УДК 681.3

АЛГОРИТМ ПРЕОБРАЗОВАНИЯ ИЗ МОДУЛЯРНОГО КОДА В ПОЛИАДИЧЕСКУЮ СИСТЕМУ ОСНОВАНИЙ ДЛЯ СИСТЕМ ОБНАРУЖЕНИЯ И КОРРЕКЦИИ ОШИБОК

Стрижков Н.С., Калмыков М.И.

Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

В настоящее время системы контроля и управления доступом (СКУД), использующие биометрическую идентификацию и аутентификацию, нашли широкое применение в различных областях. Как правило, в таких устройствах используют статические образы авторизованного пользователя. Однако данные системы слабо защищены от обмана муляжом. Данного недостатка лишены методы биометрической идентификации пользователя по его динамическим параметрам. Для повышения эффективности таких систем предлагается использовать цифровую обработку сигналов (ЦОС), реализованную на основе полиномиальной системы классов вычетов (ПСКВ). Предлагается алгоритм, позволяющий осуществлять преобразование непозиционного кода ПСКВ в позиционный двоичный код. Использование полиадической системы оснований позволяет также осуществлять процедуру поиска и коррекции ошибок, возникающих в процессе функционирования.

Ключевые слова: остатки, полиномиальная система классов вычетов, коэффициенты обобщенной полиадической системы счисления, обнаружение и коррекция ошибок.

ALGORITHM FOR CONVERTING FROM THE MODULAR CODE THE POLYADIC SYSTEM BASES FOR SYSTEMS ERROR DETECTION AND CORRECTION

Strizhkov N.S., Kalmykov M.I.

Federal state Autonomous educational institution higher professional education «North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru

Currently, system access control system (ACS) , using biometric identification and authentication are widely used in various fields. Typically, such devices rely on static images of the authorized user . However, these systems are vulnerable to fraud hoax . This deficiency deprived of biometric user identification by its dynamic parameters . To increase the effectiveness of such systems is proposed to use digital signal processing (DSP) capabilities using polynomial system of residue classes (PSKV) . An algorithm is proposed to allow for the conversion code nonpositional PSKV position in binary code. Using polyadic system bases also allows the search procedure and correct errors that occur during operation

Keywords: residues, polynomial system of residue classes, the coefficients of the generalized polyadic notations, detection and correction of errors.

Введение

В настоящее время существует множество методов обеспечения информационной безопасности автоматизированных систем. Одним из перспективных направлений в области защиты информации является биометрическая аутентификация, для которой необходимо использовать цифровую обработку сигнала (ЦОС). Применение методов ЦОС позволяет повысить эффективность работы систем, используемых для биометрической идентификации и аутентификации пользователя. Очевидно, что использование той или иной математической модели ЦОС может оказать существенное влияние на эффективность работы всей системы контроля и управления доступом (СКУД).

Постановка задачи исследований

Биометрическая идентификация и аутентификация пользователя является одним из перспективных направлений защиты информации от НСД. В настоящее время наибольшее распространение получили системы контроля и управления доступом, базирующееся на статических параметрах пользователя. Однако данные системы слабо защищены от обмана муляжом. Данного недостатка лишены методы биометрической идентификации пользователя по его динамическим параметрам.

Однако для эффективной работы систем контроля управления доступом (СКУД), использующих динамическую биометрию пользователя, необходимо осуществлять первичную обработку образа. Как правило, такая обработка основана на методах цифровой обработки сигналов. Известно, что большинство методов первичной обработки сигналов базируется на ортогональных преобразованиях, определенных в поле комплексных чисел, т.е. дискретном преобразовании Фурье, которое имеет ряд недостатков: низкая скорость обработки сигналов;

аддитивные и мультипликативные погрешности из-за иррациональных значений поворачивающих коэффициентов W^{kn}. Кроме того, необходимо, чтобы возникающие при первичной обработки сигналов ошибки, были устранены в процессе этих вычислений [3].

Решить данные проблемы можно за счет применения специальной системы кодирования, которая бы поддерживала математическую модель ЦОС, обладающую свойством кольца или поля, а также была способна обнаруживать и корректировать ошибки. Данным требованиям удовлетворяет полиномиальная система классов вычетов (ПСКВ) [2-5,9]. Если в качестве оснований новой алгебраической системы выбрать минимальные неприводимые многочлены $p_i(z)$ поля $GF(p^v)$, то любой сигнал $x(n)$, представленный в полиномиальной форме $X(z)$, удовлетворяющий условию

$$X(z) \in P_{пол}, \qquad (1)$$

где $P_{пол} = \prod_{i=1}^{n} p_i(z) = z^{p^v-1} - 1$,

можно представить в виде n-мерного вектора

$$X(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_n(z)), \qquad (2)$$

где $\alpha_i(z) = rest(A(z)/p_i(z))$, $i = 1,2,...,n$.

