Додаток А.

Комплект графічних матеріалів

«Дослідження інформативних ознак сенсорного почерку власників мобільних пристроїв»

Актуальність роботи. Ідентифікація за відбитками пальців або за 2D (3D) геометрією обличчя вже стала звичною – і майже настільки ж звичною стала інформація про те, як зловмисники можуть зламувати ці технології. Один із способів, який не є біометричним в строгому сенсі, – так званий «відбиток мобільного пристрою». У цьому випадку використовують такі характеристики, як модель пристрою, операційна система, додатки, що використовує користувач, параметри Wi-Fi-мереж, до яких часто підключається користувач, або, навіть, навушників, які він використовує. В результаті система створює свого роду профіль і пристрою, і звичок конкретного користувача. Якщо система виявляє нетиповий сценарій використання мобільного пристрою, вона використовує додаткові способи перевірки (паролі, контрольні питання тощо).

Однак цьому методу ідентифікації заважає те, що Apple, Google та інші виробники мобільних пристроїв і ПЗ обмежують набір параметрів, які можна отримати про пристрій віддалено. Це робиться з метою захисту особистих даних користувачів. Тому розвиваються нові методи біометричної ідентифікації. В першу чергу це так звана поведінкова біометрія. В її основі лежить цілий ряд параметрів, що відрізняють поведінку конкретного користувача. Так, наприклад, використовувані в смартфоні гіроскопи і акселерометри можуть оцінити і запам'ятати, як людина тримає смартфон під час використання, в якому становищі зазвичай носить його і навіть як ходить. За допомогою тачскріну і клавіатури можна встановити характерні для людини рухи рук і пальців.

«Дослідження інформативних ознак сенсорного почерку власників мобільних пристроїв»

Метою роботи є підвищення інформаційної безпеки мобільних пристроїв на основі аналізу «мобільного» клавіатурного почерку.

Для досягнення поставленої мети необхідно розв'язати наступні **задачі**:

1) провести огляд основних методів біометричної аутентифікації, що використовуються або є перспективними до використання в мобільних пристроях.;

2) провести пошук відкритих датасетів параметрів клавіатурного почерку та обрати декілька з них для подальших досліджень;

3) на основі обраних датасетів дослідити інформативність параметрів сенсорного почерку;

4) на основі проведених досліджень запропонувати сценарії використання сенсорного почерку в якості біометричної технології захисту мобільних пристроїв.

«Дослідження інформативних ознак сенсорного почерку власників мобільних пристроїв»

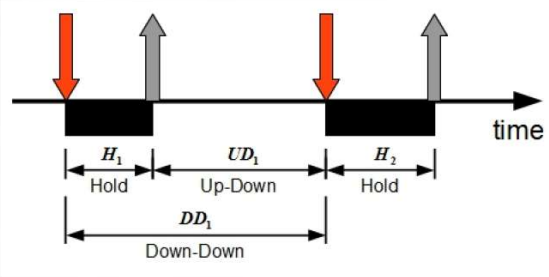
Методи біометричної аутентифікації, що використовуються або є перспективними для використання в мобільних пристроях: ***розпізнавання за обличчям, розпізнавання за голосом, розпізнавання за динамічним графічним паролем, розпізнавання за тривимірним динамічним підписом, розпізнавання за геометрією долоні, розпізнавання за райдужною оболонкою ока, розпізнавання за відбитком пальця, розпізнавання за клавіатурним почерком.***

Для методів ***розпізнання за обличчям, райдужною оболонкою ока, геометрією долоні*** важливими є рівень освітлення; спрямоване освітлення; вираз обличчя користувача; положення голови користувача; використання макіяжу і / або аксесуарів; різні розміри зіниці в моменти реєстрації і аутентифікації; неконтрольований і складний фони в процесі фотографування; швидкі зміни температури і вологості, що викликають конденсацію на об'єктиві; рух користувача або смартфона.

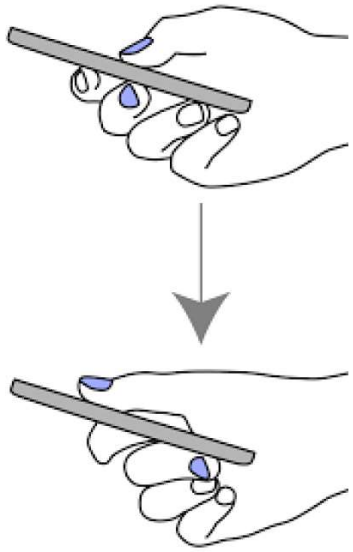
Для ***розпізнання за голосом*** важливими є рівень фонового шуму; наявність поруч з користувачем інших людей, які голосно розмовляють; завади в мікрофоні через вітер.

