ПРОГРАМНИЙ ЗАСІБ ДЛЯ ПРИХОВУВАННЯ ТЕКСТОВОЇ ІНФОРМАЦІЇ У ЦИФРОВОМУ ЗОБРАЖЕННІ

Виконав студент групи 2КІ-18м

Казаков Р. Г.

Керівник: к. т. н., доц. каф. ОТ

Савицька Л. А.

АКТУАЛЬНІСТЬ ДОСЛІДЖЕННЯ

В наш час, коли кількість використання цифрових ресурсів сягає незліченних обсягів, дослідження і впровадження стеганографії все більше схоже на вимушену міру.

Спілкування і обмін інформацією щоденно безлічі користувачів супроводжується незаконним копіюванням і розповсюдженням, яка доволі часто є особистою.

В наслідок таких дій, підвищується жага до приватності і захисту особистої інформації.

МЕТА, ОБ’ЄКТ, ПРЕДМЕТ ДОСЛІДЖЕННЯ

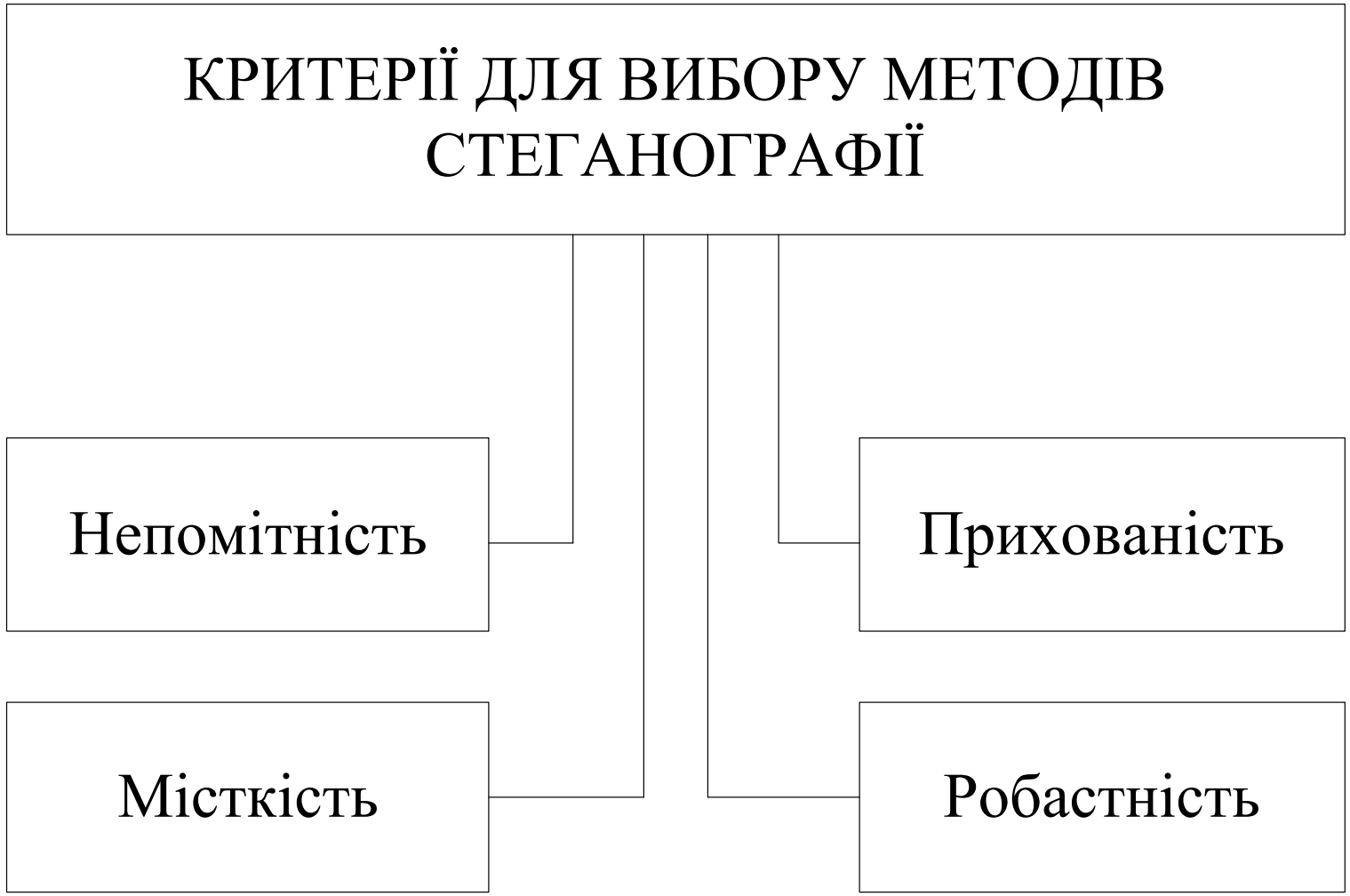
Метою дослідження є вдосконалення методу стеганографічного приховування інформації.

