УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 7 (2017), No. 1-2, pp. 96-102

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ СТЕГАНОАНАЛІТИЧНИХ АЛГОРИТМІВ ВИЯВЛЕННЯ НАЯВНОСТІ ВКЛАДЕНЬ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ У ЦИФРОВИХ ВІДЕО

Г.В. Ахмаметьєва, А.О. Єфименко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: a.v.akhmametieva@opu.ua

В роботі проводиться порівняльний аналіз ефективності алгоритмів для виявлення вкладень конфіденційної інформації у цифрових відео, що реалізують розроблені раніше автором стеганоаналітичні методи, з сучасними аналогами. Запропоновані алгоритми засновані на аналізі просторової області цифрових контентів, що дозволило уникнути додаткового накопичення обчислювальної похибки і, як наслідок, підвищити ефективність стеганоаналізу цифрових відео в умовах малих значень пропускної спроможності прихованого каналу зв'язку.

Ключові слова: стеганоаналіз, цифрові відео, аналіз ефективності

Вступ

Широке розповсюдження інформаційних технологій в усіх сферах суспільства сприяє накопиченню та зберіганню великих обсягів електронної інформації в різноманітних організаціях, підприємствах, державних установах, яка може містити конфіденційні відомості як окремих особистостей, так і державну та комерційну таємниці, які потребують захисту від розголошення та крадіжки, що може призвести до використання особистих даних шахраями, значних збитків для компаній тощо. Зокрема, крадіжка конфіденційних даних може здійснюватися за допомогою стеганографії, яка забезпечує передачу та зберігання секретної інформації у непомітному на перший погляд контейнері, в якості якого можуть виступати цифрові зображення, аудіо, відео. Використання певного виду контейнеру залежить від об'єму конфіденційних даних: дійсно, для передачі відносно невеликого повідомлення достатньо цифрового зображення, у випадку значного обсягу секретних даних перевага надається цифровим відео (ЦВ), адже стеганоповідомлення, яке є результатом вбудови додаткової інформації (ДІ) у контейнер, не повинно привертати увагу ні з точки зору непомітності для людського ока, ні з точки зору порушення статистичних характеристик самого контейнера, що часто забезпечується малими значеннями пропускної спроможності прихованого каналу зв'язку (ППС).

Використання ЦВ в якості контейнера в стеганографії має ряд переваг у порівнянні з цифровими зображеннями, зокрема за рахунок великої кількості кадрів можна передати значний обсяг даних навіть за умови малої ППС, що значно ускладнює процес стеганоаналізу, основною задачею якого є виявлення факту наявності або констатація відсутності прихованих даних у контейнері. Однак, незважаючи на зазначені переваги, стеганоаналіз цифрових відео менш розвинений, ніж стеганоаналіз цифрових зображень, що пояснюється складністю задачі і неспроможністю існуючих

підходів до її рішення. Тому розвиток і підвищення ефективності стеганоаналізу відео є важливою і актуальною задачею.

Для сучасних розробок в області стеганоаналізу відеопослідовностей [1-3] властиві наступні недоліки:

– спостерігається невисока ефективність виявлення стеганоповідомлень, сформованих при малих значеннях ППС, що обумовлено аналізом області перетворень цифрових контентів, перехід до якої супроводжується додатковим накопиченням обчислювальної похибки;

– авторами сучасних розробок в області відеостеганоаналізу експерименти, як правило, проводяться на основі малої кількості тестових відео (до 26 ЦВ), що ускладнює об'єктивну оцінку реального стану стеганоаналізу відео послідовностей;

– сучасні стеганоаналітичні розробки майже не розглядають питання покадрового аналізу ЦВ у випадку, коли вбудова ДІ здійснюється лише у частину кадрів відеопослідовності.

В роботах [4-7] були запропоновані ефективні стеганоаналітичні методи виявлення факту наявності/відсутності додаткової інформації у цифрових контентах: ЦВ [4-6] та цифрових зображеннях [7], які аналізують просторову область цифрових контентів, що дозволило уникнути додаткового накопичення обчислювальної похибки, завдяки чому були отримані високі результати виявлення стеганоповідомлень.

Метою роботи є проведення порівняльного аналізу ефективності стеганоаналітичних алгоритмів для цифрових відео, що реалізують розроблені раніше [4-7] стеганоаналітичні методи, з сучасними аналогами.

