Эффект биометрического зверинца в алгоритмах локального сопоставления

Михалев А.Д., студент 2 курса магистратуры кафедры системного программирования СПбГУ, fatum.est.series.causarum@gmail.com

Сартасов С. Ю., ст. преп. кафедры системного программирования СПбГУ, Stanislav.Sartasov@spbu.ru

Аннотация

В данной работе исследуется непропорциональное распределение ошибок сопоставления отпечатков пальцев в биометрической системе (эффект биометрического зверинца). Проводится эксперимент Ягера-Данстона с целью выявления эффекта биометрического зверинца в алгоритмах локального сопоставления.

Ключевые слова: отпечаток пальца, алгоритмы сопоставления, *Minutia Cylinder-Code*, *Feng*, эксперимент Ягера-Данстона, биометрический зверинец, *biometric zoo*

Введение

В настоящее время широко распространены биометрические системы аутентификации, использующие один из видов биометрического доступа - отпечаток пальца, благодаря его уникальности, неизменности и высокой точности. Методы распознавания отпечатков пальцев ежедневно применяются в криминалистике, а системы контроля доступа, использующие отпечатки пальцев, являются одними из самых востребованных биометрических систем. В течение последних десятилетий они всё чаще используются для верификации и идентификации пользователей с целью ограничения доступа к различного вида ресурсам и обеспечения безопасности хранения и передачи важной информации.

Такое повсеместное использование систем распознавания отпечатков обеспечило актуальность проблемы распознавания отпечатков и в настоящее время продолжает поддерживать её. Различные подходы к решению данной задачи изучаются уже давно. На данный момент существует большое количество достаточно эффективных решений, однако признать решенным вопрос распознавания отпечатков не представляется возможным, поскольку разработка более точных алгоритмов, минимизирующих накладные расходы, остается важнейшим аспектом этой проблемы.

Проблема распознавания отпечатков может сводится к задаче сопоставления отпечатков пальцев. Алгоритмы сопоставления решают данную задачу, принимая решение о совпадении отпечатков на основе некоторого порогового значения, что неизбежно приводит к ошибкам сопоставления.

Одной из главных причин ошибок в биометрической системе может служить эффект биометрического зверинца. Он изучается уже на протяжении 20 лет, и его исследование на текущий момент является очень актуальным в области биометрии.

Описание предметной области

Перед биометрической системой, ограничивающей доступ по отпечаткам пальцев, стоит задача сопоставления отпечатков. Для её решения необходимо в первую очередь зарегистрировать пользователей системы, создав для них шаблоны отпечатков и сохранив их в базе данных [1]. Шаблон формируется из извлечённых минуций для каждого отпечатка. При запросе доступа к системе шаблон, предоставленный некоторым лицом, сопоставляется с одним или множеством шаблонов из базы данных биометрической системы. При сопоставлении шаблонов дактилоскопические алгоритмы вычисляют метрику, значение которой сравнивается с пороговым значением биометрической системы. Если полученная оценка превышает пороговое значение, то пользователь получает доступ к системе, иначе – не получает.

В зависимости от того, принадлежат ли оба шаблона одному и тому же источнику данных (например, два отпечатка одного и того же пальца), выделяют два вида оценок сопоставления [1]:

- *Impostor score* – оценка сопоставления двух шаблонов отпечатков разных пользователей.
- *Genuine score* – оценка сопоставления двух шаблонов отпечатков одного и того же пользователя.

Как следствие, при сопоставлении шаблонов возникает два вида ошибок: *False Match*, *False Non-Match*, для которых возможно определить следующие вероятности [1]:

- *False Match (Acceptance) Rate (FAR)* – вероятность ошибки I рода, т.е. ложного совпадения отпечатков.
- *False Non-Match (Rejection) Rate (FRR)* – вероятность ошибки II рода, т.е. ложного несовпадения отпечатков.

Обзор литературы

Обзор решений задачи сопоставления отпечатков

На данный момент доступно огромное количество разнообразных решений задачи сопоставления [2]. Большинство из них основаны на минуциях [1]. Как показано в [3], задача сопоставления отпечатков имеет два подхода к решению:

- алгоритмы глобального сопоставления (однофазные);
- алгоритмы локального сопоставления (двухфазные).

Особый интерес в данной работе уделяется двухфазным алгоритмам локального сопоставления, поскольку они имеют ряд преимуществ над однофазными [3] и в последние пару десятилетий подлежат тщательному изучению [2].

