II. Мета роботи

Метою дослідження є розробка швидкого методу класифікації шкідливого програмного забезпечення, застосовного у високонавантажених системах.

III. Методика досліджень

Поширені та відносно ефективні методи поведінкового аналізу (імітації запуску в реальний системи та аналіз поведінки) вимагає значних обчислювальних ресурсів, та не застосовні у випадку високонавантажених систем. Для розв'язання поставленої задачі можна використовувати статистичні методи. Але у даного підходу є суттєві недоліки: необхідно використання значної за обсягом бази сигнатур, яку потрібно постійно оновлювати; не може виявити файли інфіковані новими вірусами. Наступним кроком у цій сфері досліджень є машинне навчання - узагальнена назва штучної генерації знань з досвіду. Штучна система навчається на прикладах і після закінчення фази навчання може узагальнювати. Тобто система не просто порівнює підозрілі дані з відомими зразками, як у статистичних алгоритмів, а розпізнає певні закономірності в даних для навчання.

Найбільш ефективними сучасними алгоритми машинного навчання є J48, J48 Graft, PART, нейронні мережі, SVM та інші.

Крім цього, для підвищення ефективності уже відомих алгоритмів можна використати метод бустингу. Це процедура послідовної побудови композиції алгоритмів машинного навчання, коли кожен наступний алгоритм прагне компенсувати недоліки композиції всіх попередніх алгоритмів.

Зручним Інструментом класифікації у даному дослідженні є набір засобів візуалізації та алгоритмів для аналізу даних і вирішення задач прогнозування - Weka. Weka дозволяє виконувати такі завдання аналізу даних, як підготовку даних (preprocessing), відбір ознак (feature selection), кластеризацію, класифікацію, регресійний аналіз та візуалізацію результатів.

Під час доповіді будуть наведені результати експериментального дослідження ефективності вище загаданих алгоритмів класифікації шкідливого програмного забезпечення.

Висновки

Запропоновано статистичний метод класифікації на основи SVM та методів бустингу для застосування в високонавантажених системах мережевої фільтрації.

Список використаних джерел

1. Sumeet Dua, Xian Du. Data Mining and Machine Learning in Cybersecurity. - Auerbach Pub, 2010. - 240 pp. ISBN-13: 978-1-4398-3942-3
2. Marcus A. Maloof. Machine Learning and Data Mining for Computer Security: Methods and Applications. - Springer Science & Business Media, 2006. - 210 pp. ISBN-13: 978-1846280290

УДК 004.056.53

ЛОКАЛІЗАЦІЯ РАЙДУЖНОЇ ОБОЛОНКИ ОКА ДЛЯ МОБІЛЬНОЇ СИСТЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ЛЮДИНИ

Трифонова К.О.[1)], Гришикашвілі Е.І.[2)], Кілін А.Є.[3)]

Одеський національний політехнічний університет

[1)] ст. викладач; [2,3)] студент

I. Постановка проблеми

В сучасних умовах забезпечення безпеки інформаційних ресурсів представляє собою надзвичайно актуальну задачу. Одною з найпоширеніших процедур обмеження та контролю доступу до інформаційних ресурсів вважається парольна ідентифікація. Яка не зважаючи на важливі переваги, такі як простота реалізації та використання, має значні недоліки завдяки людському фактору: величезна залежність надійності ідентифікації від користувачів, точніше, від обраних ними паролів. У зв'язку з цим та значним підвищенням вимог до інформаційної безпеки набули широкого розповсюдження біометричні методи захисту інформаційних ресурсів. При біометричній ідентифікації використовують унікальні характеристики людини. Метод ідентифікації за райдужною оболонкою ока вважається одним з найбільш точних та надійних способів ідентифікації людини. Першим етапом даного біометричного методу є локалізація, тобто визначення центру зірниці та

кордонів райдужної оболонки ока людини на цифровому зображенні. Для вирішення задачі локалізації використовують алгоритм Хафа.

