Теоретический и прикладной научно-технический журнал

ISSN 1694-5557

ИЗВЕСТИЯ

Кыргызского государственного технического университета им. И. Раззакова

2017
№ 1 (41) часть II

Бишкек

Издательский центр «Техник» 2017

Содержание

«Известия КГТУ им.И.Раззакова» № 1 (41) часть 2

ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 004.93:612.087.1

ТЕХНОЛОГИИ РАСПОЗНАВАНИЯ ОБРАЗОВ С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИИ ЛИЧНОСТИ

Алимсеитова Жулдыз, *аспирант КГТУ им. И. Раззакова Кыргызской Республики +7 777 359 81 05, E-mail: zhuldyz_al@mail.ru*
Боскебеев Калычбек Джетмишбаевич, *кандидат технических наук, профессор кафедры ИСЭ КГТУ им. И. Раззакова Кыргызской Республики, (+996) 56-13-15. E-mail: kboskebeev@mail.ru*

В статье рассматриваются технологии распознавания образов с использование биометрии личности. Быстрый рост электронных платежей и электронного документооборота остро ставит вопрос аутентификации участников процесса. Каждая из сторон должна быть уверенна в истинности друг друга. Чтобы исключить возможность подмены участников процесса все чаще используется биометрия личности. Биометрия личности используется также в паспортах, в поисках преступников. Для этих целей в статье рассмотрены аутентификационные методы используемые в биометрии. Для использования биометрии личности нужно выбрать параметр или несколько параметров, которые будут использоваться в распознавании. В статье рассмотрены и проклассифицированы биометрические параметры, их свойства, а также возможности их совместного использования.

Ключевые слова: биометрия, идентификация, аутентификация, верификация, шаблон, биометрический параметр, мультибиометрия, биометрическая характеристика.

TECHNOLOGIES OF RECOGNITION OF IMAGES WITH USE OF BIOMETRICS OF THE PERSONALITY

Alimseitova Zhuldyz, *the graduate student of KGTU of I. Razzakov of the Kyrgyz Republic +7 777 359 81 05, E-mail: zhuldyz_al@mail.ru*
Boskebeev Kalychbek Dzhetmishbaevich, *Ph.D., professor of the Department of ISE. Kyrgyz State Technical University named after I. Razzakov,Tel.: (+996) 56-13-15. E-mail: kboskebeev@mail.ru*

In article technologies of recognition of images about use of biometrics of the personality are considered. Rapid growth of electronic payments and electronic document flow sharply puts a question of authentication of participants of process. Each of the parties shall be confident in the validity of each other. To exclude a possibility of substitution of participants of process the biometrics of the personality even more often is used. The biometrics of the personality is used also in passports, in search of criminals. For these purposes in article the authentication methods used in biometrics are considered. For use of biometrics of the personality it is necessary to choose the parameter or several parameters which will be used in recognition. In article also proklassifitsirovana biometric parameters, their properties, and also possibilities of their joint use are considered.

Keywords: biometrics, identification, authentication, verification, template, biometric parameter, multibiometrics, biometric characteristic.

В связи с быстрым развитием информационных технологий и их широким использованием вопрос аутентификации личности стоит все острее. На сегодняшний день все

больше операций производится через Интернет, это оплата услуг, обмен документами и другое. И получатель и отправитель должны быть уверены в друг друге. Распознавание людей - это вид деятельности, который составляет основу нашего общества и культуры, так как для многих видов приложений необходимым условием является гарантия идентичности личности и ее авторизация. Для этого используют различные механизмы. Все они имеют свои достоинства и недостатки. Самый распространенный недостаток утеря или компрометация идентификатора. Для решения этого вопроса предлагается в качестве идентификатора использовать биометрию личности, то есть то, что неотъемлемо от человека и не возможно потерять.

Биометрическая идентификация, или биометрия, основана на идентификации отличительных признаков человека. Точнее, биометрия - это наука об идентификации или верификации личности по физиологическим или поведенческим отличительным характеристикам.

В биометрии различают два аутентификационных метода [1]:

1. Верификация - основана на уникальном идентификаторе и на биометрическом параметре. Уникальный идентификатор выделяет конкретного человека (например, идентификационный номер). То есть этот метод основан на комбинации аутентификационных приемов.

2. Идентификация - основана только на биометрических измерениях. При этом измеренные параметры сравниваются со всеми записями из базы зарегистрированных пользователей, а не с одной, выбранной на основании какого-либо идентификатора.

