МЕТОДИ КВАНТОВОЇ СТЕГАНОГРАФІЇ ЗОБРАЖЕНЬ ТА ЇХ ЗАСТОСУВАННЯ В СИСТЕМАХ ЗАХИСТУ

Головко Є.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні інформаційні системи потребують високого рівня захисту, особливо коли дані передаються відкритими каналами зв'язку. Але традиційні криптографічні підходи не приховують факт існування секретного повідомлення. Поєднання стеганографії з квантовими обчисленнями створює новий рівень безпеки, оскільки квантові стани дозволяють здійснювати операції паралельно, забезпечують високу непомітність і ускладнюють виконання стеганоаналізу [1]. Саме тому виникає необхідність наукового дослідження моделей квантового подання зображень та алгоритмів квантової стеганографії, орієнтованих на ефективне та надійне приховування даних.

Метою доповіді є дослідження моделей квантових зображень та стеганографічних методів на основі LSB, що забезпечують підвищений рівень захищеності інформації.

Квантові комп'ютери відкривають доступ до нових принципів представлення та обробки зображень, що забезпечує значні переваги порівняно з класичними системами. Моделювання зображень у квантових станах дозволяє реалізувати операції над усіма пікселями одночасно, що підвищує ефективність і розширює можливості забезпечення безпеки. Крім того, існуючі класичні стеганографічні методи є дедалі вразливішими до сучасних атак, тоді як квантові стани дозволяють мінімізувати спотворення та ускладнюють виявлення вбудованого повідомлення [2]. Актуальність зумовлена потребою у захищеній передачі зображень у таких сферах, як телемедицина, оборона, супутникова розвідка й системи спостереження, де конфіденційність і непомітність мають вирішальне значення.

Моделі зображень у квантових станах формують основу для побудови стеганографічних алгоритмів. Модель квантової решітки передбачає пряме відображення пікселів у кубіти, що робить її концептуально простою, але практично складною через потребу у великій кількості кубітів. Модель Real Ket базується на багаторівневому поділі зображення та використанні заплутування, що дозволяє виконати стиснення, однак випадковість структури зображення обмежує її ефективність у реальних застосуваннях.

Розвиток моделей призвів до створення FRQI, де координати та інтенсивність зображення зберігаються у суперпозиційних станах. Ця модель забезпечує компактність представлення та можливість паралельної обробки, але має значну обчислювальну складність і застосовується лише до квадратних зображень. На відміну від неї, модель NEQR кодує інтенсивність у базисних станах кубітів і дозволяє зменшити складність формування зображення у квантовому вигляді, що робить її технологічно зручною та придатною для використання в схемах стеганографії [3]. Усі ці моделі демонструють різний баланс між точністю представлення, кількістю необхідних кубітів та обчислювальною ефективністю,

проте саме NEQR найкраще відповідає вимогам стеганографії з огляду на простоту побудови та зручність інтеграції зі схемами вбудовування.

Квантова стеганографія зображень у контексті LSB-методів ґрунтується на заміні найменш значущих бітів інтенсивності пікселів на біти повідомлення. Простий LSB-алгоритм виконує таку заміну без додаткових структурних операцій, тому є легким у реалізації, але має низьку стійкість до атак, оскільки зміни на рівні окремих пікселів легко ідентифікувати за допомогою стеганоаналізу. Через це його практичне застосування обмежене.

Зовсім інші властивості демонструє блоковий LSB-алгоритм. Він передбачає розбиття квантового зображення на блоки, у межах яких формується агреговане значення LSB, і саме воно використовується для приховування одного кубіта повідомлення. Задля реалізації такої схеми необхідні додаткові квантові компоненти - лічильник і компаратор, які дозволяють виконувати підсумовування та порівняння значень у межах блоку. Вбудовування здійснюється лише для тих блоків, що відповідають позиції повідомлення, тоді як попереднє скремблювання зображення за методом кривої Гільберта забезпечує додаткову непомітність. Під час вилучення повідомлення блоки аналізуються з урахуванням порогового значення, що дозволяє відновити правильний кубіт навіть у разі часткового спотворення. Таким чином, блоковий LSB забезпечує значно вищу стійкість порівняно з простим методом, оскільки зміна одиничного LSB уже не впливає на точність вилучення інформації, а операції з блоками формують природний захист від випадкових або цілеспрямованих атак. Дослідження методів квантової стеганографії зображень демонструє перспективність їх використання у сучасних системах захисту інформації. Моделі представлення квантових зображень мають суттєві відмінності, і вибір конкретної моделі визначає ефективність побудови стеганографічної схеми. Найбільш збалансованим за складністю та продуктивністю є підхід NEQR, що дозволяє оптимально організувати приховування даних у квантових зображеннях. Аналіз алгоритмів LSB показує, що хоча простий метод має низьку стійкість, блоковий LSB забезпечує високу непомітність і можливість адаптації під різні вимоги. Обидва алгоритми базуються на сліпому вилученні, що робить їх практичними у використанні. Результати дослідження підтверджують значний потенціал квантової стеганографії та окреслюють напрям подальших робіт, пов’язаних із підвищенням стійкості, оптимізацією обчислювальних ресурсів і моделюванням реальних систем квантового приховування інформації.

Список літератури

1. Конахович Г. Ф., Шевченко О. В., Кінзеревий В. М., Хохлачова Ю. Е. Сучасні методи квантової стеганографії. Захист інформації. 2011. № 2 (51). С. 5–9.

2. Шпикуляк , І.С. 2024. Роль стенографії як засобу запису інформації. Інформаційні технології і системи в документознавчій сфері. (Бер 2024), 13-14.

3. Методи захисту інформації на основі квантової стеганографії зображень / О. Федюшин, Є. Головко, А. Смірнов, В. Сухотеплий, О. Чечуй // Радіотехніка. – 2024. – Вип. 218. – С. 44–55. – DOI : https://doi.org/10.30837/rt.2024.3.218.03