Для ***розпізнавання за відбитком пальця*** важливими є освітлення; температура і вологість; пильне або забруднене навколишнє середовище, пильні або забруднені пальці; відсутність папілярного візерунка; швидкі зміни температури і вологості, що викликають конденсацію на робочій поверхні біометричного сканера.

Інформативні характеристики клавіатурного та сенсорного почерків



1. Тривалість утримання клавіші (Hold-Time) на фізичній клавіатурі.
2. Тривалість паузи між відпусканням першої клавіші та натисканням другої клавіші (Up-Down-Time) на фізичній клавіатурі.
3. Час між натисканнями першої клавіші та другої клавіш (Down-Down-Time) на фізичній клавіатурі.



1. Тривалість утримання клавіші (Hold-Time) на віртуальній клавіатурі.
2. Тривалість паузи між відпусканням першої клавіші та натисканням другої клавіші (Up-Down-Time) на віртуальній клавіатурі.
3. Час між натисканнями першої клавіші та другої клавіш (Down-Down-Time) на віртуальній клавіатурі.
4. Тиск на екран в момент торкання пальцями екрану.

5. Розмір «плями від пальця» в момент торкання пальцями екрану.

6. Прискорення по трьох осях координат в момент торкання пальцями екрану.

7. Загальна відстань - сума відстаней (в пікселях) між двома послідовними кнопками на віртуальній клавіатурі.

8. Загальний час вводу парольної фрази.

The Mobikey Keystroke Dynamics Password Database

База даних «The Mobikey Keystroke Dynamics Password Database» містить параметри вводу трьох парольних фраз **«kicsikutyatarka»** (датасет «MOBIKEY easy»), **«Kktsf2!2014»** (датасет «MOBIKEY logicalstrong»), **«.tie5Roanl»** (датасет «MOBIKEY strong») на віртуальній клавіатурі **планшету Nexus 7**, яку набирали 54 користувача по 60 раз кожен.

Дані в кожному з датасетів представлено у форматі Excel файлу та складаються з наступних полів (рис. 3.1):

1) holdtime1 – holdtimeN – час натискання клавіші в процесі набору парольної фрази (HT). Для паролю «kicsikutyatarka» – 15 параметрів holdtime, для паролю «Kktsf2!2014» – 13 параметрів holdtime (по дві клавіші для вводу «К» та «!»), для паролю «.tie5Roanl» – 13 параметрів holdtime (по дві клавіші для вводу «.», «5» та «R»);

2) downdown1 – downdownN – час між двома послідовними натисканнями на клавіші в процесі набору парольної фрази (DD). Для паролю «kicsikutyatarka» – 14 параметрів downdown, для паролів «Kktsf2!2014» та «.tie5Roanl» – 12 параметрів downdown;

3) updown1 – updownN – час паузи між двома послідовними натисканнями на клавіші в процесі набору парольної фрази (UD). Для паролю «kicsikutyatarka» – 14 параметрів updown, для паролів «Kktsf2!2014» та «.tie5Roanl» – 12 параметрів updown;

4) pressure1 – pressureN – тиск на екран в процесі набору парольної фрази. Для паролю «kicsikutyatarka» – 15 параметрів pressure, для паролів «Kktsf2!2014» та «.tie5Roanl» – 13 параметрів pressure;

The Mobikey Keystroke Dynamics Password Database

5) fingerarea1 – fingerareaN – розмір області на сенсорному екрані від пальця користувача в процесі набору парольної фрази (FA). Для паролю «kicsikutyatarka» – 15 параметрів fingerarea, для паролів «Kktsf2!2014» та «.tie5Roanl» – 13 параметрів fingerarea;

6) meanholdtime – середнє значення часу натискання клавіш в процесі набору парольної фрази (MHT);

7) meanpressure – середнє значення тиску на екран в процесі набору парольної фрази (MP);

8) meanfingerarea – середнє значення розміру області на сенсорному екрані від пальця користувача в процесі набору парольної фрази (MFA);

9) meanxacceleration – середнє значення прискорення по вісі «X» відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAX);

