

ОГЛЯД ПІДХОДІВ К РОЗПІЗНАВАННЮ БІОМЕТРИЧНОГО ПОРТРЕТА КОРИСТУВАЧА ЗА КЛАВІАТУРНИМ ПОЧЕРКОМ

В роботі проаналізовані найбільш відомі роботи й алгоритми розпізнавання біометричного портрета користувача за клавіатурним почерком, їх переваги й недоліки. Показано, що жоден з підходів не забезпечує достовірне розпізнавання користувача.

Завдання ідентифікації людини є критичною у багатьох повсякденних ситуаціях. Все частіше доводиться зіштовхуватися з випадками шахрайства осіб, що видають себе за інші при спробі входу в готельні номери, знятті готівки через банківські термінали, одержання доступу в мережі ЕОМ або здійсненні інтерактивної покупки.

Традиційні методи ідентифікації особи, в основі яких перебувають різні ідентифікаційні карти, ключі або унікальні дані, такі як, наприклад, пароль не є надійними на тому рівні, який потрібний зараз. Наступним кроком у підвищенні надійності ідентифікаторів стали спроби використання біометричних технологій для систем розпізнавання особи.

Важливе місце серед біометричних продуктів займають прилади і програми, побудовані на аналізі динамічних образів особистості (аутентифікація по динаміці рукописного підпису, по клавіатурному почерку, по роботі з комп'ютерною мишею і т.д.)

Унікальні властивості клавіатурного почерку можна виявити як по набору ключової фрази, так і «вільного» тексту. Ідентифікація по набору ключової фрази широко досліджена [1-2]. Вірогідність аутентифікації при наборі ключової фрази становить 99% при використанні нейромережевого підходу.

Розробкою систем аутентифікації користувачів по клавіатурному почерку (по «вільному» тексту) займаються порівняно недавно. Автором однієї з перших робіт є Гейнс [3], який в 1980 р. провів ряд експериментів із сімома секретарями. Він їх запросив набрати одні й ті ж самі два параграфи два рази з перервою в 4 місяці. Як результат була зібрана й проаналізована обмежена кількість біграм. З них обрані були лише ті, частота появи яких

перевершувала 10. Порівняння зразків відбувалося виходячи із припущення, що час затримання й відхилення всіх біграм повинні бути повністю еквівалентні.

Авторами іншої роботи є Леггет, Умпресс і Вільямс [4]. Вони проводили експеримент із 17 програмістами. Вони використовували виміряні інтервали між натисканням клавіш, відомі як диграфи. Перша множина складалася з 1400 символів і використовувалась на стадії навчання. Друга множина складалася з 300 символів і використовувалась для перевірки. У своїй доповіді Леггет указав коефіцієнт вірогідності аутентифікації 89,5%. У своїх експериментах автори припустили можливе відхилення середнього часу затримання біграм рівної 0.5, користувач уважався впізнаним, якщо 60% і більше тимчасових затримок збігалися із припустимим відхиленням зі зразком.

Також деякі роботи в цій області були проведені Гарсіом, Янгом і Хемоном. У підході була використана матриця співзмін векторів зв'язаних затримок, як величина (параметр) в якій містяться дані про індивідуальний почерк. Потім використалася функція відстані Махаланобіса, щоб визначити подібність між почерком, що ідентифікується, і профілем користувача. На відміну від інших, Янг і Хаммон використали Евклідову відстань між двома векторами для порівняння кількості атрибутів.

Відомі роботи Рика Джойса й Гупта Гопала [2]. Метод заснований на використанні інформації про тимчасові затримки між натисканнями клавіш, отриманих під час уведення логіна в модифікованій процедурі ідентифікації. Цій системі необхідно, щоб кожний новий користувач вісім разів вводив логін і пароль. За час верифікації користувач надає зразок випробуваного почерку T , що рівняється з M (зразок почерку), щоб визначити величину різниці між двома профілями. Дані $M = \{m_1, m_2, m_3 \dots m_n\}$ і $T = \{t_1, t_2, t_3 \dots t_n\}$, де n -загальна кількість затримок у почерку, функція що верифікується розраховує величину різниці як норму $L1$. Ідентифікація вважається позитивною, якщо ця різниця не перевершує певного порога змінюваності почерку. Середня й стандартна девіація норм $= |M - S_i|$, де S_i - один з восьми пробних почерків, використовується, щоб визначити поріг прийнятної різниці векторів між даними T і M . Результати вірогідності системи не приводяться.

Відома робота Расторгуєва С.П. У своїй монографії автор процедуру ідентифікації розділив на два види. Перший вид це парольна ідентифікація, де користувач по парольній фразі проходить процедуру аутентифікації. Другий вид – ідентифікація користувачів по набору випадкової фрази. А також виділив два режими процедури ідентифікації: процедуру настроювання системи й процедуру аутентифікації.

При ідентифікації користувачів по наборі вільного тексту в режимі настроювання системи ідентифікації клавіатуру подумки розділили на чотири частини. При роботі користувача за клавіатурою обчислювалися тимчасові інтервали між цими чотирма частинами не залежно від того яка клавіша була натиснута в цих частинах. І аналогічно парольної ідентифікації значення заносилися в еталон. У режимі ідентифікації поточні значення порівнювалися з еталонними, і система приймала рішення. Одне з допущень було те, що розподіл тимчасових характеристик користувачів представлялися нормальним гауссівським законом. А також у роботі були представлені алгоритми виключення грубих помилок, настроювання системи й ідентифікації.

Більшість розглянутих робіт базується на основі геометричних методів розпізнавання, використовуючи різноманітну міру близькості між зразком почерку та його еталоном (Евклідова, Махаланобіса і т.д.). Гранична знайдена вірогідності аутентифікації таких систем становить 89,5%. У проаналізованих методах були виявлені суттєві недоліки в плані надійного розпізнавання користувача. Це обумовлює необхідність подальшого вдосконалення досліджень у цієї галузі.

Перелік літератури

1. Jarmo Plonen Keystroke dynamics. Lappeenranta University of Technology, Skinnarilankatu 34, 53850 Lappeenranta, Finland.
2. Rick Joyce and Gopal Gupta. Identity authentication based on keystroke latencies. Communications of the ACM, 33(2): 168 - 176, February 1990.
3. R. Gaines, W. Lisowski, S. Press, and N. Shapiro, "Authentication by Keystroke Timing: Some Preliminary Results," Rand Report R-256-NSF, Rand Corporation, Santa Monica, C A, 1980

4. J. Leggett and Williams, "Verifying identity via keystroke characteristics"
International Journal of Man-Machine Studies, 28:67-76,1988.