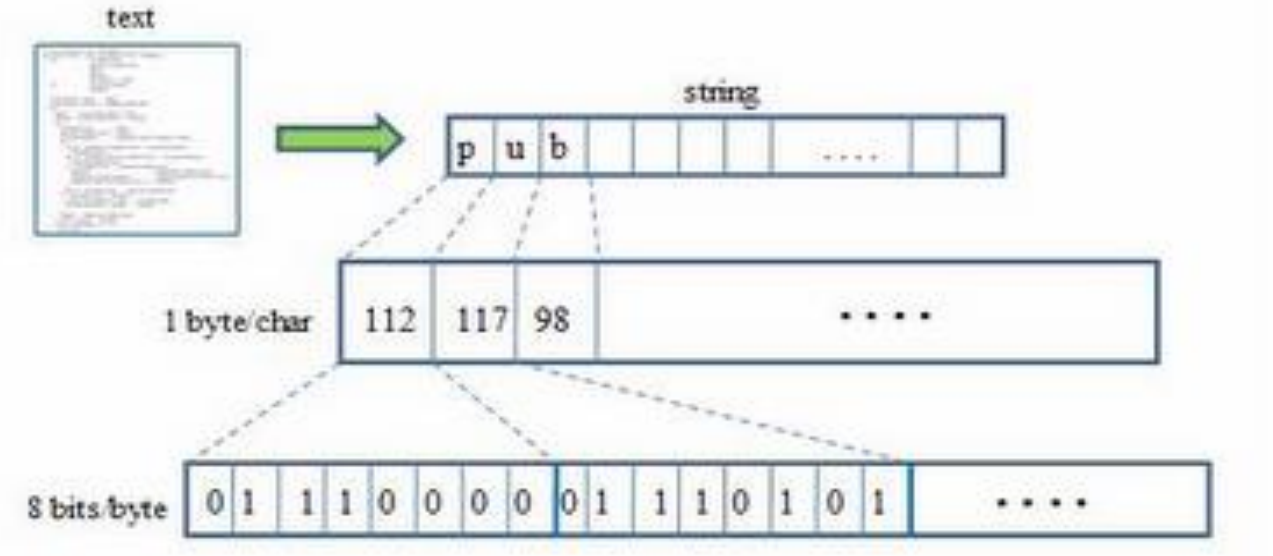
Об’єкт дослідження – процес обробки даних з метою вкраплення текстової інформації у цифрове зображення.

Предмет дослідження – методи та алгоритми стеганографічного приховування.