Для биометрической идентификации используются только биометрические характеристики (удостоверяющие данные). Такая система связана с биометрической базой данных (справа), содержащей биометрические образцы или репрезентации биометрических образцов (называемые шаблонами) [1].

Биометрическая система идентификации способна вести поиск по базе данных, чтобы определить, есть ли в ней шаблоны, имеющие сходства с тем биометрическим параметром, который ввел объект. Эта функция представлена в среднем блоке рисунка 1. Шаблоны из базы данных сравниваются с представленным образцом по очереди. В конце процедуры система выдает список идентификаторов, которые имеют сходство с введенным биометрическим параметром.

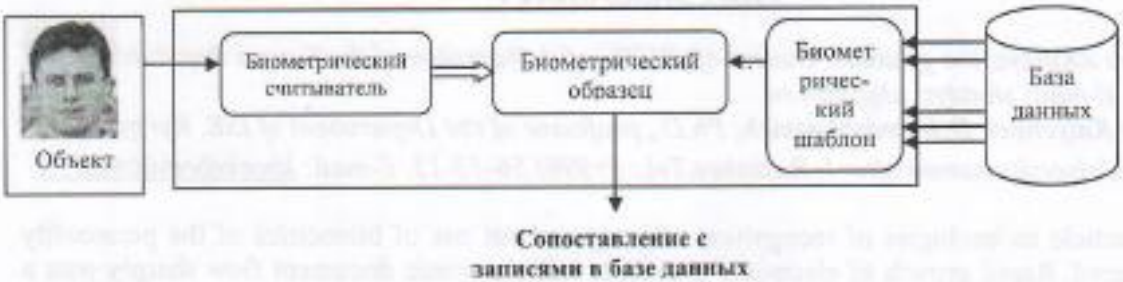

Рисунок 1- Биометрическая идентификация

Такая биометрическая система идентификации может работать в двух режимах [1]:

- положительная идентификация. Система определяет, зарегистрирована ли данная личность в базе данных. При этом могут быть допущены ошибки ложного доступа или ложного отказа доступа.

- отрицательная идентификация. Система проверяет отсутствие объекта в некоторой отрицательной базе данных. Это может быть, например, база данных разыскиваемых преступников. При этом могут возникнуть ошибки пропуска сходства - ложное отрицание, и ошибки ложного определения сходства - ложное признание.

Биометрическая система идентификации может находить в базе данных несколько кандидатов, имеющих сходство с объектом. При положительной идентификации требуется, чтобы в списке кандидатов был только один человек или, по крайней мере, чтобы количество

кандидатов можно было уменьшить до одного. При негативной идентификации желательно, чтобы список кандидатов был небольшим для удобства его обработки оператором.

Биометрическая верификация отличается от идентификации тем, что представленные биометрические образцы сопоставляются с одной зарегистрированной записью в базе данных. Сама база данных может быть большой, но пользователь предоставляет что-либо, что указывает на один биометрический шаблон из базы данных. Сопоставление можно провести двумя способами, которые изображены на рисунке 2.

