Додаток А.

Комплект графічних матеріалів

«Дослідження ефективності ідентифікації особи за графічним паролем»

Актуальність роботи. Ідентифікація за відбитками пальців або за геометрією обличчя вже стали звичною практикою – і майже настільки ж звичною стала інформація про те, як зловмисники зламують 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 ефективності ідентифікації особи за графічним паролем»

Метою роботи є підвищення інформаційної безпеки мобільних пристроїв на основі аналізу цифрового рукописного рідпису.

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 цифрового рукописного підпису та обрати один з них для подальших досліджень;

3) на основі обраних датасетів дослідити інформативність параметрів цифрового рукописного підпису;

4) на основі проведених досліджень запропонувати сценарії використання цифрового рукописного підпису в якості біометричної технології захисту мобільних пристроїв.

«Дослідження ефективності ідентифікації особи за графічним паролем»

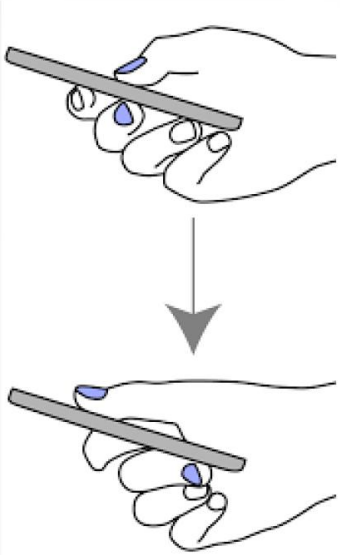
Основні методи біометричної аутентифікації, що використовуються або є перспективними для використання в мобільних пристроях: ***розпізнавання за обличчям, розпізнавання за динамічним графічним паролем, розпізнавання за тривимірним динамічним підписом, розпізнавання за відбитком пальця, розпізнавання за клавіатурним почерком.***

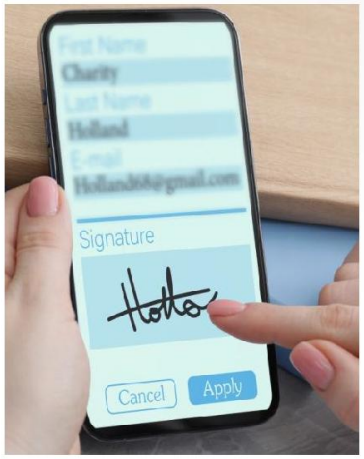
Зручність використання кожної біометричної модальності залежить від умов навколишнього середовища.

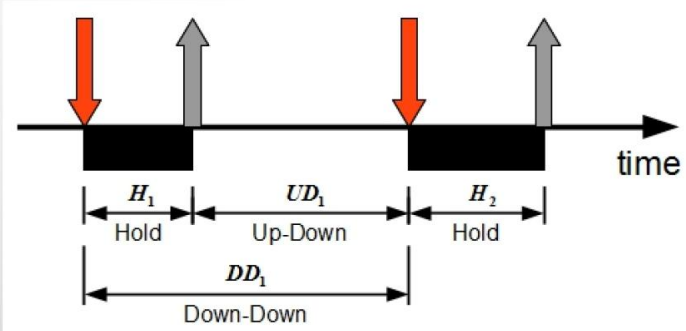
Для методів ***розпізнання за обличчям*** важливими є рівень освітлення (занадто світло / занадто темно); спрямоване освітлення (приводить до тіней на фотографіях); вираз обличчя користувача; положення голови користувача; використання макіяжу і / або аксесуарів (капелюх, шарф, сонцезахисні окуляри тощо); неконтрольований і складний фони в процесі фотографування; швидкі зміни температури і вологості, що викликають конденсацію на об'єктиві; рух користувача або смартфона (наприклад, рух поїзда, судна або літака).

