БИОМЕТРИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 007

Методы обнаружения живучести в биометрических системах

Р. М. Алгулиев, д-р техн. наук, чл.-кор. НАНА;
Я. Н. Имамвердиев, канд. техн. наук; *В. Я. Мусаев*
Институт информационных технологий Национальной академии наук Азербайджана, г. Баку, Азербайджан

Методы обнаружения живучести являются важными мерами противодействия фальсификации биометрических характеристик. Эти методы автоматически определяют, что поступающий в биометрическую систему биометрический образец принят от живого человека. Опубликовано сравнительно мало результатов исследований эффективности этих мер, поэтому пользователи биометрических систем встречаются с трудностями при выборе метода обнаружения живучести, отвечающего требованиям безопасности. Анализируются методы обнаружения живучести для разных биометрических характеристик; указываются направления дальнейших исследований по методам обнаружения живучести.

Ключевые слова: биометрические технологии, спуфинг-атаки, обнаружение живучести, отпечатки пальцев, распознавание лица, радужная оболочка.

Введение

Биометрические технологии содержат методы автоматического распознавания личности на основе его уникальных измеряемых физиологических **и** поведенческих характеристик. Для распознавания личности используются различные биометрические характеристики, такие как лицо, отпечатки пальцев, радужная и сетчатая оболочки глаза, голос, ручная подпись, геометрия руки, рисунок вен на руке **и** т. д.

Биометрические системы находят широкое применение в системах информационной безопасности, электронной коммерции, при раскрытии и предотвращении преступлений, судебной экспертизе, пограничном контроле, телемедицине и т. д. Но они уязвимы к атакам на различных стадиях обработки информации. Эти атаки возможны на уровне сенсора, где принимается изображение или сигнал от индивидуума, атаки повтора (replay) на линиях коммуникаций, атаки на базу данных, где хранятся биометрические шаблоны, атаки па модули сравнения и принятия решений **[1].**

Основную потенциальную угрозу на уровне сенсора представляют атаки спуфинга (spoofing). Спуфинг — это обман биометрических систем путем предоставления биометрическому сенсору копий, муляжей, фотографий, отрезанных пальцев, заранее записанных звуков и т. п.

Цель атаки спуфинга при верификации — представление незаконного пользователя в системе как законного, а при идентификации — добиться необнаружения индивидуума, содержащегося в базе данных (БД). Противодействия атакам спуфинга более трудны, так как злоумышленник непосредственно имеет контакт с сенсором и невозможно использовать криптографические и другие методы защиты.

Статьи об успешных спуфинг-атаках на биометрические устройства появились в научных и популярных изданиях в конце 1990-х гг. В 1998 г. в журнале Network Computing появилась статья, где сообщалось о принятии фальшивых отпечатков за настоящие устройствами распознавания отпечатков пальцев [2]. Из шести тестированных устройств четыре оказались уязвимыми к атакам спуфинга. В 2002 г. профессором Национального университета Иокогама (Япония) Т. Матсумото и его студентами были разработаны два метода спуфинга устройств распознавания отпечатков пальцев [3]. В первом методе пользователь сотрудничает со злоумышленником, и для создания искусственного пальца используется живой палец, во втором — используется латентный отпечаток.

Искусственные пальцы изготовлялись из желатина. Используя их, удалось с большей вероятностью (68 — 100 %) обмануть системы **распозна-**

вания отпечатков пальцев с оптическими и емкостными сенсорами. В ноябре 2002 г. в германском журнале "C't" были опубликованы результаты тестирования различных биометриических устройств от ведущих производителей [4]. Тесты охватывали устройства распознавания отпечатков пальцев, лица и радужной оболочки. Системы распознавания лица удалось обмануть воспроизведением видео в обратном направлении. Сканеры радужной оболочки были обмануты удержанием высококачественной фотографии радужной оболочки перед лицом человека, для обнаружения живого зрачка на фотографии была сделана дырка. Некоторые сканеры отпечатков пальцев удалось обмануть просто дыханием или наложением полиэтиленового пакета на оставленные на поверхности сканера отпечатки, а также извлечением графитовым порошком латентных отпечатков пальцев.

