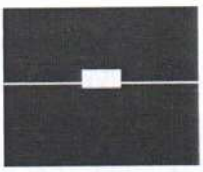

ПОРТФЕЛЬ РЕДАКЦИИ

БИТ

V.I. Vasilyev, E.V. Buraya

Recognition Errors Control In Biometric Identification Cryptosystems

Keywords: biometric encryption, fingerprint, fuzzy extractor

The method of biometric cryptosystem design on the basis of fuzzy extractor, in which main disadvantages of biometric and cryptographic systems are absent, is considered. The main idea of this work is a control of identity recognition errors with use of fuzzy extractor, which operates with Reed-Solomon correcting code. The fingerprint features vector is considered as a biometric user identifier.

В.И. Васильев, Е.В. Бурая

УПРАВЛЕНИЕ ОШИБКАМИ РАСПОЗНАВАНИЯ В БИОМЕТРИЧЕСКИХ КРИПТОСИСТЕМАХ

Введение

Надежная авторизация и аутентификация личности становятся необходимыми атрибутами повседневной жизни: сегодня люди используют их при совершении самых обычных действий, например, при посадке на самолет, проведении финансовых операций. Вместе с тем, верификация личности становится трудной задачей, когда требуется высокая точность распознавания, т.е. низкая вероятность ошибок принятия решений [1].

В общем случае, к преимуществам использования биометрических параметров относятся [2]:

- избавление от необходимости использования кодов и паролей, которые имеют большое количество потерь (до 30%);
- практически невозможное использование их третьими лицами;
- доступность применения в любом возрасте, отсутствие языковых барьеров;
- высокая доказательность доступа к информационным ресурсам;
- фиксирование биометрического портрета злоумышленника.

Однако у биометрических систем есть также ряд недостатков [2]:

- значительные ошибки распознавания;
- большое время аутентификации и идентификации;
- сложность и индивидуальность используемых технических средств.

На практике в биометрических системах возникают такие проблемы, как обработка персональных биометрических данных в открытых системах. В такой ситуации злоумышленник может легко манипулировать биометрической базой данных. Выходом из сложившейся ситуации послужило бы шифрование, т.е. использование криптографических систем. Но при этом появляются проблемы, связанные с необходимостью создания и хранения ключа, передачей ключа и т.п. [3].

Вышеперечисленные проблемы, наоборот, отсутствуют в биометрических системах. Универсальным решением было бы создание гибридной системы, в которой объединялись преимущества биометрических и криптографических систем. Однако биометрические идентификаторы не постоянны, что делает невозможным применение к ним каких-либо алгоритмов шифрования без использования специальных технологий, которые так и называются – механизмы биометрической криптографии [4].

Существует много механизмов биометрической криптографии, из которых в данной работе рассматривается только один – нечеткий экстрактор(fuzzyextractor). Использование данного механизма биометрической криптографии дает возможность управления ошибками распознавания, так как применение нечеткого экстрактора не только решает проблему обработки персональных данных в открытых системах, но и обеспечивает устойчивое кодирование биометрических шаблонов. Все это позволит существенно уменьшить ошибки первого и второго рода при определенных настройках корректирующего кода, лежащего в основе построения нечеткого экстрактора.

В следующем разделе статьи рассматриваются уязвимые места биометрической системы во время регистрации нового пользователя. Дается перечисление возможных решений для защиты уязвимых мест. Далее излагается идея управления ошибками распознавания и дается описание выбранного способа защиты биометрических идентификаторов, а именно, построение биометрической системы на основе нечеткого экстрактора. И в заключение представлены проведенные эксперименты, доказывающие возможность управления параметрами рабочей характеристики приемного устройства (РХПУ) – в частности, блока сравнения шаблонов биометрической системы с помощью предложенного способа, а значит, и возможность управления ошибками распознавания.

Уязвимости биометрической системы

На рис. 1 представлена схема обобщенной биометрической системы и уязвимые места (точки) регистрационной подсистемы.

Биометрическая система рассматривается в данном случае как система распознавания шаблонов [1], состоящая из двух подсистем:

- аутентификационная система;
- регистрационная система.

Аутентификационная система состоит из четырех частей (блоков):

- блок получения образца биометрического идентификатора с помощью сенсора;
- блок обработки биометрического образца для получения вектора информационных признаков пользователя;
- блок сравнения шаблонов между собой, а именно, оценки сходства шаблона вводимого образца с ранее зарегистрированными шаблонами, хранимыми в базе данных шаблонов;
- приложение, с которым работает пользователь.