II. Мета роботи

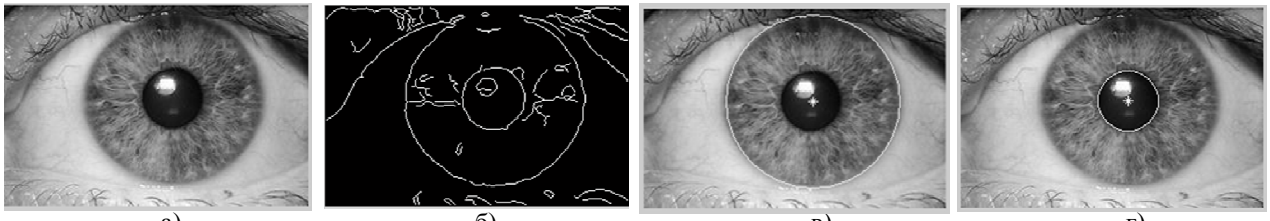
Метою дослідження є вирішення задачі локалізації райдужної оболонки ока людини для реалізації біометричної системи ідентифікації людини засобами мобільного пристрою.

III. Основна частина

Метод Хафа є одним з найбільш ефективних методів пошуку аналітично заданих кривих на цифровому зображенні. Основна ідея методу полягає у врахуванні характеристик кривої не як рівняння побудованого по точкам цифрового зображення, а в термінах її параметрів [1]. Метод Хафа будує для визначення кривих простір Хафа, розмірність якого визначається кількістю параметрів кривої, що розшукується на зображенні. Основним кроком методу Хафа є відображення цифрового зображення в простір Хафа з подальшим застосуванням процедури аналізу. Отже, алгоритм метода Хафа складається з наступних кроків: бінаризація [2]; побудова акумулятивної матриці; порогова сегментація акумулятивної матриці.

Висновок

В результаті даної роботи досліджено та реалізовано алгоритм Хафа для локалізації райдужної оболонки ока людини, що є першим кроком реалізації біометричної системи ідентифікації людини для мобільного пристрою. Програмна реалізація проведена для мобільної платформи Android з використанням засобів мови програмування високого рівня Java. Подальша робота спрямована на завершення реалізації біометричної системи ідентифікації людини для мобільного пристрою. На рисунку 1 представлено результат роботи алгоритму Хафа.



а) б) в) г)

Рис. 1 – Застосування методу Хафа а) – вихідне зображення; б) – бінарне представлення контурів; в) – визначення параметрів райдужної оболонки ока; г) – визначення параметрів зіниці ока.

Список використаних джерел

1. Duda, R.O. Use of the Hough transform to detect lines and cures in pictures / R.O. Duda, P.E. Hart . – Comm.AC, 197,Vol. 15, №11. – P.11-15
2. Трифонова, К.О. Визначення контурів райдужної оболонки ока для системи біометричної ідентифікації людини / К.О. Трифонова, Е.І. Гришикашвілі, А.Р. Агаджанян // Научный и производственно-практический сборник. Труды Одесского политехнического университета. – Вып.1(45). – 2015. – С.107–112

УДК 004.056.56: 655.25

СПОСІБ ЗАХИСТУ ДРУКОВАНИХ ДОКУМЕНТІВ НА ОСНОВІ ЛАТЕНТНИХ ЕЛЕМЕНТІВ ЗА ДОПОМОГОЮ ЕФЕКТУ МУАРУ

Троян О.А.

Національний університет «Львівська політехніка», аспірант

Пропонуємо спосіб захисту документів з допомогою створення латентних елементів, які забезпечують захист інформації. Вибір параметрів дає можливість отримати різні вигляди графіків, що дозволяє персоніфікувати кожен документ. Розроблено новий вид захисту документів на основі муарних ефектів, який задовольняє критерії економічності та надійності. Новий метод заснований на оптичному ефекті, який призводить до виникнення муару. Запропонований метод ґрунтується на створенні захисних елементів за допомогою тонких неперервних ліній.

З розвитком комп’ютерної техніки фальсифікація документів стає поширеним явищем. [3] Технології виготовлення документів стають простішими у наслідок чого фальсифікація набуває все більшого розвитку. [1]У зв’язку з цим виникає потреба захисту електронних та друкованих документів новими способами. Комп’ютерна індустрія та сучасна копіювально-розмножувальна