Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет «Комп'ютерні технології і системи»
(назва факультету)

Кафедра «Електронні обчислювальні машини»
(повна назва кафедри)

Пояснювальна записка

до кваліфікаційної роботи
бакалавра
(ступінь вищої освіти)

на тему: Розробка комплексу засобів стеганографічного захисту інформації. Стеганографічний захист інформації з використанням текстових контейнерів

за освітньою програмою Кібербезпека

зі спеціальності: 125 Кібербезпека
(шифр і назва спеціальності)

Виконав: студент групи: КБ1811

_____ / Катерина АНАНЬЄВА /
(підпис студента) (Ім'я ПРІЗВИЩЕ)

Керівник: _____ / доцент, Денис ОСТАПЕЦЬ /
(підпис) (посада, Ім'я ПРІЗВИЩЕ)

Нормоконтролер: _____ / ст. викладач, Володимир ДЗЮБА/
(підпис) (посада, Ім'я ПРІЗВИЩЕ)

Консультанти:

_____ _____ / _____ /
(назва розділу) (підпис) (посада, Ім'я ПРІЗВИЩЕ)

_____ _____ / _____ /
(назва розділу) (підпис) (посада, Ім'я ПРІЗВИЩЕ)

_____ _____ / _____ /
(назва розділу) (підпис) (посада, Ім'я ПРІЗВИЩЕ)

Засвідчую, що у цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Дніпро –2022 рік

Ministry of Education and Science of Ukraine
Ukrainian State University of Science and Technologies

Faculty «Computer technologies and systems»
(faculty)

Department «Electronic computers»
(department)

Explanatory Note
to Bachelor's Thesis
first (bachelor's)
(higher education degree)

on the topic: Development of a set of means of steganographic protection of information. Steganographic protection of information using text containers

according to educational curriculum Cybersecurity

in the Speciality: 125 Cybersecurity
(speciality and its code)

Done by the student of the group: KB1811 / Kateryna Ananieva /
(name, surname)

Scientific Supervisor: / Associate Professor, Denis Ostapets /
(position, name, surname)

Normative controller : / Senior lecturer, Volodymyr Dziuba /
(position, name, surname)

Supervisors

(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)

Dnipro – 2022

Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет: Комп'ютерні технології і системи
Кафедра: ЕОМ
Рівень вищої освіти: Перший (бакалаврський)
Освітня програма: Кібербезпека
Спеціальність: 125 Кібербезпека
(шифр та назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри ЕОМ
(підпис) Ігор Жуковицький (Ім'я ПРІЗВИЩЕ)
Дата 22.06.2022

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра
(ступінь вищої освіти)

студенту Ананьєвій Катерині Олегівні
(Прізвище, Ім'я По батькові)

1. Тема роботи: Розробка комплексу засобів стеганографічного захисту інформації. Стеганографічний захист інформації з використанням текстових контейнерів

Керівник роботи: Остапець Денис Олександрович, к.т.н, доцент
(Прізвище, Ім'я, По батькові, науковий ступінь, вчене звання)

затверджені наказом від "07" 12 2021 р. № 67ст

2. Строк подання студентом роботи: 13.06.2022 р.

3. Вихідні дані до роботи: Методи стеганографічного захисту інформації

4. Зміст пояснювальної записки (перелік питань, які потрібно опрацювати):

4.1 Аналітична частина:

Аналіз методів стеганографії, що використовують текстові контейнери

4.2 Основна частина:

- Огляд методів стеганографічного захисту інформації;
- Режими роботи та інформаційна структура комплексу;
- Розробка програмного забезпечення комплексу

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):

- Порівняльний аналіз методів стеганографії;
- Склад та функції комплексу;
- Структура даних;
- Основні алгоритми програми;
- Приклади роботи комплексу

6. Консультанти розділів роботи:

Розділ	Прізвище, ініціали та посада консультанта	Завдання видав: (підпис консультанта, дата)	Завдання прийняв: (підпис студента, дата)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Огляд методів стеганографічного захисту інформації	25.04.22	20%
2	Режими роботи та інформаційна структура комплексу	11.05.22	30%
3	Розробка та налагодження програмного забезпечення	06.06.22	45%
4	Реферат, вступ, висновки	13.06.22	5%
5	Подання кваліфікаційної роботи до кафедри	13.06.22	
6	Захист кваліфікаційної роботи на засіданні Екзаменаційної комісії	23.06.22	

Студент _____ (підпис) Катерина АНАНЬЄВ (Ім'я ПРІЗВИЩЕ)

Керівник роботи _____ (підпис) Денис ОСТАПЕЦЬ (Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи бакалавра:

60 с., 24 рис., 1 табл., 10 додатків, 12 джерел.

Об’єкт розробки – засоби стеганографічного захисту інформації з використанням текстових контейнерів за методом зміни порядку проходження маркерів кінця рядка CR / LF та модифікованим методом хвостових пробілів.

Мета роботи – розробка програмного комплексу, який реалізує та демонструє методи стеганографічного захисту інформації з використанням текстових контейнерів.

Приведено опис та порівняльну характеристику методів текстової стеганографії. Обґрунтовано вибір методів зміни порядку проходження маркерів кінця рядка CR / LF та хвостових пробілів (модифікований). Описано функціонування комплексу та структури даних. Розроблені блок-схеми узагальнених алгоритмів роботи комплексу. Написано та відлагоджено його програмне забезпечення, перевірено його працездатність. Написано інструкцію з використання комплексу.

Результати роботи можуть бути використані у навчальному процесі студентів відповідних спеціальностей при проведенні лабораторних і практичних робіт.

Ключові слова: СТЕГАНОГРАФІЯ, ЗАХИСТ ІНФОРМАЦІЇ, ТЕКСТОВИЙ КОНТЕЙНЕР, МОДИФІКОВАНИЙ МЕТОД ХВОСТОВИХ ПРОБІЛІВ, МЕТОД ЗМІНИ ПОРЯДКУ ПРОХОДЖЕННЯ МАРКЕРІВ КІНЦЯ РЯДКА CR /LF, C#, AES128.

