

Дана корисна модель відноситься до способів розпізнавання образів [G06K9/00], а саме біометричної (тобто базованої на параметрах людського тіла) інформації у вигляді зображень відбитків пальців, контурів кінцівок, обличчя та іншого і призначений для створення паролів.

Під біометричною характеристикою розуміється людська фізіологічна або поведінкова характеристика, яку можна виміряти [3].

Під паролем розуміється секретна комбінація цифр, знаків, що служить для захисту інформації чи іншого від несанкціонованого доступу.

Використання паролів є загально прийнятим способом забезпечення захисту інформаційних та інших ресурсів: в комп'ютерних мережах, банкоматах, телефонних картках, та ін. Всі ці системи як правило вимагають знання користувачем паролю, вибраного особисто чи призначеного.

Призначені паролі, як правило, важкі для запам'ятовування, в той час як записування (чи зберігання якимось іншим чином) паролів зводить на унівець їх основну функцію: обмеження доступу авторизованими користувачами.

Вибрані особисто паролі, як правило, створюються за відомим користувачу алгоритмом (за днем народження, номером телефону, та ін.), що робить їх вразливими до викриття шляхом підбору або розвідувальних дій по відношенню до власника паролю або його оточення.

Загально відомо, що надійним способом захисту та ідентифікації повинен бути такий, що унікальне ідентифікує користувача та який неможливо загубити чи забути. Цим вимогам відповідає біометрична ідентифікація, використання якої базується на наступному [1, 2, 3]:

- сканування зображення, наприклад відбитку пальця,
- розпізнавання та кодування всіх чи основних його параметрів, наприклад характерних точок капілярних ліній відбитку пальця,

- збереження образу зображення (еталону) в базі даних чи енергонезалежній пам'яті,
- порівняння еталону з зображенням що вводиться при ідентифікації.

В той же час, біометрична ідентифікація є досить дорогою при впровадженні та має ряд суттєвих недоліків [7]:

1. Необхідно створювати та надійно захищати засоби передачі, зберігання (напр. шифровані бази даних) та розпізнавання зображень (наприклад сканер, приєднаний до бази даних), що накладає обмеження на область розповсюдження системи біометричного захисту, наприклад, тільки певним підприємством,

2. Існування досить високих вимог до техніки та програмного забезпечення з метою мінімізації випадків недопущення „свого“ та пропуску „чужого“. Тобто, апаратне забезпечення повинно видавати якісне зображення, наприклад, відбитків пальців, а програмне забезпечення повинно правильно їх розпізнавати за характерними точками, рельєфом всієї поверхні пальця або за комбінацією цих способів.

3. Існує можливість підробки біометричних характеристик (наприклад відбитку пальця) навіть при застосуванні датчиків живого тіла (що вимірюють тиск крові, температуру, пульс, ін.). В зв'язку з цим виникає необхідність додаткового захисту біометричних систем, в основному за допомогою паролів.

4. Пошкодження біометричної характеристики (наприклад подряпина на пальці) можуть приводити до відмови у доступі легітимному користувачеві.

Усунення вищенаведених недоліків, як по відношенню до використання паролів, так і по відношенню до біометричної ідентифікації, проводиться шляхом комбінації цих способів. Наразі використовується декілька шляхів такої комбінації:

- біометричний захист бази паролів, тобто коли пароль стає доступним після біометричної ідентифікації користувачем. Цей спосіб по суті створює лише невелику зручність для користувача, що не повинен запам'ятовувати багатьох паролів, проте не усуває недоліків, що має біометрична ідентифікація.

- створення паролів за біометричними характеристиками, тобто, коли, наприклад при скануванні відбитку пальця, за його характерними ознаками і проводиться створення паролю.

Переваги створення паролів за біометричними характеристиками полягає в:

- простоті, гнучкості та доступності впровадження за рахунок того, що не треба створювати та підтримувати спеціальні бази для обробки та зберігання образів зображень,

- простоті у використанні за рахунок створення надійного паролю на базі унікальних біометричних характеристик.

Слід зазначити, однак, що переважна більшість паролів, що генеруються цим способом є одноразовими, призначеними для рішення окремих питань ідентифікації та авторизації.

Наразі, автору відомий лише один спосіб генерації постійного паролю, що є близьким до даного винаходу - винахід згідно патенту США 7006673 „Спосіб генерації хеш-рядку” [4].⁽¹⁾ Хеш-рядок, є коротким числом, отриманим шляхом перетворення великого масиву даних за допомогою хеш-функції таким чином, щоб зберегти максимальну відповідність хеш-рядку масиву даних при мінімальному значенні цього хеш-рядку.)

