УДК 004.056.5 **DOI:10.30837/rt.2021.2.205.03**

О.О. КУЗНЕЦОВ, д-р техн. наук, А.В. КОНОНЧЕНКО

СТЕГАНОГРАФІЧНІ МЕТОДИ В ВЕКТОРНІЙ ГРАФІЦІ

Вступ

Приховування інформаційних повідомлень у різні надмірні дані (так звані контейнери, носії, cover-файли, тощо) вивчається стеганографією [1 – 3]. Тобто метою стеганографічних методів є приховування факту існування інформаційних повідомлень [4, 5]. Контейнери (зображення, аудіо, відео, тексти, тощо) передаються відкритими каналами (наприклад, через Інтернет), але не викликають ні в кого підозр. В той же час вповноважена особа, що знає таємний ключ, може витягти приховані дані, тобто відновити інформаційне повідомлення [1 – 3].

Найбільш вдалим для проведення стеганографічних перетворень є формат векторної графіки SVG [6], який завдяки своїй структурі дозволяє легко маніпулювати об’єктами, з яких складається. Його широка підтримка різними платформами також дозволяє підвищити рівень скритності при проведенні передачі секретних даних шляхом передачі звичайних на перший погляд файлів медіа.

Існуючі наукові публікації з методів приховування інформаційних повідомлень стосуються переважно растрової графіки, а роботи щодо векторної в основному полягають у кодуванні відстаней між геометричними об’єктами, що містяться у зображенні, або створенні додаткових точок [7 – 10]. Усі методи вбудовування у векторні зображення мають вразливість до атак афінного перетворення [11, 12].

Найпоширенішими видами афінних перетворень є операції перенесення, повороту, зсуву та масштабування з можливими варіаціями (зсуву за осями абсцис та ординат, масштабування пропорційне та непропорційне, зі стисненням та із розширенням) [13, 14].

Більшість методів вбудовування інформації у векторні зображення забезпечують одноразову стійкість до афінних перетворень, при цьому при повторному накладенні операцій зміни положення об’єктів, повідомлення може зруйнуватися взагалі. Запропоновані у [11, 12] способи приховування даних можуть реалізувати більший рівень стійкості до різного роду перетворень при їх багаторазовому проведенні.

Метою цієї статті є вивчення технік приховування повідомлень в векторні зображення з [11, 12] та експериментальні дослідження стійкості до афінних атак.

Афінні перетворення для реалізації стеганоатак

Афінні перетворення найбільш імовірно можуть бути використані для реалізації стеганоатак, тобто як спосіб руйнування прихованого повідомлення. Так, у загальному випадку афінне перетворення відбувається наступним чином [13, 14]:

$$\begin{bmatrix} a & b & c \\ d & e & f \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} ax+by+c \\ dx+ey+f \\ 1 \end{bmatrix}. \quad (1)$$

При відповідних коефіцієнтах над координатами точок, що піддаються операції, відбувається перетворення, що призводить до зміни положення геометричного об’єкта на полотні. Так, основними афінними перетвореннями є перенесення, поворот, зсув та масштабування (рис. 1). При цьому зсув може відбуватися за осями абцис та ординат, а масштабування може бути пропорційним та непропорційним, зі стисненням та розширенням.

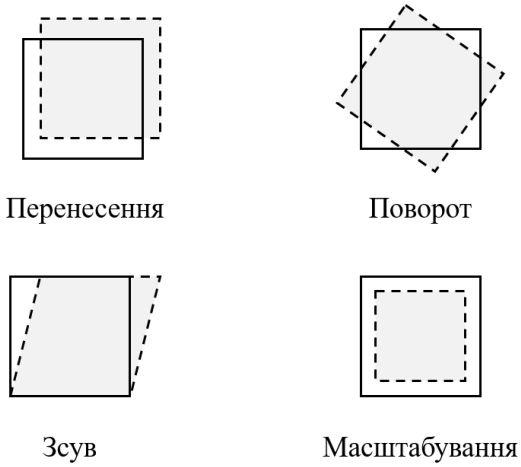

Рис. 1. Основні види афінних перетворень

Вираз (1) для різних випадків може бути записаний наступним чином [12]:

- операція перенесення:

$$\begin{bmatrix} 1 & 0 & c \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} x+c \\ y+f \\ 1 \end{bmatrix}; \tag{2}$$

- операція повороту:

$$\begin{bmatrix} \cos(\alpha) & -\sin(\alpha) & 0 \\ \sin(\alpha) & \cos(\alpha) & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \\ = \begin{bmatrix} x\cos(\alpha) - y\sin(\alpha) \\ x\sin(\alpha) + y\cos(\alpha) \\ 1 \end{bmatrix}; \tag{3}$$

- операція зсуву за віссю абсцис:

$$\begin{bmatrix} 1 & b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} x+by \\ y \\ 1 \end{bmatrix}; \tag{4}$$

- операція зсуву за віссю ординат:

$$\begin{bmatrix} 1 & 0 & 0 \\ d & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} x \\ dx+y \\ 1 \end{bmatrix}; \tag{5}$$

- операція масштабування:

$$\begin{bmatrix} a & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} ax \\ ey \\ 1 \end{bmatrix}; \tag{6}$$

- операція майже афінного перетворення з додаванням шуму:

$$\begin{bmatrix} a+n_1 & b+n_2 & 0 \\ d+n_3 & e+n_4 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x+n_5 \\ y+n_6 \\ 1 \end{bmatrix} = \\ = \begin{bmatrix} (a+n_1)(x+n_5)+(b+n_2)(y+n_6) \\ (d+n_3)(x+n_5)+(e+n_4)(y+n_6) \\ 1 \end{bmatrix}. \quad (7)$$

Більшість відомих стеганографічних технік над векторними зображеннями не забезпечують стійкості до поширених видів афінних перетворень при їх багаторазовому застосуванні на контейнері. Наведені результати останніх досліджень Кінзяревого [11, 12] пропонують стійкість до афінних перетворень при їх повторному накладанні. Саму тому тематикою роботи є аналіз запропонованих технік та їх експериментальні дослідження.

Методика досліджень

В роботах [11, 12] запропоновано два методи приховування інформації у векторні зображення (побітовий метод та метод паттернів). Для проведення експериментальних досліджень в роботі програмно реалізовано обидва методи із рекомендованими автором параметрами.

Дослідження стійкості до афінних перетворень виконувалось програмним чином, використовуючи формули (2) – (7). Спочатку реалізовується операція вбудовування інформації довжиною 2400 біт у контейнер. Потім над закодованим контейнером відбувається певне афінне перетворення і виконується спроба вилучити повідомлення. Для наступного перетворення використовуватиметься стегоконтейнер, отриманий на попередньому кроці. Таким чином забезпечується багаторазове накладання операції зміни положення координат на одне й теж ж саме зображення.

Згідно з формулами (2)-(7) для перетворень використовуються такі коефіцієнти:

- перенесення – $(c, f) \in [-500, 500]$;
- поворот – $\alpha = 1$;
- зсув за віссю абсцис – $b = 0,01$;
- зсув за віссю ординат – $d = 0,01$;
- масштабування для стиснення – $a = e = 0,99$;
- масштабування для розширення – $a = e = 1,01$;
- майже афінне перетворення повороту з додаванням шуму:

$$a = \cos(\alpha),\ b = -\sin(\alpha),\ d = \sin(\alpha),\ e = -\cos(\alpha),\ \alpha = 1,\ n_1 = n_4 = n_6 = -0,0001,$$
$$n_2 = n_3 = n_5 = 0,0001.$$

Такі ж самі дослідження було проведено у дисертаційній роботі [12]. Нашою метою була вибіркова перевірка отриманих результатів.

При проведенні наших експериментів операції приховування та вилучення виконуються з різними наборами значень кількості біт, що вбудовуються в одну криву, точності розрахунку координат та похибки відтворення. Вихідні дані для проведення експериментів наведено у табл. 1.

