

# СТАТИСТИЧНИЙ СТЕГОАНАЛІЗ ЦИФРОВИХ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ УНІВЕРСАЛЬНОЇ МОДЕЛІ CDF

Д. О. Панічева<sup>1, а</sup>, Д. О. Прогонов<sup>1, б</sup>

<sup>1</sup>Національний технічний університет України «Київський політехнічний інститут»

## Анотація

У роботі досліджено точність виявлення стегограм з даними, вбудованими в області перетворення зображення-контейнера, при використанні універсальної CDF-моделі. Показано, що застосування CDF-моделі дозволяє підвищити ймовірність виявлення стегограм у порівнянні із статистичними моделями зображення SPAM та CC-PEV навіть у випадку слабого заповнення зображення-контейнера стегоданими.

*Ключові слова:* статистичний стегоаналіз, CDF-модель

## Вступ

Поява нових методів приховання повідомлень у цифрових зображеннях (ЦЗ) суттєво ускладнює виявлення сформованих стегограм. Особливий інтерес становить випадок вбудовування стегоданих в області перетворення контейнера (ОПК), що дозволяє забезпечити високу стійкість стегограм до відомих методів пасивного та активного стегоаналізу.

Одним із найбільш поширених підходів у стегоаналізі цифрових зображень (ЦЗ) є статистичний аналіз, що включає два основні етапи — побудова статистичної моделі зображення та класифікація отриманих векторів параметрів із використанням засобів машинного навчання [1].

Існуючі статистичні моделі ЦЗ можуть бути розділені на три класи: моделі, що будуються у просторовій області ЦЗ, в частотній області ЦЗ та універсальні моделі, отримані шляхом об'єднання перших двох. У роботах [2, 3] було показано високу ефективність використання моделей SPAM (просторова область зображення) та CC-PEV (частотна область зображення) при виявленні стегограм, сформованих в ОПК. Тому цікавим є дослідження ефективності застосування універсальної CDF-моделі [1], що є результатом їх об'єднання, при виявленні приховання даних відповідно до різних стегографічних схем.

Метою роботи є порівняння ефективності виявлення одноетапних, багатоетапних та комплексних методів вбудовування в ОПК при використанні налаштованого стегодетектора на основі CDF-моделі.

## 1. Сучасні методи приховання повідомлень в області перетворення зображення-контейнера

У роботі було досліджено сучасні одноетапні (метод Дея) [4], багатоетапні (метод Джозефа) [5] та комплексні (метод Елайона) [6] методи вбудовування

даних у ЦЗ. Дані методи засновані на використанні двовимірного дискретного вейвлет-перетворення (ДДВП).

Вбудовування стегоданих здійснюється шляхом додавання коефіцієнтів перетворення зображення-контейнера (ЗК) та стегоданих з ваговим коефіцієнтом  $G$  [4]:

$$S_{ST} = S_C + \alpha \cdot S_{SD},$$

де  $S_{ST}$ ,  $S_C$ ,  $S_{SD}$  — коефіцієнти розкладу за ДДВП стегограми, ЗК та стегоданих, відповідно, а  $G$  — ваговий коефіцієнт вбудовування стегограми (частка змінених коефіцієнтів перетворення ЦЗ).

При вбудовуванні за двоетапним методом Джозефа додатково застосовується сингулярний розклад (СР) ЦЗ [5]:

$$A = U \cdot S \cdot V^T,$$

де  $U$ ,  $V$  — ортогональні матриці порядків  $m$  та  $n$ , що складаються із лівих та правих сингулярних векторів, відповідно, а  $S$  — діагональна  $m \times n$ -матриця сингулярних чисел матриці  $A$ .

Особливістю методу Елайона є застосування до ЗК процедури конвертації із RGB у YcbCr, а до стегоданих — перетворення Арнольда (ПА), що призводить до уподібнення стегоданих до власного шуму ЗК, і, як наслідок, зменшення ймовірності виявлення [6]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \bmod(N),$$

де  $\begin{bmatrix} x \\ y \end{bmatrix}$  та  $\begin{bmatrix} x' \\ y' \end{bmatrix}$  — координати положення пікселів зображення до та після перетворення,  $N \times N$  — розмір ЦЗ у пікселях.

## 2. Універсальна модель CDF цифрових зображень

Статистична модель CDF була запропонована в роботі [1] та заснована на об'єднанні двох моделей: SPAM (просторова область ЦЗ) та CC-PEV (частотна область ЦЗ).

