КСЗІ

Практическое занятие 13 23-03-21р.

Тема: Биометрические методы и их сравнительный анализ

Цель: Изучение и сравнение широко применяемых методом биометрической идентификации.

Вопрос 1. Показатели эффективности биометрических систем.

Вопрос 2. Верификация – идентификация. Переходной вопрос к практическому занятию: «Основные критерии оценки биометрических методов» .

Практичне заняття 11.
Якісне та кількісне порівняння біометричних методів ідентифікації осіб.

Цель практического занятия: сравнение методов биометрической идентификации, применяемых на практике.

Вопрос 1. Комплексное применение методов биометрической идентификации.

Вопрос 2. Паспортно-визовые документы.

Джерела інформації:

1. Jain, A. K.; Ross, Arun & Prabhakar, Salil (January 2004), "«An introduction to biometric recognition»", IEEE Transactions on Circuits and Systems for Video TechnologyT. 14th (1): 4-20

2. "CHARACTERISTICS OF BIOMETRIC SYSTEMS". Cernet. Архивировано из первоисточника 5 мая 2012.

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

5. 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.

6. 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.

7. 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"", «», US Department of Homeland Security.

Вопрос 1. Показатели эффективности биометрических систем.

1.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.

2.Коэффициент ложного отклонения (FRR) , 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.

3. 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).

4.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.

5. 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.

6. Коэффициент ошибочного удержания (FTC) — в автоматизированных системах это вероятность того, что система не способна определить биометрические входные данные, когда они представлены корректно.

7.Ёмкость шаблона — максимальное количество наборов данных, которые могут храниться в системе.

Вопрос 2.

Как было сказано на предыдущих занятиях, любая биометрическая система состоит из:

- **биометрического сканера - физического устройства, позволяющего измерять ту или иную биометрическую характеристику, и**
- **алгоритма сравнения измеряемой характеристики с предварительно зарегистрированной (биометрическим шаблоном).**

При этом возможны два режима работы системы:

- верификация ("сравнение одного с одним");

-идентификация ("сравнение одного со многими").

- **В режиме верификации пользователь вводит свое имя, пароль или пин-код, предъявляет электронную карточку либо другим способом объявляет системе, "кто он такой". Ее задача в этом случае - проверить "правдивость" полученной информации, т. е. сверить соответствие измеряемой биометрической характеристики с записанным ранее шаблоном заявленного индивидуума.**
- **В режиме идентификации пользователь просто "предъявляет биометрику", и задача алгоритма - принять решение, принадлежит ли пользователь к числу известных индивидуумов, и если принадлежит, то - кто он? В этом случае измеряемая биометрическая характеристика сравнивается с базой данных ранее записанных шаблонов всех "известных" системе людей.**

Вопрос 1. П/З.

Наиболее часто на практике применяют три основных биометрических метода:

- распознавание по отпечатку пальца;
- распознавание по изображению лица;
- распознавание по радужной оболочке глаза.

При этом методы распознавания по изображению лица могут работать с двумерным изображением лица (2D-фото) или с трехмерным (3D-фото).

Сравним качественно и количественно основные биометрические методы.

Приведём сравнительную таблицу (см. таблицу), где качественные характеристики различных биометрических методов сведены вместе. В столбцах указаны те критерии, которым должен отвечать в той или иной степени любой биометрический метод, и качественная оценка каждого биометрического метода по этим критериям.

Критерий / Метод	Измеримость	Устойчивость к окружающей среде	Устойчивость к подделке	Точность распознавания
Радужная оболочка глаза	П	Х	П	Х
Палец	П	П	П	Х
3D-лицо	Х	Х	Отл.	Х
2D-лицо	Х	П	П	П

Условные обозначения: Отл. —"отлично"; Х — "хорошо"; П — "плохо".

1. Измеримость.

Биометрическая характеристика должна быть легко измерима.

Измеримость можно количественно оценить величиной FTE (Failure to Enroll) - процентным отношением индивидуумов, которые не смогли пройти регистрацию (система не смогла построить биометрический шаблон), и средним временем распознавания (Recognition Time).