Таким образом, были продемонстрированы уязвимости различных биометрических устройств в процессе верификации. Исследования, проведенные в университете Кларксон, показали, что в лабораторных условиях можно достичь 90 % успеха в принятии поддельных пальцев за настоящие [5]. В этих экспериментах тестировались четыре типа устройств распознавания отпечатков пальцев, использовались отпечатки, взятые с рук трупов, и искусственные пальцы, созданные из пластика, желатина и пластилина. При использовании метода обнаружения живучести процент успешной верификации фальшивых образцов был менее **10** *%.*

Методы противодействия атакам спуфинга

Биометрическая общественность ответила атакам спуфинга введением ряда механизмов протииводействия. Меры антиспуфинга в биометрических системах включают следующие методы [6, 7].

• *Рандомизация данных верификации.*

Система может рандомизировать отпечатки пальцев или выражения лиц, запрашиваемых для верификации. Это уменьшает вероятность предоставления фальшивых биометрических образцов для верификации.

• *Использование нескольких биометрических образцов.*

В процессе регистрации в системе на каждого пользователя регистрируется, например, несколько отпечатков пальцев (в идеале все 10). После этого в процессе аутентификации у пользователя запрашиваются для проверки несколько пальцев в произвольной последовательности, что значительно затрудняет вход в систему по фальшивым пальцам.

• • *Мулыпимодальная биометрия.*

Для обнаружения живучести можно использовать несколько биометрических характеристик одновременно, например отпечаток пальца и форма лица или радужная оболочка глаза и т. д. Это создает для злоумышленника трудности сфальсифицировать несколько биометрических характеристик одновременно, нежели чем одну характеристику.

• *Мультифакторная аутентификация.*

Мультифакторная аутентификация, использующая наряду с биометрией смарт-карты, токены или пароли, может уменьшить вероятность обмана биометрических систем. В этом случае для обмана последней злоумышленнику вместе с фальшивыми биометрическими данными требуются дополнительные идентификаторы. Но мультифакторная аутентификация также уменьшает основное преимущество биометрических систем — удобство использования,

• *Контроль над процессом верификации (иден тификации).*

Контроль над операциями биометрических систем может повысить уровень безопасности системы. Очевидно, что предпринять атаку спуфинга против контролируемой биометрической системы в этом случае труднее. Супервизор поможет пользователям правильно представить свои биометрические характеристики и минимизировать ошибки.

• *Запрос — ответ.*

В методе запрос — ответ пользователя просят посмотреть на что-то, прослушать или прочувствовать что-то, а потом в ответ сделать что-то. Запрос, требующий один ответ из нескольких возможных, может затруднить простое воспроизведение сигналов, заранее записанных злоумышленником. В качестве примера можно привести изменение выражения лица (улыбнуться или хмуриться) (используется в Identix) или воспроизведение множества случайно генерированных фраз (используется в VeriVoice). Этот метод применяют обычно против атак воспроизведения, но его можно использовать и как метод обнаружения живучести.

Может использоваться и непроизвольный запрос—ответ. Сюда относятся рефлекс на удары, изменение зрачка в зависимости от интенсивности света, рефлекс мышц на электрическое раздражение. Ясно, что методы, в которых используются удары, не одобряются пользователями. Важный аспект заключается в том, что запрос —ответ показывает только присутствие человека, но он может быть и неавторизованным пользователем.

• *Обнаружение живучести.*

Цель обнаружения живучести в биометрических системах заключается в том, чтобы убедиться, что для регистрации, верификации и идентификации используются только "подлинные" биометрические характеристики. В принципе обнаружение живучести основывается на совпадении одного или нескольких признаков биометрического образца с признаками, связываемыми с живым биометрии**ческим** образцом.

Подходы по обнаружению живучести можно разделить: на обнаружения живучести и обнаружения неживучести. На практике биометрические системы чаще разрабатываются на обнаружение живучести, чем на неживучести.

В методах обнаружения живучести в качестве признаков жизни используется физиологическая или поведенческая информация или информация, содержащаяся в биометрическом образце. В системах распознавания отпечатков пальцев для обнаружения живучести используются измерение температуры, пульса, диэлектрического сопротивления, обнаружение подкожных признаков, сравнение последовательно принятых биометрических образцов и т. д.

Для других биометрических характеристик методы обнаружения живучести, как правило, основываются на анализе произвольного и непроизвольного поведения. Системы распознавания лица могут требовать от пользователя движения головы, губ, глаз или изменения выражения лица. Системы распознавания голоса могут запрашивать пользователя произнести случайно генерированную фразу или буквенно-цифровую последовательность, чтобы предотвратить воспроизведение записанных звуков.