Принцип их работы заключается в сопоставлении локальных структур, определённых для каждого шаблона, и предоставлении на выходе *матрицы локальных схожестей*, каждый элемент которой - *локальная оценка* сопоставления двух локальных структур из разных шаблонов.

Далее к полученной матрице схожести применяется *алгоритм консолидации*, который выбирает лучшие локальные оценки сопоставления локальных структур из матрицы схожести и объединяет их в *глобальную оценку* сопоставления двух шаблонов.

Эффект биометрического зверинца

В 2007г. Н.Ягер и Т.Данстон в [4] обобщили работу Дж.Доддингтона [5], в которой он ввёл термин *biometric menagerie / biometric zoo / биометрический зверинец*. В 2007 и 2010 гг. они провели эксперимент (далее эксперимент Ягера-Данстона) по выявлению эффекта биометрического зверинца, предварительно разделив пользователей биометрической системы на 8 классов [4, 6]

В [6] рассматривается множество пользователей системы $\mathcal{P}$ и множество оценок S. Для каждой пары пользователей $j, k \in \mathcal{P}$ существует множество $S(j,k) \subset S$, содержащее оценки сопоставлений для одного из шаблонов *j*-го пользователя с шаблонами, принадлежащими пользователю k.

Для каждого пользователя системы определяются два множества оценок:

- $G_k = S(k,k)$ - *genuine* оценки пользователя k, соответствующие тому, насколько хорошо пользователь сопоставляется сам с собой.

- $I_k = S(j,k) \cup S(k,j)$ - *impostor* оценки пользователя k для всех $j \neq k$, соответствующие тому, насколько хорошо пользователь сопоставляется с другими пользователями.

Для каждого из множеств оценок пользователя *k* строится статистика [6]:

- $g_k = \overline{G_k}$ - средняя *genuine* оценка из множества G_k для k-го пользователя.
- $i_k = \overline{I_k}$ - средняя *impostor* оценка из множества I_k для k-го пользователя.

Определяется $\mathcal{G} = \bigcup_{k \in \mathcal{P}} g_k$ – множество средних *genuine* оценок для всех пользователей. Множество $\mathcal{G}$ упорядочивается по увеличению g_k, тогда согласно [6]:

- $\mathcal{G}_H \subset \mathcal{P}$ – наибольшие 25% элементов множества $\mathcal{G}$, т.е. самые высокие *genuine* статистики.
- $\mathcal{G}_L \subset \mathcal{P}$ – наименьшие 25% элементов множества $\mathcal{G}$, т.е. самые низкие *genuine* статистики.
- Аналогичным образом определяются $\mathcal{I}_L$ и $\mathcal{I}_H$.

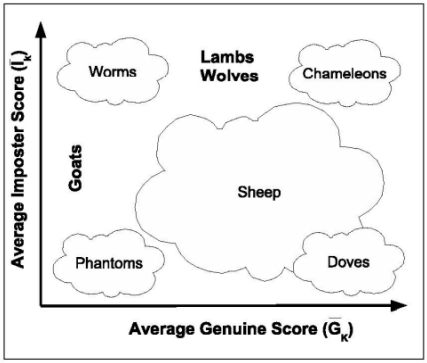

Рис. 1: Расположение классов относительно *genuine* и *impostor* оценок.(рис. из [4])

Таким образом, Н.Ягер и Т.Данстон дополнили классификацию Дж.Доддингтона, добавив к четырём существующим четыре новых класса определив все классы биометрического зверинца в терминах *genuine* и *impostor* оценок (рис. 1) [6]:

- **Sheeps** – большинство пользователей системы. Они легко распознаются биометрической системой.

- **Goats** – пользователи, сопоставление с которыми затруднительно. Они характеризуются низкими *genuine* и *impostor* оценками сопоставления и привносят в систему непропорциональное увеличение *FRR*.

- **Lambs** – пользователи, которых легко имитировать. Они характеризуются высокими *impostor* оценками при сопоставлении других пользователей с ними и привносят в систему непропорциональное увеличение *FAR*.

- **Wolves** – пользователи, которые легко имитируют других пользователей. Они характеризуются высокими *impostor* оценками сопоставления с другими пользователями системы и привносят в систему непропорциональное увеличение *FAR*.

