9. Sizykh V.N., Shlykova I.A. Adaptivnoe neiroupravlenie tipovym tekhnologicheskim modulem na osnove metoda skorostnogo gradient [Adaptive neural control by a typical technological module based on the speed gradient method]. *Mekhanika i protsessy upravleniya: materialy XXXXI Vseros. Simpoziuma* [*Mechanics and control processes: materials of the XXXXIth All-Russian symposium*]. Moscow: RAS Publ., 2011, Vol.2, pp. 246–255.
10. Daneev A.V. Entropiya A.N. Panchenkova [A.N. Panchenkov's Entropy]. *A.N. Panchenkov: fizik, matematik, inzhener* [*A.N. Panchenkov: a physicist, a mathematician, an engineer*]. Irkutsk: Irkutsk State Technical University Publ., 2005, pp. 103–128.
11. Daneev A.V., Rusanov V.A, Kumenko A.E. Entropiologiya sil'nykh differentsial'nykh modelei i ikh Fur'e-analiz [Entropyology of strong differential models and their Fourier analysis]. *A.N. Panchenkov: fizik, matematik, inzhener* [*A.N. Panchenkov: a physicist, a mathematician, an engineer*]. Irkutsk: Irkutsk State Technical University Publ., 2005, pp. 167–189.
12. Daneev A.V., Rusanov V.A, Sharpinskii D.Yu. Printsip maksimuma entropii v strukturnoi identifikatsii dinamicheskikh sistem [The principle of maximum entropy in the structural identification of dynamical systems]. *Izv. vuzov. Matematika* [*Russian Mathematics (Iz. VUZ)*], 2005, No. 11, pp. 64–69.
13. Daneev A.V., Vorob'ev A.A., Lebedev D.M. Algoritmy upravleniya slozhnymi organizatsionno-tekhnicheskimi sistemami [Algorithms for managing complex organizational and technical systems]. *Izvestiya IGEA* [*Bulletin of Baikal State University*], 2010, No. 4 (72), pp. 83–87.
14. Daneev A.V., Vorob'ev A.A., Lebedev D.M., Kumenko A.E., Mastin A.B. Metodika formirovaniya kompleksa sredstv uprav-leniya slozhnoi organizatsionno-tekhnicheskoi sistemoi [The method of forming a complex of management tools of a complex organizational and technical system]. *Vestn. BGU* [*The Buryat State University Bulletin*], Issue 9, 2010, pp. 263–269.
15. Daneev A.V., Vorob'ev A.A., Lebedev D.M. Issledovanie dinamiki povedeniya slozhnykh organizatsionno-tekhnicheskikh sistem v usloviyakh vozdeistviya neblagopriyatnykh faktorov [Investigation of the dynamics of behavior of complex organizational and technical systems under the influence of unfavorable factors]. *Vestn. Voronezh. in-ta MVD Rossii* [*The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia*], 2010, No. 2, pp. 163–172.

Информация об авторах

Данеев Алексей Васильевич - д. т. н., профессор кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: daneev@mail.ru

Данеев Роман Алексеевич - к. т. н., преподаватель кафедры информационно-правовых дисциплин, Восточно-Сибирский институт МВД России, г. Иркутск, e-mail: romasun@mail.ru

Сизых Виктор Николаевич - д. т. н., профессор кафедры «Автоматизация производственных процессов», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sizykh_vn@mail.ru

Authors

Aleksey Vasilievich Daneev – Doctor of Engineering Science, Professor of the Department of Information Systems and Information Protection, Irkutsk State Transport University, Irkutsk, e-mail: daneev@mail.ru

Roman Alekseevich Daneev – Ph.D. in Engineering Science, Prof., the Subdepartment of Information and Legal Disciplines, East-Siberian Institute of the Ministry of Internal Affairs of Russia, Irkutsk, e-mail: romasun@mail.ru,

Victor Nikolayevich Sizykh – Doctor of Engineering Science, Prof., the Subepartment of Automation of Production Processes, Irkutsk State Transport University, Irkutsk, e-mail: sizykh_vn@mail.ru

Для цитирования

Данеев А. В. Нечеткое управление человеко-машинной системой на основе энтропийного подхода и антропоцентрической модели оператора / А. В. Данеев, Р. А. Данеев, В. Н. Сизых // Современные технологии. Системный анализ. Моделирование. — 2017. — Т. 56, № 4. — С. 144-151. — DOI: 10.26731/1813-9108.2017.4(56).144-151.

For citation

Daneev A.V. Nechetkoe upravlenie cheloveko-mashinnoi sistemoi na osnove entropiinogo podkhoda i antropotsentricheskoi modeli operatora [Fuzzy control of the human-machine system based on an entropy approach and an anthropocentric model of the operator]. *Sovremennye tekhnologii. Sistemnyi analiz. Modelirovanie* [*Modern Technologies. System Analysis. Modeling*], 2017. Vol. 56, No. 4, pp. 144–151. DOI: 10.26731/1813-9108.2017.4(56).144-151.

