Scientific Visualization, 2019, volume 11, number 2, pages 99 - 99, DOI: 10.26583/sv.11.2.08

Использование методов визуальной аналитики для получения комплексного показателя качества биометрической аутентификации с использованием механизма жестовой манипуляции

Ю.Е. Козлов

Финансовый университет при правительстве Российской Федерации, Москва, Россия

ORCID: 0000-0002-4448-0232, kozlovye@yandex.ru

Аннотация

Применение мультимодальных методик аутентификации в мобильных приложениях, использующих в своей работе несколько взаимоувязанных параметров, требует изучения их с точки зрения надежности. Одним из распространенных способов определения характеристик таких методик является определение ошибок первого и второго рода, а также получение комплексного показателя качества, которое можно определить при визуализации компромисса между ошибками первого рода (FRR) и ошибками второго рода (FAR).

Совместное построение графиков зависимости FRR и FAR от значения порога возможно лишь с использованием компьютерного моделирования и инструментов визуальной аналитики, позволяющих наглядно убедиться в правильности сделанных выводов. Традиционно для биометрических систем аутентификации, имеющих вероятностные показатели надежности, параметром, характеризующим комплексный показатель качества, является равный уровень ошибок (EER), располагающийся на пересечении кривых FRR и FAR.

В настоящей статье предложено исследование, позволившее наглядно сравнить эффективность ряда алгоритмов при проведении процедуры аутентификации, и определить наиболее выгодные из них с точки зрения надежности применительно к биометрической аутентификации в мобильных приложениях при помощи механизма жестовой манипуляции.

Ключевые слова: подпись в воздухе, МТДП, подпись, носимое устройство, аутентификация.

1. Введение

Наряду с традиционными биометрическими системами аутентификации, широко распространенными в мобильных приложениях, такими как: аутентификация по отпечатку пальца, по форме лица или по речевым характеристикам, появляются новые методики, использующие иные биометрические признаки. Это связано, прежде всего, с увеличением числа сообщений о взломах биометрических систем. Проблемы биометрии вызваны несовершенством технологий и свойствами методик, делающими их уязвимыми [1-4]:

- биометрические признаки не секретны и могут быть скопированы;
- биометрические признаки невозможно заменить (например, нельзя заменить рисунок отпечатка пальца или рисунок радужной оболочки глаза);
- алгоритмы обработки биометрических признаков не являются тайной и являются общедоступными.

Среди методик, частично парирующих данные недостатки, можно выделить методики аутентификации с помощь жестовых манипуляций. Суть этих методик в том, что биометрическими признаками являются жесты, регистрируемые акселерометром или

гироскопом смартфона, фитнес браслета, умных часов или несколькими устройствами одновременно [5-7].

В данной статье рассматривается методика биометрической мультимодальной аутентификации с использованием специального жеста в воздухе, выполняемого одним или несколькими мобильными устройствами одновременно (далее - механизм жестовой манипуляции). В качестве биометрического признака аутентификации служит жест, выбранный в качестве эталона и пороговые значения (меры схожести), при превышении которых жест будет признан несоответствующим эталону. Совокупность этих данных названа мультимодальной трехмерной динамической подписью (далее - МТДП) [8, 9]. Регистрация жеста проводится акселерометрами двух устройств – смартфона и умных часов, взаимодействующих друг с другом при помощи интерфейса bluetooth.

Особенностью данной методики является фиксация пользователем момента начала и окончания жеста. Это реализуется удержанием кнопки громкости или кнопки на экране смартфона во время выполнения жеста. Применение данного механизма избавляет от необходимости выделять нужную информацию из потока данных.

Преимущество методики МТДП в сочетании трех типов аутентификации:

– что пользователь имеет (умные часы можно рассматривать, в качестве токена);

– что пользователь знает (жест необходимо помнить);

– что есть сам пользователь (жесты содержат биометрические особенности жестикуляции человека, по аналогии с рукописной подписью).

Данная методика имеет еще два преимущества – легкая смена биометрического идентификатора (жеста) и возможность проводить аутентификацию скрытно в людном месте, если выбран жест типичный для обычного поведения человека.

Основная цель статьи - наглядно оценить эффективность алгоритмов, которые могут быть использованы для идентификации при помощи МТДП. Благодаря визуализации можно видеть динамику работы того или иного алгоритма при изменении порога, что бывает важно при принятии решения об его использовании.

Одновременная визуализация всего объема попыток аутентификации позволяет наглядно убедиться в отсутствии явных ошибок моделирования или сбора данных. Например, необоснованные выбросы или провалы заставят задуматься об их природе и подтолкнут к анализу их появления. Такие явления, хорошо заметные на рисунке, могут быть не замечены при другой форме отображения результата, например, табличной.

Кроме того, материалы данной статьи должны лечь в основу настройки системы учета и контроля доступа (СКУД), использующую методику МТДП. Анализируя показанные в статье графики, можно будет иметь ориентировочную оценку ошибок первого и второго рода при определённом пороге.

2 Аутентификация при помощи механизма жестовой манипуляции

Данные акселерометров умных часов и смартфона - это шесть временных рядов, каждый из которых хранит значения ускорений по одной из осей - три временных ряда для смартфона и три временных ряда для часов. Эталонный жест также хранится как шесть временных рядов.

