ХАРАКТЕРИСТИКИ СИСТЕМ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ, ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К НИМ

Никитин В.В.
г. Горно-Алтайск, Республика Алтай
nikitin.aktash@mail.ru

Аннотация. *В статье описываются основные используемые в настоящее время характеристики существующих систем идентификации и аутентификации человека, представлено их описание и значение. Кроме указанных статистических характеристик, приведены описания и графических параметров, используемых при описании различных систем. В статье сформулированы и представлены требования к существующим и проектируемым системам идентификации и аутентификации. Обозначено перспективным направление разработки мультибиометрической систем идентификации, показаны его преимущества.*

Ключевые слова: *биометрия, идентификация, коэффициент, вероятность ошибки.*

CHARACTERISTICS OF THEBIOMETRIC IDENTIFICATION AND AUTHENTICATION SYSTEMS, THEIR REQUIREMENTS

V.V. Nikitin
Gorno-Altaisk, Altai Republic

Abstract. *The paper describes the main currently used characteristics of existing systems to identify and authenticate a person, presented their description and value. In addition to these statistical characteristics, there are description of the two graphic parameters, which used in the in various systems. The article defines and provides requirements for existing and planned systems of identification and authentication. Indicated promising development direction multibiometric identification systems, showing its advantages.*

Key words: *biometrics identification coefficient, the error probability.*

Биометрическая идентификация в настоящее время является актуальным направлением современных исследований и работ в области защиты информации и безопасности, поскольку она решает целый ряд задач по разграничению прав доступа и возможностям использования ресурсов различных сетей и систем связи. Системы защиты от несанкционированного доступа, построенные на основе биометрической идентификации имеют большую практическую значимость и целый ряд преимуществ по отношению к классическим организационно-техническим мерам:

- отсутствует возможность отчуждения персонального идентификатора от конечного пользователя;
- нет необходимости запоминать пароль;
- затруднена атака подбора биометрических характеристик;

Для характеристик различных биометрических систем идентификации в настоящее время активно применяют два параметра [1] – коэффициент ложного приема *FAR* (коэффициент ложного совпадения – *FMR*) и коэффициент ложного отклонения *FRR* (коэффициент ложного несовпадения *FNMR*).

FAR характеризует коэффициент ложного пропуска, т.е. вероятность ложной идентификации, а именно, вероятность того, что система идентификации по ошибке признает подлинность введенных данных пользователя, не зарегистрированного в системе. Данный коэффициент легко находится по следующему выражению:

$$FAR = \frac{1}{N}\sum_{n=1}^{N} FAR(n),$$

где *FAR(n)* – отношение количества успешных независимых (осуществленные с различными людь-

ми) попыток распознаться как персона к общему количество попыток. Очевидно, что чем больше попыток будет осуществлено, тем более статистически надежные результаты будут получены

FMR показывает вероятность ложного сравнения системой идентификации входного образца с несоответствующим шаблоном в базе данных.

FRR представляет собой оценку коэффициента ложного отказа доступа – вероятность того, что система идентификации не признает подлинность полученных данных зарегистрированного в ней пользователя, т.е. процент случаев отказа в доступе. Данный коэффициент может быть определен для каждого человека в отдельности, поскольку он может существенно различаться у разных людей, с помощью следующего выражения:

$$FRR = \frac{1}{N}\sum_{n=1}^{N} FRR(n),$$

где *FRR(n)* – соотношение количества отказов в доступе к общему количеству осуществленных попыток.

Более того, *FRR* зависит не только от конкретного человека, но и может изменяться в течении некоторого времени, как правило данный показатель уменьшается по мере того, как человека обучается работать с системой идентификации/аутентификации, именно из-за этого факта в литературе и техническом описании таких систем указывают значения *FRR* для обученных и необученных пользователей.

FNMR характеризует вероятность ошибки системы идентификации в определении совпадений между входным образцом и соответствующим шаблоном из базы данных.

В настоящее время чувствительность биометрических сенсоров (сканеров и датчиков) постоянно и неуклонно увеличивается, то можно сделать вывод о том, что коэффициент *FAR* постепенно уменьшается, а *FRR*, напротив, увеличивается, т.к. связь между ними обратно пропорциональная.

Для визуализации параметров характеристик *FAR* и *FRR* активно применяется графический метод построения рабочей характеристики системы (относительной рабочей характеристики – *ROC*), который представляет собой нахождение компромисса между характеристиками *FAR* и *FRR*. В общем случае в алгоритме сравнениясистемы идентификации заложено принятие решение на основании порога, который определяет, насколько близко должен быть входной образец данных к шаблону, чтобы определить это совпадением. Если порог был уменьшен, то будет меньше ложных несовпадений, но больше ложных приемов. Соответственно, высокий порог уменьшит *FAR*, но увеличит *FRR*. Линейный график свидетельствует о различиях для высокой производительности (меньше ошибок – реже возникают ошибки).

