ВЛИЯНИЕ ВХОДНЫХ ПАРАМЕТРОВ АЛГОРИТМОВ ДАКТИЛОСКОПИИ НА КАЧЕСТВО ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

Н.В. Едакин, Н.Н. Минакова
Алтайский государственный университет, г. Барнаул

Введение

Биометрическая система аутентификации в зависимости от контекста применения может работать в двух режимах: верификации (сравнение один к одному) и идентификации (сравнение один ко многим) отпечатков пальцев. Задача верификации состоит в подтверждении личности, в то время как задачей идентификации является установление личности субъекта доступа. Метод дактилоскопической регистрации и последующего дактилоскопического анализа в целях идентификации личности, как высокоэффективный и не требующий больших материальных затрат, широко применяется не только при защите информации, но и в судебно-медицинской экспертной практике и в других областях. Ы связи с этим разработка новых эффективных дактилоскопических методов идентификации личности является актуальной задачей.

Существует большое количество программных систем, реализующих идентификацию по отпечатку пальца с помощью разных алгоритмов. Все алгоритмы можно условно разделить на три класса [1]: корреляционное сравнение (вычисление взаимной корреляции двух изображений отпечатка [2]), сравнение минуций [3, 4], сравнение потоков папиллярных линий и папиллярных узоров [5]. Наиболее часто применяется подход, основанный на сравнении минуций, из-за того, что данный подход достаточно легко реализуем и достаточно не требователен к ресурсам вычислительной машины. Минуцией (или точкой Гальтона) называется особая точка папиллярной линии, как правило, обрыв линии или раздвоение линии (бифуркация). В этом случае задача верификации отпечатков пальцев сводится к задаче сравнения двух множеств точек, т.е. поиску такого геометрического преобразования (как правило, аффинного), переводящего максимальное количество точек из первого отпечатка в точки второго.

В статье ставится цель провести сравнительный анализ двух подходов, которые реализуют популярный алгоритм сравнения по особым точкам. Первый из подходов, будет реализовывать сравнение только на основе минуций, а второй, будет проводить это же сравнение, но с дополнительными модификациями. В процессе сравнения необходимо узнать не только, какой из алгоритмов будет производить идентификацию лучше, но и выявить взаимосвязь качества идентификации от входных параметров. Для этого необходимо решить ряд сопутствующих задач:

- провести экспериментальные сравнения качества идентификации выбранных подходов, используя изображения отпечатков пальцев из открытых баз данных FVC2004 [6] и CrossMatchDB [7];
- используя показатели эффективности биометрических систем, провести анализы полученных результатов;
- выявить влияние примененного подхода и входных параметров на качество идентификации.

Сравнение подходов

Для сравнения между собой из всех доступных подходов было выбрано два, которые находятся в открытом доступе. Первый подход, Kjanko, написан на языке программирования Python и реализует простое сравнение отпечатков по особым точкам [8]. Второй подход - SourceAFIS выполнен в виде библиотеки для разных языков программирования. Была выбрана реализация для языка Java. Для использования этой библиотеки была написана программа на языке программирования Scala, работающая на платформе Java. Сам подход SourceAFIS

реализует сравнение отпечатков по особым точкам с добавлением направлений точек и ребер, связывающих ближайшие точки, высчитываемые методом k-ближайших соседей [9].

Источниками отпечатков пальцев выступили две открытых базы данных FVC2004 [6] и CrossMatchDB [7]. Характеристики изображений из этих баз представлены в таблице 1. База данных FVC2004 была выбрана потому, что она имеет в себе изображения разного качества, снятые разными сенсорами. А также на данном типе БД проводились соревнования по дактилоскопии. Также для проведения анализа были необходимы изображения высокого качества. Для этих целей хорошо подошла база данных CrossMatchDB.

Каждый файл с отпечатком в обеих базах именован следующим образом: x_y_z.tif., где x - это уникальный идентификатор пользователя, предоставившего свои отпечатки для БД, y - номер пальца этого пользователя и z — номер самого изображения. В каждой базе у каждого пользователя имеется по восемь отпечатков каждого пальца. Отпечатки из баз были разделены на две части: тестовые изображения и эталонные. Из восьми изображений каждого пальца отдельного пользователя в тестовую выборку пошло пять изображений, в эталонную — три. В данном случае эталонные изображения играют роль базы данных системы контроля доступа, а тестовые изображения - это изображения отпечатков пользователей, которые пытаются получить доступ в эту систему.