Регистрационная система, в свою очередь, состоит из двух частей:

- блок, осуществляющий регистрацию нового пользователя (регистрация);
- база данных зарегистрированных шаблонов.

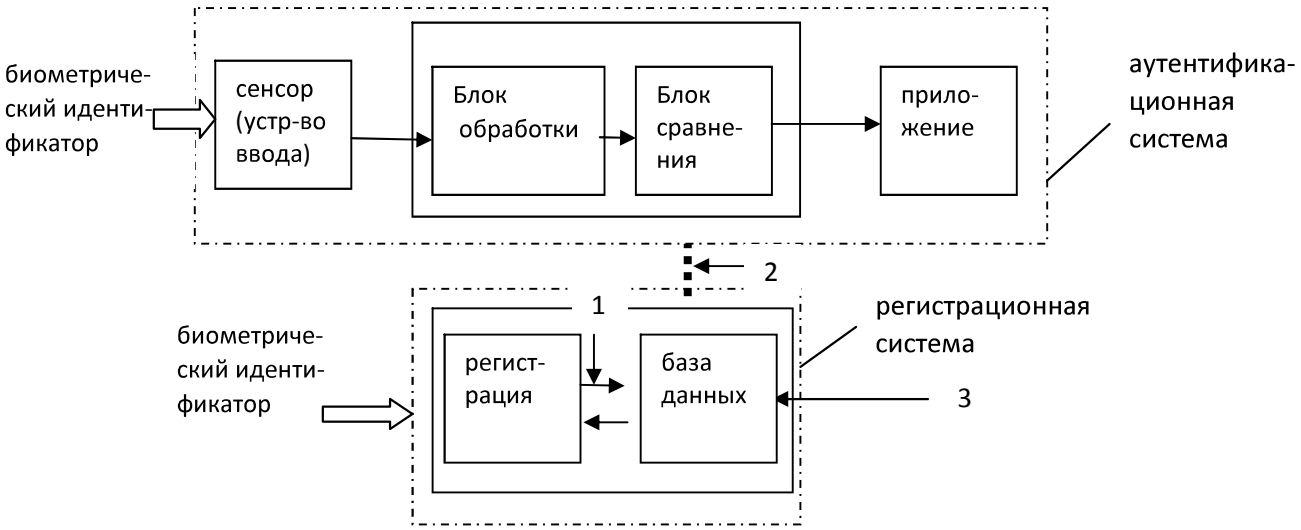

Рис. 1. Обобщенная биометрическая система

Процессы регистрации и создания базы данных представляют собой важную для биометрической системы функцию – регистрацию подходящих объектов или создание списка контроля доступа. «Чистота» базы данных крайне важна, так как сама аутентификационная система настолько безопасна, насколько безопасна используемая база данных [1]. Здесь можно выделить три возможные точки атаки:

1 – канал передачи зарегистрированных данных (шаблонов) в базу данных;

2 – канал связи базы данных с аутентификационной системой;

3 – база данных зарегистрированных пользователей.

В данной работе рассматривается только точка атаки 3, т.е. база данных биометрических шаблонов.

Чтобы избежать атак на биометрическую базу данных, на сегодняшний день предложено несколько способов ее защиты:

- шифрование биометрических образов;
- использование нескольких идентификаторов и т.д.

В данной статье в качестве способа защиты будет рассматриваться шифрование биометрических идентификаторов с использованием механизма биометрической криптографии – нечеткого экстрактора.

Управление ошибками распознавания с помощью нечеткого экстрактора

Управление ошибками распознавания

Для оценки ошибок распознавания необходимо определить меру сходства между биометрическими шаблонами пользователей. Такую метрику можно подсчитать, например, с помощью расстояния Хемминга – это доля отличающихся битов в двух бинарных строках, являющихся информационными векторами биометрических идентификаторов (шаблонов). Расстояние Хемминга подсчитывается при этом для шаблонов зарегистрированного (легального) пользователя (V) и для шаблонов, принадлежащих другим пользователям(V'):

$$D(V,V') = \frac{1}{N}\sum_{j=1}^{N}\left|V_j - V_j'\right|, \quad (1)$$

где N – размерность (длина) биометрического вектора.

Для разделения пользователей на два класса – зарегистрированных (Authentic) и злоумышленников (Intruder) – используется следующее правило (2):

V є Intruder, если D≥C,

или V є Authentic, если D<C; (2)

где V – биометрический вектор (шаблон) пользователя;
D – мера сходства шаблонов,
C – критерий принятия решений (порог).

