ВИЯВЛЕННЯ СТЕГАНОГРАМ З ВИКОРИСТАННЯМ УНІВЕРСАЛЬНИХ СТАТИСТИЧНИХ МОДЕЛЕЙ КОНТЕЙНЕРУ

Прогонов Д. О.; Панічева Д. О.
Фізико-технічний інститут, Національний технічний університет України «Київський політехнічний інститут», м. Київ, Україна

Для приховання факту несанкціонованої передачі конфіденційних даних у інформаційно-комунікаційних системах (ІКС), наприклад, соціальних мережах, службах обміну мультимедійними даними, зловмисниками та терористами широко використовуються методи цифрової стеганографії [1]. В якості файлів-контейнерів для приховання повідомлень (стегоданих) найбільш часто використовуються мультимедійні дані, зокрема цифрові зображення (ЦЗ) [1, 2]. Вбудовування стегоданих в більшості випадків проводиться з використанням поширених (наприклад, двовимірного дискретного вейвлет перетворення (ДДВП)) та спеціальних (зокрема, сингулярного розкладу (СР)) методів обробки матриць яскравості пікселів ЦЗ, що дозволяє досягти компромісу між стійкістю прихованих повідомлень (стеганограм) до методів пасивного та активного стегоаналізу. Тому актуальною задачею є пошук ефективних методів виявлення стеганограм незалежно від області вбудовування стегоданих.

Для детектування факту наявності прихованих повідомлень у цифрові зображення широко використовуються методи статистичного стегоаналізу, зокрема статистичні моделі зображень-контейнерів (СМК) [1]. В роботах [3, 4] було показано, що застосування статистичних моделей ЦЗ в просторовій (модель SPAM) та частотній (модель CC-PEV) областях дозволяє з високою ймовірністю виявляти стеганограми, сформовані із використанням ДДВП зображення-контейнеру (ЗК). Ефективність цих моделей суттєво знижується у випадку використання СР матриць яскравості пікселів ЗК. Внаслідок цього становить інтерес застосування універсальних СМК для підвищення ймовірності виявлення стеганограм з даними, вбудованими з використанням СР матриць яскравості пікселів ЗК.

В роботі розглянуто випадок вбудовування стегоданих у ЦЗ з використанням СР матриць яскравості пікселів ЗК згідно методу Агарваля [5]. Формування стеганограм згідно цього методу проводиться шляхом додавання векторів сингулярних чисел матриць яскравості пікселів каналів кольору зображення-контейнеру Λ_I та стегоданих Λ_D, представлених у вигляді кольорових ЦЗ, з ваговим коефіцієнтом G, що залежить від енергії прихованих повідомлень:

$$\Lambda_S = \Lambda_I + G \times \Lambda_D, \tag{1}$$

де Λ_S – вектор сингулярних чисел заповненого ЗК.

Для виявлення стеганограм в роботі використовувалися стегодетекто-

ри SD_{SPAM}, SD_{CC-PEV} та SD_{CDF}, засновані на статистичних моделях ЗК для просторової (модель SPAM) та частотної (модель CC-PEV) областей [3, 4], а також їх об'єднання (універсальна) модель CDF [6].

Дослідження точності виявлення стеганограм, сформованих згідно методу Агарваля, при використанні статистичної моделі CDF проводилося на тестовому пакеті ЦЗ зі 9000 зображень псевдовипадковим чином вибраних зі стандартного пакету MIRFlickr-25k та масштабованих до однакового розміру 512×512 пікселів. В якості стегоданих були використані ЦЗ з різним ступенем деталізації: «Креслення» (567×463 пікселів), «Карта» (800×800 пікселів) та «Портрет» (565×850 пікселів). Ступінь заповнення ЗК стегоданими Δ_C (частка модифікованих сингулярних чисел ЗК) змінювалася від 5% до 25% з кроком 5% та від 25% до 95% з кроком 10%. Значення вагового коефіцієнту G у формулі (1) змінювалося від $G_{\min}=0.02$ (нижня границя відновлення стегоданих) до $G_{\max}=0.08$ (поява візуальних спотворень ЦЗ) з кроком $\Delta_G=0.02$.

У таблиці 1 наведені результати дослідження точності виявлення стеганограм (метрика Area-under-ROC curve (*AUC*) [7]), сформованих, згідно методу Агарваля, при використанні SD_{SPAM}, SD_{CC-PEV} та SD_{CDF} у випадку слабкого ($\Delta_C=10\%, AUC_{\min}$) при $G=G_{\min}$ та сильного ($\Delta_C=85\%, AUC_{\max}$) при $G=G_{\max}$ заповнення ЗК стегоданими.

