## Введение

Биометрия или биометрическое распознавание – это автоматическое распознавание индивидов на основе их поведенческих или биологических характеристик [Словарь IEEE], таких как отпечатки пальцев, радужная оболочка глаза, лицо, голос, походка, почерк и т.д. Также под биометрией часто понимают соответствующую область теории распознавания образов, связанную с изучением этих характеристик. Биометрия находит широкое применение в криминалистике, системах безопасности, системах контроля и учёта рабочего времени [ссылка на biolab?] и активно изучается как в России, так и за рубежом. Наиболее распространёнными до сих пор остаются автоматизированные дактилоскопические идентификационные системы (АДИС), то есть системы, основанные на сопоставлении отпечатках пальцев [ссылка на отчёт]. Это связано с тем, что изображения отпечатков пальцев относительно легко получить, алгоритмы их сопоставления хорошо разработаны [handbook], а размер машинного представления одного отпечатка достаточно мал [ссылка на FVC].

Хотя биометрия в целом и дактилоскопия в частности энергично развивались в течение последних 120 лет, в области автоматизированного распознавания отпечатков до сих пор остаются открытые вопросы. Главным из них является надёжность алгоритма распознавания. На сегодняшний день все машинные представления биологических и поведенческих характеристик человека создаются с неизбежной потерей информацией в процессе получения. Например, машинное представление отпечатка пальца, получаемое оптическим сканером, это двумерное растровое изображение части папиллярных линий, причём эластично деформированных в результате соприкосновения подушечки пальца с поверхностью считывающего устройства. Как следствие для любого алгоритма существует некоторая вероятность, что два изображения одного отпечатка будут ошибочно распознаны как принадлежащие разным пальцам и, напротив, два отпечатка разных пальцев будут восприняты как изображения одного и того же. Одним из способов уменьшить эту вероятность является совершенствование алгоритмов, выделение и исследование максимально возможного количества информации из имеющихся данных. Технические специалисты, работающие с готовыми модулями и программными комплексами, как правило, не могут напрямую модифицировать алгоритмы, и поэтому находят такую рабочую точку алгоритма, которая так или иначе минимизирует стоимость ошибки биометрической системы, хотя это связано со снижением вероятности одного типа ошибок за счёт роста вероятности другой.

В начале 2000-х годов был предложен иной подход к улучшению надёжности распознавания биометрических алгоритмов – биометрическая интеграция (biometric fusion) [Росс]. Его суть заключается использовании не одного, а комбинации алгоритмов обработки данных, желательно, дополняющих друг друга по используемой информации. Биометрическая интеграция может осуществляться разными способами, начиная от интеграции по данным, в том числе по разным биометрическим признакам, и заканчивая совместным принятием решения. И хотя этот подход даёт хорошие результаты, его математический аппарат слабо разработан. В настоящей работе рассматриваются несколько возможных сценариев биометрической интеграции, делается их теоретико-вероятностный анализ и на основе экспериментальных данных даются рекомендации по их использованию.

С другой стороны, с момента внедрения первых, неавтоматизированных дактилоскопических систем в правоохранительных органах стала известна другая фундаментальная проблема биометрических систем – проблема масштабирования данных в идентификационных системах, где ведётся распознавание единственного отпечатка со всей имеющейся базой. Современные системы обрабатывают запросы к базам размером в сотни тысяч и миллионы отпечатков (например, компания Safran Morpho внедря), и к этим системам предъявляются различные требования по быстродействию в зависимости от назначения. Особенно жёсткие требования ставятся в системах реального времени, например, на биометрических проходных.