УДК *004.056.55: 303.732.4: 519.1* ***DOI:*** *10.26731/1813-9108.2017.4(56).151-158*

О. В. Кузьмин, И. А. Зеленцов

Иркутский государственный университет, г. Иркутск, Российская Федерация
Дата поступления: *24 октября 2017 г.*

КОДИРОВАНИЕ ЗВУКОВОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ АЛГОРИТМА ПЕРЕСТАНОВКИ

Аннотация. *В настоящее время имеется несколько областей совместного применения комбинаторного анализа и теории кодирования. С одной стороны, теория кодирования имеет разнообразные приложения при решении комбинаторных задач большой размерности. С другой стороны, активно развиваются комбинаторные методы, применяемые в различных алгоритмах кодирования и декодирования различных видов информации, к которым можно отнести текстовую, графическую, звуковую и ряд других. Известыо алгоритмы шифрования на основе стандарта расширенного шифрования (AES). Однако AES имеет ограничения в отношении некоторых специфических требований к мультимедиа, что создает необходимость в разработке других алгоритмов шифрования. Данная статья посвящена разработке алгоритма шифрования звуковой информации с помощью перестановок. Предложенный алгоритм использует процедуру перестановки для выполнения шифрования аудиофайлов,*

применяя метод шифрования потока. Алгоритм использует закрытый ключ для выполнения шифрования, зависящего от ключа и данных. Шифрование аудиофайлов было выполнено в пять шагов. В этих шагах применяется замена таблиц и различные способы перестановки аудиоданных для выполнения шифрования без потерь. Разработанный авторами алгоритм был реализован и протестирован с различными типами аудиофайлов разных размеров. Эмпирический анализ показал, что данный алгоритм эффективен для шифрования аудиофайлов среднего или высокого качества. Статистический анализ с использованием гистограмм, пикового отношения сигнала к шуму, корреляции и энтропии показал, что алгоритм неуязвим для статистических атак, если он не используется для шифрования низкокачественных аудиофайлов.

Ключевые слова: *криптография, потоковый шифр, алгоритм, шифрование, дешифрование, системный анализ, перестановки, звук, аудиофайл.*

O. V. Kuz'min, I. A. Zelentsov

Irkutsk State University, Irkutsk, the Russian Federation
***Received**: October 24, 2017*

CODING SOUND INFORMATION WITH A PERMUTATION ALGORITHM

Abstract. *At present, there are several areas of joint application of a combinatorial analysis and a coding theory. On the one hand, the coding theory has a variety of applications for solving combinatorial problems of large dimension. On the other hand, combinatorial methods are actively being developed, used in various algorithms for encoding and decoding various types of information, which include text, graphics, sound, and a number of others. There are known encryption algorithms based on the Advanced Encryption Standard (AES). However, AES has limitations on certain specific multimedia requirements, which makes it necessary to develop other encryption algorithms. This article is devoted to the development of an algorithm for encrypting audio information using permutations. The proposed algorithm uses a permutation procedure to perform encryption of audio files using a stream encryption method. The algorithm uses a private key to perform encryption, depending on the key and data. Encryption of audio files was performed in five steps. In these steps, tables are replaced and various ways of rearranging audio data are used to perform lossless encryption. The algorithm developed by the authors was implemented and tested with different types of audio files of different sizes. Empirical analysis has shown that this algorithm is effective for encryption of medium or high quality audio files. Statistical analysis using histograms, peak signal-to-noise ratio, correlation and entropy showed that the algorithm is not vulnerable to statistical attacks if it is not used to encrypt low-quality audio files.*

Keywords: *cryptography, stream cipher, algorithm, encryption, decryption, system analysis, permutations, sound, audio file.*

Введение

В настоящее время имеется несколько областей совместного применения комбинаторного анализа и теории кодирования [19]. С одной стороны, теория кодирования имеет разнообразные приложения при решении комбинаторных задач, большой размерности [20]. С другой стороны активно развиваются комбинаторные методы, применяемые в различных алгоритмах кодирования и декодирования различных видов информации, к которым можно отнести текстовую, графическую, звуковую и ряд других.

Стандарт расширенного шифрования (Advanced Encryption Standard, или AES) [1], хорошо известен для обеспечения безопасного шифрования. Было разработано множество алгоритмов шифрования на основе AES. Однако AES имеет ограничения в отношении некоторых специфических требований к мультимедиа, что создает необходимость в разработке других алгоритмов шифрования [2-5].

Некоторые алгоритмы, такие как [4], [6-8], [14-17] применяли различные методы перестановки для шифрования текстовых файлов и изображений. Работа [9] использовала алгоритм RSA для шифрования речевых файлов, состоящих из отдельных слов. Авторы извлекали каждое слово и преобразовывали его в текст. Этот метод не может быть легко обобщен для применения к общему аудиосодержанию. В [5] была представлена хаотическая система для аудиошифрования. Авторы получили несколько ключей шифрования через хаотическую карту, где на каждой итерации процесса шифрования используется другой ключ. Шифрование аудиофайлов в [10] было выполнено в пять шагов. В этих шагах применяется замена таблиц и различные способы перестановки аудиоданных для выполнения шифрования без потерь.

Некоторые исследовательские работы в области системных методов обработки информации направлены на сокращение времени шифрования аудио путем шифрования отдельных частей аудиофайла [11-13], [16, 17]. Частичное шифрование аудиофайлов может быть выполнено с использованием дискретного преобразования Фурье для шифрования нижних частотных диапазонов [11]. В качестве альтернативы эффективный алгоритм шифрования, такой как AES, может быть применен к выбранным частям аудиофайла за счет незначительного снижения безопасности зашифрованных файлов [12, 13].

