УДК 004.056.523:004.931
DOI: https://doi.org/10.30837/IYF.IRTTPI.2024.407

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ІДЕНТИФІКАЦІЇ ОСОБИ ЗА ГРАФІЧНИМ ПАРОЛЕМ

Горелов Д.Ю., Терновий Я.І.
Науковий керівник – к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
студентський науковий гурток «Біометричні технології контролю доступу»
каф. КРіСТЗІ, м. Харків, Україна
e-mail: yaroslav.ternovyi@nure.ua

Using the database "The MOBISIG signature database" and the Orange software, a study of the impact on the accuracy of identification by a signature of various informative features: dynamic parameters of the movement of the fingertip on the screen, parameters of interaction with the screen (pressure and size of the "spot" from the finger) and parameters characterizing the position of the smartphone in the user's hand and the vibrations of the smartphone in space during the process of entering a signature.

У найближчі кілька років забуті або викрадені паролі вважатимуться проблемою минулого, адже все більше як користувачів, так і організацій використовують біометричні дані для аутентифікації. За прогнозами аналітиків, до 2025 року 75 % великих компаній не використовуватимуть паролі.

Аналогічна ситуація спостерігається і на ринку мобільних пристроїв, де відбиток пальця та розпізнавання обличчя витіснили класичні PIN або графічний пароль при розблокуванні смартфону.

Однак ступінь довіри до цих методів біометричної аутентифікації – невисока, оскільки часто в Інтернет можна зустріти статті про успішну атаку на той чи інший смартфон. Один із способів, що не є біометричним у строгому сенсі, – так званий відбиток девайсу. У цьому випадку використовують такі характеристики, як модель гаджета, операційна система, завантажені користувачем програми, параметри Wi-Fi-мереж, до яких часто підключається користувач, тощо. В результаті система створює свого роду профіль і гаджета, і звичок конкретного користувача.

Однак цьому способу ідентифікації заважає те, що Apple і Google обмежують набір параметрів, які можна дізнатися про пристрій віддалено. Це робиться з метою захисту особистих даних користувачів.

Тому останнім часом фахівці в галузі інформаційної безпеки приділяють увагу поведінковим біометричним характеристикам власників смартфонів, а саме клавіатурному почерку, динамічному графічному паролю цифровому рукописному підпису.

Нині можна виділити 8 основних біометричних характеристик люди-

ни, що можна використовувати в мобільних систему аутентифікації.

З цих восьми характеристик п'ять, а саме обличчя, голос, відбиток пальця, райдужна оболонка та геометрія долоні крім високої схильності до спуфінг атак (атак підробки) у разі використання дешевих сканерів (а саме такі і встановлюються навіть у влагманські смартфони з метою зменшити кінцеву вартість гаджета) мають ще один суттєвий недолік: висока залежність точності роботи системи аутентифікації від зовнішніх умов.

Цей факт додає актуальності поведінковим біометричним характеристикам власників смартфонів, оскільки вони менш схильні до впливу умов зовнішніх умов.

Наразі опубліковано велику кількість робіт, присвячених мобільному клавіатурному почерку. Тут інформативними ознаками виступають тривалість утримання клавіш і тривалість паузи між відпусканням першої клавіші та натисканням другої клавіші на віртуальній клавіатурі, тиск на екран в момент торкання пальцями екрану та розмір «плями від пальця» в момент торкання пальцями екрану.

Альтернативою мобільному клавіатурному почерку є цифровий рукописний підпис, який також містить і собі інформацію про динаміку введення парольної фрази (підпису) та особливості взаємодії користувача зі смартфоном в процесі введення парольної фрази (підпису).

В якості дослідного датасету було обрано «The MOBISIG signature database» [1-2], що містить параметри вводу унікальних 83 парольних фраз, що входять до перших 100 найпоширеніших угорських імен. Кожна сигнатура 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. Також слід зазначити, що за умовами експерименту потенційним зловмисникам були відомі і сам підпис і відео з динамікою введення підпису верифікованим користувачем.

В якості програмного засобу для проведення досліджень було використано інструмент інтелектуального аналізу даних Orange. В якості алгоритму класифікації використовувався метод випадкових лісів [3]. В якості інструменту оцінки точності класифікації користувачів використовувалась крос-валідація за 10 блоками [4].

На рис. 1 наведено узагальнені результати досліджень.

Перша таблиця містить результати оцінки точності ідентифікації користувачів в залежності від використаних інформативних ознак цифрового рукописного підпису. Як видно жоден з параметрів, що характеризує динаміку відтворення рукописного підпису не забезпечує прийнятної

точності. Найменша точність – 32.7 % (327 випадки на 1000 спроб) для FRR та 41.06 % (410 випадків на 1000 спроб) для FAR – відповідає швидкості переміщення кінчика пальця за координатами x та y.

Найвища точність – 16 % (160 випадки на 1000 спроб) для FRR та 18.3 % (183 випадки на 1000 спроб) для FAR – відповідає тиску і «площі плями» від кінчика пальця в процесі вводу парольної фрази.

Найунікальнішими параметрами введення цифрового рукописного підпису є прискорення планшету в тривимірному просторі, що характеризують положення планшету в руці користувача в процесі вводу парольної фрази – 0.96 % (10 випадків на 1000 спроб) для FRR та 1.2 % (12 випадків на 1000 спроб) для FAR.