Таблица 1. Характеристики изображений в базах данных

Выборка данных	Тип сенсора	Размеры изображения	Разрешение сенсора
FVC2004 DB1	Optical Sensor	640x480	500 dpi
FVC2004 DB2	Optical Sensor	328x364	500 dpi
FVC2004 DB3	Thermal sweeping Sensor	300x480	512 dpi
FVC2004 DB4	SFinGe v3.0	288x384	около 500 dpi
CrossMatchDB	Verifier 300	504x480	500 ppi

Выбранные подходы были адаптированы к решению поставленной цели. В подходе Kjanko была оптимизирована функциональность предобработки изображений. Добавлена функциональность, позволяющая уменьшать размерность исходного изображения без значительной потери качества идентификации по полученному отпечатку. Убраны функции дополнительной скелетизации отпечатка, которые не давали прироста в качестве идентификации, но значительно замедляли выполнение программы. Были разработаны функции генерации шаблонов, которые представляли собой предобработанные изображения исходных отпечатков пальцев. Эти функции позволили ещё ускорить выполнение алгоритма. Шаблоны создавались при старте программы на основе всех входных изображений, и в процессе выполнения для сравнения использовались именно шаблоны.

Для обоих подходов, SourceAFIS и Kjanko, были написаны программные функции, позволяющие проводить расчёт показателей эффективности, и функции сравнения отпечатков «один ко многим», где «одним» отпечатком выступал отпечаток из тестового набора, а «многими» - отпечатки из эталонной выборки. Для удобного проведения сравнения каждый входной файл отпечатка был преобразован в модель «пользователь». Модель состоит из следующих полей: идентификатор пользователя, идентификатор пальца, номер изображения и шаблон самого отпечатка.

Само сравнение происходило следующим образом. Оба подхода работают по одному принципу. Входной отпечаток преобразовывается в модель, описанную ранее, далее из модели берётся шаблон отпечатка и сравнивается со всеми шаблонами отпечатков пальцев из эталонной выборки. В процессе сравнения используется основной параметр, называемый порог срабатывания (threshold). Порог срабатывания

– это количество особых точек, которые должны совпасть, чтобы система решила, что отпечатки совпадают. В результате сравнения система возвращает ответ, который относится к одному из двух классов. Первый класс – отпечатки совпадают. Ответ системы: 1. Второй класс – отпечатки не совпадают. Ответ системы: 0. Далее ответ системы сравнивается с реальным значением совпадения проверенных отпечатков. В результате конечный ответ может быть четырёх видов:

- True positive (TP) – система дала ответ, что отпечатки совпадают, и отпечатки на самом деле совпадают;
- False Positive (FP) – система дала ответ, что отпечатки совпадают, но на самом деле они не совпадают. Ошибка первого рода;
- True Negative (TN) – система дала ответ, что отпечатки не совпадают, и они на самом деле не совпадают;
- False Negative (FN) – система дала ответ, что отпечатки не совпадают, а на самом деле они совпадают.

Для наглядности все возможные варианты ответа системы представлены в таблице 2.

Таблица 2. Варианты ответов системы

	y = 1	y = 0
$\hat{y} = 1$	True Positive (TP)	False Positive (FP)
$\hat{y} = 0$	False Negative (FN)	True Negative (TN)

Здесь $\hat{y}$ – ответ системы при сравнении, а y – истинный результат сравнения. В виде входных параметров системы выбраны следующие:

- Тип сенсора;
- Исходное разрешение изображения;
- Исходный размер изображения;
- Порог срабатывания.

Из всех перечисленных входных параметров регулировать мы можем только один – это порог срабатывания системы. Контролируя этот параметр необходимо определить, как он и другие, неконтролируемые параметры, повлияют на результаты идентификации.

Для сравнения подходов были выбраны следующие показатели эффективности биометрических систем.

