УДК 004.932.052.2

О. В. Салієва
А. В. Ніколаєнко

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ МАТРИЧНИХ ФІЛЬТРІВ В АЛГОРИТМАХ ПРИХОВУВАННЯ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

У доповіді здійснено дослідження алгоритмів приховування інформації, що використовують матричні фільтри для вбудовування інформації в зображення. Досліджено роботу матричних фільтрів та здійснено їх детальне порівняння, в результаті якого виявлено сильні та слабкі сторони розглянутих алгоритмів.

Ключові слова: стеганографія, прихована інформація, матричні фільтри, зображення.

Abstract

The report researches information hiding algorithms that use matrix filters to embed information in images. The work of matrix filters has been studied and a detailed comparison and identification of strengths and weaknesses of the considered algorithms has been carried out.

Keywords: steganography, hidden information, matrix filters, images.

Вступ

На сучасному етапі стрімкого розвитку інформаційних технологій та швидкого прогресу зв'язку, забезпечення безпеки конфіденційної інформації стає значущим викликом. Поступове поширення технологічної інтеграції та її вплив на засоби комунікації акцентують постійне удосконалення стратегій захисту інформації. Передача секретних повідомлень через незахищені мережеві канали становить серйозну загрозу для конфіденційності та цілісності інформації. Атаки, спрямовані на зміну кольорів у зображеннях, можуть викликати розкриття захищеної інформації, порушення її конфіденційності, та навіть призвести до втрати важливих даних. Розробка та вдосконалення методів передачі секретної інформації в незахищених мережах стають основними завданнями для забезпечення безпеки даних. Використання алгоритмів з матричними фільтрами для захисту інформації у зображеннях може забезпечити додатковий рівень стійкості до атак, що дозволить ефективно захищати секретні повідомлення в мережевих каналах.

У зв’язку з цим, дослідження використання матричних фільтрів в алгоритмах приховування інформації є надзвичайно важливим та актуальним.

Результати дослідження

Матричні фільтри (або як їх ще називають ядра) використовуються при обробці зображень. Зазвичай, ядро – це невелика матриця, що застосовується для нанесення різних ефектів на зображення. Процес обробки ядром зображення називається згорткою. Дана функція обраховує кожен піксель зображення. Тобто для отримання візуального ефекту на зображенні потрібно виконати згортку між ядром і зображенням. Загальний вигляд згортки представлений за допомогою формули 1.

$$g(x,y) = \omega \times f(x,y) = \sum_{i=-a}^{a} \sum_{j=-b}^{b} \omega(i,j) \times f(x-i, y-j) \quad (1)$$

де $g(x,y)$ – відфільтроване зображення, $f(x,y)$ – оригінальне зображення, а ω – ядро функції.

Кожен елемент ядра фільтра розглядається як (2):

$$-a \leq i \leq ai - b \leq j \leq b \quad (2)$$

Приклади роботи різних ядер показано на рисунку 1.

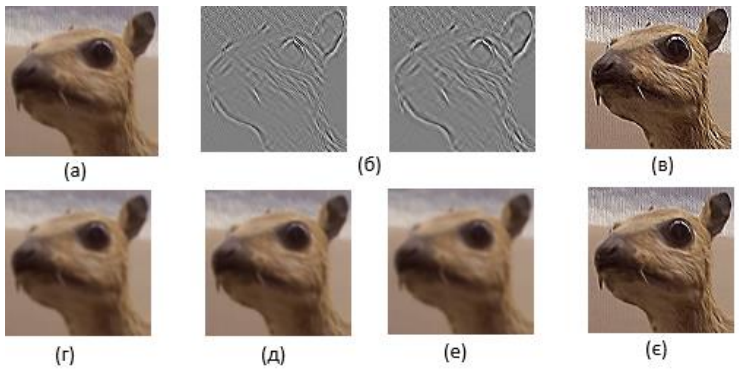

Рисунок 1 – Приклади роботи згортки з різними ядрами, дані зображення відповідають операціям: (а) ідентичність, (б) виявлення краю, (в) гострі краї, (г) розмиття рами, (д) Гаусове розмиття 3x3, (е) Гаусове розмиття 5x5, (є) нерізке маскування 5x5 [1]

Матричні фільтри можуть ефективно використовуватися для пошуку складних ділянок зображення, які можна застосовувати для приховування інформації.

Розглянемо алгоритм Edge Least Significant Bitembedding (ELSB), в якому використовуються всі крайні пікселі зображення. Спочатку обчислюється замасковане зображення, маскуючи два біти LSB на титульному зображенні. Потім визначається крайні пікселі за допомогою методу виявлення Canny Edge, що є різновидом матричних фільтрів. Після отримання крайніх пікселів дані приховуються лише в бітах LSB крайніх пікселів [2].

Даний метод є досить надійним для приховування інформації в зображенні. Більшість методів, що використовують пошук крайніх пікселів використовується LSB.

У роботі [3] запропоновано алгоритм для приховування інформації в крайових пікселях, де використовує три типи фільтрів для виявлення країв: Лапласіанський, Собеля та Превітта. На рисунку 2 показано приклад виявлення ребер за допомогою фільтра Собеля [4].