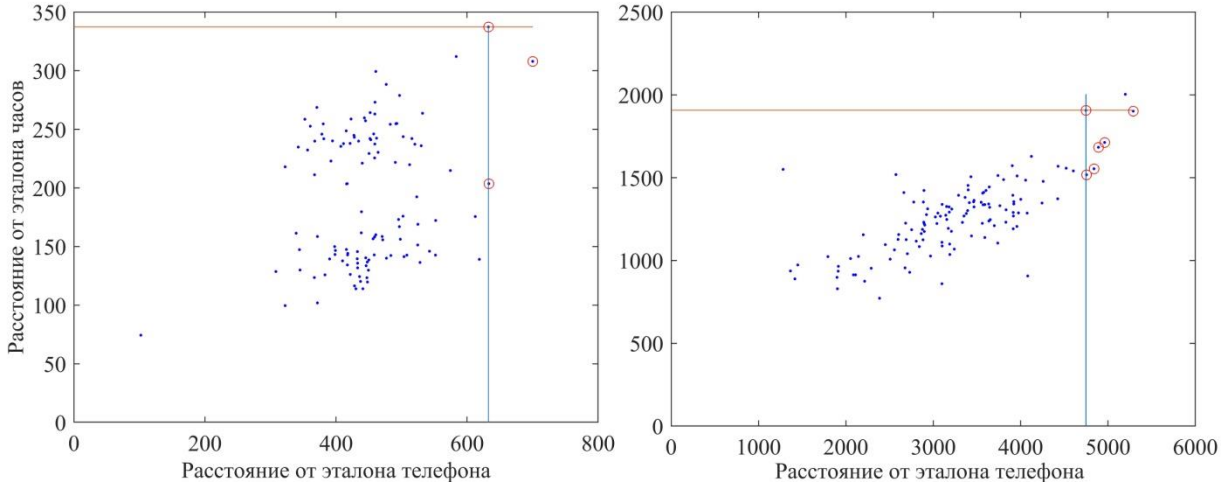
При опробовании методики был разработан макет, позволяющий сохранять данные попыток аутентификации.

Макет позволил опробовать методику на группе людей и набрать данные для последующего анализа. В основе работы макета был заложен алгоритм динамической трансформации шкалы времени DTW, определяющий меру схожести между эталоном и воспроизведенным жестом. Уровень порогов определялся как максимальное расстояние, полученное из пяти попыток воспроизведения жеста.

Эксперимент показал, что уровень порогов сильно разнится в зависимости от интенсивности (активности) и длительности жеста. Если отобразить по оси ординат расстояния между эталоном и сделанным жестом для умных часов, а по оси абсцисс расстояния для смартфона, мы получим распределения попыток аутентификации на плоскости.

Необходимо отметить, что макет предполагал до трех попыток для аутентификации. Моделирование также предполагало до трех попыток. Если за три попытки системе не предъявлялся жест удовлетворяющий порогам, аутентификация считалась не пройденной.

Визуализация попыток аутентификации для спокойного и интенсивного жестов представлена рис 1.



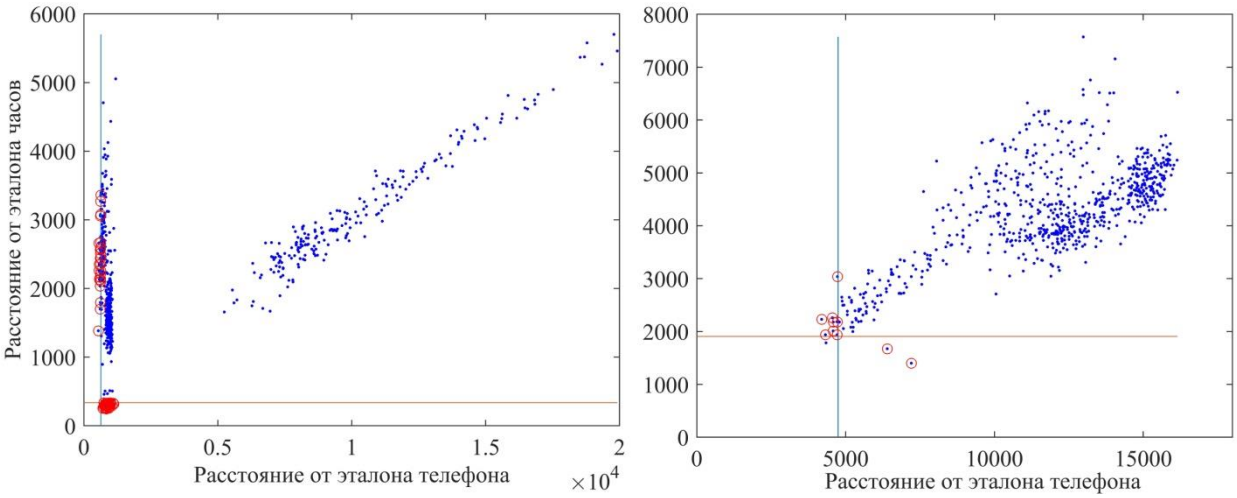
а) спокойный жест б) интенсивный жест

Рис. 1. - Распределение попыток аутентификации. Вертикальная черта – порог срабатывания для телефона. Горизонтальная черта – порог срабатывания для умных часов. Кружком обведены попытки, отсеченные порогом только одного устройства.

Из рисунка видно, что значение порогов отличаются почти в 10 раз, и чем интенсивнее жест, тем больше численное значение порога МТДП. Данный рисунок не позволяет сделать вывод, что один из жестов менее надежен, чем другой, а лишь иллюстрирует удачные и неудачные аутентификации пользователя.

FRR (False Rejection Rate – отказ в аутентификации верному пользователю) - ошибка первого рода для обоих жестов была равна нулю. Для первого жеста сделано 154 попытки, а для второго 389 попыток аутентификации (как было сказано выше, аутентификация дает пользователю до трех попыток).

Для получения лучшего представления о надежности было проведено моделирование для визуализации ошибки второго рода FAR (False Acceptence Rate - принятие чужого жеста за свой). Для этого попытки для иных МТДП, представленных в базе, были использованы в качестве попыток аутентификации. На рис. 2 – визуализация попыток аутентификации при помощи других жестов.



а) спокойный жест б) интенсивный жест

Рис. 2. Распределение попыток аутентификации при помощи иных жестов

По результатам моделирования вариант а) пропустил одну неверную аутентификацию из 1077 попыток, вариант б) не пропустил ни одной из 840 попыток, что позволяет говорить о приемлемой надежности обоих вариантов МТДП, однако рисунки 1 и 2 не дают достаточно информации о правильности выбранного алгоритма и надежности методики в целом. Для того чтобы делать выводы необходимо еще представлять динамику изменений ошибок FAR и FRR в зависимости от выбранного порога, а также значение равного уровня ошибок.

3. Сравнительная оценка качества алгоритмов идентификации с применением визуальной аналитики

Выработка порогов указанным выше способом не допускает их корректировки и изменения соотношений ошибок первого и второго рода. Кроме того, для полноценного исследования следует сравнить эффективность известных алгоритмов, позволяющих осуществлять аутентификацию.