10) meanyacceleration – середнє значення прискорення по вісі «Y» відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAY);

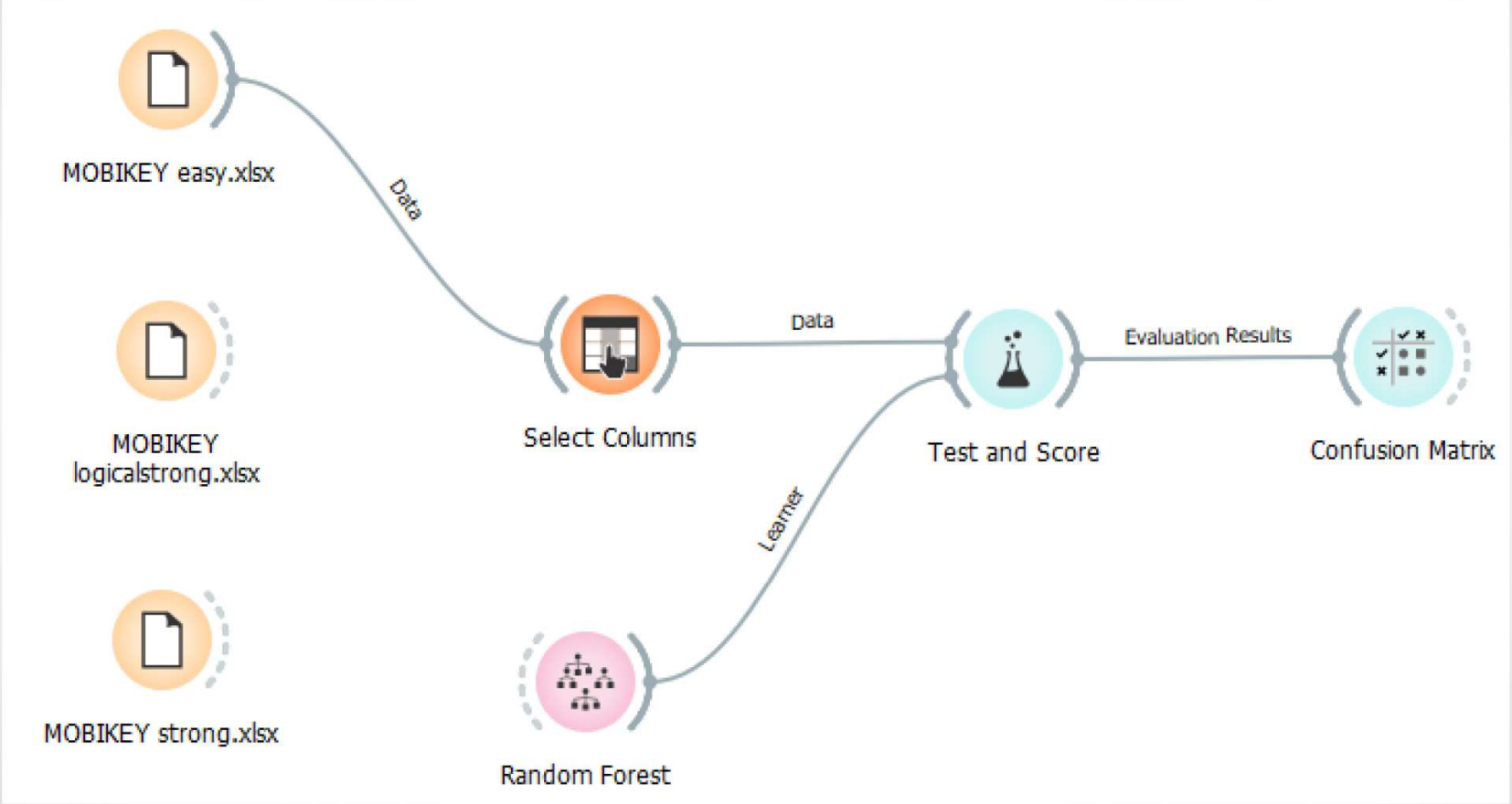
11) meanzacceleration – середнє значення прискорення по вісі «Z» відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAZ);

12) totaldistance – сума відстаней (у пікселях) між двома послідовними кнопками на віртуальній клавіатурі (TD);

13) totaltime – час вводу парольної фрази (TT);

