УДК 004.032.26:004.421

А.В. Андреев, Д.А. Скоринов
Московский Физико-Технический Институт (ГУ), г. Москва, Россия
andresj@mail.ru; skorinov@mail.ru

Алгоритмы слияния данных в биометрических системах и применение в них нейросетевых технологий

Биометрическое слияние данных – это процесс объединения информации от нескольких источников, изначально полученной от пользователя с помощью захвата нескольких образцов одной биометрической модальности многими сенсорами, или получением нескольких образцов множества модальностей, или с захватом одного образца с последующей его обработкой многими алгоритмами. В данной статье подается систематическое описание известных методик биометрического слияния в задачах верификации и идентификации, подробно рассмотрены достоинства и недостатки алгоритмов слияния на различных уровнях иерархии биометрической системы, приведены наиболее распространенные методы нормализации данных в биометрических системах.

Вводные понятия

Биометрическая характеристика – измеримая биологическая или поведенческая характеристика человека, измерения которой являются достаточной информацией для надежного различия индивидуума от других пользователей.

Биометрическая модальность – каждая из биометрических характеристик, одна или более из которых используются в биометрических процессах.

Биометрический процесс – автоматический процесс, использующий одну или несколько биометрических характеристик одного индивида с целью регистрации, верификации или идентификации.

Мультибиометрический процесс – биометрический процесс, использующий биометрическое слияние данных.

Мультибиометрическая система – система, обеспечивающая автоматическое распознавание индивидов на основе биологических или поведенческих характеристик с использованием биометрического слияния данных.

Мультимодальная система – система, использующая несколько биометрических модальностей.

Мультиалгоритмический процесс – процесс с использованием нескольких алгоритмов для обработки одного и того же биометрического образца.

Многосенсорная система – система с использованием нескольких сенсоров для измерения одного биометрического экземпляра.

Структура биометрической системы. Иерархия уровней слияния данных

В качестве базиса для определения уровней слияния данных в мультибиометрических системах сначала следует определить однобиометрический процесс и составляющие

его блоки на примере системы авторизации. На рис. 1 показана блок-схема однобиометрического процесса.

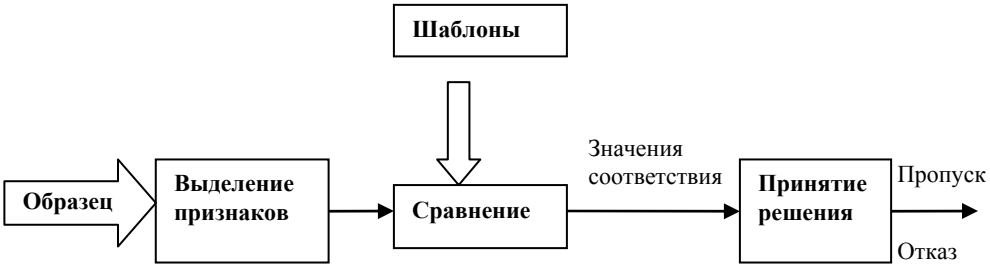

Рисунок 1 – Схема однобиометрического процесса

Биометрическим сенсором проводится захват биометрического образца (например, снимок отпечатка пальца) и передается модулю выделения признаков. С помощью методов обработки сигнала модуль выделения признаков преобразует образец в вектор признаков (например, набор минуций для отпечатков пальцев), которые формируются в представлении, пригодном для сравнения. Устройство сравнения получает на вход вектор признаков и сравнивает его с сохраненным шаблоном. Результатом являются значения соответствия, используемые модулем вынесения решения для получения ответа (часто, с применением порогового значения) на вопрос, соответствует ли предложенный образец сохраненному шаблону. Выходными данными модуля является бинарное значение «соответствие/несоответствие».

Обобщая вышеописанный процесс, на случай мультибиометрической системы можно выделить следующие уровни, на которых возможно применение методов слияния. Объединение информации может производиться на уровне вынесения решений (1), на уровне значений соответствия (2), на уровнях признаков (3) и биометрических образцов (4). Отметим, что слияние на уровнях (1) и (2) происходит после привлечения устройства сравнения, в то время как уровни (3) и (4) проводят операции до того, как устройство сравнения выдаст результирующие данные. Хотя интеграция данных возможна на всех перечисленных уровнях, слияние на уровнях множества признаков, значений соответствия и вынесения решений используется наиболее часто. На рис. 2 показаны различные уровни слияния на случай мультимодальных систем.