Сравнения качества работы нескольких алгоритмов с точки зрения надежности можно провести, определив ошибки FAR и FRR, а также, определив равный уровень ошибок EER (equal error rate), который можно считать комплексным показателем качества для биометрических систем аутентификации.

В статье рассмотрены девять алгоритмов сравнения, позволяющих получить меру схожести - обозначим ее как z, для временных рядов $X=x_1...x_n$ и $Y=y_1...y_m$. Для прохождения алгоритма аутентификации требуется получить шесть мер схожести (для каждой исследуемой оси) и сравнить их с порогом.

Отличительной особенностью методики аутентификации с помощью механизма жестовой манипуляции является необходимость индивидуальной установки порогов в зависимости от сложности жеста, следовательно, надежность и ошибки FAR и FRR, также будут зависеть от сложности жеста. При этом сложность жеста для смартфона и умных часов будет различной - в жесте участвуют движения запястьем, предплечьем и кистью руки, поэтому на каждом рисунке представлены графики отдельно для смартфона и для умных часов.

При правильной установке порога уровень EER для МТДП будет не выше минимального из них. Одновременно раздельные графики позволяют оценить надежность аутентификации только одним из устройств.

Всего в моделировании участвовало 1229 реальных попыток аутентификации для 8 МТДП, выполненных разными людьми. На основе этих попыток для каждого алгорит-

ма смоделировано 6,1x10^7 попыток для визуализации кривой FRR и 4,3x10^8 попыток для визуализации кривой FAR.

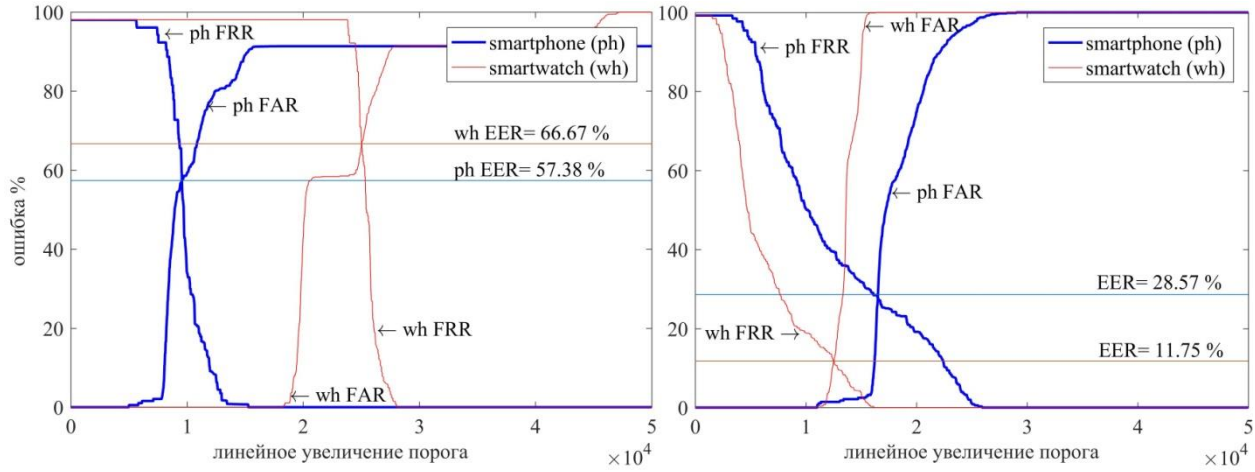
Моделирование предполагало линейное увеличение порога таким образом, чтобы наиболее наглядно отобразить на графике пересечение FRR и FAR.

Графики FAR и FRR, аналогичные показанным ниже, были получены для всех восьми МТДП. В статье представлены два типичных случая – жест с высокой надежностью (интенсивный жест - сумма модулей ускорений по всем осям около 15000 у.е., при этом из показаний не убиралась гравитационная составляющая) и слабой надежностью (спокойный жест - сумма модулей ускорений по всем осям около 1500 у.е.). Подробно о нахождении суммы модулей ускорений изложено в статье «Подходы к определению надежности мультимодальной трехмерной динамической подписи» [9].

Для первых шести алгоритмов размерность входных данных должна быть одинакова, для их работы входной сигнал Y обрезался или дополнялся последним из значений – y_m пока размерность Y не становилась равной эталону X.

1 Расстояние Евклида $z = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$.

На рис. 3 представлены зависимости ошибок FRR и FAR от порога и уровень EER при использовании расстояния Евклида для аутентификации.

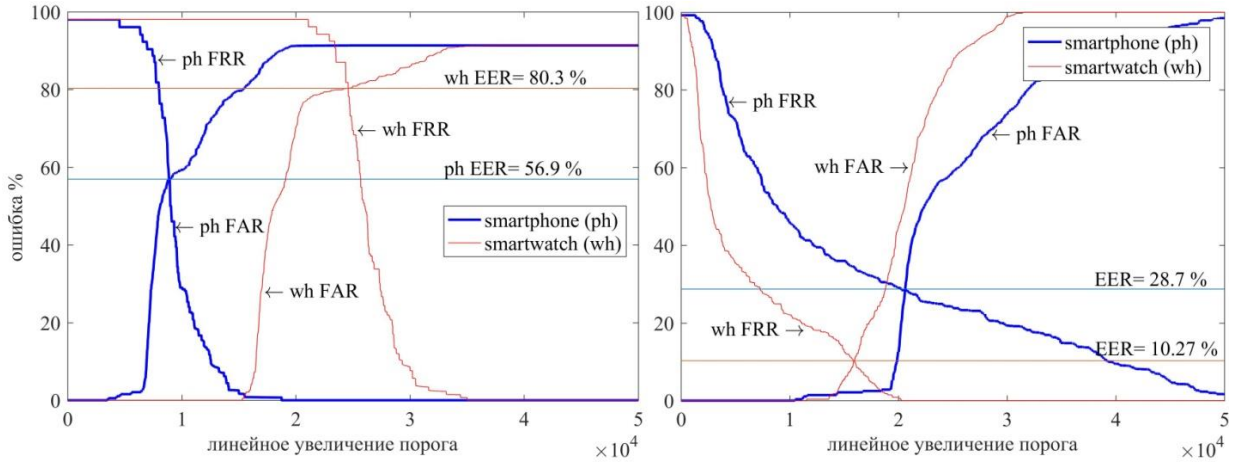


а) спокойный жест б) интенсивный жест

Рис. 3. FRR, FAR и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма Евклида

2 Квадратичное расстояние Евклида $z = \sum_{i=1}^{n}(x_i - y_i)^2$.