Далее представлен новый алгоритм для выполнения шифрования с использованием поточного шифрования в случайном порядке. Алгоритм

был реализован и протестирован, и анализ выполнен, чтобы показать его эффективность.

Выполнение шифрования аудиофайлов с помощью перестановки

Этот алгоритм принимает аудиофайл и ключ в качестве входных данных и выполняет байтовую перестановку [18] аудиоданных. Аудиофайл рассматривается как поток, и выполняемое шифрование зависит как от ключа, так и от данных. Ниже приведен алгоритм шифрования.

Алгоритм 1.

For i = 1 to k

fixBit = Hash(Key, i)

D = вектор, где D [j] - значение бит (fixBit) j-го байта текущего потока

S0 = вектор, содержащий числа байтов текущего потока (j), которые имеют (D [j] = = 0)

S1 = вектор, содержащий числа байтов текущего потока (j), которые имеют (D [j] = = 1)

Перемещение = Сцепление S0 с S1

Замените байты текущего потока так, чтобы новое местоположение байта (j) было байтом (Перемещение [j])

EndFor

Этот алгоритм работает следующим образом. Один бит, назовём его *fixBit*, выбирается Hash-функцией на основе ключа и номера итерации. Вектор перестановки (одномерный массив) строится путем перечисления чисел байтов, которые имеют значение битового числа *fixBit*, равное нулю, за которым следуют числа байтов, которые имеют значение битового числа *fixBit*, равное единице. Этот вектор дает отображение, которое определяет новое местоположение каждого байта в частично зашифрованном потоке. Этот шаг повторяется для нескольких итераций. Каждая итерация использует другой *fixBit* и применяет те же шаги к новому частично зашифрованному потоку, который был результатом предыдущей итерации. Число итераций, *k*, представляет собой небольшое целое число, выбранное ключевой функцией. Следующий простой пример показывает, как это шифрование применено.

Следующий простой пример показывает, как это шифрование применяется. Пусть двоичное представление ввода: *11110101 00101101 10100011 10001100* с ключом *= (3, 5)*. Для простоты предположим, что две итерации применяются с значениями *fixBit*, выбранными напрямую и последовательно из ключа. На первой итерации *fixBit = 3*, и этот бит подчеркивается на входе выше. Исходя из значений этого *fixBit*, *S0 = (1, 3)* и *S1 = (2, 4)*, которые делают вектор перестановки *(1, 3, 2, 4)*. Следовательно, после замены перестановки будет *11110101 10100011 00101101 10001100*. Вторая итерация применяется к этому результату таким же образом, но с *fixBit = 5*.

Прежде чем шифровать аудиофайлы с использованием вышеуказанного алгоритма, данные должны быть нормализованы в один или несколько потоков байтов. В зависимости от качества, звуковая дорожка может использовать 8, 16 или более бит для представления значений звука. Если для каждого значения используется 8 бит (1 байт), звуковой файл нормализуется в один аудиопоток. Если используется звук более высокого качества, аудиофайл нормализуется в большее количество потоков, где количество потоков равно количеству байтов, необходимых для представления значений звука.

Рассмотрим, например, значения в типичном аудиоформате, которые варьируются от -1 до 1, где другие аудиоформаты могут быть нормализованы аналогичным образом. Если для представления каждого значения используются 16 бит (2 байта), добавьте 1 к каждому значению, а затем умножьте его на 127. Это преобразует каждое значение в рациональное число в диапазоне от 0 до 254. Мы отделяем целую часть от части дроби, где каждая часть требует 8 бит (1 байт). Когда выполняется шифрование, целые части рассматриваются как один поток, а части дроби рассматриваются как другой поток. Каждый поток зашифровывается отдельно. Напомним, что вектор перестановки строится путем перечисления чисел байтов, которые имеют значение битового числа *fixBit*, равное нулю, за которым следуют числа байтов, которые имеют значение битового числа *fixBit*, равное единице. Поэтому каждый из этих двух потоков будет генерировать другой вектор тасования, даже если они используют один и тот же ключ. Следовательно, когда используется больше потоков, будет происходить большее перемешивание, что приведет к повышению безопасности.

Алгоритм дешифрования аналогичен алгоритму шифрования. Он выполняется с таким же количеством итераций, используемых в шифровании, где каждая из итераций шифрования инвертирована. Ниже описан алгоритм дешифрования.

Алгоритм 2.

For i = k - 1 step -1

fixBit = Hash(Key, i)

D = вектор, где D [j] - значение бит (fixBit) j-го байта текущего потока

S0 = вектор, содержащий числа байтов текущего потока (j), которые имеют (D [j] = = 0)

S1 = вектор, содержащий числа байтов текущего потока (j), которые имеют (D [j] = = 1)

Перемещение = Сцепление S0 с S1

Замените байты текущего потока так, чтобы новое местоположение байтового номера (Shuffle [j]) было байтовым числом (j)
EndFor

Когда шифрование разделяет входной файл на два или более потока, процесс дешифрования также сделает это. Каждый поток дешифруется отдельно, а затем окончательные дешифрованные потоки объединяются и восстанавливаются в аудиоформат.