Таблиця 1

Вхідні дані для експериментальних досліджень

Номер експерименту	Біт/крива	Точність	Похибка
e_1	40	5	0,0002
e_2	40	5	0,0004
e_3	40	6	0,0002
e_4	40	6	0,0004
e_5	60	5	0,0002
e_6	60	5	0,0004
e_7	60	6	0,0002
e_8	60	6	0,0004
e_9	80	5	0,0002
e_{10}	80	5	0,0004
e_{11}	80	6	0,0002
e_{12}	80	6	0,0004

Накладання перетворень виконувались 10 раз на кожен попередній контейнер. Зміна кроку для побітового методу дорівнює 0.0005, для побітового методу початковий крок дорівнює 0,0005, а довжина паттерну – 4.

Результати експериментів

Отримані результати зображено на рис. 2 – 15, на яких відображені графіки залежності відсотка втрачених біт від експерименту при проведенні різних перетворень. По шкалі абсцис наведено кількість послідовно виконаних тих самих перетворень.

Графіки на рис. 2, 3 відповідають перетворенню перенесення. Кожний контейнер набував нового вигляду шляхом послідовного додавання до координат значень від -500 до 500 з кроком 100. Побітовий метод продемонстрував високі показники стійкості (рис. 2) – з 12 експериментів лише при першому та дев'ятому експериментах було втрачено невеликий відсоток інформаційних бітів. Метод паттернів у більшості випадків також стійкий до перенесення, при цьому при п'ятому, дев'ятому та десятому експериментах показники втрат досягають 30 – 40 %.

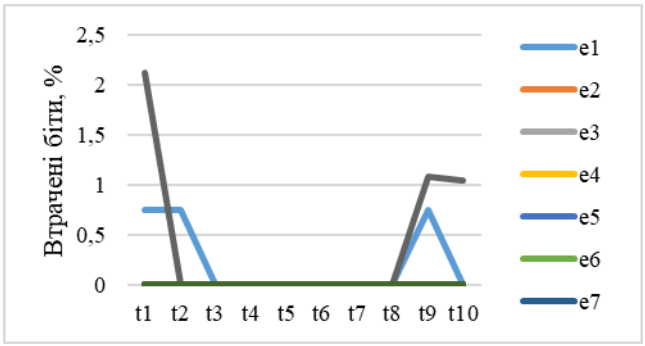

Рис. 2. Результати вилучення інформації з контейнерів після перетворення перенесення побітовим методом

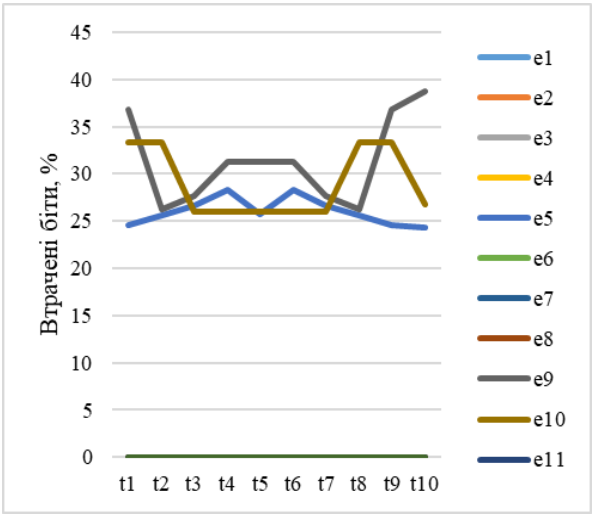

Рис. 3. Результати вилучення інформації з контейнерів після перетворення перенесення методом пат тернів

На рис. 4, 5 відображені графіки залежності відсотка втрачених біт від експерименту при проведенні перетворення повороту. У цьому випадку контейнер поступово повертався на один градус десять разів. Для побітового методу при найнесприятливіших параметрах досягається втрата бітів у приблизно 45 %, а для методу паттернів – 100 %.

