

МЕТОДИ СТЕГАНОГРАФІЧНОГО АНАЛІЗУ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ НЕЙРОННИХ МЕРЕЖ

Вінницький національний технічний університет

Анотація

Дослідження присвячені розгляду та аналізу сучасних підходів, які використовуються сьогодні для стегоаналізу зображень. Це особливо важливо в зв'язку з актуальністю проблеми захисту мереж від забороненої інформації, яку можна приховати у зображеннях.

Ключові слова: стеганографія, нейронні мережі, аналіз зображень, приховування інформації.

Abstract

The research is devoted to the review and analysis of modern approaches which are used today for steganalysis of images. This is important especially in relation with actual problem of protection of computer networks from forbidden data which can be hidden in images.

Key words: steganography, neural networks, image analysis, data hiding.

В даний час комп'ютерна стеганографія інтенсивно розвивається, застосовуються відомі і розробляються нові методи стеганографії, засновані на різноманітних областях науки. Стеганографічні системи переходять в нову фазу свого розвитку, сьогодні вже велика їх частина при приховуванні інформації враховує характеристики і природу стегоконтейнера, що містить дані. Важливим завданням стегоаналіза є визначення істотних властивостей стегоконтейнера, виявлення їх певних ознак, які задовольняли б вимогам репрезентативності і контекстної незалежності, і одночасно змінювалися б при вбудовуванні в контейнер додаткової інформації.

Постає проблема того, що цими системами можуть скористатися пірати, терористи, працівники ворожих спецслужб. Для пошуку прихованих повідомлень пропонується використовувати інтелектуальні технології, а саме нейронні мережі завдяки своїй здатності до навчання для розв'язання слабкоформалізованих задач. За останні кілька років нейронні мережі показали свою ефективність у багатьох застосуваннях. Штучні нейронні мережі є потужним інструментом аналізу даних та моделювання. Вони можуть знаходити і точно представляти як лінійні так і нелінійні взаємозв'язки, і є безцінним інструментом для апроксимуючих функцій, кластеризації даних і розпізнавання образів, які в іншому випадку непомітні[1].

У стеганографії із використанням зображень у якості контейнера використовується зображення. Для приховування інформації в такому підході використовуються властивості пікселів. Загалом, стеганографія у зображеннях класифікується за такими аспектами:

- а) ємність;
- б) помітність змін;
- в) робастність;
- г) стійкість до спотворення;
- д) складність обчислень.

Методи стегоаналізу засновані на використанні нейронних мереж малодосліджені. Вони використовують статистичні методи стегоаналізу в поєднанні з можливостями нейронних мереж до навчання та класифікації. Існуючі методи засновані на алгоритмах навчання з учителем. Аналіз літературних джерел показав, що для стегоаналізу використовуються в основному два типа нейронних мереж: зі зворотнім поширенням та прямого поширення [2-5] (табл. 1).

Як видно із табл. 1 комбінована нейронна мережа показала найкращі показники виявлення прихованих повідомлень, проте аналіз відбувався з різними наборами даних, також в основі кожного методу знаходилися різні способи аналізу зображень.

Таблиця 1 Порівняльна характеристика основних видів стегоаналізу на основі нейромереж

Вид стегоаналізу	Стегоаналіз перетворень	Вейвлетний стегоаналіз	Стегоаналіз текстури зображень
Тип нейронної мережі	Зі зворотним поширенням	Комбінована	Прямого поширення
Нейромережа використовується	Для класифікації	Для класифікації	Для обирання
Кількість методів приховування	Один	П'ять	Один
Кількість проаналізованих зображень	1000	1096	1000
Результати	Виявлено прихованих повідомлень:85.4% Виявлено відсутність прихованих повідомлень:75.0%	Виявлено прихованих повідомлень:98.7% Виявлено відсутність прихованих повідомлень:66.1%	Виявлено прихованих повідомлень:68.5% Виявлено відсутність прихованих повідомлень:99.1%

Тому на основі доступних складно сказати який з методів є ефективнішим. Крім того, точність класифікації досить далека від ідеальної чи прийнятної. Також в наукових дослідженнях щодо розв'язання задач стегоаналізу на основі нейронних мереж практично не зустрічаються самонавчаючі адаптивні системи. Це може бути пов'язано із неможливістю класичних мереж розв'язувати такі задачі або ж зі складністю формалізації задачі.

Для розв'язання задачі стегоаналізу пропонується застосовувати комплексний підхід як на основі статичних методів, так і з використанням інтелектуальних технологій. Якщо класичні методи досить детально досліджені то інтелектуальні, зокрема нейронні мережі, пропрацьовані значно менше. Оскільки задача сліпого стегоаналізу по визначенню не тільки наявності прихованих даних, але і певних характеристик самих даних, наприклад, місце розташування, розмір і т.п. відноситься до важко формалізованих багатопараметричних задач великої розмірності, то доцільним є розробка та застосування нових перспективних підходів. Одним із таких є глибокі нейронні мережі (глибоке навчання). Це частина більш широкого сімейства методів машинного навчання - навчання уявленням, де вектори ознак розташовуються відразу на безлічі рівнів [6]. Ці ознаки визначаються автоматично і пов'язують один з одним, формуючи вихідні дані. На кожному рівні представлені абстрактні ознаки, засновані на ознаках попереднього рівня. Таким чином, чим глибше ми просуваємося, тим вище рівень абстракції. У нейронних мережах безліч шарів являє собою безліч рівнів з векторами ознак, які генерують вихідні дані. Застосування такої технології для задач стегоаналізу може дати значні позитивні результати. Перевірці даного припущення і присвячені напрямки подальших наукових досліджень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Хайкин С. Нейронные сети: полный курс/ С. Хайкин; пер. с англ. – 2-е изд.– М.: ООО "И.Д. Вильямс", 2006. – 1104 с.
2. N.Kobsi, H.F.Merouani Neural Network Based Image Steganalysis: A Comparative Study / Journées Internationales sur l'Informatique Graphique, JIG'2007, Issue 3, pp.235-240
3. Liu Shaohui, Yao Hongxun, Gao Wen, "Neural Network Based Steganalysis in Still Images" — Proceedings of IEEE ICME, 2003.
4. Yun et al "Steganalysis Based on Moments of Characteristic Functions Using Wavelet Decomposition Prediction-Error Image and Neural Network" / Multimedia and Expo, 2005. Proc.IEEE
5. Patricia Lafferty, Farid Ahmed "Texture based steganalysis: results for color images" / Proc. SPIE, Mathematics of Data/Image Coding, Compression, and Encryption VII, with Applications (M. S. Schmalz) — August 2004, Volume 5561, pp. 145-151.
6. Yoshua Bengio. Learning deep architectures for ai. Foundations and TrendsSM in Machine Learning, 2(1):1–127, 2009.

Кривенюк Борислав Сергійович — студент групи ІБС-146, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, Україна

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

Krymeniuk Boryslav — Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University

Kupershtein Leonid — PhD, Associate Professor of Information Protection Chair, Vinnytsia National Technical University