Биометрия

ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%8F

Биометрия предполагает систему распознавания людей по одной или более физическим или поведенческим чертам. В области информационных технологий биометрические данные используются в качестве формы управления идентификаторами доступа и контроля доступа. Также биометрический анализ используется для выявления людей, которые находятся под наблюдением (широко распространено в США, а также в России — отпечатки пальцев)

В Диснейуорлде биометрическим распознаванием отпечатков пальцев проверяют, что один билет используется каждый раз одним и тем же человеком

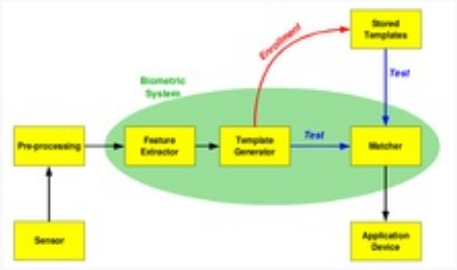
Основные принципы

Биометрические данные можно разделить на два основных класса:

- **Физиологические** — относятся к форме тела. В качестве примера можно привести: отпечатки пальцев, распознавание лица, ДНК, ладонь руки, сетчатка глаза, запах, голос.
- **Поведенческие** — связаны с поведением человека. Например, походка и речь. Иногда для этого класса биометрии используется термин англ. *behaviometrics*.

Определения

Основные определения, используемые в сфере биометрических приборов:[1]



Приблизительная структурная схема биометрического анализа (англ.)

- Универсальность — каждый человек должен обладать измеряемой характеристикой.
- Уникальность — это насколько хорошо человек отделяется от другого с биометрической точки зрения.
- Постоянство — мера того, в какой степени выбранные биометрические черты остаются неизменными во времени, например в процессе старения.
- Взыскания — простота осуществления измерения.
- Производительность — точность, скорость и надёжность используемых технологий.
- Приемлемость — степень достоверности технологии.
- Устранение — простота использования замены.

Биометрическая система может работать в двух режимах:

- Верификация — сравнение один к одному с биометрическим шаблоном. Проверяет, что человек тот, за кого он себя выдает. Верификация может быть осуществлена по смарт-карте, имени пользователя или идентификационному номеру.
- Идентификация — сравнение один ко многим: после «захвата» биометрических данных идет соединение с биометрической базой данных для определения личности. Идентификация личности проходит успешно, если биометрический образец уже есть в базе данных.

Первое частное и индивидуальное применение биометрической системы называлось регистрацией. В

процессе регистрации биометрическая информация от индивида сохранялась. В дальнейшем биометрическая информация регистрировалась и сравнивалась с информацией, полученной ранее. Обратите внимание: если необходимо, чтобы биометрическая система была надежна, очень важно, чтобы хранение и поиск внутри самих систем были безопасными.

Первая часть (сенсор) — промежуточная связь между реальным миром и системой; он должен получить все необходимые данные. В большинстве случаев это изображения, но сенсор может работать и с другими данными в соответствии с желаемыми характеристиками.

Вторая часть (блок) осуществляет все необходимые предварительные процессы: она должна удалить все «лишнее» с сенсора (датчика) для увеличения чувствительности на входе (например, удаление фоновых шумов при распознавании голоса)

В третьей части (третьем блоке) извлекаются необходимые данные. Это важный шаг, так как корректные данные нуждаются в извлечении оптимальным путём. Вектор значений или изображение с особыми свойствами используется для создания шаблона. Шаблон — это синтез (совокупность) релевантных характеристик, извлечённых из источника. Элементы биометрического измерения, которые не используются в сравнительном алгоритме, не сохраняются в шаблоне, чтобы уменьшить размер файла и защитить личность регистрируемого, сделав невозможным воссоздание исходных данных по информации из шаблона.

Регистрация, представленная шаблоном, просто хранится в карте доступа или в базе данных биометрической системы, или в обоих местах сразу. Если при попытке входа в систему было получено совпадение, то полученный шаблон передается к сравнителю (какому-либо алгоритму сравнения), который сравнивает его с другими существующими шаблонами, оценивая разницу между ними с использованием определённого алгоритма (например, англ. *Hamming distance* — расстояние Хемминга — число позиций цифр в двух одинаковой длины кодовых посылках (отправленной и полученной), в которых соответствующие цифры отличаются). Сравнивающая программа анализирует шаблоны с поступающими, а затем эти данные передаются для любого специализированного использования (например, вход в охраняемую зону, запуск программы и т. д.).