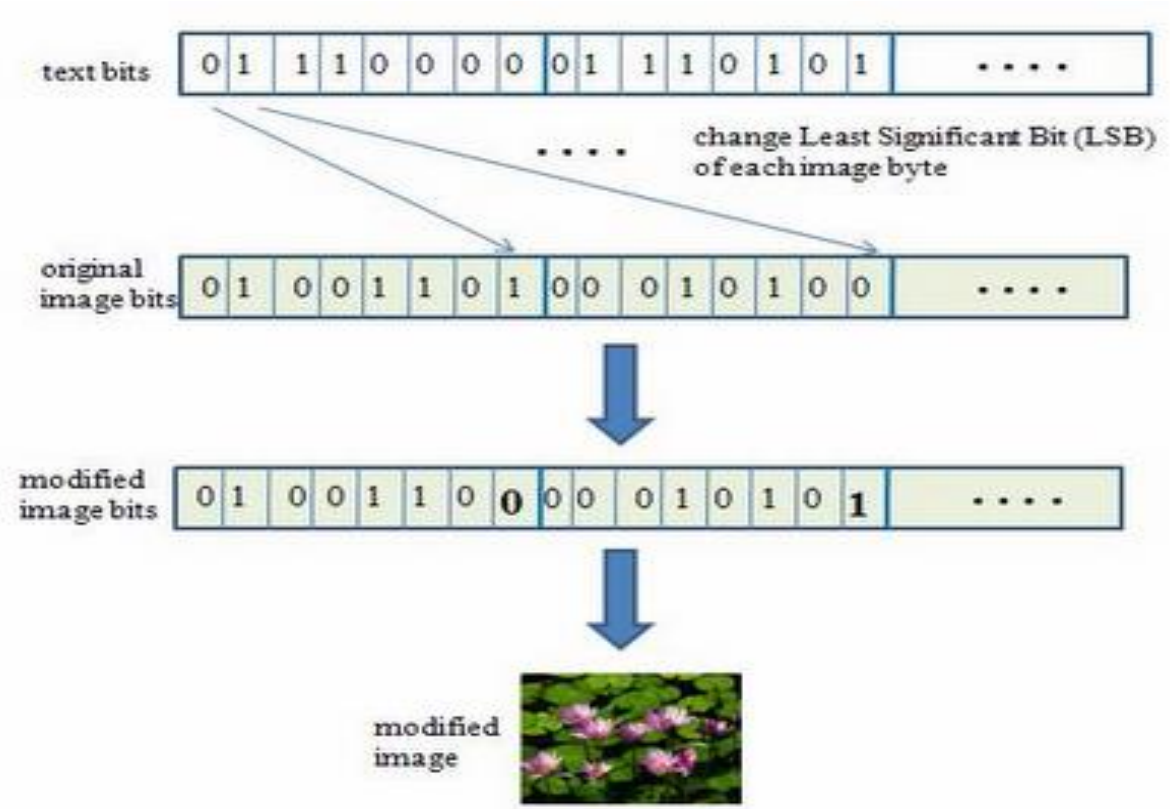
ВИДИ ФАЙЛІВ, ЯКІ ПРИДАТНІ ДЛЯ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ

КРИТЕРІЇ ДЛЯ ВИБОРУ МЕТОДІВ СТЕГАНОГРАФІЇ





Перетворення тексту в байтову послідовність



Принцип роботи

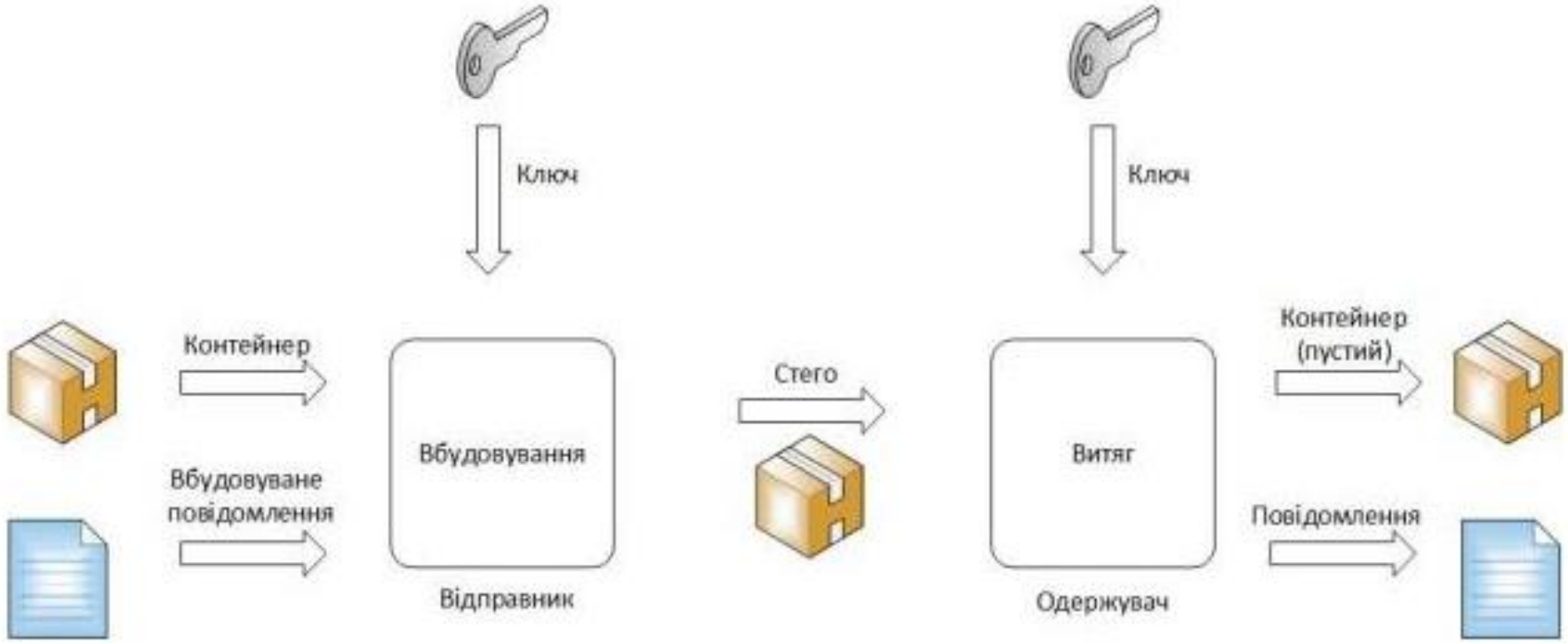
АЛГОРИТМ ШИФРУВАННЯ RSA

RSA алгоритм дозволяє шифрувати інформацію в кількох режимах:

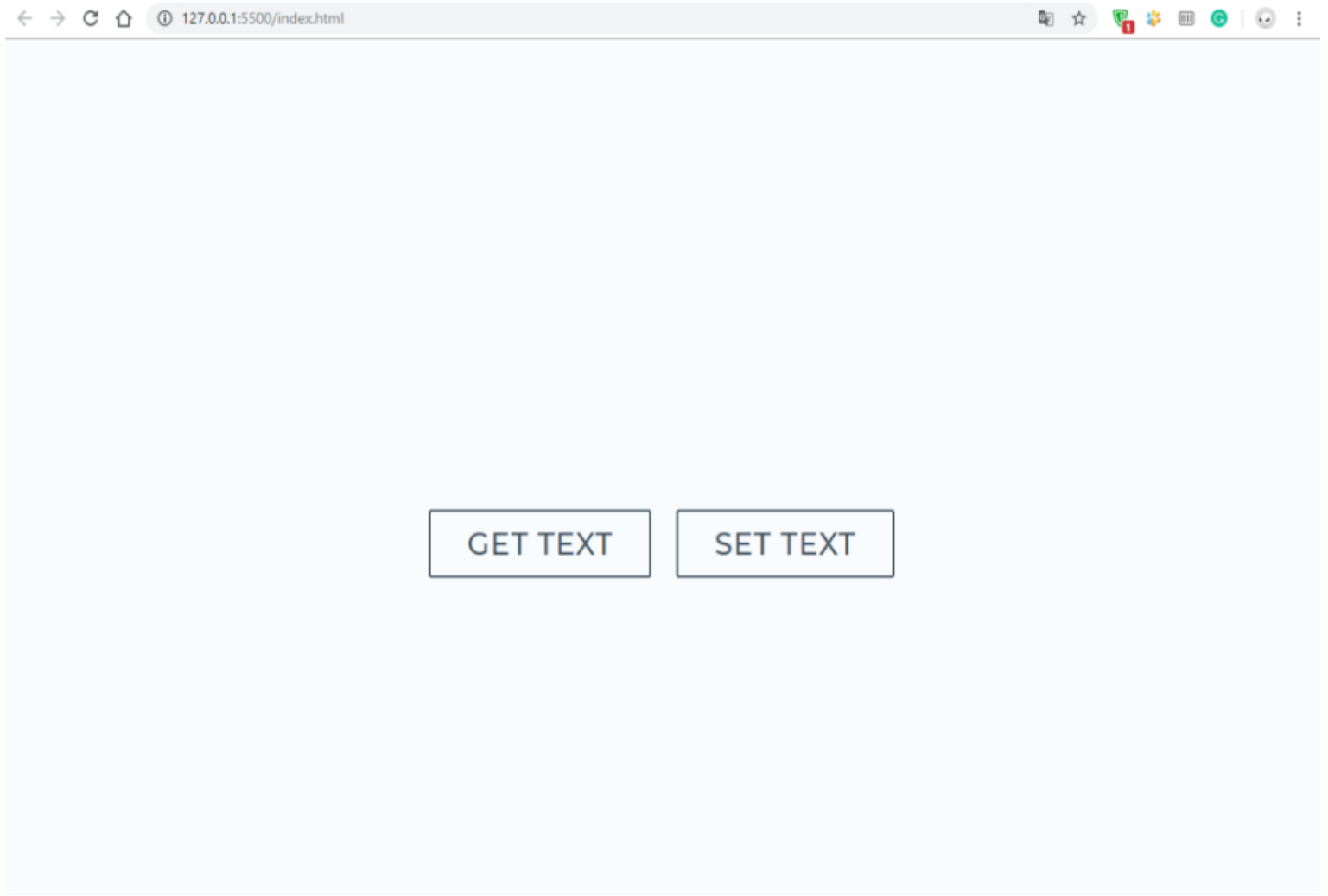
- таємний ключ відправника, у такому разі повідомлення може розшифрувати будь-яка людина, яка має в наявності відкритий ключ.