Реализация и анализ

Безопасность этого алгоритма исходит из сложности операции тасования. Если один или несколько битов в клавише изменены, выбирается другой бит в случайном порядке, и замена заменяется. Для каждого потока данных есть $k \cdot 2^b$ различных возможных векторов тасования для ввода байтов размера b, зашифрованных в k итерациях. Так как у типичного аудиофайла нет размера меньше, чем несколько килобайт, атака «в лоб» на зашифрованный файл невозможна.

Алгоритм был применен к 25 аудиофайлам различных типов и размеров, где их средний размер составлял 39 килобайт. Когда с одним и тем же файлом использовались разные ключи, они создавали разные зашифрованные файлы. Кроме того, анализ с использованием гистограмм, пикового отношения сигнала к шуму (Peak Signal-to-Noise Ratio или PSNR), корреляция и энтропия показывают свойства алгоритма, которые противостоят статистическим атакам.

Когда качество входного звука использовало два или более байта для каждого значения, входной файл был разделен на два или более потока, и каждый поток был зашифрован отдельно. Затем зашифрованный файл был восстановлен в аудиоформат. Для низкокачественных аудиофайлов, требующих одного байта за значение, файл считался одним потоком, а затем зашифровывался и восстанавливался в аудиоформат.

Мы построили звуковые значения для разных файлов, чтобы наблюдать за эффектом шифрования. На рис. 1 и 2 показаны построенный образец аудио (Sample.wav) и его зашифрованный звук соответственно. Размер Sample.wav составляет 229 килобайт. При сравнении рис. 1 и 2 можно видеть, что зашифрованный звук не имеет сходства с оригиналом и не показывает никаких признаков, которые могут помочь атаке. Алгоритм дешифрования успешно восстановил исходный звук, воспроизведя звук на рис. 1. Эти наблюдения были одинаковыми для всех протестированных аудиофайлов.

Когда для каждого качества звука требовалось два или более байта, гистограммы зашифрованных файлов в этих случаях отличались от гистограмм исходных файлов. Они не дали никаких указаний, которые могут помочь в статистических атаках. Однако, когда для качества входного аудио требуется только один байт для каждого значения, гистограммы зашифрованных файлов были похожи на гистограммы исходного файла. Это связано с тем, что перестановка одного потока сохраняет свои значения неизменными, в отличие от случаев, которые разделяют значения в двух или более потоках и перетасовывают их отдельно. Следовательно, наш алгоритм не подходит для шифрования низкокачественных аудиофайлов, поскольку они будут уязвимы для статистических атак. В этом случае аудиофайл может быть зашифрован с использованием комбинации нашего алгоритма с другим алгоритмом шифрования, который изменяет звуковые значения.

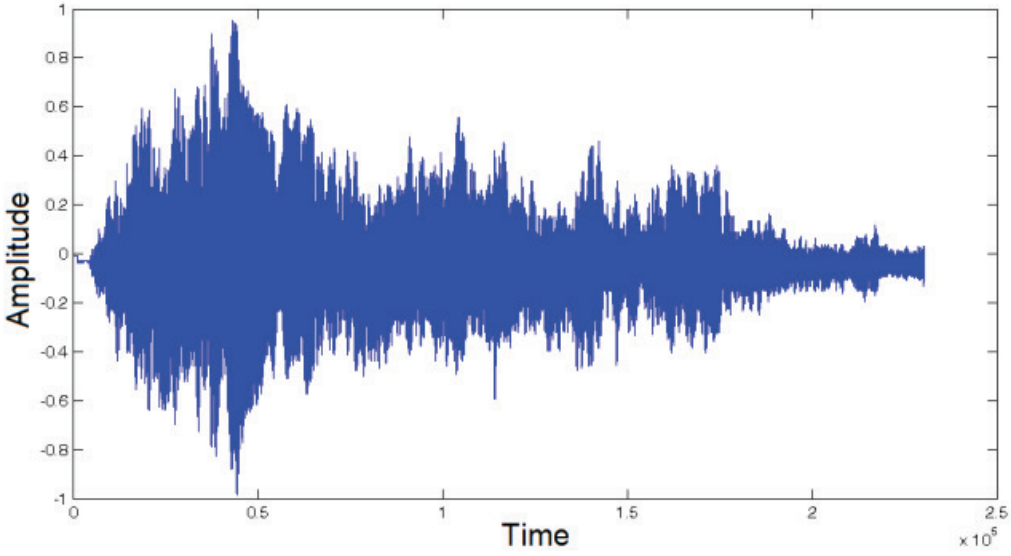

Рис. 1. Оригинал аудиофайла Sample.wav

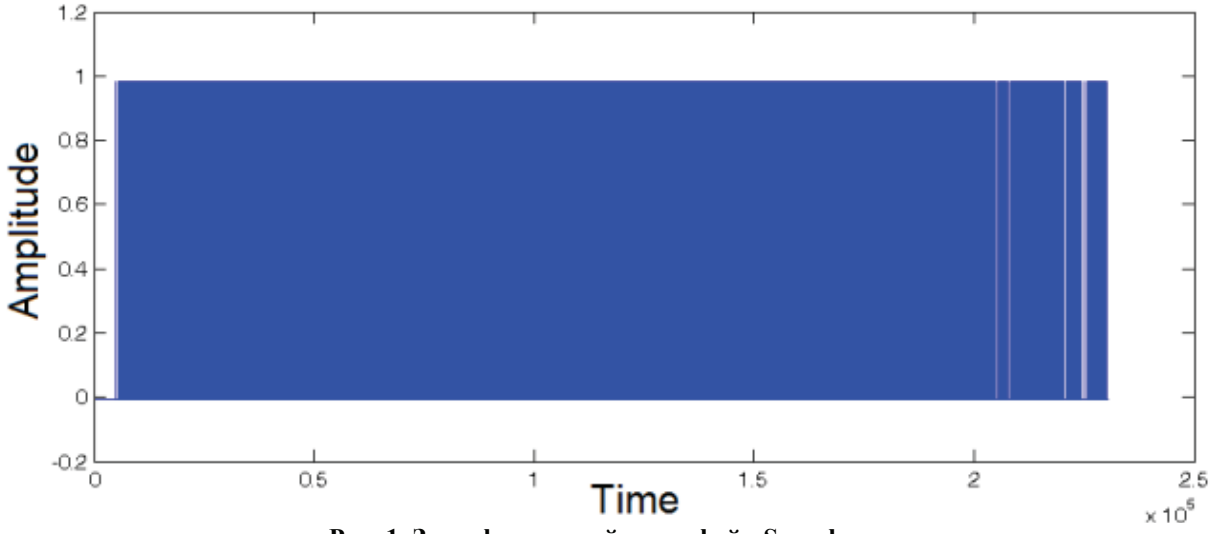

Рис. 1. Зашифрованный аудиофайл Sample.wav

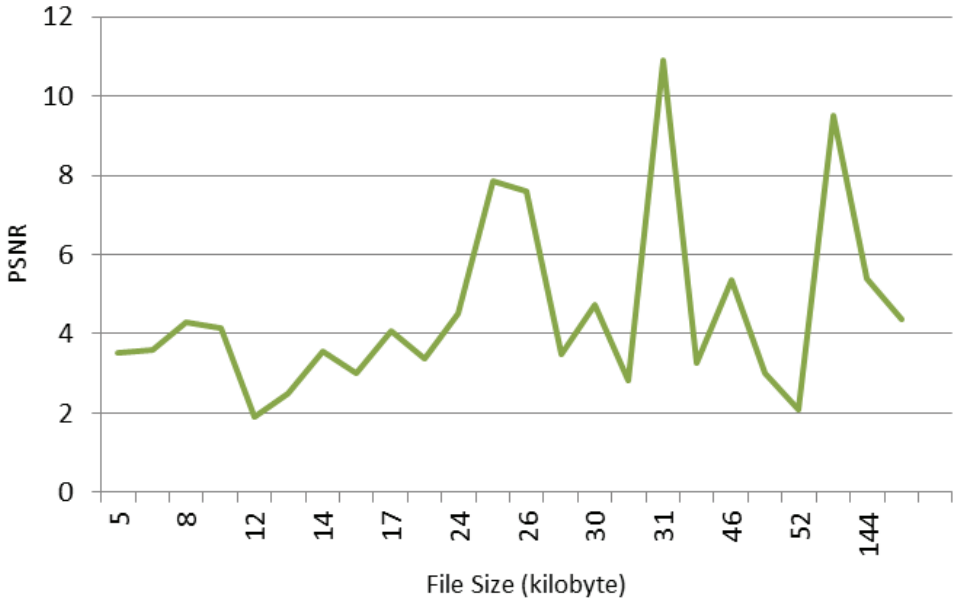

Рис. 3. PSNR зашифрованных аудиофайлов

Средняя квадратичная ошибка для двух потоков, хранящихся в векторах A и B, вычисляется следующим образом:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(A[i] - B[i])^2.$$

Если потоки A и B выше представляют собой оригинальный аудиофайл и его шифрование, тогда PSNR вычисляется как:

$$PSNR = 10\lg\left(\frac{MAX^2}{MSE}\right),$$

где MAX – максимальное значение в потоке. Для зашифрованных файлов требуется более низкое значение PSNR, так как оно указывает на большее сопротивление атакам. PSNR, полученный при шифровании Sample.wav, составлял 4,373 децибел (дБ). На рис. 3 показаны значения PSNR, рассчитанные для всех зашифрованных аудиофайлов, где среднее значение для этих значений составляло 4,536 дБ. Эти низкие значения PSNR указывают на высокий уровень шума в зашифрованных аудиофайлах, что делает их более устойчивыми к атакам.

Корреляция r между двумя аудиофайлами, хранящимися в векторах $\overline{A}$ и $\overline{B}$, вычисляется следующим образом, где A и B являются средними значениями для векторов $\overline{A}$ и $\overline{B}$ соответственно:

$$r = \frac{\sum_{i=1}^{n}(A[i] - \overline{A})(B[i] - \overline{B})}{\sqrt{\sum_{i=1}^{n}(A[i] - \overline{A})^2 \sum_{i=1}^{n}(B[i] - \overline{B})^2}},$$

Более низкое значение корреляции между звуковым файлом и его шифрованием указывает на меньшее сходство между ними, что обеспечивает большую устойчивость к атакам. Значение корреляции для Sample.wav было –0,0274. Значе-

ния корреляции для всех зашифрованных файлов показаны на рис. 4. Среднее значение корреляции, рассчитанное для абсолютных значений корреляции для зашифрованных файлов, связанных с их соответствующими оригиналами, было 0,0263.

Случайность значения может быть измерена энтропией. Энтропия вычисляется следующим образом:

$$H = -\sum_{i=1}^{MAX} (P(i)\log_2(P(i))),$$

где MAX – максимальное значение аудиоданных, а $P(i)$ – вероятность появления значения i. Высшая энтропия указывает на более высокую случайность и, следовательно, более высокую устойчивость к статистическим атакам. Энтропия для Sample.wav была 2,5932, а для ее зашифрованного файла 6,2214. Среднее значение энтропии для исходных аудиофайлов составляло 2,6498, где среднее значение энтропии для их зашифрованных файлов составляло 5,2338. Энтропия всех зашифрованных файлов и исходных файлов проиллюстрирована на рис. 5. Как видно на рисунке, шифрование вызвало заметное увеличение энтропии при шифровании файлов. Это указывает на увеличение случайности значений, что снижает риск атак.

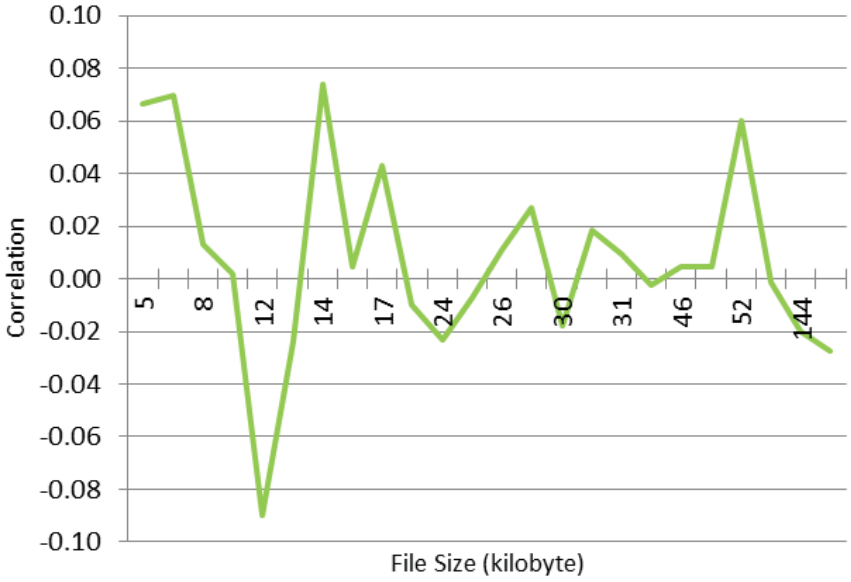

Рис. 4. Корреляция между исходными аудиофайлами и соответствующими зашифрованными файлами

