УДК 004.056.55
ЯценкоА.К.[1], Зайко Т.А.[2]
[1] студ. гр. КНТ-129 НУ «Запорізька Політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

СУЧАСНІ МЕТОДИ СТЕГАНОГРАФІЇ

У вік інформаційних технологій багато даних зберігається у цифровому форматі, тож постає питання підвищення рівня безпеки. Для досягнення цієї мети використовують криптографію та стеганографію.

Стеганогра́фія – тайнопис, при якому повідомлення закодоване таким чином, що не виглядає як повідомлення – на відміну від криптографії. Таким чином непосвячена людина принципово не може розшифрувати повідомлення,бо не знає про факт його існування.

Кращий захист інформації забезпечується використанням одночасно стеганографії та криптографії.

Для стеганографії використовують п'ять основних видів контейнерів: текст, зображення, аудіо, відео та мережевий протокол.

Стеганографія тексту полягає у тому, щоб приховати секретне повідомлення в кожній n-й літері кожного слова текстового повідомлення. Текстові файли мають невелику кількість зайвих даних, тож ці методи використовують рідко.

Стеганографія зображення. Повідомлення вбудовується в цифрове зображення за допомогою алгоритму вбудовування з використанням секретного ключа.

Аудіостеганографія. Ці методи використовують той факт, що чутний звук може бути нечутним за наявності гучнішого чутного звуку. Це дозволяє обрати канал для приховування інформації [2].

У нових методах використовується дискретне косинусне перетворення (DCT) і дискретне вейвлет-перетворення (DWT) [3].

Стеганографія відео. У цьому методі також використовуються перетворення DCT і DWT. Оскільки вбудовування виконується в певний відеокадр, це додає додатковий рівень безпеки, оскільки зловмиснику буде важко ідентифікувати, який з кількох сотень відеокадрів є стего.

Стеганографія протоколу. Інформацію приховують в заголовку пакета мережевого протоколу (наприклад, TCP/IP) в деяких полях, які можуть бути необов'язковими або ніколи не використовуватися.

Найбільш популярними є методи стеганографії зображень. Розглянемо наступні методи:

Техніка просторової області. Всі різновиди цієї техніки змінюють деякі біти значень пікселів зображення. Деякі методи просторової області: Заміна найменшого значущого біта (LSB), Співпадіння LSB, Вбудовування матриці, Різниця значень пікселів (PVD) та Розширення спектру (SS).

Стеганографія на основі найменшого значущого біта (LSB) приховує секретне повідомлення в LSB значень пікселів, не вносячи багато помітних спотворень. Вбудовування бітів повідомлення може здійснюватися як послідовно, так і випадковим чином.

Перевагами техніки є менше погіршення оригінального зображення та те, що в зображенні може зберігатися багато інформації.

Основним недоліком є те, щоприховані дані можуть бути втрачені під час маніпуляцій із зображеннями.

Різниця значень пікселів – все зображення розбивається на пари сусідніх пікселів. В залежності від різниці їх значень, до цієї різниці додаються кілька бітів повідомлення [4].

Розширення спектру – до зображення-контейнеру додається псевдовипадковий шум, ступінь якого залежить від повідомлення. Використовуються алгоритми DCT та обчислення ентропії [5].

Маскування та фільтрація. Ці методи приховують інформацію, маркуючи зображення так само, як і водяні знаки на папері. Приховане повідомлення становиться невід'ємним від зображення-контейнера.

Ці методи набагато надійніші при стисненні, ніж заміна LSB, оскільки інформація більш інтегрована в зображення

Недоліки: методи можуть бути застосовані лише до зображень у відтінках сірого та обмежені 24 бітами.

Техніка області трансформації. На відміну від технік просторової області, яка має справу з конкретними пікселями, область трансформації має справу з частотними характеристиками зображення і саме сюди вбудовується повідомлення.

Мають більшу стійкість, тому що при стисканні та обрізанні частотні характеристики майже не спотворюються.

Найбільш відомі алгоритми перетворення даних у частотно-фазову форму [3]:

- методика дискретного перетворення Фур'є (DFT);
- методика дискретного косинусного перетворення (DCT);
- метод дискретного вейвлет-перетворення (DWT).

Табліця 1 – Порівняння методів стеганографії зображень

Метод	Область	Ємність	Виявлення	Стійкість	Складність	Коментар
LSB	Простор.	Висока	Висока	Низька	Низька	Незалежний від формату

						зображення та текстури
SS	Простор.	Низька	Низька	Середня	Середня	Розкладає інформацію по всьому зображенню
PVD	Простор.	Середня	Середня	Низька	Низька	Підходить для висококонтрастних зображень
DCT	Трансф.	Середня	Низька	Середня	Середня	Найпростіший у трансформації
DFT	Трансф.	Середня	Низька	Середня	Середня	Залучає складні розрахунки
DWT	Трансф.	Середня	Низька	Висока	Висока	Тісно збігається з візуальним сприйняттям людини

Стеганографія може використовуватися для цифрових водяних знаків, електронної комерції та транспортування конфіденційних даних [6]. У поточних транзакціях електронної комерції використовується біометричне сканування відбитків пальців, яке поєднується з унікальними ідентифікаторами сеансів.

Наразі не існує ідеального метода стеганографії. Стеганографічні алгоритми, ефективні для одних контейнерів, можуть виявитися неефективними для інших, тож необхідно порівнювати методи з різних аспектів та обрати найкращий для конкретного використання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ramanpreet Kaur Survey and analysis ofvarious steganographice chniques / R. Kaur, Baljit Singh. – International Journal of Engineering Science & Advanced Technology Volume-2 , Issue-3, , May-June 2012. – P. 561 – 566

2. Vijay Kumar Sharma, Vishal Shrivastava “Asteganography algorithm for hiding image in image by improved lsb substitution by minimize detection” Journal of The oretical and Applied Information Technology 15th February 2012. – Vol. 36 No.1 – P.1-8

3. N. F. Johnson A Survey of steganographic techniques / N. F. Johnson , S. Katzenbeisser, F. Petitcolas. – Information Hiding Techniques for Steganography and Digital Watermarking Ed. London : Artech House, 2000. – P. 43-78

4. Anita Pradhan Adaptive PVD Steganography Using Horizontal, Vertical, and Diagonal Edgesin Six-Pixel Blocks / Anita Pradhan, K. Raja Sekhar,

Gandharba Swain. – Security and Communication Networks, 2017. – vol. 2017, Article ID 1924618. – 13 p.

5. Jordy Ardian Bagaskara Analysis of JPEG Image Steganography Using Spread Spectrum Method / Jordy Ardian Bagaskara, Tito Waluyo Purboyo, Ratna Astuti Nugrahaeni. – International Journal of Applied Engineering Research, 2017. – Volume 12, Number 23

6. József Lenti Steganographic methods / József Lenti. – Periodica Polytechnicaser. El. Eng., 2000. – Vol. 44, No. 3– 4. – P. 249–258.