а) **Уровень решений:** каждый отдельный биометрический процесс в качестве выходных данных получает булево значение. Обычно процесс их слияния происходит с помощью объединяющих алгоритмов на основе логических функций дизъюнкции и конъюнкции.

б) **Уровень значений** соответствия: каждый отдельный биометрический процесс обычно выдает как результат значение соответствия, но иногда это может быть и массив значений.

в) **Уровень признаков:** каждый процесс имеет на выходе набор признаков. Процесс слияния объединяет эти наборы в одно множество или в один вектор признаков.

г) **Уровень образца:** каждый отдельный процесс получает в качестве выходных данных набор образцов. При слиянии эти наборы преобразуются в единый биометрический образец.

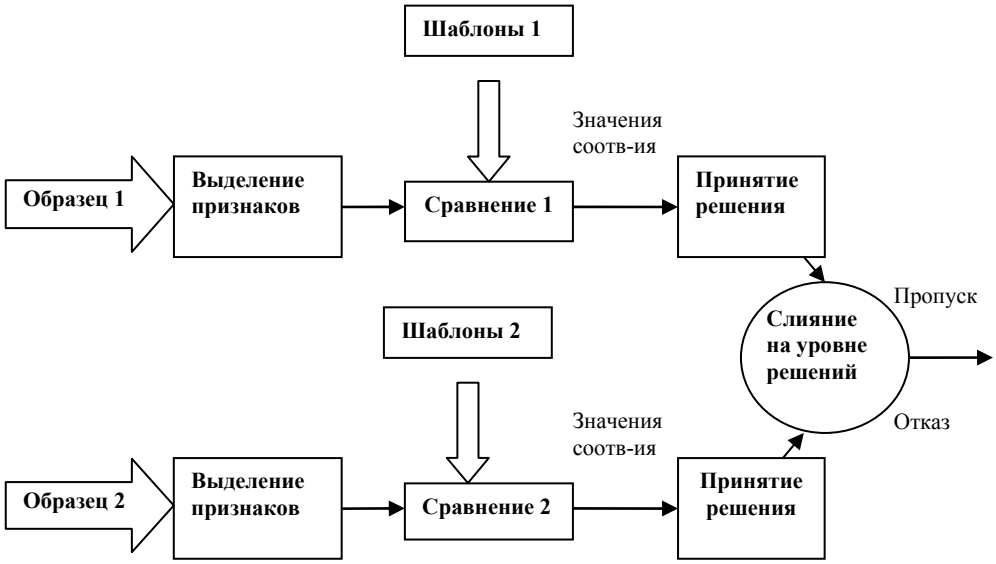

Рисунок 2 – Слияние данных на уровне принятия решений

Рисунок 3 – Слияние данных на уровне значений соответствия

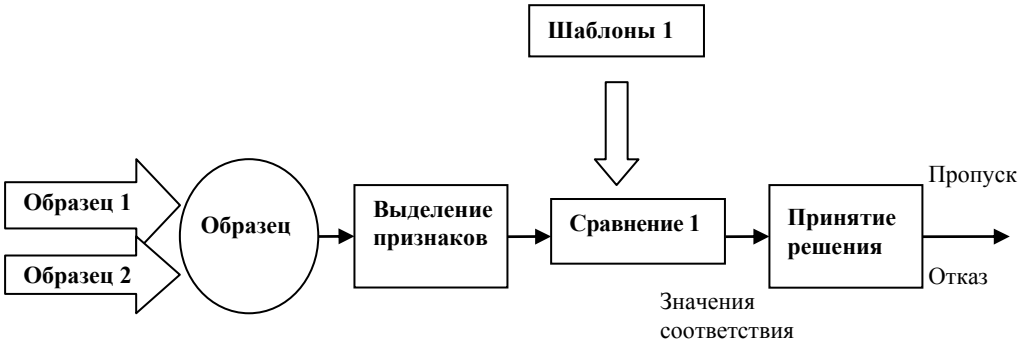

Рисунок 4 – Слияние данных на уровне образцов

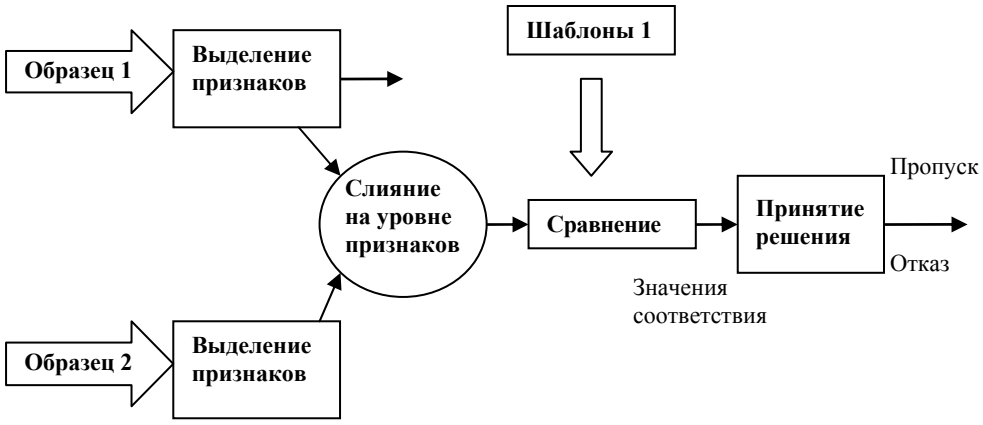

Рисунок 5 – Слияние данных на уровне выделения признаков

Слияние на уровне решений

Для биометрических систем, состоящих из небольшого числа компонент, в качестве оценки соответствия удобно использовать логические значения таким образом, чтобы алгоритм слияния формулировался в виде логических функций. Наиболее часто для этого используются функции логических И и ИЛИ. Для биометрических систем с многими компонентами в качестве метода слияния общепринято использовать схемы голосования, наиболее распространенной из которых является схема большинства голосов.