- **Chameleons** – пользователи системы, для которых характерны высокие *genuine* и высокие *impostor* оценки: $\mathcal{G}_H \cap \mathcal{I}_H$. Они привносят в систему непропорциональное увеличение *FAR*.

- **Phantoms** – пользователи системы, для которых характерны низкие *genuine* и низкие *impostor* оценки: $\mathcal{G}_L \cap \mathcal{I}_L$. Они привносят в систему непропорциональное увеличение *FRR*.

- **Doves** – пользователи системы, для которых характерны высокие *genuine* и низкие *impostor* оценки: $\mathcal{G}_H \cap \mathcal{I}_L$. Сопоставление их отпечатков очень редко приводит к ошибкам сопоставления.

- **Worms** – пользователи системы, для которых характерны низкие *genuine* и высокие *impostor* оценки: $\mathcal{G}_L \cap \mathcal{I}_H$. Они привносят в систему непропорциональное количество *FAR* и *FRR* ошибок.

Постановка задачи

Основной целью данной работы является изучение влияние эффекта биометрического зверинца в дактилоскопических алгоритмах сопоставления. Для достижения поставленной цели в рамках текущего исследования были поставлены следующие задачи:

1. Повторить эксперимент Ягера-Данстона для выявления эффекта биометрического зверинца.

2. Выявить ограничения подхода Ягера-Данстона.

3. Поставить эксперимент Ягера-Данстона на локальном уровне дактилоскопических алгоритмов сопоставления.

Выявление эффекта биометрического зверинца на глобальном уровне

Эксперимент Ягера-Данстона позволяет определить наличие или отсутствие классов биометрического зверинца во множестве пользователей биометрической системы с некоторым уровнем значимости. Ожидаемое количество пользователей каждого из классов определяется по следующей формуле: $p \times |P|, p = (1/4)^2$ [6].

Рассмотрим в качестве примера класс *chameleons* C (для остальных классов аналогично), представляющий пользователей (назовём их хамелеонами), которые имеют высокие *genuine* и высокие *impostor* оценки. Пусть ν - ожидаемое количество хамелеонов в системе, $\nu = |C|$.

Сформулируем гипотезу H_0, которая утверждает, что вероятность того, что пользователь является хамелеоном, есть $p = 1/16$. Для проверки гипотезы считается вероятность того, что количество хамелеонов больше или равно предполагаемого значения ν [6]:

$$f(\nu, n, p) = \sum_{i=\nu}^{n} \binom{n}{\nu} p^i (1-p)^{n-i},$$

где $n = |\mathcal{P}|$ - количество испытаний в эксперименте. Гипотеза H_0 отклоняется, если $f(\nu, n, p) < \alpha$, где $\alpha = 0.05$ - уровень значимости.

Ограничение подхода Ягера-Данстона

Согласно описанию эффекта биометрического зверинца $S(j,k)$ - *множество глобальных оценок* сопоставления, поскольку $S(j,k)$ содержит оценки сопоставлений для одного из шаблонов *j*-го пользователя с шаблонами, принадлежащими пользователю *k*.

При проведении эксперимента Ягера-Данстона рассматривались множества $\mathcal{G}_H$, $\mathcal{G}_L$, $\mathcal{I}_H$, $\mathcal{I}_L$, принадлежность к которым помогает выявить эффект биометрического зверинца. Они последовательно строились из множеств $S(j,k)$:

1. Определялись множества *genuine* G_k и *impostor* I_k оценок.

2. Строились статистики $g_k = \overline{G_k}$, $i_k = \overline{I_k}$.

3. Определялись множества $\mathcal{G} = \bigcup\limits_{k \in \mathcal{P}} g_k$ и $\mathcal{I} = \bigcup\limits_{k \in \mathcal{P}} i_k$

4. Определялись $\mathcal{G}_H \subset \mathcal{P}, \mathcal{G}_L \subset \mathcal{P}, \mathcal{I}_H \subset \mathcal{P}, \mathcal{I}_L \subset \mathcal{P}$

Таким образом, в подходе Ягера-Данстона с использованием множеств $\mathcal{G}_H$, $\mathcal{G}_L$, $\mathcal{I}_H$, $\mathcal{I}_L$ для *глобальных оценок сопоставления* выявлялся эффект биометрического зверинца на *глобальном уровне*.