Описание

Используемые показатели эффективности биометрических систем[2]:

- Коэффициент ложного приема (FAR), или коэффициент ложного совпадения (FMR)
  FAR — коэффициент ложного пропуска, вероятность ложной идентификации, то есть вероятность того, что система биоидентификации по ошибке признает подлинность (например, по отпечатку пальца) пользователя, не зарегистрированного в системе
  FMR — вероятность, что система неверно сравнивает входной образец с несоответствующим шаблоном в базе данных.
- Коэффициент ложного отклонения (FRR), или коэффициент ложного несовпадения (FNMR)
  FRR — коэффициент ложного отказа доступа — вероятность того, что система биоидентификации не признает подлинность отпечатка пальца зарегистрированного в ней пользователя.
  FNMR — вероятность того, что система ошибётся в определении совпадений между входным образцом и соответствующим шаблоном из базы данных. Система измеряет процент верных входных данных, которые были приняты неправильно.
- Рабочая характеристика системы, или относительная рабочая характеристика (ROC)
  График ROC — это визуализация компромисса между характеристиками FAR и FRR. В общем случае сравнивающий алгоритм принимает решение на основании порога, который определяет, насколько близко должен быть входной образец к шаблону, чтобы считать это совпадением. Если порог был уменьшен, то будет меньше ложных несовпадений, но больше ложных приёмов. Соответственно, высокий порог уменьшит FAR, но увеличит FRR. Линейный график свидетельствует о различиях для высокой производительности (меньше ошибок — реже

возникают ошибки).

- Равный уровень ошибок (коэффициент EER), или коэффициент переходных ошибок (CER) — это коэффициенты, при которых обе ошибки (ошибка приёма и ошибка отклонения) эквивалентны. Значение EER может быть с лёгкостью получено из кривой ROC. EER — это быстрый способ сравнить точность приборов с различными кривыми ROC. В основном, устройства с низким EER наиболее точны. Чем меньше EER, тем более точной будет система.
- Коэффициент отказа в регистрации (FTE или FER) — коэффициент, при котором попытки создать шаблон из входных данных безуспешны. Чаще всего это вызвано низким качеством входных данных.
- Коэффициент ошибочного удержания (FTC) — в автоматизированных системах это вероятность того, что система не способна определить биометрические входные данные, когда они представлены корректно.
- Ёмкость шаблона — максимальное количество наборов данных, которые могут храниться в системе.

Так как чувствительность биометрических приборов увеличивается, то FAR уменьшается, а FRR увеличивается.

Задачи и проблемы

Конфиденциальность и разграничение

Данные, полученные во время биометрической регистрации, могут использоваться с целями, на которые зарегистрированный индивид не давал согласия (не был осведомлён).

Опасность для владельцев защищённых данных

В случае, когда воры не могут получить доступ к охраняемой собственности, существует возможность выслеживания и покушения на носителя биометрических идентификаторов с целью получения доступа. Если что-либо защищено биометрическим устройством, владельцу может быть нанесен необратимый ущерб, который возможно будет стоить больше самой собственности. Например, в 2005, малайзийские угонщики отрезали палец владельцу Мерседес-Бенц S-класса при попытке угнать его машину[3].

Биометрические данные с возможностью отмены

Преимуществом паролей над биометрией является возможность их смены. Если пароль был украден или потерян, его можно отменить и заменить новой версией. Это становится невозможным в случае с некоторыми вариантами биометрии. Если параметры чьего-либо лица были украдены из базы данных, то их невозможно отменить либо выдать новые. Биометрические данные с возможностью отмены являются тем самым путём, который должен включить в себя возможность отмены и замены биометрии. Первыми его предложили Ratha и др.[4]

Было разработано несколько методов отменяемой биометрии. Первая система биометрии с возможностью отмены, основанная на отпечатках пальцев, была спроектирована и создана Туляковым.[5]. Главным образом, отменяемая биометрия представляет собой искажение биометрического изображения или свойств до их согласования. Вариативность искаженных параметров несёт в себе возможности отмены для данной схемы. Некоторые из предложенных техник работают, используя свои собственные механизмы распознавания, как работы Teo[6] и Саввида[7] , в то время как другие (Дабба[8]) используют преимущества продвижения хорошо представленных биометрических исследований для своих интерфейсов распознавания. Хотя увеличиваются ограничения системы защиты, всё же это делает модели с возможностью отмены более доступными для биометрических технологий.

Одним из частных вариантов решения может быть, например, использование не всех биометрических параметров. Например, для идентификации используется рисунок папиллярных линий только двух пальцев (к примеру, больших пальцев правой и левой руки). В случае необходимости (например, при ожоге подушечек двух «ключевых» пальцев) данные в системе могут быть откорректированы так, что с определённого момента допустимым сочетанием будет указательный палец левой руки и мизинец правой (данные которых до этого не были записаны в систему — и не могли быть скомпрометированы).

Международный обмен биометрическими данными

Многие страны, включая США, уже участвуют в обмене биометрическими данными. Данное заявление было сделано в 2009 в Комитете по Ассигнованиям, подкомитете по Национальной безопасности по «биометрической идентификации» Кэтлин Крэнингер и Робертом Мокни[9]:

> *Чтобы быть уверенными в том, что мы можем пресечь деятельность террористических организаций до того, как они доберутся до США, мы должны занять ведущее место в продвижении международных стандартов по биометрии. Развивая совместимые системы, мы сможем безопасно передавать информацию о террористах между странами, поддерживая нашу защищенность. Также как мы улучшаем пути сотрудничества внутри Правительства США по выявлению и устранению террористов и иных опасных личностей, у нас ещё есть обязательства перед нашими партнерами за границей совместно предотвращать любые действия террористов.*