Методы обнаружения живучести отпечатков пальцев

Проблема защиты биометрических систем от атак спуфинга — одна из самых сложных в первую очередь для технологии распознавания отпечатков пальцев. Связано это с тем, что эта технология распространена широко, и отпечатки пальцев можно получить относительно легко по сравнению, например, с радужной оболочкой глаза, и изготовление фальшивого отпечатка пальца также сравнительно более простая задача.

Для обнаружения живучести отпечатков пальцев были предложены различные подходы на основе измерения температуры [8], пульса на кончике пальца [9], электрической проводимости, диэлектрического сопротивления кожи **[10],** толщины кожи и т. д. Для этой цели были использованы также такие характеристики как искажение кожи **[11],** диффузия пота [12], запах кожи [13]. По способу реализации все методы обнаружения живучести отпечатков пальцев можно разделить на две группы: методы, реализованные на уровне программного обеспечения, работающего с изображением , и методы, реализованные **аппаратно** на уровне считывающего устройства.

Технология, предложенная Nixon и др. на основе спектроскопии,w может использоваться для верификации личности **и** обнаружения живучести (применяются оптические свойства кожи человека) **[14].** Используется множество длин волн для освещения кожи. Получаемый спектр отраженного света характеризует сложное взаимодействие между структурой и химическими свойствами тканей человеческой кожи. Результаты исследований показали, что эти спектральные характеристики кожи человека являются отличительными признаками в сравнении с другими материалами. Кроме того, имеются также явные признаки, отличающие одного человека от другого.

Спектральный сенсор малого размера, разработанный исследователями Lumidigm Inc., использует неподвижные оптические компоненты, работающие в спектральной области видимого света и очень близкого к инфракрасному (400 — 940 нм). Он с большой точностью измеряет отраженный спектр кожи [15]. Эти сенсоры могут применяться как для идентификации личности, так и обнаружения живучести. Эластичный сенсор малого размера может пропускать свет через кожу фактически в любой точке тела человека.

Большинство методов обнаружения живучести в системах распознавания отпечатков пальцев лишь предложены. Эффективность их не тестировалась на обнаружение живучести, и результаты не публиковались. Каждый из этих методов имеет свои недостатки. Например, измеритель температуры можно обмануть просто нагреванием. Измеритель пульса и электрокардиограф могут обнаружить живучесть даже при предоставлении злоумышленником фальшивого пальца. Злоумышленник может использовать фальшивый палец в виде полупрозрачной пленки, покрывающей только отпечаток пальца. Несмотря на получение патентов, большинство вышеупомянутых систем не реализовано в виде коммерческих продуктов. Исключением являются системы на основе измерения диэлектрического сопротивления и полного сопротивления **[Ю].**

Методы обнаружения живучести лица

В системах распознавания лиц спуфинг-атаки можно применять фотографию лица, записанное видео, 3D модели лица с движением губ, 3D модели с различными выражениями лица и т. д. [16].

A. Jain и др. **[16]** используют анализ спектра частот одного изображения лица или последовательности изображений лиц, определяют два дескриптора для измерения соотношения высоких частот и временную дисперсию всех частот. Их метод основан на плохом качестве фотографии или изменении расположения живых лиц.

Некоторые методы обнаружения живучести лица основаны на измерении информации об 3D глубине. В работе **[17]** строится карта глубин с восстановлением 3D структуры. Карту глубин можно использовать для определения входного изображения, полученного от живого человека или фотографии. При движении фотографии сама карта

глубин остается неизменной, а живое лицо дает переменные значения глубины.

В работе [18] применяется метод оптического потока для оценки структуры последовательности изображений. В методе оптического потока сегментируется карта оптического потока и группируются пиксели, принадлежащие отдельным объектам. После вычисления потока каждого пикселя можно оценить 3D координаты точек поверхности.

Алгоритм, предложенный в работе [19], основан на анализе движения глаз в последовательности изображений. В общем вариации в форме компонентов лиц в последовательности изображений очень незначительны, но вариации в форме глаза могут быть большими, наше мигание глаза и движение зрачка глаза всегда являются непроизвольными.

В работе [20] для обнаружения живучести разработан метод слежения за лицами в реальном времени. Признаки лица извлекаются с помощью фильтров Габора и классифицируются SVM-экс-пертами. Для производительности в реальном времени выбранные точки были использованы для формирования региональных моделей лица.

G. Deng и др. сообщают о разработке метода обнаружения живучести лица на основе SVM (Support Vector Machine) с использованием модели движения глаз [21]. Модель движения глаз обучается с использованием многочисленных образцов позиции глаз. В этом методе обнаружения живучести чтобы пройти тест, пользователь должен мигать глазами. Фальшивые изображения лица, не умеющие мигать, не поступают в стадию распознавания **и** останавливаются.

