УДК 004.93

О.А. Сущенок

Харьковский национальный университет радиоэлектроники, Харьков

ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОТЫ БИОМЕТРИЧЕСКИХ СИСТЕМ

Описываются основные параметры определяющие, эффективность работы биометрических систем, приведена тестовая база, по которой определяются эти параметры. Сформулированы рекомендации и критерии выбора значений параметров.

Ключевые слова: *биометрия; идентификация; отпечаток пальца; критерий; значение FAR; система.*

Введение

В настоящее время в связи с усилением борьбы с преступностью и терроризмом, подстегивающей рост индустрии безопасности, идентификация личности, которая производится с помощью биометрических технологий, - одно из самых перспективных и бурно развивающихся направлений. Среди биометрических методов и средств идентификации личности, ведущие позиции занимают биометрические (дактилоскопические) системы. В настоящей статье рассматривается количественная оценка их качества.

1. Количественная оценка работы биометрических систем

После того как система спроектирована, перед разработчиками встает задача ее тестирования для получения количественных характеристик, в частности, определение скорости работы и вероятности появления ошибок.

Для оценки качества работы алгоритма сравнения отпечатков пальцев существуют характеристики, по которым легко можно получить количественные показатели, определяющие надежность создаваемых систем [1].

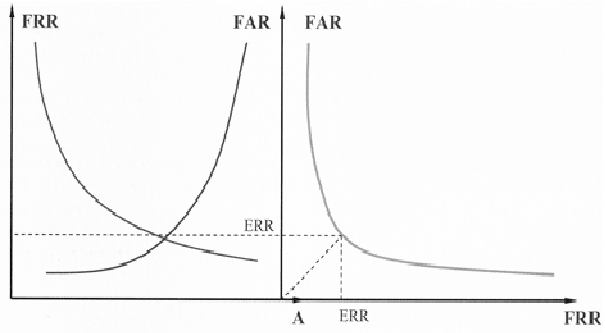
Эти характеристики сопровождаются наличием ошибок первого и второго рода.

Ошибка первого рода появляется при сравнениях "свой" к "своему", когда "свой" признается системой "чужим". Обозначается как FRR (False Rejection Rate) - вероятность ошибки первого рода, то есть вероятность отказа "своему". При этом существует и обратная характеристика ошибки первого рода: GAR (Genuine Acceptance Rate) = 1 - FRR, вероятность пропуска "своего".

Ошибка второго рода появляется при сравнениях "чужой" к "чужому", когда "чужой" признается "своим". Обозначается как FAR (False Acceptance Rate) - вероятность ошибки второго рода, то есть вероятность пропуска "чужого". Для комплексной оценки алгоритма существует параметр EER (Equal Error Rate) - уровень ошибок биометрической системы доступа, при котором FAR и FRR равны.

2. Тестовая база отпечатков

Для проведения испытаний с целью получения графиков FAR, FRR, GAR и точки EER необходимо подготовить специальную базу данных отпечатков пальцев. От ее размера зависит та точность, с которой эти характеристики будут определены. Такая база данных состоит из n (number of fingers) разных пальцев и m (number of samples) вариантов отпечатков каждого пальца, то есть общее число отпечатков в базе будет равно (n·m).



FRR – вероятность ошибки первого рода;
FAR – вероятность ошибки второго рода;
A – значение порога обнаружения;
EER – точка равенства вероятностей
(комплексный показатель качества)

Рис. 1. График FAR, FRR, GAR и точки EER

При создании тестовой базы отпечатков пальцев следует учитывать то обстоятельство, что использование синтезированных отпечатков не позволит получить реальную картину качества работы алгоритма. Таким образом, появляется необходимость набора больших баз реальных отпечатков разного типа.

Для упрощения этой процедуры возможно применение ряда алгоритмов, позволяющих значительно сократить объемы тестовых баз данных.