Доля ошибок первого рода (FAR - False Acceptance Rate), формула 1. Эти ошибки происходят, когда система определяет незарегистрированного пользователя как зарегистрированного. Этот тип ошибки критичен для безопасности, поскольку злоумышленник получает доступ на объект.

$$FAR = \frac{FP}{FP+TN} \quad (1)$$

Доля ошибок второго рода (FRR - False Rejection Rate), формула 2. Этот вид ошибок происходит, когда сканер не может распознать зарегистрированного пользователя. Это не критично для безопасности, но создает неудобства, так как нужно проводить вторичную проверку биометрического параметра. Эти две характеристики являются стандартными для биометрических систем [10].

$$FRR = \frac{FN}{FP+TN} \quad (2)$$

Для оценки качества работы системы на каждом из классов по отдельности введем метрики precision (точность), формула 3, и recall (полнота), формула 4. Precision можно интерпретировать как долю изображений, названных системой как совпадающие и при этом действительно совпадающих, а recall показывает, какую

долю изображений из тех, которые должны были совпасть, были найдены системой. Именно введение precision не позволяет системе записывать все изображения в один класс, так как в этом случае мы получаем рост уровня False Positive. Recall демонстрирует способность системы обнаруживать данный класс вообще, а precision — способность отличать этот класс от других классов.

$$Precision = \frac{TP}{TP+FP} \quad (3)$$

$$\text{R}ecall = \frac{TP}{TP+FN} \quad (4)$$

Существует несколько различных способов объединить точность и полноту в агрегированный критерий качества. F-мера — среднее гармоническое точности и полноты, формула 5. F-мера достигает максимума при полноте и точности, равными единице, и близка к нулю, если один из аргументов близок к нулю. Выбранные метрики часто используются при анализе несбалансированных выборок [11-13]. F-мера дает возможность определить порог, при котором система точнее всего произвела идентификацию.

$$F\text{мера} = 2\frac{precision \cdot recall}{precision+recall} \quad (5)$$

Одним из способов оценить систему в целом, не привязываясь к конкретному порогу срабатывания, является AUC-ROC (или ROC AUC) — площадь под кривой ошибок (Area Under Curve - Receiver Operating Characteristic curve). Данная кривая представляет собой линию от (0,0) до (1,1) в координатах True Positive Rate (TPR или доля истинно положительных результатов), формула 4, и False Positive Rate (FPR или доля ложноположительных результатов), формула 6. TPR рассчитывается точно так же как и полнота, поэтому мы ссылаемся на формулу, указанную ранее, а FPR показывает, какую долю из изображений, которые на самом деле не совпадают, система предсказал неверно. В идеальном случае, когда система не делает ошибок (FPR = 0, TPR = 1), то получается площадь под кривой, равная единице; в противном случае, когда система случайно выдает вероятности классов, AUC-ROC будет стремиться к 0.5, так как программа будет выдавать одинаковое количество TP и FP. Каждая точка на графике соответствует выбору некоторого порога срабатывания. Площадь под кривой в данном случае показывает качество алгоритма (больше — лучше), кроме этого, важной является крутизна самой кривой — необходимо максимизировать TPR, минимизируя FPR, а значит, полученная кривая в идеале должна стремиться к точке (0,1) [14].

$$FPR = \frac{FP}{TN+FP} \quad (6)$$

Результаты сравнений

Был проведён ряд расчетов, благодаря которым было установлено, что достаточно взять область порога срабатывания систем от 2 до 100 особых точек с шагом в 2 точки. В области этих значений рассчитывались все показатели эффективности биометрических систем. На рисунках 1 и 2 представлены графики ошибок первого и второго рода для обеих баз данных FVC2004 и CrossMatchDB. Для удобства на всех графиках и во всех таблицах применены сокращения: SA – это алгоритм SourceAFIS, KJ – алгоритм Kjanko, CMDB – база данных CrossMatchDB, FVC_DBx – выборки базы данных FVC2004, где x - номер выборки.

На графике ниже мы видим, что уровень ошибок первого рода постепенно уменьшается с увеличением уровня порога, а ошибки второго рода, наоборот, увеличиваются. Причём, ошибки первого рода уменьшаются очень быстро, а ошибки второго рода увеличиваются постепенно. Нам интересна область графика, в которой значения ошибок будут минимальны. Такая область находится между значениями

порога срабатывания от 5 до 25. Здесь обе ошибки для всех выборок достигают минимальных значений.

