Известия Гомельского государственного университета
имени Ф. Скорины, №2(41), 2007

УДК 621.391.25

Хаотический алгоритм защиты мультимедийных данных

А. А. Борискевич, А. А. Меркушов

Введение

Развитие телекоммуникационных и мультимедийных технологий способствует увеличению потоков информации и вызывает необходимость в создании новых алгоритмов защиты информации от несанкционированного доступа. Поиск новых технологий защиты обусловлен не стремлением увеличения криптостойкости традиционных схем шифрования, а необходимостью не зависеть от существующих стандартов и «нерешенных» математических проблем, которые могут перестать быть препятствием перед несанкционированным пользователем.

Одним из решений данной проблемы является использование алгоритмов хаотического шифрования [1, 2, 3]. Для повышения качества шифрования и расширения спектра защищаемой информации в данной работе предлагается хаотический алгоритм для защиты мультимедийных данных, основанный на использовании хаотических последовательностей, обладающих высокой чувствительностью к ключевой информации: начальному значению хаотической переменной и управляющему параметру.

Описание алгоритма

Данный алгоритм является эффективным средством для защиты аудио-, видео- и графических изображения данных. Сущность алгоритма состоит в поточном шифровании исходного полутонового изображения с использованием хаотического отображения. Исходное изображение $\{f(x,y)\}_{x=0,y=0}^{x=M-1,y=N-1}$ представляется в виде одномерной последовательности $\{f(l)\}_{l=0}^{MN-1}$, которая делится на $MN/16$ блоков (M, N – размеры изображения):

$\{f^{(16)}(0),\ldots,f^{(16)}(k),\ldots,f^{(16)}(MN/16-1)\}$, где $f^{(16)}(k)=\{f(16k+0),\ldots,f(16k+15)\}$ – k-й блок последовательности, $k=\overline{0,MN/16-1}$ – номер блока.

Суть алгоритма для k-го блока пикселей $f^{(16)}(k)$ заключается в следующем.

1) Выбор хаотического отображения $x(i+1)=F(\mu,x(0),x(i))$, где $x(i)$ – текущее значение хаотической переменной, $x(0)$ – начальное значение хаотической переменной, μ – значение управляющего параметра, F – тип хаотического отображения, и его ключевых параметров $x(0)$ и μ, используемых в качестве секретных ключей для всего исходного изображения

В данном алгоритме используется одно из наиболее известных отображений – логистическое отображение:

$$x(i+1)=\mu\cdot x(i)\cdot(1-x(i)). \qquad (1)$$

2) Формирование псевдослучайной бинарной последовательности $\{b(i)\}_{i=0}^{3MN/2-1}$ длиной $3MN/2$ из псевдослучайной последовательности $\{x(i)\}_{i=0}^{MN/16-1}$ посредством ее квантования в 24-х битные значения.

3) Вычисление 8-ми битных ключевых слов $Key1(k)$ и $Key2(k)$ для k-го блока пикселей

$$Key1(k)=\sum_{i=0}^{7}b(24k+i)\times 2^{7-i}, \qquad (2)$$

$$Key2(k) = \sum_{i=0}^{7} b(24k+8+i) \times 2^{7-i} . \quad (3)$$

4) Перестановка соседних пикселей k-го блока ($i = \overline{0,7}$ – номер перестановки) при выполнении условия $b(24k+16+i) = 1$:

$$Perm_{b(24k+16+i)}(f(16k+2i), f(16k+2i+1)) . \quad (4)$$

5) Выполнение *XOR* (или *XNOR)* между k-м блоком пикселей и ключевыми словами $Key1(k)$ и $Key2(k)$ для $j = \overline{0,15}$, где j – номер пикселя в k-м блоке:

$$f'(16k+j) = f(16k+j) \oplus Key(16k+j),$$

где

$$Key(16k+j) = \begin{cases} Key1(k), & B(k,j) = 3, \\ \overline{Key1(k)}, & B(k,j) = 2, \\ Key2(k), & B(k,j) = 1, \\ \overline{Key2(k)}, & B(k,j) = 0; \end{cases} \quad (5)$$

$B(k,j) = 2 \times b(24k+j) + b(24k+j+1)$ – параметр выбора ключевого слова.

