3. Беззубцева М.М., Ружьев В.А. Формирование компетентности менеджера магистрантов-агроинженеров // Международный журнал прикладных и фундаментальных исследований. – 2014. – № 4. С. 179-180.

4. Беззубцева М.М., Волков В.С. Рекомендации по проектированию электромагнитных механоактиваторов // Международный журнал экспериментального образования. 2014. № 5-2. С. 128-129.

5. Беззубцева М.М., Волков В.С., Прибытков П.С. Расчет электромагнитного механоактиватора с применением программного комплекса ANSYS // Известия Санкт-Петербургского государственного аграрного университета. – 2009. – №15. – С. 150-153.

6. Беззубцева М.М., Волков В.С. Моделирование процесса электромагнитной механоактивации в среде программного комплекса ANSYS // Научное обеспечение развития АПК в условиях реформирования. – СПб.: СПбГАУ, 2011. – С. 378-379.

7. Беззубцева М.М., Волков В.С. Компьютерное моделирование процесса электромагнитной механоактивации в дисковом электромагнитном механоактиваторе (ЭДМА) в программном комплексе ANSYS // Международный журнал экспериментального образования. – 2013. – №11. Ч.1. – С. 151-153.

8. Беззубцева М.М., Прибытков П.С. Расчет электромагнитного механоактиватора с применением программного комплекса ANSYS.В сборнике: Научное обеспечение развития АПК в условиях реформирования Пастернак П.П. сборник научных трудов: материалы научной конференции профессорско-преподавательского состава, научных сотрудников и аспирантов СПбГАУ. Министерство сельского хозяйства Российской Федерации, Санкт-Петербургский государственный аграрный университет; редкол.: П.П. Пастернак и др. 2009. С. 245-246.

«Проблемы передачи и обработки информации» ОАЭ (Дубай), 16-23 октября 2014 г.

Физико-математические науки

КОДИРОВАНИЕ ИНФОРМАЦИИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЧИСЕЛ

Когай Г.Д., Тен Т.Л.

КарГТУ «Карагандинский государственный технический университет», Караганда, e-mail: tentl@mail.ru

На данный момент в мире существует множество алгоритмов, обеспечивающих различные уровни криптографической стойкости, основанные на различных принципах защиты, от применения секретных алгоритмов (морально устаревшие методы), до использования математических методов, основанных на вычислительной сложности. Одно из современных перспективных направлений криптографической защиты информации в распределенных компьютерных сетях есть применение алгоритмов, основанных на поведенческих свойствах нелинейных динамических систем, так называемых «детерминированном хаосе».

Цель. Исследовать и разработать криптографический алгоритм на основе отображения нелинейной динамической системы для шифрования графической информации. Провести исследования данного криптографического алгоритма по всем необходимым параметрам.

Описание алгоритма

При шифровании в основном исследуются телекоммуникационные технологии, основанные на использовании различных способов кодирования матриц. Наряду с использованием сложных регулярных закономерностей для кодирования матриц рассматривалась возможность применения нерегулярных процессов [1]. При этом для перестановки элементов матрицы использован стандартный генератор псевдослучайных чисел.

Наряду с тем, что при применении модели матрицы возможно восстановление потерь «голографическим» методом, в принципе, при перестановке элементов матрицы возможно и вскрытие шифра, хотя в ряде случаев это – очень сложно. В то же время с помощью псевдослучайных генераторов можно получать довольно стойкие криптосистемы, если осуществлять не перестановку элементов матрицы, а изменение цвета элементов, формирующих изображение. При этом в качестве генераторов псевдослучайных сигналов, как представляется, весьма подходят генераторы с хаотической динамикой, и особенно искусственно сконструированные. Они предпочтительнее тем, что хаос, описываемый их уравнениями (при относительной простоте записи) может быть более развитым.

Рассматривается новый способ шифрования информации, основанный на хаотическом изменении цвета символов, формирующих изображение. Для генерирования псевдослучайной последовательности чисел используется одномерное отображение [2,3]. Особенностью системы, обладающей хаотической динамикой является высокая чувствительность к изменению параметров. Именно это затрудняет несанкционированное дешифрование при использовании для кодирования информации детерминированного хаоса.

Использование хаотических решений рассмотренного отображения позволяет создать достаточно сложный шифр, который не поддается раскрытию, если не воспроизведены точные значения начальных условий и параметров динамической системы, при которых выполнялось ее решение.

Подмешивание псевдослучайной последовательности чисел, получаемой на основе решения хаотического отображения, целесообразно осуществлять так, чтобы происходило хаотическое изменение их палитры цвета. Это является основой разработанной программы, обеспечивающей шифрование и дешифрование с использованием системы с хаотической динамикой.