На рис. 4 представлены зависимости ошибок FRR и FAR от порога и уровень EER при использовании квадратичного расстояния Евклида для аутентификации.

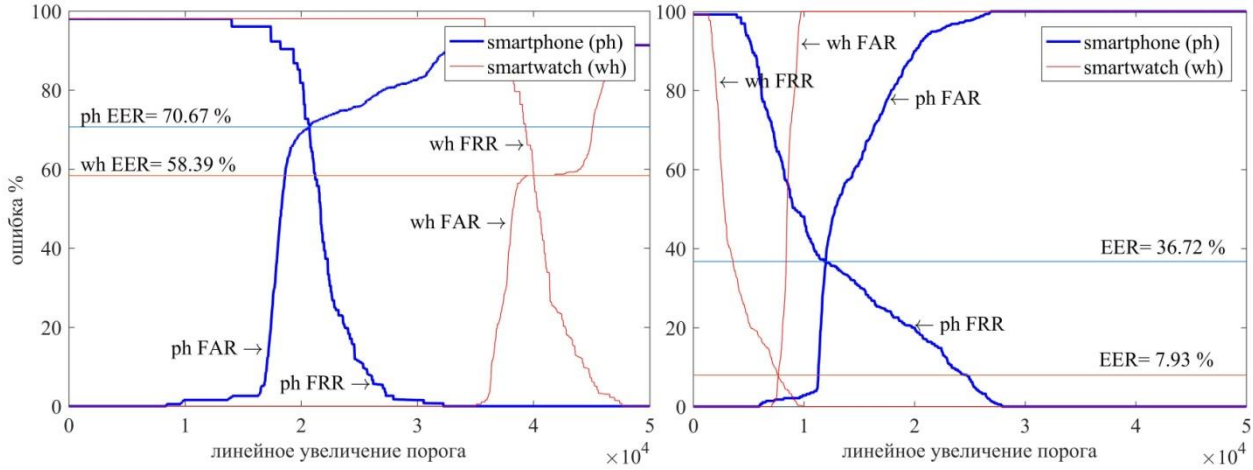


а) спокойный жест б) интенсивный жест

Рис. 4. FRR, FAR и EER умных часов (красные графики) и смартфона (синие графики) при использовании квадратичного расстояния Евклида

3 Расстояние городских кварталов $z = \sum_{i=1}^{n}|x_i - y_i|$.

На рис. 5 представлены зависимости ошибок FRR и FAR от порога и уровень EER при использовании расстояния городских кварталов в аутентификации.

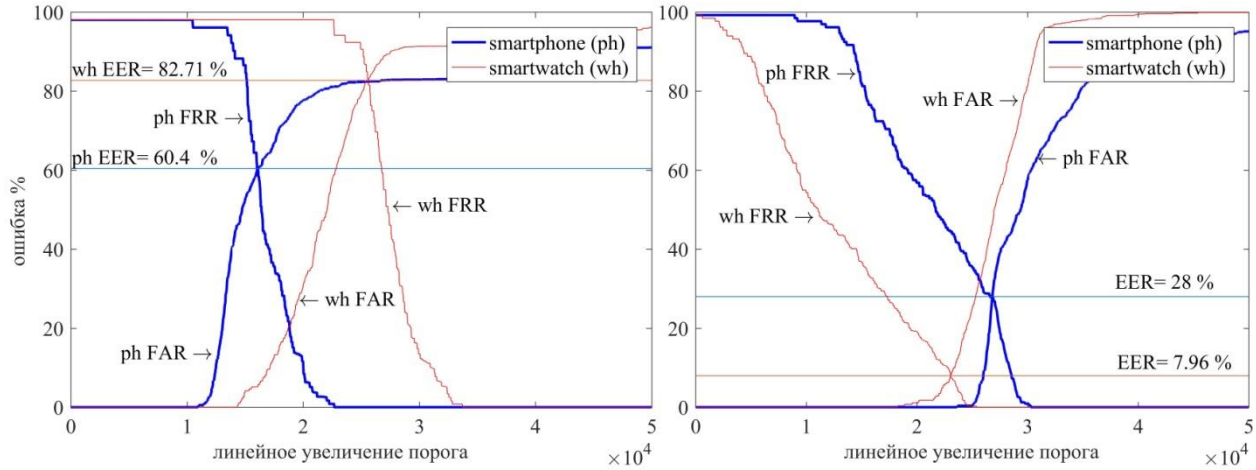


а) спокойный жест б) интенсивный жест

Рис. 5. FRR, FAR и EER умных часов (красные графики) и смартфона (синие графики) при использовании расстояния городских кварталов

4 Расстояние Чебышева $z = max_{i=1,\dots,n}\{|x_i - y_i|\}$.

На рис. 6 представлены зависимости ошибок FRR и FAR от порога и уровень EER при использовании расстояния Чебышева для аутентификации.