Если сигнал с выхода аналого-цифрового преобразователя (АЦП) представить в полиномиальной форме, то его можно закодировать в ПСКВ в виде совокупности остатков, полученных в результате деления исходного полинома на минимальные многочлены, определяемые в расширенных полях Галуа. Тогда операции сложения, вычитания, умножения над операциями можно свести к аналогичным операциям над остатками. Переход к выполнению арифметических действий над малоразрядными остатками позволяет повысить быстродействие вычислительной системы [4-8].

Наряду с повышением скорости обработки данных ПСКВ позволяет обеспечить свойство устойчивости к ошибкам, которые возникают в процессе функционирования непозиционного устройства ЦОС [1,4,7-10].

Анализ работ показал, что полином, представленный в ПСКВ, не содержит ошибки, если справедливо

$$A(z) \in P_{раб}(z) = \prod_{i=1}^{k} p_i(z), \qquad (3)$$

где k – количество информационных оснований ПСКВ $(k<n)$.

В противном случае, если в результате выполнения вычислений произошла ошибка, то полином $A^*(z)$ будет лежать вне рабочего диапазона.

Для обнаружения и коррекции ошибок в кодах ПСКВ используются позиционные характеристики [1,4,7-10]. Особое место среди таких позиционных характеристик занимают коэффициенты обобщенной полиадической системы (ОПС) [6].

Пусть задана полиномиальная система классов вычетов, состоящая из пяти минимальных многочленов. В данном случае определены следующие полиномиальные основания:

- рабочие $p_1(z) = z+1$, $p_2(z) = z^2 + z + 1$, $p_3(z) = z^4 + z^3 + z^2 + z + 1$;

- контрольные $p_4(z) = z^4 + z^3 + 1$, $p_5(z) = z^4 + z + 1$.

В обобщенной полиадической системе полином $A(z)$ представляется в виде

$$A(z) = a_1 + a_2 p_1(z) + a_3 p_1(z) p_2(z) + a_4(z) p_1(z) p_2(z) p_3(z) + a_5(z) p_1(z) p_2(z) p_3(z) p_4(z) \qquad (4)$$

Если наложить ограничение на количество информационных оснований $(k=3)$, то рабочий диапазон будет равен

$$P_{ðàá}(z) = \prod_{i=1}^{3} p_i(z) = z^7 + z^6 + z^5 + z^2 + z + 1.$$

Тогда равенство (3) можно представить в следующем виде

$$A(z) = a_1 + a_2 p_1(z) + a_3 p_1(z) p_2(z) + a_4(z) P_{раб}(z) + a_5(z) P_{раб} p_4(z). \qquad (5)$$

Из последнего равенства наглядно видно, что если полином $A(z)$, представленный в ПСКВ, не содержит ошибок, т.е. удовлетворяет условию

$$\deg A(z) < \deg P_{раб}(z), \qquad (6)$$

то значения старших коэффициентов ОПС в равенстве (5) должны быть нулевыми. Другими словами, $a_4(z)=0$, $a_5(z)=0$. В противном случае, полином содержит ошибки.

Для эффективной реализации вычислений коэффициентов ОПС по значениям остатков ПСКВ был разработан алгоритм

перевода из кода ПСКВ в код ОПС, который базируется на китайской теореме об остатках.

$$A(z)=\sum_{i=1}^{k+r}\alpha_i(z)B_i(z)\bmod P_{полн}(z), \quad (7)$$

где $B_i(z)\equiv 1 \bmod p_i(z)$ – ортогональный базис i-го основания ПСКВ; k – количество информационных оснований; r – количество контрольных оснований.

Представив ортогональные базисы в виде коэффициентов ОПС, получаем

$$A=\alpha_1\left[\gamma_1^1,\gamma_2^1,...,\gamma_{k+r}^1\right]+...$$
$$+\alpha_{k+r}\left[0,\quad 0,...,\quad \gamma_{k+r}^{k+r}\right], \quad (8)$$

где γ_i^j – коэффициенты ОПС j-го ортогонального базиса.

Тогда, проведя умножение вычетов α_i на соответствующие коэффициенты ОПС помодульно и поразрядно, при этом, учитывая превышение модуля $p_i(z)$ как перенос единицы при суммировании результата, коэффициенты ОПС могут быть найдены

$$a_i=\left|\sum_{j=1}^{i}\ \left|\alpha_j(z)\gamma^j(z)\right|^{+}_{p_i(z)}\right|^{+}_{p_i(z)}+$$

$$+\delta_{i-1}(z)\Big|^{+}_{p_i(z)}, \quad (9)$$

где $\delta_{i-1}(z)$ – переполнение, полученное при суммировании по модулю $p_{i-1}(z)$.