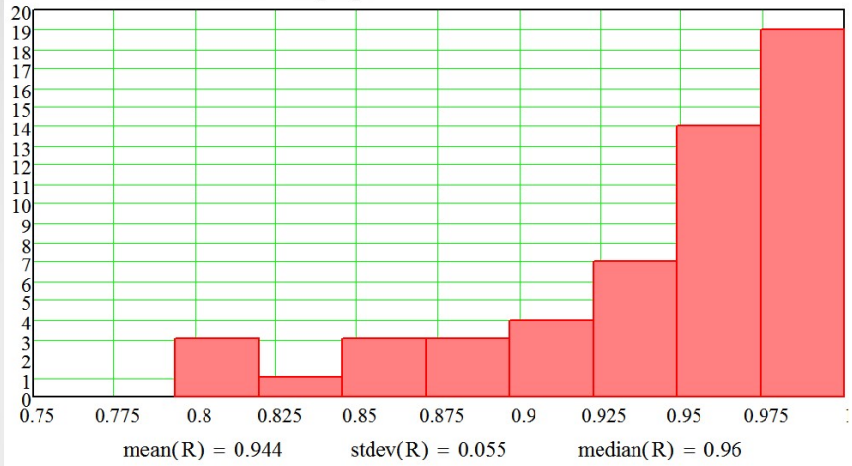
14) velocity – швидкість, обчислювалась як частка відстані та загального часу.

Схема експерименту у Orange



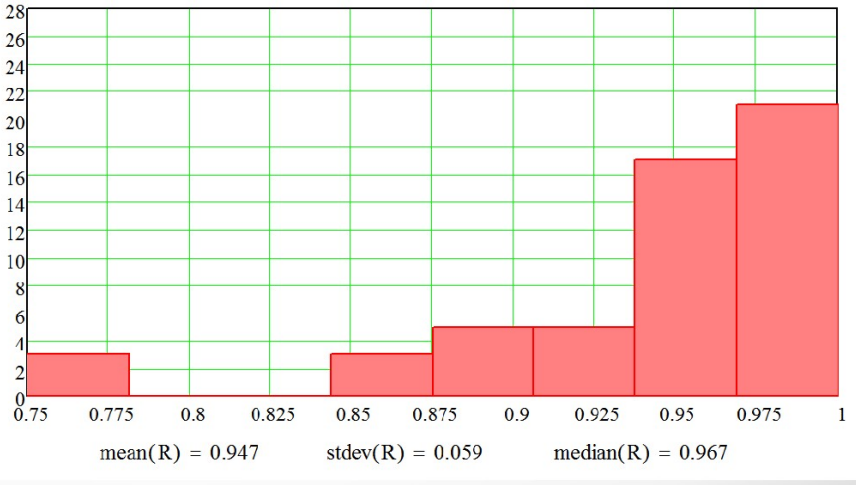
Результати проведених досліджень

The MOBIKEY Keystroke Dynamics Password Database
Пароль «kicsikutyatarka»
82 інформативні ознаки



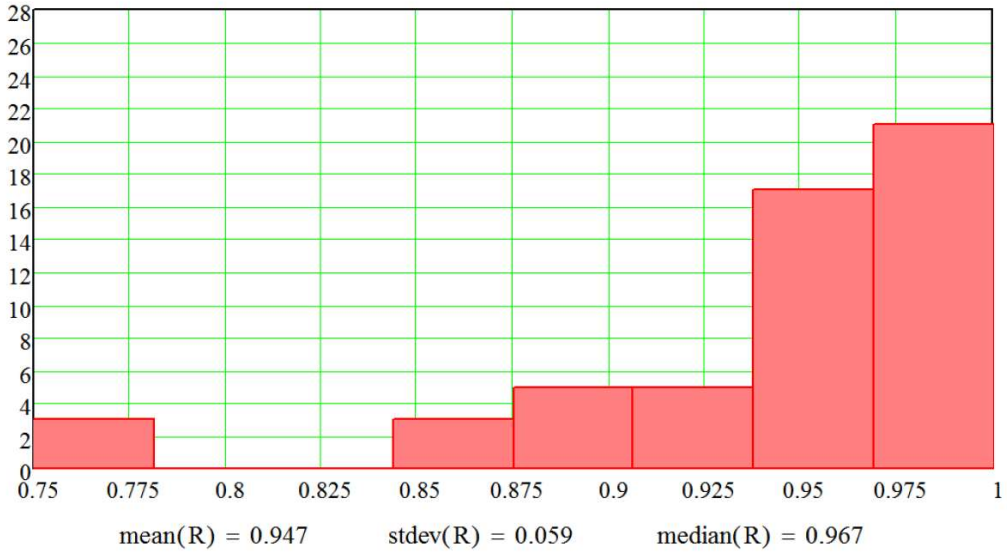
The MOBIKEY Keystroke Dynamics Password Database
Пароль «Kktsf2!20»
72 інформативні ознаки