На рис. 2 показаны плотности распределения вероятностей для зарегистрированного пользователя (ψ_{au}) и для злоумышленника (т.е. незарегистрированного пользователя) (ψ_{im}). Области пересечения, обозначенные как FalseRejectRate (FRR) и FalseAcceptRate (FAR), являются ошибками распознавания соответственно первого и второго рода. Площади этих областей пересечения, а значит, и значения ошибок распознавания зависят от выбора порогового значения (C), основываясь на котором, биометрическая система принимает решение о совпадении биометрических образцов (шаблонов). Взаимозависимость ошибок распознавания можно показать с помощью рабочей характеристики приемного устройства (РХПУ), координатами которой являются значения указанных ошибок 1-го и 2-го рода:

$$FRR = \int_C^1 \psi_{au}(D)dD, \quad (3)$$

$$FAR = \int_0^C \psi_{im}(D)dD. \quad (4)$$

Так как применение рассмотренного далее нечеткого экстрактора в биометрической системе позволяет уменьшить расстояние Хемминга для шаблонов подлинного пользователя, а для шаблонов злоумышленника – оставить это расстояние постоянным, то в результате ошибки распознавания будут уменьшены.

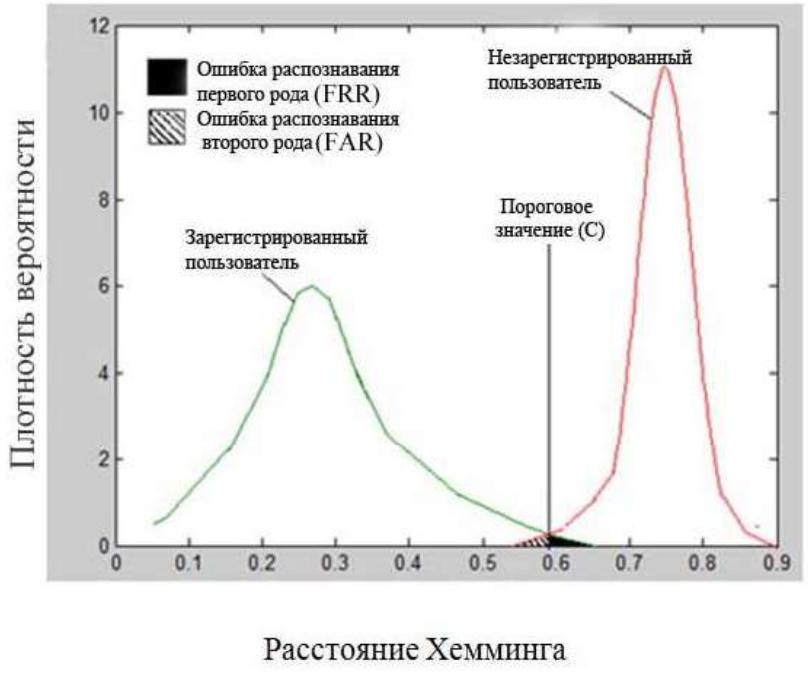

Рис. 2. Плотности распределения вероятностей для различных групп шаблонов

Нечеткий экстрактор

Суть нечеткого экстрактора заключается в том, что он позволяет извлечь случайную равномерно распределенную последовательность символов (секретный ключ) из первоначальных биометрических данных и далее однозначно восстанавливает ее из любых входных данных, достаточно схожих с первоначальными. Для воспроизведения секретного ключа при этом требуются дополнительные открытые данные (открытый ключ), соответствующие этому ключу, которые хранятся в памяти.

Общая схема построения нечеткого экстрактора приведена на рис. 3.

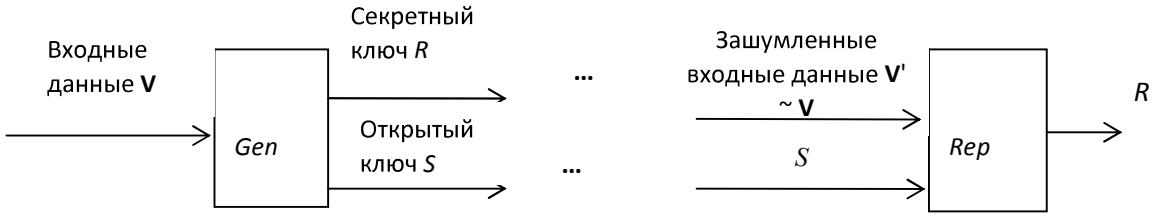

Рис. 3. Схема построения нечеткого экстрактора

Блоки, представленные на рис. 3, выполняют следующие функции:

- *Gen* (от англ. *Generation*) – генерация защищенного биометрического шаблона пользователя, включающая в себя формирование ключей *R* и *S* по предъявленным системе биометрическим данным;

- *Rep (*от англ.*Reproduction)* – воспроизведение секретного ключа *R*' по известному открытому ключу для зашумленных (**V**') входных данных.

Заметим, что качество нечетких экстракторов во многом определяется качеством применяемых в них корректирующих кодов, обнаруживающих и исправляющих ошибки, поэтому выбор эффективного метода кодирования и параметров этих кодов занимает в данном случае одно из центральных мест [3]. Возможность нечеткого экстрактора восстанавливать шаблоны биометрических идентификаторов позволяет не только шифровать биометрические шаблоны, но и управлять ошибками распознавания.

Эксперименты

Предложенный нечеткий экстрактор состоит из кодера и декодера Рида-Соломона. В нашем случае нечеткий экстрактор использует код Рида-Соломона (8,4). Такой код работает в поле Галуа GF(2^9) и способен исправить до 3-х тетроидов из 9-ти. В качестве биометрических признаков используются отпечатки пальцев, взятые из открытой базы данных FVC2002 DB1_B[5].

В табл. 1 на примере одного пользователя (подлинный пользователь) показаны:

- в строке «Исходный блок сравнения» – подсчитанные расстояния Хемминга для образов данного пользователя при условии, что образ отпечатка 101_1 выступает в качестве зарегистрированного признака;

- в строке «Полученный блок сравнения» – подсчитанные расстояния Хемминга для блока сравнения шаблонов, построенного на основе нечеткого экстрактора (образы отпечатков пальцев те же).

Таблица 1. Расстояние Хемминга для шаблонов одного пользователя

	101_2	101_3	101_4	101_5	101_6	101_7
Исходный блок сравнения шаблонов	0,423	0,320	0,310	0,287	0,260	0,220
Полученный блок сравнения шаблонов	0,035	0,228	0,284	0,329	0,353	0,456

В табл. 2 приведены результаты расчета расстояния Хемминга для образов других пользователей при условии, что зарегистрированным образом остается 101_1.

Таблица 2. Расстояние Хемминга для шаблонов разных пользователей

	102_1	103_1	104_1	105_1	106_1	107_1
Исходный блок сравнения шаблонов	0,197	0,245	0,232	0,229	0,246	0,199
Полученный блок сравнения шаблонов	0,216	0,298	0,268	0,284	0,287	0,280

На основе полученных данных были построены РХПУ для исходного блока сравнения шаблонов и для блока сравнения на основе нечеткого экстрактора (рис. 4).

Из рис. 4 видно, что РХПУ блока сравнения шаблонов, построенного на основе нечеткого экстрактора, расположена значительно ниже, чем РХПУ исходного блока сравнения шаблонов. В рассматриваемом примере для конкретного набора пользователей ошибка первого рода (FRR) в среднем уменьшилась на 13%, а ошибка второго рода (FAR) – на 33,3%.

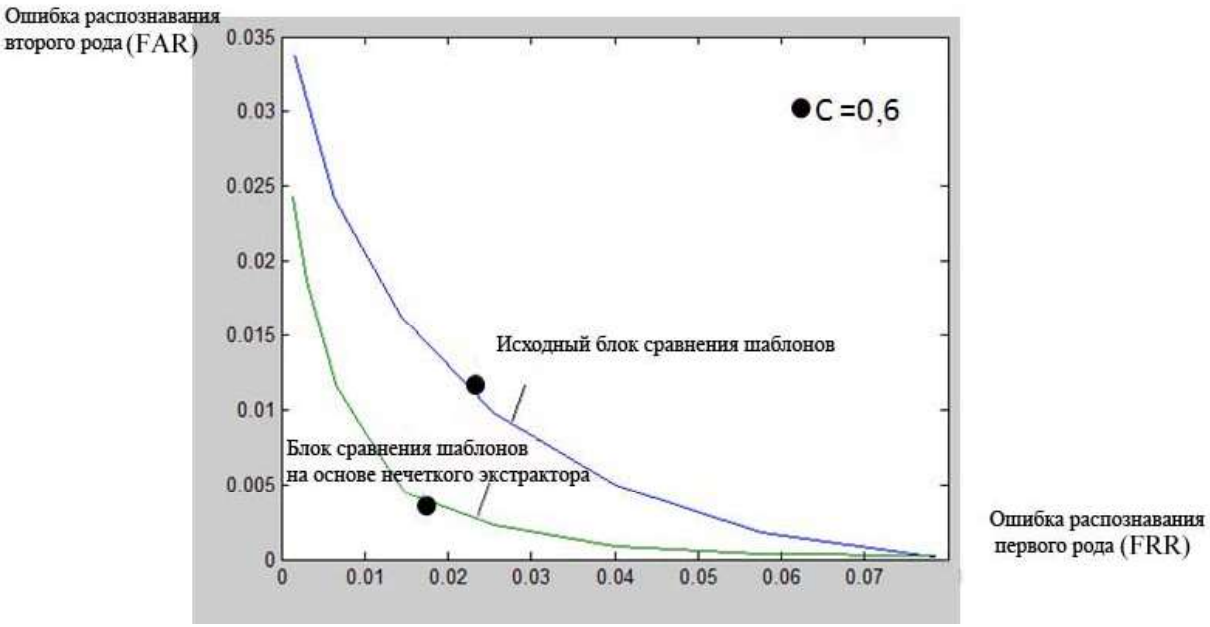

Рис. 4. РХПУ исходного блока сравнения шаблонов и блока сравнения шаблонов на основе нечеткого экстрактора

Вместе с тем, необходимо отметить, что рассмотренный нечеткий экстрактор представляет собой подсистему блока сравнения шаблонов биометрической системы,

использование которой позволит увеличить не только уровень защищенности системы, но и время верификации. В расчете на одноядерный процессор с тактовой частотой 2,5 ГГц время верификации для блока сравнения шаблонов, построенного на основе нечеткого экстрактора, составляет в среднем 52,4 мс, тогда как для исходного блока сравнения шаблонов – 32 мс, т.е. производительность падает в среднем на 38%.

Заключение

Достижение требуемой точности биометрической системы на данный момент является одной из самых актуальных проблем в области биометрии. Одно из возможных решений – поиск нужного нечеткого экстрактора и его адаптация под конкретный биометрический признак.

Рассмотренный нечеткий экстрактор демонстрирует устойчивое кодирование непостоянных биометрических данных. Уровень ошибок распознавания первого и второго рода в рассмотренном примере при этом уменьшается на 13 и 33,3% соответственно, что компенсирует снижение на 38% производительности системы.

Данный нечеткий экстрактор обладает возможностью гибкой настройки корректирующих кодов, что позволяет при необходимости изменить его характеристики. Это, в свою очередь, дает возможность изменить допустимую степень восстановления биометрических шаблонов, а значит, манипулировать ошибками распознавания, которые и являются показателями качества биометрии.

СПИСОК ЛИТЕРАТУРЫ:

1. Болл Руд М., М. Болл Руд, Х. Коннел Джонатан, Ш. Панканти, К. Налини Ратха, У. Сеньор Эндрю. Руководство по биометрии – М.: Техносфера, 2007. – 368 с.
2. Брюхомицкий, Ю.А. Вероятностный метод классификации биометрических параметров личности // Материалы X Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2008. – 318 с.
3. Васильев, В.И., В. И. Васильев. Интеллектуальные системы защиты информации: учеб. пособие. – М.: Машиностроение, 2012. – 199 с.
4. Stan, Z. Li Encyclopedia of Biometrics, Berlin, SpringerScience+Business Media, 2009.
5.Set «B» ofDatabase 1 [Электронный ресурс]. URL: http://bias.csr.unibo.ithttp://bias.csr.unibo.it /fvc2002/download.asp (дата обращения: 3.11.2014).

REFERENCES:

1. Bolle R. M., Connel J.H., Pankanti Sh., Ratha N. K., Senior A. W. Guide to Biometrics, Springer – Verlag, N.Y., Inc., 2004.
2. Bryukhomitsky Yu. A. Probabilistic method of identity's biometric parameters classification, Proc.of X Intern. Scientific-practical conference «Information Security», Part I, Taganrog, TTI YuFU Pub., 2008. (In Russian).
3. Vasilyev V.I. Intelligent information security systems, Moscow, Mashinostroyenie Pub., 2012.(In Russian).
4. Stan, Z. Li Encyclopedia of Biometrics, Berlin, Springer Science+Business Media, 2009.
5. Set «B» ofDatabase1. URL:http://bias.csr.unibo.ithttp://bias.csr.unibo.it /fvc2002/download.asp.