Изменение количества линейных участков приводит к усложнению АЦП при аппаратурной реализации.

Ограничение на использование данного алгоритма выполнения аналого-цифрового преобразования обусловлено наличием равномерной сетки при кусочно-линейной аппроксимации с равным числом точек отсчета на линейных участках, т.е. постоянства ΔT_i и Δt_j при изменениях i и j. Это связано с тем, что значение точек перегиба аналогового сигнала должно с наперёд заданной точностью соответствовать значению аналогового сигнала в граничных узлах кусочно-линейных функций.

Несмотря на это, алгоритм преобразования не претерпит существенных изменений, если выбирать значения ΔT_i различными для отдельных отрезков при условии совпадения точки перегиба аналогового сигнала с его значениями на концах линейных отрезков ΔT_i, что связано с вычислениями *M* для каждого из линейных участков аппроксимации.

Литература

1. Бабаян Р.Р. Микроэлектронные АЦП и ЦАП.—"Датчики и системы", 2008, № 8, с. 40-44.

2. Мерзликин С.А. Сверхбыстродействующая АЦП: особенности архитектуры.- - "Электроника: наука, технология, бизнес", 2008, №1, с. 30-33.

3. Гуменюк А.С., Бочаров Ю.И. Устройства выборки хранения быстродействующих АЦП. - "Микроэлектроника", 2007, 36, № 5, с 390-400.

4. Корсунов Н.И. Корсунова Е.В., Муромцев В.В. – «Вопросы радиоэлектроники», сер. ЭВТ, 2011, вып 1, с. 155-159.

Статья поступила 09 12 2011

Д.т.н., проф. Н.И. Корсунов, А.И. Титов (НИУ «БелГУ»)

N.I. Korsunov, A.I. Titov

ЗАЩИТА ИНФОРМАЦИИ БАЗ ДАННЫХ, ХРАНЯЩИХСЯ НА УДАЛЕННЫХ СЕРВЕРАХ

PROTECTION OF INFORMATION DATABASES STORED ON REMOTE SERVERS

В статье предлагается метод кодирования данных с использованием ключа Эволюционный процесс получения скрытного кода данных обеспечивает прохождение в следующий ряд селекции кодов ключа, получаемых случайным изменением указанных кодов с вводимых по определенным правилам расширения. и данных предыдущего ряда, удовлетворяющих заданному критерию отбора

The article proposes an evolutionary method of encoding data using a key The evolutionary process of obtaining a concealed package provides data processing in the next row selection code key and the previous number that satisfy a selection criterion, obtained by random variation in these codes with inpu by certain rules extension

Ключевые слова криптостойкость, селекция, расширение полей, поколение

Key word cryptographic, selection, extension fields generation

При разработке программного обеспечения для документооборота и архивного дела постоянно встает вопрос о защите информации от несанкционированного доступа. Одним из способов защиты информации является скрытность кодирования, называемая шифрованием [1].

Шифрование данных связано с введением ключа k и функции шифрования E, в результате чего из открытых данных P формируются скрытные данные

$$C=E_k(P)$$

В [2] отмечается, что без введения ключа применение одной и той же функции шифрования к одним и тем же данным приводило бы всегда к получению одних и тех же скрытных данных. В этом случае скрытность данных полностью определяется неизвестностью функции шифрования, а это невозможно обеспечить при современном уровне информационных технологий. Процесс шифрования неразрывно связан с процессом дешифрования, обратным процессу шифрования

$$P=D_k(C)$$

В зависимости от типа используемых ключей k и k' системы шифрования разделяют на симметричные k=k' и асимметричные k<>k'. В асимметричных системах секретен должен быть только один из ключей.

К основным способам симметричного скрытного кодирования данных относят: перестановки, подстановки и гаммирование [3]. При шифровании перестановкой символы скрытного текста переставляются в соответствии с правилом, задаваемым ключом. Данный способ шифрования обеспечивает высокую скорость получения скрытных данных, но использует узкий диапазон ключей и сохраняет частотные характеристики открытого текста после шифрования.

При шифровании с помощью подстановки осуществляется замещение символов скрытного текста символами, определяемыми правилами, задаваемыми ключом шифрования. Достоинством данного способа является маскирование частоты появления различных символов открытого текста.

К недостаткам этого способа шифрования относят малое число возможных ключей.

При гаммировании открытый текст преобразуется в шифр-текст последовательно по одному биту путем наложения на открытый текст гаммы шифра с помощью какой-либо обратимой операции. Основным преимуществом данного метода является высокая производительность.

К недостаткам следует относить открытость гаммы шифра, что приводит к восстановлению текста после гаммирования, пользуясь той же самой операцией.