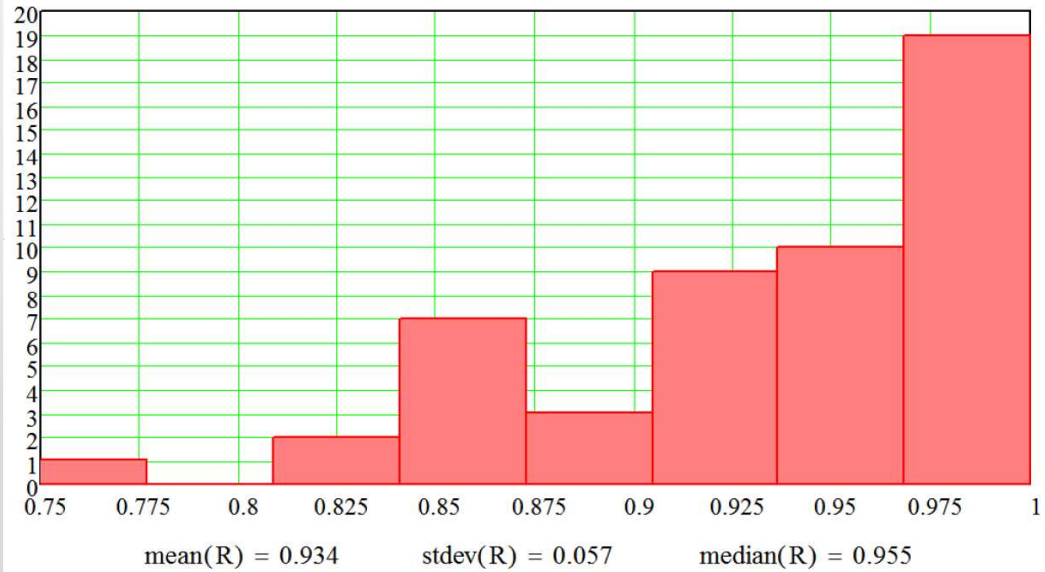
The MOBIKEY Keystroke Dynamics Password Database
Пароль «.tie5Roanl»
72 інформативні ознаки



Результати проведених досліджень

Сенсорний почерк
The MOBIKEY Keystroke Dynamics Password Database
Пароль «.tie5Roanl»
72 інформативних ознаки