Фирма Identix для обнаружения живучести предлагает систему запрос —ответ, так называемое множественное фрейм/видео-тестирование [22]. Система дает указание пользователю улыбнуться или мигнуть, чтобы убедиться за короткий период времени, что изображение лица принадлежит данному человеку, оба движения нельзя совершить одновременно. Эта технология обнаружения живучести требует обычно 2 — 3 с и не требует специального оборудования.

В работе [23] предлагается метод обнаружения живучести для системы аутентификации "лицо-голос" на основе двух признаков. Эти признаки основаны на латентном семантическом анализе (ЛСА) и каноническом корреляционном анализе (ККА). Метод увеличивает устойчивость систем аутентификации к атакам воспроизведения видео. Эксперименты с базами данных "речь — лицо" при слиянии векторов признаков "лицо — голос" дали на 42 % меньше ошибок с ЛСА-признаками и на 61 % — ошибок с признаками ККА.

Методы обнаружения живучести радужной оболочки

J. Daugman выделит четыре категории методов обнаружения живучести для распознавания радужной оболочки [24]:

фотонические и спектрографические противодействия;

поведенческие противодействия;

противодействия аналого-физическим атакам;

противодействия атакам цифрового воспроизведения.

Фотоннческие и спектрографические противодействия аналогичны методам спектроскопии, используемым в системах распознавания отпечатков пальцев. При исследовании волнами различной длины пигментов ткани, крови, жира и меланина получают разные результаты. Этот факт можно использовать для обнаружения живучести.

Из поведенческих методов обнаружения живучести радужной оболочки можно указать следующие:

• обнаружение малых "колебаний" (hippus) зрачка. В результате сложного взаимодействия мышц радужной оболочки диаметр зрачка остается неизменным при малых колебаниях с частотой ~0,5 Гц. Контролируя эти движения, можно убедиться, живой ли это образец;

• изучение реакции зрачка на изменение освещения. Зрачок реагирует на внешние раздражители (резкий свет, громкий голос и т. п.) определенным образом и с определенным опозданием, эти реакции являются безусловными рефлексами. Зрачок меняет свой размер от 0,8 до 8,0 мм в зависимости от яркости света. Построив график реакции зрачка (пупиллограм), и связывая его с моментом подачи импульса-раздражителя, с высокой точностью можно предотвратить попытки фальсификации.

Для обнаружения живучести можно использовать также микродвижения, характеризующие живые глаза.

Противодействия аналого-физическим атакам могут использоваться для обнаружения фотографий радужной оболочки, напечатанных с высокой разрешимостью, и контактных линз. Эти методы могут обнаружить точечные матрицы и цвета, используемые в некоторых оборудованиях для печати, или могут обнаружить кривизну контактных линз по сравнению с кривизной радужной оболочки. Кроме того, в этих методах противодействия также можно использовать отражения, присутствующие в живых глазах, но отсутствующие в фотографиях, например эффект Пуркинье.

Эффект Пуркинье связан с фактом большой чувствительности зрительной системы к коротковолновому свету при слабом освещении. В результате при слабом освещении коротковолновый свет кажется ярче длинноволнового света: днем красная и зеленая поверхности имеют одинаковую яркость, а при закате зеленая поверхность

кажется более яркой, чем красная.

Для обнаружения живучести можно использовать также эффект "красных глаз", который связан с отражением света от сетчатой оболочки глаза. Он чувствуется ярче у детей, у людей со светлым
цветом глаз и волос. При использовании фотовспышки в темной комнате в момент освещения зрачок не успевает сузится, и свет отражается от сетчатой оболочки, покрытой маленькими кровяными сосудами, и на фотографии глаза получаются красными. Для обнаружения живучести можно использовать также оценку спектра отражения от роговицы. Роговица живого глаза постоянно увлажняется, мертвый глаз быстро высыхает. Спектры отражения влажной и сухой роговицы различаются. Например, метод управляемого отражения света основан на отражении инфракрасного света от влажной роговицы при раздражении источниками света, случайно расположенными в пространстве.