Но в то же время мы можем построить множества $\mathcal{G}_H, \mathcal{G}_L, \mathcal{I}_H, \mathcal{I}_L$ для *локальных оценок сопоставления*, что позволит выявить эффект биометрического зверинца не среди пользователей системы, а среди локальных структур шаблонов пользователей системы, т.е. на *локальном уровне*.

Выявление эффекта биометрического зверинца на локальном уровне

Эффект биометрического зверинца на локальном уровне может быть в выявлен в ходе эксперимента Ягера-Данстона, если в качестве входных данных вместо оценок сопоставления шаблонов пользователей подать оценки сопоставления локальных структур шаблонов, которые могут быть получены на первом этапе в ходе работы двухфазных алгоритмов сопоставления. Такие алгоритмы принимают на вход два шаблона A и B, для каждого из них строят локальные структуры для всех минуций. Затем алгоритмы выполняют сопоставление локальных структур и записывают результаты в матрицу локальных схожестей (Local Similarity Matrix, LSM) Γ.

Матрица $\Gamma_{\{j,k\}}$ - *множество локальных оценок*, содержащее результаты сопоставления локальных структур одного из шаблонов j-го пользователя с локальными структурами шаблона, принадлежащих пользователю k. Её строки соответствуют локальным структурам шаблона j, столбцы - локальным структурам шаблона k. На локальном уровне $\Gamma_{\{j,k\}}$ является аналогом *множества глобальных оценок* $S(j,k)$, содержащего оценки сопоставлений для одного из шаблонов j-го пользователя с шаблонами, принадлежащими пользователю k.

В рамках данной работы был разработан алгоритм, который позволяет выделить множества G_k и I_k для локальных структур из *LSM*. Основываясь на локальных множествах G_k и I_k, можно расширить ограничение стандартного подхода Ягера-Данстона, построив множества $\mathcal{G}_H, \mathcal{G}_L, \mathcal{I}_H$ и $\mathcal{I}_L$, что позволит выявить эффект биометрического зверинца для локальных оценок сопоставления, т.е. на локальном уровне.

Далее для локальных оценок сопоставления проводится эксперимент по той же методологии, что и в изначальном эксперименте Ягера-Данстона для глобальных оценок, поскольку формат входных данных остаётся неизменным (множество оценок), меняется только способ определения *genuine* и *impostor* оценок во входных данных.

Используемые технологии

Для извлечения минуций и построения шаблонов используется программное обеспечение *Griaule Fingerprint SDK* [7], которое находит в исходном изображении отпечатка координаты минуций и их направление.

Согласно обзору [2] в качестве двухфазных алгоритмов были выбраны наиболее точные: *MCC* [3], *Feng* (упрощённая, но не менее точная версия базового алгоритма с *minutiae-based* локальными структурами) [8], *Bozorth3* [9] и *Deng* [10]. Однако два алгоритма из четырёх не рассматриваются, т.к. *Bozorth3* не имеет открытой реализации, а *Deng* дополнительно требует тип минуций. Так же из [3] были взяты четыре алгоритмы консолидации *LSS, LSA, LSS-R, LSA-R*.

Реализация [12, 11, 13] алгоритма *MCC* взята из *MCC* [14], реализации *minutiae-based* версии алгоритма Feng и алгоритмов консолидации *LSS, LSA, LSS-R, LSA-R* написаны на языке *Python* [15].

Результаты экспериментов

Входными данными для проведения эксперимента выступают базы данных отпечатков пальцев: *FVC2000*, *FVC2002*, *FVC2004* [16, 17, 18]. Каждая база имеет 4 выборки по 80 изображений отпечатков для 10 разных пальцев, по 8 отпечатков на каждый палец. Всего 12 выборок и 960 отпечатков.

Из отпечатков извлекаются минуции, на основе которых строятся локальные структуры, и с помощью алгоритмов локального сопоставления вычисляются матрицы локальных схожестей. Далее проводятся эксперименты Ягера-Данстона для глобальных и локальных оценок сопоставления.

Поскольку эксперимент Ягера-Данстона подразумевает статистическую обработку данных, то была применена модификация эксперимента с целью получить устойчивую к выбросам статистику и сравнить её с базовой, а именно, для построения множеств *genuine* G_k и *impostor* I_k оценок была выбрана медиана.