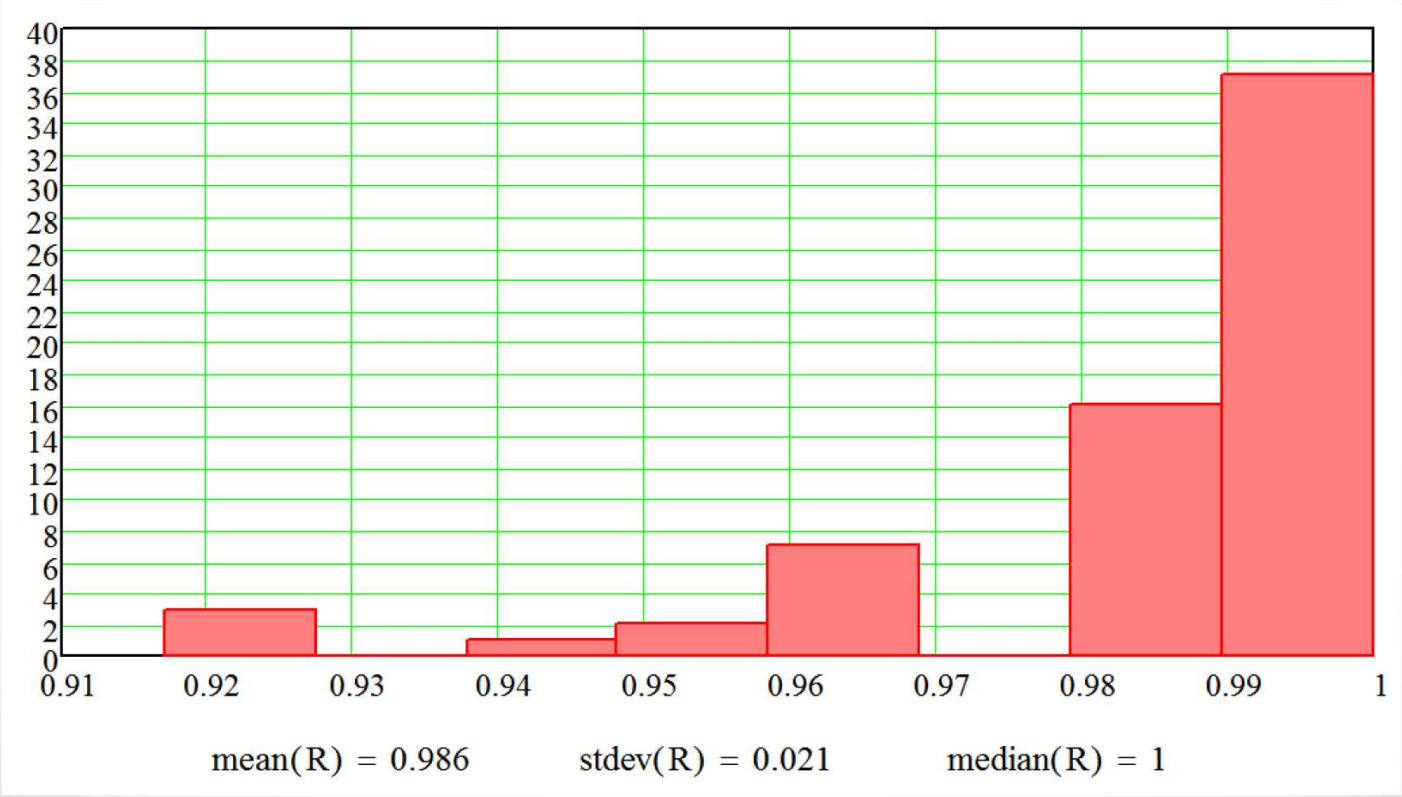




Клавіатурний почерк
Keystroke Dynamics Benchmark Data Set
Пароль «.tie5Roanl»
31 інформативна ознака

Результати проведених досліджень

The MOBIKEY Keystroke Dynamics Password Database
Пароль «.tie5Roanl»
66 експериментів оцінки точності двійкової класифікації користувачів:
«100», «203», «303», «503», «602», «605», «1004», «1203», «1204»,
«102», «302», «1301»



Результати проведених досліджень

The MOBIKEY Keystroke Dynamics Password Database
Пароль «Kktsf2!20»

Інформативний параметр	Критерій							Сумарна вага
	Info. gain	Gain ratio	Gini	ANOVA	χ^2	ReliefF	FCBF	
meanholdtime	1.000	1.000	1.000	1.000	0.940	1.000	1.000	6.940
meanfingerarea	0.777	0.777	0.834	0.553	1.000	0.385	0.806	5.131
velocity	0.653	0.653	0.636	0.745	0.809	0.597	0.707	4.801
meanzaccelaration	0.612	0.612	0.620	0.334	0.523	0.620	0.676	3.998
meanpressure	0.533	0.533	0.531	0.622	0.569	0.431	0.617	3.836
meanyaccelaration	0.596	0.596	0.603	0.256	0.416	0.698	0.000	3.165
meanxaccelaration	0.450	0.450	0.456	0.271	0.377	0.343	0.558	2.904
meanupdown	0.225	0.225	0.251	0.000	0.187	0.003	0.000	0.892
totaltime	0.176	0.176	0.186	0.029	0.203	0.000	0.000	0.771
meandowndown	0.175	0.175	0.184	0.028	0.195	0.000	0.000	0.758
totaldistance	0.000	0.000	0.000	0.076	0.000	0.103	0.273	0.453

Результати проведених досліджень

The MOBIKEY Keystroke Dynamics Password Database
Мультикласова класифікація
Пароль «Kktsf2!20»
7 інформативних параметрів:
«meanholdtime», «meanfingerarea»,
«velocity», «meanpressure»,
«meanzaccelaration»,
«meanxaccelaration»,
«meanyaccelaration»