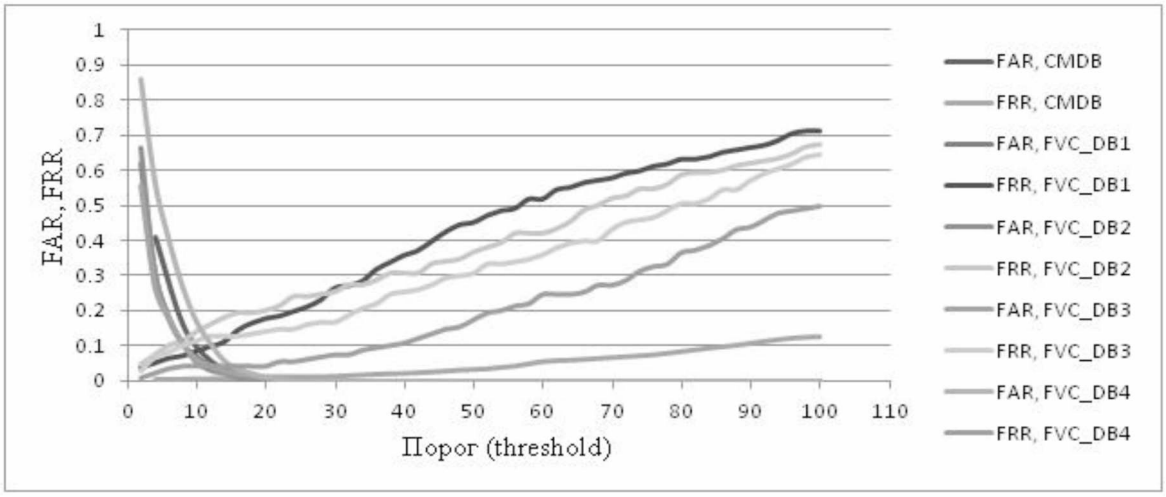

Рисунок 1 – ошибки первого и второго рода для подхода SourceAFIS

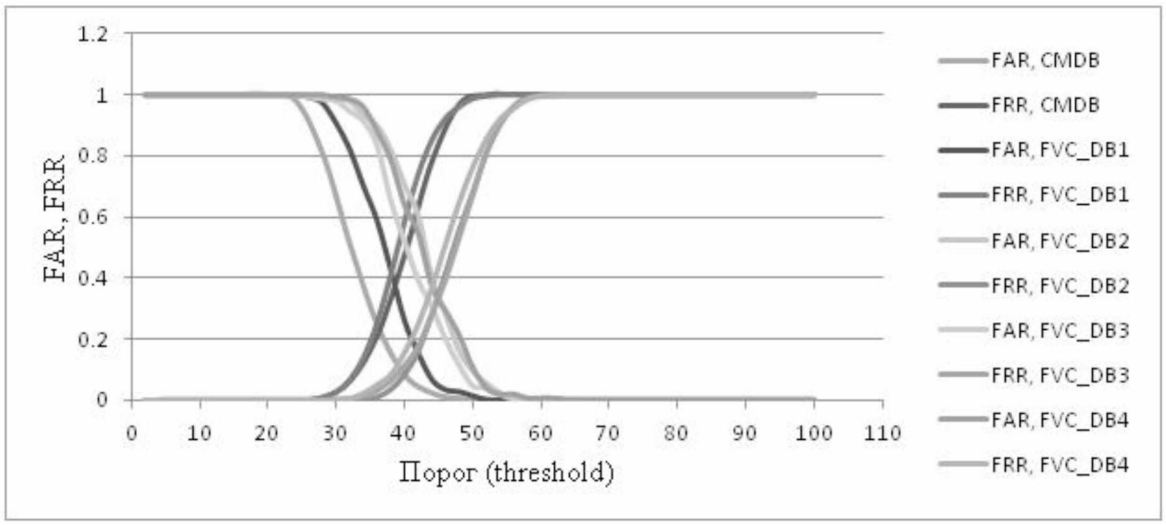

Рисунок 2 – ошибки первого и второго рода для подхода Kjanko

Проанализировав график на рисунке 2, можно прийти к выводу, что порог у системы Kjanko значительно сместился в сторону большего значения, по сравнению с SourceAFIS. Также видно характерное уменьшение ошибок первого рода с увеличением порога срабатывания, и, соответственно, увеличение ошибок второго рода. Ещё одно отличие от системы SourceAFIS заключается в том, что убывание и возрастание значений ошибок происходит очень резко. Значения порога срабатывания, примерно до 25 особых точек полностью пропускают все входные отпечатки, а после порога в 60 точек, система все их блокирует. Тем самым возводя ошибку первого рода в единицу, т.е. в 100%, до порога в 25, а ошибку второго рода в ноль, и наоборот, после порога в 60, устанавливая ошибку первого рода в ноль, а второго – в единицу. Оптимальные значения ошибок лежат в границах от 35 до 50 единиц порога срабатывания. В этой области наблюдаются минимальные значения обеих ошибок.