Под временем распознавания подразумевается либо время верификации, либо время идентификации - в зависимости от режима, в котором работает система.

При решении задач контроля доступа и особенно в применении к сложным транспортным системам время распознавания напрямую определяет время прохода, т. е. скорость потока, проходящего через контролируемую точку.

FTE устанавливает процент людей, которые не смогут воспользоваться системой, а значит, будут блокировать проход.

FTE включает в себя случаи, когда у индивидуумов нужная биометрическая характеристика отсутствует, но главным образом случаи, когда характеристика есть, но по тем или иным причинам ее измерение у данного человека на данном сканере затруднено.

Например, для распознавания по радужной оболочке глаза требуется ее изображение высокого разрешения, что приводит к определенным затруднениям, связанным с необходимостью точного позиционирования глаза по отношению к устройству.

В результате значение FTE относительно высоко (3-4%). Те же причины приводят к повышению времени распознавания, а также к FRR- вероятности ложного нераспознавания.

а). Распознавание многих групп людей по отпечатку пальца затруднено, особенно это касается работников физического труда, людей со слабо выраженными и стертыми папиллярными узорами, с дерматологическими дефектами, а также пожилых людей с сухой кожей.

Кроме того, сканеры из-за постоянного контакта с пальцами часто загрязняются.

Б). Методы распознавания по изображению лица (как двумерному, так и трехмерному) - бесконтактные и поэтому обладают высокой измеримостью биометрической характеристики.

2. Устойчивость к окружающей среде.

Биометрический метод должен быть устойчив к изменению окружающей среды. Эксплуатационные качества разных методов в значительной степени зависят от окружающих условий и могут терять стабильность при изменении этих условий.

Например, сканеры отпечатков пальцев, как правило, быстро загрязняются и качество работы падает, а для двумерных методов распознавания лица очень большое значение имеет распределение внешней освещенности.

3. Устойчивость к подделке.

Биометрическая система должна быть устойчивой к подделке (несанкционированному доступу). Система распознавания по двумерному (2D) изображению лица может быть легко обманута предъявлением фотографии "правильного" человека из числа "знакомых" системе.

Изображение чужой радужной оболочки глаза "украсть", конечно, сложнее, чем фотографию лица, но если эта задача выполнена, то соответствующие системы также могут быть обмануты фотографическим изображением "нужного" глаза, распечатанным с высоким разрешением или нанесенным на контактную линзу.

Для получения несанкционированного доступа по отпечатку пальца часто бывает достаточно просто подышать на оставленный на сканере отпечаток пальца предыдущего пользователя, и тогда устройство сработает. Системы распознавания разного типа - оптические, оптико-электронные, зарядовые (capacitive DC) и емкостные (capacitive AC) - могут быть обмануты при помощи "фальшивого" отпечатка, изготовленного из материала для зубных слепков, глины, пластилина, обычной жевательной резинки, кондитерского желатина и других влагосодержащих материалов. Современные цифровые технологии позволяют снять отпечатки пальцев "нужного" индивидуума, оставленные на любой поверхности, оцифровать и обработать полученное изображение на компьютере и затем изготовить "фальшивый" палец либо накладку на него для несанкционированного доступа или же для фабрикации фальшивых улик на месте преступления.