Преобразование графической матрицы осуществляется путем присвоения каждому символу, формирующему изображение, нового цвета в соответствии не только с хаотическими решениями рассматриваемого отображения, но и с его исходной палитрой цвета. В этом случае выполняется условие, при котором индекс нового цвета пикселя равен исходному индексу цвета пикселя плюс дополнительный индекс цвета пикселя, определяемый решением хаотического

отображения. При этом каждый символ графической матрицы последовательно преобразуется в одном и том же стековом блоке памяти. При дешифровании используется аналогичный алгоритм преобразований. Отличие заключается лишь в том, что при формировании палитры цвета осуществляется вычитание псевдослучайной последовательности чисел, формируемых на основе решений тех уравнений, которые использовались при шифровании.

Таким образом, алгоритм шифрования графического объекта будет состоять из следующих шагов:

1) Сопоставление пикселю графического изображения трех координат *r, g, b* (эти числа составляют RGB-код пикселя);

2) Задание начальных условий (параметров) динамической системы;

3) На основе решения нелинейного отображения с хаотической динамикой – генерация последовательности значений псевдослучайных чисел *h*;

4) Определение индексов нового цвета пикселя

$$I_{r'} = I_r + I_h ,$$

$$I_{g'} = I_g + I_h ,$$

$$I_{b'} = I_b + I_h ;$$

5) Получение нового (абсолютно другого) цвета пикселя;

6) Выполнение шагов 1-5 для всех элементов многоцветной матрицы.

Как уже говорилось выше, для дешифрования используется аналогичный алгоритм преобразований:

1) Получение трех координат r’, g’, b’ пикселя зашифрованного графического изображения;

2) Задание начальных условий (параметров) динамической системы;

3) Восстановление последовательности значений псевдослучайных чисел h по известным значениям управляющих параметров;

4) Восстановление значений индексов первоначального цвета пикселя

$$I_r = I_{r'} - I_h ,$$

$$I_g = I_{g'} - I_h ,$$

$$I_b = I_{b'} - I_h ;$$

5) Формирование RGB-код пикселя, т.е. восстановление его первоначального цвета;

6) Выполнение шагов 1-5 для всех элементов многоцветной матрицы.

Для иллюстрации процессов шифрования и дешифрования использовалась цветная матрица 24 бита в виде графического изображения (рис. 1).

Рис. 1. Исходный графический объект

Хотя изображение на рис. 1 является цветным, оно распечатано на принтере как черно-белое. Поэтому изменение цвета пикселей на этом рисунке отображается тональностью серого. Изображение, представленное на рис. 1 после процедуры преобразования в зашифрованной матрице принимает вид, иллюстрируемый на рис. 2. Зашифрованное изображение отображает хорошее (хаотическое) перемешивание цветов (в представленном виде – тональности серого) пикселей, так что исходная информация надежно замаскирована.

При шифровании в случае (рис. 2а) в нелинейном отображении с хаотической динамикой при T=0,8 заданы (для примера) следующие значения варьируемых параметров: a=1,12345671234567, g=1,3. При санкционированном дешифровании (рис. 2а), когда параметры a, g,T введены с абсолютной точностью, исходный графический объект, показанный на рис. 1 воспроизводится без изменения.

а) *б)*

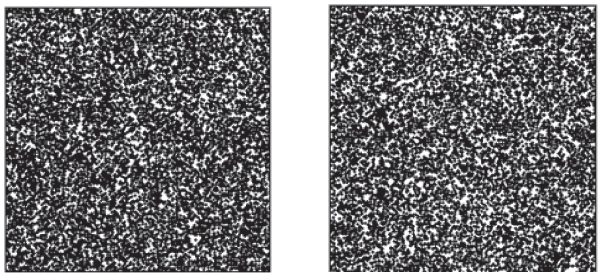

Рис. 2:
а – изображение рисунка 1 в зашифрованном виде; б – изображение рисунка 1 при неправильном дешифровании

В случае малейших ошибок хотя бы по одному параметру (например, при несанкционированном входе) дешифрование оказывается невозможным, т.к. в результате будет получено изображение, не соответствующее реальному (исходному). Даже при ошибке в определении одного из параметров, составляющей 10^{-15} вид матрицы остается подобным рисунку, показанному на рис. 2а, при этом распределение цвета пикселей, естественно иное (рис. 2б).

Приведенные исследования шифрования и дешифрования свидетельствуют о том, что при кодировании цвета символов, формирующих изображение, могут быть использованы псевдослучайные последовательности целых чисел, являющихся результатом решений нелинейного отображения с хаотической динамикой.