Считается, что ввиду потери информации при преобразовании необработанных данных в вектор признаков и, в конечном счете, в выходные данные модулей принятия решения можно ожидать, что точность классификации будет наиболее низкой для слияния на уровне решений. Тем не менее, известно, что искажение информации по причине шумов потенциально выше, и требования к регистрации данных жестче именно на нижних уровнях слияния. Кроме этого, низкоуровневое слияние менее устойчиво к поломке сенсоров и требует большей обучающей выборки, т.к. обычно в нем используется большее число свободных параметров, нежели в слиянии на более высоких уровнях. В дополнение к этому часто используемое в целях упрощения работы предположение о независимости между данными отдельных сенсоров лучше выполняется на уровне решений, в случае, если классификаторы не принадлежат к одному типу.

Слияние на уровне признаков

При слиянии на уровне признаков объединение биометрической информации происходит после выделения признаков из образца, но перед проведением сравнения. В случае, когда признаки не являются независимыми, например, в случае мультибиометрических систем, хороший алгоритм слияния на уровне признаков позволяет использование зависимостей в более полной мере, по крайней мере, при некоторых обстоятельствах, чем это возможно при слиянии на уровне значений соответствия, что позволит достичь лучшей производительности системы. Однако слияние на этом уровне является сложной задачей с практической точки зрения в силу ряда причин:

– векторы признаков от разных модальностей могут быть несовместимы (например, набор минуций для отпечатка пальцев или собственные векторы для изображения лица);

– соотношения между множествами значений различных биометрических векторов могут быть неизвестны;
– объединение двух векторов признаков может привести к образованию вектора с чрезмерно большой размерностью, и, следовательно, возможен случай проблемы «проклятия размерностей»;
– может потребоваться значительно более сложное устройство сравнения для обработки объединенного вектора признаков.