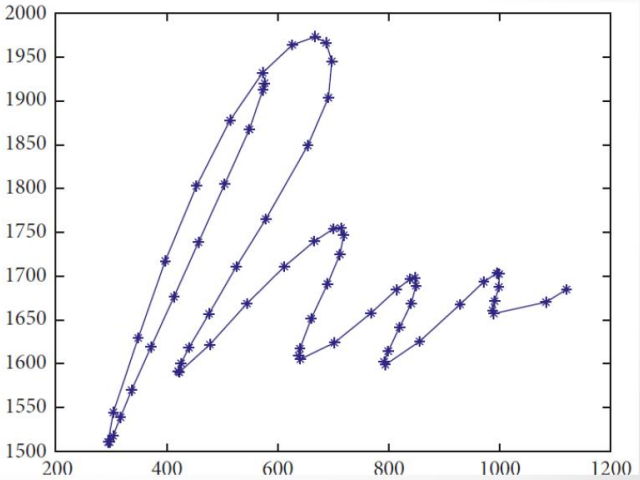
Для ***розпізнавання за відбитком пальця*** важливими є освітлення (пряме освітлення може впливати на роботу оптичного біометричного сканера; температура і вологість (можуть призводити до надмірно сухої або надмірно вологої шкіри, ускладнюючи збір відбитків пальців); пильне або забруднене навколишнє середовище, пильні або забруднені пальці (можуть призводити до забруднення робочої поверхні біометричного сканера); відсутність папілярного візерунка; швидкі зміни температури і вологості, що викликають конденсацію на робочій поверхні біометричного сканера.