Поскольку графики дают лишь примерное понимание, при каком пороге срабатывания выбранные подходы дают самый лучший результат идентификации, поэтому была построена таблица 3. В ней представлены пороги срабатывания систем, при которых ошибки первого и второго рода (FAR и FRR) были минимальны (значения указаны в процентах).

Таблица 3. Значения ошибок первого и второго рода

	SourceAFIS					Kjanko				
	CMDB	FVC DB1	FVC DB2	FVC DB3	FVC DB4	CMDB	FVC DB1	FVC DB2	FVC DB3	FVC DB4
Порог	20	10	10	10	22	36	46	38	44	44
FAR	0,8	7	5,4	6,3	1,2	21,6	28,3	41,1	28	36,9
FRR	1	8,6	14	11.3	4	24,1	40	42,6	30,6	37,3

Из таблицы видно, что оба подхода показали самый малый процент ошибок на выборке данных из базы CrossMatchDB. Система SourceAFIS: 0,8% - ошибки первого рода, 1% - ошибки второго рода, Система Kjanko: 21.6% и 24.1% соответственно. Самый большой процент ошибок подход SourceAFIS показал на данных из базы FVC2004_DB2, там ошибки первого рода составили 5.4%, а ошибки второго рода — 14%. Подход Kjanko так же, имеет самый большой процент ошибок на данных FVC2004_DB2. Ошибки первого рода — 41.1%, второго — 42.6%.

На рисунке 3 приведены результаты сравнения ROC-кривых обеих систем. Штрихпунктирной линией, проходящей через точки 0;0 и 100;100, на графике обозначена прямая x = y, что соответствует случайному определению класса изображения системой.

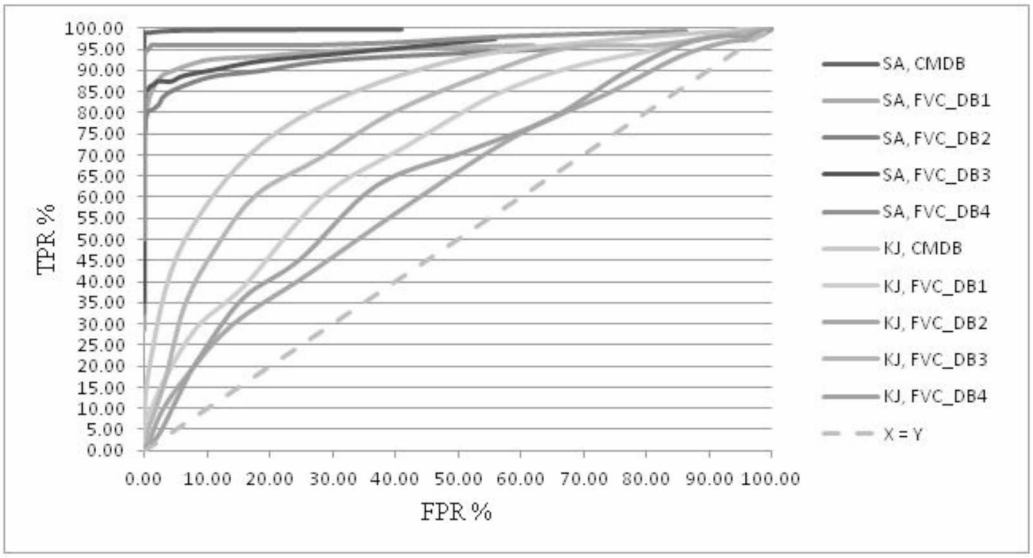

Рисунок 3 – сравнение ROC-кривых алгоритмов SourceAFIS и Kjanko

Проанализировав график на рисунке 3, можно понять, что подход SourceAFIS показывает очень хорошие значения идентификации на всех базах данных. Об этом сигнализирует тот факт, что ROC-кривые стремятся к значениям в 100% по обеим осям и по очень крутой траектории. Минимальное качество идентификации было продемонстрировано на данных из базы FVC2004_DB2, а максимальное – на базе CrossMatchDB. Подход Kjanko, справился с идентификацией отпечатков хуже, чем алгоритм SourceAFIS. Максимальные показатели также были получены при обработке отпечатков из базы данных CrossMatchDB и FVC2004_DB2. Из графика и всего вышесказанного можно сделать вывод, что алгоритм SourceAFIS лучше производит идентификацию на всех представленных базах данных.

