УДК 004.056.2

ШИФРОВАНИЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ХАОТИЧЕСКОЙ ДИНАМИКИ С ЭЛЕМЕНТАМИ ГЕНЕТИЧЕСКОГО АЛГОРИТМА

д-р техн. наук, проф. А.В. СИДОРЕНКО, М.С. ШИШКО
(Белорусский государственный университет, Минск)

Предложен новый алгоритм шифрования на основе хаотической динамики с элементами генетического алгоритма и осуществлена его реализация. В схеме предложенного алгоритма шифрования выделяются три этапа: инициализация, генерация изображений-шифров и применение элементов генетического алгоритма. В качестве критерия при выполнении этапов генерации изображений-шифров и применения элементов генетического алгоритма используется выбранное значение информационной энтропии в зашифрованном изображении. Определена стойкость алгоритма к статистическому и дифференциальному криптоанализу. Для оценки стойкости рассчитывались коэффициенты: NPCR (Number of Pixel Change Rate) и UACI (Unified Averaged Changed Intensity). Проведена оценка производительности рассматриваемого алгоритма. Представленный алгоритм может быть интегрирован в аппаратуру.

Ключевые слова: *шифрование, изображение, динамический хаос, алгоритм, стойкость алгоритма.*

Введение. Широкое распространение информационных технологий и Интернета вызывают проблемы обеспечения безопасного хранения и передачи данных в виде изображений. Одним из наиболее эффективных способов для решения этой задачи является шифрование информации [1]. Стандартные методы шифрования, включая AES, DES или RSA, из-за особенностей, свойственных изображениям, практически не дают эффекта.

В последние годы появился ряд алгоритмов шифрования изображений, использующих для маскирования динамический хаос. Благодаря присущим динамическому хаосу особенностям, связанным с наличием чувствительности к начальным условиям и случайности, такие методы подходят для шифрования изображений с высокой степенью защиты. При этом шифрование, как правило, происходит с использованием перестановки и диффузии. При перестановке с помощью хаотического отображения производится перераспределение пикселей изображения без изменения уровня их яркости. На стадии диффузии путем применения хаотической последовательности к изображению изменяется значение каждого пикселя.

В данной работе предлагается алгоритм шифрования изображений с использованием модели дезоксирибонуклеиновой кислоты (ДНК) [2] и динамического хаоса. В схеме предложенного нами алгоритма шифрования выделяются три этапа: инициализация, генерация изображений-шифров и использование генетического алгоритма. Два последних могут повторяться до тех пор, пока не будут удовлетворять выбранным критериям. В нашем случае в качестве критерия используется достижение соответствующего уровня информационной энтропии в зашифрованном изображении, что обусловлено необходимостью обеспечения лучшего быстродействия функционирования алгоритма. Рассмотрим подробнее этапы алгоритма.

Инициализация параметров алгоритма шифрования. Вводятся данные о необходимом значении энтропии, величине начальной популяции и значении процента мутирующих членов популяции. Производится вычисление хеш-суммы для изображения по алгоритму SHA-256. Для этого хеш-сумма разбивается на блоки, с помощью которых определяются начальные условия для хаотического отображения. Формирование начальной популяции производится при генерации хаотических последовательностей путем итерации логистического отображения. Она образуется за счет последовательностей, число которых равно размеру популяции, а размер каждой последовательности в три раза превышает количество пикселей шифруемого цветного изображения. Затем с помощью соответствующих кодировок начальная популяция и шифруемое изображение преобразуются в ДНК-последовательности. При этом получается ДНК-последовательность, соответствующая изображению, и некоторое количество ДНК-последовательностей, соответствующих начальной популяции (ДНК-маски).

Генерация изображений – шифров. На данном этапе происходит маскирование изображения ДНК-масками. После кроссовера для каждой ДНК-маски рассчитывается энтропия. Получаем несколько замаскированных ДНК-последовательностей, для которых рассчитывается энтропия замаскированных изображений.

Использование элементов генетического алгоритма. После вычисления энтропии происходит кроссовер между парами ДНК-масок, которые выбираются случайным образом по правилу рулетки, размеры векторов которой пропорциональны энтропии каждого члена. Точка кроссовера выбирается посередине каждой ДНК-маски. Маски с минимальным значением энтропии проходят процесс мутации и заменяются на новые маски, генерируемые как и члены начальной популяции. Рассчитывается энтропия. Если в популяции ДНК-масок есть хотя бы одна с энтропией, большей требуемого значения, то эта ДНК-маска используется для шифрования изображения, а соответствующие ей начальные условия – в качестве ключа расшифрования. При отсутствии этого популяция вновь проходит стадию кроссовера и мутации, пока не появится подходящая маска.

