АССОЦИАТИВНЫЕ АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКИХ ПРОЦЕССОВ

В.Д. Трофимук, В.С. Садов
Факультет радиофизики и компьютерных технологий, кафедра интеллектуальных систем,
Белорусский государственный университет
Минск, Республика Беларусь
E-mail: {trolionsilver, vasiliy.sadov}@gmail.com

Данный материал посвящён актуальной на сегодняшний день проблеме эффективной реализации защищённых информационных систем. В статье проводится пристальный анализ известных алгоритмов работы информационных систем, а также авторами предлагается собственный вариант системы, в основу которого положена ассоциативная адресация памяти и шифрование данных с помощью детерминированных хаотических процессов. Произведена реализация информационной системы разработанной структуры на программной платформе Java, её исследование по основным характеристическим показателям, показана эффективность описанного подхода. Результаты проведённой работы представляют интерес как с научной, так и с практической точки зрения.

Введение

Проблема эффективной реализации защищённой информационной системы не является новой и подробно рассматривается во многих источниках, к примеру [1], [2]. Основными подходами к её решению являются криптографическое шифрование данных (в статье используется нейронная сеть Фейстеля согласно [3]) и организация ассоциативной адресации памяти в адресном пространстве ЭВМ [4]. Ключевым недостатком методов симметричного шифрования на основе сети Фейстеля является применение детерминированных алгоритмов генерации раундовых ключей [3], что может быть использовано злоумышленником для раскрытия шифра. Что касается ассоциативной адресации памяти, то её аппаратная реализация является сложной как с теоретической, так и с практической точки зрения [5], в то же время программная реализация требует значительно меньших вложений ресурсов и потому часто используется в информационных системах с реляционными базами данных [6]. Таким образом, в данной статье рассматривается симметричное шифрование файлов изображений сетью Фейстеля с раундовыми ключами, поставляемыми собственной реализацией генератора хаотических числовых последовательностей, при этом как к открытым, так и к зашифрованным данным предоставляется ассоциативный доступ за счёт использования механизма индексирования в СУБД [7].

I. Детерминированный хаос как явление и понятие

Явление детерминированного хаоса было открыто в 1963 г. метеорологом Э. Лоренцем в ходе проведения расчётов прогноза погоды [8]. После этого соответсвующее явлению понятие стало применяться при рассмотрении поведения многих физических и иных систем [9 –11]. При этом основными численными оценкам степени хаотичности поведения той или иной системы являются спектр показателей Ляпунова (1), значение корреляционной функции (2), энтропия Колмогорова (3), временной горизонт прогнозирования (4) [12].

$$\lambda(x_0) = \lim_{N\to\infty} \lim_{\epsilon\to 0} \frac{1}{N} \ln \left| \frac{f^n(x_0+\epsilon) - f^n(x_0)}{\epsilon} \right| = \lim_{N\to\infty} \frac{1}{N} \ln \left| \frac{df^n(x_0)}{dx_0} \right|. \quad (1)$$

$$\mathrm{C(m)} = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-m-1} \langle x_{i+m} \rangle \langle x_i \rangle . \quad (2)$$

$$\mathrm{K} = \int d^d x \rho(x) \sum_i \lambda_i^+(x). \quad (3)$$

$$\mathrm{T}_m \sim \frac{1}{K} \ln \frac{1}{l} \approx \frac{1}{\lambda}. \quad (4)$$

II. Генераторы динамического хаоса: общий обзор

Целенаправленная разработка моделей генераторов динамического хаоса ведётся с середины 60-х годов прошлого века. При этом основными и наиболее классическими в рамках теории хаоса являются реализации генераторов на основе системы уравнений Лоренца [13] и электрической цепи Чуа [14] (рис. 1).