ЗМІСТ

ВСТУП

Захист інформації від несанкціонованого доступу є важливим питанням у реаліях сьогодення. Одним із перших варіантів вирішення цього питання стала стеганографія – приховування таємного повідомлення, шляхом приховування факту існування даного процесу. Розвиток технологій зумовив появу комп'ютерної стеганографії. Ця галузь ґрунтується на широкому розповсюдженні обчислювальної техніки, що посприяло можливості активного обміну інформацією у вигляді текстів, зображень, звуку, відео та архівів. Дана робота присвячена розробці засобів стеганографічного захисту інформації з використанням текстових контейнерів. Тому тема роботи є актуальною.

Тема роботи затверджена наказом № 67 ст від 07.12.2021 .

Мета роботи – розробка програмного комплексу, який реалізує та демонструє методи стеганографічного захисту інформації з використанням текстових контейнерів.

Основні положення даної роботи доповідались та були схвалені на 81 Всеукраїнській науково-технічній конференції молодих учених, магістрантів та студентів «Наука і сталий розвиток транспорту» та XV Міжнародній конференції «Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості та освіті» у 2021 році (див. додатки А та Б).

Дана робота складається зі вступу, 3 розділів та висновків.

1 ОГЛЯД МЕТОДІВ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Загальні відомості

Необхідність захисту інформації від несанкціонованого доступу була актуальна з давніх часів існування людства. Ще в стародавньому світі було створено два основні напрямки рішення цього питання: стеганографія та криптографія.

Слово «стеганографія» походить з грецької мови і має два кореня: «прихований» та «пишу», його можна перекласти як «тайнопис» [1]. Стеганографія передає повідомлення, що зашифроване таким чином, що приховується сам факт передачі повідомлення. Існують різноманітні способи передачі тайнопису, але їх об’єднує одна риса – таємне повідомлення формується, як на перший погляд, абсолютно нічим не примітний об’єкт. Криптографія – це спосіб захисту інформації за допомогою шифрування таємного повідомлення. При криптографії, на відміну від стеганографії, таємне повідомлення саме по собі зацікавлює зловмисників. Тому стеганографія та криптографія взаємно доповнюють та забезпечують додатковий рівень захисту інформації.

Можна виділили два основні напрямки у сучасній стеганографії: технологічний та інформаційний. До технологічної можна віднести методи, що опираються на використання фізичних або хімічних властивостей матеріальних носіїв інформації. До інформаційної стеганографії відносяться лінгвістична та комп’ютерна стеганографія.[2]

Розвиток комп’ютерної стеганографії відбувається завдяки розповсюдженню у всіх сферах життя людини засобів обчислювальної техніки, що посприяло можливості активного обміну інформацією у вигляді текстів, зображень, звуку, відео та архівів.

Стеганографічна система (стегосистема) – це сукупність методів та засобів, які використовуються для створення прихованого каналу передачі інформації. Вона виконує задачу вбудовування та виділення повідомлень з іншої інформації [3].

Загальна схема стегосистеми [2] представлена на рисунку1. Слід відзначити, що наявність ключа не є обов’язковою умовою існування стегосистеми.

При створенні стегосистеми треба зважати на дані положення:

- Зловмисник знається на тому, як працює стегосистема, у всіх її деталях. Але він не знає ключ, з допомогою якого можна дізнатись про те, що існує таємне повідомлення та його зміст.
- Якщо зловмиснику стане відомо про факт існування таємного повідомлення, то до тих пір, поки йому не відомий ключ, це не повинно дати змогу дізнатися зміст таємного повідомлення.
- Потенційний зловмисник не повинен володіти якимось технічними перевагами у розпізнаванні або розкритті таємного повідомлення.

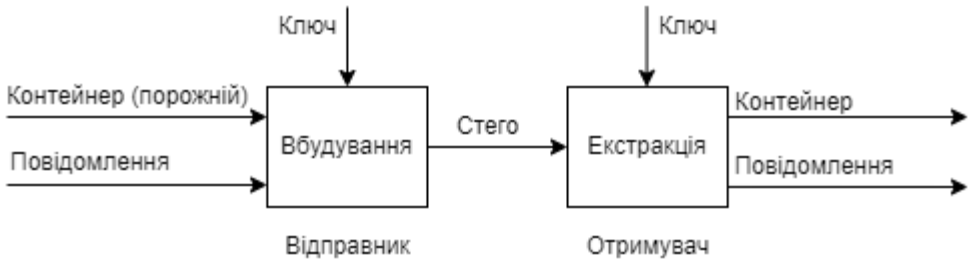


Рисунок 1.1 – Модель стегосистеми

Контейнер – це будь-які інформаційні дані, що використовуються для приховування таємних повідомлень (текст, зображення, звук і тд).

Повідомлення (таємне) – це те, що вбудовується в контейнер.

Стеганографічний канал (стегоканал) - канал передачі таємної інформації [3].

Стегоключ (просто ключ) – це секретний ключ, потрібний для приховування інформації.

В стегосистеми може бути один або кілька стегоключів. Це залежить від кількості рівнів захисту. Подібно до криптографії, по типу стегоключа стегосистеми можна поділити на два типи: з секретним ключем та з відкритим ключем [4].

У стегосистеми з секретним ключем [4] використовується один ключ, який визначається або до початку обміну секретними повідомленнями, або передається по захищеному каналу.

У стегосистеми з відкритим ключем створюються різні ключі таким чином, щоб неможливо було за допомогою обчислень вивести один ключ з іншого. Тому відкритий ключ може передаватися вільно по незахищеному каналу зв'язку. Крім того, дана схема добре працює і при взаємній недовірі відправника і одержувача [4].

1.2. Огляд методів стеганографії з використанням текстових контейнерів

Нині існує досить багато методів текстової стеганографії. Їх можна поділити на дві основні групи: синтаксичну та лексичну.

Синтаксичні методи ґрунтуються на використанні особливостей пунктуації, скорочень та абревіатур. Також, дані методи засновані на зміні стилю і структури речень без значного спотворення вихідного змісту [5].

Секретна інформація в текстових файлах найчастіше кодується шляхом зміни кількості пробілів, використанням невидимих символів [5], великих та малих літер, шляхом зміни міжрядкових інтервалів, табуляцій і т д. Перевагою є простота вбудовування синтаксичних конструкцій у будь-який текст, незалежно від його змісту, призначення та мови.