Основна частина

В основі стеганоаналітичних методів [4-6] лежить аналіз кількості блоків з однаковими значеннями яскравості в матрицях колірних складових цифрових контентів. Було встановлено, що $n \times n$-блоки виду

$$A = \begin{pmatrix} a & a & \dots & a \\ a & a & \dots & a \\ \dots & \dots & \ddots & \dots \\ a & a & \dots & a \end{pmatrix}, \quad a \in \{1,2,3,...,255\}, \tag{1}$$

мають єдине ненульове сингулярне число $\sigma_1 > 0, \sigma_2 = \dots = \sigma_n = 0,$ причому таке, що належить множині натуральних чисел ($\sigma_1 \in \mathrm{N}$) і кратне розміру блока n ($\sigma_1 \vdots n$). Така особливість є чутливою до малих збурень, адже в загальному випадку сингулярні числа для довільної матриці є невід'ємними дійсними числами [8]. Зміна лише одного елементу матриці (1), яка може виникнути в результаті стеганоперетворення, призведе до того, що $\sigma_1 \notin \mathrm{N}$. На основі встановленої особливості збурення єдиного ненульового сингулярного числа σ_1 $n \times n$-блоків виду (1) визначено відповідність між областю сингулярного розкладання відповідних матриць та просторовою областю цифрових контентів, що не тільки дозволило уникнути додаткового накопичення обчислювальної похибки, а й додаткових обчислювальних витрат, пов'язаних з переходом в область перетворень і назад, при розробці стеганоаналітичних алгоритмів.

Стеганоаналітичний метод [4] та його удосконалення [5] засновані на аналізі відносної (по відношенню до загальної кількості $n \times n$-блоків у матриці колірної складової кадру ЦВ) кількості блоків з однаковими значеннями яскравості в матрицях цифрових контентів в результаті первинного і повторного стеганоперетворення, що

обумовлено гіпотезою, що кількість $n \times n$-блоків виду (1) у стеганоповідомленні буде незначною (можливо такі блоки будуть відсутні), що призведе до малих значень відносної кількості таких блоків після повторної вбудови ДІ у порівнянні з первинною вбудовою ДІ. Основні кроки алгоритму САА1, що реалізує запропонований метод, співпадають з наведеними в [4-5] при порогових значеннях $T_R = 27.5$, $T_G = 19.5$, $T_B = 11.5$ для ЦВ в форматі з втратами, $T_R = 1.6$, $T_G = 1.7$, $T_B = 1.6$ для ЦВ в форматі без втрат.

Метод, розроблений в [6], заснований на врахуванні характеру зміни кількості блоків з однаковими значеннями яскравості в результаті первинного і повторного стеганоперетворення. Встановлено, що в результаті первинної вбудови ДІ у більшості матриць колірних складових кадрів ЦВ (не залежно від формату оригінального контейнеру) спостерігається зменшення кількості блоків з однаковими значеннями яскравості (аж до 0, особливо, якщо ППС при первинній вбудові ДІ складала 0.25-0.5 біт/піксель), а в результаті повторної вбудови ДІ у стеганоповідомлення – або незначне збільшення таких блоків, або їх незмінність. Основні кроки алгоритму САА2, що реалізує розроблений метод, співпадають з наведеними в [6] при пороговому значенні $T = 3$. Даний алгоритм, на відміну від САА1, дозволив ефективно виявляти стеганоповідомлення, сформовані вбудовою ДІ у ЦВ з малим розміром кадрів при значеннях ППС, не менше 0.167 біт/піксель.

В роботі [7] запропонований стеганоаналітичний алгоритм (далі САА3) виявлення стеганоповідомлень, сформованих вбудовою ДІ лише в одну будь-яку колірну складову цифрових зображень в форматі з втратами, заснований на врахуванні кількості послідовних тріад колірних триплетів в матриці унікальних кольорів UCT розміром $U \times 3$, яка містить унікальні колірні триплети (r_i, g_i, b_i), $i = \overline{1,U}$, що містяться в зображенні. Розроблений алгоритм був адаптований для ЦВ (САА3v), для аналізу окремих кадрів відео послідовності слід використовувати алгоритм САА3, основні кроки якого наведені в [7].

Для оцінки ефективності розроблених алгоритмів були проведені обчислювальні експерименти для 200 відеопослідовностей розміром кадру 320×240, отриманих камерами мобільних пристроїв, з розширенням *.3gp або *.mp4 (при стиску використовуються кодеки H.263 або H.264) – набір 1, та 167 відео послідовностей розміром кадру 320×240, отриманих відеокамерою з розширенням *.avi (при стиску використовується кодек Xvid) – набір 2. По результатам експериментів, направлених на апробацію розроблених алгоритмів, були визначені помилки першого та другого роду, наведені в табл. 1.