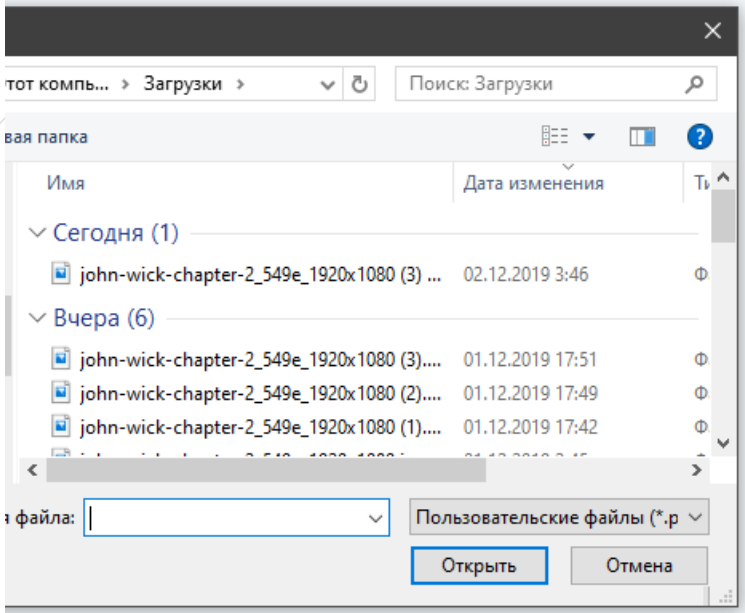
- відкритий ключ отримувача, дає змогу дешифрувати повідомлення власнику таємного ключа, але процес дешифровки буде успішним при наявності відкритого ключа, тому що вони є парними.

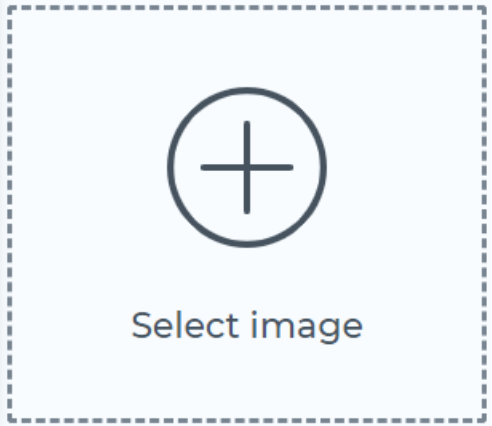
- таємний ключ відправника та відкритий ключ отримувача повідомлення, тільки тоді повідомлення може бути розшифрованим на стороні отримувача.



Узагальнена модель стегосистеми


127.0.0.1:5500/index.html
GET TEXT
SET TEXT





Enter some text..

SET TEXT

Дане повідомлення буде приховано!

SET TEXT

Дане повідомлення буде приховано!

SUCCESS


GET TEXT
SET TEXT

GET TEXT

Дане повідомлення буде приховано!

SUCCESS

GET TEXT

Висновки

У даній магістерській кваліфікаційній роботі було розроблено покращений алгоритм, який заснований на приховуванні за допомогою найменш значущого біта. Модифікований тим, що порядок вибору найменш значущого біта є довільним, а це в свою чергу дає можливість уникнути вияв факту передачі за допомогою методу Хі-квадрат та RS-атак.

Стеганографічний алгоритм приховування працює у поєднанні з криптографічним алгоритмом RSA, через його можливі варіації та стійкість до зламу. Така комбінація дозволяє не тільки приховувати вміст повідомлення, для передачі по відкритому або не захищеному каналу зв'язку, а й додатково створити захист на випадок якщо повідомлення все ж таки буде виявлено.

Дякую за увагу !