Для чистоты проведённого сравнения в дополнение к анализу ошибок первого и второго рода и ROC-кривым на рисунке 4 был построен график, отражающий значения F-мер для обеих систем. Благодаря этой мере, можно также определить значение порога срабатывания, при котором система дала лучший результат идентификации.

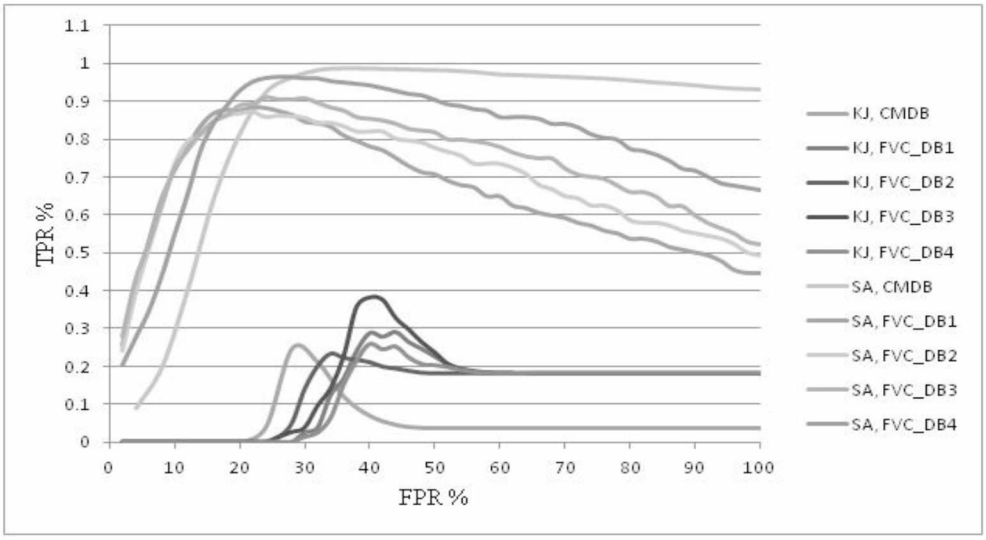

Рисунок 4 – результаты расчёта F-мер для обоих алгоритмов

После анализа результатов расчёта F-мер была составлена таблица 4, которая показывает, при каком уровне порога алгоритмы дали максимальный результат. Эти значения были рассчитаны для всех рассматриваемых баз данных и подходов. Как говорилось ранее, при каждом сравнении одного входного отпечатка с одним эталонным отпечатком системы давали ответ одного из четырёх видов. Значения в строках: «TP», «FP», «TN» и «FN» отражают количество сравнений отнесённых к каждому из ответов. В строке «Всего» указано общее количество проведённых сравнений. В графе «порог» указан порог срабатывания системы для каждого набора данных, измеряемый количеством особых точек. И наконец, значение «F-меры» указанно в процентах.

Таблица 4. Результаты расчёта F-мер

	SourceAFIS					Kjanko				
	CMDB	FVC DB1	FVC DB2	FVC DB3	FVC DB4	CMDB	FVC DB1	FVC DB2	FVC DB3	FVC DB4
TP	751	122	114	125	141	153	76	45	72	54
FP	4	4	1	0	1	311	150	190	153	212
TN	38246	1346	1349	1350	1349	37939	1200	1160	1197	1138
FN	14	28	36	25	9	612	74	105	78	96
Всего	39015	1500	1500	1500	1500	39015	1500	1500	1500	1500
Порог	36	22	26	30	26	44	44	34	40	40
F-мера	98,8	88,4	86	90,9	96,5	39	29	23	35	26

Рассмотрим подробнее значения, представленные в таблице. Для каждого подхода было проведено разделение по столбцам на выборки, на которых они выполняли идентификацию. Первые 4 строчки указывают о том, какое количество сравнений из общего количества, строка «всего» было отнесено системой к каждому из четырёх возможных вариантов ответа. Например, первый столбец. В 751 сравнении система отнесла сравниваемые отпечатки к первому классу, т.е. к совпадающим, и они действительно принадлежали этому классу. В 38246 сравнениях, система верно отнесла сравниваемые отпечатки ко второму классу. Только в 4 сравнениях система ошибочно отнесла сравнённые отпечатки к первому классу, когда они принадлежали второму. И в 14 сравнениях система ошибочно отнесла

сравниваемые отпечатки из первого класса, ко второму. Всего было проведено 39015 сравнений. В результате, при пороге срабатывания в 36 особых точек было получено значение F-меры Равное 98,8%.