Приведенные недостатки обусловили применение при симметричном шифровании комбинаций из этих методов, как это реализовано в криптосистемах DES с модификациями и ГОСТ 28147-89. Так как важнейшим показателем качества построенного шифротекста является отсутствие каких-либо закономерностей в шифротексте, то в чистом виде не используются шифр-перестановок или подстановок.

Большинство современных криптосистем относится к блочным шифрам, в которых открытый текст разбирается на блоки фиксированной длины. При этом к каждому блоку применяется функция шифрования, использующая перестановки битов блока и многократное повторение операций подстановки и гаммирования, после чего над зашифрованными блоками может повторяться дополнительная операция перед включением их в шифр-текст.[4]

Проведенный анализ способов симметричного скрытного кодирования данных показывает, что для скрытных тестов большой

длины главной проблемой симметричного шифрования является генерация, хранение и распространение ключа шифрования достаточной длины.

В [4] для решения данной задачи предлагалось для генерации шифров необходимой длины вместо наложения гаммы шифра перед случайным изменением содержимого ключа вводить поле расширения по определенным правилам и использовать в дальнейшем уже более длинный ключ. При этом обеспечение необходимой длины ключа достигается многократными расширениями длины ключа. Однако, за счет функции преобразования, в виде сложения по модулю два, скрытого текста с текстом ключа требовалось не только секретность ключа, но и секретность способа его расширения.

В статье для повышения криптостойкости кода предлагается использовать подход, при котором шифр-код формируется в результате эволюционного отбора на заданном шаге селекции, при этом нет необходимости в скрытости кода ключа.

Как и в [4] случайным образом задают код ключа, длина которого совпадает с длиой шифруемого кода. Задают две функции $f_1(x_1,x_2)$ и $f_2(x)$, первая из которых задается для формирования скрытного кода по значениям исходного кода и кода ключа, а вторая – для расширения длины исходного кода и кода ключа. Необходимым условием является существование функции $\varphi 1=f_1^{-1}(x)$ и $\varphi 2=f_2^{-1}(x)$, соответственно, для f_1 и f_2 Задают также количество поколений эволюционного отбора N и критерий участия потомков, полученных на данном шаге селекции отборе следующего поколения.

Для формирования скрытного кода на i-м шаге селекции по значениям кода и ключа, полученным на i-1-ом шаге. Вначале проводят расширения полей ключей $k_{\lambda i}$ и шифрованного кода k_{gi}

$$k\lambda i = f2(k\lambda i - 1),$$
$$kgi = f2(kgi - 1), \qquad (1)$$

и затем формируют шифрованный код в функции $k^*_{\lambda i}$ и k^*_{gi}, т.е.

$$kgi = f1(k^*_{\lambda i}, k^*_{gi}), \qquad (2)$$

$$f1 = (k_{\lambda i} \oplus k_{gi}) \qquad (3)$$

где $k^*_{\lambda i}$ и k^*_{gi} получают случайным изменением значений кодов, полученных в результате преобразования (1). Значение k_{gi}, полученное

в результате преобразования (3) и значение $k_{\lambda i}$ принимают за значение $k_{\lambda i-1}$ и k_{gi-1} для следующего шага селекции, при удовлетворении заданному критерию $k^*_{\lambda i}$ и k^*_{gi}. В противном случае повторяется случайное изменение значений $k_{\lambda i}$ и k_{gi}, полученных в результате преобразования (1).

В качестве критерия отбора при двоичном кодировании исходного кода и ключа может быть выбрана кратность корректирующей ошибки. В этом случае функция f2 округляется по длине кода ключа, для нее всегда существует и может быть вычислена обратная функция φ_2^{-1}.

В качестве функции f1 может быть выбрана функция сложения по заданному модулю, как и в любой из известных систем скрытного кодирования данных[5].

Криптостойкость полученного кода обеспечивается заданием необходимого поколения селекции N и функциями f1 и f2 , а также критериями отбора для следующего шага селекции. Так как f1 обычно известна, то необходимо обеспечить секретностьN,f2 и критерия отбора. Даже если принять известными характер f2 и критерий отбора, то вследствие неоднозначности задания f2 всегда существует секретность выбора конкретной функции $f^*_2 \in f_2$ и секретность выбора количества поколений N. Если для определения одного из M значений f2 по k элементам потребуется количество переборов, определяемое бином Ньютона, то количество функций двух переменных при числе поколений $N = 2^{2^{*N}}$, что приводит к неразрешимой проблеме даже при использовании суперкомпьютеров.

Таким образом, применение эволюционных методов при кодировании данных обеспечивает достаточно высокую скрытность кода и требует меньшего количества ресурсов при реализации.