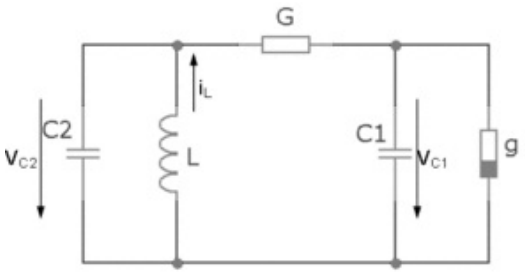

Рис. 1 – Классическая схема Чуа

В качестве основной модели генератора динамического хаоса для данной работы выступила модифицированная схема Чуа, построенная на таких элементах, как усилители и сетевые сумматоры (рис. 2). Описанная выше цепь разработана и протестирована авторами работы в надстройке Simulink среды Matlab.

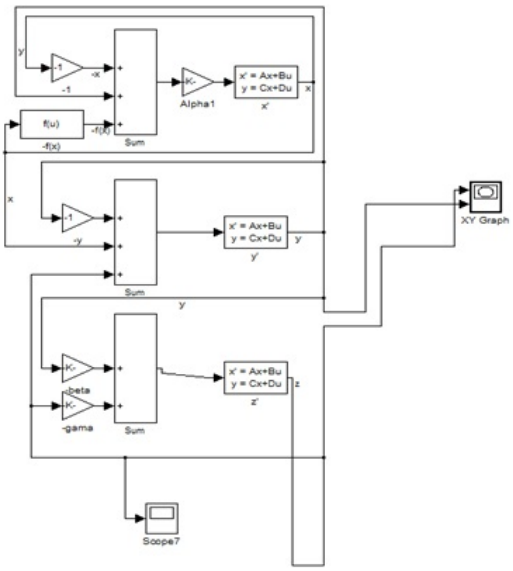

Рис. 2 – Модифицированная схема Чуа на усилителях и сетевых сумматорах

Внешний вид хаотического сигнала, генерируемого модифицированной схемой Чуа приведён далее (рис. 3)

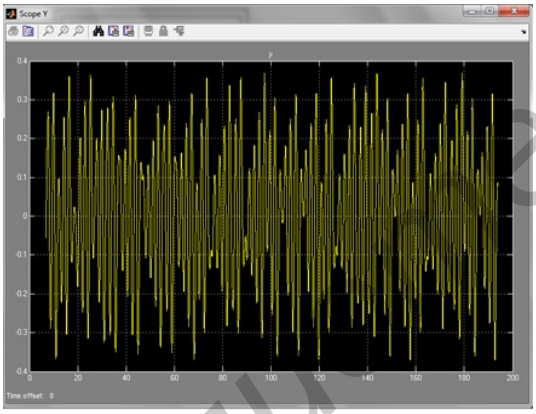

Рис. 3 – Вид хаотического сигнала, генерируемого модифицированной схемой Чуа, построенной на усилителях и сетевых сумматорах

III. Анализ генерируемых хаотических сигналов

Анализ генерируемых хаотических сигналов в данной работе производится путём исследования зависимости одной из фазовых координат (в нашем случае – Y) от независимого параметра (в качестве которого естественным образом полагается время t). При этом фазовый портрет системы, полученный в среде Matlab, является аттрактором типа «двойной завиток» (рис. 4), что соответствует теории рассматриваемого процесса.

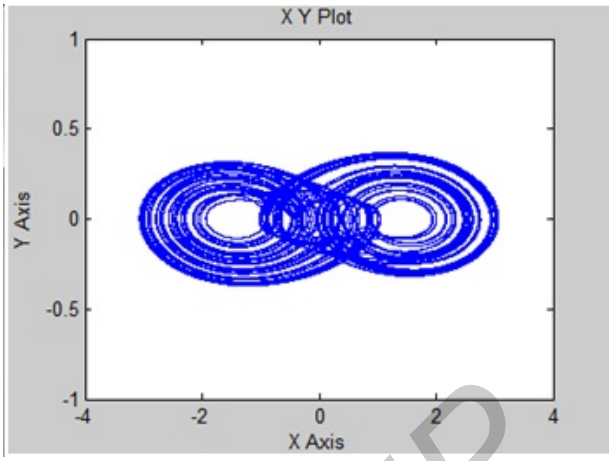

Рис. 4 – Фазовый портрет модифицированной схемы Чуа на усилителях и сетевых сумматорах

Расчётные значения спектра показателей Ляпунова модифицированной схемы Чуа на усилителях и сетевых сумматорах составили [0,9330; -1,0883]. Так как в спектре присутствует положительный показатель – поведение системы может рассматриваться как хаотическое.