Стоит обратить внимание на тот факт, что значения порога срабатывания, полученные с помощью расчёта F-меры, в основном больше, чем значения, полученные при попытке минимизировать ошибки первого и второго рода в таблице 3. Результатом такого расхождения в показаниях является тот факт, что при расчёте F-меры учитываются оба показателя точность и полнота, и чем больше эти значения, тем больше сама мера. Но если хотя бы один из этих показателей резко идёт вниз. То и значение F-меры, так же резко уменьшается. При большем пороге срабатывания уменьшение ошибки первого рода происходило быстрее, чем увеличение ошибки второго рода. За счёт этого, а также за счёт отношения правильно определённых отпечатков к неправильно определённым, точность и полнота имели большие значения на этом уровне порога, чем на том, который был выбран в таблице 3.

Проведя анализ всех результатов, полученных в процессе расчёта показателей эффективности биометрических систем, можно проследить искомую зависимость качества идентификации от входных параметров. Все показатели дали чёткое понимание того, что порог срабатывания является самым значимым входным параметром. От него напрямую зависело качество идентификации. И если его подобрать неправильно, взять слишком маленьким – будет большой процент ошибок первого рода, взять слишком большим – увеличиваются ошибки второго рода. Но также на качество идентификации влияли и неконтролируемые параметры - такие, как размер изображения, его разрешение и тип сенсора. Разрешение изображений из базы CrossMatchDB а также тип сенсора, оказались лучшими из всех выбранных баз. При правильно подобранном пороге срабатывания результаты всех показателей эффективности для обоих подходов на этой базе данных были самыми высокими, несмотря на то, что разрешение изображения было не самым большим из представленных. Выстроим в порядке убывания качества идентификации все использованные в статье источники данных для каждого подхода.

SourceAFIS:

1. CrossMatchDB. Самый высокий процент F-меры - 39% и самые маленькие проценты ошибок первого – 21,6% и второго рода – 24,1%. Размер изображения 504x408, исходное разрешение 500 ppi, тип сенсора Verifier 300.
2. FVC2004_DB4. F-мера 96,5%, ошибка первого рода - 1,2%, второго – 4%. Размеры изображений - 288x384, разрешение около 500dpi, тип сенсора - SFinGe v3.0.
3. FVC2004_DB3. F-мера – 90,9%, ошибка первого рода – 6,3%, второго – 11,3%. Изображения из данной базы имеют размер изображения 300x480, разрешение в 512 dpi, тип сенсора Thermal sweeping Sensor.
4. FVC2004_DB1. F-мера – 88,4%, ошибка первого рода – 7%, второго - 8,6%. Размеры изображений в данной базе самые большие, 640x480, разрешение – 500 dpi, тип сенсора – оптический.
5. FVC2004_DB2. F-мера – 86%, ошибка первого рода – 5,4%, второго – 14%. Размеры изображения 328x364, разрешение - 500 dpi, сенсор оптический.

Kjanko:

1. CrossMatchDB. Так же самый высокий процент F-меры - 39% и самые маленькие проценты ошибок первого – 21,6% и второго рода – 24,1%. Размер изображения 504x408, исходное разрешение 500 ppi, тип сенсора Verifier 300.
2. FVC2004_DB3. F-мера – 35%, ошибка первого рода – 28%, второго – 30,6%. Изображения из данной базы имеют размер изображения 300x480, разрешение в 512 dpi, тип сенсора Thermal sweeping Sensor.

3. FVC2004_DB1. F-мера – 29%, ошибка первого рода – 28.3%, второго - 40%. Размеры изображений в данной базе самые большие, 640x480, разрешение – 500 dpi, тип сенсора – оптический.
4. FVC2004_DB4. F-мера - 26%, ошибка первого рода – 36,9%, второго – 37,3%. Размеры изображений - 288x384, разрешение около 500dpi, тип сенсора - SFinGe v3.0.
5. FVC2004_DB2. F-мера – 23%, ошибка первого рода – 41,1%, второго – 42,6%. Размеры изображения 328x364, разрешение - 500 dpi, сенсор оптический.