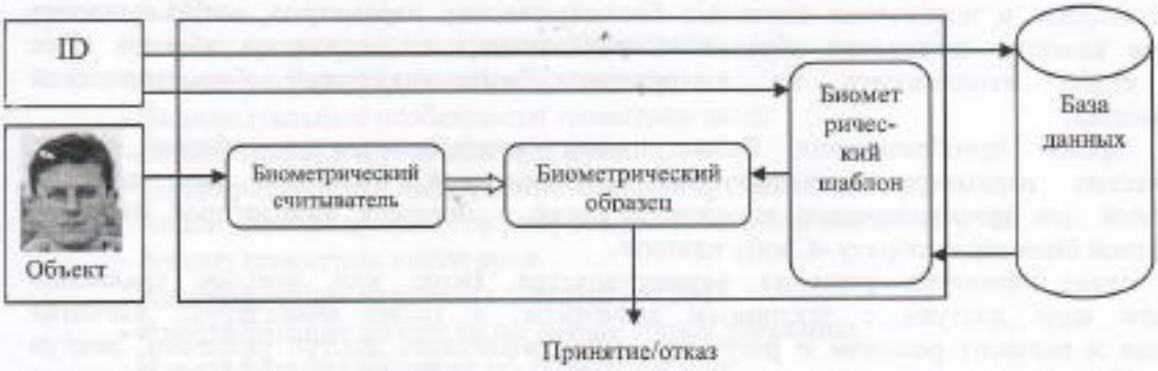

Рисунок 2 - Биометрическая верификация

Как и система идентификации, система верификации имеет доступ к базе данных (справа). Эта база содержит биометрические шаблоны, связанные с объектами. Однако, в отличие от биометрической идентификации, здесь с каждым биометрическим шаблоном связывается уникальный идентификатор. Следовательно, биометрический шаблон, ассоциированный с определенной личностью, легко найти в базе данных по связанному с ним уникальному идентификатору. Система верификации требует предоставления биометрического образца объекта в дополнение к какому-то идентификатору, связанного с личностью, за которую выдает себя объект. После сравнения биометрического шаблона из базы данных, определенного с помощью предоставленного объектом уникального идентификатора, и биометрического образца система принимает решение о принятии/отказе [1].

Рассмотрев вышеприведенные системы биометрической идентификации и верификации можно увидеть, что у каждой из них есть недостатки. Если в системе идентификации необходимо сопоставление со всеми записями в базе данных, то в системе верификации требуется введение уникального идентификатора.

Исходя из этого предлагается использовать модель высоконадежной биометрической аутентификации, приведенной на рисунке 3.

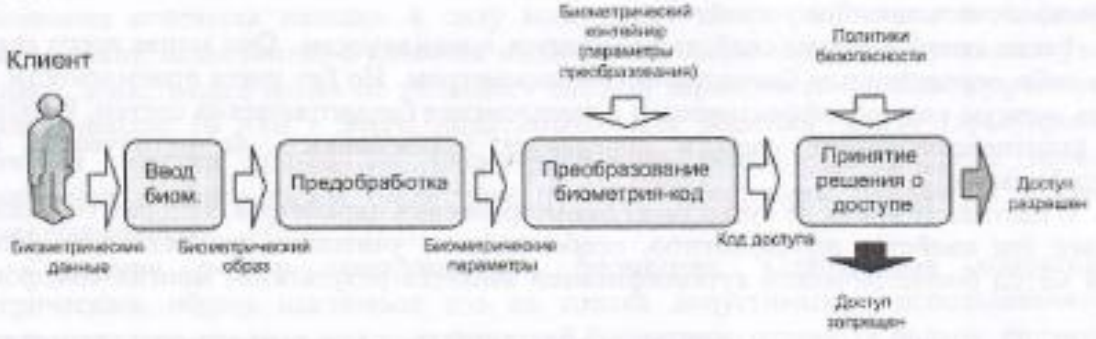

Рисунок 3 - Модель высоконадежной биометрической аутентификации

–Поддержка нескольких вариантов аутентификации. Применением нескольких альтернативных биометрических технологий аутентификации можно избежать потери авторизации в случае временной утраты способности ввода биометрии (например, в случае пореза пальца или «потери» голоса во время болезни). Запасной вариант аутентификации позволит выполнять операции в полном объеме без необходимости блокировки счета после компрометации части тайных биометрических образов или PIN-кодов. В этом случае клиенту достаточно заявить о потере возможности выполнения аутентификации одним или несколькими способами, а банк должен выполнить их блокировку. Альтернативные варианты аутентификации позволяют также реализовать совместное использование одного банковского счета супругами. В настоящий момент совместное использование карточного счета реализуется через выпуск нескольких идентичных копий пластиковых карт для одного счета.

–Поддержка нескольких участников. Ряд протоколов аутентификации требует использования нескольких ключей, хранимых отдельно друг от друга. Связь составных частей ключа с отдельными биометрическими образами позволяет использовать различные схемы объединения и контроля доступа со стороны третьих лиц или организаций. Важно отметить, что в случае биометрической авторизации передать полномочия на выполнение банковских операций намного сложнее, чем в случае с электронными носителями кодов доступа или PIN-кодов.

–Поддержка схем разделения секрета. При необходимости с помощью биометрии может быть выполнено связывание с частями секретов, распределенных между несколькими участниками процесса биометрической аутентификации.

–Сохранение требований безопасности к мультибиометрическому преобразователю по сохранению тайны выходного кода и биометрических данных, требований по их уничтожению после завершения обучения, сложность организации атак с использованием хранимых параметров возможны только при выполнении требований пакета стандартов ГОСТ Р 52633 при разработке подсистемы биометрической авторизации участников платежных операций.