Мобільний клавіатурний почерк та цифровий рукописний підпис



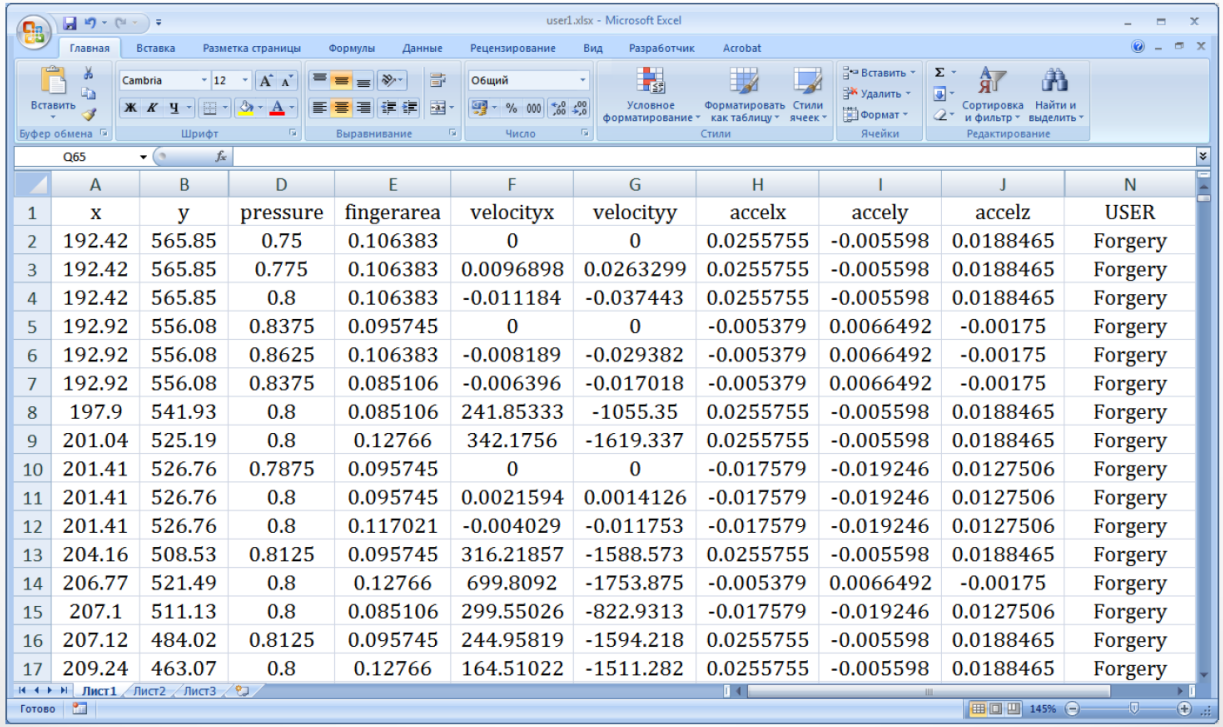






The MOBISIG signature database

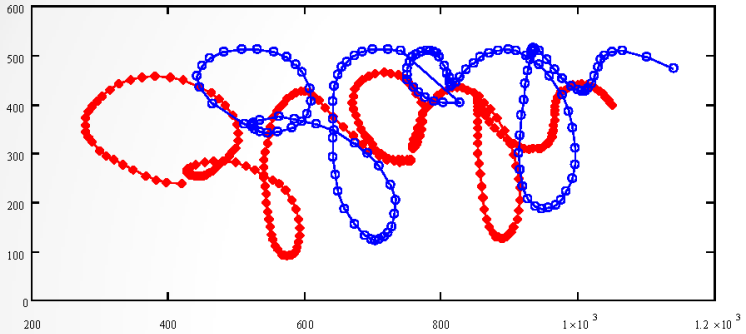
Датасет містить параметри вводу унікальних 83 парольних фраз, що входять до перших 100 найпоширеніших угорських імен. Кожна сигнатура (спроба введення підпису) є послідовністю дискретних значень **[x, y, p, f, vx, vy, ax, ay, az]**, де **[x, y]** – значення координат **x** та **y** в процесі вводу парольної фрази; **[p, f]** – тиск і розмір «плями» кінчика пальця в процесі вводу парольної фрази; **[vx, vy]** – швидкості переміщення кінчика пальця за координатами x та y відповідно в процесі вводу парольної фрази; **[ax, ay, az]** – прискорення планшету в тривимірному просторі, що характеризують положення планшету в руці користувача в процесі вводу парольної фрази.



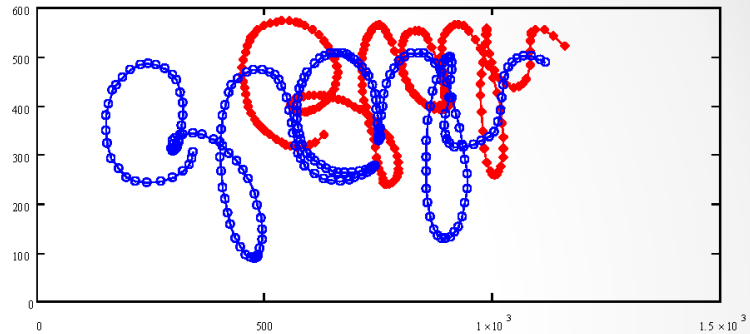
	A	B	D	E	F	G	H	I	J	N
1	x	y	pressure	fingerarea	velocityx	velocityy	accelx	accely	accelz	USER
2	192.42	565.85	0.75	0.106383	0	0	0.0255755	-0.005598	0.0188465	Forgery
3	192.42	565.85	0.775	0.106383	0.0096898	0.0263299	0.0255755	-0.005598	0.0188465	Forgery