Метод зміни регістрів символів передбачає кодування нульового біта таємного повідомлення рядковим символом контейнера, а одиничного – прописним символом. Вміст файлу-контейнера зчитується посимвольно і якщо черговий символ є буквою, то відбувається кодування біта повідомлення.

Зміна інтервалу між рядками. Кожен рядок тексту, що маскує повідомлення, зсувається трохи вгору або вниз щодо свого вихідного положення, кодуючи одиницю та нуль, відповідно.

Вирівнювання тексту за допомогою пробілів. Суть даного методу полягає в додаванні пробілів між словами, коли один пробіл відповідає, наприклад, нулю, а два пробілу – одиниці**.** Найбільш ефективно у випадку приховування повідомлень текстів великого об’єму з вирівнюванням по ширині. Однак, звичайне застосування даного методу робить оформлення тексту неохайним, що дозволяє легко запідозрити в ньому наявність стего.

Метод зміни порядку проходження маркерів кінця рядка CR / LF. Суть даного метода полягає в тому, що у переважної більшості засобів відображення текстової інформації, ніяк не відображається порядок проходження символів переведення рядка (CR) і повернення каретки (LF). Тому, звичайний порядок проходження CR / LF відповідає нулю, а інвертований LF / CR – одиниці.

Метод хвостових пробілів передбачає дописування в кінці кожного рядка файлу-контейнера одного пробілу, в разі кодування одиничного біта та відсутність додаткового пробілу у разі кодування нульового біта.

Модифікований метод хвостових пробілів передбачає дописування в кінці рядків від 0 до 15 пробілів, що приховують значення полубайта таємного повідомлення.

Метод знаків однакового накреслення передбачає заміну кириличного символу латинським того ж накреслення, або відсутність такої заміни, кодуючи одиницю та нулю, відповідно. Для реалізації цього методу потрібно скласти таблицю замін.

Недоліками представлених методів є висока ймовірність руйнування прихованого повідомлення при повторному наборі тексту, або при використанні більш складних текстових редакторів, здатних здійснювати ряд автоматичних операцій над текстом. Методи, які оперують безпосередньо самим текстом, окремими його реченнями і словами, характеризуються значно більшою стійкістю до подібних спотворень.

Лінгвістична стеганографія (лексичні або семантичні методи) передбачує використання семантичних особливостей мови [6]. Для даних методів характерна висока ефективність, що пов’язана із застосуванням маніпуляцій над самими реченнями та словами. Найбільш розповсюдженими є методи, які базуються на використанні синонімів.

Якщо для деякого слова існує набір більш ніж з одного синоніма, то можливе формування спеціальних таблиць замін. У таких таблицях кожному синоніму відповідає деяке кодове слово, що складається більш ніж з одного двійкового символу. Однак необхідно відзначити, що в ряді випадків використання методів ускладнене певними

нюансами. Першим з них є неоднозначне використання слів в українській мові. Другим фактором є широке використання в українській мові великої кількості закінчень слів.

Недоліком даного методу є складність у реалізації простим машинним алгоритмом, адже тільки людина може з легкістю виконати дану роботу. Також заміна деяких слів може спотворити стиль мови.

Важливо відзначити, що застосування простого методу заміни слів можна вважати доречним тільки в разі використання коротких текстових повідомлень. Використання даного методу для відносно великих текстів призведе до можливості виявлення прихованого каналу методами статистичного аналізу.

1.3. Порівняльний аналіз методів стеганографії з використанням текстових контейнерів

Автором проведено порівняльний аналіз наведених вище методів текстової стеганографії. Результати аналізу зведено у таблиці 1.1.

Варто відзначити, що синтаксичні конструкції набагато легше вбудовуються в будь-який текст, ніж лінгвістичні. Тому реалізація методу з використанням синонімів буде найважчою з усіх. Однак, цей метод характеризується високою ефективністю, адже він більш стійкий до стегоаналізу, за умови, що його використовують для відносно невеликих текстів.

Щодо ємності контейнеру, то найбільш ефективними для маскування текстів великого об’єму є метод зміни регістрів символів та вирівнювання за допомогою пробілів.

Синтаксичні конструкції не стійкі до якихось змін у контейнері. Наприклад, при повторному наборі тексту, або при використанні більш складних текстових редакторів велика ймовірність втратити таємне повідомлення.

Таблиця 1.1 – Порівняльна характеристики методів стеганографії з використанням текстових контейнерів

Характеристика / Назва методу	Стійкість до спотворень	Складність реалізації	Стійкість до стегоаналізу	Стійкість до візуального аналізу	Ємність контейнера
Зміна регістрів символів	ВН	АН	АН	АН	АВ
Зміна інтервалу між рядками	ВН	АН	АН	АН	С
Вирівнювання тексту за допомогою пробілів	ВН	ВН	ВН	АН	АВ
Зміна порядку проходження маркерів кінця рядка CR / LF	ВН	ВН	ВН	ВВ	ВН
Хвостові пробіли	ВН	ВН	ВН	ВВ	ВН
Хвостові пробіли (Модифікований метод)	ВН	ВН	ВН	ВВ	ВВ
Знаки однакового накреслення	С	ВВ	С	ВВ	ВВ
Заміна синонімами	АВ	АВ	ВВ	АВ	ВН

Примітка: Для оцінювання методів відносно один одного, використовується шкала відносних характеристик: АВ- абсолютно висока; ВВ- відносно висока; С – середня; ВН – відносно низька; АН – абсолютно низька.

Для подальшої реалізації в роботі прийнято рішення використовувати метод зміни порядку проходження маркерів кінця рядка CR / LF та модифікований метод хвостових пробілів у зв’язку з тим, що вони є достатньо простими у реалізації та мають достатньо високу ефективність.

1.4 Висновки за розділом

Розглянуті основні поняття в галузі стеганографії. Наведено короткий опис стеганографічних методів. Проведено порівняльну характеристику методів текстової стеганографії. Для подальшої реалізації в роботі прийнято рішення використовувати метод зміни порядку проходження маркерів кінця рядка CR / LF та модифікований метод хвостових пробілів.