Выводы:

-модель высоконадежной биометрической аутентификации решает недостатки биометрической системы идентификации и верификации;

-рассмотрены виды биометрических параметров и их свойства, которые показывают, что применение мультибиометрических систем имеют большие перспективы.

Список литературы

1. Болл Р. М., Коннен Дж. Х., Панканти Ш., Ратха Н. К., Сеньор Э. У. Руководство по биометрии. М.: Техносфера, 2007. – 368 с.

2. ГОСТ Р ИСО/МЭК 19794-2-2005. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Ч.2. Данные изображения отпечатка пальца – контрольные точки. – М.: Стандартинформ, 2006. – 42 с.

3. Иванов, А.И. Прогнозирование уровня защищенности, обеспечиваемого папиллярным рисунком отпечатка пальца / А.И. Иванов, Д.А. Фунтиков, С.Л. Агафонов // Современные технологии безопасности. – 2005. – №3 (14). – С. 36-37.

4. Кухарев, Г.А. Биометрические системы: методы и средства идентификации личности человека / Г.А. Кухарев. – СПб.: Политехника, 2001. – 240 с

5. Akhmetov B.S., Ivanov A.I., Kartbaev T.S., Malygin A.U., Mukapil K. Biometric Dynamic Personality Authentication in Open Information Space International Journal of Computer Technology and Applications (IJCTA), 2013, Vol 4 (5), 846-855.

6. Ахметов Б.С., Алибиева Ж.М., Бекетова Г.С. Биометрия, биометриялық идентификаторлар мен технологиялар. Вестник НАН РК, 2014. - № 6. - С. 3-6

7. European ACTS projects. M2VTS Project: multi-modal biometric person authentication // Online version on the site http://www.tele.ucl.ac.be/ PROJECTS/M2VTS.

8. Ахметов Б.С., Иванов А.И., Малыгин А.Ю., Фунтиков В.А. Основы биометрической аутентификации личности. Алматы: КазНТУ, 2014.

УДК 621.391.82:004.031

МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ КАНАЛА СВЯЗИ В СРЕДЕ MATLAB/SIMULINK

Арстанбеков Кайрат Арстанбекович, *специалист СКБ ИЭТ при КГТУ им. И.Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Мира 66,e-mail: kairathuxury@mail.ru*
Кармышаков Аскарбек Камалдинович, *к.т.н., доцент, КГТУ им. И.Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Мира 66,e-mail: askar1969@mail.ru*

Целью данной работы является моделирование и исследование помехоустойчивости канала связи с использованием известного пакета Matlab/Simulink. Для достижения поставленной цели решались задачи:

- исследование основных методов кодирования для систем передачи информации;
- моделирование каналов связи в пакете программ Matlab+Simulink;
- получение осциллограмм сигналов;
- сравнительный анализ и обработка результатов моделирования.

Ключевые слова: кодирование, спектр сигналов, цифровая информация, система передачи информации, синхронизация сигналов, битовые ошибки.

MODELING AND INVESTIGATION OF INTERFERENCE CODING OF THE COMMUNICATION CHANNEL IN THE MEDIUM MATLAB / SIMULINK

Arstanbekov Kairat Arstanbekovich, *specialist SDB IET at KSTU named after I.Razzakova, Kyrgyzstan, 720044, Bishkek, Kyrgyzstan, e-mail: kairathuxury@mail.ru*
Karmyshakov Askarbek Kamaldinovich, *PhD (Engineering), Associate professor, KSTU named afterI.Razzakova, Kyrgyzstan, 720044, Bishkek, Kyrgyzstan, e-mail: askar1969@mail.ru*

The purpose of this work is to simulate and study the noise immunity of the communication channel using the well-known Matlab / Simulink package. To achieve this goal, the following tasks were solved:

- The study of basic coding methods for information transmission systems;
- Simulation of communication channels in the Matlab/Simulink software package;
- Reception of oscillograms of signals;
- Comparative analysis and processing of simulation results/

Keywords: coding, spectrum of signals, digital information, information transmission system, signal synchronization, bit errors.

Исследование основных методов кодирования передачи информации

При обработке, передаче и приеме цифровой информации важное значение имеет определение (детектирование) ошибок и их коррекция. При выборе способа кодирования нужно одновременно стремиться к достижению нескольких целей:

- минимизировать ширину спектра сигнала, полученного в результате кодирования;