4) Процедура расшифрования подобна шифрованию, но процедура *XOR* (или *XNOR)* выполняется до перестановки каждого блока пикселей.

Для повышения безопасности предложенного алгоритма параметры μ и $x(0)$ целесообразно обновлять при защищенной передаче мультимедийных данных. [4]

Алгоритм обновления параметров μ и $x(0)$ заключается в следующем.

1) Выбор начальных значений μ_0 и $x(0)_0$.

2) Шифрование начальных значений μ_0 и $x(0)_0$ посредством следующих выражений: $X_{enc,0} = x(0)_0 \oplus X_b$ и $\mu_{enc,0} = \mu_0 \oplus \mu_b$, где μ_b и X_b – встроенные аппаратные ключи в предлагаемой криптосистеме; $\mu_{enc,0}$ и $X_{enc,0}$ – ключи, используемые при шифровании медиаданных.

3) Передача зашифрованных $\mu_{enc,0}$ и $X_{enc,0}$ для восстановления исходных начальных значений μ_0 и $x(0)_0$ с помощью операции *XOR* : $\mu_0 = \mu_{enc,0} \oplus \mu_b$ и $x(0)_0 = X_{enc,0} \oplus X_b$.

4) Итерационное обновление секретных параметров μ и $x(0)$ и их восстановление осуществляется соответственно с помощью следующих соотношений:

$\mu_{enc,p} = \mu_p \oplus \mu_{p-1}$,

$$X_{enc,p} = x(0)_p \oplus x(0)_{p-1}, \text{ и}$$

$$\mu_p = \mu_{enc,p} \oplus \mu_{p-1},$$

$$x(0)_p = X_{enc,p} \oplus x(0)_{p-1},$$

где p – номер шага итерации обновления.

Частота обновления параметров μ и $x(0)$ зависит от особенностей структуры видео- и аудио- потоков в мультимедийных данных.

Анализ криптостойкости и вычислительной сложности алгоритма

Так как сигнал длины N разбивается на $\lceil N/16 \rceil$ блоков и каждый блок требует 24 служебных бита из бинарной хаотической последовательности $\{b(i)\}_{i=0}^{3MN/2-1}$, то в итоге требуется $\lceil N/16 \rceil \times 24$ бит для шифрования сигнала. Следовательно, число возможных результатов шифрования равно $2^{\lceil N/16 \rceil \times 24}$. Например, для изображения размером 256x256 пикселей (N = 65536) число возможных шифрограмм равно 2^{98304} (или $\cong 10^{29590}$). Однако криптостойкость

данного алгоритма определяется выбором разрядности параметров μ и $x(0)$. Поскольку алгоритм оперирует 24-х разрядными числами, а секретный ключ состоит из двух параметров μ и $x(0)$, то разрядность секретного ключа составляет 48 бит.

Для получения значения логистического отображения требуется одно вычитание и два умножения, а полное число итераций равно $N/16$. Следовательно, общее количество вычитаний и умножений для логического отображения соответственно равно $N/16$ и $N/8$. Так как для хаотических последовательностей вероятности $P(b(k)=1)=P(b(k)=0)=1/2$, то число перестановок 8-ми бит в памяти равно $N/4$. Кроме того, число операций XOR (XNOR) равно N. Число различных видов операций над сигналом длины N представлено в таблице 1. Из таблицы видно, что число операций умножения, перестановки, логических операций XOR/XNOR, и операций сложения/вычитания составит $38N/16$, N, $N/4$, и $110N/16$ соответственно. Следовательно, вычислительная сложность алгоритма равна $O(N)$.