Так как наибольшим быстродействием обладает способ шифрования перестановкой, то именно его следует реализовать при кодировании данных эволюционными методами. В этом случае производится совмещение кодов шифруемых данных и ключа, что приводит к шифрованию слова

$$C = C^* K^*, \qquad (4)$$

где: C^* - код подлежащий шифрованию,

K^* - случайным образом сгенерированный ключ длины l1 равный длине C^*.

В соответствии с функцией f2(x) проводят расширение полей C^* и K^* в результате получают в соответствии с (1) код

$$C_1 = C^* K^*, \quad (5)$$

длина которого l2>l1 и затем случайным образом изменяет C^*_1 и K^*_1. Это приводит к получению

$$C^1_1 = C^{*1}_1 K^{*1}_1. \quad (6)$$

После этого проверяют C^1_1 на соответствие критерия отбора и, если он не удовлетворяется, вновь к (5) применяют случайное изменение. При удовлетворении критерию отбора, в соответствии функцией f1, производят в (6) заданные перестановки.

Описанные действия повторяют циклически до тех пор, пока не будет выбрано требуемое поколение. Код $C^2_1 = f_1(C^{*1}_n K^{*1}_n)$ принимают за скрытый код данных.

Следует отметить, что в данном случае значение кода ключа не имеет значения, т.к. оно также не потребуется при выполнении обратного преобразования.

Для выполнения обратного преобразования необходимо значение функции f1 для каждого из N поколений, а также прямая и обратная функции f2. А т.к. f2 и $f_2{}^1$ определяются правилами расширения полей данных и ключа, например в виде

$$D_p = D_X A, \quad (7)$$

где: D – матрица строка данных длины m ,

A– матрица размером lxl, то a_{ij} должны быть скрытыми.

Процесс дешифрования сводится к последовательному восстановлению C^* , начиная со значения скрытного кода C^2_n . Для этого для каждого из поколений применяют следующие операции для i=n,n-1, . . , l:

$C^1_i = f_i{}^1(C^2_n)$ – обратная перестановка

$C_i = f_i^{-1}(C^2_n)$ – восстановление значения кода после случайного изменения

C=f3(C1) – исключение K^*.

Операция $f_2^{-1}(C^1_i) = C^1_i + \delta_i$, где искаженный код суммируется по модулю 2 с синдромом, образуемым произведением C^1_i на матрицу обратную А.

Так как при шифровании и дешифровании данных выполняются линейные операции, то сохраняется быстродействие, присущее методу шифрования перестановкой , а длина ключа может

быть увеличена заданием соответствующего количества поколений N. Защищенность системы от взлома определяется скрытыми параметрами: количеством поколений селекции (отбором) N, размерами матрицы m, l и ее коэффициентами a_{ij}. В этом случае значение N позволяет осуществлять скрытное кодирование для отдельных абонентов.

Литература

1. Девятин П.Н., Михальский О.О., Правиков Д.И., Серебряков А.Ю. Теоретические основы компьютерной безопасности. М., Радио и связь, 2000.

2. Баричев С.Г., Гончаров В.В., Серов О.Е. Основы современной криптографии. М., Горячая линия-телеком, 2001.

3. Щербанов А.Ю. Прикладная криптография. Исследование и синтез криптографических интерфейсов. М., Русская редакция, 2003.

4. Корсунов Н.И., Муромцев В.В., Титов А.И. Метод расширения ключа для шифрования информации. – "Научные ведомости БелГУ", сер. История, Политология, Экономика, Информатика, 2010, № 19.

5. Зубов А.Ю. Совершенные шифры. М., Гелиос АРВ, 2003. 160 с.

Статья поступила 09.12.2011

Н.П. Путивцева (НИУ «БелГУ»)

N.P. Putivzeva

КОМПЬЮТЕРНАЯ ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ ОБ УРОВНЕ ПРОФЕССИОНАЛЬНЫХ ЗНАНИЙ В СФЕРЕ ИКТ

PROGRAM SUPPORT OF DECISION MAKING ABOUT THE LEVEL OF PROFESSIONAL KNOWLEDGE IN THE ICT SPHERE

В статье представлена системная процедура оценивания уровня профессиональных знаний в сфере ИКТ на основе иерархической процедуры парных сравнений по типу экспертной процедуры отбора и обработки информации, при которой испытуемый, чей уровень профессиональных знаний определяется, рассматривается в качестве эксперта, а также программная поддержка данной процедуры, автоматизирующая процесс оценки

In the article the system procedure to the evaluation of the level of professional knowledge in the ICT sphere on the basis of the