УДК 004.8

Б.С.Крименюк
Л.М.Куперштейн

НЕЙРОМЕРЕЖЕВЕ МОДЕЛЮВАННЯ В ЗАДАЧІ СТЕГО-АНАЛІЗУ СТАТИЧНИХ JPEG-ЗОБРАЖЕНЬ

Вінницький національний технічний університет;

Анотація

Проведено огляд існуючих підходів та методик до стегоаналізу зображень. Було запропоновано та показано дієвість використання неройнних мереж для стегоаналізу.

Ключові слова: нейронні мережі, стеганографія, стегоаналіз, зображення, JPEG.

Abstract

An overview of existing methods of image steganalysis was conducted. It was proposed and demonstrated the effectiveness of the use of neural networks for steganalysis.

Keywords: neural networks, steganography, steganalysis, images, JPEG.

Вступ

Стегоаналіз стає все більш актуальним, оскільки застосування методів стеганографії поширюється серед терористів та кіберзлочинців. Про це може свідчити те що Лабораторія Касперського вперше випустила доповідь про застосування стеганографії у нападах на комп'ютерні системи саме у 2017 році [1]. До того застосування стеганографії кіберзлочинцями не вважалося проблемою з настільки руйнівними наслідками.

Приховування інформації злочинцями використовувалось і до 2017 року. Наприклад, вже у 2011 році терорист Аль-Каїди, якого було викрито у Німеччині, отримував інформацію про об'єкти наступних атак, що була прихована у порно-відео [2]. У 2013 році вийшла публікація управління ООН з наркотиків та злочинності у якій йшлося про те що стеганографія набуває поширення серед терористів з колумбійського угруповання ФАРК(Революційні збройні сили Колумбії — Армія Народу) [3].

З боку кіберпростору відомо що вади у соціальній мережі Instagram та операційній системі MacOS дають можливість зловмисникам перехопити керування комп'ютером користувача, коли той просто дивиться фотографії [4].

Серед недавніх кібератак стеганографія застосовувалась у наступних кібератаках: Microcin (AKA six little monkeys); NetTraveler; Zberp; Enfal (Zero.T); Shamoon; KinS; ZeusVM; Triton (Fibbit) [5].

Наведені вище приклади свідчать про актуальність проблеми та небезпеку стеганографії, яка на відміну від криптографії приховує сам факт передачі даних.

Результати дослідження

Методи стегоаналізу зображень поділяються на два основних види – спеціальні та універсальні [6].

Спеціальні методи націлені на конкретний алгоритм стеганографічного вбудовування. Ці методи аналізують зображення для знаходження вбудованого повідомлення і сконцентровані на якійсь властивості зображення або статистичних даних, які модифіковані цим стеганографічним алгоритмом.

Хоча спеціальні методи стеганалізу дають точні рішення при випробуванні тільки на конкретному, проте вони не можуть отримати дані приховані іншим методом і тим більше не можуть виявити дані приховані новим методом. Універсальні методи стегоаналізу долають недоліки спеціальних методів стегоаналізу.

Універсальні методи стегоаналізу можна представити як виявлення та класифікацію досліджуваного зображення як пустого або як такого що містить приховані дані. Загалом, класифікація складається з двох частин - виявлення ознак і класифікація шаблонів. Так як дані зображення, як правило, дуже великі, потребується представлення інформації в зображенні у меншій розмірності, по відношенню до виконуваної задачі. Властивість є таким низьковимірним представленням даних зображення і має велике значення у багатьох завданнях, пов'язаних з класифікацією, в тому числі у стегоаналізі. Кращі властивості для стегоаналізу повинні містити інформацію про зміни спричинені приховуванням інформації, а не про зміст зображення.

Гіпотеза полягає в тому що нейронні мережі завдяки можливості навчатися на нових прикладах можуть виявити повідомлення приховані іншими алгоритмами.

Для перевірки гіпотези було створено набір з 20 зображень, у якому10 зображень містили приховане пові-

домлення, а 10. Попередньо нейронна мережа була навчена на вибірці зі 100 зображень.

Нехай набір матриць 8х8 у зображенні N містить матриці N_p, що містять приховане повідомлення (належать до класу +), і матриці N_n – не містять (належать класу -). В результаті класифікації цих матриці, до класу + з прихованим повідомленням віднесені TP матриць, без прихованих – FP, до класу - правильно віднесені TN матриць, неправильно – FN.