Таблица 1

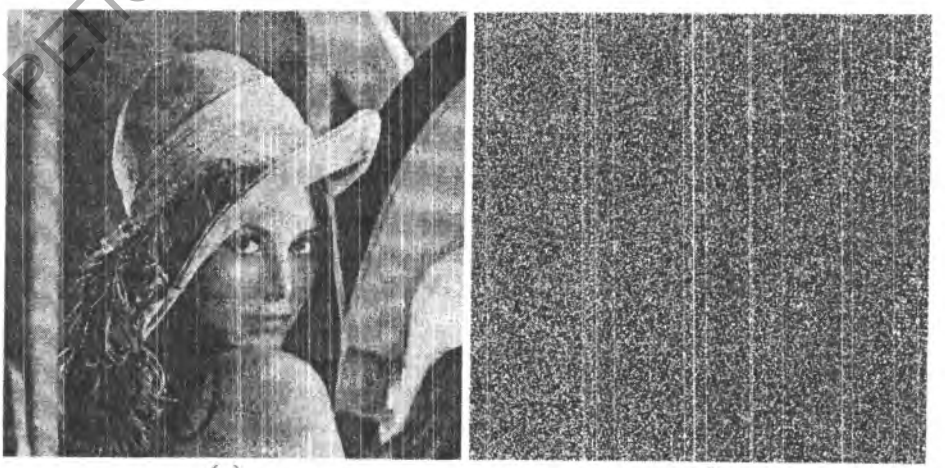
Операция	УМН_1	УМН_2	XOR и XNOR	Перестановки	Сложение и вычитание
Операция (1)	N/8	0	0	0	N/16
Операция (2)	N/16	7N/16	0	0	14N/16
Операция (3)	0	7N/16	0	0	14N/16
Операция (4)	0	5N/16	0	N/4	17N/16
Операция (5)	0	N	N	0	4N
Итого	3N/16	35N/16	N	N/4	110N/16

УМН_1 обозначает умножение двух чисел с плавающей запятой, а УМН_2 – умножение числа с плавающей запятой на число степени 2.

Результаты моделирование алгоритма в среде Matlab

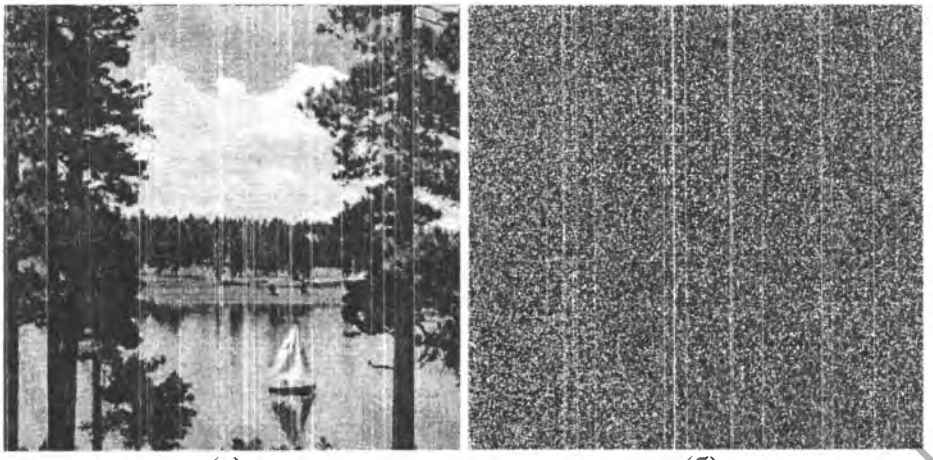
Для оценки эффективности разработанного алгоритма были взяты 8 стандартных тестовых изображений размером 512x512 пикселей [5]. На рисунке 1 и 2 представлены два тестовых изображения "Lena" и "Sailboat" и результаты их шифрования.

Из рисунка 1 и 2 видно, что в зашифрованных изображениях отсутствуют следы исходного изображения. Для уменьшения субъективности оценки качества шифрования целесообразно использовать количественные оценки. В связи с этим в качестве количественных критериев качества шифрования используются энтропия изображения и одна из оценок гистограммы изображения.



(а) (б)

Рисунок 1 – Исходное (а) и зашифрованное (б) изображение "Lena".



(а) (б)

Рисунок 2 – Исходное (а) и зашифрованное (б) изображение "Sailboat".

В таблице 2 приведены значения энтропии интенсивности пикселей для 8-ми тестовых изображений. Оценка энтропии изображения вычисляется из гистограммы с помощью следующего соотношения:

$$H = -\sum_{k=0}^{2^n-1} p(k)\log_2(p(k)),$$

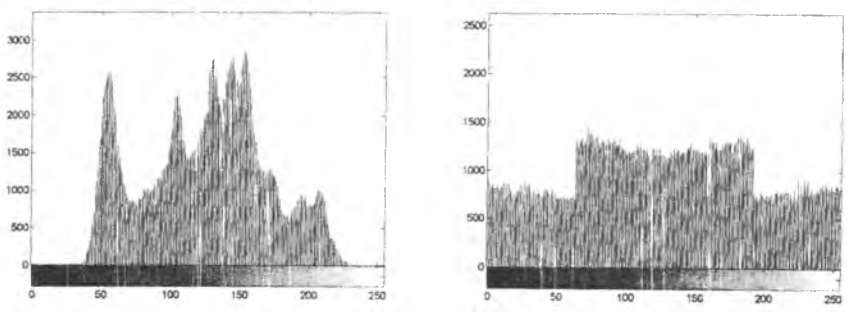
где $p(k) = h(k)/MN$ – вероятность появления k-го значения уровня серого в изображении размера MN; $h(k)$ – количество пикселей с k-м значением уровня серого; n – число бит на пиксель в изображении.

Таблица 2

Изображение	Lena	Sailboat	Peppers	Cman	Baboon	Jet	Gray21	Testpat
Исходное	7.3478	7.3918	7.5062	7.1226	7.3154	6.7170	4.3922	5.3631
Зашифрованное	7.9592	7.9960	7.9569	7.9788	7.9226	7.9823	7.9824	7.9663

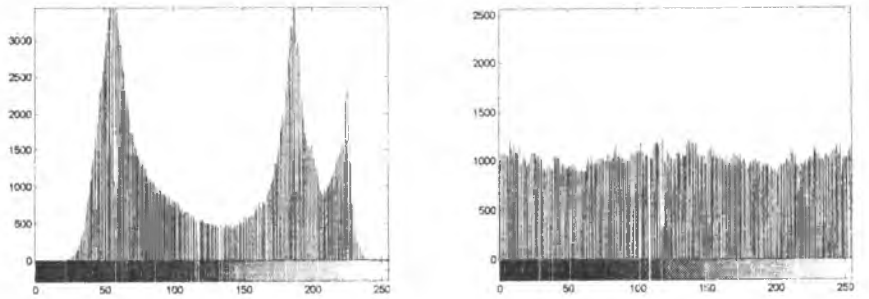
Из таблицы 2 видно, что энтропия зашифрованных изображений близка к своему максимальному значению – 8. Это означает, что появление любого значения из множества уровней серого 2^n равновероятно, т.е. изображение близко к хаотическому.

На рисунке 3 и 4 представлены гистограммы исходного и зашифрованного изображений, представляющие собой графики распределения значения уровней серого в изображениях, по горизонтальной оси которых представлена яркость, а по вертикали – число пикселей с данным значением яркости. Данная характеристика дает общее представление о степени хаотичности изображения. Для случайного изображения количество пикселей с различным значением яркости должно быть приблизительно одинаковым.



(а) (б)

Рисунок 3 – Гистограмма исходного (а) и зашифрованного (б) изображения "Lena".



(а) (б)

Рисунок 4 – Гистограмма исходного (а) и зашифрованного (б) изображения "Sailboat".

Для количественной оценки степени равномерности гистограммы используется отношение среднего геометрического к среднему арифметическому: G/A, где $A(x_1,\ldots,x_n) = x_1 + \ldots + x_n/n$ – среднее арифметическое n чисел; $G(x_1,\ldots,x_n) = (x_1 \cdot \ldots \cdot x_n)^{1/n}$ – среднее геометрическое n чисел.

