ЗАСТОСУВАННЯ ЕНТРОПІЇ ДЛЯ ІДЕНТИФІКАЦІЇ СИМВОЛІВ ЗА ЇХ 2D ЗОБРАЖЕННЯМИ

Адамович А. Р.
студент
Університету Короля Данила
м. Івано-Франківськ, Україна
Науковий керівник: ***Мельничук С. І.***
доктор технічних наук, професор

Ідентифікація об'єктів за імовірнісними характеристиками їх 2D шаблонів – поставлена задача розробки нового способу розпізнавання об'єктів шляхом використання значення однієї або декількох сумісно імовірнісних характеристик фрагментів зображення обчислених за еталонними шаблонами образів, що дозволяє спростити алгоритмічну і програмну реалізацію, а також забезпечити покращення достовірності розпізнавання у випадках суттєвої зашумленості. В якості таких характеристик використовують ентропію, розподіл ймовірностей станів, дисперсію, середнє квадратичне відхилення [1].

Вирішення поставленої задачі стає можливим завдяки тому, що при опрацюванні послідовності непохідних елементів, яка представляє розпізнаваний об'єкт, для порівняння використовують значення однієї або декількох сумісно імовірнісних характеристик фрагментів зображення обчислених за еталонними шаблонами образів.

Значення імовірнісної характеристики стаціонарних процесів, що обчислюються за елементами шаблонних фрагментів зображення прямує до постійної величини, яка залежить від характеристик зображення та наявних спотворень. В ході опрацювання таких фрагментів відбувається зміна результуючого значення відповідної імовірнісної характеристики, що використовується як ознака форми об'єкту.

В результаті отримав подальшого розвитку спосіб, у якому ідентифікацію об'єктів здійснюють шляхом оцінювання значення імовірнісних характеристик фрагментів зображення обчислених за еталонними шаблонами образів, що забезпечує покращення достовірності а також кількісних та якісних характеристик цифрових систем розпізнавання [2].

Для ідентифікації (розпізнавання) об'єкту, за його 2D зображенням, використовують цифрові значення (код) кольору відповідних точок (пікселів), отриманих при оцифровуванні. Для кожного образу створюється окремий еталонний шаблон. При опрацюванні шаблон

(еталонні шаблони образів) визначає фрагмент зображення (фрагмент зображення за елементами якого розраховується оцінка ентропії H_i), за яким обчислюється оцінка ентропії, значення якої в подальшому використовується в якості ознаки форми [3].

У випадку ідентифікації одного об'єкту, наближення оцінки ентропії до нульового значення визначає ступінь його відповідності до задіяного еталонного шаблону образу об'єкту.

У випадку множинної ідентифікації об'єктів використовують набір еталонних шаблонів, за яким розраховується набір оцінок ентропії мінімальне значення якого, визначає приналежність отриманого зображення до відповідного образу об'єкту.

Описаний спосіб забезпечує спрощення алгоритмічної та програмної реалізації, можливості використання в малопродуктивних обчислювальних системах, а також зменшення чутливості до рівномірного спотворення зображень, що зумовлена впливом навколишнього середовища при оцифровуванні.

Тобто при побудові проекції формують відображення зображення у вектор, значення якого представляють як результат обчислення однієї або декількох сумісно імовірнісних характеристик фрагментів цифрового представлення розташованих вздовж визначених напрямків.

Множина усіх монохромних зображень розміру $n+m$ пікселів знаходиться у бієктивній відповідності з множиною усіх бінарних матриць порядку $n+m$, тобто є векторним простором розмірності над скінченним полем. Означино відображення простору $\{0.1\}^n$ (простір впорядкованих наборів з "0" та "1" довжиною n) у відрізок [0.1] (оцінок інформаційної ентропії таких наборів), тобто відображення

$$\hat{h}_n : \{0,1\}^n \to [0,1] \tag{1}$$

$$\hat{h}_n(i_1, i_2, ..., i_n) = P^{"0"} \cdot \log_2 P^{"0"} + P^{"1"} \cdot \log_2 P^{"1"}, \tag{2}$$

де $i_j \in \{0,1\}$,

$$P^{"1"} = \frac{1}{n} \sum_{j=1}^{n} i_j, \tag{3}$$

$$P^{"0"} = 1 - P^{"1"}. \tag{4}$$

Нехай бінарна матриця X $\{0,1\}^{nxm}$ є представленням деякого об'єкту. Означимо тепер відображення оцінок ентропії наступним чином:

$$\hat{h}_h(X) = (\hat{h}_m(x_{11}, x_{12},..., x_{1m}), \hat{h}_m(x_{21}, x_{22},..., x_{2m}),..., \hat{h}_m(x_{n1}, x_{n2},..., x_{nm})) \quad (5)$$

де x_{ij} – елемент матриці X або матриці отриманої з X незалежними перестановками елементів у її стовпцях.

$$\hat{h}_v(X) = (\hat{h}_n(x_{11}, x_{21},..., x_{n1}), \hat{h}_n(x_{12}, x_{22},..., x_{n2}),..., \hat{h}_n(x_{1m}, x_{2m},..., x_{nm})) \quad (6)$$

де x_{ij} – елемент матриці X або матриці отриманої з X незалежними перестановками елементів у її рядках.

Індекси h та v у позначенні $\hat{h}$ відображення фактично вказують на те, що $\hat{h}_h$ – діє на рядки а $\hat{h}_v$ – діє на стовпці матиці X.

Таким чином кожному бінарному зображенню об'єкта (рисунок 6) ставиться у відповідність набір проекцій – векторів оцінок ентропії, які отримуються через застосування відображень h_h та h_v до матриці X та її заданих перестановок [20, 21].