<sup>а</sup>panicheva.d@gmail.com

<sup>б</sup>progonov@gmail.com

Табл. 1. Максимальні та мінімальні значення математичного очікування значень площі під ROC-кривою для різних методів вбудовування

Тип стегоданих	Метод вбудовування		
	Дея	Джозеф	Елайон
"Креслення"	1; 0,913	1;0,661	1;0,99
"Карта"	1;0,916	1;0,556	1;0,99
"Портрет"	0,99;0,898	1;0,532	1; 0,99
Всі типи стегоданих	0,99;0,99	1;1	1;1

Статистична модель SPAM базується на моделюванні різниць яскравості між сусідніми пікселями ЦЗ для восьми напрямків (горизонтальних, вертикальних та діагональних) як марківського процесу другого порядку. Вектори параметрів SPAM-моделі формуються шляхом усереднення матриць ймовірності переходу Маркова у діапазоні  $[-T, T]$  при  $T = 3$  для горизонтального, вертикального та діагональних напрямків. Кількість параметрів моделі становить  $k = (2T + 1)^3 = 686$  [7].

В якості параметрів статистичної моделі SS-PEV використовуються два набори параметрів, вилучених у частотній області ЦЗ – параметри Маркова та параметри дискретного косинус-перетворення (ДКП). Для отримання опорних зображень застосовується процедура калібрування ЦЗ, що відповідає розпакуванню вихідного ЦЗ  $J_1$  із застосуванням зворотного ДКП, кадруванню на  $n$  пікселів в обох напрямках та стисненню зображення з тим же коефіцієнтом якості. Відповідно до початкового припущення [1], результуюче опорне зображення  $J_2$  має бути близьким до вихідного ЗК, тому калібровані параметри визначалися як різниця між параметрами вилученими із  $J_1$  та  $J_2$ . Проте, з метою зменшення ризику втрати потенційно корисної інформації та для підсилення слабких змін статистичних характеристик ЦЗ, обумовлених прихованням повідомлень, застосовується декартовий добуток параметрів, вилучених із  $J_1$  та  $J_2$  [8]:

$$F_c(J_1) = [F(J_1), F(J_2)].$$

Кількість параметрів SS-PEV моделі становить 548.

### 3. Процедура налаштування стегодетектора

Згідно з рекомендаціями [9] в якості стегодетектора було використано ансамбль класифікаторів – лінійних дискримінантів Фішера.

Для оцінки точності виявлення стегоданих було використано похідні метрики ROC-аналізу, а саме площу під ROC-кривою (AUC), що визначається як [10]:

$$\int_{-\infty}^{\infty} TPR(T) \cdot FPR'(T) dT;$$

$$TPR = \frac{TP}{TP + FN}; FPR = \frac{FP}{TN + FP},$$

де  $TP$  – істинно позитивне рішення,  $TN$  – істинно негативне рішення,  $FP$  – хибно позитивне рішення,

$FN$  – хибно негативне рішення,  $TPR$  – чутливість (частка істинно позитивних рішень від загальної кількості),  $FPR$  – частка хибно позитивних рішень від загальної кількості.

Площа під ROC-кривою дає інформацію про ймовірність того, що класифікатор призначить більшу вагу випадково обраному позитивному об'єкту, ніж негативному. Метрика AUC приймає значення у діапазоні  $[0, 1]$ , де 1 відповідає випадку ідеальної класифікації, 0,5 – віднесення досліджуваного зображення до класу ЗК або стеганограм випадковим чином, 0 – віднесення зображення-контейнеру до класу стеганограм та навпаки [10].

### 4. Результати роботи

Дослідження точності виявлення стеганограм з використанням стегодетектора  $SD_{CDF}$  проводилося з використанням вибірки об'ємом 9000 ЦЗ у форматі JPEG (пакек MIRFlickr-25к), яку було розділено на навчальну і тестові підвибірки однакового розміру. Тестові зображення було масштабовано до розміру  $512 \times 512$  пікселів. У якості стегоданих було використано три типи повноколірних зображень з різним ступенем деталізації: «Креслення», «Карта» та «Портрет» – представлених у форматі BMP.

Ступінь заповнення ЗК стегоданими (частка змінених коефіцієнтів перетворення ЦЗ) змінювався від 5% до 25% з кроком 5% та від 25% до 95% з кроком 10%. Ваговий коефіцієнт  $G$ , пропорційний енергії стеганограми, змінювався від мінімального (відповідає нижній границі відновлення даних) до максимального (відповідає появі помітних візуальних спотворень):  $[0, 02; 0, 04; 0, 06; 0, 08]$  (метод Дея),  $[1; 4; 8; 12]$  (метод Джозефа),  $[0, 5; 1; 2; 5]$  (метод Елайона).

Тестування стегодетектора проводилося для випадків вбудовування різних типів стегоданих у канали кольору ЗК. Для оцінки усередненої точності виявлення окремі канали кольору ЦЗ було об'єднано. У таб. 1 представлені мінімальні та максимальні значення метрики AUC для стегодетектора на основі CDF-моделі при використанні одноетапного, багатоетапного та комплексного методів для формування стеганограм.