Слияние на уровне значений соответствия

Теоретически для любого количества соответствующим образом описанных биометрических процессов можно так провести слияние их значений соответствия, что объединенная система будет гарантированно работать не хуже одиночных биометрических устройств. Ключевым моментом является верное нахождение надежного метода объединения этих значений соответствия, максимизирующего улучшение производительности. Как для задачи верификации (1:1), так и для задачи идентификации (1:N) системы могут поддерживать слияние данных на уровне значений соответствия. Тем не менее, системы идентификации могут также проводить объединение данных на уровне информации о ранге претендента (что является формой уровня значений с многими параметрами или индексами, полученными на множестве значений соответствия). В контексте задачи верификации, существует два различных подхода к слиянию данных на уровне значений соответствия. Один метод состоит в постановке слияния как задачи классификации данных, в то время как другой подход представляет собой проблему правильного сложения значений. При классификации из значений соответствия отдельных устройств сравнения составляется вектор признаков, который затем классифицируется в один из двух классов: «Пропуск» (подлинный пользователь) или «Отказ» (злоумышленник). В общем случае используемый для этого классификатор (например, дерево решений, нейросетевые модели, машины вспомогательных векторов и пр.) обучается правильному определению границ классов независимо от способа получения вектора признаков.

В другом подходе значения отдельных устройств сравнения объединяются для получения единой скалярной величины, которая впоследствии используется для вынесения окончательного решения о «пропуске»/«отказе». Для обеспечения качественного объединения значений с различных модальностей значения должны быть сначала преобразованы к одному типу. Этот процесс известен как нормализация значений.

Методы нормализации значений соответствия

В большинстве случаев распределения каждого набора значений зависят от модальности или алгоритма сравнения, потому распределения этих значений не обязательно будут принадлежать одному численному диапазону. Таким образом, необходимо, чтобы процессу слияния предшествовал процесс нормализации значений. Наиболее распространенные методы нормализации приведены ниже (далее используются обозначения: n – нормализованные значения, s – необработанные результаты, std() – среднеквадратичное отклонение):

Минимум-Максимум, ММ (Min-Max): необработанные результаты масштабируются на отрезок [0;1]. При этом величины min и max являются границами диапазона нормализуемых значений:

$$n = \frac{s - \min(S)}{\max(S) - \min(S)}.$$

Тангенциальный метод, TH (Tanh): тангенциальный метод является одним из так называемых устойчивых статистических методов, который отображает необработанные результаты на интервал (0;1):

$$n = \frac{1}{2}\left[\tanh\left(0.01\frac{\left(s-\overline{S}\right)}{std\left(S\right)}\right)+1\right].$$

Z-преобразование, (Z-score): данный метод преобразует данные в распределение с нулевым средним и среднеквадратичной ошибкой std(S), равной 1.

$$n = \frac{s-\overline{S}}{std\left(S\right)}.$$

Однако существуют и более сложные вычислительные методы нормализации, для лучшего соответствия условиям конкретных задач:
Адаптивная нормализация AD, метод двух квадратов (Two-Quadrics) и метод квадрат-прямая-квадрат (Quadric-Line-Quadric)

$$n = \begin{cases} \dfrac{1}{mid}n_{MM}^2, & n_{MM} \le mid \\ mid + \sqrt{(1-mid)(n_{MM}-mid)}, & n_{MM} > mid \end{cases},$$

mid – середина пересечения предварительно известных распределений, d – ширина области пересечения.

Во втором методе неизменной остается зона перекрытия распределений, прочие области преобразуются аналогично вышеуказанному способу.

$$n = \begin{cases} \dfrac{1}{mid-\frac{d}{2}}n_{MM}^2, & n_{MM} \le \left(mid-\frac{d}{2}\right) \\ n_{MM}, & \left(mid-\frac{d}{2}\right) < n_{MM} \le \left(mid+\frac{d}{2}\right) \\ \left(mid+\frac{d}{2}\right)+\sqrt{(1-mid)(n_{MM}-c)}, & n_{MM} > \left(mid+\frac{d}{2}\right) \end{cases}$$

Аппроксимация с помощью HBF нейронных сетей

Метод заключается в приближении функции распределения значений соответствия, полученных при сравнении подлинных образцов с шаблонами из базы данных, с помощью нейросетевой модели, обученной на распознавании образцов злоумышленников и подлинных пользователей.