З табл. 1 видно, що найкращі результати детектування наявності ДІ досягаються методом САА3v, однак, як було зазначено вище, даний алгоритм може використовуватися лише у випадку, коли ДІ вбудовується лише в одну колірну складову кольорових контейнерів. На відміну від САА3v, алгоритми САА1 та САА2 можуть використовуватися як для кольорових ЦВ, так і ЦВ в градаціях сірого, крім того вони спроможні виявляти наявність ДІ, вбудованої у дві або три колірні складові, оскільки аналіз колірних матриць відбувається окремо для кожної колірної складової.

Порівняльний аналіз ефективності розроблених алгоритмів САА1, САА2, САА3v та САА3 для виявлення вкладень ДІ в окремих кадрах ЦВ з сучасними аналогами здійснюється шляхом оцінки точності детектування AD, що характеризує долю правильно виявлених подій [9-11]:

$$AD = \frac{TP + TN}{TP + FN + TN + FP}, \qquad (2)$$

де FN – помилки першого роду; FP – помилки другого роду; TP – відсоток правильно виявлених стеганоповідомлень, $TP = 100 - FN$; TN – відсоток правильно виявлених незаповнених контейнерів, $TN = 100 - FP$.

Таблиця 1.

Ефективність детектування вкладень ДІ у ЦВ алгоритмами CAA1, CAA2, CAA3v, %

Алгоритм	Помилки	ППС, біт/піксель					
		0.5	0.25	0.167	0.125	0.1	0.05
ЦВ з набору 1							
CAA1	1-го роду	0	0	2.19	11.68	51.09	90.88
	2-го роду	0.36	0.36	0.36	0.36	0.73	6.14
CAA2	1-го роду	0	0	0	64.23	97.08	100
	2-го роду	0	0	0	0	0	0
CAA3v	1-го роду	0	0	0	0.73	2.19	32.12
	2-го роду	0	0	0	0	0	0
ЦВ з набору 2							
CAA1	1-го роду	0	0	19.56	98.26	100	100
	2-го роду	0	0	0	0	0	0
CAA2	1-го роду	0	0	0	80	100	100
	2-го роду	0	0	0	0	0	0
CAA3v	1-го роду	0	0	0	0	0	10
	2-го роду	0	0	0	0	0	0

Для порівняльного аналізу ефективності розроблених стеганоаналітичних алгоритмів, направлених на виявлення наявності/відсутності ДІ в ЦВ, використовуються ефективні сучасні аналоги:

- $V1$ (2005) [12] (10 відео по 124 кадри);
- $V2$ (2005) [13] (10 відео по 124 кадри);
- $V3$ (2007) [1] (10 відео по 124 кадри);
- $V4$ (2013) [2] (9 відео по 150-300 кадрів);
- $V5$ (2015) [3] (26 відео по 100 кадрів).

У дужках представлена інформація про обсяг обчислювальних експериментів, що використовувались авторами відповідних алгоритмів при оцінці їх ефективності. Результати порівняння точності детектування AD розроблених стеганоаналітичних алгоритмів для 367 ЦВ з наборів 1-2 з обраними аналогами наведені в табл. 2, при цьому ДІ вбудовувалась в одну постійну колірну складову всіх кадрів ЦВ.

В результаті порівняння значень точності детектування AD (табл. 2) можна зробити висновок, що розроблені стеганоаналітичні алгоритми є ефективнішими, ніж сучасні аналоги. Якщо вбудова ДІ здійснювалась з ППС 0.167-0.5 біт/піксель, алгоритмами CAA3v і CAA2 досягнутий абсолютний результат для точності детектування $AD = 1$. У випадку малих значень ППС найбільш ефективним є алгоритм CAA3v: результати детектування за допомогою CAA3v на 2.3% перевищують аналог $V5$ і більше ніж на 10% аналоги $V1 - V3$ (для ППС 0.1 біт/піксель). Найбільше підвищення ефективності досягається при виявленні вкладень ДІ, вбудованої зі значеннями ППС, меншими за 0.1 біт/піксель: точність детектування CAA3v на 14.93% перевищує аналог $V4$ при значенні ППС 0.0625 біт/піксель; у випадку ППС 0.05 біт/піксель сучасні аналоги навіть не тестувалися, для алгоритму CAA3v точність детектування складає $AD = 0.9391$. Точність детектування алгоритмів CAA1 і CAA2 при ППС 0.125 біт/піксель і менше нижче аналогів, оскільки порівняльний аналіз враховує результати аналізу ЦВ з наборів 1 і 2, однак у випадку використання CAA1 для стеганоаналізу ЦВ, отриманих камерами мобільних пристроїв (набір 1), точність

детектування при ППС 0.125 біт/піксель досягає $AD = 0.94$, що на 1.2% перевищує аналог $V4$.