Найбільша точність виявлення стеганограм була досягнута у випадку формування стеганограм за методом Елайона (значення площі під ROC-кривою незначно відхиляються від 1), незалежно від типу стегоданих. Це пояснюється тим, що результатом застосування ПА, що лежить в основі методу Елайона, є фрактальний шум, який добре моделюється CDF-моделлю. Найменші значення (0, 661, 0,556 та 0,532) було отримано для методу Джозефа, оскільки вбудовування здійснюється у сингулярні числа ЦЗ, що ускладнює виявлення при малих значеннях вагового коефіцієнта стеганограми.

На рис. 1 представлені середні значення площі під ROC-кривою для випадку стегоданих типу «Карта» при варіації ступеня заповнення контейнера та вагового коефіцієнта стеганограми для різних методів вбудовування.

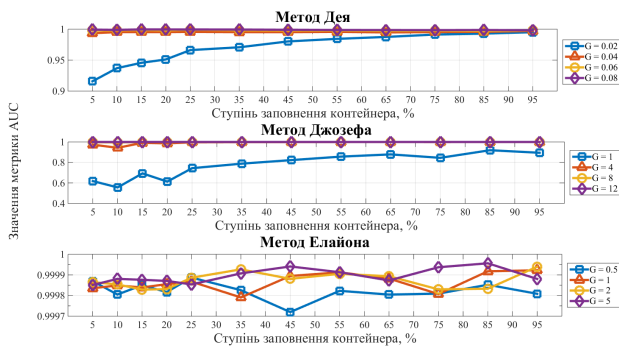


Рис. 1. Середні значення площі під ROC-кривою для випадку стегоданих типу «Карта» для різних методів вбудовування

Значення метрики AUC є близькими до 1 (висока точність класифікації) для всіх методів вбудовування даних незалежно від ступеня заповнення контейнера даними та вагового коефіцієнта стеганограми, окрім випадків мінімальних значень, що відповідає нижньому порогу відновлення даних. Проте навіть за таких умов факт приховання даних може бути встановлений з високою точністю при малих значеннях ступеня заповнення контейнера (25%).

## Висновки

За результатами порівняльного аналізу ефективності використання CDF-моделі при виявленні різних методів вбудовування даних в ОПК встановлено, що при застосуванні універсальної статистичної моделі ЦЗ з високою точністю може бути виявлено факт стеганографічного вбудовування як за одноетапними так і за багатоетапними методами приховання даних: мінімальні значення площі під ROC-кривою становлять 0,898, 0,532 та 0,99 для методів Дея, Джозефа та Елайона, відповідно.

## Перелік використаних джерел

1. J. Kodovsky, J. Fridrich, Calibration revisited, In J. Dittmann, S. Craver, and J. Fridrich, editors, Proceedings of the 11th ACM Multimedia and Security Workshop, Princeton, NJ, September 7–8, 2009.
2. Прогонов Д., Панічева Д., Куц С. Виявлення стеганограм з використанням комплексних статистичних моделей цифрових зображень. – Матеріали IV-ої Міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем». – Львів: Українська академія друкарства, 2015. – с. 127-128.
3. Прогонов Д. О., Панічева Д. О. Виявлення стеганограм з використанням універсальних статистичних моделей контейнеру – Матеріали Міжнародна науково-технічної конференції «Радіотехнічні поля, сигнали, апарати та системи». – Київ, 2016. – с. 228-230.
4. N. Dey, A. Bardhan Roy and S. Dey, A Novel Approach of Color Image Hiding using RGB Color planes and DWT, International Journal of Computer Applications, Volume 36– No.5, December 2011.
5. Anumol Joseph1, K. Anusudha, Robust watermarking based on DWT SVD, International Journal on Signal & Image Security, Issue. 1, Vol. 1, Oct 2013.
6. Atefeh Elahian et al, Improved robust DWT-watermarking in YCbCr color space, GJCAT, Vol 1 (3), 2011, 300-304.
7. T. Pevny, P. Bas, and J. Fridrich, Steganalysis by Subtractive Pixel Adjacency Matrix IEEE Trans. on Info. Forensics and Security, vol. 5(2), pp. 215-224, 2010.
8. T. Pevny and J. Fridrich, Merging Markov and DCT features for multiclass JPEG steganalysis, In E. J. Delp and P. W. Wong, editors, Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, volume 6505, pages 3 1–3 14, San Jose, CA, January 29–February 1, 2007.
9. J. Kodovsky, J. Fridrich, and V. Holub, Ensemble classifiers for steganalysis of digital media, IEEE Transactions on Information Forensics and Security, 2012.
10. Swets, John A.; Signal detection theory and ROC analysis in psychology and diagnostics : collected papers, Lawrence Erlbaum Associates, Mahwah, NJ, 1996.