Для оцінювання точності класифікатора вводяться наступні метрики:

Коефіцієнт дійсно позитивних оцінок (true positive ratio) – це відношення діагонального елемента і суми всіх елементів відповідного рядка. Тобто, яка частина передбачень цього класу була вірна. За змістом, це «влучність» класифікатора. Наскільки часто він потрапляє в факт, коли працює в даному класі.

$$TPR = \frac{TP}{TP + FN};$$

Коефіцієнт хибно позитивних оцінок (false positive ratio) – це те ж саме, але тільки для стовпця. Тобто, яка частка фактичних подій цього класу була правильно передбачена. За змістом, це «чутливість» класифікатора. На скільки він «відчуває» факт.

$$FPR = \frac{FP}{FP + TN};$$

TPR і FPR дають досить вичерпну характеристику класифікатора, причому «з різних кутів». Якщо намагатися підвищити FPR, роблячи класифікатор більш «оптимістичним», це призводить до падіння TPR через збільшення числа помилково-позитивних відповідей. Якщо ж змінювати класифікатор, роблячи його більш «песимістичним», наприклад, сильніше фільтруючи результати, то при зростанні TPR це викличе одночасне падіння FPR через відбракування якогось числа правильних відповідей. Тому зручно для характеристики класифікатора використовувати одну величину, так звану загальну точність (total accuracy)[7]:

$$TA = \frac{TP + TN}{TP + FN + FP + TN}$$

Результати тестування нейронної мережі наведено в табл. 1.

Таблиця 1 – Результати тестування нейронної мережі

№ Зображення	Правильно класифіковані		Неправильно класифіковані	
	TP	TN	FP	FN
1	+			
2	+			
3			+	
4	+			
5				+
6		+		
7		+		
8				+
9			+	
10	+			
11		+		
12	+			
13	+			
14	+			
15		+		
16		+		
17				+
18	+			
19		+		
20				+

На основі отриманих результатів тестування необхідно обрахувати метрики:

$$TPR = \frac{8}{8+2} = 0{,}8;$$

$$FPR = \frac{8}{8+4} = 0{,}66;$$

$$TA = \frac{8+6}{8+6+4+2} = 0.7$$

Отримані результати занесені до табл. 2.

Таблиця 2 – Оцінка системи при тестуванні нейронної мережі

Всього класифіковано	Правильно класифіковано	TPR, %	FPR, %	TA, %
20 зображень	14 зображень	80	66	70

Загальна точність класифікатора становить 70%, що свідчить про те що засіб виявляє приховані повідомлення з великим рівнем ймовірності, що перевищує статистичну похибку. При збільшенні навчальної та тестової вибірок прогнозується зростання точності.

Висновки

Проведено огляд існуючих підходів та методик до стегоаналізу зображень. Було продемонстровано можливість використання Запропоновано апаратну частину системи захисту Розумного Будинку. Розглянута схема є середньої складності й дозволяє забезпечити безпеку на належному рівні, також її можливо інтегрувати в систему Розумного будинку як складовий механізований елемент.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kaspersky Lab Identifies Worrying Trend in Hackers Using Steganography (23.01.2018) [Електронний ресурс]. Режим доступу: https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-identifies-worrying-trend-in-hackers-using-steganography
2. Steganography: how al-Qaeda hid secret documents in a porn video (19.12.2017) [Електронний ресурс]. Режим доступу: https://arstechnica.com/information-technology/2012/05/steganographyhow- al-qaeda-hid-secret-documents-in-a-porn-video/
3. United Nations Publication Describes Terrorist Use of Steganography (04.11.2017) [Електронний ресурс] Режим доступу: https://www.backbonesecurity.com/TerroristUse ofSteganography.aspx
4. Attack Uses Image Steganography For Stealthy Malware Ops On Instagram (13.09.2017) [Електронний ресурс] Режим доступу: https://www.darkreading.com/endpoint/attack-uses-image-steganographyfor- stealthy-malware-ops-on-instagram/d/d-id/1327170?
5. Steganography in contemporary cyberattacks (23.01.2018) [Електронний ресурс]. Режим доступу: https://securelist.com/steganography-in-contemporary-cyberattacks/79276/
6. L. Singh, R. Chhikara. A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted – International Journal of Engineering and Innovative Technology (IJEIT)Volume 3, Issue 4, October 2013 / L. Singh, R. Chhikara – ITM University, Gurgaon, Haryana, India.
7. Немного о Precision и Recall [Електронний ресурс]. – Режим доступу: http://blog.gramant.ru/2012/06/06/f1-measure/ – Назва з екрану.

Крименюк Борислав Сергійович — студент, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна, e-mail: krimenyukb@gmail.com

Науковий керівник:

Куперштейн Леонід Михайлович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна

Krymeniuk Boryslav— Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: krimenyukb@gmail.com

Supervisor:

Kupershtein Leonid — phd. Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, Ukraine