2 РЕЖИМИ РОБОТИ ТА ІНФОРМАЦІЙНА СТРУКТУРА КОМПЛЕКСУ

2.1 Функціонування комплексу

Розроблюваний комплекс являє собою демонстраційну програму, яка показує роботу стеганографії з використанням текстового контейнера. Використовуючи сукупність вищезазначених методів, дана програма реалізує метод зміни порядку проходження маркерів кінця рядка CR / LF та модифікований метод хвостових пробілів. Постановку задачі приведено у додатку Л.

У якості контейнера використовується текстовий файл з розширенням .txt. Таємним повідомленням може бути файл з будь-яким розширенням.

Для посилення захисту інформації використовується шифрування AES128. Advanced Encryption Standard (AES)— симетричний алгоритм блочного шифрування. Розмір ключа у AES128 становить 128 біт. Вхідні дані розбиваються на блоки по 16 байт і якщо розмір даних не кратний 16, то вони збільшуються до тих пір, поки не стануть кратними [7].

В режимі приховування користувач повинен обрати файли з контейнером і таємним повідомленням. Також, він обирає метод приховування та необхідність шифрування. Далі, (за необхідності) вводить пароль із 16 символів. У результаті користувач отримує заповнений контейнер (див. рис. 2.1).

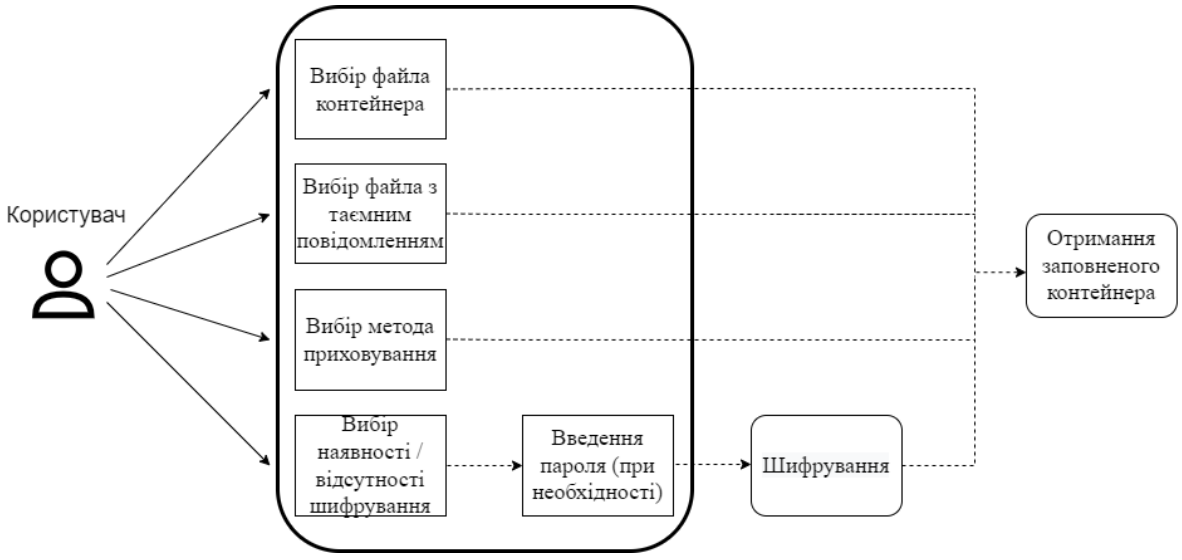


Рисунок 2.1 – Робота комплексу в режимі приховування повідомлення

В режимі отримання таємного повідомлення користувач повинен обрати файл з заповненим контейнером, обрати метод приховування та ввести пароль (за необхідності). У результаті виконання програми буде отримано таємне повідомлення (див. рис. 2.2).