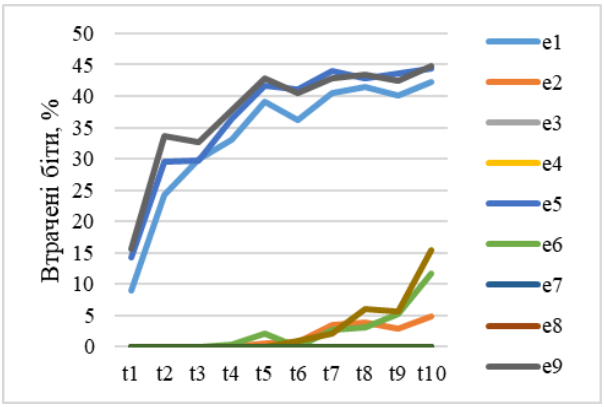

Рис. 4. Результати вилучення інформації з контейнерів після перетворення повороту побітовим методом

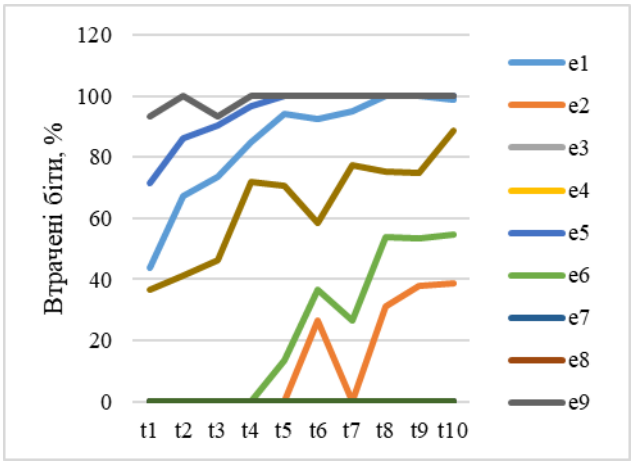

Рис. 5. Результати вилучення інформації з контейнерів після перетворення повороту методом паттернів

На рис. 6, 7 відображені графіки залежності відсотка втрачених біт від експерименту при проведенні перетворення зсуву за віссю абсцис. При цьому *x*-координата змінюється у 0,01 раз, забезпечуючи поступовий зсув контейнера. Для побітового методу при найнесприятливіших параметрах досягається втрата бітів у приблизно 45 %, а для методу паттернів – 100 %.

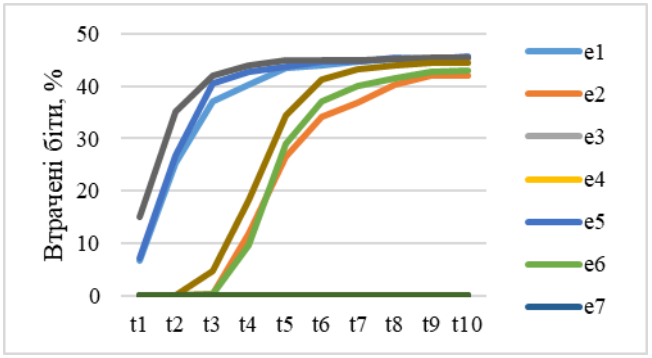

Рис. 6. Результати вилучення інформації з контейнерів
після перетворення зсуву за віссю абсцис побітовим методом

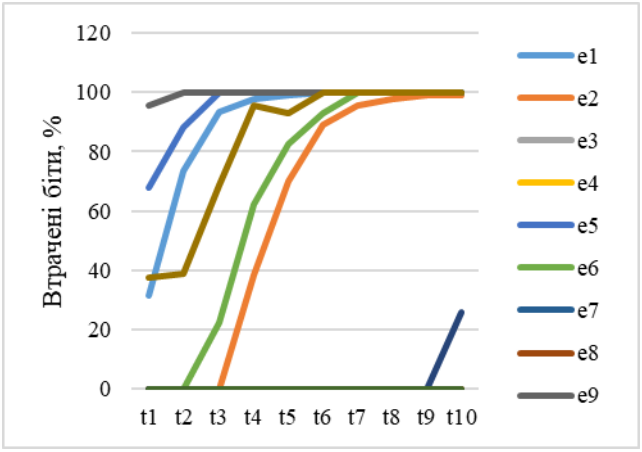

Рис. 7. Результати вилучення інформації з контейнерів
після перетворення зсуву за віссю абсцис методом паттернів