Эксперимент Ягера-Данстона на глобальном уровне

Для обработки матриц локальных схожестей на глобальном уровне к ним применяются алгоритмы консолидации, предоставляющие множество глобальных оценок, которое разделяется на *genuine* и *impostor* оценки.

Далее проводится эксперимент Ягера-Данстона по выявлению классов биометрического зверинца среди шаблонов пользователей для каждой статистики (математического ожидания и медианы).

Результаты представлены в таблицах 1 и 2. Строки таблицы соответствуют названиям классам биометрического зверинца столбцы - комбинации локального алгоритма сопоставления с некоторым алгоритмом консолидации и статистикой, которая применялась к *genuine* и *impostor* оценкам. Число в ячейке таблицы отражает в скольких выборках из 12 был найден класс, соответствующий данной строке. Таким образом, можно сделать следующие выводы:

- Алгоритмы *MCC* и *Feng* привносят эффект биометрического зверинца в глобальный уровень.
- Оба алгоритма всегда находят класс *chameleons*, который характеризуется высокими *genuine* и высокими *impostor* оценкам. Стоит подумать над тем, как бороться с представителями этого класса.
- Алгоритм *Feng* по сравнению с *MCC* привносит эффект биометрического зверинца в большее количество выборок, что позволяет сделать вывод о том, что локальные структуры *Feng* чаще послужат причиной непропорционального распределения ошибок в биометрической системе.
- Случаи, когда находится класс *Doves*, нам не страшны, и даже полезны. Представители этого класса - лучшие пользователи биометрической системы, поскольку они имеют высокие *genuine* и низкие *impostor* оценки.
- Существенных различий между разными алгоритмами консолидации и статистками, применяемыми к одному алгоритму локального сопоставления, не наблюдается.
- Для алгоритма *MCC* с точки зрения эффекта биометрического зверинца алгоритм консолидации *LSS-R* является наихудшим.
- Для алгоритма *Feng* с точки зрения эффекта биометрического зверинца лучшим алгоритмом консолидации является *LSA-R*.

MCC								
	LSS		LSS-R		LSA		LSA-R	
	mean	median	mean	median	mean	median	mean	median
Chameleons	2	1	2	3	1	2	1	2
Phantomes	0	0	0	0	0	0	0	0
Doves	0	0	0	0	0	0	1	1
Worms	0	0	0	0	0	0	0	0

Таблица 1: Результаты для алгоритма *MCC* на глобальном уровне

Feng								
	LSS		LSS-R		LSA		LSA-R	
	mean	median	mean	median	mean	median	mean	median
Chameleons	10	8	11	10	7	3	2	4
Phantomes	5	6	7	7	5	6	5	4
Doves	1	1	0	0	1	1	0	0
Worms	0	0	0	0	0	0	0	0

Таблица 2: Результаты для *minutia-based* версии алгоритма *Feng* на глобальном уровне

Эксперимент Ягера-Данстона на локальном уровне

Для данного эксперимента обработка матриц локальных схожестей происходит иначе. Данные матрицы являются множеством локальных оценок сопоставления локальных структур шаблонов. Из множества локальных оценок с помощью специального алгоритма выделяются *genuine* и *impostor* оценки.

Далее проводится эксперимент Ягера-Данстона по выявлению классов биометрического зверинца среди локальных структур шаблонов пользователей для каждой статистики (матожидания и медианы).

Результаты представлены в таблицах 3 и 4. Обозначения в данных таблицах аналогичны таблицам 1, 2.Таким образом, можно сделать следующие выводы:

- Алгоритмы *MCC* и *Feng* привносят эффект биометрического зверинца в локальный уровень.
- Алгоритм *Feng* справляется хуже *MCC* и в большем количестве выборок находит классы зверинца. В тоже время, появление класса *Worms* можно избежать с помощью выбора нужной статистики.
- Для алгоритма *MCC* наблюдаются существенные различия между алгоритмами консолидации *LSS*, *LSA* и *LSS-R*, *LSA-R*. Алгоритмы *LSS-R*, *LSA-R* привносит большее количество классов *Phantomes* и *Chameleons*.

- Для алгоритма *Feng* существенных различий между применяемыми алгоритмами консолидации не наблюдается.
- Найденные классы *Doves* - это хорошо, т.к. представители этого класса - лучшие пользователи для биометрической системы с точки зрения распознавания.