На основі таких проекцій формують еталонні представлення для заданої кількості k об'єктів H^e : {H^{e1}, H^{e2},…,H^{ek}} з використанням яких, в подальшому, розраховується коефіцієнти парної кореляції з об'єктом, що ідентифікується.

В результаті формується матриця коефіцієнтів кореляції задіяних проекцій об'єкту H^{ob} та наявних еталонів H^e:

Відповідність об'єкту до одного з наявних еталонів визначається за найбільшою кількістю максимальних значень коефіцієнтів парної кореляції R_{xy} (h^e, h^{ob}) в одному рядку. Якщо в матриці виявлено рядки з рівною кількістю максимальних R_{xy} (h^e, h^{ob}) то відповідність не встановлено, тобто інформації отриманої за проекціями об'єкту H^{ob} недостатньо для його ідентифікації [4]. Структурну схему реалізації описаного методу подано на рисунку 7.

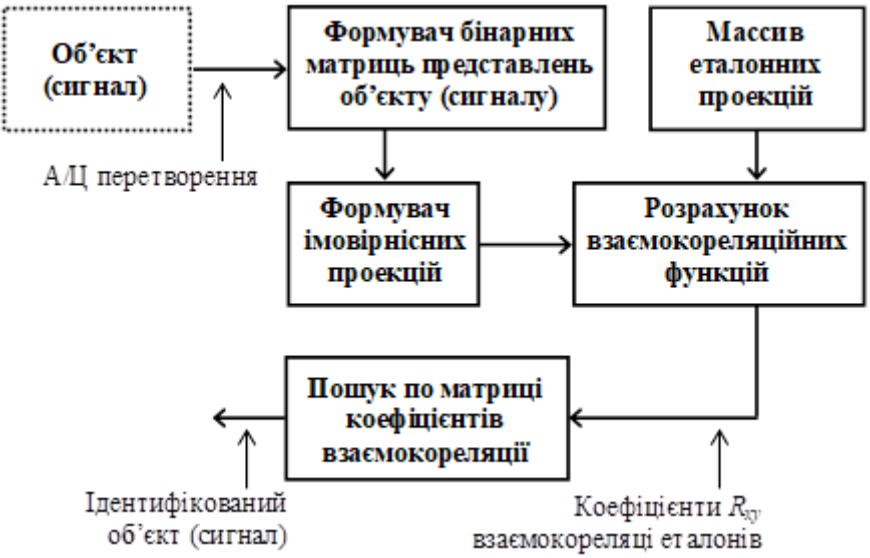

Рисунок 7 – Схема ідентифікації об'єкту (сигналу) за його імовірнісними проекціями

Запропонований підхід побудови проекцій за оцінками інформаційної ентропії, які розраховують за формулою Шеннона, є інваріантним до інверсного представлення об'єкту [5].

Література:

1. Горелик А. Л. Методы распознавания / Л. А. Горелик – М.: Высшая школа, 2004. – 262 с.
2. Бонгард М. М. Проблема узнавання / М. М. Бонгард – М.: Наука, 1967. – 320 с.
3. Бардаченко В. Ф. Перспективи застосування імпульсних нейронних мереж з таймерним представленням інформації для розпізнавання динамічних образів / В.Ф. Бардаченко, О.К. Колесницький, С.А. Василецький // УСіМ. – 2003, No6. – С. 73 – 82.
4. Імад І.А. Система реконструкції тривимірних об'єктів за невпорядкованими даними аерозображень / І. А. Імад, В. Ємець, О. Карпін // Матеріали І Міжнародної конференції: Modern problems of radioelectronics, telecommunications and instrument making (MPRTI-2005). Vinnitsa 2-5 June 2005. – 105 с.

5. Захожай О.І. Основні аспекти структурної організації комбінованих систем розпізнавання образів / О.І. Захожай, Ю.Е. Паеранд // Вестник ХНТУ №1 (44). – Херсон: «Олди-Плюс». – 2012 – С. 221 – 225.

ВРАЗЛИВОСТІ WI-FI МЕРЕЖ

Білевська О. С.
науковий співробітник
Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
м. Київ, Україна

Радіоканал передачі даних, який використовується в Wi-Fi мережах, потенційно схильний до втручанню з метою порушення конфіденційності, цілісності і доступності інформації. При підключенні до мережі передбачена аутентифікація та шифрування, але ці елементи захисту мають свої вади.

Шифрування значно знижує швидкість передачі даних, і, найчастіше, воно усвідомлено відключається адміністратором для оптимізації трафіку. Початковий стандарт шифрування WEP (Wired Equivalent Privacy) був дискредитований за рахунок вразливостей в алгоритмі розподілу ключів RC4 (Rivest Cipher 4). Стандарт WPA2 представляє собою покращений WPA. Основна відмінність між WPA і WPA2 полягає в технології шифрування, який поєднує симетричний алгоритм блочного шифрування AES (Advanced Encryption Standart) та TKIP. WPA2 забезпечує більш високий рівень захисту мережі, так як TKIP дозволяє створювати ключі довжиною до 128 біт, а AES – до 256 біт.

Більшість атак починаються з розвідки, під час якої виконується сканування мережі, збір і аналіз пакетів. Багато службових пакетів в мережі Wi-Fi передаються у відкритому вигляді. При цьому вкрай проблематично з'ясувати, хто легальний користувач, який намагається підключитися до мережі, а хто збирає інформацію. Після розвідки приймаються рішення про подальші кроки можливої атаки.

Найбільш поширеними є два технічних сценаріїв атак на мережі Wi-Fi – це перехоплення пакетів, які пов'язані з аутентифікацією клієнта (рукостискання – handshake) з подальшим перебором пароля за словником, і створення підробленої точки доступу з паралельним проведенням атаки «відмови в обслуговуванні» на справжню точку доступу.