На рис. 8, 9 відображені графіки залежності відсотка втрачених біт від експерименту при проведенні перетворення зсуву за віссю ординат. При цьому y-координата змінюється у 0,01 раз, забезпечуючи поступовий зсув контейнера. Для побітового методу при найнесприятливіших параметрах досягається втрата бітів у приблизно 46 %, а для методу паттернів – 100 %.

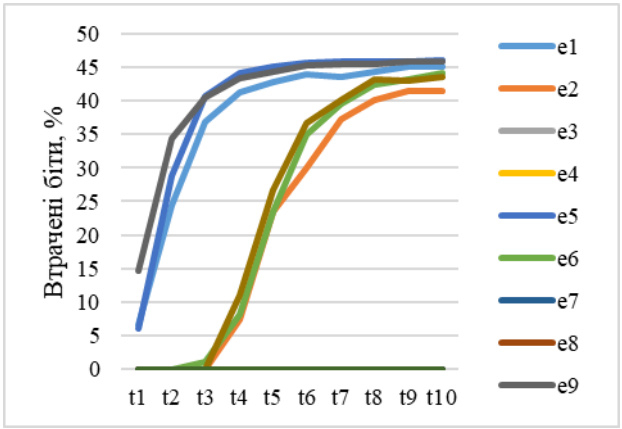

Рис. 8. Результати вилучення інформації з контейнерів
після перетворення зсуву за віссю ординат

побітовим методом

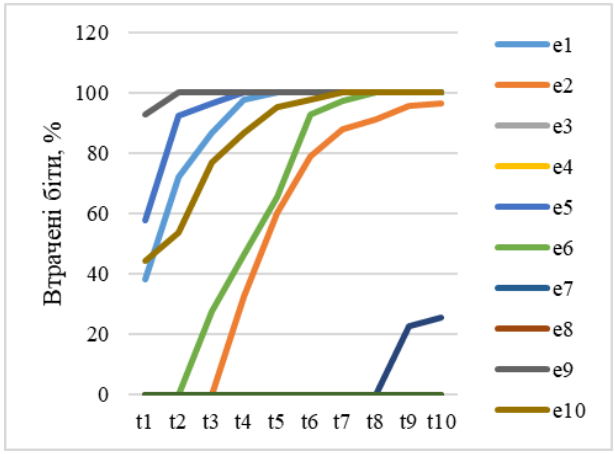

Рис. 9. Результати вилучення інформації з контейнерів
після перетворення зсуву за віссю ординат методом паттернів

На рис. 10, 11 відображені графіки залежності відсотка втрачених біт від експерименту при проведенні перетворення масштабування для стиснення. При цьому кожна координата змінюється у 0,99 раз, забезпечуючи поступове стиснення контейнера. Для побітового методу при найнесприятливіших параметрах досягається втрата бітів у приблизно 44 %, а для методу паттернів – 100 %.

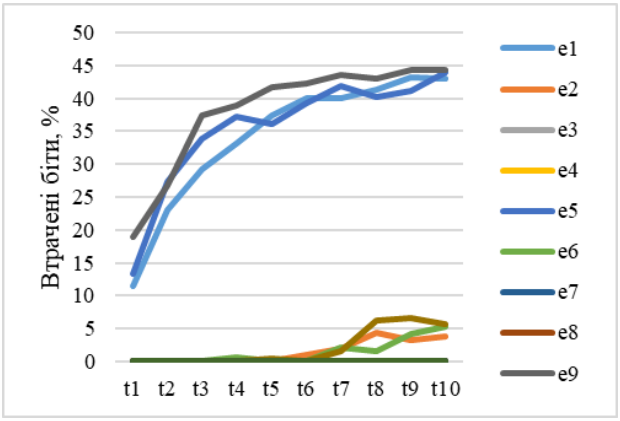

Рис. 10. Результати вилучення інформації з контейнерів
після перетворення масштабування для стиснення побітовим методом