Predicted

Actual	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	93.3 %	0.0 %	0.0 %	3.3 %	1.7 %	1.7 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	60
102	0.0 %	100.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	62
203	0.0 %	0.0 %	87.7 %	0.0 %	0.0 %	1.5 %	0.0 %	0.0 %	6.2 %	0.0 %	4.6 %	0.0 %	65
302	1.7 %	0.0 %	0.0 %	96.7 %	0.0 %	1.7 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	60
303	1.7 %	0.0 %	0.0 %	0.0 %	96.7 %	0.0 %	1.7 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	60
503	1.7 %	1.7 %	1.7 %	0.0 %	0.0 %	86.7 %	0.0 %	0.0 %	8.3 %	0.0 %	0.0 %	0.0 %	60
602	1.6 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	95.2 %	1.6 %	0.0 %	1.6 %	0.0 %	0.0 %	62
605	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	95.2 %	0.0 %	3.2 %	1.6 %	0.0 %	62
1004	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	6.6 %	0.0 %	0.0 %	88.5 %	1.6 %	3.3 %	0.0 %	61
1203	0.0 %	0.0 %	1.6 %	0.0 %	0.0 %	3.3 %	0.0 %	3.3 %	1.6 %	88.5 %	1.6 %	0.0 %	61
1204	0.0 %	3.3 %	8.3 %	0.0 %	3.3 %	0.0 %	0.0 %	1.7 %	0.0 %	6.7 %	76.7 %	0.0 %	60
1301	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	100.0 %	62
Σ	60	65	64	60	61	61	60	63	64	62	53	62	735

Predicted

Actual	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	95.0 %	0.0 %	0.0 %	0.0 %	1.7 %	1.7 %	0.0 %	0.0 %	0.0 %	0.0 %	1.7 %	0.0 %	60
102	0.0 %	98.4 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	1.6 %	0.0 %	0.0 %	0.0 %	0.0 %	62
203	0.0 %	1.5 %	92.3 %	0.0 %	0.0 %	0.0 %	0.0 %	1.5 %	3.1 %	0.0 %	1.5 %	0.0 %	65
302	0.0 %	0.0 %	0.0 %	100.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	60
303	0.0 %	0.0 %	1.7 %	0.0 %	98.3 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	60
503	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	90.0 %	0.0 %	1.7 %	8.3 %	0.0 %	0.0 %	0.0 %	60
602	0.0 %	0.0 %	1.6 %	0.0 %	0.0 %	1.6 %	91.9 %	0.0 %	3.2 %	0.0 %	1.6 %	0.0 %	62
605	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	93.5 %	0.0 %	6.5 %	0.0 %	0.0 %	62
1004	4.9 %	1.6 %	0.0 %	0.0 %	0.0 %	3.3 %	0.0 %	0.0 %	90.2 %	0.0 %	0.0 %	0.0 %	61
1203	1.6 %	0.0 %	0.0 %	0.0 %	1.6 %	4.9 %	0.0 %	1.6 %	1.6 %	88.5 %	0.0 %	0.0 %	61
1204	1.7 %	1.7 %	1.7 %	0.0 %	1.7 %	0.0 %	0.0 %	1.7 %	1.7 %	1.7 %	88.3 %	0.0 %	60
1301	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	100.0 %	62
Σ	62	64	63	60	62	61	57	63	66	59	56	62	735

The MOBIKEY Keystroke Dynamics Password Database
Мультикласова класифікація
Пароль «Kktsf2!20»
72 інформативні параметри

Висновки

1. Виконано огляд основних методів біометричної аутентифікації, що використовуються або є перспективними для використання в мобільних пристроях. Це розпізнавання за голосом, розпізнавання за динамічним графічним паролем, розпізнавання за тривимірним динамічним підписом, розпізнавання за геометрією долоні, розпізнавання за райдужною оболонкою ока, розпізнавання за відбитком пальця, розпізнавання за клавіатурним почерком. Використання сенсорного почерку має потенціал для застосування як додаткова міра, що підвищує загальний рівень безпеки при аутентифікації.

Крім того одним з плюсів поведінкової біометрії, до якої відноситься сенсорний почерк, є розпізнавання не тільки знайомих загроз, а й виявлення нових шахрайських схем. Оскільки цей метод заснований на характеристиках поведінки, він дозволяє розпізнавати аномальну поведінку незалежно від схеми атаки – а значить, є ефективним засобом запобігання новим, ще невідомим, типам атак.