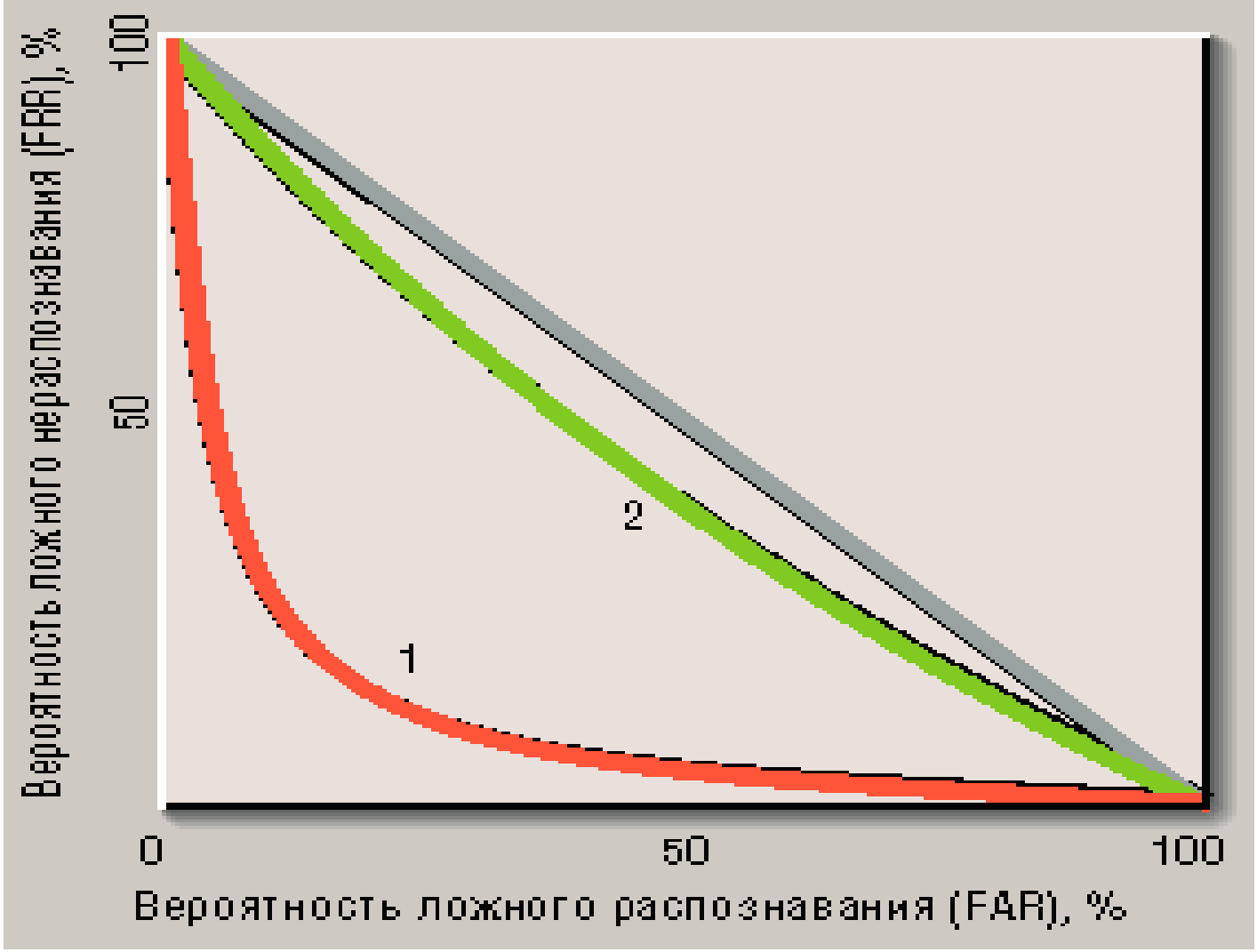
Наиболее устойчивой к подделке на данный момент представляется технология распознавания по трехмерному изображению лица.

Для того чтобы обмануть такую систему, потребовалось бы изготовить точную твердотельную маску лица, повторяющую во всех деталях его геометрию. При этом если система трехмерного распознавания работает в реальном времени, то она может легко включать в себя проверку на естественные микродвижения лица, что имитировать при помощи твердотельной маски крайне затруднительно.

4. Точность распознавания.

Любую биометрическую систему можно настроить на разную степень "бдительности", т. е. на разное значение вероятности ложного распознавания FAR (False Acceptance Rate), другими словами - вероятности того, что система "спутает" двух индивидуумов, признав "чужого" за "своего". Но уменьшение FAR всегда приводит к уменьшению чувствительности метода или - что эквивалентно - к увеличению вероятности ложного нераспознавания FRR (False Rejection Rate), т. е. вероятности того, что система не распознает "знакомого" ей субъекта.

Таким образом, чем "бдительнее" настроена система на непропускание "чужих", тем она хуже пропускает "своих".