Например, для получения статистики ошибок первого рода необходимо произвести сравнение попарно между отпечатками одного ряда для обеспечения сравнений типа "свой" к "своему". Если первый отпечаток в ряду сравнивать со всеми другими

отпечатками ряда, то получается (m-1) сравнений; второй отпечаток в ряду сравнивать со всеми отпечатками, идущими после него, поскольку он уже сравнивался с первым отпечатком, то получаем (m-2) сравнения и т.д. Предпоследний отпечаток сравнивается только с последним отпечатком, получается одно сравнение. Таким образом, число сравнений в ряду составит:

$$V_i = (m-1)+(m-2)+K+1 = \frac{m(m-1)}{2}. \quad (1)$$

Если число рядов n, тогда возможное число сравнений "свой" к "своему" в базе из n пальцев по m отпечатков каждого будет:

$$VFRR = \frac{nm(m-1)}{2}. \quad (2)$$

Для получения статистики ошибок второго рода необходимо произвести сравнения попарно между отпечатками разных рядов, для обеспечения сравнений типа "чужой" к "чужому".

Первый отпечаток первого ряда сравнивается со всеми отпечатками всех остальных рядов, и получается (n-1)·m сравнений; также сравнивается второй отпечаток первого ряда, и получается еще (n-1)·m сравнений. После сравнений m отпечатков первого ряда со всеми отпечатками других рядов получаем $m^2(n-1)$ сравнений.

Отпечатки второго ряда сравниваются с отпечатками всех (n-2) рядов после него, поскольку они уже сравнивались с отпечатками первого ряда, и получается еще m^2 (n-2) сравнений. Указанная процедура осуществляется до предпоследнего ряда, который сравнивается уже только с единственным, последним, рядом, и получается еще m^2 сравнений. Это значит, что число возможных сравнений "чужой" к "чужому" в базе из n пальцев по m отпечатков каждого будет [2]:

$$VFAR = m^2\left[(n-1)+(n-2)+K+1\right] = \frac{m^2 n(n-1)}{2}. \quad (3)$$

Таким образом, например, в базе из 350 пальцев по 6 вариантов отпечатков каждого (Рисунок 1), возможно следующее число сравнений:

$$VFRR = \frac{nm(m-1)}{2} = \frac{350\times 6\times(6-1)}{2} = 5250;$$

$$VFAR = \frac{m^2 n(n-1)}{2} = \frac{6^2\times 350\times(350-1)}{2} = 2198700.$$

Использование такого метода позволяет получать достаточно большое количество вариантов сравнений, необходимых для построения характеристик при несопоставимо меньших количествах отпечатков пальцев в тестовой базе.

Рис. 2. Пример различных положений отпечатка пальца при сканировании

3. Критерии выбора значений FAR и FRR

Прежде чем приступить к формулированию критериев выбора требуемых значений FAR и FRR, постараемся еще раз проанализировать роль каждого из параметров.

С одной стороны, высокое значение FRR (вероятность ошибочного задержания "своего") может привести к дискредитации системы и снижению эффективности ее функционирования, так как при частых ложных срабатываниях персонал охраны практически перестает обращать внимание на задержания или отказы в доступе. С другой стороны, высокое значение FAR (вероятность ошибочного пропуска "чужого") увеличивает вероятность несанкционированного доступа. Учитывая зависимость FAR, FRR от установленных порогов обнаружения, следует отметить, что задача выбора порогов для администратора системы безопасности объекта чрезвычайно актуальна. Постараемся наметить пути для определения методик выбора требуемых значений и последующей их оптимизации.

Для этого выясним, какой из параметров следует задать, а какой в процессе эксплуатации и отработки системы улучшить. Очевидно, что критерии выбора значения параметра должны опираться на требования регламентирующих документов, которые устанавливают, что любая автоматизированная система безопасности объекта строится исходя из принципов равнопрочности, зональности, адаптивности, адекватности, надежности, контролируемости.

