uniform distribution. Actually, for the majority of practical cases* ***d*** *= 256 is applicable. The proposed algorithm has been tested as follows. The correlation coefficients have been computed for the original and encrypted images, and also for the adjacent elements in the vertical, horizontal, diagonal directions. The algorithm key sensitivity has been evaluated. Besides, the values of the unified average change intensity (UACI) and the ratios of differing bits to the total number of bits have been determined. As demonstrated by the testing results, the proposed algorithm is highly operable and may be successfully used to solve the tasks of information security.*

Keywords: *dynamic chaos, chaotic map, encryption, image, information security.*

Авторы

Сидоренко Алевтина Васильевна. Профессор кафедры физики и аэрокосмических технологий БГУ.

Научные интересы: защита информации в телекоммуникационных системах, теоретическая информатика, радиофизика, биофизика. E-mail: sidorenkoa@yandex.ru.

Шакинко Иван Владимирович. Аспирант кафедры телекоммуникаций и информационных технологий БГУ.

Научные интересы: защита информации в телекоммуникационных системах, динамический хаос и его применение.

Сидоренко Юлия Владимировна. Доцент кафедры физики полупроводников и наноэлектроники БГУ, к. ф.-м. наук.

Научные интересы: защита информации, физика полупроводников.