Магістерська кваліфікаційна робота на тему:

Підвищення захисту потокового відео у системах безпеки від несанкціонованої модифікації з використанням крихких цифрових водяних знаків

Виконав: студент групи УБ-17м Білик О.П.
Керівник: к.т.н., доц. Карпінець В.В.

Мета, об'єкт, предмет дослідження:

- **Мета роботи:** аналіз існуючих методів вбудовування цифрових водяних знаків та способів атак на стегосистеми. На основі розглянутої інформації – здійснити покращення стеганографічного методу вбудовування крихких цифрових водяних знаків для підвищення захисту потокового відео від несанкціонованої модифікації.
- **Об'єкт дослідження:** покращення методу захисту потокового відео з використанням крихких цифрових водяних знаків
- **Предмет дослідження:** методи приховування інформації та методи захисту потокового відео.

Актуальність

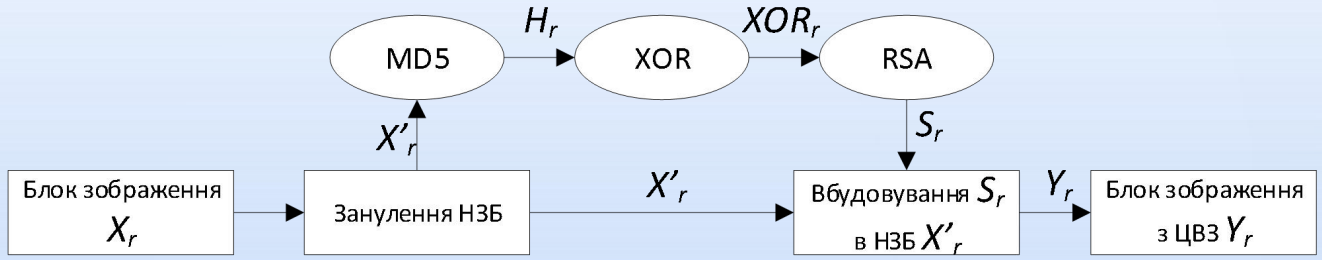
Зі збільшенням популярності мережі Інтернет, все більше даних передаються незахищеними каналами, де вони можуть бути перехоплені та несанкціоновано модифіковані. Отже постає проблема можливості доведення авторства та оригінальності контенту.

Існуючі методи вбудовування ЦВЗ використовують:

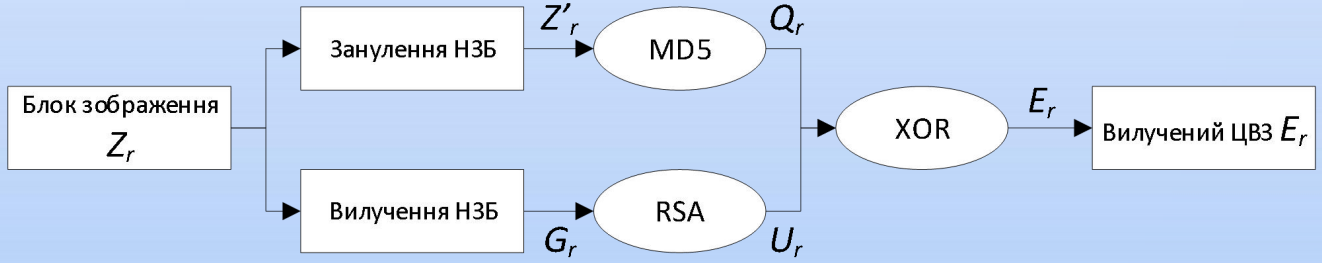
- найменш значущий біт (НЗБ/LSB);
- дискретне перетворення Фур'є (ДПФ);
- дискретне косинусне перетворення (ДКП);
- дискретне вейвлет-перетворення (ДВП);
- генерація випадкових послідовностей;

Алгоритм крихких водяних знаків на основі блоків (алгоритм Вонга)

Вбудовування крихких ЦВЗ



Вилучення ЦВЗ



Запропоноване покращення методу

1. Використання функції з секретним ключем HMAC-SHA-256 замість MD5
2. Вбудовування інформації у два останні найменш значущі біти
3. Вибір кадрів з достатньою руховою активністю