Таблиця 1

Значення метрики *AUC* для статистичних стегодетекторів SD_{SPAM}, SD_{CC-PEV} та SD_{CDF} при виявленні стеганограм, сформованих згідно методу Агарваля, при слабкому ($AUC_{\min}$) та сильному ($AUC_{\max}$) заповненні ЗК стегоданими

Стегодетектор / Тип стегоданих	SD_{SPAM}		SD_{CC-PEV}		SD_{CDF}	
	$AUC_{\max}$	$AUC_{\min}$	$AUC_{\max}$	$AUC_{\min}$	$AUC_{\max}$	$AUC_{\min}$
«Креслення»	0.992	0.696	0.947	0.545	0.997	0.764
«Карта»	0.989	0.687	0.945	0.535	0.997	0.769
«Портрет»	0.979	0.697	0.890	0.536	0.992	0.755

За результатами аналізу отриманих даних встановлено, що точність виявлення стеганограм слабко залежить від типу прихованих повідомлень при використанні стегодетекторів SD_{SPAM}, SD_{CC-PEV} та SD_{CDF} (табл. 1). Використання універсальної статистичної моделі CDF дозволяє суттєво підвищити точність виявлення стеганограм (метрика *AUC*) у порівнянні зі статистичними моделями SPAM та CC-PEV, навіть у випадку слабкого заповнення ЗК стегоданими ($\Delta_C=10\%, AUC_{\min}$, табл. 1).

Перелік посилань

1. Fridrich J. Steganography in Digital Media: Principles, Algorithms and Applications. – 2010. – Cambridge University Press,New York, USA. – 437 p.

2. Конахович Г. Ф. Компьютерая стеганография. Теория и практика /

Конахович Г. Ф., Пузыренко А. Ю. – К.: "МК–Пресс", 2006. – 288 с.

3. Прогонов Д. Виявлення стеганограм з використанням комплексних статистичних моделей цифрових зображень / Прогонов Д., Панічева Д., Кущ С. – Матеріали IV-ої Міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем». – Львів: Українська академія друкарства, 2015. – с. 127-128.

4. Progonov D. Passive Steganalysis of Multidomain Embedding Methods / Progonov D., Kushch S. // International Journal "Information Theories & Applications". – Volume 22, Number 1. – 2015. – pp. 86-99.

5. Agarwal R. Digital watermarking in the singular vector domain / Agarwal R., Santhanam M.S. // International Journal of Image and Graphics. – 2008. – Volume 8, Issue 3. – pp. 351–362 – DOI 10.1142/S0219467808003131.

6. Kodovsky J. Modern steganalysis can detect YASS / Kodovsky J., Pevny T., Fridrich J. – Proc. SPIE 7541, Media Forensics and Security II. – San Jose, California, USA, 2010. – Ed. Memon Nasir D., Dittmann Jana, Alattar Adnan M., Delp Edward J. – pp. 1–11.

7. Murphy K. P. Machine Learning: A Probabilistic Perspective. – 1st Edition. – The MIT Press, 2012. – 1104 p.

Анотація

В роботі досліджена точність виявлення стеганограм, сформованих з використанням сингулярного розкладу матриць яскравості пікселів зображення-контейнеру, при застосуванні статистичних моделей цифрових зображень в просторовій (модель SPAM) та частотній (модель CC-PEV) областях, а також універсальної статистичної моделі CDF. Встановлено, що використання моделі CDF дозволяє суттєво підвищити точність виявлення стеганограм, у порівнянні з моделями SPAM та CC-PEV, навіть у випадку слабкого заповнення зображення-контейнеру стегоданими.

Ключові слова: статистичний стегоаналіз, сингулярний розклад.

Аннотация

В работе проведены исследования точности обнаружения стеганограмм, сформированных с применением сингулярного разложения матриц яркостей пикселей изображения-контейнера, при с использованием статистических моделей цифровых изображений в пространственной (модель SPAM) и частотной (модель CC-PEV) областях, а также универсальной статистической модели CDF. Показано, что использование модели CDF позволяет существенно повысить точность обнаружения стеганограмм, в сравнении с моделями SPAM и CC-PEV, даже в случае слабого заполнения изображения-контейнера стегоданными.

Ключевые слова: статистический стегоанализ, сингулярное разложение.

Abstract

The paper is devoted to analysis the accuracy of stego image detection by usage of statistical models the cover image in spatial (SPAM model) and frequency (CC-PEV) domains, as well as universal CDF model. It is considered the case of message hiding with usage of singular decomposition of cover image matrices. We demonstrate that usage of universal CDF model allows significantly improve the accuracy of stego image detection, even in case of low cover image payload.

Keywords: statistical steganalysis, singular decomposition.