График нормированной автокорреляционной функции Y(t) приведён ниже (рис. 5)

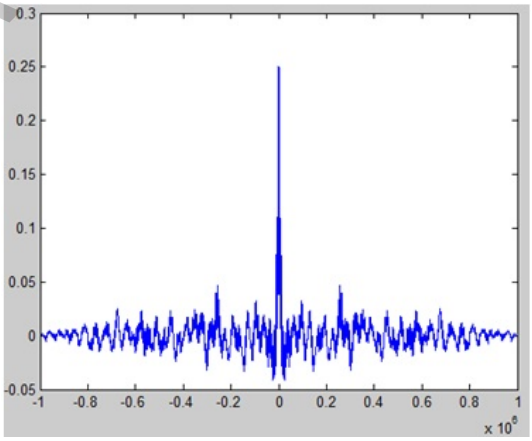

Рис. 5 – График нормированной автокорреляционной функции модифицированной цепи Чуа на усилителях и сетевых сумматорах

Взаимная корреляционная функция – характеристика хаотичности системы, показывающая насколько два различных, но очень близких по начальным условиям сигнала, генерируемых одной и той же системой, в среднем связаны между собой. В данной работе различия начальных условий при генерации хаотичесих сигналов модифицированной схемой Чуа принимались равными 0,001 от абсолютных величин. На основании полученных результатов построен график (рис. 6).

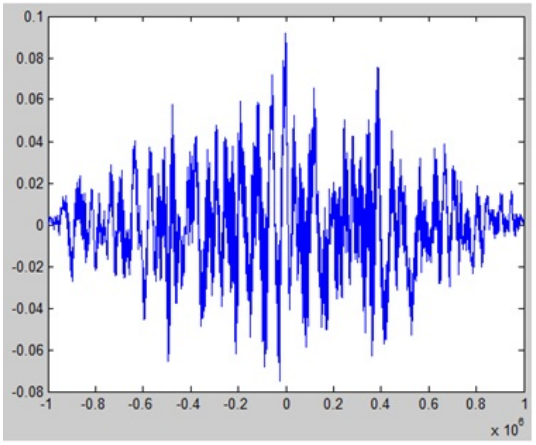

Рис. 6 – График взаимной корреляционной функции двух сигналов, генерируемых модифицированной цепью Чуа на усилителях и сетевых сумматорах с близкими значениями начальных условий

Также стоит отметить, что полученные расчётные значения энтропии Колмогорова и временного горизонта прогнозирования системы составили, соответственно 0,933 бит/с и 1,0718 с. Все описанные в данном разделе результаты согласуются с теорией на очень высоком уровне, что позволяет эффективно внедрять разработанный генератор псевдослучайных числовых последовательностей в модель защищённой информационной системы.

IV. Разработка модели криптосистемы с ассоциативным кодированием информации на основе детерминированнного хаоса

В качестве основы разрабатываемой системы авторами принята структурная схема, состоящая из 3-х логических частей [3] (рис. 7).

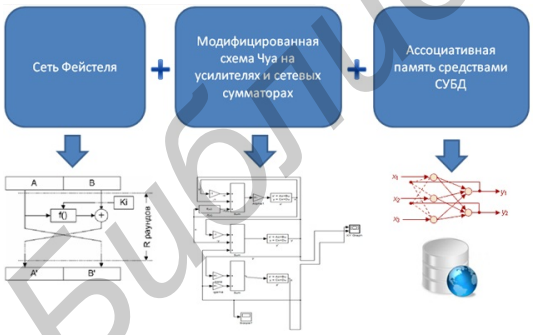

Рис. 7 – Общая структурная схема системы ассоциативного кодирования информации с обеспечением её криптографической защиты

Таким образом, в системе, структурная схема которой приведена на рис. 7, роль криптографического блока играет схема Фейстеля; хаотические, но при этом воспроизводимые значения раундовых ключей поставляет разработанный ранее генератор динамического хаоса – модифицированная схема Чуа на усилителях и сетевых сумматорах; быстрый и удобный доступ к информации зарегистрированному пользователю предоставляет организованная ассоциативным образом память, реализуемая средствами СУБД (в нашем случае использовалась Oracle Database).