Таблиця 2.

Порівняння AD для розроблених стеганоаналітичних методів і сучасних аналогів

ППС, біт/піксель	$V1$ 2005 (10)	$V2$ 2005 (10)	$V3$ 2007 (10)	$V4$ 2013 (9)	$V5$ 2015 (26)	CAA1 (367)	CAA2 (367)	CAA3v (367)
0.5	0.925	0.955	0.98	1	0.9991	0.9991	**1**	**1**
0.4	0.885	0.94	0.97	–	–	0.9991	**1**	**1**
0.3	0.825	0.92	0.945	–	–	0.9991	**1**	**1**
0.25	–	–	–	0.996	0.9988	0.9991	**1**	**1**
0.2	0.68	0.875	0.925	–	–	0.9691	**1**	**1**
0.167	–	–	–	–	–	0.9537	**1**	**1**
0.125	–	–	–	0.928	–	0.7757	0.7530	**0.9991**
0.1	0.555	0.755	0.89	–	0.9744	0.7139	0.6703	**0.9973**
0.0625	–	–	–	0.794	–	0.5157	0.5	**0.9433**
0.05	–	–	–	–	–	0.5074	0.5	**0.9391**

Для випадку, коли вбудова ДІ здійснюється лише в деякі окремі кадри ЦВ (часткова вбудова), проводиться покадровий аналіз ЦВ за допомогою алгоритму CAA3. Результати порівняння ефективності алгоритму CAA3 з єдиним сучасним аналогом $V5$, для якого наводяться результати покадрового аналізу ЦВ, в умовах часткової вбудови ДІ наведені в табл. 3.

Таблиця 3.

Порівняння AD для стеганоаналітичного алгоритму CAA3 і сучасного аналогу $V5$ за умови часткового заповнення кадрів ЦВ

ППС окремих кадрів ЦВ, біт/піксель	Кількість заповнених кадрів							
	80%		60%		40%		20%	
	$V5$ 2015 (26)	CAA3 (367)	$V5$ 2015 (26)	CAA3 (367)	$V5$ 2015 (26)	CAA3 (367)	$V5$ 2015 (26)	CAA3 (367)
0.5	1	1	0.9978	1	1	1	0.9932	1
0.25	1	1	1	1	0.9926	1	0.9843	0.9999
0.167	–	0.9998	–	0.9998	–	0.9998	–	0.9999
0.125	–	0.9959	–	0.9948	–	0.9948	–	0.9991
0.1	0.9381	0.9897	0.9276	0.9867	0.7974	0.9867	0.6688	0.9974
0.05	–	0.9232	–	0.9048	–	0.9048	–	0.9811

З табл. 3 видно, що у випадку часткової вбудови ДІ розроблений алгоритм CAA3 (стосовно до кадрів ЦВ) значно ефективніше сучасного аналогу $V5$ при вбудові ДІ з малою ППС: при ППС 0.1 біт/піксель при степені заповнення кадрів 60-80% результати CAA3 на 5.5% перевищують аналог $V5$, при степені заповнення кадрів 40% і 20% відповідно на 18% і 32%. В умовах ППС 0.05 біт/піксель сучасний аналог не тестувався, однак для алгоритму CAA3 при будь-якій степені заповнення кадрів точність детектування перевищує 0.9, що є досить високим результатом.

Висновки

В роботі проведено порівняльний аналіз алгоритмів, що реалізують розроблені раніше стеганоаналітичні методи, з сучасними аналогами. Показано, що розроблені алгоритми є ефективнішими за сучасні аналоги, особливо при значеннях ППС 0.167 біт/піксель та вище. Для менших значень ППС найбільш ефективним є алгоритм CAA3 та його адаптація CAA3v, які дозволяють ефективно виявляти вкладення ДІ навіть при ППС 0.05-0.1 біт/піксель. Проведено покадровий аналіз ЦВ, в результаті якого також отримані високі результати детектування стеганоповідомлень.

Отримані результати підтверджуються масштабними обчислювальними експериментами, які дозволили отримати об'єктивно високу оцінку для розроблених стеганоаналітичних методів.

Результати отриманих оцінок ефективності алгоритмів, що реалізують розроблені методи, та аналіз області застосування розроблених методів на основі отриманих помилок першого та другого роду дозволяють розробити комплексний метод виявлення вкладень ДІ у ЦВ, такий, що аналізує просторову область цифрових контентів та спроможний ефективно виявляти стеганоповідомлення, сформовані за різних умов вбудови ДІ.