При шифровании с помощью последовательности псевдослучайных чисел, использование изменения цвета пикселов, формирующих изображение, позволяет обеспечить его надежную маскировку. Учитывая устойчивость шифра, информацию, зашифрованную рассмотренным способом можно передавать по открытым сетевым каналам, в том числе и по электронной почте, а также хранить в архивах со свободным доступом. При этом маскировка информации при ее передаче по открытым каналам не хуже, чем ее маскировка при передаче излучаемыми хаотическими колебаниями [4-8].

В качестве тестового выбрано черно-белое изображение размером 100×100 пикселов с 256 градациями серого уровня. Изображение и его спектр приведены на рисунках 3а и 3б соответственно.

а) *б)*

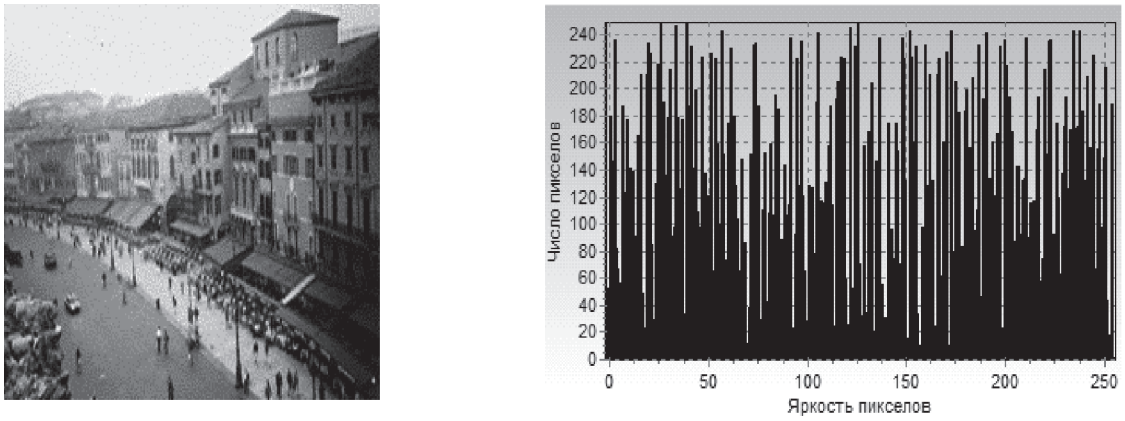

Рис. 3:
а – тестовое черно-белое изображение с 256 градациями серого уровня;
б – спектр яркости цветов пикселов изображения на рис. 3а

Первые тесты по применению этого алгоритма для шифрования информации показали его потенциальную пригодность для криптографического кодирования. Во-первых, в шифрованном изображении не присутствует никаких структур (рис. 4а), и его спектр яркости цветов пикселов стал почти однородным (рис. 4б).

а) *б)*

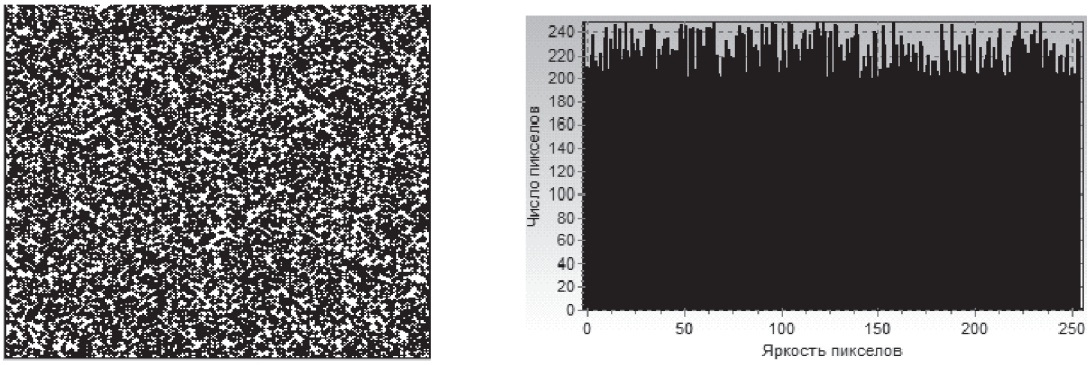

Рис. 4:
а – результат кодирования тестового изображения; б – спектр яркости цветов пикселов шифрованного изображения

Во-вторых, предложенная схема чувствительна к малейшим изменениям начальных условий и/или параметров (получаемые при этом шифры абсолютно различны). В-третьих, она малочувствительна к ошибкам в шифртексте, т.е. при расшифровывание искажения в шифртексте сказываются локально, а не распространяются на все изображение.

В заключение нужно отметить, что надежность данного алгоритма шифрования в большей степени зависит от характеристик применяемого метода генерации псевдослучайных чисел, т.к. на одном из начальных этапов шифрования мы вносим изменения в псевдослучайную числовую последовательность.

Выводы

1. Использование хаотического отображения позволяет создать достаточно сложный шифр, который не поддается раскрытию, если не воспроизведены точные значения начальных условий и параметров динамической системы, при которых выполнялось ее решение.

2. Разработанный криптографический алгоритм преобразования текстовой и графической информации базируется на том, что для хаотических динамических систем существуют периодические возмущения, приводящие к стабилизации цикла заданного периода.

3. Информация шифруется с помощью таких стабилизированных циклов. В качестве передаваемого сигнала используются возмущения, а ключом для расшифровки полученного сообщения служит вид отображения.

4. Приведенные исследования кодирования свидетельствуют о том, что при кодировании как текстовой информации, так и цвета символов, формирующих изображение, могут быть использованы псевдослучайные последовательности целых чисел, являющихся результатом решений нелинейного отображения с хаотической динамикой.

Список литературы

1. Хоффман Л.Дж. Современные методы защиты информации. – М.: Советское радио, 1980. – 264 с.

2. Бейсенби М.А., Ойнаров А.Р. Детерминированный хаос в развитии экономической системы. – Проблемы автоматики и управления. Институт автоматики НАН КР. – Бишкек, Илим, 2004.

3. Тен Т.Л., Бейсенби М.А., Когай Г.Д. Разработка системы защиты информации в распределенных сетях: Монография. – Караганда, КарГТУ, 2012. – С.193-197.

«Фундаментальные и прикладные проблемы медицины и биологии»
ОАЭ (Дубай), 16-23 октября 2014 г.

Медицинские науки

ИЗМЕНЕНИЕ СВЯЗЫВАЮЩЕЙ СПОСОБНОСТИ ГЕМОГЛОБИНА ПРИ ГИПОКСИЧЕСКОМ СОСТОЯНИИ

Мартынова М.И., Родина Н.Н., Кузьмичева Л.В., Новожилова О.С., Громова Н.В., Ревина Э.С., Тайрова М.Р.

ФГБОУ ВПО «Мордовский государственный университет им. Н.П. Огарева», Саранск, e-mail: masha-martynova.92@mail.ru

При многих патологических процессах (инфаркт, инсульт, злокачественные опухоли и т.д.) наблюдается развитие хронической гипоксии и лактоацидоза, активация свободно-радикального окисления в плазме крови и в функционально важных клетках. Важным является изучение различных повреждающих факторов на эритроциты, так как они выполняют важнейшие для организма функции: транспорта кислорода, адаптивной и, возможно, эндокринной. В связи с этим целью нашей работы было изучение состояния гемоглобина в условиях лактоацидоза и гипергликемии. В работе была использована лактатная модель гипоксического состояния (Boning D. et. al., 1989) в условиях гипергликемии, путем инкубации фракции чистых эритроцитов в среде Рингера-Локка (1:1) при 37^0 С в течение 30 мин с добавлением молочной кислоты в концентрации 7,5 мМ/л и глюкозы – 7,5 мМ/л. Исследование выполнено на рамановском спектрометре in via Basis фирмы Renishaw с короткофокусным высокосветосильным монохроматором (фокусное расстояние не более 250 мм). Для возбуждения рамановских спектров использовался лазер (длина волны излучения 532 нм, мощность излучения 100 мВт, объектив 100х). Оцифрованные спектры обработаны в программе WIRE 3.3. Произведена коррекция базовой линии, сглаживание спектров. Для анализа конформации и O_2-связывающих свойств гемоглобина (Гб) использовали следующие полосы КР спектров эритроцитов (указаны положения максимумов): 1172, 1355, 1375, 1548-1552, 1580-1588, 1618, 1668 $см^{-1}$. Спектроскопия комбинационного рассеяния (КР) позволяет исследовать состояние атома железа и лигандов, связанные с ним, по изменению структуры тетрапиррольного цикла гемопорфирина гемоглобина. Содержание МДА в эритроцитах определяли по Конюховой С. Г. В гемолизате, после центрифугирования эритроцитарной взвеси, спектрофотометрически измеряли экстинкции на волновых пиках гемоглобина (430 и 555 нм), оксигемоглобина (536 и 572 нм) и метгемоглобина (630 нм). Как показали наши исследования при умеренном ацидозе (7,5 ммоль/л) наблюдается снижение колебаний пиррольных колец гемопорфирина гемоглобина эритроцитов на 5,9% по отношению к контролю. При этом относительное количество оксигемоглобина, способность гемоглобина связывать и выделять лиганды, а также сродство гемоглобина к кислороду практически не изменяется. Содержание комплексов гемоглобина с NO при отсутствии