V. Реализация программного комплекса

Для непосредственной реализации программного комплекса авторами избрана платформа и язык программирования Java. Язык Java является одним из самых распространённых в мире за счёт императивности, объектной ориентированнасти и кроссплатформенности. Кроме того, существует немалое количество совместимых с Java технологий и надстроек (frameworks), позволяющих решать те или иные конкретные задачи. Для реализации защищённой информационной криптосистемы по обработке изображений с графическим пользовательским интерфейсом авторами использовались следующие программные инструменты:

- Java SE 7
- Swing (графическая библиотека)
- Oracle Database 11g XE
- Hibernate (ORM-framework)
- NetBeans 7.0
- Oracle SQL Developer + SQL Data Modeller
- NClass

Реляционная модель разработанной для приложения простейшей базы данных приведена на рис. 8.

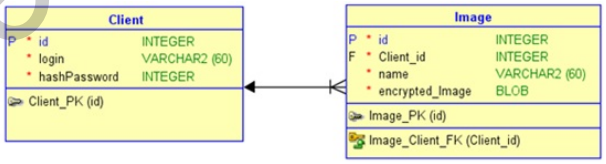

Рис. 8 – Реляционная модель базы данных разработанного приложения

Внешний вид основного окна разработанного приложения приведён на рис. 9.

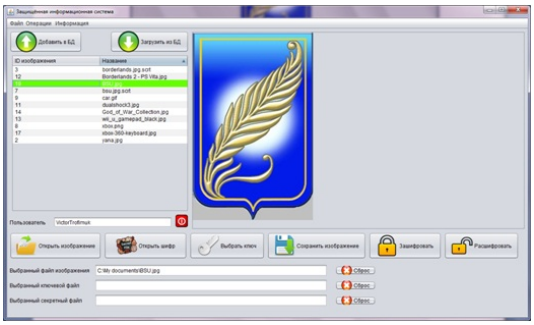

Рис. 9 – Основное окно разработанного приложения

В заключение авторами приводится корреляционная оценка эффективности функционирования разработанного приложения. Для этого выделяются некоторые характерные группы изображений и исследуется по одному опытному

образцу из каждой. В качестве наглядного примера зашифрованного изображения предлагается рассмотреть электрическую схему (см. рис. 10, 11).

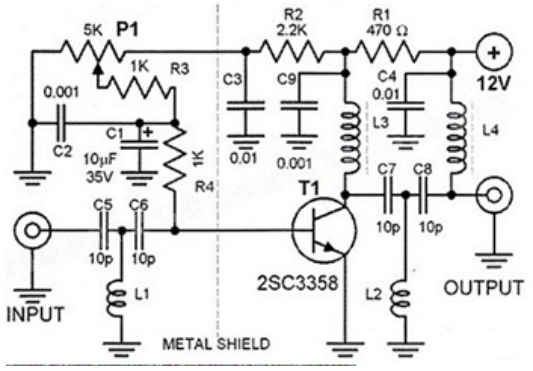

Рис. 10 – Открытое изображение электрической схемы

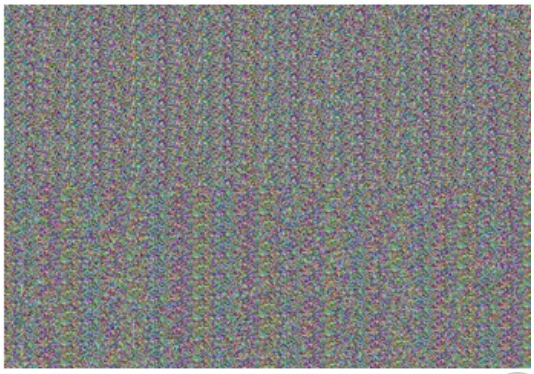

Рис. 11 – Зашифрованное изображение электрической схемы

Для всех исследованных групп изображений корреляционная зависимость между исходным и зашифрованным файлами составила менее 3 %, что является хорошим результатом кодирования для разработанной информационной системы.