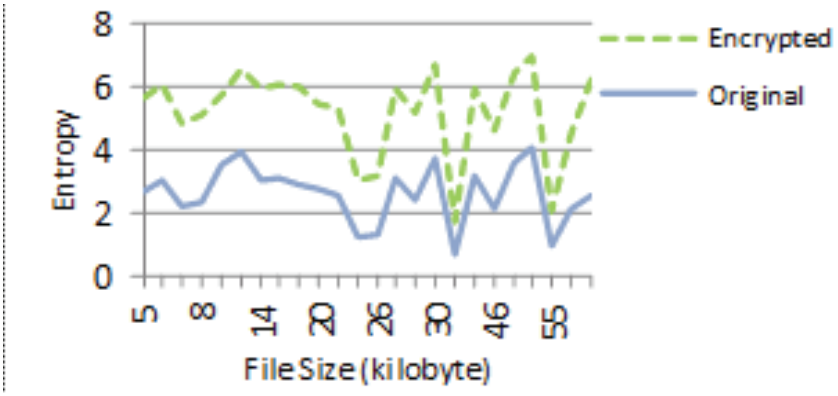

Рис. 5. Энтропия оригинальных и зашифрованных аудиофайлов

Заключение

В статье представлен новый алгоритм шифрования аудиофайлов. Предложенный алгоритм выполняет шифрование с использованием процедуры перестановки. Статистический анализ с использованием гистограмм, PSNR, корреляции и энтропии показал, что алгоритм не уязвим для статистических атак, если он не используется для шифрования низкокачественных аудиофайлов. Кроме того, огромное количество возможных ключей делает атаку «в лоб» на алгоритм невозможной.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Advanced encryption standard (AES) (FIPS 197). [Electronic resource]. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. (access date: 12.03.2017).
2. Кузьмин О.В., Оркина К.П. Построение кодов, исправляющих ошибки, с помощью треугольника типа Паскаля // Вестн. Бурят. гос. ун-та. 2006. № 13. С. 32–39.
3. McDevitt T., Leap T. “Multimedia cryp-tology,” Cryptologia (Taylor & Francis). 2009. vol. 33. no. 2, Pp. 142–150.
4. Кузьмин О.В., Старков Б.А. Фрактальные свойства бинарных матриц, построенных при помощи арифметики треугольника Паскаля, и помехоустойчивое кодирование // Современные технологии. Системный анализ. Моделирование. 2016. № 4 (52). С. 138–142.
5. Gnanajeyaraman R., Prasadh K. “Audio encryption using higher dimensional chaotic map,” Int. J. Recent Trends Eng., no. Academy Publ. 2009. vol. 1. no. 2. P. 103–107.
6. Tamimi A., Abdalla A., “A double-shuffle image-encryption algorithm,” in The 2012 Int. Conf. Image Processing, Computer Vision, and Pattern Recognition (IPCV '12). Las Vegas, NV, USA. 16-19 July 2012. Printed in Image Processing, Computer Vision, and Pattern Recognition, CSREA Press, 2012. P. 496–499.
7. Кузьмин О.В., Старков Б.А. Бинарные матрицы, построенные при помощи треугольника Паскаля, и помехоустойчивое кодирование // Современные технологии. Системный анализ. Моделирование. 2016. № 1 (49). С. 112–117.
8. Yahya A., Abdalla A. “An AES-based encryption algorithm with shuffling,” in The 2009 Int. Conf. Security & Management (SAM '09), Las Vegas, NV, USA. 13-16 July 2009. Printed in Security and Management, CSREA Press, 2009. P. 113–116.
9. Rahman Md. M., Saha T. K., Bhuiyan Md. A.-A. “Implementation of RSA algorithm for speech data encryption and decryption,” Int. J. Comput. Sc. & Netw. Secur., 2012. vol. 12, no. 3, P. 74–82.
10. Sharma D. “Five level cryptography in speech processing using multi hash and repositioning of speech elements,” Int. J. Emerging Technol. and Adv. Eng., 2012. vol. 2, no. 5, P. 21–26.
11. Sharma S., Kumar L., Sharma H. “Encryption of an audio file on lower frequency band for secure communica-tion,” Int. J. Adv. Res. Comput. Sc. & Software Eng., 2013. 3, no. 7, P. 79–84.
12. Gadanayak B., Pradhan C., Dey U. C. “Comparative study of different encryption techniques on MP3 compression,” Int. J. Comput. Appl., 2011. vol. 26, no. 3. P. 28–31.
13. A. Yahya and A. Abdalla. “A shuffle encryption algorithm using Sbox,” J. Comp. Sci. (Science Publications), 2008. vol. 4, no. 12, P. 999–1002.
14. Зеленцов И. А. Псевдослучайные последовательности и кодирование информации // Вопросы естествознания. 2017. № 2 (14). С. 30–37.
15. Кузьмин О.В. Старков Б.А. Бинарные матрицы с арифметикой треугольника Паскаля и символьные последовательности // Изв. Иркут. гос. ун-та. Сер.: Математика. 2016. Т. 18. С. 38–47.
16. Конин В.В., Юрчук А.А., Шутко В.Н. Формирование псевдослучайного кода сигнала E5 спутниковой радионавигационной системы GALILEO // Радиотехника. 2011. Вып. 167. С. 148–152.
17. Кузьмин О.В., Тимошенко А.А. Анализ алгоритмов декодирования стандарта радиосвязи MIL-STD-186-141B // Вестн. ИрГТУ. 2015. № 2 (97). С. 188–192.
18. Кузьмин О.В. Введение в перечислительную комбинаторику. Иркутск : Изд-во Иркут. гос. ун-та, 1995. 112 с.
19. Кофман А. Введение в прикладную комбинаторику. М. : Наука, 1975. 480 с.
20. Рейнгольд Э., Нивергельт Ю., Део Н. Комбинаторные алгоритмы: теория и практика. М. : Мир, 1980. 478 с.

REFERENCES

1. Advanced encryption standard (AES) (FIPS 197). [Electronic resource]. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. (access date: 12.03.2017).
2. Kuz'min O.V., Orkina K.P. Postroenie kodov, ispravlyayushchikh oshibki, s pomoshch'yu treugol'nika tipa Paskalya [Construction of codes correcting errors using a triangle of Pascal type]. *Vestn. Buryat. gos. un-ta* [*The Buryat State University Bulletin*], 2006, No. 13, pp. 32–39.
3. McDevitt T., Leap T. Multimedia cryptology. Cryptologia (Taylor & Francis), 2009, Vol. 33, No. 2, pp. 142–150.
4. Kuz'min O.V., Starkov B.A. Fraktal'nye svoistva binarnykh matrits, postroennykh pri pomoshchi arifmetiki treugol'nika Paskalya, i pomekhoustoichivoe kodirovanie [Fractal properties of binary matrices constructed using Pascal's triangle arithmetic, and noise-immune coding]. *Sovremennye tekhnologii. Sistemnyi analiz. Modelirovanie* [*Modern Technologies. System Analysis. Modeling*], 2016, No. 4 (52), pp. 138–142.
5. Gnanajeyaraman R., Prasadh K. Audio encryption using higher dimensional chaotic map. *Int. J. Recent Trends Eng.*, no. Academy Publ. 2009, Vol. 1, No. 2, pp. 103–107.
6. Tamimi A., Abdalla A. A double-shuffle image-encryption algorithm. *The 2012 Int. Conf. Image Processing, Computer Vision, and Pattern Recognition (IPCV '12). Las Vegas, NV, USA. 16-19 July 2012*. Printed in Image Processing, Computer Vision, and Pat-tern Recognition, CSREA Press, 2012, pp. 496–499.
7. Kuz'min O.V., Starkov B.A. Binarnye matritsy, postroennye pri pomoshchi treugol'nika Paskalya, i pomekhoustoichivoe kodirovanie [Binary matrices constructed using the Pascal triangle, and noise-resistant encoding]. *Sovremennye tekhnologii. Sistemnyi analiz. Modelirovanie* [*Modern Technologies. System Analysis. Modeling*], 2016, No. 1 (49), pp. 112–117.
8. Yahya A., Abdalla A. An AES-based encryption algorithm with shuffling. *The 2009 Int. Conf. Security & Management (SAM '09), Las Vegas, NV, USA. 13-16 July 2009*. Printed in Security and Management, CSREA Press, 2009, pp. 113–116.
9. Rahman Md. M., Saha T. K., Bhuiyan Md. A.-A. Implementation of RSA algorithm for speech data encryption and decryption. *Int. J. Comput. Sc. & Netw. Secur.,* 2012, Vol. 12, No. 3, pp. 74–82.
10. Sharma D. Five level cryptography in speech processing using multi hash and repositioning of speech elements. *Int. J. Emerging Technol. and Adv. Eng*., 2012, Vol. 2, No. 5, pp. 21–26.