Суттєві ознаки даного способу полягають в створенні паролів за характерними рисами відбитку пальця та координатами цих характерних рис. наступним чином:

- сканування відбитку пальця на пластині з встановленою системою координат. При цьому центральна точка відбитку (термін використовується в дактилоскопії) співпадає з перетином координатних ліній;

- розпізнавання характерних рис відбитку пальця, як це прийнято в дактилоскопії,

- кодування ключових характерних рис за певним алгоритмом, напр. „петля” - 12,

- створення хеш-рядків за кількістю, та розміщенням характерних рис в секторах,

- генерація пароля за хеш-рядками.

Важкою перевагою даного способу є наступні:

- необхідність забезпечення досить точного встановлення пальця на координатну сітку для того щоб центральна точка відбитку з центром відліку координат.

- можливість використання тільки характерних, а не всіх рис відбитку пальця, що зменшує рівень безпеки при генерації паролю шляхом хешування та підвищує ризик генерації однакових паролів при масовому використанні способу.⁽²⁾ ⁽²⁾ Хешування передбачає ймовірність існування однакових значень хеш-рядків для різних масивів

даних.)

Даний спосіб також є складним для впровадження, так як, наскільки відомо автору, з дати реєстрації патенту на „Спосіб генерації хеш-ряду” в 2001р., на ринку не пропонуються продукти на його основі.

Усунення вказаної вади досягається тим, що автором пропонується наступне:

- використання не статичної, а динамічної точки відліку координат, тобто немає необхідності точного розміщення біометричної характеристики на сканері чи забезпечення певного допуску при скануванні; користувач відліку встановлює самостійно, або вона розпізнається автоматично за встановленими параметрами. Це дозволить забезпечити максимальну точність сканування.

- розпізнавання та кодування не тільки характерних, але всіх рис біометричної характеристики об'єкта, що дозволить створювати абсолютно унікальний код.

Схема реалізації способу створення паролю за біометричними характеристиками зображена на блок схемі, Фіг.1. Суть даного способу полягає в тому, що після сканування біометричної характеристики (блок 1), наприклад відбитку пальця, та вибору користувачем певної системи координат, області кодування та таблиці кодування (блок 2), проводиться вирахування координат точок, що утворюють зображення біометричної характеристики та кодування отриманих координат в пароль (блок 3). Отриманий пароль перевіряється (блок 4), і при неправильному значенні процедура починається спочатку.

Під системою координат розуміється Декартова, кутова, або інша система координат з точкою відліку та шкалою що призначаються користувачем. В випадку з відбитками пальців точкою відліку системи координат може бути центральна точка відбитку А або будь яка характерна для користувача точка, наприклад, точка В (див. Фіг.2, 3).

Під областю кодування розуміється область певної графічної форми (наприклад прямокутник) та розміру (наприклад квадрат зі стороною 10мм), в якій відбувається вирахування координат точок, що утворюють зображення біометричної характеристики (див. Фіг.4).

Під таблицею кодування розуміється таблиця відповідності координат точок, що формують зображення біометричної характеристики певним цифрам та знакам. Наприклад, координати точки А (Фіг.3) в Декартові системі координат (0,0) можуть відповідати символу „а” (буква а англійського алфавіту в нижньому регістрі). Варіантів таблиць кодування може бути безліч, тому питання їх формування в даному описі не розглядається.

Секретність паролю, що створюється залежить від наступних параметрів, що може змінювати користувач:

- форма та розмір області кодування, так як це впливає на кількість та якість біометричних характеристик, наприклад кількість ліній відбитку пальця та їх риси всередині області кодування (див. Фіг.3).

- ціною ділення шкали системи координат, так як це впливає на кількість параметрів, що сформують пароль,

- місцезнаходження точки відліку системи координат, так як це є основою для вирахування координат, а відповідно і створення паролю,

- типу кодової таблиці для створення паролю.

Таким чином, даний спосіб є простим для впровадження, надійним в експлуатації, а відповідно доступним для масового використання.

Спосіб може бути реалізовано, наприклад; за допомогою пристрою, блок-схему роботи якого наведено на Фіг.5.