4	192.42	565.85	0.8	0.106383	-0.011184	-0.037443	0.0255755	-0.005598	0.0188465	Forgery
5	192.92	556.08	0.8375	0.095745	0	0	-0.005379	0.0066492	-0.00175	Forgery
6	192.92	556.08	0.8625	0.106383	-0.008189	-0.029382	-0.005379	0.0066492	-0.00175	Forgery
7	192.92	556.08	0.8375	0.085106	-0.006396	-0.017018	-0.005379	0.0066492	-0.00175	Forgery
8	197.9	541.93	0.8	0.085106	241.85333	-1055.35	0.0255755	-0.005598	0.0188465	Forgery
9	201.04	525.19	0.8	0.12766	342.1756	-1619.337	0.0255755	-0.005598	0.0188465	Forgery
10	201.41	526.76	0.7875	0.095745	0	0	-0.017579	-0.019246	0.0127506	Forgery
11	201.41	526.76	0.8	0.095745	0.0021594	0.0014126	-0.017579	-0.019246	0.0127506	Forgery
12	201.41	526.76	0.8	0.117021	-0.004029	-0.011753	-0.017579	-0.019246	0.0127506	Forgery
13	204.16	508.53	0.8125	0.095745	316.21857	-1588.573	0.0255755	-0.005598	0.0188465	Forgery
14	206.77	521.49	0.8	0.12766	699.8092	-1753.875	-0.005379	0.0066492	-0.00175	Forgery
15	207.1	511.13	0.8	0.085106	299.55026	-822.9313	-0.017579	-0.019246	0.0127506	Forgery
16	207.12	484.02	0.8125	0.095745	244.95819	-1594.218	0.0255755	-0.005598	0.0188465	Forgery
17	209.24	463.07	0.8	0.12766	164.51022	-1511.282	0.0255755	-0.005598	0.0188465	Forgery