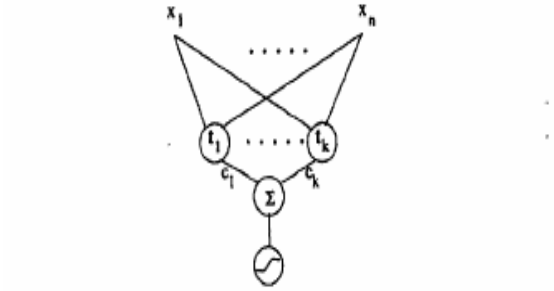

Рисунок 6 – Схема предлагаемой сети HyperBF

Минимизируя ошибку *E*, мы получаем расположение *t*, форму ∑ и высоту *c* каждого гауссовского пика:

$$E = \sum_i \left[y_{ij} - \sigma\left(\sum_\alpha c_\alpha G\left(\left| x_{ij} - t_\alpha \right|_\sum \right) \right) \right]^2 ,$$

где y_{ij} – вектор значений из базы данных

$$G(x) = e^{-x^2}$$

$$\sigma(x) = \frac{1}{1 + e^{4(x-1/2)}}$$

$$L(x, t, c, \alpha, \sum) = \sigma\left(\sum_\alpha c_\alpha G\left(\left| X - t_\alpha \right|_\sum \right) \right),$$

где L(x) – семейство функций, приближающих искомую функцию распределений.

При обучении используются как позитивные, так и негативные случаи распознавания пользователя, и суть метода состоит в правильном распределении полученных значений степени соответствия между 0 (отказ) и 1 (пропуск).

Алгоритмы слияния нормализованных значений соответствия

Суммирование нормализованных сигналов с различными весами (Weighted Sum)

Если принять все веса одинаковыми, то все биометрические датчики будут иметь равное значение в вынесении решения, вне зависимости от точности их работы или физических особенностей пользователей. Потому следующие методы могут не быть достаточно эффективными:

– *Простая сумма* $f = \sum_i n_i$ (i – номер устройства сравнения);

– *Минимальное значение* $f = \min(n_1, n_2, n_3 \text{K})$;

– *Максимальное значение* $f = \max(n_1, n_2, n_3 \text{K})$

(здесь и далее: f – объединенное значение, результат объединения значений отдельных датчиков, w – присвоенный вес).

Разумно присваивать каждому датчику вес в зависимости от его точности, т.е. обратно пропорционально его суммарной ошибке на начальной (обучающей) выборке. В задаче верификации удобно также изменять значение весовых коэффициентов датчиков в зависимости от конечного пользователя.

Сумма с весами датчиков

$$f = \sum_i w_i n_i$$

$$w_i = \frac{\frac{1}{ERR_i}}{\sum_j \frac{1}{ERR_j}}$$

, где *i* – номер датчика.

$$\sum_i w_i = 1$$

ERR = FAR + FRR – сумма ошибок ложного пропуска (False Acceptance Rate) и ложного отказа (False Rejection Rate) соответственно.

Необходимо отметить, что значение ошибок ложного пропуска и отказа (FAR и FRR) для каждой биометрической системы вычисляется при конкретном пороговом значении. Поэтому, при отсутствии возможности менять пороговые значения одномодальных биометрических систем, слишком большое влияние на итоговый результат объединения имеют настройки и точность одномодальных систем, тем самым уменьшается роль алгоритма объединения.

Какой бы алгоритм не был выбран для суммирования с весовыми коэффициентами входных сигналов, критерий решения о пропуске или отказе данному пользователю будет зависеть от порогового значения для суммарного результата *f*, что и является основной сложностью данных алгоритмов.

Нейросетевые методы и методы, основанные на линейной классификации, лишены этой сложности.

Методы классификации в задаче слияния данных на уровне значений соответствия

С точки зрения задачи классификации образов, при подходе классификации в слиянии данных, цель модели слияния состоит в нахождении оптимального разделителя двух классов на классы авторизованных и неавторизованных пользователей. Классификатор получает вектор значений соответствия от устройств сравнения и определяет его к одному из двух классов. С этой целью определяются две области решений в пространстве векторов признаков, одна для класса подлинных пользователей и вторая для злоумышленников. Эти области разделены границами решений, которые следует оптимизировать в процессе разработки модели слияния. Вне зависимости от выбранного метода конечной целью является нахождение границ решений, улучшающих производительность классификатора, удовлетворяющего конкретному приложению. Ниже описаны наиболее распространенные классификаторы.