Одним из важнейших свойств кодов ПСКВ, определенных в расширенных полях Галуа $GF(p^v)$, является отсутствие межразрядных переносов при вычислении результата по модулю $p_i(z)$. Это позволяет свести операцию итеративного получения коэффициентов обобщенной полиадической системы к однотактовой процедуре, определяемой выражением

$$a_i(z)=\left|\sum_{j=1}^{i}\ \alpha_j(z)\gamma^j(z)\right|^{+}_{p_i(z)}\Bigg|^{+}_{p_i(z)}, \quad (10)$$

где $i = 1,2, \ldots, n$ – количество оснований кода ПСКВ.

На базе данного алгоритма был разработан преобразователь, который осуществляет параллельное вычисление коэффициентов смешанной системы счисления, реализованное с помощью нейроподобных вычислительных устройств [6]. При этом характерной чертой патентованного устройства является то, что не только обнаруживает и корректирует ошибки, но и осуществляет обратное преобразование из непозиционного кода ПСКВ в позиционный двоичный код.

Предложено для реализации данной процедуры использовать коэффициенты обобщенной полиадической системы (ОПС). Разработана нейронная сеть, позволяющая осуществлять преобразование ПСКВ-ОПС, для поля Галуа $GF(2^4)$, с основаниями $p_1(z)=z+1; p_2(z)=z^2+z+1; p_3(z)=z^4+z^3+z^2+z+1; p_4(z)=z^4+z^3+1; p_5(z)=z^4+z+1$. Тогда ортогональные базисы ПСКВ, представленные в ОПС равны:

$$B_1(z)=z^{14}+z^{13}+z^{12}+z^{11}+z^{10}+z^9+z^8+z^7+z^6+z^5+$$
$$+z^4+z^3+z^2+z+1=[1\ z\ z^3+z\ z^3\ z^3+z^2+z];$$
$$B_2(z)=z^{14}+z^{13}+z^{11}+z^{10}+z^8+z^7+z^5+z^4+z^2+z=$$
$$=[0\ z\ z^3+z^2+z\ z^3+z^2+1\ z^3+z^2];$$
$$B_3(z)=z^{14}+z^{13}+z^{12}+z^{11}+z^9+z^8+z^7+z^6+z^4+z^3+$$
$$+z^2+z=[0\ 0\ z^2+z+z\ z^2+1\ z^3+z^2+z];$$
$$B_4(z)=z^{14}+z^{13}+z^{12}+z^{11}+z^9+z^7+z^6+z^3=$$
$$=[0\ 0\ 0\ z^2+z\ z^3+z^2+z];$$
$$B_5(z)=z^{12}+z^9+z^8+z^6+z^4+z^3+z^2+z=[0\ 0\ 0\ 0\ z]..$$

Пусть дан полином

$$A(z)= z^6+z^5+z^4+z+1=$$
$$=(1,\ z+1,\ z^3+z^2+z+1,\ z^3+z^2+z,\ z^3+z),$$

принадлежащий

$$P_{раб}(z)=z^7+z^6+z^5+z^2+z+1.$$

Воспользуемся выражением (10). Получаем значения коэффициентов ОПС

$$a_1(z)=1,\ a_2(z)=z+1,$$
$$a_3(z)=z^3+z^2+z+1,\ a_4(z)=0,\ a_5(z)=0.$$

Так как старшие коэффициенты равны нулю, то это свидетельствует о том, что данный полином не содержит ошибки.

Пусть в коде ПСКВ произошла ошибка по первому основанию и ее глубина $\Delta\alpha_1(z)=1$.

Тогда $A^*(z)=(0,\ z+1,\ z^3+z^2+z+1,\ z^3+z^2+z,\ z^3+z)$.

Воспользуемся выражением (10) и вычислим значения коэффициентов ОПС. В результате старшие коэффициенты ОПС равны соответственно

$$a_4(z)=z^3 \text{ и } a_5(z)=z^3+z^2+z.$$

Таким образом, очевидно, что кодограмма ПСКВ содержит ошибку.

В таблице 1 приведены значения старших коэффициентов ОПС при различных однократных ошибках для выбранного набора оснований ПСКВ.