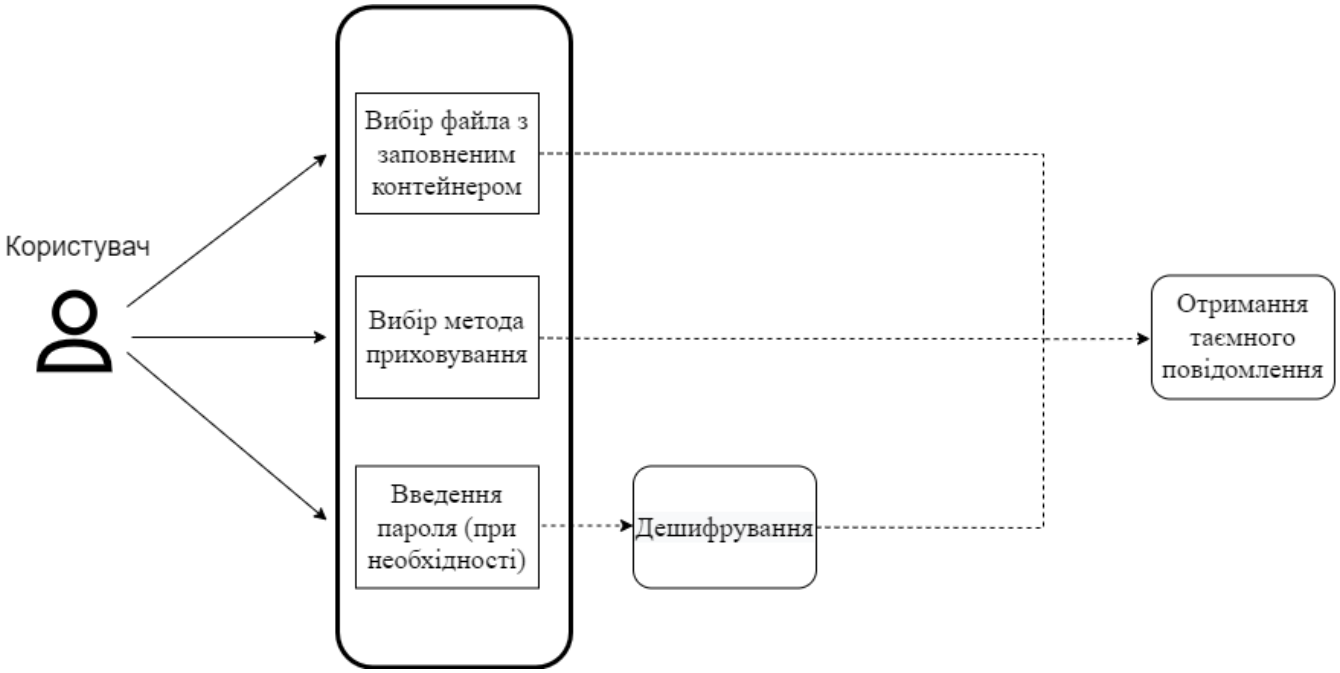


Рисунок 2.2 – Робота комплексу в режимі отримання повідомлення

2.2 Структура даних

Задля передачі службової інформації у заповненому контейнері використовується заголовок. Він представляє собою послідовність із 24-х бітів, у яких записана довжина таємного повідомлення, а останній 23-й біт відповідає за наявність (одиниця), або відсутність (нуль) шифрування (див. рис. 2.3). Запис заголовка відбувається тим методом, яким в даному випадку виконується заповнення контейнера таємним повідомленням. При виконанні модифікованого методу хвостових пробілів для заголовка виділяється перші 6 рядків контейнера, а при методі зміни порядку проходження маркерів кінця рядка – 24 рядки. Максимальна довжина таємного повідомлення становить 8388607Б (майже 8МБ).

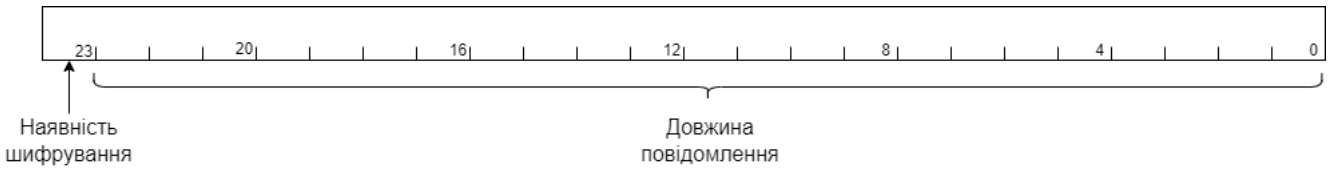


Рисунок 2.3 – Структура заголовка таємного повідомлення

Текстовий контейнер представляє собою текстовий файл. Його мінімальний розмір залежить від довжини та методу приховування повідомлення. У методі зміни порядку проходження маркерів кінця рядка має бути по 8 рядків на кожний байт таємного повідомлення (крім рядків для заголовка), а у модифікованому методі хвостових пробілів – по 2 рядки.

На рисунку 2.4 показано схему порожнього контейнера, де сірий квадрат відповідає символу, а білий – пробілу.

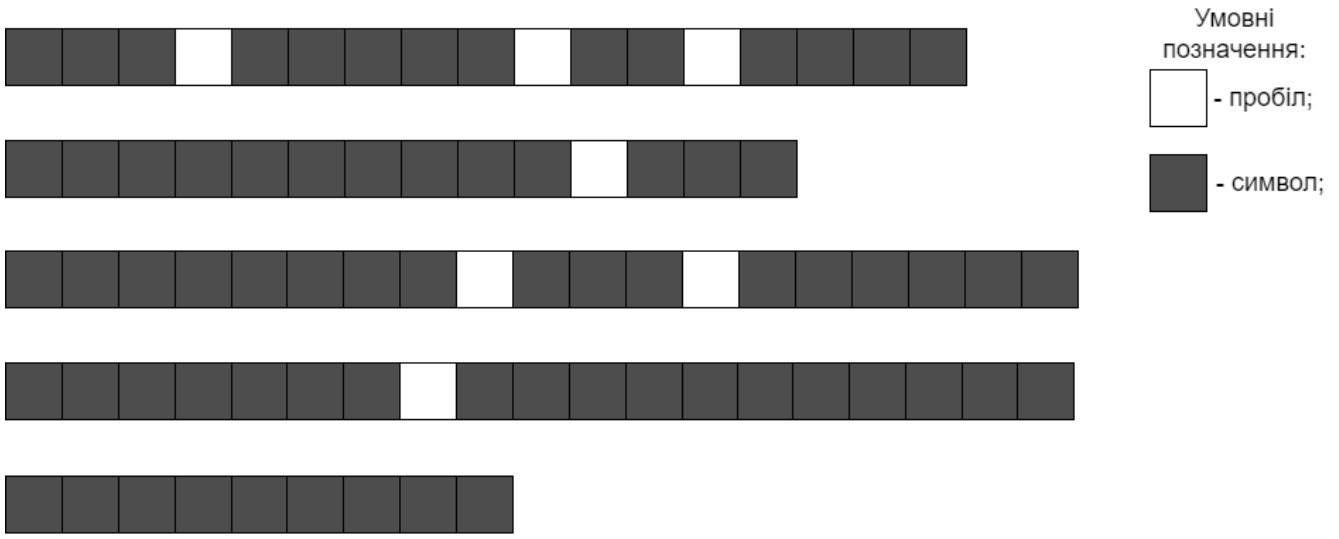


Рисунок 2.4 – Приклад порожнього контейнера

На рисунку 2.5 показано схему заповненого контейнера модифікованим методом хвостових пробілів, де сірий квадрат відповідає символу, білий – звичайному пробілу, а заштрихований – пробілу, що відповідає за приховування. Таємним повідомленням є слово «time», його представлення у двійковій та шістнадцятковій системах числення відповідно:

- 74 69 6D 65,
- 0111 0100 0110 1001 0110 1101 0110 0101.