Вероятность ложного нераспознавания (FRR), %
100
50
0
50
100
Вероятность ложного распознавания (FAR), %
1
2

В зависимости от конкретной задачи система настраивается на определенный компромисс между допустимыми значениями FAR и FRR, или, как их принято называть в теории статистических решений, - ошибками 1-го и 2-го рода.

Для оценки точности работы любой биометрической системы принято использовать характеристическую кривую, или ROC-кривую (Receiver Operating Characteristic).

Она устанавливает зависимость между ошибками 1-го и 2-го рода: FRR=FRR (FAR). Примеры ROC-кривых в условном виде приведены на рисунке. Метод с характеристической кривой 1, очевидно, более эффективен, чем метод с характеристической кривой 2.

При анализе и сравнении ROC-кривых очень важно понимать методику тестирования, в результате которого они получены. В частности - при каких условиях, в каких обстоятельствах проводилось тестирование, каков был сценарий использования системы, какова исходная совокупность тестируемых людей как по количеству, так и по составу, и т. д.

В зависимости от методики различают технологическое, сценарное и операционное тестирование. Результаты, полученные при различных методиках тестирования, могут сильно различаться для одной и той же системы. Обычно для любого конкретного приложения можно зафиксировать допустимое значение FAR, и тогда значение FRR является интегральным критерием точности для данной системы.

Приблизительные значения точности верификации в режиме операционного тестирования для основных биометрических методов показаны в таблице. Все значения взяты из последних публичных отчетов о результатах тестирования.

Метод	3D-фото лица	2D-фото лица	Отпечаток пальца (один палец)				Радужная оболочка глаза
FAR	FRR A4Vision	FRR (лучший 2D-алгоритм)	FRR сканер 1	FRR сканер 2	FRR сканер 3	FRR сканер 4	FRR (лучший сканер)
0,1%	0,2 %	19%	0,4%	1,5%	5%	8%	4,7%
0,01%	1 %	28%	1%	2%	7%	10%	5,3%
0,001%	1,5%	-	1,3%	3%	8%	14%	6%

Конкретные показатели сильно варьируются в зависимости от производителя и погрешности тестирования, но важно то, что три метода распознавания - по отпечатку пальца, по трехмерному изображению лица и по радужной оболочке глаза - обладают сравнимой точностью.

При этом распознавание по двумерному изображению лица уступает перечисленным методам по точности на порядок, так же как и другие не показанные в таблице биометрические методы (распознавание по геометрии руки, по голосу и др.).

С другой стороны, следует отметить, что двумерное изображение лица наиболее удобно для визуального сравнения оператором.

Указанные вероятности ложного распознавания FAR соответствуют случаю верификации, т.е. сравнению двух биометрических шаблонов между собой.

Для большинства практических задач точность, достигаемая в этом случае, при использовании любого из трех перечисленных выше методов вполне достаточна.

Для групп КБ-41 и КБ-42 следует акцентировать внимание на том, что в случае идентификации вероятность ложного распознавания FAR увеличивается пропорционально количеству людей в базе данных системы при той же чувствительности (FRR). Так, например:

Если при FRR, равном 1,3%, лучший пальцевый сканер в режиме верификации обеспечивает FAR, равный 0,001% (один шанс из ста тысяч), то в режиме идентификации при том же FRR и базе данных в N=10000 человек FAR составляет 10% (один шанс из десяти), что уже является недопустимым для большинства приложений.

Таким образом:

В режиме идентификации при базах данных на 1000-2000 человек некоторые существующие методы (по радужке, пальцу, 3D-фото) могут обеспечить приемлемую точность для систем контроля доступа.

При базах данных более 2000 человек ни один из биометрических методов "в чистом виде" не применим для большинства задач. Для некоторых задач приемлемы полуавтоматические решения, когда человек-оператор получает список наиболее похожих людей и принимает окончательное решение.

Для увеличения точности в режиме идентификации целесообразно использование нескольких биометрических методов одновременно.

Одним из наиболее распространенных "мультимодальных" решений является распознавание по нескольким пальцам.

