

МЕХАНІЗМИ АВТЕНТИФІКАЦІЇ ЗА ВІДБИТКОМ ПАЛЬЦЯ

Морозов О.Ю.

Науковий керівник – к.т.н., доц. Гріненко Т.О.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. БІТ, тел. (057) 702-14-25)

e-mail: oleksii.morozov@nure.ua

The object of research was the authentication without password. The results of the analysis and research of some methods of authentication are given in the work. They are based on people physical characteristics such as unique fingerprint.

Надійна авторизація та автентифікація стають необхідними атрибутами сучасного життя. Біометричні системи розпізнають людей на основі їх анатомічних особливостей. Оскільки ці риси фізично пов'язані з користувачем, біометричне розпізнавання є дуже надійним механізмом автентифікації. Роль механізму – стежити, щоб тільки ті, хто пройшов автентифікацію, могли отримати доступ до інформації. Таким чином, при грамотній реалізації у відповідних додатках біометричні системи забезпечують високий рівень захищеності [1,2].

Механізми автентифікації поділяються на оптичні, ультразвукові та напівпровідникові, останні в свою чергу діляться на ємкісні, радіочастотні та з використанням термосканерів [1,2]. При оптичному методі автентифікації світло, що випромінюється світлодіодами, відбивається від пальця і потрапляє на світлочутливу матрицю, яка перетворює оптичний сигнал в цифровий. Зчитується, аналізується і порівнюється не саме зображення відбитка, а його геометрія – відстань між лініями, форма, кривизна. Є два основних типи оптичного сканера. Перший – коли робиться знімок потрібної області пальця при дотику до сканера. У другому типі оптичного сканера ми повинні проводити пальцем по сканеру. Сканер робить серію знімків і програмно об'єднує їх в один. Такий метод називається протяжним. В силу необхідності використання більшої матриці для повного знімка відбитка пальця перший тип оптичного сканера є більш дорогим, але, в той же час, більш зручним для кінцевого користувача. Загальним недоліком оптичних сканерів є схильність забруднення, подряпин, впливу фізичного стану пальця (наприклад, вологість). Крім того, перевірку сканера можна обійти за допомогою знімка відбитка пальця.

Напівпровідниковий метод автентифікації заснований на заряді і розряді конденсаторів в залежності від відстані до шкіри в кожній окремій точці поля – якщо конденсатор розташований під горбом, він посиляє один вид сигналу, а якщо під впадиною, то інший. Сигнали об'єднуються і порівнюються із зашифрованою інформацією про відбиток, яка зберігається на пристрої. Такі сканери бувають ємкісними,

радіочастотними та термічними. Ємкісні сканери є сьогодні найбільш поширеними напівпровідниковими пристроями для отримання зображення відбитка пальця. Перевага таких сканерів – низька собівартість та надійність, а недолік – неефективний захист від муляжів.

Перевагою радіочастотних сканерів є те, що ймовірність обману даного сканера прагне до нуля (оскільки аналізуються фізіологічні властивості шкіри). Недолік – нестійка робота при поганому контакті з пальцем.

Метод автентифікації на основі термосканерів має безліч переваг: висока стійкість до електростатичного розряду; стійка робота в широкому температурному діапазоні; ефективний захист від муляжів. До недоліків даного методу можна віднести те, що зображення швидко зникає. При прикладанні пальця в перший момент різниця температур значна і рівень сигналу, відповідно, високий. Після закінчення короткого часу (менше однієї десятої частки секунди) зображення зникає, оскільки палець і датчик приходять до температурної рівноваги.

Найперспективнішим методом роботи сканера відбитків пальців є ультразвуковий метод розпізнавання [1,2]. Ультразвукові сканери використовують принцип медичного УЗД для того, щоб створити візуальний образ відбитку пальця. На відміну від оптичних, ці сканери використовують дуже високі частоти звукових хвиль, які здатні проникати в епідермальний шар шкіри. А він має неповторну структуру. Це виключає потребу в чистому, сухому, непошкодженому пальці. Ультразвуковий сканер неможливо обдурити за допомогою знімка відбитка, так як він формує 3D-картину будови шкіри.

Порівняльний аналіз методів автентифікації наведено у табл. 1.

Таблиця 1 – Порівняльний аналіз методів автентифікації

Методи автентифікації	Складність реалізації	Ефективність захисту	Собівартість
Оптичні	Середня	Висока	Середня
Полупровідникові	Низька	Середня	Низька
Ультразвукові	Висока	Висока	Висока

За результатами дослідження можна зробити висновок, що розглянуті методи автентифікації мають свої переваги та недоліки. При цьому оптичний метод автентифікації є найбільш ефективним за характеристиками складності та ціни. Він частіше за все застосовується в мобільних телефонах та забезпечує високу надійність.

Список джерел:

1. Задорожний В.Г. Идентификация по отпечаткам пальцев, Часть 1, 2004, 400 с.
2. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. Политехника, 2001, 240 с.