The MOBISIG signature database

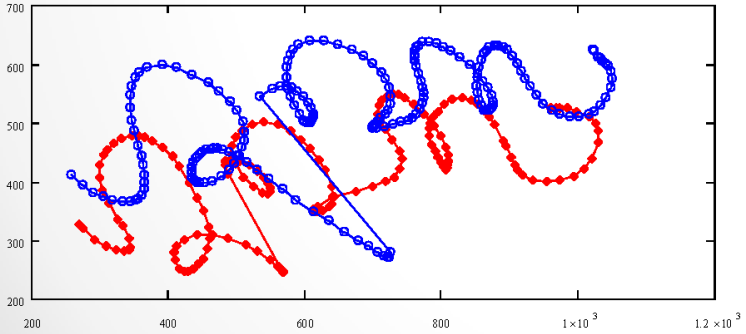
Користувач 17, парольний підпис “OLAH”



Спроби підробки парольного підпису “OLAH” користувачами 18 та 21



Користувач 54, парольний підпис “VERES”



Спроби підробки парольного підпису “VERES” користувачами 56 та 58

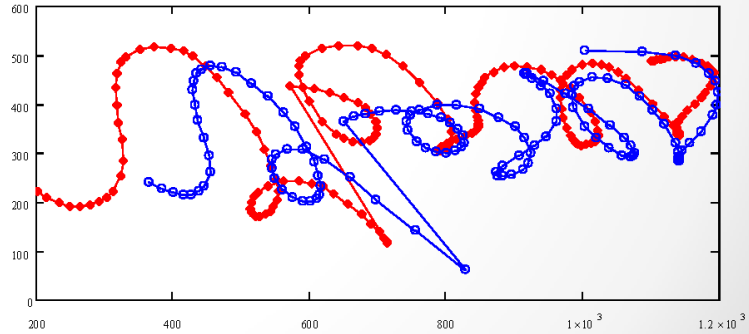
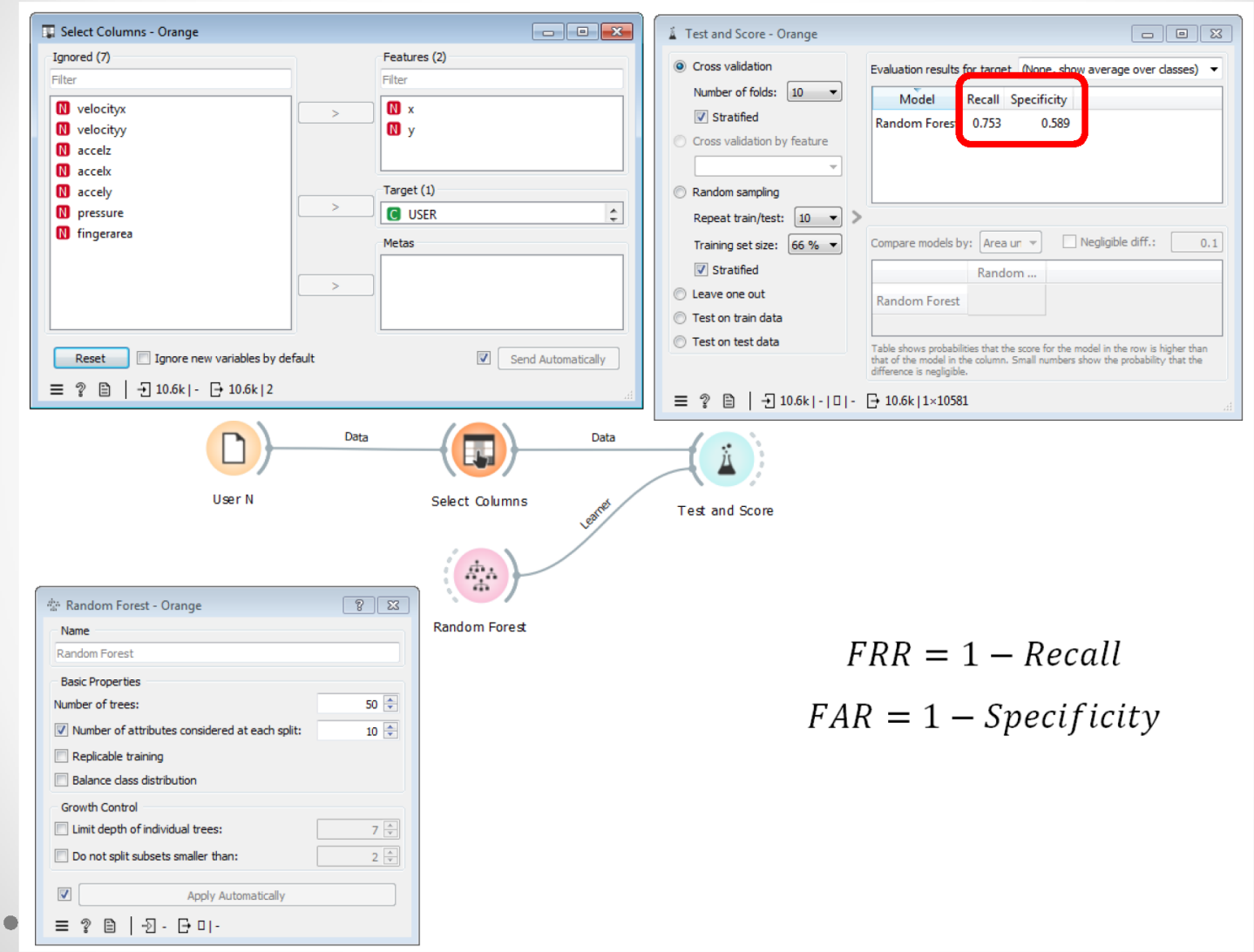


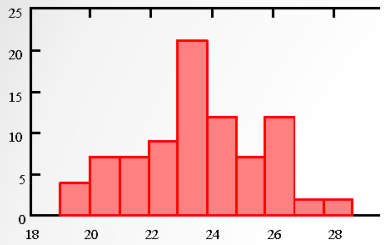
Схема експерименту у Orange



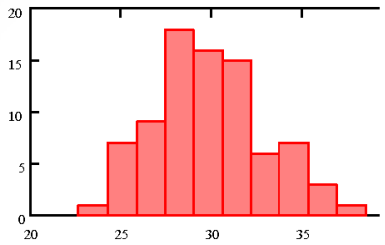
$$FRR = 1 - Recall$$

$$FAR = 1 - Specificity$$

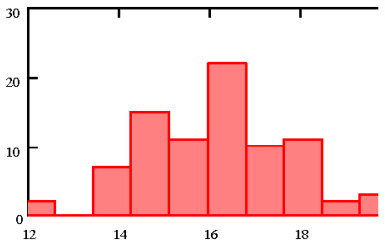
Результати проведених досліджень



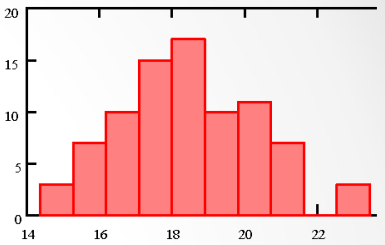
Гістограма значень FRR для параметрів $[x_t, y_t]$



