УДК 517.5.52

С. І. Кротюк [1]
Н. В. Сачанюк-Кавецька [2]

ВИКОРИСТАННЯ ПОЛЯРНИХ КООРДИНАТ ДЛЯ СТВОРЕННЯ ГРАФІЧНОГО ПАРОЛЮ

[1] Комунальний заклад «Тиврівський науковий ліцей» Вінницької обласної Ради
[2] Вінницький національний технічний університет

Анотація

Під час розв'язання тієї чи іншої задачі можна застосовувати різні координатні системи, обираючи з них ту, розв'язання в якій здійснюється простіше й доречніше. Системи, які відображають радіальну симетрію, можуть забезпечити природні налаштування для полярної системи координат, де центральна точка виступає в ролі полюса. На сучасному етапі розвитку комп'ютерної техніки інформація є важливим ресурсом, а система ідентифікації - один із ключових моментів захисту від несанкціонованого доступу. Дана робота присвячена можливості використання полярних координат для створення графічного паролю з використанням відбитків пальців.

Ключові слова: полярна система, полярний радіус, біометрика, відбитки пальців.

Abstract

When solving this or that problem, you can use different coordinate systems, choosing from them the one in which the solution is easier and more appropriate. Systems that display radial symmetry can provide natural settings for a polar coordinate system, where the central point acts as the pole. At the current stage of computer technology development, information is an important resource, and the identification system is one of the key points of protection against unauthorized access. This work is devoted to the possibility of using polar coordinates to create a graphic password using fingerprints.

Key words: polar system, polar radius, biometrics, fingerprints.

Вступ

Інформація та інформаційні системи, мережі, в яких вона функціонує, є важливими ресурсами. Поширення інформаційних та комунікаційних систем надає все нові можливості для несанкціонованого доступу до інформаційних ресурсів, а тенденція до переходу на розподілені обчислювальні системи зменшує можливості спеціалістів централізовано контролювати інформаційні системи та мережі. Тому актуальним є питання захисту інформації від несанкціонованих управлінських дій і доступу сторонніх осіб або програм до комп'ютерних даних [1].

Під час розв'язання тієї чи іншої математичної, фізичної, технічної, медичної задачі можна застосовувати різні координатні системи, обираючи з них ту, розв'язання в якій здійснюється простіше й доречніше. Системи, які відображають радіальну симетрію, можуть забезпечити природні налаштування для полярної системи координат, де центральна точка виступає в ролі полюса. Також мають потенціал для використання полярної системи координат системи з радіальною силою [2].

Сьогодні у більшості громадян є пароль. Вони використовуються для ідентифікації користувачів у різних системах та мережах. Паролі використовуються як звичайними користувачами, так і адміністраторами з особливими правами доступу. Надійність пароля кожної організації чи установи визначається політикою інформаційної безпеки, але ця політика не рекомендує користувачам методику збереження особистих паролів у своїй пам'яті. Більшість людей віддає перевагу графічному паролю, що пов'язано із особливістю людського сприйняття. Мозку людини набагато простіше запам'ятати малюнок або рух руки, ніж набір цифр.

До переваг графічних паролів можна віднести:

- Швидкість і зручність: графічні ключі можна вводити швидко і легко, що робить їх зручним способом розблокування пристроїв.

- Безпека: графічні ключі можуть бути безпечними, якщо їх вибрати правильно. Складний візерунок з мінімум 4 точок важко вгадати або зламати.
- Немає необхідності пам'ятати пароль: на відміну від паролів, графічні ключі не потрібно запам'ятовувати, що може бути зручніше для деяких людей.

Однак, щоб бути досить надійним такий пароль не повинен містити тільки прямі лінії, графічна комбінація має бути довгою, не варто використовувати легко вгадувані візерунки. Таким чином, актуальною є розробка методів графічної ідентифікації з використанням систем, які відображають радіальну симетрію та особливі характеристики, притаманні конкретній особі.

Результати дослідження

Існує три найпоширеніші види ідентифікації: парольна, апаратна та біометрична. При парольній ідентифікації кожен зареєстрований користувач будь-якої системи одержує набір персональних реквізитів, які він повторює при кожній спробі входу в систему. Перевага такого підходу – простота реалізації та використання, мінімізація витрат. Головним недоліком даного виду ідентифікації є величезна залежність надійності від користувачів. При апаратній ідентифікації визначення особистості користувача ґрунтується на якомусь «ключі», що перебуває в його ексклюзивному користуванні. Головною перевагою застосування апаратної ідентифікації є досить висока надійність. Слід відмітити, що найбільш серйозною небезпекою такої ідентифікації є можливість крадіжки зловмисниками токенів або карт (проксіміті, смарт, магнітних і т. п.) у зареєстрованих користувачів, плюс їх висока ціна. Останнім часом досягнуто успіхів у розробці біометричних методів, що базуються на ідентифікації людини за унікальними, властивими тільки їй біологічними ознаками [3]. Сьогодні експлуатується вже більше десятка різних біометричних ознак. Головною перевагою біометричних технологій є найвища надійність (див. табл. 1). Можливими проблемами біометричних систем доступу є імовірність перехоплення інформації під час її передачі від сканера до бази даних, а також несанкціонований доступ до масиву еталонних записів. Зрозуміло, що значно вищу ефективність дає застосування ідентифікації суб'єкта заснованої на різних біометричних методах.