Для различных систем идентификации, использующих в своей работе определенное количество конечных пользователей, эксплуатационные характеристики можно отобразить изображают в виде кривой *XCC* [2]. Кривая является функцией числа транзакций, при которых идентификатор испытуемого субъекта присутствует среди *k* первых возвращенных идентификаторов, от значения параметра *k*.

Существуют и другие коэффициенты, применяемы для оценки эффективности систем идентификации:

- равный уровень ошибок (*EER*), или коэффициент переходных ошибок (*CER*) – коэффициенты, при которых обе ошибки (ошибка приема и ошибка отклонения) эквивалентны. Значение данного коэффициента легко получить с помощью кривой *ROC*. В основном, коэффициент *EER* используется для сравнения точности различных систем идентификации (с различными кривыми *ROC*). Как правило, системы идентификации с малым значение коэффициента *EER* наиболее точны;
- коэффициент отказа в регистрации (*FTE* или *FER*) – характеристика системы идентификации/аутентификации, показывающая процентное соотношение попыток создать определенный шаблон из входных данных безуспешны. Чаще всего это вызвано низким качеством входных данных от пользователя, обусловленного различными внешними (объективными) и внутренними (субъективными) факторами. *FTE* рассчитывается для

каждой пользователя системы индивидуально как отношение количества неуспешных попыток регистрации к общее число попыток – *FTE(n)*. Для получения общего *FTE* системы все полученные индивидуальные показатели усредняют:

$$FTE = \frac{1}{N}\sum_{n=1}^{N} FTE(n).$$

- коэффициент ошибочного удержания (*FTC*) – в системах идентификации показывает вероятность отсутствия способности системы определить биометрические входные данные, когда они представлены корректно;
- емкость памяти и шаблона – максимальное количество наборов данных, которые могут храниться в системе и в одном из шаблонов системы идентификации соответственно.

Основные характеристики систем идентификации тесно связаны с требованиями, предъявляемыми к ним. Одно из самых серьезных требований это показатели точности проводимой процедуры, характеризующиеся вышеперечисленными коэффициентами (*FAR* и *FRR*). Именно данное требование закладывается как основополагающее при разработке систем идентификации многими производителями.

Многочисленные исследования различных биометрических систем показывают невозможность правильной идентификации с вероятностью

100% при существующих технологиях. Вместе с тем, расширяющаяся сфера использования систем идентификации предъявляет все более жесткие требования к их показателям точности. Результаты тестирования этих систем свидетельствуют о том, что ни одна из них не позволяет обеспечить достаточный уровень точности для идентификации личности на больших массивах данных в автоматическом режиме. Таким образом, в настоящее время повышение точности информационных биометрических систем является актуальной научной и практической проблемой.

Следующим ограничением является скорость проводимых вычислений, от которой зависит быстрота выполняемых операций. Данный показатель несущественен при работе системы идентификации на ограниченном коротком диапазоне пользователей, но существенно возрастает при расширении его верхней границы.

Особое внимание в системах идентификации уделяется возможности обработки исключительных случаев – невозможности регистрации биометрических параметров (невозможность использования, регистрации, получения). Конечно, данные случаи уникальны в своем роде, но не исключены и должны учитываться при разработке биометрических систем идентификации.

Экономические затраты на разработку, внедрение и полноценное использование систем идентификации характеризуются ее стоимостными показателями. Современные высокоточные биометрические системы идентификации обладают высокими техническими характеристиками, которые существенным образом отражаются и на их стоимости. Порой возникают ситуации, когда их применение экономически не оправданно, ценность защищаемой информации уступает стоимости применяемых систем защиты, что крайне неэффективно и конечно же, необходимо учитывать.

К системам биометрической идентификации предъявляются требования и по безопасности прохождения процедуры пользователем, противном случае использование таких систем будет просто невозможным. К этой же категории требований относятся и вопросы безопасности самой системы идентификации от внешних угроз, возможных атак и компрометации.

Как и все технологии обеспечения безопасности и разграничения доступа системы идентификации должны и обязаны согласно законодательству гарантировать соблюдение конфиденциальности пользователей, что в свою очередь является еще одним требованием к системам биометрической идентификации.

Как следствие, перспективным направлением является проектирование и разработка мультибиометрических систем идентификации, обладающих повышенной точностью за счет учета ряда различных параметров (модальностей), экономически-выгод-

ными, благодаря использованию стандартных (недорогих) сенсоров, обладающих быстротой анализа и получения результатов. Данные системы должны обладать простотой и надежностью функционирования, компактным исполнения, для получения широкого распространения и комфортного использованиями различными категориями пользователей. Использование методов периодической скрытой динамической идентификации пользователя в таких системах позволит решить проблему «постоянства личности» и избежать атаки «подмена пользователя», что также приведет к повышению показателей степени защищенности охраняемой информации или объекта.

Список литературы

1. Болл Руд М. и др. Руководство по биометрии // Москва, Техносфера, 2007 – 368 с.
2. ГОСТ Р ИСО/МЭК 19795-1-2007 Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура.
3. Кухарев Г.А. Биометрические системы: методы и средства идентификации личности человека. – СПб.: Политехника, 2001 – 240. с.