Линейная классификация. Дискриминантный анализ Фишера

Пусть на основе предварительной выборки n_1 и n_2 – множества векторов двух классов, вектор x принадлежит соответственно одному из этих классов, тогда:

$m_i = \frac{1}{n_i}\sum_{x \in C_i} x$ – средние вектора для обоих классов $i \in \{1;2\}$;

$S_i = \sum_{x \in C_i} (x - m_i)(x - m_i)^T$ – матрицы рассеивания внутри классов $i \in \{1;2\}$;

$S_0 = (m_2 - m_1)(m_2 - m_1)^T$ – матрица расстояния между классами.

Тогда искомое направление p проекции $y = p^T x$ находится из максимизации следующего функционала:

$F(p) = \frac{p^T S_0 p}{p^T (S_1 + S_2) p}$ и достигается при $p = (S_1 + S_2)^{-1}(m_1 - m_2)$.

Полученное множество обладает наибольшим расстоянием между двумя классами, потому задача вынесения решения сводится к сравнению $y(x)$, получен-

ного от проверяемого претендента, со значением разделяющей плоскости $Y(X_0)$. Отметим, что для данного метода требуется, чтобы множества входных данных были линейно-разделимы.

Нейросетевые методы классификации

Нейросетевой подход с успехом применяется в задачах кластеризации и классификации данных, а также в задачах слияния данных в робототехнике и распознавании контекста.

В биометрической постановке проблемы требуется разбиение входного потока данных на два класса (злоумышленников и авторизованных пользователей), для чего могут использоваться различные виды нейронных сетей – нейросети с радиальными базисными функциями RBF (Radial Basis Function), персептронные модели с одним и более скрытыми слоями, модели с обратным распространением ошибки и пр. Часто используемый в мультимодальных биометрических системах метод слияния данных с помощью байесовских оценок также реализуем на базе нейросети.

На вход нейросети подаются нормализованные данные с различных датчиков, каждому из которых сеть в ходе обучения находит весовой коэффициент, минимизируя ошибку распознавания. Обучение происходит на предварительно сформированной базе данных шаблонов. При этом нейросеть может присваивать вес входу в зависимости от конкретного конечного пользователя. Положительным моментом является то, что для обучения нейросетей можно применять как шаблоны авторизованных пользователей, так и заведомо неверные шаблоны. Таким образом, получается точное приближение распределений авторизованных и неавторизованных пользователей, что облегчает задачу классификации.

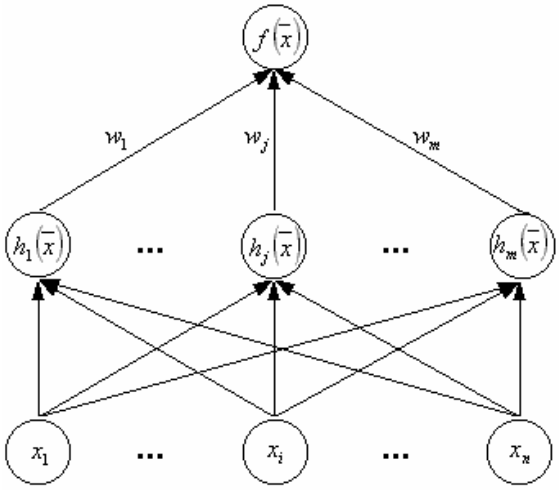

Рисунок 7

В зависимости от используемой модели приближение может производиться различными функциями. Например, нейросети с радиальными базисными функциями используют следующий класс функций:

$$h(x) = \exp\left(-\frac{\left\|\bar{x}-\bar{c}\right\|^2}{r^2}\right),$$

где c – смещение пика Гаусса, а r – его ширина.

Следует отметить, что основная вычислительная нагрузка приходится именно на процесс обучения сети, в рабочем режиме вычисления сводятся к суммированию

сигналов датчиков с различными весами, что обеспечивает высокую скорость работы системы.

В задаче верификации целесообразно обучать отдельную нейросеть для каждого пользователя из базы данных, при этом достигается хорошая точность, превосходящая точность алгоритмов Фишера и сумм с весами.

К сожалению, в настоящее время нейросетевые технологии мало применяются в задачах слияния данных в биометрических системах, несмотря на успешный опыт их применения в других системах слияния данных. Очевидно, что нейросетевой подход обеспечивает большую гибкость и адаптивность системы к внешним воздействиям. Например, на точности работы системы не отразится случай неисправности одного из датчиков или невозможности получения одного биометрического признака.