Гістограма значень FAR для параметрів $[x_t, y_t]$



Гістограма значень FRR для параметрів $[p_t, f_{a_t}]$



Гістограма значень FAR для параметрів $[p_t, f_{a_t}]$

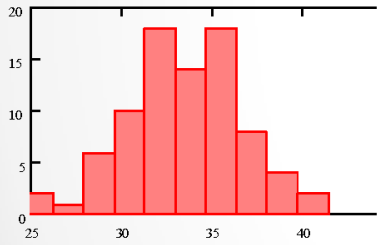


Рисунок 3.16 – Гістограма значень FRR для параметрів $[vx_t, vy_t]$

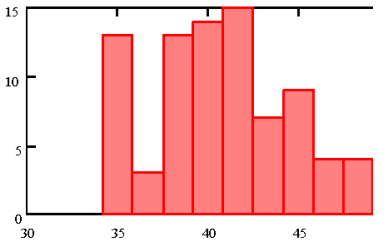
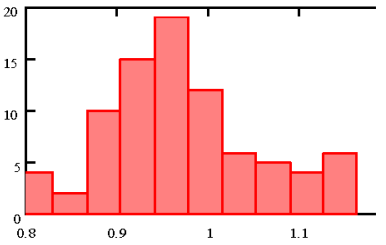
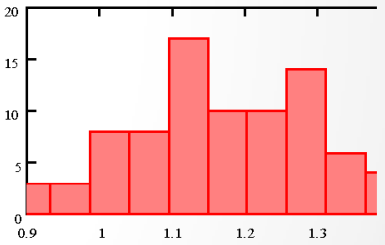


Рисунок 3.17 – Гістограма значень FAR для параметрів $[vx_t, vy_t]$



Гістограма значень FRR для параметрів $[ax_t, ay_t, az_t]$



Гістограма значень FAR для параметрів $[ax_t, ay_t, az_t]$

Результати проведених досліджень

Інформативні ознаки	False Reject Rate (помилкова відмова «своєму»), %			False Accept Rate (помилковий пропуск «чужого»), %		
	Максимальне значення	Мінімальне значення	Середнє значення	Максимальне значення	Мінімальне значення	Середнє значення
$[x_t, y_t]$	28.588	19.007	23.94	38.393	22.678	29.8
$[p_t, f_{a_t}]$	20.106	11.726	16	23.398	14.377	18.38
$[x_t, y_t, p_t, f_{a_t}]$	11.281	3.497	7.28	10.958	6.505	8.4
$[vx_t, vy_t]$	41.289	24.524	32.72	50.672	34.154	41.06
$[p_t, f_{a_t}, vx_t, vy_t]$	15.301	8.796	10.04	19.142	10.64	13.941
$[ax_t, ay_t, az_t]$	1.163	0.792	0.96	1.417	0.879	1.179
$[p_t, f_{a_t}, ax_t, ay_t, az_t]$	0.05	0.031	0.04	0.099	0.064	0.08

Інформативні ознаки	False Reject Rate (помилкова відмова «своєму»), %		False Accept Rate (помилковий пропуск «чужого»), %	
	Користувач 19 / максимальне значення	Користувач 75 / мінімальне значення	Користувач 19 / максимальне значення	Користувач 75 / мінімальне значення
$[x_t, y_t]$	28.016 / 28.588	19.216 / 19.007	37.664 / 38.393	23.426 / 22.678
$[p_t, f_{a_t}]$	19.623 / 20.106	12.101 / 11.726	22.719 / 23.398	14.895 / 14.377
$[x_t, y_t, p_t, f_{a_t}]$	11.100 / 11.281	3.647 / 3.497	10.673 / 10.958	6.700 / 6.505
$[vx_t, vy_t]$	41.165 / 41.289	25.064 / 24.524	50.013 / 50.672	34.530 / 34.154
$[p_t, f_{a_t}, vx_t, vy_t]$	14.551 / 15.301	9.051 / 8.796	18.357 / 19.142	11.140 / 10.64
$[ax_t, ay_t, az_t]$	1.144 / 1.163	0.800 / 0.792	1.350 / 1.417	0.915 / 0.879
$[p_t, f_{a_t}, ax_t, ay_t, az_t]$	0.048 / 0.05	0.032 / 0.031	0.096 / 0.099	0.064 / 0.064