Принцип равнопрочности предполагает сбалансированность значений физической укрепленности и вероятностных характеристик обнаружения по всей границе охраняемой зоны. Как известно, граница представляет собой совокупность средств охранной сигнализации, телевизионного наблюдения, управления доступом и инженерной защиты, располагаемых по периметру и КПП объекта. Таким образом, руководствуясь данным требованием, можно

предположить, что вероятность обнаружения нарушителя на КПП должна быть, по крайней мере, сопоставима с вероятностью обнаружения на периметре (при соблюдении условий примерного равенства параметров, характеризующих физическую защищенность рубежей охраны). Допустим, что вероятность обнаружения на периметре равна P, тогда требуемое значение FAR определятся формулой: FAR = 1 - P. Таким образом, задаваясь значением FAR и исходя из принципа равнопрочности, необходимо выполнить условия физической защищенности КПП, к которым можно отнести следующие:

– использование шлюзовых (блокирующих) технологий, обеспечивающих автоматическое задержание несанкционированного лица;

– видеоподтверждение и видеодокументирование случаев задержания;

– допущение только одной попытки предъявления биометрических параметров;

– совмещение процедур биометрического контроля с проверкой полномочий по другим, в том числе присвоенным признакам (коды, пароли и т.д.).

Если руководствоваться предложенной методикой оценки значения FAR, становится очевидным, что принцип зонального построения и адекватности также будет влиять на выбранное значение FAR.

Следует подчеркнуть необходимость соблюдения принципов адаптивности и контролируемости параметров биометрической системы. В данном случае адаптивность предполагает обязательное наличие возможности в применяемой системе изменения порогов обнаружения.

Принцип контролируемости должен обеспечиваться в первую очередь наличием встроенных средств расчета FAR и FRR. При этом для расчета FAR целесообразно использовать математический аппарат сравнения методом "чужой" к "чужому" хранящихся в базе данных "эталонов" при вариации порога обнаружения.

Для оценки FRR целесообразно использовать отношение количества отказов в доступе по критерию "биометрический контроль не пройден" к общему количеству попыток предъявления биометрических параметров (в упрощенном случае - к общему числу проходов).

К сожалению, при первом запуске системы данные для определения FRR указанным методом, или сравнением "свой" к "своему" в системе по понятным причинам отсутствуют.

Таким образом, установив значение FAR как обязательный для реализации системный параметр и, следовательно, порог обнаружения, включаем систему на массовый проход.

Выводы

Рассмотрены особенности оценки эффективности работы биометрических систем, которые заключаются в больших массивах, подлежащих обработке. Показано, что:

1) при создании тестовой базы отпечатков пальцев следует учитывать то обстоятельство, что использование синтезированных отпечатков не позволит получить реальную картину качества работы алгоритма;

2) возможно применение ряда алгоритмов, позволяющих значительно сократить объемы тестовых баз данных;

3) необходимо соблюдение принципов адаптивности и контролируемости параметров биометрической системы;

4) принцип зонального построения и адекватности также влияет на выбранное значение FAR.

Список литературы

1. Вакуленко А. Биометрические методы идентификации личности: обоснованный выбор и внедрение / А. Вакуленко, А. Юхин. – М.: Наука, 2007. – 224 с.

2. Зиятдинов А.И. Принципы построения систем биометрической аутентификации / А.И. Зиятдинов. – М.: МФТИ, 2005. – 188 с.

Поступила в редколлегию 14.03.2011

Рецензент: д-р техн. наук, проф. А.М. Синотин, Харьковский национальный университет радиоэлектроники, Харьков.

ОЦІНКА ЕФЕКТИВНОСТІ РОБОТИ АЛГОРИТМІВ БІОМЕТРИЧНИХ СИСТЕМ

О.О. Сущенок

Описуються основні параметри визначаючі, ефективність роботи біометричних систем, наведена тестова база, по якій визначаються ці параметри. Сформульовані рекомендації й критерії вибору значень параметрів.

Ключові слова: *біометрія, ідентифікація, відбиток пальця, критерій, значення FAR, система.*

ESTIMATION OF AN OVERALL PERFORMANCE OF BIOMETRIC SYSTEMS

O.A. Sushchenok

Key parameters defining are presented, the overall performance of biometric systems, is resulted test baseline on which these parameters are defined. Guidelines and criteria of sampling of values of parameters are formulated.

Keywords: *biometrics, identification, a fingerprint, criterion, value FAR, system.*