

ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ВБУДОВУВАННЯ ІНФОРМАЦІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ВЕКТОРНИХ ЗОБРАЖЕНЬ

Вінницький національний технічний університет

Анотація

В доповіді розглянуто метод захисту цілісності векторних зображень цифровими водяними знаками (ЦВЗ) із забезпеченням зменшення впливу його вбудовування на якість зображення. Було проведено аналіз впливу ЦВЗ на якість векторних зображень та стійкості запропонованого методу до найпоширеніших зловмисних атак, спрямованих на знищення чи підміну ЦВЗ, результати якого показали достатній рівень стійкості на рівні з відомими методами.

Ключові слова: стеганографія, цифровий водяний знак, захист авторського права, дискретне косинус-перетворення, векторні зображення

Abstract

The report observed the method of protecting the integrity of vector images digital watermarks with provision to reduce the influence of its embedding image quality. It analyzes the impact of watermark on quality vector images and sustainability of the proposed method is the most common malicious attacks aimed at the destruction or substitution of digital watermark, the results of which showed a sufficient level of stability

Keywords: steganography, digital watermark, copyright protection, discrete cosine transform, vector image..

Вступ

Діяльність великої кількості підприємств та організацій пов'язана зі створенням та обробкою інформації у цифровому вигляді, лівову частку якої складають цифрові зображення, зокрема векторного формату. Наприклад, векторні цифрові карти є основою системи державного земельного кадастру та картографічної промисловості. Зображення векторного формату використовуються промисловими підприємствами при проектуванні будь-якої техніки від портативної до авіатранспорту. При цьому на створення векторних зображень витрачається багато коштів та часу і часто вони є результатом наукових розробок та основою інноваційних технологій.

На сьогодні в Україні існує серйозна проблема захисту векторних зображень від несанкціонованого використання та їх зміни третіми особами. В багатьох зарубіжних країнах для вирішення такої проблеми використовують стеганографічні методи та засоби захисту цілісності інформації, що дозволяють визначити факт несанкціонованого використання чи модифікації векторних зображень. Для цього навіть прийняті відповідні закони, що дозволяють використовувати стеганографічні засоби для визначення правомірності використання цифрової інформації. На відміну від зарубіжних країн в Україні проблема захисту векторних зображень залишається не вирішеною.

Недоліком закордонних стеганографічних засобів та сервісів захисту цілісності інформації є їх висока ціна та необхідність адаптації для специфіки українського споживача. Для усунення зазначених недоліків пропонується розробка нового методу та сервісу захисту цілісності цифрових векторних зображень (ЦВЗ), що не потребує наявності оригіналу зображення при витягуванні ЦВЗ. При цьому запропоновані метод та сервіс забезпечать кращий рівень захисту, спрощену та швидшу процедуру підтвердження цілісності, а також у 2-2,5 рази нижчу вартість у порівнянні з зарубіжними аналогами.

Результати дослідження

В доповіді висвітлено такі питання.

1. Проведено аналіз існуючих на сьогодні стеганографічних методів вбудовування стійких ЦВЗ у векторні зображення з точки зору впливу ЦВЗ на якість векторних зображень та стійкості до зловмисних атак [1-3]. При цьому особливу увагу приділено аналізу методів, які для витягування ЦВЗ не потребують наявності оригіналу зображення чи самого ЦВЗ, що значно спрощує процедуру підтвердження авторства.

2. Проведено дослідження можливості захисту цілісності векторних цифрових зображень без використання оригіналу зображення при її перевірці та із забезпеченням меншого рівня спотворень внаслідок вбудовування ЦВЗ.

3. Проведено аналіз можливості зменшення рівня спотворень векторних зображень внаслідок вбудовування ЦВЗ з точки зору вибору базового перетворення. Проведений аналіз частотних перетворень показав перевагу двовимірного ДКП над одновимірним з точки зору розподілу зміни коефіцієнтів на більшу кількість точок зображення і, відповідно, меншу зміну координат цих точок близько у 8 разів [4-5].

4. Запропоновано метод захисту цілісності векторних зображень ЦВЗ із забезпеченням зменшення впливу його вбудовування на якість зображення. Було проведено аналіз впливу ЦВЗ на якість векторних зображень та стійкості запропонованого методу до найпоширеніших зловмисних атак, спрямованих на знищення чи підміну ЦВЗ, результати якого показали достатній рівень стійкості на рівні з відомими методами [6-7].

Висновки

Проведено аналіз існуючих на сьогодні стеганографічних методів вбудовування стійких ЦВЗ у векторні зображення з точки зору впливу ЦВЗ на якість векторних зображень та стійкості до зловмисних атак. Проведено дослідження можливості захисту цілісності векторних цифрових зображень без використання оригіналу зображення при її перевірці та із забезпеченням меншого рівня спотворень внаслідок вбудовування ЦВЗ. Запропоновано метод захисту цілісності векторних зображень ЦВЗ із забезпеченням зменшення впливу його вбудовування на якість зображення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Карпинець В. В., Яремчук Ю. Є. Аналіз впливу цифрових водяних знаків на якість векторних зображень // Сучасний захист інформації. – 2011. – №1. – С.72-82.

2. Карпинець В. В., Яремчук Ю. Є. Аналіз рівня спотворень векторних зображень внаслідок вбудовування цифрових водяних знаків / В.В. Карпинець, Ю.Є. Яремчук // Сучасний захист інформації. – 2011. – №2. – С.94 – 99

3. Карпинець В. В., Яремчук Ю. Є. Аналіз сучасних методів вирішення проблеми захисту авторського права векторних зображень / В.В. Карпинець, Ю.Є. Яремчук // Сучасна спеціальна техніка. – №3, 2013. – С. 102–113.

4. Карпинець В. В., Яремчук Ю. Є. Забезпечення захисту векторних зображень від атак спрямованих на видалення цифрових водяних знаків / В.В. Карпинець, Ю.Є. Яремчук // Вісник Східноукраїнського національного університету імені Володимира Даля. – №15 (204), Частина 1, 2013. – С. 62–68.

5. Карпинець В. В., Яремчук Ю. Є. Аналіз впливу параметрів відбору придатних матриць ДКП векторних зображень на спотворення та розмір ЦВЗ / В.В. Карпинець, Ю.Є. Яремчук // Інформаційна безпека. – №1, 2013. – С. 68–77.

6. V. Karpinets, Ju. Yaremchuk, M. Prokofjev. Матеріали конференції, Technical University of Gabrovo. International scientific conference UNITECH'12. / V. Karpinets, Ju. Yaremchuk, M. Prokofjev. // Proceedings. Volume I, 16–17 November 2012, Gabrovo. – Рр. 348 – 352.

7. Яремчук Ю. Є. Метод асиметричного шифрування інформації на основі рекурентних послідовностей / Ю. Є. Яремчук // Сучасна спеціальна техніка. – 2012. – №4. – С.79-87.

8. Shiyan A. A. Management Technologies for Higher Level Officers, Presidents, Prime-Ministers and Parliamentarians / A. A. Shiyan // Political Behavior: Cognition, Psychology, & Behavior eJournal. – 2012. – V. 6, Issue 7. – 581 p..

Василь Васильович Карпинець – к.т.н., доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Vasyl V Karpinets – Cand. Sci. (Eng.), Docent of Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia.