Результаты, полученные с использованием оптимизированных уравнений модели, соответствуют экспериментальным, что свидетельствует об эффективности применения предложенного подхода при адаптации диффузионно-дрейфовой модели наноразмерных приборов.

Литература

1. Аоки М. Введение в методы оптимизации. М, 1977.
2. Реклейтис Г., Рейвиндран А., Регсдел К. Оптимизация в технике. Книга 1. М, 1986.
3. "Well-Tempered" Bulk-Si NMOSFET Device Home Page [Электронный ресурс]. – Режим доступа: http://www-mtl.mit.edu/ researchgroups/Well/ – Дата доступа: 20.05.2014.

УДК 004.8

АССОЦИАТИВНОЕ КОДИРОВАНИЕ ФАЙЛОВ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

студент Трофимук В.Д.
Научный руководитель – канд. техн. наук, доцент Садов В.С.
Белорусский государственный университет
Минск, Беларусь

В современном мире, где информационные технологии проникают в повседневную жизнь человека с каждым днём всё глубже и глубже, критическую роль играет удовлетворение требованиям конфиденциальности, целостности и доступности данных. Реализация защищённой программной среды, в которой за счёт тех или иных средств обеспечивается соответствие упомянутым выше критериям, является важной и актуальной проблемой, интересной как с научной, так и с практической точки зрения (непосредственное воплощение разработок в виде программного кода). Данная работа посвящена созданию системы хранения информации с ассоциативной адресацией и симметричной криптографической обработкой файлов изображений с использованием псевдослучайных числовых последовательностей.

Прежде всего, стоит отметить тот факт, что симметричных криптосистем известно великое множество. Немалая их часть является блочными и в процессе функционирования в базовой или модифицированной форме использует нейронную сеть Фейстеля (алгоритмы шифрования DES, ГОСТ, Blowfish, RC6). При этом конфиденциальность информации в подобных системах обеспечивается за счёт сохранения в секрете отправляющей и принимающей сторонами шифр-ключа, задающего вектор начальных условий для соответствующего генератора раундовых ключей — процедуры расширения (по одному на каждую итерацию алгоритма). Большинство процедур расширения алгоритмов шифрования на основе сети Фейстеля используют численные значения, поставляемые предопределёнными методами генерации. Детерминированность используемого в процедуре расширения преобразования начального шифр-ключа в совокупность раундовых ключей, по существу является самым слабым местом симметричных блочных криптоалгоритмов, поскольку при использовании различных вариантов таблиц замен и перестановок шифр может как проявлять высокую криптостойкость, так и быть уязвимым к определённым видам атак (к примеру, 64-битный DES при современных вычислительных мощностях прямым перебором ключей взламывается за разумное время, а стойкость Blowfish напрямую зависит от типа используемой процедуры расширения). Поэтому очевидным улучшением является обеспечение большей хаотичности и меньшей предопределённости выбора числовых значений внутри процедуры расширения ключа.

В рамках работы проведено исследование генераторов псевдослучайных числовых последовательностей на основе явления детерминированного хаоса (системы уравнений Лоренца, схемотехнической модели Чуа). Также на базе последней разработана реализация генератора хаоса с использованием в качестве структурных элементов усилителей и сетевых сумматоров (рис. 1).

Исследованы параметры разработанной модели на хаотичность (вид фазового портрета, спектр показателей Ляпунова, автокорреляционная функция, взаимная корреляционная функция, энтропия Колмогорова, временной горизонт прогнозирования). Спроектирована структура защищённой информационной системы с ассоциа-

тивной адресацией памяти и криптографическим шифрованием файлов изображений (рис. 2).

Впоследствии система реализована в виде кроссплатформенного приложения на языке Java с применением СУБД Oracle (рис. 3).

Большинство полученных в ходе выполнения работы результатов хорошо согласуются с теорией. Разработанный программный комплекс может быть использован в обучающих и научно-практических целях для наглядной демонстрации возможностей криптографического кодирования информации на основе явления детерминированного хаоса.

Таким образом, проведённая работа по созданию защищённой информационной системы демонстрирует преимущества применения генераторов хаотических числовых последовательностей.