Список літератури

1. Vinod Pankajaksan. Improving video steganalysis using temporal correlation / Vinod Pankajaksan, A.T.S. Ho // Third international conference on intelligent information hiding and multimedia signal processing, 2007. – Vol. 1. – Pp. 287-290.
2. Songbin Li. Detection of Information Hiding by Modulating Intra Prediction Modes in H.264/AVC / Songbin Li, Peng Liu, Qiongxing Dai, Xiuhua Ma, Haojiang Deng // Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013). – Pp. 590-593.
3. Kaicheng Wu. Research of Video Steganalysis Algorithm Based on H265 Protocol / Kaicheng Wu // MATEC Web of Conferences 25, 2015. – Pp. 03003-1 - 03003-7.
4. Кобозева, А.А. Стеганоаналитеческий метод для цифровых контейнеров, хранящихся в формате без потерь / А.А. Кобозева, А.В. Ахмаметьева, А.А. Ефименко // Інформаційна безпека. – 2014. – №1(13). – С. 31-42.
5. Ахмаметьева, А.В. Усовершенствование стеганоаналитического метода, основанного на анализе пространственной области цифровых контейнеров / А.В. Ахмаметьева // Інформатика та математичні методи в моделюванні. – 2015. – Т.5. – № 4. – С. 367-375.
6. Маєвський, Д.А. Стеганоаналітичний алгоритм, заснований на аналізі просторової області цифрових контейнерів / Д.А. Маєвський, Г.В. Ахмаметьєва // Інформатика та математичні методи в моделюванні. – 2016. – Т.6. – №1. – С. 52-60.
7. Ахмаметьева, А.В. Стеганоанализ цифровых изображений, хранящихся в формате с потерями / А.В. Ахмаметьева // Захист інформації. – 2016. – Випуск 23. – С.135-145.
8. Деммель, Дж. Вычислительная линейная алгебра. Теория и приложения. / Дж. Деммель. – Пер. с англ. – М.: Мир, 2001. – 430 с.
9. Fawcett, T. An introduction to ROC analysis / Tom Fawcett // Pattern Recognition Letters. – 2006. – No. 27. – Pp. 861–874.
10. Bin Li. A Survey on Image Steganography and Steganalysis / Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi // Journal of Information Hiding and Multimedia Signal Processing. – 2011. – Vol. 2. – No. 2. – Pp. 142-172.
11. Receiver operating characteristic [Electronic resource] // From Wikipedia, the free encyclopedia. On-line: https://en.wikipedia.org/wiki/Receiver_operating_characteristic
12. Xuan, G. Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions / G. Xuan // Lecture Notes in Computer Science – 2005. – Vol. 3727. – Pp. 262–277.
13. Shi, Y.Q. Steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network / Y.Q. Shi, G. Xuan, D. Zou, J. Gao, C. Yang, Z. Zhang, P. Chai, W. Chen, C. Chen // Proceedings of the IEEE International Conference on Multimedia and Expo, July 2005. – 4 p.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ СТЕГАНОАНАЛИТИЧЕСКИХ АЛГОРИТМОВ ВЫЯВЛЕНИЯ НАЛИЧИЯ ВЛОЖЕНИЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ЦИФРОВЫХ ВИДЕО

А.В. Ахмаметьева, А.А. Ефименко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: a.v.akhmametieva@opu.ua

В работе проводится сравнительный анализ эффективности алгоритмов для выявления вложений конфиденциальной информации в цифровых видео, реализующих разработанные ранее автором стеганоаналитические методы, с современными аналогами. Предложенные алгоритмы основаны на анализе пространственной области цифровых контентов, что позволило избежать дополнительного накопления вычислительной погрешности и, как следствие, повысить эффективность стеганоанализа цифровых видео в условиях малых значений пропускной способности скрытого канала связи.
Ключевые слова: стеганоанализ, цифровые видео, анализ эффективности

COMPARATIVE EFFICIENCY ANALYSIS OF STEGANALYTIC ALGORITHMS FOR DETECTING THE PRESENCE OF ATTACHMENTS OF CONFIDENTIAL INFORMATION IN DIGITAL VIDEO

A.V. Akhmametieva, A.A. Efimenko

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: a.v.akhmametieva@opu.ua

The paper presents a comparative efficiency analysis of algorithms for detecting the presence of attachments of confidential information in digital video, that implement the author's previously developed steganalytic methods, with modern analogs. Proposed algorithms are based on the analysis of the spatial domain of digital contents, that allowed to avoid additional accumulation of computational error and, as a result, to increase the efficiency of steganalysis of digital video in conditions of low hidden capacity.
Keywords: steganalysis, digital video, efficiency analysis