Обчислення рухової активності

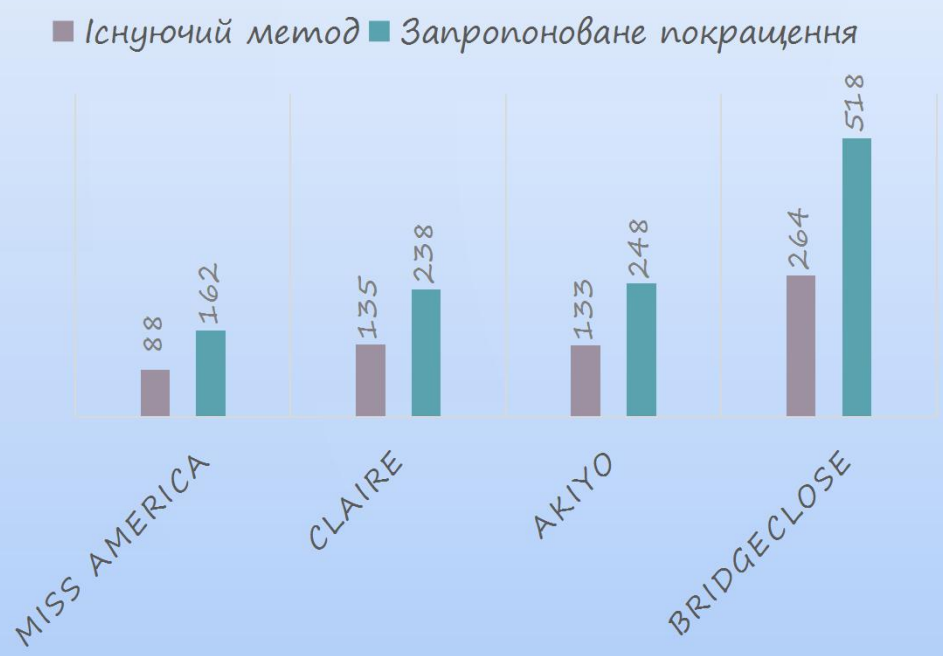
- Матриця рухової активності кадру: $MV(i,j) = \sqrt{\left(MV_x(i,j)\right)^2 + \left(MV_y(i,j)\right)^2}$, де (i,j) позначають індекси блоку
- Середнє значення матриці активності кадру: $C^{avg} = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} C(i,j)$, де M та N – ширина та висота блоку
- Рухова активність кадру: $\sigma_{Fi} = \sqrt{\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(C(i,j) - C^{avg}(i,j)\right)^2}$