В таблице 3 приведены значения отношения G/A для 8-ми тестовых изображений.

Таблица 3

Изображение	Lena	Sailboat	Peppers	Cman	Baboon	Jet	Gray21	Testpat
Исходное	0.1993	0.3417	0.4418	0.4280	0.2535	0.1687	0.0021	0.2329
Зашифрованное	0.9715	0.9973	0.9699	0.9853	0.9457	0.9881	0.9879	0.9785

Из таблицы 3 видно, что выбранное отношение для зашифрованных изображений близко к своему максимальному значению – 1. Это означает, что гистограмма зашифрованного изображения близка к равномерной, т.е. изображение близко к хаотическому.

Для оценки чувствительности результатов шифрования к изменению начального значения $x(0)$ и управляющего параметра μ используется среднеквадратичное расстояние (RMSD):

$$RMSD = \left(\frac{1}{L \times P} \sum_{i=0}^{L-1} \sum_{j=0}^{P-1} (f'_{\mu_1 x_1(0)}(i,j) - f'_{\mu_2 x_2(0)}(i,j))^2 \right),$$

где $f'_{\mu_1 x_1(0)}$ – значение яркости пикселей зашифрованного изображения размера MN пикселей при μ_1 и $x_1(0)$; $f'_{\mu_2 x_2(0)}$ – значение яркости пикселей зашифрованного изображения размера MN пикселей при μ_2 и $x_2(0)$.

Значения RMSD для оценки результатов шифрования при фиксированном $x(0) = 0,25$ и изменяющимся μ с шагом 10^{-5} представлено в таблице 4, а значения RMSD при фиксированном $\mu = 3,92$ и изменяющимся $x(0)$ с шагом 10^{-5} – в таблице 5.

Таблица 4

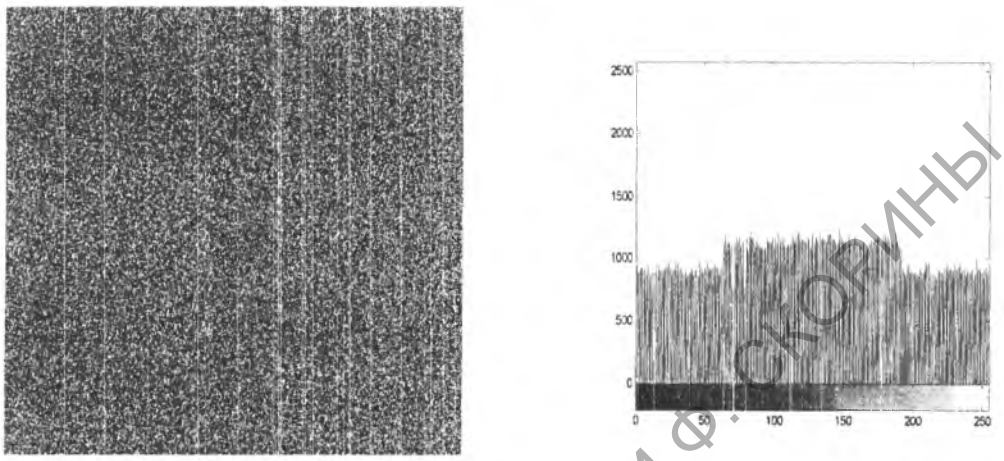
μ_1	3.92000	3.92001	3.92002	3.92003	3.92004	3.92005	3.92006	3.92007	3.92008	3.92009
μ_2	3.92001	3.92002	3.92003	3.92004	3.92005	3.92006	3.92007	3.92008	3.92009	3.92010
RMSD	111.083	112.506	113.531	112.286	112.917	113.800	113.534	112.624	111.505	110.853