Висновки

1. Виконано огляд основних методів біометричної аутентифікації, що використовуються або є перспективними для використання в мобільних пристроях. Це розпізнавання за динамічним графічним паролем, розпізнавання за тривимірним динамічним підписом, розпізнавання за відбитком пальця, розпізнавання за геометрією обличчя. Використання динамічних біометричних характеристик має потенціал для застосування як додаткова міра, що підвищує загальний рівень безпеки при аутентифікації.

2. У роботі проаналізовано інформативні ознаки цифрового рукописного підпису. Можна виділити три основних класи: динамічні параметри руху кінчика пальця екраном, параметри взаємодії з екраном (тиск та розмір «плями» від пальця) та параметри, що характеризують положення смартфону в руці користувача та коливання смартфону в просторі в процесі введення цифрового рукописного підпису.

3. За даним датасету «The MOBISIG signature database» інтегральна точність класифікації за динамічними параметрами руху кінчика пальця екраном становить 24 % (FRR) та 30 % (FAR). Таким чином, нестабільність динамічних параметрів обумовлює неможливість побудови ідентифікаційних систем, що враховують лише ці параметри.

Висновки

4. За даним датасету «The MOBISIG signature database» інтегральна точність класифікації за параметрами взаємодії з екраном (тиск та розмір «плями» від пальця) становить не менше 16 % (FRR) та 18.4 % (FAR). Аналіз робіт, що присвячені вивченню проблеми мобільного клавіатурного почерку, підтверджує отриманий результат – тиск та розмір «плями» від пальця не відносяться до найінформативніших параметрів мобільного клавіатурного почерку.

6. За даними датасету «The MOBISIG signature database» найінформативнішими параметрами цифрового рукописного підпису є прискорення планшету в тривимірному просторі, що характеризують положення планшету в руці користувача в процесі вводу парольної фрази. Використання лише цих трьох параметрів дає інтегральну точність ідентифікації 0.96 % (FRR) та 1.2 % (FAR).

7. Найвищу точність ідентифікації забезпечує комбінація тиску та розміру «плями» від пальця та прискорення планшету в тривимірному просторі в процесі вводу парольної фрази – 0.04 % (FRR) та 0.08 % (FAR). Це дуже високий результат, що не поступається точності ідентифікації за відбитком пальця, але, при цьому, цифровий рукописний підпис більш захищений від підробок.

8. Оскільки розраховані показники точності ідентифікації за цифровим рукописним підписом отримані для планшету з частотою дискретизації 60 Гц можна стверджувати про потенційну ще вищу точність, оскільки сучасні смартфони та планшети мають частоту опитування екрану до 480 Гц.

Номер документу	Позначення	Найменування	Прим.
		Текстові документи	
1		Пояснювальна записка	90 с.
		Графічний матеріал	
2-4		Дослідження ефективності	3хА4 ел.ф.
		ідентифікації особистості	
		за графічним паролем	
5		Мобільний клавіатурний почерк	А4 ел.ф.
		та цифровий рукописний підпис	
6		The MOBISIG signature database	А4 ел.ф.
7		Схема експерименту у Orange	А4 ел.ф.
8		Результати проведених досліджень	А4 ел.ф.
9-10		Висновки	2хА4 ел.ф.

Из	Лист	№ докум.	Підпис	Дата				
Розроб.		Пономаренко			*Дослідження ефективності ідентифікації особи за графічним паролем*	Літера	Лист	Листів
Перев.		Горелов				Д		
						ХНУРЕ Кафедра КРіСТЗІ		
Н.контр.		Милютченко			Відомість кваліфікаційної роботи магістра			
Затв.		Антіпов						