Пристрій складається зі сканера відбитків пальців (блок 5) та процесору з встановленим програмним забезпеченням (блок 6), що проводить кодування відбитку пальця, створення паролю та передачу паролю для ідентифікації в базі даних паролів (блок 8) через форму авторизації (блок 7), наприклад вебсайту.

Сканери відбитків пальців та процесори є розповсюдженими продуктами на ринку, наприклад, як у винаході згідно патенту України №75873 [5].

Програмне забезпечення також можливе для впровадження, так як воно працює на існуючих принципах розпізнавання та кодування зображень [6] та принципах геометрії та шифрування:

- сприйняття зображення: передача даних від сканера до програми,

- підготовка зображення для обробки,

- сегментація - процес пошуку однорідних областей на зображенні, в основному за яскравістю та текстурою,

- покращення або фільтрація зображення,

- вирахування координат областей зображення згідно вибраної системи координат,

- кодування паролю за координатами.

Перелік фігур креслення:

Фіг.1 Блок-схема способу створення пароля за біометричними характеристиками – показує послідовність дій при використанні способу.

Фіг.2. Зображення відбитку пальця з характерними точками показує приклади характерних точок які розглядаються в дактилоскопії.

Фіг.3. Зображення відбитку пальця з координатною сіткою та центром – показує принцип розміщення координатної сітки з використанням характерної (центральної) точки відбитку пальця.

Фіг.4. Зображення відбитку пальця з координатною сіткою та областю кодування С у вигляді квадрата зі стороною 10мм - показує принцип вибору області кодування для вирахування координат точок, що формують зображення всередині області кодування

Фіг.5. Блок-схема роботи пристрою для створення пароля за біометричними характеристиками показує складові частини пристрою та потоки передачі даних при реалізації способу.

Список літератури:

1. Peter Komarinski „Automated Fingerprint Identification Systems (AFIS)” // Elsevier Academic Press - 2005

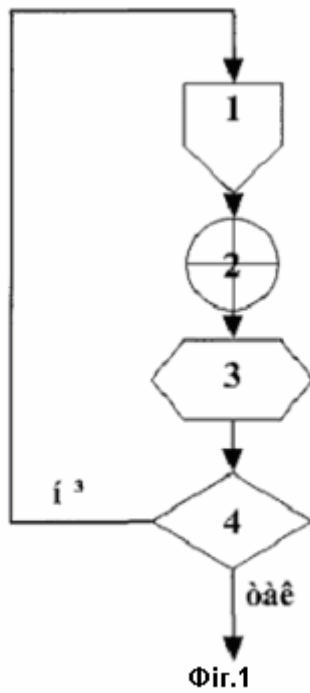
2. David Zhang «Biometric Image Discrimination Technologies” // Idea Group Publishing - 2006

3. Davide Maltoni «Handbook of fingerprint recognition» // Springer - 2003

4. United States Patent 7006673 «Method of hash string extraction»

5. Назва винаходу Портативний пристрій, здатний розпізнавати користувача за біометричними характеристиками, Номер патенту 75873

6. Chen C.H., Rau L.F. and Wang P.S.P. (eds.). „Handbook of pattern recognition and computer vision" // Singapore-New Jersey-London-Hong Kong: World Scientific Publishing Co. Pte. Ltd., 1995.
7. Paul Reid "Biometrics for Network Security" // Prentice Hall PTR - 2003



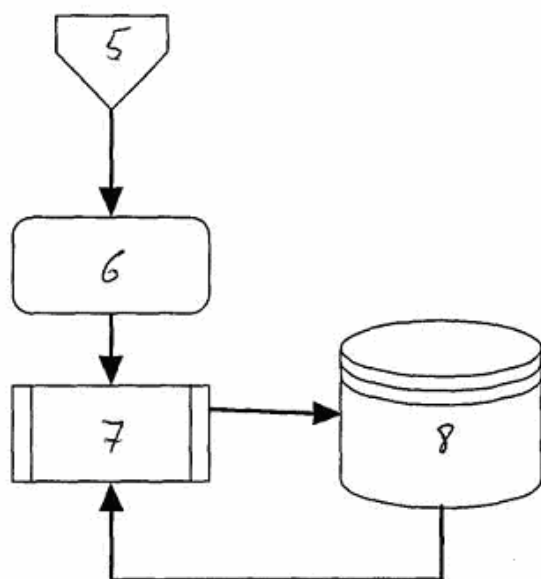
Φir.2



Φir.3



Φir.4



Φir.5