2. У роботі проаналізовано інформативні ознаки сенсорного почерку. Можна виділити три основних класи: часові параметри, взаємодії з екраном (тиск та розмір «плями» від пальця) та психофізіологічні параметри, де до тиску та розміру «плями» додаються показання акселерометру та динаміка руху кінчика пальця по екрану.

Висновки

3. За даними датасету «The Mobikey Keystroke Dynamics Password Database» інтегральна точність мультикласової класифікації за сенсорним почерком становить 94.7%. Отже, системи розпізнавання за сенсорним почерком можуть забезпечити точність ідентифікації, яка притаманна системам ідентифікації за клавіатурним почерком. Проте для забезпечення такої точності необхідно збирати більші масиви даних.

4. Для досвідчених користувачів перехід до паролів, що містять великі і маленькі букви, цифри та символи не є необхідним з точки зору підвищення якості ідентифікації. Для недосвідчених користувачів подібний перехід є більш бажаним, оскільки кількість користувачів з точністю розпізнавання 90 % зростає зі збільшенням складності паролю.

5. Точність розпізнавання за часовими параметрами сенсорного почерку становить 83%. Таким чином, нестабільність часових параметрів сенсорного почерку обумовлює неможливість побудови аутентифікаційних систем, що враховують лише ці часові параметри.

6. Точність розпізнавання за параметрами взаємодії з екраном складає 67.7%. Таким чином, тиск та розмір «плями» не є настільки унікальними параметрами сенсорного почерку, щоб будувати тільки за ними аутентифікаційну систему.

7. Найінформативнішими параметрами сенсорного почерку є прискорення по трьох осях координат, динаміку руху кінчика пальця по екрану та усереднений час натискання клавіш в процесі набору парольної фрази. Використання цих семи параметрів дає інтегральну точність мультикласової класифікації 91.1 %.

Висновки

8. Підвищити точність ідентифікації можна за рахунок побудови двійкової системи класифікації, коли цільовому користувачу присвоюється клас 1, тобто «зареєстрований», а усім іншим користувачам – клас 2, тобто «зловмисник». Це можливо, оскільки на відміну від комп'ютера, де зареєстрованими користувачами можуть бути декілька людей, у мобільного пристрою завжди тільки один власник.

Проведені дослідження дозволяють зробити висновок про забезпечення інтегральної помилки FAR 1.58 %. Враховуючи також той факт, що зловмисник апріорі має сформований сенсорний почерк, оскільки сфера його професійних навичок вимагає тривалого часу взаємодії зі смартфонами (один з пари користувачів вже має унікальний почерк), то з плином часу значення помилки FAR буде зменшуватись, оскільки інформативні ознаки сенсорного почерку легітимного користувача також ставатимуть більш унікальними (обидва користувачі в парі мають унікальний почерк). За результатами проведених досліджень можна очікувати зменшення рівня помилки FAR до 1.2 %, тобто 12 пропусків зловмисника на 1000 спроб.

Рівень помилки FRR (доступ заборонений користувачеві, зареєстрованому в системі) за умови недосвідченого користувача може становити до 1.36 %. Якщо ж враховувати лише користувачів з унікальним почерком, то рівень помилки FRR зменшується до 0.54 %, тобто 54 недопуски верифікованого користувача на 10000 спроб.

Номер документу	Позначення	Найменування	Прим.
		Текстові документи	
1		Пояснювальна записка	100 с.
		Графічний матеріал	
2-4		Дослідження інформативних ознак	3хА4 ел.ф.
		сенсорного почерку власників	
		мобільних пристроїв	
5-6		Інформативні характеристики	2хА4 ел.ф.
		клавіатурного та сенсорного почерків	
7-8		The Mobikey Keystroke Dynamics	2хА4 ел.ф.
		Password Database	
9		Схема експерименту у Orange	А4 ел.ф.
10-14		Результати проведених досліджень	5хА4 ел.ф.
15-17		Висновки	3хА4 ел.ф.

Из	Лист	№ докум.	Підпис	Дата				
Розроб.		Кураксін			*ДОСЛІДЖЕННЯ ІНФОРМАТИВНИХ ОЗНАК СЕНСОРНОГО ПОЧЕРКУ ВЛАСНИКІВ МОБІЛЬНИХ ПРИСТРОЇВ*	Літера	Лист	Листів
Перев.		Горелов				Д		
						ХНУРЕ Кафедра КРіСТЗІ		
Н.контр.		Милютченко						
Затв.		Антіпов			Відомість кваліфікаційної роботи магістра			