Заключение

В материале подробно рассмотрена проделанная работа по реализации собственной модели генератора динамического хаоса (с исследованием её основных характеристических параметров), а также по внедрению разработанного генератора в конкретный программный комплекс, представляющий собой защищённую информационную среду для хранения и криптографического шифрования файлов изображений. Полученные практические результаты в существенной мере хорошо согласуются с соответствующей теорией, что позволяет судить об эффективности полученного приложения в рамках сформулированных задач. Разработанные алгоритмы, структурные схемы и программные решения могут непосредственно применяться в научно-образовательных целях при изучении курсов криптографии и стеганографии.

1. Защищённые информационные системы // Информационный документ корпорации Microsoft [Электронный ресурс]. -– 2002. -– Режим доступа: http://download.microsoft.com/documents/rus/security/certificate/concept.doc. – Дата доступа: 25.06.2014.
2. Information Security // Wikipedia - – The Free Encyclopedia [Electronic resource]. -– 2014. -– Access mode: http://en.wikipedia.org/wiki/InformationSecurity. – Access date: 26.06.2014.
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.
4. Кохонен Т. Ассоциативная память, адресация по содержанию и ассоциативная выборка / Т. Кохонен // Ассоциативные запоминающие устройства -– М., 1982, – С. 3-30
5. Крайзмер Л. П., Бородаев Д. А., Гутенмахер Л. И. Схемы ассоциативных запоминающих устройств / Л. П. Крайзмер // Ассоциативные запоминающие устройства -– Ленинградское отделение издательства «Энергия», 1967, – С. 108-140.
6. Нужна ли ассоциативная память // iXBT.com [Электронный ресурс]. -– 2001. -– Режим доступа: http://www.ixbt.com/mainboard/associative-memory.shtml. – Дата доступа: 14.02.2014.
7. Кайт Т. Индексы в Oracle DB / Т. Кайт // Oracle для профессионалов, Москва. -– DiaSoft, 2003, – С. 341-346.
8. Джеймс Г. Памяти Эдварда Лоренца: «эффект бабочки». / Г. Джеймс // Хаос: создание новой науки. [Электронный ресурс]. -– 2007. -– Режим доступа: http://www.namerenie9.ru/publ/nauka/pamjati ehdvarda nortona lorenca ehffekt babochki/4-1-0-36. – Дата доступа: 16.02.2013.
9. Швец А. Ю. Детерминированный хаос сферического маятника при ограниченном возбуждении / А. Ю. Швец // Украинский математический журнал. – 2007, – том 59, № 4.
10. Ланда П. С. Возникновение турбулентности в незамкнутых течениях жидкости как неравновесный шумоиндуцированный фазовый переход второго рода / П. С. Ланда // Журнал технической физики. – 1998, -– том 68, № 1.
11. Лоскутов А. Ю., Мушенков А. В., Одинцов А. И., Федосеев А. И. Нестационарные и хаотические режимы генерации в лазерных системах с поперечной прокачкой / А. Ю. Лоскутов, А. В. Мушенков, А. И. Одинцов, А. И. Федосеев // НИИ Ядерной физики МГУ. [Электронный ресурс]. – 1999, -– Режим доступа: http://optics.sinp.msu.ru/sci/hpl98pre/hpl98pre.html. – Дата доступа: 02.03.2013.
12. Шустер Г. Характеристики хаотического движения / Г. Шустер // Детерминированный хаос: введение -– М., 1988, – С. 12-18; 31-39.
13. Антипов В. В. Анализ временного сигнала системы Лоренца: автореферат / В. В. Антипов, П. С. Волегов к.ф.-м.н., доц. каф. ММСП ПНИПУ — Пермь, 2005, -– 17 с.
14. 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.