Тестирование и оценка производительности алгоритма. В данной работе проведена оценка стойкости шифра к статистическому и дифференциальному криптоанализам. При проведении статистического анализа шифрованного текста рассчитаны коэффициенты, позволяющие оценить стойкость шифра к статистическому криптоанализу: корреляция между соседними пикселями изображения и информационная энтропия. Как показали результаты проведенных вычислений, модуль коэффициента корреляции близок к нулевому значению и не превосходит двух сотых. Энтропия же в зашифрованном изображении близка к своему максимальному значению. В совокупности с низким уровнем корреляции это означает хорошую стойкость алгоритма к статистическому анализу.

Дифференциальный криптоанализ заключается в следующем. В исходное изображение вносится небольшое изменение, затем производится шифрование исходного и измененного изображений. После чего определяют различия в двух рассматриваемых изображениях, чтобы найти закономерности между изменениями в зашифрованных и исходных изображениях.

Для оценки стойкости к данному типу анализа открытый текст изображения зашифровывается, получаем изображение-шифр C1. Затем в открытом тексте изображения произвольно меняется один пиксель. Это измененное изображение зашифровывается тем же ключом, получаем изображение-шифр C2. С помощью коэффициентов NPCR (Number of Pixel Change Rate) и UACI (Unified Averaged Changed Intensity) [3] проводим сравнительный анализ полученных C1 и C2.

Тестирование проводилось с использованием изображений «Лена» и «Бабуин» с различным разрешением. Полученные результаты показывают, что и коэффициенты NPCR и UACI стремятся к своим идеальным значениям, что свидетельствует о хорошей стойкости к дифференциальному криптоанализу.

В данной работе проведена оценка производительности предложенного алгоритма, которая осуществлялась с помощью процессора Intel Core i5-3230M 2,4 GHz с 6 GB RAM. Результаты приведены на рисунках 1–3.

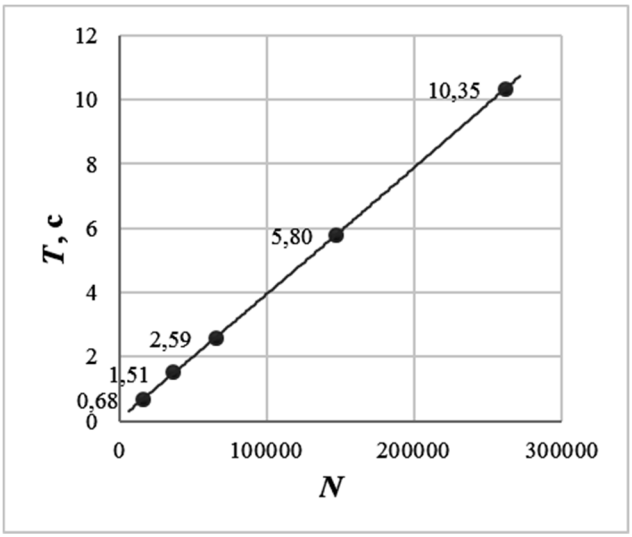

Рисунок 1. – График зависимости времени шифрования *T* (в секундах) от размера изображения *N* (в пикселях)

Как видно из рисунка 1, время шифрования растет по линейному закону в зависимости от количества пикселей изображения при постоянных остальных параметрах.

Приведенная на рисунке 2 зависимость времени шифрования от заданного значения энтропии показывает, что при малых значениях энтропии время шифрования практически остается постоянным. Это

связано с тем, что для достижения данного уровня достаточно одной итерации генетического алгоритма. Далее по графику происходит экспоненциальный рост времени шифрования от заданного значения энтропии.