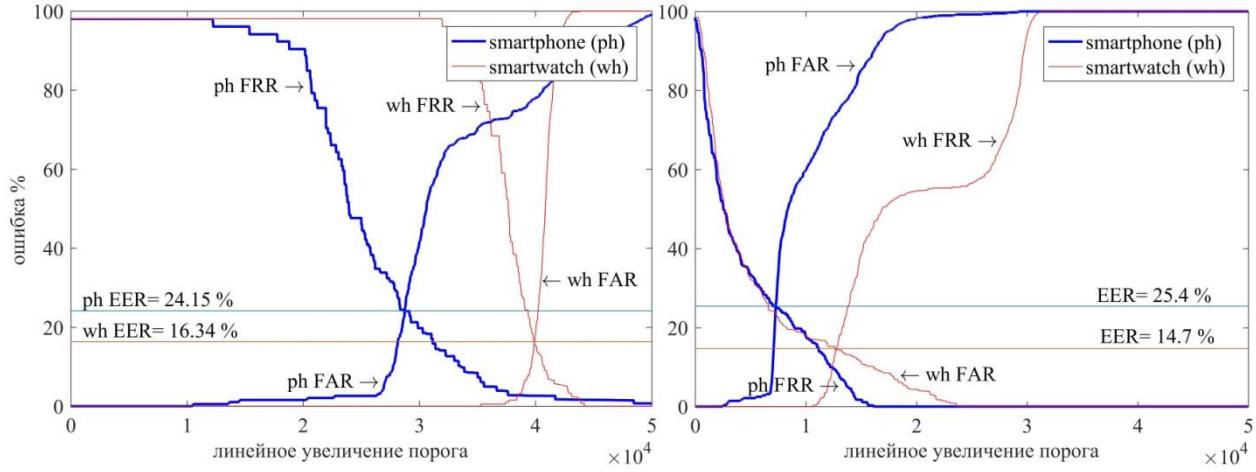
а) спокойный жест б) интенсивный жест

Рис. 6. FRR, FAR и EER умных часов (красные графики) и смартфона (синие графики) при использовании расстояния Чебышева

5 Косинусное расстояние – для временных рядов это мера сходства, которая используется для измерения косинуса угла между ними. Мера показывает хорошую эффективность в обработке изображений [10] (1):

$$z = \frac{\sum_{i=1}^{n} x_i \times y_i}{\sqrt{\sum_{i=1}^{n} (x_i)^2} \times \sqrt{\sum_{i=1}^{n} (y_i)^2}} \quad (1),$$

На рис. 7 представлены зависимости ошибок FRR и FAR от порога и уровень EER при использовании косинусной меры сходства для аутентификации.



а) спокойный жест б) интенсивный жест

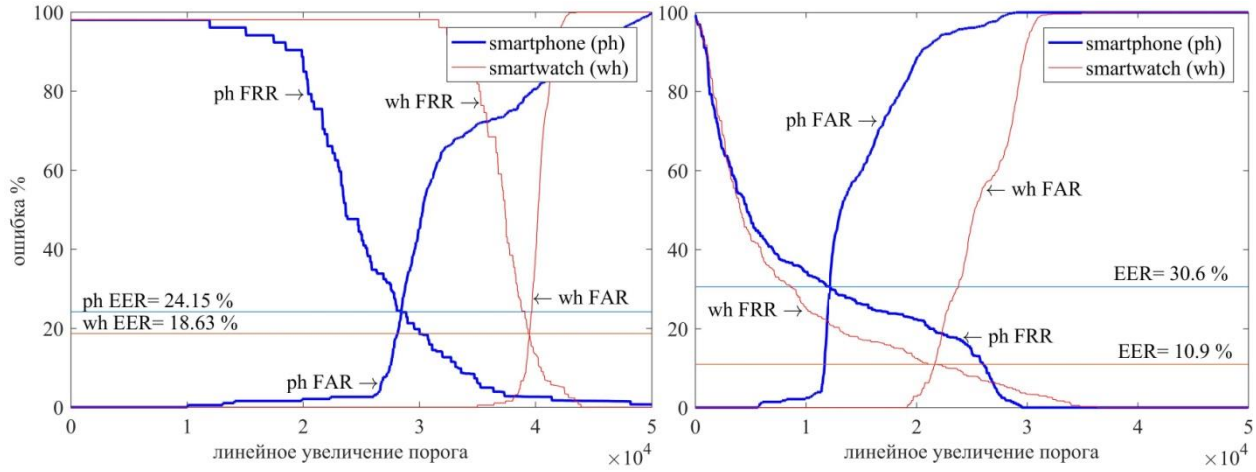
Рис. 7. FRR, FAR и EER умных часов (красные графики) и смартфона (синие графики) при использовании косинусного расстояния

6 Корреляционное расстояние (3):

$$z = 1 - \frac{\sum(X-\overline{X})(Y-\overline{Y})}{\sqrt{\sum(X-\overline{X})^2 \sum(Y-\overline{Y})^2}} \quad (3),$$

где $\overline{X} = \frac{1}{n}\sum_{i=1}^{n} x_i$ и $\overline{Y} = \frac{1}{n}\sum_{i=1}^{n} y_i$ - среднее значение временного ряда.

На рис. 8 представлены зависимости ошибок FRR и FAR от порога и уровень EER при использовании корреляционного расстояния для аутентификации.



а) спокойный жест б) интенсивный жест

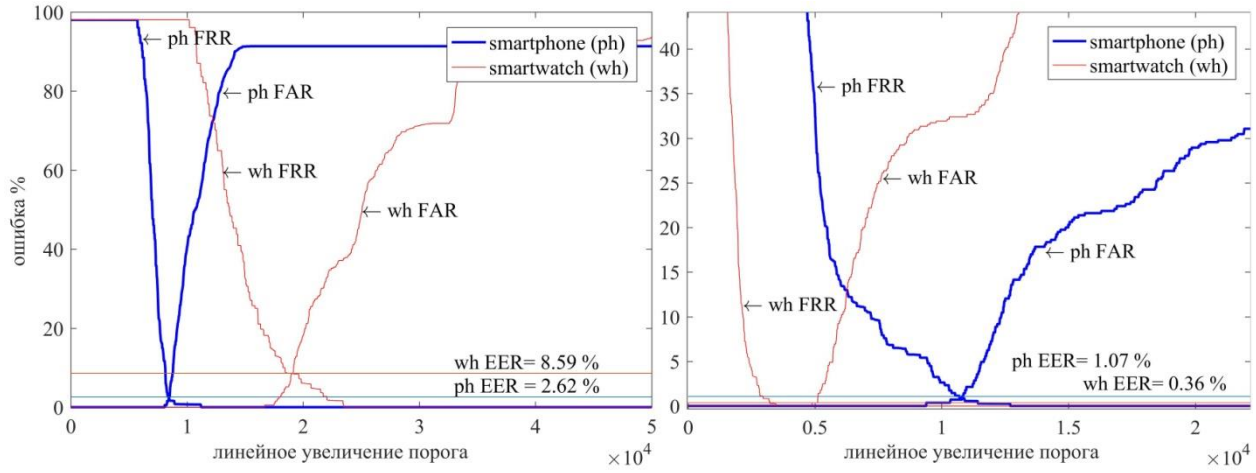
Рис. 8. FRR, FAR и EER умных часов (красные графики) и смартфона (синие графики) при использовании корреляционного расстояния

Последние три алгоритма являются вариантами алгоритма DTW (динамической трансформации шкалы времени). Особенность алгоритмов DTW в том, что для проведения вычислений не требуется нормализации входных данных.