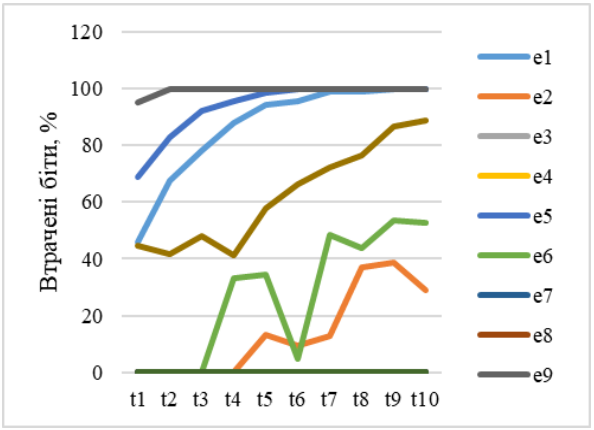

Рис. 11. Результати вилучення інформації з контейнерів
після перетворення масштабування для стиснення методом паттернів

На рис. 12, 13 відображені графіки залежності відсотка втрачених біт від експерименту при проведенні перетворення масштабування для розширення. При цьому кожна координата змінюється у 1,01 раз, забезпечуючи поступове розширення контейнера. Для побітового методу при найнесприятливіших параметрах досягається втрата бітів у приблизно 45 %, а для методу паттернів – 100 %.

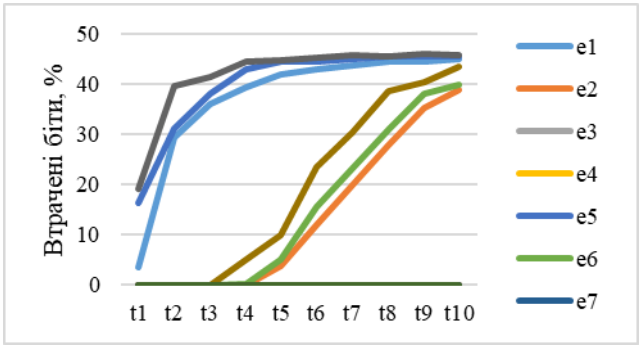

Рис. 12. Результати вилучення інформації з контейнерів
після перетворення масштабування для розширення побітовим методом

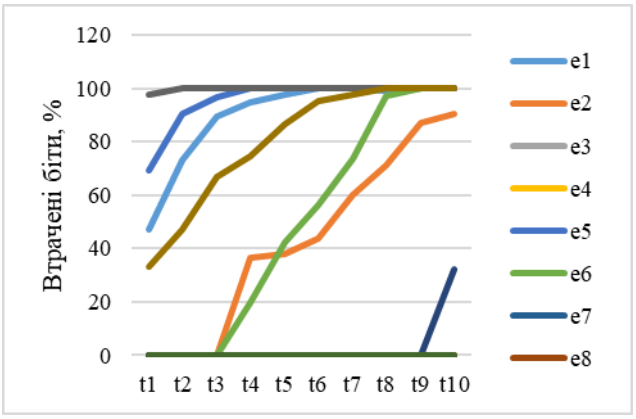

Рис. 13. Результати вилучення інформації з контейнерів
після перетворення масштабування для розширення методом паттернів

На рис. 14, 15 відображені графіки залежності відсотка втрачених біт від експерименту при проведенні майже афінного перетворення повороту. У цьому випадку контейнер поступово повертався на один градус десять разів, і до кожної координати додавалось певне значення, яке відповідає за шум. Для побітового методу при найнесприятливіших параметрах досягається втрата бітів у приблизно 33 %, а для методу паттернів – 100 %.

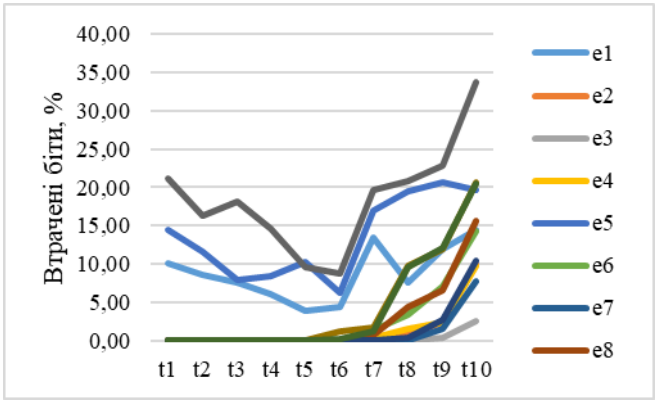

Рис. 14. Результати вилучення інформації з контейнерів
після майже афінного перетворення повороту побітовим методом

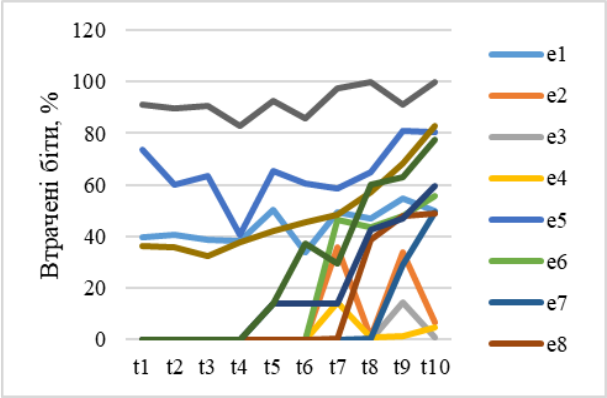

Рис. 15. Результати вилучення інформації з контейнерів
після майже афінного перетворення повороту методом паттернів

Таким чином, проведені експериментальні дослідження показали, що методи приховування інформаційних повідомлень у векторні зображення з [11, 12] дійсно забезпечують деяку стійкість до афінних атак.

Отримані результати відрізняються від вперше представлених у роботах [11, 12] більш високими показниками втрачених біт навіть при меншій кількості разів проведення перетворень над контейнером. Це можна пояснити особливостями програмної реалізації, використовуваними контейнерами, більшим об'ємом відстежуваних винятків при вбудовуванні/вилученні повідомлення тощо.

У загальному випадку отримані результати за допомогою програмно розроблених у даній роботі методів співпадають із представленими результатами О. Кінзерявого [11, 12]. Виключенням є сто відсоткова втрата блоків при застосуванні методу паттернів при таких перетворення як поворот, зсув за осями абсцис та ординат, масштабування для стиснення та розширення, а також при деяких параметрах майже афінного перетворення повороту. В обох реалізація найбільш сприятливим є параметр точності у розмірі 6, при якому не залежачи від кількості біт, що кодуються в криву, та похибки відтворення, досягається нульовий (або майже нульовий) відсоток втрачених або неправильно вилучених біт.

За допомогою програмно розроблених методів можлива реалізація розглянутих методів у різноманітних веб-застосунках для виконання факту перевірки ключових даних. Такими даними можуть бути мітки часу або певна величина, яка формується шляхом відстежування усіх елементів на сторінці і може бути використана для запобігання зловмисного впровадження надбудованих конструкцій, що можуть бути застосовані для перехоплення персональних даних користувачів (така технологія обману носить назву клікджекінгу). Мітки часу можуть бути використані в якості підтвердження існування певних даних у деякий момент.

Окрім цього існує практика створення компонентів DOM-структури із SVG зображень і цілком можливою є ситуація, коли вся веб-сторінка або її складова частина складається із елементів векторної графіки. Цей факт може бути використаний не тільки для збереження даних, а й у якості підтвердження прав авторства, володіння тощо.