Рисунок 2 – Приклад використання фільтру Собеля [4]

Після виявлення країв алгоритм поміщає крайні пікселі в ключову матрицю і застосовує дискретне косинусне перетворення (ДКП) до кольорових каналів для побудови трьох різних векторів (по одному вектору для кожного каналу). Вектор повідомлення перетворюється в двійковий код, а його довжина зберігається в початкових кутових пікселях зображення. Для кожної позиції (i, j) у ключовій матриці враховуються її значення для червоного та синього каналів після перетворення, використовуючи формули 3 та 4 [3]:

$$X = dctred(key(i), key(j)) \quad (3)$$

$$Y = dctblue(key(i), key(j)) \quad (4)$$

Значення для зеленого каналу визначається на основі наступного біта повідомлення за формулами 5 та 6.

$$dctgreen(key(i), key(j) = (X - Y)/2, for\ 0 \quad (5)$$

$$dctgreen(key(i), key(j)) = (X + Y)/2, for\ 1 \quad (6)$$

Це означає, що якщо біт повідомлення дорівнює 0, то відповідна позиція в зеленому каналі дорівнює половині різниці червоного і синього каналів; в іншому випадку – це середнє значення червоного і синього каналів [3].

Крім того, варто звернути увагу на метод запропонований Mangat Rai Modi, Saiful Islam, та Phalguni Gupta, який працює на кольорових зображеннях. Ребра знаходять за допомогою алгоритму Canny Edge в одній з площин. Потім вибираються пікселі в двох інших площинах, що відповідають крайнім пікселям. Ці пікселі будуть містити біти секретного повідомлення. З набору цих обраних пікселів генерується випадковий блукаючий алгоритм, який використовує пароль, необхідний для розшифрування. Цей пароль, також відомий як стего-ключ, який є спільним для відправника та отримувача секретного повідомлення [5].

Детальне порівняння розглянутих вище алгоритмів, наведено в таблиці 1. Здійснено оцінювання проаналізованих алгоритмів за шкалою від 1 до 10, де 1 – це найбільш нестійкий та слабкий алгоритм, а 10 – алгоритм, що задовольняє вимоги стійкості, непомітності та ємності на високому рівні.

Таблиця 1 – Порівняння досліджуваних алгоритмів

Алгоритм	Стійкість	Непомітність	Ємність	Оцінка
Алгоритм ELSB [2]	Стійкий до візуальних атак, атаки SPAM, структурних атак. Вразливий до статистичних атак та до деяких видів атак колірної гами. Різниця в структурі зображення може впливати на ефективність приховування і виявлення прихованої інформації.	Залежить від кількості прихованої інформації	10% від зображення (норма)	7
Алгоритм приховування даних в крайових пікселях [6]	Стійкий до статистичних атак, візуальних атак. Не стійкий до атак основі аналізу зсуву та деяких атак зміни колірної гами.	Залежить від кількості прихованої інформації	8% від зображення (норма)	8
Алгоритм на основі границь [5]	Стійкий до візуальних атак. Не стійкий до атак стиснення та обрізання. Не стійкий до атак зміни колірної гами.	Залежить від кількості прихованої інформації	10% від зображення (норма)	6

Таким чином, кожен з трьох алгоритмів є стійким до візуальних атак та має досить високий показник ємності. Однак, невидимість прихованої інформації для кожного алгоритму досить сильно залежить від кількості прихованих даних. Крім того, досліджувані алгоритми мають спільний недолік – відсутність стійкості до атак зміни колірної гами.

Висновок

В даній роботі було досліджено різні матричні фільтри та алгоритми приховування інформації, що їх використовують. Застосування матричних фільтрів для приховання інформації є надійним та доступним методом для побудови або вдосконалення стеганоалгоритму. Актуальною є розробка та удосконалення алгоритму приховування інформації, що буде стійким до атак зміни колірної гами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ядро (обробка зображень). Вікіпедія.URL: https://en.wikipedia.org/wiki/Kernel_(image_processing) (дата звернення: 16.11.2023).

2. Навін БрахмаТеджа К., Мадхуматі Г. Л., Рама Котешвара Рао К. Приховування даних за допомогою стеганографії на основі EDGE. Міжнародний журнал новітніх технологій і передової техніки. 2012. Вип. 2, № 11.¬ — С. 285–290.

3. Аломіра Р. Алгоритм стеганографії на основі країв для приховування тексту в зображеннях : магістерська робота. Окленд, 2019. 95 с. URL: https://www.researchbank.ac.nz/bitstream/handle/10652/4502/MComp_2019_Reem%20Alomirah.pdf?sequence=1 (дата звернення: 16.11.2023).

4. Фільтр Собеля для виявлення зображень. Мікрочіп: веб-сайт. URL: https://onlinedocs.microchip.com/pr/GUID-37AD5EEE-6FAB-48FC-89F6-CAA649534B2A-en-US-1/index.html (дата звернення: 16.11.2023).

5. Моді М. Р., Іслам С., Гупта П. Стеганографія на основі країв на кольорових зображеннях. Конспект лекцій з інформатики. 2013.— Р. 593–600.

6. Мукерджі С., Гутам С. Стеганографія зображення на основі фізичного рівняння з електромагнітним вбудовуванням. Мультимедійні засоби та програми. 2019 рік.

Салієва Ольга Володимирівна – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@gmail.com

Ніколаєнко Андрій Володимирович – студент групи 2КІТС-22м, факультет менеджменту інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: andrey.nikolaienko.0@gmail.com

Saliieva Olha V. – Doctor of Philosophy (PhD) in specialty 125 «Cyber Security», Associate Professor of the Department of Information Systems Management and Security, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@gmail.com

Nikolayenko Andrii V. – student of group 2KITS-22m, Faculty of Information Security Management, Vinnytsia National Technical University, Vinnytsia, e-mail: andrey.nikolaienko.0@gmail.com