Алгоритмы DTW, несмотря на большее количество вычислений по сравнению с предыдущими, очень часто используется для получения меры схожести временных рядов. Кроме того, существуют модификации позволяющие повысить его быстродействие, что особенно важно для смартфонов, имеющих не очень высокие вычислительные мощности [11].

7 Алгоритм DTW, использующий для построения матрицы расстояний расстояние Евклида: $z = \min\left\{\frac{\sqrt{\sum_{h=1}^{K} d(w_h)}}{K}\right\}$, где K - длина пути, а $d(w_h)=(x_i-y_j)^2$ элемент пути [12].

На рис. 9 представлены зависимости ошибок FRR и FAR от порога и уровень EER при использовании для аутентификации алгоритма DTW, использующего расстояние Евклида для построения матрицы расстояний.

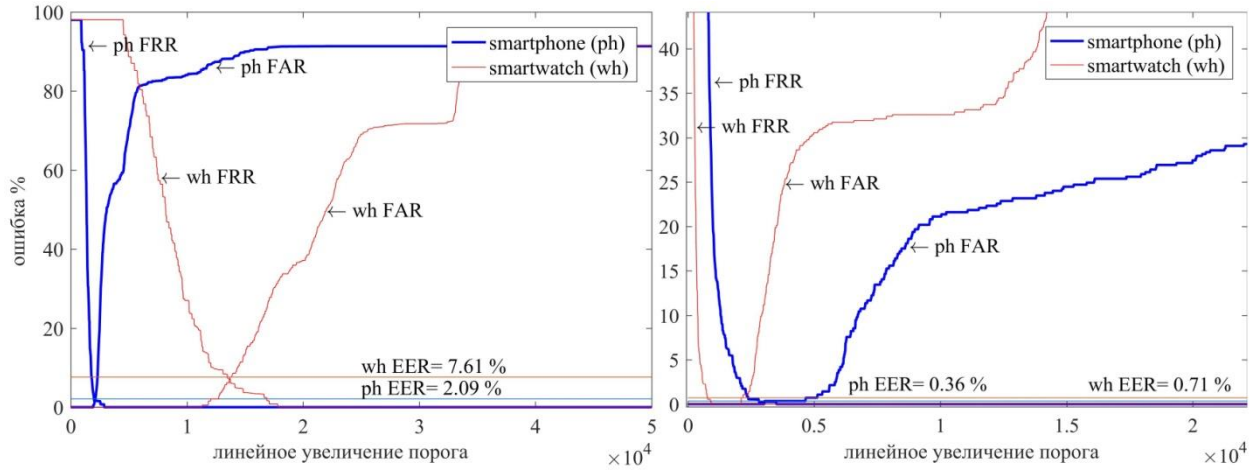


а) спокойный жест б) интенсивный жест

Рис. 9. FRR, FAR и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма DTW, использующий расстояние Евклида для построения матрицы расстояний

8 Алгоритм DTW использующий для построения матрицы расстояний квадрат расстояния Евклида: $z = \min\left\{\frac{\sum_{h=1}^{K} d(w_h)}{K}\right\}$, где K - длина пути, а $d(w_h)=(x_i-y_j)^2$ элемент пути (рис. 10).

На рис. 10 представлены зависимости ошибок FRR и FAR от порога и уровень EER при использовании для аутентификации алгоритма DTW, использующего квадрат расстояния Евклида для построения матрицы расстояний.

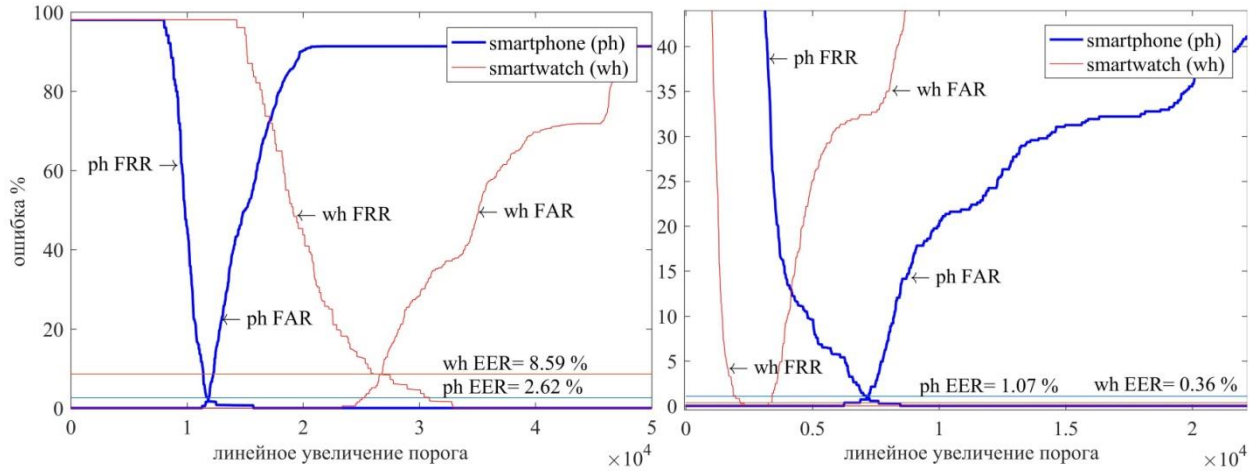


а) спокойный жест б) интенсивный жест

Рис. 10. FRR, FAR и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма DTW, использующий для построения матрицы расстояний квадрат расстояния Евклида

9 Алгоритм DTW использующий для построения матрицы расстояний алгоритм городских кварталов $z = \min\left\{\frac{\sum_{h=1}^{K} d(w_h)}{K}\right\}$, где K - длина пути, а $d(w_h)=|x_i-y_j|$ элемент пути.