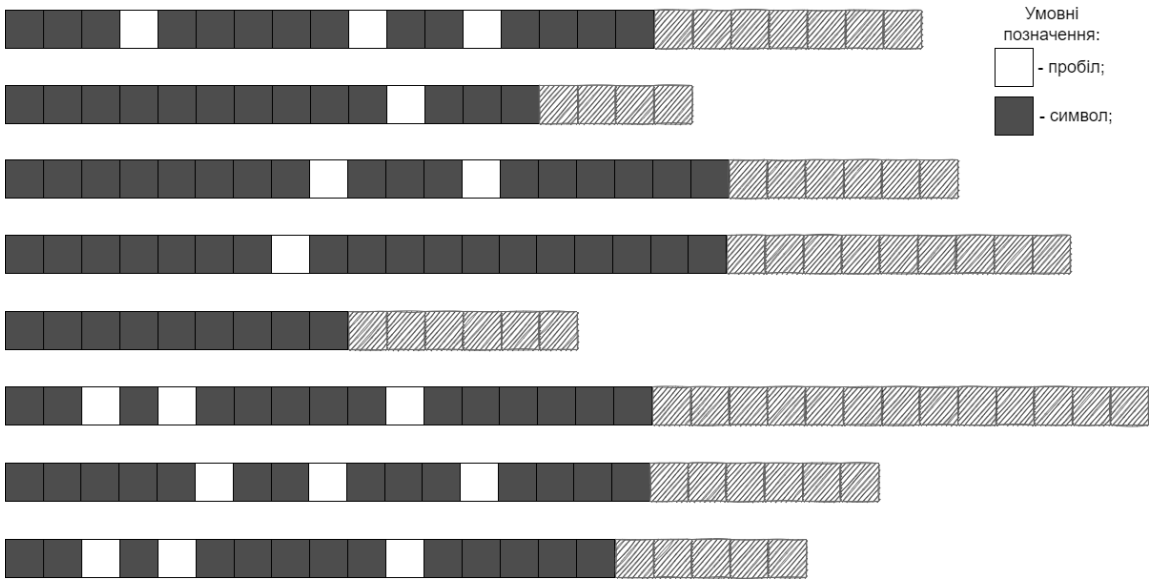


Рисунок 2.5 – Приклад заповненого контейнера методом хвостових пробілів

На рисунку 2.6 показано схему заповненого контейнера методом зміни порядку проходження маркерів кінця рядка, де сірий квадрат відповідає символу, білий – пробілу, CR – переведення рядка, LF – повернення каретки. Звичайний порядок проходження CR / LF відповідає нулю, а інвертований LF / CR – одиниці. Таємним повідомленням є літера «t», її представлення у двійковій системі числення: 0010 1110.

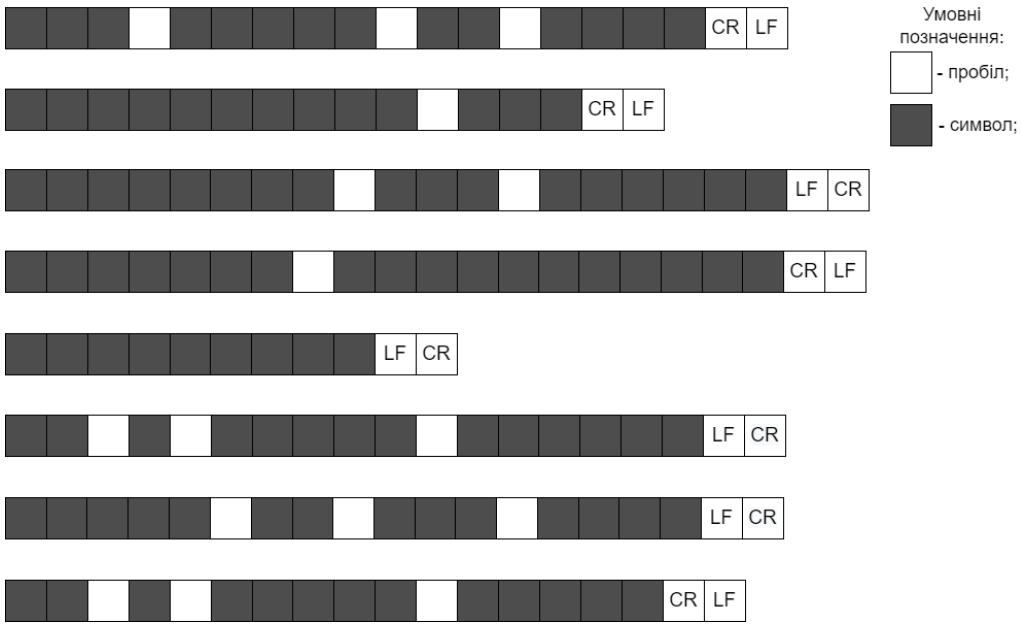


Рисунок 2.6 – Приклад заповненого контейнера методом CR/LF

2.3 Висновки за розділом

Сформовано функціонування даного комплексу у режимах приховування та отримання таємного повідомлення. Прийнято рішення використовувати шифрування AES128 задля додаткового захисту інформації. Створено структуру даних. Розглянуто структуру заголовка таємного повідомлення. Наведені приклади заповнення контейнера методом зміни порядку проходження маркерів кінця рядка CR / LF та модифікованим методом хвостових пробілів.

3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСУ

3.1 Вибір середовища та засобів розробки

Для створення графічного додатку було прийнято рішення використовувати повнофункціональне середовище розробки Visual Studio 2022. Visual Studio 2022 – найбільш швидка, продуктивна та спрощена версія, що призначена для учнів, а також користувачів, які створюють рішення промислового масштабу. Visual Studio 2022 для Windows тепер є 64-розрядною програмою. Це дає змогу відкривати, змінювати, запускати та налагоджувати навіть найбільші та складніші рішення, не турбуючись про брак пам'яті [8].

Для реалізації розроблюваного комплексу засобів стеганографічного захисту інформації обрано мову програмування C#. Мова програмування C# являє собою об’єктно-орієнтовну мову [9]. Синтаксис подібний до C++ та Java. Мова C# підтримує інкапсуляцію, успадкування та поліморфізм. C# була обрана у зв’язку з тим, що засобів даної мови достатньо для того, щоб реалізувати розроблюваний комплекс.

Технологія Windows Forms.NET [10] була обрана задля створення графічного інтерфейсу даної програми. Вона являє собою набір керованих бібліотек, які спрощують виконання стандартних завдань, таких як читання з файлової системи і запис в неї [10]. Використовуючи візуальний конструктор в Visual Studio, дана технологія реалізує один з найефективніших способів створення класичних програм. Такі функції, як розміщення візуальних елементів керування шляхом перетягування, полегшують створення класичних додатків.