Таблиця 1

Порівняльні характеристики біометричних систем

№	Модель	Біометричний метод	Ймовірність несанкціонованого допуску	Ймовірність помилкового допуску
1	Eyedentify ICAM	Сітківка ока	0,0001	0,4
2	Iriscan	Райдужка ока	0,0008	0,0007
3	FingerScan	Відбиток пальця	0,0001	1,0
4	BioMet	Геометрія руки	0,1	0,1
5	Vocord (2D)	Геометрія обличчя	0,01	0,2
6	Hitachi VeinID	Вени руки	0,0008	0,01

Як видно з таблиці 1, досить малу ймовірність несанкціонованого допуску дає відбиток пальця. Тому доцільно формувати графічний пароль, використовуючи відбитки пальців. Більшість малюнків відбитків утворюють рисунок, схожий на концентричні кола певного радіуса. Тому їх зображення та аналітичне задання легко реалізувати в полярній системі координат. Полярна система координат – це двовимірна система координат, в якій кожна точка на площині визначається двома числами – кутом та відстанню. Полярна система координат зазвичай задається променем, який називають нульовим або полярною віссю. Точка, з якої виходить цей промінь називається початком координат або полюсом. Наприклад, для визначення положення точки M у полярній системі координат вказують відстань від полюса до цієї точки (ρ, радіальна координата) і напрямок (φ, кутова координата), у якому вона знаходиться Розбиваємо область від 0 до 2π на п'ять частин (відповідно до кількості пальців руки). Малюнки кожного пальця правої руки для шульги та лівої руки в іншому випадку також розбиваємо на п'ять частин (рівнів) і для кожного рівня визначаємо полярний радіус. В полярній системі координат графічний пароль створюємо таким чином.

Будуємо п’ять секторів із кроком 72^0 та полярним радіусом, що відповідає обраному рівню малюнку відбитку обраного пальця руки. Рівні пальців та самі пальці можна міксувати довільним чином. Для кращого ефекту можна додати заливку побудованих секторів (кольорову чи різноманітні способи штриховки). Можливий варіант такого графічного пароля наведено на рис. 1

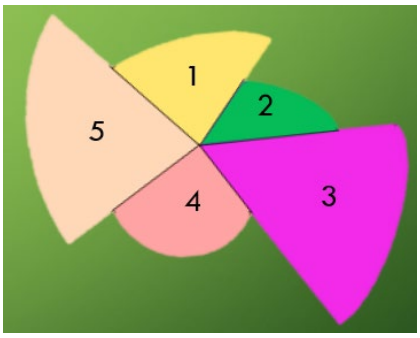

Рисунок 1. Можливий варіант графічного пароля з використанням полярної системи координат та відбитків пальців

Висновки

При використанні графічного пароля користувач формує сучасний погляд на проблему інформаційної безпеки, а людський фактор в тому, як його запам'ятовувати і використовувати, зводиться до мінімуму. Новий метод аутентифікації повинен, перш за все, сприяти підвищенню зручності користувачів, що використовують комп'ютер.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кошева Н. А. Ідентифікація користувачів інформаційно-комп’ютерних систем: аналіз і прогнозування підходів / Кошева Н. А., Мазниченко Н. І. // Інфокомунікаційні системи. Серія Системи обробки інформації. – 2013. – Вип. 6 (113). – С. 215 – 223
2. Libre Texts mathematics (2024). Режим доступу: https://math.libretexts.org/Bookshelves/Calculus/Calculus_(Guichard)/10%3A_Polar_Coordinates_and_Parametric_Equations/10.01%3A_Polar_Coordinates (дата звернення 01.04.2024).
3. Чередниченко В. Б. Біометричні методи у системах захисту інформації / Чередниченко В. Б., Чередниченко К. Е. // Захист інформації в інформаційно –телекомунікаційних системах. Серія Системи обробки інформації. – 2012. – Вип. 4 (102). – Т.1. – С. 145 – 148.

Кротюк Сніжана Іллівна**,** комунальний заклад «Тиврівський науковий ліцей» Вінницької обласної Ради, учениця 11 класу, snizhana.krotiuk@gmail.com
Сачанюк-Кавецька Наталія Василівна **-** к. .т. н., доцент, Вінницький національний технічний університет, кафедра вищої математики, skn1901@gmail.com
Науковий керівник: ***Сачанюк-Кавецька Наталія Василівна*** **-** к. .т. н., доцент, Вінницький національний технічний університет, кафедра вищої математики, skn1901@gmail.com

Krotiuk Snizhana I., communal institution "Tyvriv Scientific Lyceum" of the Vinnytsia Regional Council, 11th grade student, snizhana.krotiuk@gmail.com
Sachaniuk-Kavets`ka Natalia V. Candidate of Technical Sciences, Associate Professor, Department of Higher Mathematics, Vinnytsia National Technical University, skn1901@gmail.com
Supervisor: ***Sachaniuk-Kavets`ka Natalia V.*** - Candidate of Technical Sciences, Associate Professor, Department of Higher Mathematics, Vinnytsia National Technical University, skn1901@gmail.com