Таблица 1

Зависимость коэффициентов ОПС от ошибки

Величина ошибки	Коэффициенты ОПС	
	$a_4(z)$	$a_5(z)$
$\Delta\alpha_1 = 1$	z^3	$z^3 + z^2 + z$
$\Delta\alpha_2 = 1$	$z^3 + z + 1$	$z^3 + z^2$
$\Delta\alpha_2 = z$	$z^3 + z^2 + z$	$z^3 + z$
$\Delta\alpha_3 = 1$	$z^2 + 1$	$z^3 + z^2 + z$
$\Delta\alpha_3 = z$	$z^3 + z$	$z^3 + z^2 + z + 1$
$\Delta\alpha_3 = z^2$	$z^3 + z^2$	$z^3 + z^2$
$\Delta\alpha_3 = z^3$	1	$z^3 + z$
$\Delta\alpha_4 = 1$	$z^2 + z$	$z^3 + z^2 + z$
$\Delta\alpha_4 = z$	$z^3 + z^2$	$z^3 + z^2 + z + 1$
$\Delta\alpha_4 = z^2$	1	$z^3 + z^2$
$\Delta\alpha_4 = z^3$	z	$z^3 + z + 1$
$\Delta\alpha_5 = 1$	0	z
$\Delta\alpha_5 = z$	0	z^2
$\Delta\alpha_5 = z^2$	0	z^3
$\Delta\alpha_5 = z^3$	0	$z + 1$

Анализ таблицы 1 показывает, что в выбранной системе оснований ПСКВ с двумя контрольными основаниями можно однозначно определить местоположение и глубину ошибки в модулярном коде. При этом характерной чертой данной позиционной характеристики является то, что она может одновременно использоваться при переводе из ПСКВ в позиционный код. Таким образом, при реализации непозиционного СП ЦОС, который используется в СКУД, можно обеспечить сокращение схемных затрат по сравнению с классическим алгоритмом перевода.

Вывод

Современные системы контроля и управления доступом широко используют биометрические средства идентификации и аутентификации пользователя. Повысить эффективность их работы можно за счет применения алгоритмов ЦОС, реализованных в полиномиальной системе классов вычетов. В работе показана возможность осуществления поиска коррекции ошибок на основе коэффициентов обобщенной полиадической системы. Применение данной позиционной характеристики позволяет сократить схемные затраты по сравнению с классической реализацией СП ЦОС класса вычетов за счет совмещения операций обратного перевода в ПСС и процедур поиска и коррекции ошибок.

Список литературы

1. Гахов В.Р., Емарлукова Я.В., Калмыков И.А. Устройство обнаружения и коррекции ошибок в кодах полиномиальной системы классов вычетов // Патент России № 2300801. 30.06.2005. Бюл. № 16 от 10.06.2007.

2. Емарлукова Я.В., Калмыков И.А., Зиновьев А.В. Высокоскоростные систолические отказоустойчивые процессоры цифровой обработки сигналов для инфо-

телекоммуникационных систем // Инфокоммуникационные технологии. Самара. – 2009. – №2. – С. 31-37.

3. Калмыков И.А., Бережной В.В., Червяков Н.И., Щелкунова Ю.О., Шилов А.А. Нейросетевая реализация в полиномиальной системе классов вычетов операций ЦОС повышенной разрядности // Нейрокомпьютеры: разработка и применение. – 2004. – № 5-6. – С. 94.

4. Калмыков И.А., Бережной В.В., Червяков Н.И., Щелкунова Ю.О., Шилов А.А. Архитектура отказоустойчивой нейронной сети для цифровой обработки сигналов // Нейрокомпьютеры: разработка и применение. – 2004. – № 12. – С. 51-57.

5. Калмыков И.А., Чипига А.Ф. Структура нейронной сети для реализации цифровой обработки сигналов повышенной разрядности // Вестник Ставропольского государственного университета. – 2004. – Т.38. – С. 46.

6. Калмыков И.А., Лободин М.В., Алексишин Е.В., Щелкунова Ю.О. Нейронная сеть для вычисления коэффициентов обобщенной полиадической системы, представленных в расширенных полях Галуа GF(2^v) // Патент России № 2258956. Бюл. № 23 от 20.08.2005.

7. Лободин М.В., Чипига А.А., Калмыков И.А. Устройство спектрального обнаружения и коррекции в кодах полиномиальной системы классов вычетов // Патент России № 2301441. Бюл. № 17 от 20.06.2007.

8. Петлеванный С.В., Калмыков И.А., Сагдеев А.К., Емарлукова Я.В. Устройство для преобразования числа из полиномиальной системы классов вычетов в позиционный код с коррекцией ошибки // Патент России № 2309535. 31.03.2006. Бюл. № 30 от 27.10.2007.

9. Хайватов А.Б., Калмыков И.А. Математическая модель отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов // Инфокоммуникационные технологии. – 2007. – Т.5. – №3. – С.39-42.

10. Червяков Н.И., Калмыков И.А., Щелкунова Ю.О., Бережной В.В. Математическая модель нейронной сети для коррекции ошибок в непозиционном коде расширенного поля Галуа // Нейрокомпьютеры: разработка и применение. – 2003. – № 8-9. – С. 10-17.