ПРОБЛЕМНІ ПИТАННЯ ЗАСТОСУВАННЯ БЛОКОВОЇ LSB СТЕГАНОГРАФІЇ ДЛЯ КВАНТОВИХ ЗОБРАЖЕНЬ

Головко Є.В., Федюшин О.І.
Харківський національний університет радіоелектроніки, Харків, Україна

LSB квантова стеганографія - це сучасний напрямок в області захисту інформації, що поєднує ідеї квантових обчислень і класичної стеганографії, зокрема техніки Least Significant Bit (LSB), при якому інформація вбудовується в найменш значущі біти (LSB) цифрових зображень, аудіо або відео для приховування даних [1, 2].

Така інтеграція забезпечує надвисокий рівень конфіденційності, стійкості до атак і ускладнює виявлення прихованої інформації.

На даний час відомі два види LSB квантової стеганографії: класична та блокова.

При блоковій стеганографії модифікується не окремий елемент, а цілий блок елементів або квантових станів для підвищення рівня секретності. Блочний підхід дозволяє підвищити стійкість і ефективність прихованого обміну повідомленнями у квантових або квантово-класичних системах [3, 4].

Метою доповіді є аналіз методу блокової LSB стеганографії квантових зображень, можливих сфер застосування та проблемних питань його використання.

При блоковому методі квантове представлення ділиться на блоки розміром m×n (наприклад, 8×8 кубітів). Це дозволяє локалізовано вбудовувати дані, що підвищує стійкість до атак і спрощує адаптивну обробку. У кожному блоці змінюються найменш значущі біти кубітів. Це робиться зміною станів кубітів без порушення суперпозиції. За допомогою квантових алгоритмів аналізу зображення вибираються ті блоки, які мають високий рівень складності (текстура, шум). Це ускладнює виявлення прихованої інформації навіть при стеганоаналізі.

Завдяки розподілу по блоках та використанню квантових ефектів зменшується ризик повного витоку даних. Також такі системи більш стійкі до стеганоаналізу, атак з підміною та шумів. Пропонується додатково застосовувати квантове шифрування повідомлення перед вбудовуванням.

Проведений аналіз показав, що основними сферами застосування блокової LSB стеганографії є:

– захист конфіденційної інформації шляхом приховування секретних повідомлень у квантових зображеннях;

– медична передача даних зі збереженням конфіденційності пацієнтів в телемедицині або медичній діагностиці;

– супутникова та аерокосмічна розвідка. Приховування аналітичних даних у зображеннях з дронів, супутників чи літаків;

– безпечний обмін даними в IoT системах;

– захист авторських прав через приховану ідентифікацію власника в цифрових зображеннях;

– квантова криміналістика та стеження. Збір доказів, що приховані в цифровому вигляді без можливості виявлення сторонніми особами;

– квантові системи безпеки в складних схемах передачі даних в умовах квантового каналу, де шифрування йде разом зі стеганографією.

Використання квантової блокової LSB-стеганографії дозволяє не просто "приховати дані", а й використовувати переваги квантової суперпозиції, паралельної обробки та заплутаності для безпечнішого приховування.

При цьому на даний час існує низька проблемних питань в застосуванні блокової LSB квантової стеганографії:

1. Недосконаліть квантових технологій у практиці. На сьогодні квантові пристрої ще не готові до широкого застосування, а більшість методів квантової стеганографії реалізуються лише в симуляторах.

2. Складність квантового представлення блоків. Кодування зображень або сигналів у NEQR, QRMW чи інших форматах потребує значних обчислювальних і квантових ресурсів. Проблема розбиття на блоки зберігає свою складність у квантовій системі, особливо при обробці великих обсягів даних.

3. Вразливість до квантового стеганоаналізу. Існує ризик створення квантових стеганоаналізаторів, що можуть виявляти закономірності навіть у квантових станах. Якщо шаблон вбудовування не є адаптивним або непередбачуваним, можливе виявлення змін у фазах або поляризації.

4. Проблеми синхронізації між сторонами. Для коректного декодування інформації потрібно: знати розбиття на блоки; параметри LSB-вбудовування; стани заплутаності, якщо вони використовувались. Будь-який збій у синхронізації робить повідомлення потенційно нерозшифрованим.

5. Невисока ємність приховування. Кількість інформації, яку можна вбудувати, обмежена: кількістю LSB-бітів у блоках; допустимим рівнем модифікації, щоб уникнути виявлення. У квантових системах додатково накладаються фізичні обмеження на кількість доступних кубітів.

Список літератури

1. Zhou, R. G., Luo, J., Liu, X., Zhu, C., Wei, L., & Zhang, X. (2018). A novel quantum image steganography scheme based on LSB. International Journal of Theoretical Physics, 57, 1848-1863.

2. Li, P., & Lu, A. (2018). LSB-based steganography using reflected gray code for color quantum images. International journal of theoretical physics, 57(5), 1516-1548.

3. A. AL-Salhi, Y. E., & Lu, S. (2016). Quantum image steganography and steganalysis based on LSQu-blocks image information concealing algorithm. International Journal of Theoretical Physics, 55, 3722-3736.

4. Zhou, R. G., Hu, W., & Fan, P. (2017). Quantum watermarking scheme through Arnold scrambling and LSB steganography. Quantum Information Processing, 16, 1-21.