Методы противодействия атакам цифрового воспроизведения для обнаружения живучести используют характеристики шаблонов радужной оболочки (irisCode). Размеры всех кодов IrisCode одинаковы. Они используют одинаковую структуру кодирования, скремблирование байтов (bytecrambling) может быть применено для создания шаблонов пермутаций в неограниченном количестве. Но если зарегистрированные и представленные шаблоны не кодированы с использованием одного и того же метода, то повторное предоставление заранее записанной радужной оболочки будет бесполезным.

Заключение

Как и любой метод аутентификации, биометрические технологии полностью не защищены от атак спуфинга. Методы обнаружения живучести являются наиболее часто обсуждаемой мерой противодействия спуфингу. Обнаружение живучести является одной из важных процедур в процессах регистрации, верификации и идентификации. Следовательно, его необходимо рассматривать как составную компоненту биометрической системы. Конечно, обнаружение живучести влияет на процент ложного принятия или ложного отказа, на процент отказа от регистрации и на другие индикаторы производительности. При реализации методов обнаружения живучести должны приниматься во внимание такие аспекты оценки биометрических систем, как удобство использования, универсальность и т. д.
Некоторые технологии обнаружения живучести уже используются на практике, но оценка их производительности и оценка их влияния на итоговую производительность биометрической системы требуют независимого тестирования. Большинство вендоров не раскрывают собственные методы обнаружения живучести," чтобы обеспечить конкурентное преимущество. Эти методы обычно защищаются как коммерческие тайны и не обсуждаются в общественной среде. Следовательно, их производительность невозможно оценить, поэтому заявления об успехах обнаружения живучести могут быть завышенными и обманчивыми.

Методы обнаружения живучести могут уменьшить риск атаки фальшивыми биометрическими характеристиками, но невозможно обеспечить абсолютную защиту системы от атак спуфинга. Это отрицательно влияет на использование биометрических технологий в качестве средств аутентификации в приложениях, где предъявляются высокие требования к безопасности. Уязвимость к атакам спуфинга и ошибки биометрического совпадения подразумевают, что нельзя рассматривать решения биометрической системы как решающий вердикт верификации и идентификации. К окончательным результатам идентификации личности должны быть подключены также и другие факторы. Например, в некоторых правоохранительных и гражданских приложениях биометрический поиск для принятия окончательного решения о совпадении и несовпадении предусматривает участие человека-оператора. Автоматизированные биометрические системы создаются не для замены процесса принятия решений человеком, а для оказания ему помощи.

Авторы выражают благодарность директору Центра тестирования биометрических технологий при Государственном университета Сан-Хосе (Калифорния), доктору James L. Wayman за плодотворные обсуждения и ценные комментарии, которые дали много полезного при подготовке настоящей работы.

Работа выполнена при финансовой поддержке Американского фонда гражданских исследований и развития (U.S. Civilian Research & Development Foundation, CRDF) и Национального научного фонда Азербайджана (Azerbaijan National Science Foundation, ANSF), грант № AZM1-3112-BA-08.

Библиография

1. *Ratha N. K., Connell J. H., Bolle R. M,* Enhancing Security and Privacy in Biometrics-Based Authentication Systems//IBM Systems Journal, 2001. V. 40. No. 3. P. 614-634.

2. *Matsumoto T., Matsumoto H., Yamada K., Hoshino S.* Impact of Artificial "Gummy" Fingers on Fingerprint Systems// Proceedings of SPIE. V. 4677. Optical Security and Counterfeit Deterrence Techniques IV, 24 — 25 January 2002.

3. *Willis D., Lee M.* Six Biometric Devices Point the Finger at Security. Biometrics under Our Thumb//Network Computing, June, 1998.

4. *Thalheim L., Krissler J,* Body Check: Biometric Access Protection Devices and their Programs Put to the Test// C't Magazine, November 2002.

Derakhshani R., Schuckers S., Hornak L., O'Gorman L., Determination of vitality from a non-invasive biomedicai measurement for use in fingerprint scanners//Pattern Recognition, 2003. V. 17. No. 2.

6. *Schuckers S. A. C.* Spoofing and Anti-Spoofing Measures//Information Security Technical Report, Elsevier. 2002. V. 7. No 4. P. 56-62.

7. Liveness Detection in Biometric Systems, International Biometric Group white paper, Available at http:// www.biometrikgroup.com/reports/public/rcports/livcncss.html

8. *Osten D., Carim H. Ml, Arneson M. R., Blan B. L.* Biometric, Personal Authentication System, Minnesota Mining and Manufacturing Company: Patent US #5,719,950, February' 17, 1998.