Машины поддерживающих векторов SVM (Support Vector Machine)

Целью метода является нахождение функции f, разделяющей преобразующее пространство значений входных данных на множество классов (состоящей из 2 классов, в данном случае злоумышленников и подлинных пользователей).

$$f : \Re^n \longrightarrow \{+1,-1\}$$

$$x_k \longrightarrow y_k$$

При этом линейная функция решения имеет вид $f(x) = sign(w * x + b)$, а задача состоит в отыскании оптимального набора параметров $\{w,b\}$, что может быть приведено к задаче квадратичного программирования. Основная особенность алгоритма – конечное выражение функции содержит только значения, лежащие близко к разделяющей поверхности, так называемые поддерживающие вектора.

Недостатком метода является большая вычислительная сложность расчетов для SVM. Несмотря на то, что ресурсоемкость вычислений предполагает трудности только на предварительном этапе обучения и зависит от количества входных данных, а при эксплуатации этап классификации с помощью SVM является простым суммированием с заранее определенными коэффициентами, данный метод является сложным для применения.

Заключение

В современных задачах биометрического распознавания личности преимущества мультимодальных систем становятся все более очевидными. Обязательным этапом работы таких систем является нормализация данных, выбор метода которой зависит от условий практической задачи. Вышеизложенные методы бинарной классификации входных данных весьма эффективны, при этом выгодным отличием нейросетевых алгоритмов является меньшая зависимость от пороговых значений одномодальных систем, качества приближения функций распределения значений соответствия пользователей и наличия обучающей выборки изображений подлинных пользователей.

Литература

1. ISO/IEC JTC 1/SC 37 N 1506 “Multimodal and Other Multibiometric Fusion” 2006-05-28.
2. YunhongWang, Tieniu Tan, and Anil K. Jain. Combining Face and Iris Biometrics for Identity Verification. – National Lab of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Department of Computer Sciences Engineering, Michigan State University: fjaing@cse.msu.edu

3. Roberto Brunelli and Daniele Falavigna. Person Identification Using Multiple Cues // IEEE Transactions on Pattern Analysis and Machine Intelligence. – Vol. 17, no. io, october 1995.
4. Souheil Ben-Yacoub, Yousri Abdeljaoued, and Eddy Mayoraz. Fusion of Face and Speech Data for Person Identity Verification // IEEE Transactions On Neural Networks, Vol. 10, № 5, September 1999.
5. Anil K. Jain and Arun Ross. Learning User-Specific Parameters In A Multibiometric System. – Department of Computer Science and Engineering, Michigan State University
6. Arun Ross, Anil Jain. Iformation Fusion in biometrics. – Department pf Computer science and Engineering, Michigan State University.
7. Arun Ross and Anil K. Jain. Multimodal Biometrics: An Overview. – West Virginia University; Michigan State University; ross@csee.wvu.edu jain@cse.msu.edu
8. Claude C. Chibelushi, Farzin Deravi. A Review of Speech-Based Bimodal Recognition // IEEE Transactions On Multimedia. – Vol. 4, № 1, March 2002.

А.В. Андрєєв, Д.А. Скорінов

Алгоритми злиття даних у біометричних системах і застосування у них нейромережних технологій

Біометричне злиття даних – це процес об'єднання інформації від декількох джерел, з початку отриманої від користувача за допомогою захоплення декількох зразків однієї біометричної модальності багатьма сенсорами, або отриманням декількох зразків багатьох модульностей, або із захопленням одного зразка з наступною його обробкою багатьма алгоритмами. У даній статті подано систематичний опис відомих методик біометричного злиття в задачах верифікації та ідентифікації, детально розглянуто переваги та недоліки алгоритмів злиття на різних рівнях ієрархії біометричної системи, наведено найбільш поширені методи нормалізації даних у біометричних системах.

A.V. Andreyev, D.A. Skorinov

Biometric Data Fusion Techniques and Neural Networks Technologies Applications

Current article provides a comprehensive overview of up to date Data Fusion methods concerning verification and identification problems. In addition, drawbacks and benefits of biometric data fusion on different levels are considered. Moreover, a most frequently used normalization techniques for matching scores are described. Special attention is put on the applications of neural networks technologies for their good performance in the clusterization and classification problems.

Статья поступила в редакцию 23.06.2006.