Висновки

Результати досліджень показників стійкості до афінних перетворень показали, що метод паттернів програє побітовому. Це пов’язано у першу чергу із алгоритмом вилучення інформації методу паттернів. Так, можлива ситуація втрати цілих блоків інформаційних бітів, коли не знаходиться перша частина послідовності (перший паттерн), а звідси – неможливим стає знаходження наступного коефіцієнту побудови кривої, при якому відбулося б об’єднання сегментів. Така залежність присутня в обох методах, однак побітовий у випадку, коли не виконується умова відтворення, вилучають двійковий «0» (тобто це може бути навіть неправильно вилучений біт), і процес декодування продовжується.

Дослідження стійкості до афінних перетворень також показали, що найбільш сприятливими для приховання та вилучення є випадки, в яких застосовувалась точність 6 для розрахунку координат, при цьому похибка та кількість біт, що приходяться на одну криву, – неважливі.

Практичне застосування методів приховування інформації у векторній графіці полягає у можливості збереження таких даних як мітки часу, права авторства або володіння, значень контрольної суми компонентів DOM-структури для аналізу стану веб-застосунку у випадках застосування анти-клікджекінгових технологій тощо.

Список літератури:

1. Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications. Illustrated Edition. Cambridge; New York: Cambridge University Press, 2009. 466 p.
2. Yahya A. Steganography Techniques // Steganography Techniques for Digital Images / ed. Yahya A. Cham: Springer International Publishing, 2019. P. 9–42.
3. Yahya A. Introduction to Steganography // Steganography Techniques for Digital Images / ed. Yahya A. Cham: Springer International Publishing, 2019. P. 1–7.
4. Manoj I.V.S. Cryptography and Steganography // IJCA. 2010. Vol. 1, № 12. P. 63–68.
5. Menon N., Vaithiyanathan. A survey on image steganography // 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy). 2017. P. 1–5.
6. Basic Shapes – SVG 1.1 (Second Edition) [Electronic resource]. URL: https://www.w3.org/TR/SVG11/shapes.html (accessed: 12.05.2021).
7. Doncel V.R., Nikolaidis N., Pitas I. An Optimal Detector Structure for the Fourier Descriptors Domain Watermarking of 2D Vector Graphics // IEEE Transactions on Visualization and Computer Graphics. 2007. Vol. 13, № 5. P. 851–863.
8. Wang X. et al. Reversible Data-Hiding Scheme for 2-D Vector Maps Based on Difference Expansion // IEEE Transactions on Information Forensics and Security. 2007. Vol. 2, № 3. P. 311–320.
9. Wu D., Wang G., Gao X. Reversible Watermarking of SVG Graphics // 2009 WRI International Conference on Communications and Mobile Computing. 2009. Vol. 3. P. 385–390.
10. Peng F. et al. Reversible Data Hiding in Encrypted 2D Vector Graphics Based on Reversible Mapping Model for Real Numbers // IEEE Transactions on Information Forensics and Security. 2019. Vol. 14, № 9. P. 2400–2411.
11. Kinzeryavyy O. et al. Steganographic Method of Bitwise Information Hiding in Point-Defined Curves of Vector Images // Advances in Computer Science for Engineering and Education / ed. Hu Z. et al. Cham: Springer International Publishing, 2019. P. 478–486.
12. Kinzeryavyy O. Steganographic methods for hiding data into vector images that are resistant to active attacks based on affine transformations: Thesis. 2015.
13. Coste A. Image Processing : Affine Transformation, Landmarks registration, Non linear Warping. 2012.
14. Weisstein E.W. Affine Transformation [Electronic resource]: Text. Wolfram Research, Inc. URL: https://mathworld.wolfram.com/AffineTransformation.html (accessed: 24.05.2021).

Надійшла до редколегії 11.03.2021

Відомості про авторів:

Кузнецов Олександр Олександрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: kuznetsov@karazin.ua, ORCID:https://orcid.org/0000-0003-2331-6326

Кононченко Ганна Володимирівна – Харківський національний університет імені В.Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: akononpro@gmail.com, ORCID: https://orcid.org/0000-0002-8101-6500