11. Sharma S., Kumar L., Sharma H. Encryption of an audio file on lower frequency band for secure communication. *Int. J. Adv. Res. Comput. Sc. & Software Eng.*, 2013, 3, No. 7, pp. 79–84.
12. Gadanayak B., Pradhan C., Dey U. C. Comparative study of different encryption techniques on MP3 compression. *Int. J. Comput. Appl.*, 2011, Vol. 26, No. 3, pp. 28–31.
13. Yahya A., Abdalla A. A shuffle encryption algorithm using Sbox, *J. Comp. Sci.* (Science Publications), 2008, Vol. 4, No. 12, pp. 999–1002.
14. Zelentsov I. A. Psevdosluchainye posledovatel'nosti i kodirovanie informatsii [Pseudo-random sequences and information coding]. *Voprosy estestvoznaniya* [*Issues of Natural Science*], 2017, No. 2 (14), pp. 30–37.
15. Kuz'min O.V. Starkov B.A. Binarnye matritsy s arifmetikoi treugol'nika Paskalya i simvol'nye posledovatel'nosti [Binary matrices with arithmetic of Pascal's triangle and symbol sequences]. *Izv. Irkut. gos. un-ta. Ser.: Matematika* [*The Bulletin of Irkutsk State University. Series "Mathematics"*], 2016, Vol. 18, pp. 38–47.
16. Konin V.V., Yurchuk A.A., Shutko V.N. Formirovanie psevdosluchainogo koda signala E5 sputnikovoi radionavigatsionnoi sistemy GALILEO [Formation of the pseudo-random code of the E5 signal of the satellite radio navigation system GALILEO]. *Radiotekhnika* [], 2011, Issue 167, pp. 148–152.
17. Kuz'min O.V., Timoshenko A.A. Analiz algoritmov dekodirovaniya standarta radiosvyazi MIL-STD-186-141B [Analysis of decoding algorithms for the radio communication standard MIL-STD-186-141B]. *Vestn. IrGTU* [*Proceedings of Irkutsk State Technical University*], 2015. No. 2 (97), pp. 188–192.
18. Kuz'min O.V. Vvedenie v perechislitel'nuyu kombinatoriku [Introduction to enumeration combinatorics]. Irkutsk: Irkut. state un-ty Publ., 1995, 112 p.
19. Kofman A. Vvedenie v prikladnuyu kombinatoriku [Introduction to applied combinatorics]. Moscow: Nauka Publ., 1975, 480 p.
20. Reingol'd E., Nivergel't Yu., Deo N. Kombinatornye algoritmy: teoriya i praktika [Combinatorial Algorithms: Theory and Practice]. Moscow: Mir Publ., 1980, 478 p.

Информация об авторах

Кузьмин Олег Владимирович - д. ф.-м. н., профессор, заведующий кафедрой теории вероятностей и дискретной математики, Институт математики, экономики и информатики, Иркутский государственный университет, г. Иркутск, e-mail: quzminov@mail.ru

Зеленцов Илья Анатольевич - магистрант ИМЭИ, Иркутский государственный университет, г. Иркутск, e-mail: izelentsov.isu@gmail.com.

Authors

Oleg Vladimirovich Kuz'min – Dr. Sci. in Physics and Mathematics, Prof., Head of the Subdepartment of Probability and Discrete Mathematics, Institute of Mathematics, Economics and Informatics, Irkutsk State University, Irkutsk, e-mail: quzminov@mail.ru

Ilya Anatolyevich Zelentsov – Master's student of the Head of the Subdepartment of Probability and Discrete Mathematics, Irkutsk State University, Irkutsk, e-mail: izelentsov.isu@gmail.com

Для цитирования

Кузьмин О. В. Кодирование звуковой информации с помощью алгоритма перестановки / О. В. Кузьмин, И. А. Зеленцов // Современные технологии. Системный анализ. Моделирование. — 2017. — Т. 56, № 4. — С. 151–158. — DOI: 10.26731/1813-9108.2017.4(55).151-158.

For citation

Kuz'min O.V., Zelentsov I.A. Kodirovanie zvukovoi informatsii s pomoshch'yu algoritma perestanovki [Coding sound information with a permutation algorithm]. *Sovremennye tekhnologii. Sistemnyi analiz. Modelirovanie* [*Modern Technologies. System Analysis. Modeling*], 2017. Vol. 56, No. 4, pp. 151–158. DOI: 10.26731/1813-9108.2017.4(56).151-158.