Для реалізації шифрування алгоритмом AES128 у програмі використовується стандартний клас Aes [11].

3.2 Розробка програмного забезпечення комплексу в режимі приховування таємного повідомлення

Як вказано в попередніх розділах, комплекс реалізує 2 метода стеганограми: модифікований метод хвостових пробілів та метод зміни порядку проходження маркерів кінця рядка CR / LF. Блок-схема узагальненого алгоритму методу хвостових пробілів у режимі приховування таємного повідомлення наведена на рисунку 3.1. Вихідний код на мові C# наведено у Додатку В.

Блок 1 – запуск прогами у режимі приховування таємного повідомлення.

Блок 2-3 – зчитування файлів з контейнером та таємним повідомленням.

Блок 4 - введення флагу шифрування та ключа шифрування (за необхідності).

Блок 5 – перевірка наявності шифрування.

Блок 6 – підпрограма з шифруванням.

Блок 7 – поділ тексту контейнера на рядки.

Блок 8 – перетворення масиву байтів таємного повідомлення у шістнадцяткову систему.

Блок 9 - підготувати заголовок з інформацією про наявніть шифрування та розміром таємного повідомлення.

Блоки 10-12 – цикл, що перетворює байти таємного повідомлення на пів-байти та записує їх до загального списку пів-байтів.

Блок 13 – утворення заповненого контейнера.

Блок 14 – закінчення виконання програми у даному режимі.

Блок-схема узагальненого алгоритму методу зміни порядку проходження маркерів кінця рядка CR / LF у режимі приховування таємного повідомлення наведена на рисунку 3.2. Вихідний код на мові C# наведено у Додатку Г.

Блок 1 – запуск прогами у режимі приховування таємного повідомлення.

Блок 2-3 – зчитування файлів з контейнером та таємним повідомленням.

Блок 4 - введення флагу шифрування та ключа шифрування (за необхідності).

Блок 5 – перевірка наявності шифрування.

Блок 6 – підпрограма з шифруванням.

Блок 7 – поділ тексту контейнера на рядки.

Блок 8 – перетворення масиву байтів таємного повідомлення у біти.

Блок 9 - підготувати заголовок з інформацією про наявніть шифрування та розміром таємного повідомлення.

Блоки 10-12 – цикл, що інвертує CR і LF за умови, що біт[i] дорівнює одиниці.

Блок 13 – утворення заповненого контейнера.

Блок 14 – закінчення виконання програми у даному режимі.

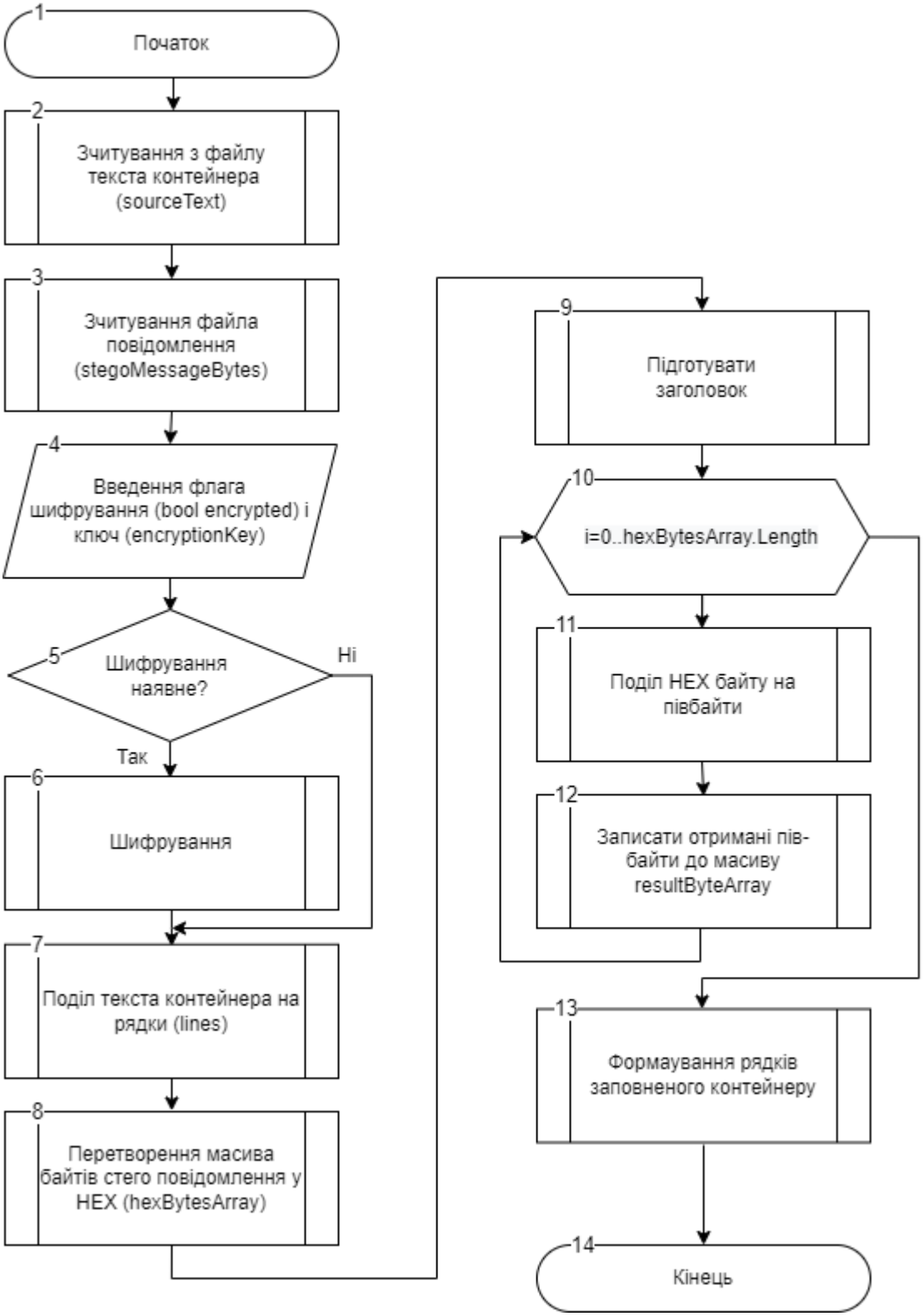


Рисунок 3.1 – Блок-схема узагальненого алгоритму виконання приховування методом хвостових пробілів