и

> *Что же дальше? Нам нужно усиленно следовать за инновациями. Те, кто хотят причинить нам вред, продолжают искать наши слабости. Поэтому мы не можем позволить себе замедлить развитие.*

и

> *Мы понимаем, что при помощи биометрии и международного сотрудничества мы можем изменить и расширить возможности для путешествий а также защитить народы разных стран от тех, кто хочет причинить нам вред.*

Согласно статье, опубликованной С. Магнусон в журнале «Национальная Безопасность» (National Defense Magazine), Департамент национальной безопасности США под давлением вынуждает распространять биометрические данные[10]. В статье говорится:

> *Миллер (консультант Ведомства Национальной Безопасности и по делам безопасности в Америке) сообщает, что США имеет двусторонние договоренности по обмену биометрическими данными с 25 странами. Каждый раз, когда какой-либо иностранный лидер посещал Вашингтон за последние несколько лет, Государственный департамент обязательно заключал с ним подобный договор.*

Законодательное регулирование в России

Статья 11 Федерального закона «О персональных данных» № 152-ФЗ от 27 июля 2006 г. регламентирует основные особенности использования биометрических данных.

Биометрия в массовой культуре

Технологии биометрии были освещены в популярных кинофильмах. Только это уже вызвало интерес потребителей к биометрии, как к средству идентификации человека. В фильмах 2003 года «Люди-Х» и «Халк» использовались биометрические технологии распознавания: в виде доступа по отпечатку руки и в фильме «Люди-Х2» и по отпечатку пальца в «Халке».

Но это не было так показательно, пока в 2004 году не вышел фильм «Я, робот» с Уиллом Смитом в главной роли. Футуристический фильм демонстрировал развитие новейших технологий, которые даже на сегодняшний день ещё недостаточно развиты. Использование технологий распознавания голоса и ладони в фильме зафиксировалось в представлении будущего у людей и обе эти технологии, которые используются сегодня для охраны зданий или информации — лишь два из возможных применений биометрии.

В 2005 году вышел в прокат фильм «Остров». Дважды за фильм клоны используют биометрические данные: чтобы проникнуть в дом и завести машину.

Фильм «Гаттака» рисует общество, в котором существует два класса людей: продукты генной инженерии, созданные для того, чтобы быть высшими (так называемые «Действительные»), и низшие обычные люди («Инвалиды»). Люди, считавшиеся «Действительными», имели большие привилегии, и доступ к запретным зонам был ограничен для таких людей и контролировался автоматическими биометрическими сканерами, похожими на сканеры отпечатков пальцев, но коловшие палец и получавшие пробу ДНК из взятой крови.

В фильме «Разрушитель» персонаж Саймон Феникс, которого играл Уэсли Снайпс, вырезает жертве глаз, чтобы открыть дверь со сканером сетчатки.

В картине «Монстры против пришельцев» студии DreamWorks военный помощник проникает в зону, используя биометрию.

См. также

- Медицинская метрология
- Биометрические технологии

Примечания

1. ↑ *Jain, A. K.; Ross, Arun & Prabhakar, Salil (January 2004), "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology T. 14th (1): 4-20, DOI 10.1109/TCSVT.2003.818349*
2. ↑ "CHARACTERISTICS OF BIOMETRIC SYSTEMS". Cernet. Архивировано из первоисточника 5 мая 2012.
3. ↑ BBC News: Malaysia car thieves steal finger Another report, giving more credence to the story: [1]
4. ↑ N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems, " IBM systems Journal, vol. 40, pp. 614—634, 2001.
5. ↑ S. Tulyakov, F. Farooq, and V. Govindaraju, "Symmetric Hash Functions for Fingerprint Minutiae, " Proc. Int'l Workshop Pattern Recognition for Crime Prevention, Security, and Surveillance, pp. 30-38, 2005
6. ↑ A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs, " Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 28, pp. 1892—1901, 2006.

7. ↑ M. Savvides, B. V. K. V. Kumar, and P. K. Khosla, "«Corefaces»- Robust Shift Invariant PCA based Correlation Filter for Illumination Tolerant Face Recognition, " presented at IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'04), 2004.
8. ↑ M. A. Dabbah, W. L. Woo, and S. S. Dlay, "Secure Authentication for Face Recognition, " presented at Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on, 2007.
9. ↑ *Kraniger, K & Mocny, R. A. (March 2009), "Testimony of Deputy Assistant Secretary for Policy Kathleen Kraninger, Screening Coordination, and Director Robert A. Mocny, US-VISIT, National Protection and Programs Directorate, before the House Appropriations Committee, Subcommittee on Homeland Security, "Biometric Identification"", <http://www.dhs.gov/ynews/testimony/testimony_1237563811984.shtm>*
10. ↑ *Magnuson, S (January 2009), "Defense department under pressure to share biometric data.", NationalDefenseMagazine.org, <http://www.nationaldefensemagazine.org/ARCHIVE/2009/JANUARY/Pages/DefenseDepartmentUnderPressuretoShareBiometricData.aspx>*

Ссылки

- Movies & biometrics / Le cinéma et la biométrie