Если основываться на построенных списках, становится ясно, что для системы SourceAFIS самым влиятельным входным параметром являлся тип сенсора, далее разрешение изображения и только потом размеры изображения. Для системы же Kjanko самым важным параметром оказалось разрешение изображения, потом его размеры и самое последнее это тип сенсора.

Выводы

Подход SourceAFIS показал лучшие результаты на всех протестированных выборках по сравнению с алгоритмом Kjanko. Из этого можно судить о том, что главное различие данных подходов, а именно применение в подходе SourceAFIS направления особых точек и рёбер, связывающих k-ближайших соседей, и сыграло важную роль в конечном качестве идентификации отпечатков пальцев. Тогда как подход Kjanko работал только с особыми точками и не смог достичь таких результатов.

Анализ результатов выполненных численных экспериментов позволяет оценить зависимость качества идентификации от входных параметров. Было определено, что самый важный параметр, который необходимо настраивать для каждой новой выборки данных – порог срабатывания системы (threshold). Анализ данных, представленных в таблицах 3 и 4, показал, что алгоритмы при работе с разными выборками давали качественный результат при разных уровнях порога. На качество идентификации влияет также исходное качество изображений и используемый сканер. Для подхода SourceAFIS более значимым оказался тип сенсора, когда как для подхода Kjanko – разрешение изображения.

Библиографический список

1. Гудков В.Ю., Клюев Д.А. Скелетизация бинарных изображений и выделение особых точек для распознавания отпечатков пальцев// Веник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». - 2015. – Т.15, - № 3. – С.11-17.
2. Bazen A.M., Verwaaijen G.T.B., Gerez S.H., Veelenturf L.P.J., van der Zwaag B.J. Correlation Based Fingerprint Verification System // A Proc. Workshop on Circuits Systems and Signal Processing. (ProRISC 2000), - 2000. С.205-213.
3. Starink J., Backer E. Finding point correspondences using simulated annealing // Pattern Recognition. - 1995. - Т. 28 №. 2. - С. 231-240.
4. Bebis, G., Deaconu, T., Georgiopoulos, M. Fingerprint identification using Delaunay triangulation // Proceedings 1999 International Conference on Information Intelligence and Systems. - 1999. - Cat.No.PR00446. - С. 452-459.
5. Ito K., Morita A., Aoki T., Nakajima H., Kobayashi K. and Higuchi T. A Fingerprint Recognition Algorithm Combining Phase-Based Image Matching and Feature-Based Matching // Proc. Int. Conf. on Biometrics. - 2006. - LNCS 3832. - С. 316–325.
6. DISI. Biometric System Laboratory. FVC databases. [Электронный ресурс] / DISI - University of Bologna. – Чезена, 2019. – URL: http://biolab.csr.unibo.it/DatabaseSoftware.asp?organize=Databases&select=22&selObj=&pathAttiv=&pathSubj=

7. Минакова Н.Н., Поляков В.В., Толстошеев С.Н. Методы технической и правовой защиты информации в сети Интернет //Барнаул: Изд-во Алтайского ун-та, 2015. – 155с.
8. Kjanko. python-fingerprint-recognition [Электронный ресурс] / Сан-франциско, 2007-2019. – URL: https://github.com/kjanko/python-fingerprint-recognition
9. Robert, Važan. SourceAFIS. How it works [Электронный ресурс] / Братислава, 2017-2019. – URL: https://sourceafis.machinezoo.com/algorithm
10. Фролов И.И. Протоколы систем биометрической идентификации // Доклады БГУИР. - 2016. - №3 (97). – С. 49 - 55.
11. Михайлов А.А, Колосков А.А., Дронов Ю.И. Основные параметры биометрических систем // Алгоритм безопасности. – 2015. - №5. – С. 58-61
12. Lee, T.J., Gottschlich, Tatbul, N., Metcalf, E., Zdonik, S.B. Precision and Recall for Range-Based Anomaly Detection / ArXiv. - 2018. - abs/1801.03175.
13. Micikevicius, P., Narang, S. Mixed Precision Training // ArXiv. - 2017. - abs/1710.03740.
14. Muschelli, John. ROC and AUC with a Binary Predictor: a Potentially Misleading Metric // ArXiv. – 2019. – abs/1903.04881