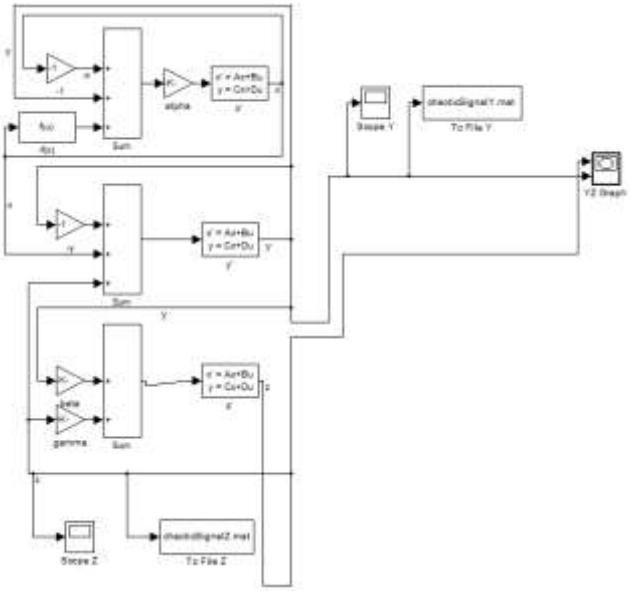

Рис. 1. Модифицированная модель схемы Чуа,
построенная на усилителях и сетевых сумматорах

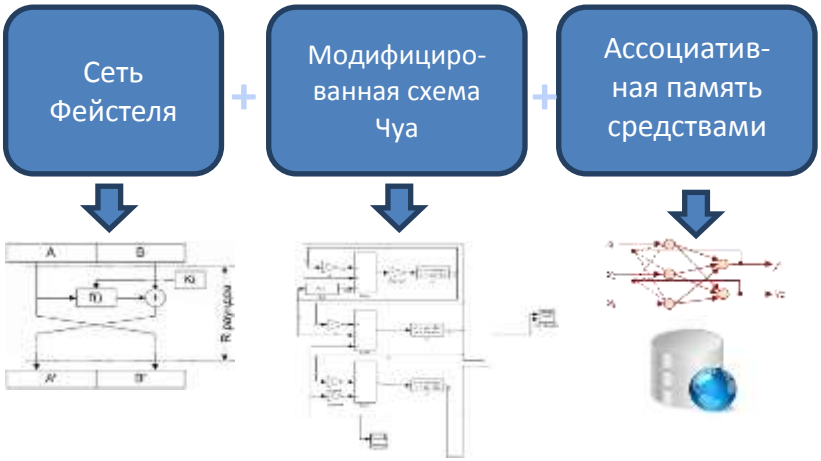

Рис. 2. Структурная схема защищённой информационной системы

Рис. 3. Основное рабочее окно разработанного приложения

В будущем данный труд будет развит за счёт дополнительных исследований реализованной модели генератора хаоса и доработки программного комплекса с целью повышения его криптостойкости.

Литература

1. Пономаренко В. И., Бугаевский М. Ю. Исследование поведения цепи Чуа / В. И. Пономаренко, М. Ю. Бугаевский // Саратовский филиал института радиотехники и электроники РАН, учебно-научная лаборатория «Нелинейная динамика (физический эксперимент)». – 1999, С. 4–19.

2. Андриевский Б. Р., Фрадков А. Л. Управление хаосом: методы и приложения / Б. Р. Андриевский, А. Л. Фрадков // Институт проблем машиноведения РАН, Санкт-Петербург – 2004, С. 11–25.

3. Довгаль В. М., Тарасов А. А. «Криптографическая защита электронных документов на основе сети Фейстеля с применением детерминированных хаотических отображений» / В. М. Довгаль // Известия Курского государственного технического университета, № 1 (30), 2010, С. 44–48

УДК 004.3

ARDUINO КАК УДОБНАЯ ПЛАТФОРМА ДЛЯ БЫСТРОГО МОДЕЛИРОВАНИЯ И РАЗРАБОТКИ АППАРАТНО-ПРОГРАММНЫХ СИСТЕМ

студент гр. 103710 Малахов Т.И.
Научный руководитель - Гулай В.А.
Белорусский национальный технический университет
Минск, Беларусь

Arduino – аппаратная вычислительная платформа, основными компонентами которой являются простая плата ввода-вывода и среда разработки на языке Processing/Wiring. Arduino может использоваться как для создания автономных интерактивных объектов, так и подключаться к программному обеспечению, выполняемому на компьютере (например, Adobe Flash, Processing, Max).

Плата Arduino состоит из микроконтроллера Atmel AVR (ATmega328P и ATmega168 в новых версиях и ATmega8 в старых), а также элементов обвязки для программирования и интеграции с другими схемами (рис. 1). На многих платах присутствует линейный стабилизатор напряжения +5 В или +3,3 В. Тактирование осуществляется на частоте 16 или 8 МГц кварцевым резонатором (в