Найвищу точність ідентифікації забезпечує комбінація тиску і «площі плями» від кінчика пальця та прискорення планшету в тривимірному просторі в процесі вводу парольної фрази – 0.04 % (4 випадки на 10000 спроб) для FRR та 0.08 % (8 випадків на 10000 спроб) для FAR.

Це дуже добрий результат, що не поступається точності ідентифікації за відбитком пальця.

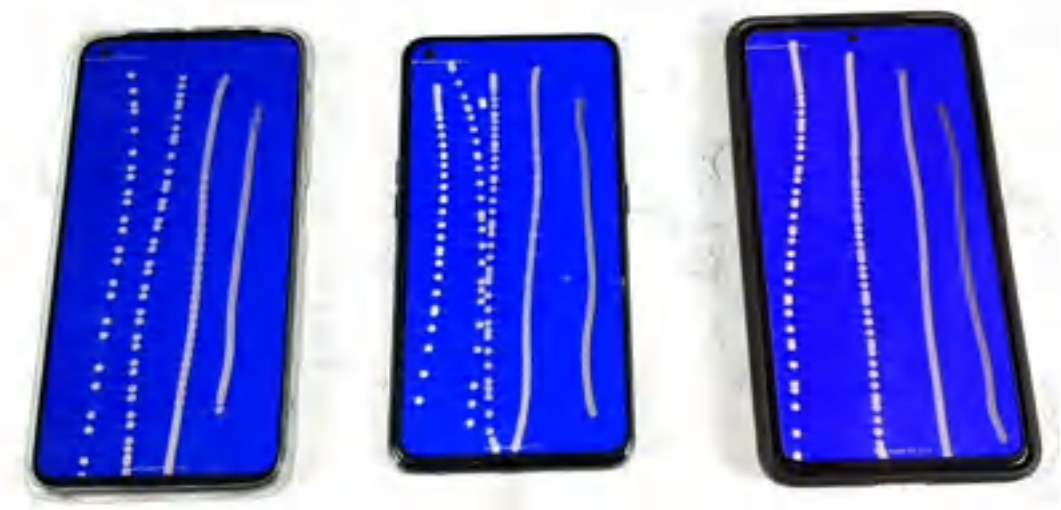
Інформативні ознаки	False Reject Rate (помилкова відмова «своєму»), %			False Accept Rate (помилковий пропуск «чужого»), %		
	Максимальне значення	Мінімальне значення	Середнє значення	Максимальне значення	Мінімальне значення	Середнє значення
$[x_t, y_t]$	28.588	19.007	23.94	38.393	22.678	29.8
$[p_t, f_{a_t}]$	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	37.668 / 38.393	23.426 / 22.678
$[p_t, f_{a_t}]$	19.623 / 20.106	12.103 / 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	25.069 / 24.524	50.013 / 50.672	34.530 / 34.154
$[p_t, f_{a_t}, vx_t, vy_t]$	15.551 / 15.301	9.051 / 8.796	18.357 / 19.142	11.140 / 10.64
$[ax_t, ay_t, az_t]$	1.194 / 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

Рисунок 1

Також варто відзначити, що датасет було отримано у 2015-2016 роках на планшеті з частотою опитування екрану 60 Гц. Це призводить до того, що у випадку коротких паролів довжина дослідних сигнатур становить 50-60 відліків. Сучасні смартфони та планшети мають частоту опитування ек-

рану 480 Гц, що значно б підвищило точність ідентифікації (рис. 2).



60 Гц 120 Гц 180 Гц

Рисунок 2 – Ілюстрація різних частот опитування екрану смартфону

Для підтвердження цієї тези в другій таблиці наведено значення FRR та FAR для двох користувачів – 19 (найкоротші інформативні послідовності) та 75 (найдовші інформативні послідовності). Як можна бачити, значення FRR та FAR для користувача 19 близькі до максимальних серед усіх користувачів. В той же час значення FRR та FAR для користувача 75, навпаки, близькі до мінімальних серед усіх користувачів.

Список використаних джерел:

1. The MOBISIG on-line signature database. URL: https://www.ms.sapientia.ro/~manyi/mobisig.html (дата звернення: 20.12.2023).

2. Margit ANTAL, László Zsolt SZABÓ and Tunde TORDAI (2018). On-line Signature Verification on MOBISIG Finger Drawn Signature Corpus, 2018

3. Hastie T., Tibshirani R., Friedman J. Random Forests // The Elements of Statistical Learning: Data Mining, Inference, and Prediction. 2nd ed. Springer-Verlag, 2009. Chapter 15. 746 p.

4. Cross-validation: evaluating estimator performance. URL: https://scikit-learn.org/stable/modules/cross_validation.html (дата звернення: 20.12.2023).

5. Дослідження інформативних параметрів диграфів клавіатурного почерку для задач ідентифікації користувачів комп’ютерних мереж / Д.Ю. Горелов, О.О. Іванова, О.В. Кокорін, Д.В. Маслій, О.В. Литвиненко // Радіотехніка: Всеукр. Міжвід. Наук.-техн. Зб. – 2020. – вип. 201. – с. 194 – 200.

6. Дослідження можливостей використання клавіатурного почерку для задач ідентифікації студентів у системах дистанційної освіти / Д.Ю. Горелов, О.О. Іванова, О.В Литвиненко, А.А. Довбня, Д.О. Мінін // Радіотехніка: Всеукр. Міжвід. Наук.-техн. Зб. – 2021. – вип. 207. – с. 139 – 148.