9. *Lapsley P. D., Less J. A, Pare D. F.(Jr.), Hoffman N.//* Anti-Fraud Biometric Sensor that Accurately Detects Blood Flow, SmartTouch, LLC: Patent US #5,737,439, April 7, 1998.

10. *Kallo P., Kiss I., Podmaniczky A., Talosi J.* Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus//Dermo Corporation, Ltd.: Patent US #6,175,64, January 16, 2001.

11. *Antonelli A., Cappelli R., Maio D., Maltoni D.* Fake finger detection by skin distortion analysis//IEEE Transactions on Information Forcnsics and Security. V. 1. Issue 3. 2006.

12. *Parthasaradhi S. T. V., Derakshani R., Hornak L. A., Schuckers S. A. C.* Time-series detection of perspiration as a liveness test in fingerprint devices//SMC-C(35). 2005. No. 3. P. 335-343.

13. *Baldissera D., Franco A., Maio D., Maltoni D.* Fake Fingerprint Detection by Odor Analysis//Proceedings of International Conference on Biometric Authentication 2006 — ICBA06, Lecture Notes in Computer Science, 2006. V. 3832. P. 265-272.

14. *Nixon K. A., Rowe R. K., Allen J., Corcoran S. et al.* Novel spectroscopy-based technology for biometric and liveness verification//Proc. SPIE. Biometric Technology for Human Identification, 2004. V. 5404. P. 287-295.

15. Lumidigm Inc. website: http://www.lumidigrri.com/

16. *Li /., Wang Y., Tan T., Jain A. K.* Live Face Detection Based on the Analysis of Fourier Spectra//Proc. SPIE. V. 5404, Biometric Technology for Human Identification. 2004. P. 296 — 303.

17. *Choudhury T., Clarkson B., jebara T., Pentland A.* Multimodai person recognition using unconstrained audio and video//International Conference on AVBPA, 1999. P. 22-28.

18. *Aggarwal J. K., Nandhakumar N.* On the Computation of Motion from Sequences of Images — A Review//Proc. IEEE, 1998. V. 76. P. 917-935.

19. *Hyung-Keun Jee, Sung-Uk Jung, Jang-Hee Yoo.* Liveness Detection for Embedded Face Recognition System//Proceedings of World Academy of Science, Engineering and Technology, 2006. V. 18. P. 29-32."

20. *Bigun J., Fronthaler H., Kollreide K.* Assuring liveness in biometric identity authentication by real-time face tracking, CIHSPS2004//IEEE International Conference on Computational Intelligence for Homeland Security and Persona] Safety, Venice, Italy, 21-22 July. P. 104-112. IEEE Catalog No. 04EX815, 2004.

21. *Deng G., Coo B., Miao J., Gao W., Zhao D. A* Liveness Check Algorithm Based on Eye Movement Model Using SVM// The Chinese Journal of Computer aided design and computer graphics (in Chinese language). 2003. V. 15. No. 7. P. 853-857.

22. Identix Inc. website: http://www.identix.com/

23. *Chetty C, Wagner M.* Liveness detection using cross-modal correlations in face-voice person authentication, In// ;, INTERSPEECH-2005. 2005. P. 2181-2184.

24. *DaugmanJ.* Iris Recognition and Anti-Spoofing Countcrmca-sures//7th International. Biometrics Conference, London, 2004.

Liveness detection methods in biometric systems

R. M. Alguliev, Y. N. Imamverdiyev, V. Y. Musayev
Institute of Information Technology of Azerbaijan National Academy of Sciences,
Baku, Azerbaijan

Liveness detection methods are important countermeasures against falsification of biometric characterictics. These methods ensures that biometric samples captured by biometric system are aquisited from live individual. A few results of resarches on efficiency of these methods are published. For this reason biometric system users meet with difficulties when selecting /iveness detection methods according with their security requirements. In this paper f/veness detection methods for different biometric modalities are analysed. Also future directions for research in this importan field are pointed out.

Keywords: biometric technology, spofing attacks, liveness detection, fingerprint recognition, face recognition, iris recognition.

Алгулиев Расим Магамед оглы, директор института, чл.-кор. НАНА.
Тел: (+994-12)439-61-21.
E-mail: director@iit.ab.az, sccretary@iit.ab.az
Имамвердиев Ядигар Насиб оглы, зав. сектором.
Тел: (+994-12) 510-42-53. E-mail secretary@iit.ab.az
Мусаев Вюгар Ядулла оглы, аспирант.
Тел: (+994-12) 510-42-53. E-mail: vuqarmusa@gmail.com