MCC								
	LSS		LSS-R		LSA		LSA-R	
	mean	median	mean	median	mean	median	mean	median
Chameleons	1	2	2	4	1	2	3	5
Phantomes	0	0	5	5	0	0	8	10
Doves	6	6	2	2	7	6	2	1
Worms	2	1	1	1	2	1	0	0

Таблица 3: Результаты для алгоритма *MCC* на локальном уровне

Feng								
	LSS		LSS-R		LSA		LSA-R	
	mean	median	mean	median	mean	median	mean	median
Chameleons	10	11	12	11	11	12	12	12
Phantomes	7	10	9	12	8	12	11	12
Doves	0	4	0	6	0	4	0	5
Worms	0	5	1	6	0	3	0	12

Таблица 4: Результаты для *minutia-based* версии алгоритма *Feng* на локальном уровне

Заключение

В данной работе был исследован эффект биометрического зверинца в алгоритмах локального сопоставления. Полученные результаты показали, что в эффект биометрического зверинца наблюдается в алгоритмах локального сопоставления. Вместе с тем, грамотный выбор комбинации двухфазного алгоритма, алгоритма консолидации и статистики может избавить систему от некоторых классов зверинца, однако выбор такой комбинации - нетривиальная задача.

В дальнейшем предполагается провести фильтрацию локальных структур, принадлежащих к классам биометрического зверинца. После чего применить к фильтрованным шаблонам алгоритмы сопоставления и консолидации, получив оценки сопоставления. Далее провести сравнительный анализ процентного содержания ошибок для выборок содержащих оригинальные и фильтрованные шаблоны.

Литература

[1] Maltoni, D., Maio, D., Jain, A., Prabhakar, S. Handbook of fingerprinting, 2009.

[2] Peraltaa D., Galarc M., Triguerod I., Paternainc D., Garcíaa S., Barrenecheac E., Beníteza J. M., Bustincec H., Herreraa F. A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation // Information Sciences, vol. 315, issue C, pp. 67-87, Sep. 2015.

[3] Cappelli R., Ferrara M., Maltoni D. Minutia Cylinder-Code A New Representation and Matching Technique for Fingerprint Recognition // IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, issue 12, pp. 2128 - 2141, Dec. 2010

[4] Yager N., Dunstone T. Worms, chameleons, phantoms and doves: New additions to the biometric menagerie // Automatic Identification Advanced Technologies, 2007 IEEE Workshop on, pp. 1-6, IEEE, 2007.

[5] Doddington G. et al. Sheep, goats, lambs and wolves: A statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation // National institute of standarts and technology Gaithersburg MD, 1998.

[6] Yager N., Dunstone T. The biometric menagerie // IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, issue 2, pp. 220-230, 2010.

[7] Griaule biometrics. Fingerprint SDK.
http://www.griaulebiometrics.com/en-us/fingerprint_sdk

[8] Feng J. Combining minutiae descriptors for fingerprint matching // Pattern Recognition, vol. 41, issue 1, pp. 342-352, 2008.

[9] Watson C. I. et al. User's guide to NIST biometric image software, 2007.

[10] Deng H., Huo Q. Minutiae matching based fingerprint verification using delaunay triangulation and aligned-edge-guided triangle matching // International Conference on Audio-and Video-Based Biometric Person Authentication, Springer Berlin Heidelberg, pp. 270-278, 2005.

[11] Cappelli R., Ferrara M., Maltoni D. Fingerprint indexing based on minutia cylinder-code // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2011. – Т. 33. – №. 5. – С. 1051-1057.

[12] Ferrara M., Maltoni D., Cappelli R. Noninvertible minutia cylinder-code representation // IEEE Transactions on Information Forensics and Security. – 2012. – T. 7. – №. 6. – C. 1727-1737.

[13] Ferrara M., Maltoni D., Cappelli R. A Two-Factor Protection Scheme for MCC Fingerprint Templates // International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 2014.

[14] Biometric System Laboratory, University of Bologna. Minutia Cylinder-Code SDK v2.0, 2015.

[15] Minutiae-based Feng algorithm. Consolidation algorithms. Minutiae-based Feng algorithm and consolidation algorithms implementation on Python3.

[16] FVC2000. http://bias.csr.unibo.it/fvc2000/download.asp

[17] FVC2002. http://bias.csr.unibo.it/fvc2002/download.asp

[18] FVC2004. http://bias.csr.unibo.it/fvc2004/download.asp