В программе US-visit в настоящее время применяется распознавание по двум пальцам, и сегодня уже обсуждается переход на трех- или даже пятипальцевое решение. Следует заметить, что точность, достигаемая системами, работающими с пятью пальцами, на данный момент недостижима для комбинаций любых других методов. Несмотря на это, практическое использование таких систем ограничено по ряду указанных ранее критериев.

Методы получения 3D-изображения лица, как правило, позволяют одновременно получать и 2D-изображение, поэтому естественным является одновременное использование обоих источников информации.

Например, удобство обычных двумерных фотографий для визуального сравнения делает сохранение трехмерного снимка (занимающего не более 5 Кб) совместно с двумерной фотографией (занимающей не более 20-30 Кб) рациональным. Себестоимость цифровой 3D+2D-камеры при этом не сильно превышает стоимость обычной 2D-камеры.

Международный подкомитет по стандартизации в области биометрии (ISO/IEC JTC1/SC37 Biomerics) разрабатывает с 2009 года единые форматы данных для автоматического распознавания лиц, включающие двух- и трехмерные изображения.

Некоторые производители уже начали объединение этих двух методов в один. Вероятнее всего, вскоре распознавание лица с использованием обоих источников информации будет рассматриваться как один биометрический метод.

Объединение 2D- и 3D-методов распознавания лица дает существенное улучшение точности по сравнению с той, что могут дать системы, в которых используется только один из методов, а также позволяет объединить преимущества этих способов по другим критериям.

Например, комбинированный метод с использованием трехмерной технологии от A4vision и двумерной системы распознавания "Дозор" производства НПО "Информация" обеспечивает достаточную точность в режиме идентификации при базах данных размером до 10 000 лиц, а в перспективе - до 100 000 человек.

Тем не менее даже эти показатели неприемлемы для задач государственного или межгосударственного масштаба, где требуется идентификация по базам данных в несколько сотен тысяч или несколько миллионов человек. Такой задачей может быть, скажем, задача поиска человека с заданными биометрическими характеристиками в государственной базе данных выданных паспортов или виз.

В этом случае возможны комбинированные системы "много пальцев", или "палец + лицо", или "палец + радужная оболочка глаза" и т.д.

Вопрос 2. П/З.

Паспортно-визовые документы. Системы безопасности национального масштаба

Первая задача, связанная с использованием паспортно-визовых документов на транспорте и при пересечении государственных границ, - это сверка подлинности документа и его соответствия владельцу.

Применяемое сейчас визуальное сравнение с фотографией эффективно только при условии, если сотрудники служб прошли специальную подготовку.

Утомляемость и снижение внимания сотрудника при плотном потоке проверяемых лиц очень велика.

Кроме того, возможна коррупция или халатность среди работников служб паспортного контроля.

Двойная верификация подразумевает сверку биометрического шаблона, записанного в электронном паспорте или визе, с биометрическими характеристиками проверяемого пассажира.

Тройная верификация предполагает дополнительную сверку двух указанных характеристик с шаблоном, хранящимся в общегосударственном регистре биометрических данных. При этом сценарии любая попытка подделки паспорта становится бессмысленной, поскольку тройная верификация выявит несоответствие с шаблоном, записанным в государственный регистр при выдаче паспорта. Такая тройная проверка включена в рекомендации Международной организации гражданской авиации ICAO по применению биометрических систем, но этот вариант требует, чтобы сначала была создана государственная инфраструктура, поддерживающая запросы на верификацию личности по биометрическим данным.

Вторая задача, связанная в основном с выдачей паспорта или визы, - это проверка на то, что аналогичный документ не выдавался ранее гражданину с теми же биометрическими данными, но проходившему под другим именем, а также сверка биометрических данных гражданина с базами данных оперативных и специальных служб.

И в том и в другом случае решение такой задачи предполагает использование биометрических методов в режиме идентификации, при этом размер баз данных может быть очень большим.

Многие страны, включая США, 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.

Выводы:

Как следует из проведенного выше анализа, для решения первой задачи - двойной и тройной верификации по точности - подойдет любой из трех методов: по 3D-фотографии лица, по пальцу или по «радужке».

Для решения второй задачи - идентификации гражданина по большой базе данных - необходимо использование комбинированных методов.

Дякую за увагу!