Алгоритм роботи методу із запропонованим покращенням

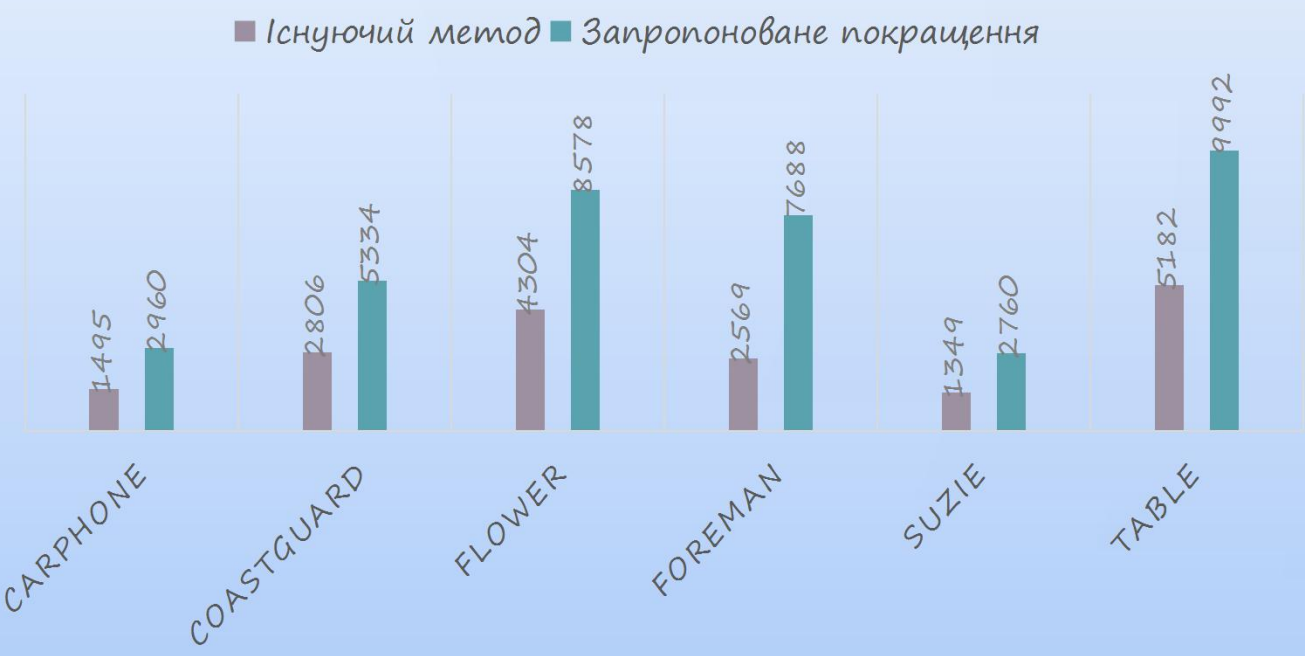
1. Розбиття відеопослідовності на групи кадрів
2. Збереження властивостей яскравості та насиченості
3. Вибір основного кадру з групи
4. Використання HMAC-SHA256 з секретним ключем та збереженими даними
5. Вибір кадрів зі значною руховою активністю
6. Вибір задовільних векторів руху
7. Квантування обраних векторів руху
8. Перевірка виконання рівності квантованих та оригінальних векторів $Q(\overline{MV_x}) = Q(MV_x)$ та $Q(\overline{MV_y}) = Q(MV_y)$
9. При виконанні рівності – вбудовування даних у кадр

Порівняння результатів використання методів (середнє корисне навантаження (біт))

