ПРОБЛЕМА ВИБОРУ РОЗМІРУ БЛОКА В СТЕГАНОГРАФІЧНИХ СИСТЕМАХ НА ОСНОВІ СИНГУЛЯРНОГО РОЗКЛАДУ

Жук Є.А., Смірнов А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростання обсягів мультимедійної інформації актуалізує проблему прихованого передавання даних у цифрових зображеннях. Для стеганографічних систем принциповим є узгодження ємності прихованого каналу, непомітності змін контейнера, стійкості до обробки зображення та обчислювальних витрат. Наявні дослідження розглядають зазначені критерії як взаємопов'язані, однак їх співвідношення істотно залежить від способу вбудовування [1, 2]. Перспективним напрямом є дослідження стеганографічного вбудовування в області сингулярного розкладу (SVD) матриць блоків зображення. Розмір блока впливає на кількість доступних позицій для вбудовування, властивості матричного представлення та складність обчислень. Попри застосування блокових методів у цифровому маркуванні, залишається актуальним обґрунтування критеріїв вибору розмірності саме для прихованого передавання повідомлень [3, 4].

Метою доповіді є визначення проблемних питань вибору розміру блока в SVD-орієнтованій стеганографії та визначення завдань майбутнього дослідження з урахуванням ємності, непомітності, завадостійкості та складності обробки.

Першим проблемним питанням є суперечність між розмірністю блока та пропускною спроможністю прихованого каналу. За фіксованого розміру зображення збільшення блока зменшує кількість незалежних фрагментів. Водночас більша матриця містить більше параметрів сингулярного представлення, але їхня придатність до надійного багатобітового вбудовування потребує окремого аналізу. Тому припущення про перевагу великих блоків не можна приймати без дослідження ефективної ємності за однакових обмежень на спотворення. У межах запланованого дослідження передбачається з'ясувати, як зміна розміру блока від 8×8 до 64×64 впливає на геометрію домінантних сингулярних векторів, відстань між станами вбудованих бітів та точність їх відновлення. Розміри блоків і умови JPEG-стиснення зокрема QF = 50 розглядаються як параметри майбутніх випробувань. Значення BER для природних і ШІ-генерованих зображень мають бути отримані та зіставлені експериментально, на цьому етапі підстав стверджувати про встановлену залежність або досягнуте зниження BER немає. Другим проблемним питанням є компроміс між непомітністю змін зображення та завадостійкістю повідомлення. Посилення модифікації сингулярних компонентів потенційно полегшує декодування після JPEG-стиснення, фільтрації чи додавання шуму, проте може збільшувати візуальні та статистичні спотворення. Для перевірки такого припущення необхідно за єдиною методикою вимірювати BER, PSNR, SSIM і виявлюваність стеганографічного вмісту, застосування лише PSNR не є достатнім критерієм прихованості [1, 4].

Третє проблемне питання полягає у залежності вибору блока від властивостей зображення. Природні фотографії, синтетичні та ШІ-генеровані зображення можуть відрізнятися розподілом текстур, контурів і сингулярних компонентів. Потрібно перевірити, чи залишається вибраний розмір блока придатним для різних класів контейнерів і чи не зростає статистична виявлюваність унаслідок багатобітового вбудовування. Дослідження блокової стеганографії в інших моделях зображень також підтверджують актуальність урахування представлення контейнера [5].

Для подальшої роботи пропонується постановка задачі адаптивного вибору блока з множини допустимих розмірів на підставі локальної структури контейнера, заданого обсягу повідомлення та очікуваного типу цифрової обробки. Критерій вибору доцільно сформулювати як багатокритеріальну задачу з обмеженнями на BER, спотворення контейнера, обчислювальний час і показники стеганоаналізу. Окремого обґрунтування потребує механізм синхронізації розбиття під час вилучення повідомлення. Програма запланованої перевірки має включати порівняння фіксованих блоків 8×8, 16×16, 32×32 і 64×64 та адаптивної схеми за однакової довжини повідомлення. Передбачається використовувати набори природних і ШІ-генерованих зображень, моделювати JPEG-стиснення, шум та фільтрацію і оцінювати BER, PSNR, SSIM, час обробки й результати стеганоаналізу. Статистичну значущість відмінностей необхідно перевіряти на незалежних вибірках.

Таким чином, наукова проблема полягає не у визначенні наперед «найкращого» розміру блока, а в установленні умов, за яких конкретна розмірність забезпечує прийнятний компроміс між ємністю, непомітністю, стійкістю та витратами ресурсів. Очікуваним результатом подальшого дослідження є обґрунтований критерій адаптивного вибору блока для SVD-орієнтованого стеганографічного вбудовування; ефективність цього підходу підлягає експериментальній перевірці.

Список літератури

1. Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2009.

2. Martovytskyi V., Ruban I., Bolohova N., Sievierinov O. et al. Development of methods for generation of digital watermarks resistant to distortion. Eastern-European Journal of Enterprise Technologies. 2021. Vol. 6, No. 2 (114). P. 103–116. DOI: 10.15587/1729-4061.2021.246641.

3. Huang H.-N., Chen D.-F., Lin C.-C., Chen S.-T., Hsu W.-C. Improving SVD-based image watermarking via block-by-block optimization on singular values. EURASIP Journal on Image and Video Processing. 2015. Article 25. DOI: 10.1186/s13640-015-0073-6.

4. Ernawan F., Kabir M. N. A block-based RDWT-SVD image watermarking method using human visual system characteristics. The Visual Computer. 2018. DOI: 10.1007/s00371-018-1567-x.

5. Федюшин О. І., Головко Є. В. Проблемні питання застосування блокової LSB стеганографії для квантових зображень. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези XV міжнар. наук.-техн. конф. 2025. Т. 3. С. 112. DOI: 10.32620/ICT.25.t3.