На рис. 11 представлены зависимости ошибок FRR и FAR от порога и уровень EER при использовании для аутентификации алгоритма DTW, использующего алгоритм городских кварталов для построения матрицы расстояний.



а) спокойный жест б) интенсивный жест

Рис. 11. FRR, FAR и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма DTW, использующий расстояние городских кварталов для построения матрицы расстояний

В таблице 1 представлены обобщенные результаты проведенного моделирования для двух МТДП.

Таблица 1

№ пп	Алгоритм	EER спокойного жеста		EER интенсивного жеста	
		смартфон, %	умные часы, %	смартфон, %	умные часы, %
1	Расстояние Евклида	57,4	66,7	28,6	11,7
2	Квадратичное расстояние Евклида	80,3	56,9	28,7	10,3
3	Расстояние городских кварталов	70,7	58,4	36,7	7,9
4	Расстояние Чебышева	82,7	60,4	28	7,6
5	Косинусное расстояние	24,2	16,3	25,4	14,7
6	Корреляционное расстояние	25,4	14,7	30,6	11
7	DTW с использованием алгоритма Евклида	8,6	2,6	1,1	0,36
8	DTW с использованием квадрата алгоритма Евклида	7,6	2,1	0,36	0,71
9	DTW с использованием алгоритма городских кварталов	8,6	2,6	1,1	0,36

Для алгоритмов 1-6 применение аппроксимации, дающей равномерное растяжение или сжатие входного сигнала, вероятно, дало бы лучшие результаты, но такой прием может привести к ухудшению стойкости биометрического признака к спуфингу (когда злоумышленник намеренно воспроизводит увиденный или записанный на видео жест с целью пройти аутентификацию за пользователя). Для МТДП продолжительность жеста имеет значение, аналогичное силе нажатия на перо в рукописной подписи.

Уровень EER был получен для всех восьми МТДП, выполненных различными людьми. База попыток МТДП, и программа визуализации EER доступна для свободного использования [13].

Визуальный анализ полученных графиков позволил не только выделить наиболее эффективные алгоритмы, но и убедиться, что математическое моделирование выполнено в целом верно – отсутствуют необъяснимые выбросы или слишком резкая динамика работы алгоритмов. Полученные графики являются очень простым и эффективным средством оценить возможные последствия в случае неверного установления порога для каждого из алгоритмов.

Исследуя полученный графический материал, не сложно убедится в важности выбора жеста для аутентификации. Для всех алгоритмов надежность спокойного простого жеста неприемлемо мала.

4 Выводы

Проводя анализ полученного визуального отображения динамики ошибок, можно отметить особенность работы алгоритмов DTW для интенсивного и спокойного жеста. Из графиков видно, что уровень EER спокойного жеста находится на месте резкого спада FRR и резкого подъема FAR. Такое поведение ошибок может не позволить установить порог нужным образом, так как любая неточность ведет к резкому увеличению вероятности какой либо из них.

Интенсивный жест имеет уровень EER в пологой области графиков, это означает, что небольшое отклонение от идеального состояния может не сказаться на общем соотношении вероятностей ошибок.

Данный анализ наводит на предположение что, при дальнейшем увеличении интенсивности жеста стоит ожидать расширения диапазона пологой области графиков, внутри которого будет лежать EER. Так как интенсивный жест характерен, прежде всего, большим объемом данных, то для более современных устройств следует ждать лучших результатов в части EER. Это будет вызвано увеличением чувствительности и скорости работы, а значит и ростом объема данных, получаемых от новых акселерометров.

Показанные уровни ошибок должны быть подтверждены практикой использования методики в реальных условиях с последующей обработкой результатов.

По результатам данного моделирования можно предполагать, что для надежных (интенсивных) жестов уровень EER для биометрической составляющей МТДП не будет выше 0,4 %.

Среди исследуемых алгоритмов наиболее выгодными, с точки зрения надежности, для обработки биометрического признака, получаемого как значения показаний акселерометров, оказались варианты алгоритмов динамической трансформации шкалы времени – DTW. Эксперимент показал высокую зависимость надежности от сложности жеста (его интенсивности). Это подтверждает необходимость вводить ограничения и рекомендации в процессе формирования МТДП, позволяющие избежать слишком простых жестов. Кроме того, по аналогии с другими видами подписи, важную роль будет играть психоэмоциональное состояние человека в процессе создания подписи и в момент ее воспроизведения [14].

Представленные в данной статье графики позволяют наглядно увидеть динамику перераспределения ошибок первого и второго рода при сдвиге порога срабатывания. Знания этой динамики позволят более точно настраивать систему аутентификации в зависимости от того какую из вероятностей ошибок (FAR или FRR) необходимо минимизировать.

Для более полного представления о надежности МТДП следует провести исследование методики на спуфинг.

Список литературы

[1] Czajka A., Bowyer K.W. Presentation Attack Detection for Iris Recognition: An Assessment of the State of the Art //arXiv preprint arXiv:1804.00194. – 2018.

[2] Goicoechea-Telleria I. et al. Attack Potential Evaluation in Desktop and Smartphone Fingerprint Sensors: Can They Be Attacked by Anyone? //Wireless Communications and Mobile Computing. – 2018. – Т. 2018.

[3] Kinnunen T. et al. A Spoofing Benchmark for the 2018 Voice Conversion Challenge: Leveraging from Spoofing Countermeasures for Speech Artifact Assessment //arXiv preprint arXiv:1804.08438. – 2018.

[4] Patel V. M., Ratha N.K., Chellappa R. Cancelable biometrics: A review //IEEE Signal Processing Magazine. – 2015. – Т. 32. – №.5. – С. 54-65.

[5] Liang G. C., Xu X. Y., Yu J. D. User-Authentication on Wearable Devices Based on Punch Gesture Biometrics //ITM Web of Conferences. – EDP Sciences, 2017. – Т. 11. – С. 01003.

[6] Griswold-Steiner I., Matovu R., Serwadda A. Handwriting watcher: A mechanism for smartwatch-driven handwriting authentication //Biometrics (IJCB), 2017 IEEE International Joint Conference on. – IEEE, 2017. – С. 216-224.

[7] Lee W. H., Lee R. Implicit sensor-based authentication of smartphone users with smartwatch //Proceedings of the Hardware and Architectural Support for Security and Privacy 2016. – ACM, 2016. – С. 9.

[8] Козлов Ю.Е., Евсеев В.Л. Мультимодальная трехмерная динамическая подпись //Безопасность информационных технологий. – 2017. – Т. 24. – №.4. – С. 44-51.

[9] Козлов Ю.Е. Подходы к определению надежности мультимодальной трехмерной динамической подписи //Безопасность информационных технологий. – 2018. – Т. 25. – №.1. – С. 74-80.

[10] Moujahid D., Elharrouss O., Tairi H. Visual object tracking via the local soft cosine similarity //Pattern Recognition Letters. – 2018. – Т. 110. – С. 79-85.

[11] Mueen A. et al. Speeding up dynamic time warping distance for sparse time series data //Knowledge and Information Systems. – 2018. – Т. 54. – №. 1. – С. 237-263.

[12] Keogh E., Ratanamahatana C. A. Exact indexing of dynamic time warping //Knowledge and information systems. – 2005. – Т. 7. – №. 3. – С. 358-386.

[13] Козлов Ю.Е. База данных МТДП [Электронный ресурс], - URL:https://github.com/Yuryko/mtds.git.

[14] Алюшин А. М. Оценка психоэмоционального состояния человека по его подписи //Вопросы психологии. – 2018. – №. 2. – С. 133-140.

Scientific Visualization, 2019, volume 11, number 2, pages 99 - 99, DOI: 10.26583/sv.11.2.08

Use of methods of visual analytics to obtain integrated indicator of the quality of biometric authentication using the mechanism gesture manipulation

Yu.E. Kozlov

Financial University under the Government of the Russian Federation
(Financial University), Moscow, Russia

ORCID: 0000-0002-4448-0232, kozlovye@yandex.ru

Abstract

Employing multimodal authentication techniques in the mobile applications which use several interconnected parameters in their operation demands studying them from the point of view of reliability. One of widespread ways of defining characteristics of such techniques is defining types I and II errors, and receiving a integrated quality indicator which can be defined upon visualizing type I errors (FRR) and type II errors (FAR).

Joint construction of dependency charts of FRR and FAR on the threshold value is possible only when using computer modeling and tools of visual analytics allowing to be convinced of correctness of the drawn conclusions visually. Traditionally for biometric authentication systems having probability indicators of reliability, the parameter which characterizes the integrated quality indicator is the equal error rate (EER) which is at the intersection of FRR and FAR curves.

The given article offers the research which has allowed to compare visually efficiency of a number of algorithms when carrying out the authentication procedure and to define the most favorable ones for biometric authentication in mobile applications by means of the in-air signature mechanism in the context of reliability.

Keywords: in-air signature, MTDS, signature, wearable device, authentication.

References

[1] Czajka A., Bowyer K.W. Presentation Attack Detection for Iris Recognition: An Assessment of the State of the Art //arXiv preprint arXiv:1804.00194. – 2018.

[2] Goicoechea-Telleria I. et al. Attack Potential Evaluation in Desktop and Smartphone Fingerprint Sensors: Can They Be Attacked by Anyone? //Wireless Communications and Mobile Computing. – 2018. – T. 2018.

[3] Kinnunen T. et al. A Spoofing Benchmark for the 2018 Voice Conversion Challenge: Leveraging from Spoofing Countermeasures for Speech Artifact Assessment //arXiv preprint arXiv:1804.08438. – 2018.

[4] Patel V. M., Ratha N.K., Chellappa R. Cancelable biometrics: A review //IEEE Signal Processing Magazine. – 2015. – T. 32. – №.5. – pp. 54-65.

[5] Liang G. C., Xu X. Y., Yu J. D. User-Authentication on Wearable Devices Based on Punch Gesture Biometrics //ITM Web of Conferences. – EDP Sciences, 2017. – T. 11. – P. 01003.

[6] Griswold-Steiner I., Matovu R., Serwadda A. Handwriting watcher: A mechanism for smartwatch-driven handwriting authentication //Biometrics (IJCB), 2017 IEEE International Joint Conference on. – IEEE, 2017. – P. 216-224.

[7] Lee W. H., Lee R. Implicit sensor-based authentication of smartphone users with smartwatch //Proceedings of the Hardware and Architectural Support for Security and Privacy 2016. – ACM, 2016. – P. 9.

[8] Kozlov Y.E., Evseev V.L. Mul'timodal'naya trekhmernaya dinamicheskaya podpis' //Bezopasnost' informacionnyh tekhnologij. – 2017. – T. 24. – №.4. – P. 44-51 [in Russian].

[9] Kozlov Y.E. Podhody k opredeleniyu nadezhnosti mul'timodal'noj trekhmernoj dinamicheskoj podpisi //Bezopasnost' informacionnyh tekhnologij. – 2018. – T. 25. – №.1. – P. 74-80 [in Russian].

[10] Moujahid D., Elharrouss O., Tairi H. Visual object tracking via the local soft cosine similarity //Pattern Recognition Letters. – 2018. – T. 110. – C. 79-85.

[11] Mueen A. et al. Speeding up dynamic time warping distance for sparse time series data //Knowledge and Information Systems. – 2018. – T. 54. – №. 1. – C. 237-263.

[12] Keogh E., Ratanamahatana C. A. Exact indexing of dynamic time warping //Knowledge and information systems. – 2005. – T. 7. – №. 3. – C. 358-386.

[13] Kozlov Y.E. Baza dannyh MTDP [accessed 09.01.2019], - URL:https://github.com/Yuryko/mtds.git.

[14] Alyushin A.M. Ocenka psihoehmocional'nogo sostoyaniya cheloveka po ego podpisi //Voprosy psihologii. – 2018. – №. 2. – S. 133-140.