Низька рухова активність



Висока рухова активність

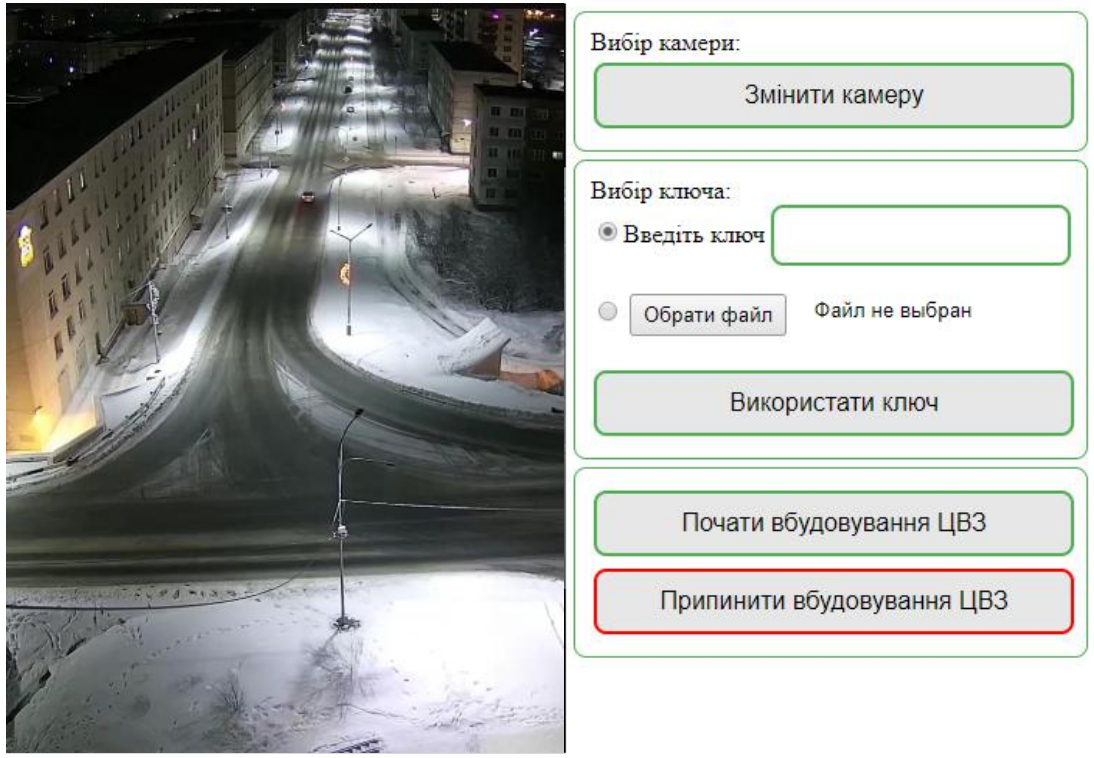


Алгоритм роботи додатку

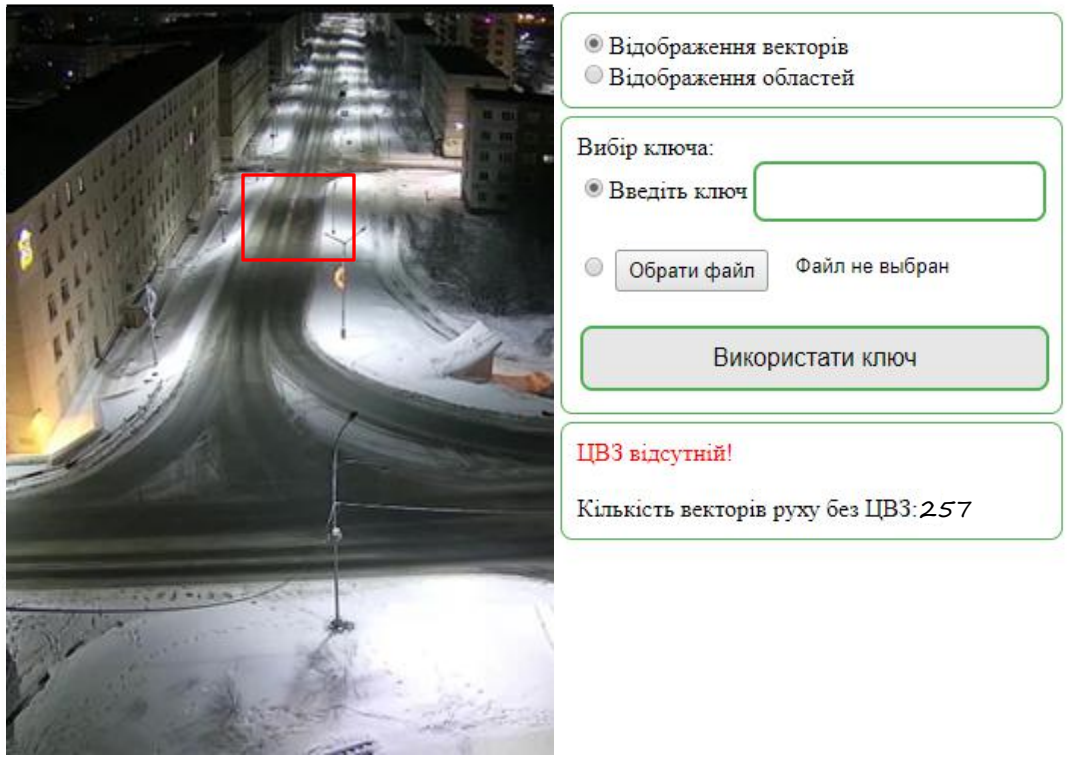
1. Запуск серверу
2. Вибір секретних ключів
3. Створення сесії відеопотоку
4. Запуск процесу вбудовування ЦВЗ у відеопотік
5. Підключення користувачів
6. Запуск процесу видобування ЦВЗ
7. Аналіз на наявність несанкціонованих можифікацій
8. Відображення областей з модифікаціями (при їх наявності)

Вигляд додатку

Сервер



Клієнт



Висновки:

- Проведено аналіз існуючих методів захисту інформації з використанням стеганографічних методів.
- Досліджено існуючі методи вбудовування цифрових водяних знаків, розгляну можливі атаки на стегосистеми.
- Детально розглянуто метод вбудовування крихких цифрових водяних знаків у відео, проаналізовано можливі шляхи вдосконалення.
- Запропоновано покращення методу вбудовування крихких цифрових водяних знаків у відеопотік.
- Розроблено програмне забезпечення, що базується на запропонованому покращенні.

Дякую за увагу!