Таблица 5

$x(0)_1$	0.25000	0.25001	0.25002	0.25003	0.25004	0.25005	0.25006	0.25007	0.25008	0.25009
$x(0)_2$	0.25001	0.25002	0.25003	0.25004	0.25005	0.25006	0.25007	0.25008	0.25009	0.25010
RMSD	112.104	112.520	111.990	113.182	112.843	114.098	114.993	112.637	113.055	114.309

Из таблиц 4 и 5 видно, что среднеквадратичное расстояние между результатами шифрования при очень маленьких колебаниях 10^{-5} в μ или $x(0)$ равно приблизительно 110, что соответствует половине динамического диапазона яркости полутонового изображения. Следовательно, результат шифрования очень чувствителен к колебанию в μ и $x(0)$.

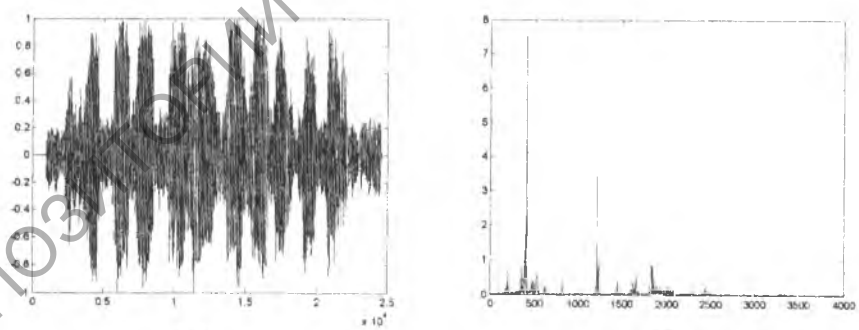
Повторное шифрование зашифрованного изображения с измененными секретными ключами улучшает качество шифрования по критерию степени равномерности гистограммы (рисунок 5).



(а) (б)

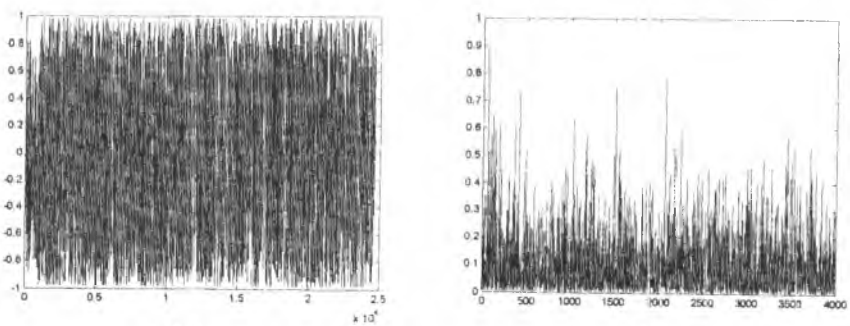
Рисунок 5 – Повторно зашифрованное изображение "Lena" (а) и его гистограмма (б).

Одной из составляющих мультимедийной информации является аудиосигнал. На рисунке 6 и 7 представлены исходный и зашифрованный речевые сигналы фразы "Я требую продолжения банкета" с частотой дискретизации 8000 Гц, 8 бит на отсчет, длительностью 3 с и их спектр мощности.



(а) (б)

Рисунок 6 – Исходный звуковой файл (а) и его спектр мощности (б).



(а) (б)

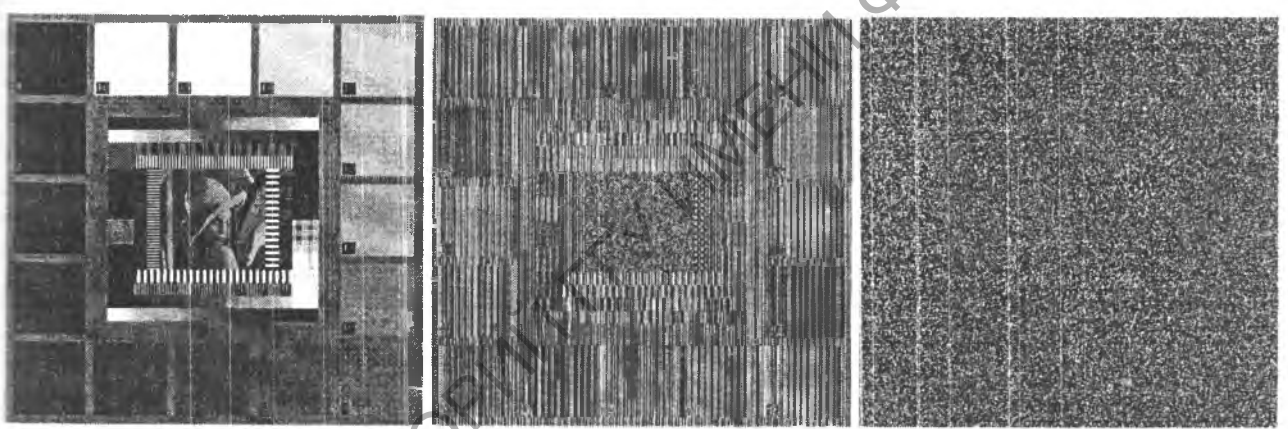
Рисунок 7 – Зашифрованный звуковой файл (а) и его спектр мощности (б).

Из характера изменения спектра мощности (рисунок 6,б и 7,б) видно, что разработанный алгоритм эффективен также для защиты аудио сигналов.

Предложенный алгоритм не только не уступает существующим классическим алгоритмам шифрования (DES, 3DES. AES), но и превосходит их по качеству шифрования медиаданных. На рисунке 8 представлены результаты шифрования тестового изображения "Testpat" разработанным алгоритмом и блочным криптоалгоритмом AES.

Заключение

Разработан эффективный алгоритм хаотического шифрования мультимедийных данных, основанный на использовании хаотических последовательностей, обладающих высокой чувствительностью к ключевой информации (начальному значению хаотической переменной и управляющему параметру) для выполнения операции хаотических перестановок и преобразований значений медиаданных. Данный алгоритм обладает высокой криптостойкостью и низкой вычислительной сложностью. Моделирование разработанного алгоритма в среде MATLAB показывает, что результаты шифрования изображений и аудиосигналов являются хаотическими по следующим критериям: энтропия, отношение среднего геометрического к среднему арифметическому гистограммы изображения и спектр мощности. Результаты сравнительного анализа разработанного алгоритма и AES показывают, что предложенный алгоритм превосходит его по качеству шифрования медиаданных.



(а) (б) (в)

Рисунок 8 – Исходное (а), зашифрованное шифром AES (128 бит) (б) и зашифрованное хаотическим алгоритмом (в) изображение "Testpat".

Abstract. An effective chaotic enciphering algorithm of the multimedia data based on the chaotic sequences is presented in the paper. The algorithm performs both random position permutation and random value transformation under the control of a binary sequence obtained from a chaotic map. The algorithm possesses high security and low computational complexity.

Литература

1. Борискевич А.А., Шакиров М.Р. Шифрование изображений методом перестановки на основе модели динамического хаоса // Вопросы информационной безопасности. Минск, ОИПИ НАНБ. – 2002. – Вып.1, С. 95-103.

2. Борискевич А.А., Шакиров М.Р. Шифрование сообщений на основе модели динамического хаоса // Сб. науч. трудов «Комплексная защита информации», ИТК НАНБ. – 2000. – Вып. 3, С. 108–117.

3. S. Li, G. Chen, and X. Zheng. Chaos-based encryption for digital images and videos. – Multimedia Security Handbook, B. Furht and D. Kirovski, Eds. CRC Press, LLC, April 2004.

4. H.-C. Chen and J.-C. Yen. A new cryptography system and its VLSI realization // J. Systems Architecture. – 2003. – Vol. 49. – P. 355–367.

5. Set of test images. Signal and Image Processing Institute of the University of Southern California, http://sipi.usc.edu/.

Белорусский государственный университет
информатики и радиоэлектроники

Поступило 16.08.06