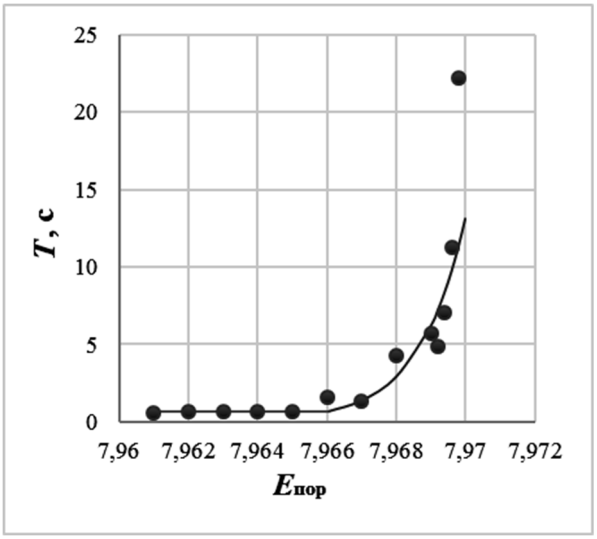

Рисунок 2. – График зависимости времени шифрования *T* (в секундах) от порогового значения энтропии $E_{пор}$

Приведенный на рисунке 3 график зависимости времени шифрования от заданного процента мутаций показывает, что существует минимум при 30% уровне мутаций.

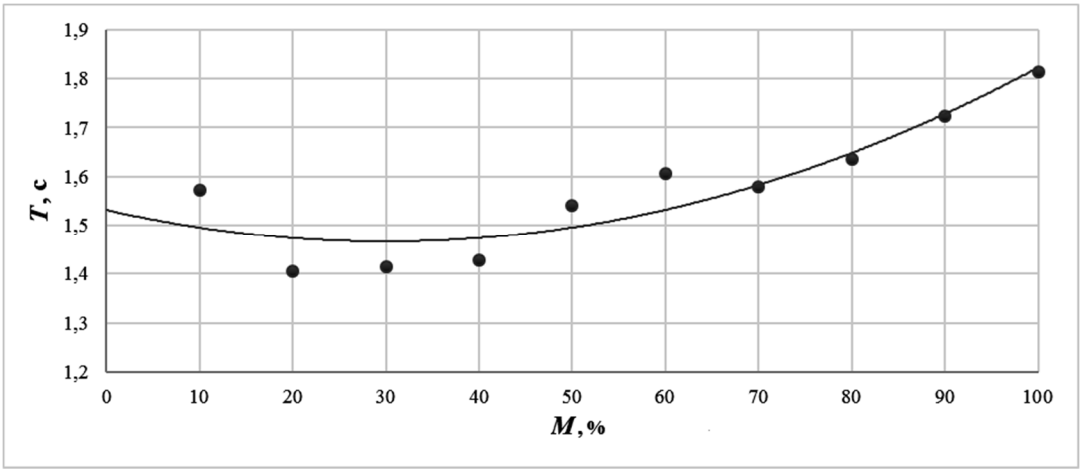

Рисунок 3. – График зависимости времени шифрования *T* (в секундах) от заданного процента мутаций *M*

Заключение. Предложенный алгоритм шифрования изображений позволяет повысить степень защиты информации, стойкость к различным атакам и может быть интегрирован в аппаратуру. Преимуществами данного алгоритма является его гибкость, а также возможность обеспечения шифрования с необходимым уровнем безопасности.

ЛИТЕРАТУРА

1. Wu, Y. NPCR and UACI Randomness Tests for Image Encryption / Y. Wu, J.P. Noonan, S. Agaian // Cyber journals: multidisciplinary journals in science and technology ; Journal of Selected Areas in Telecommunications (JSAT). – 2007. – April ed. – P. 31–38.

2. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system / X. Wei [et al.] // The Journal of Systems and Software. – 2012. – Vol. 85, iss. 2. – P. 290–299.
3. A novel image encryption scheme based on an improper fractional-order chaotic system / J. Zhao [et al.] // Nonlinear Dynamics. – 2015. – Vol. 80, iss. 4. – P. 1721–1729.

Поступила 19.03.2018

THE IMAGE ENCRYPTION BASED ON CHAOTIC DYNAMICS AND GENETIC ALGORITHM ELEMENTS

A. SIDORENKO, M. SHISHKO

New image encryption algorithm based on chaotic dynamics and genetic algorithm elements has been proposed and implemented as software. This algorithm went through three stages: initialization, generation of cipher-images and genetic algorithm elements. The chosen value of information entropy in encrypted image was used as criteria for realization the generation of cipher-images stage and genetic algorithm elements stage of considered algorithm. The resistance of the encrypted algorithm to statistic and differential cryptographic attacks has been examined. The coefficients: NPCR (Number of Pixel Change Rate) and UACI (Unified Averaged Changed Intensity) were calculated to estimate the resistance of the image encryption algorithm. The productivity estimation of the image encryption algorithm has been carried out. The present image encryption algorithm may be to integrate in the apparatus means.

Keywords: *encryption, image, dynamic chaos, algorithm, algorithm resistance.*