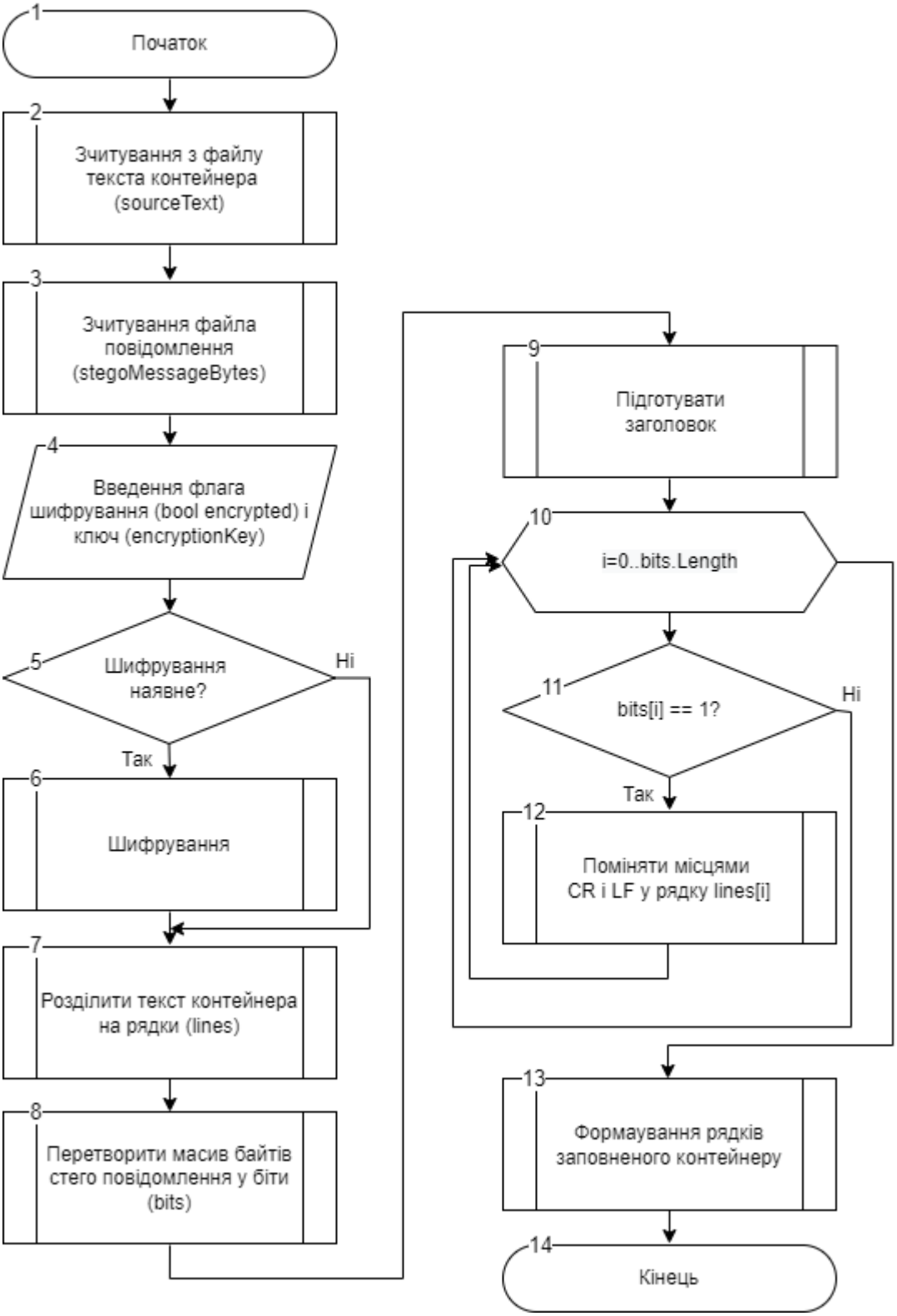


Рисунок 3.2 – Блок-схема узагальненого алгоритму виконання приховування методом зміни порядку проходження маркерів кінця рядка CR / LF

3.3 Розробка програмного забезпечення комплексу в режимі отримання таємного повідомлення

Блок-схема узагальненого алгоритму методу хвостових пробілів у режимі отримання таємного повідомлення наведена на рисунку 3.3. Вихідний код на мові C# наведено у Додатку В.

Блок 1 – запуск прогами у режимі отримання таємного повідомлення.

Блок 2– зчитування файлу з заповненим контейнером.

Блок 3 – введення ключа шифрування (за необхідності).

Блок 4 – поділ тексту контейнера на рядки.

Блок 5 – зчитування заголовка.

Блоки 6 – 11 – цикл, що формує байти із пів-байтів та записує їх до масиву.

Блок 12 – перевірка наявності шифрування.

Блок 13 – підпрограма з розшифруванням.

Блок 14 – отримання таємного повідомлення.

Блок 15 – закінчення виконання програми у даному режимі.

Блок-схема узагальненого алгоритму методу зміни порядку проходження маркерів кінця рядка CR / LF у режимі отримання таємного повідомлення наведена на рисунку 3.4. Вихідний код на мові C# наведено у Додатку Г.

Блок 1 – запуск прогами у режимі отримання таємного повідомлення.

Блок 2– зчитування файлу з заповненим контейнером.

Блок 3 – введення ключа шифрування (за необхідності).

Блок 4 – поділ тексту контейнера на рядки.

Блок 5 – зчитування заголовка.

Блоки 6 – 9 – цикл, що зчитує масив бітів таємного повідомлення.

Блок 10 – перетворення отриманих бітів у байти.

Блок 11-12 – перевірка наявності шифрування та підпрограма з розшифруванням.

Блок 13 – отримання таємного повідомлення.

Блок 14 – закінчення виконання програми у даному режимі.

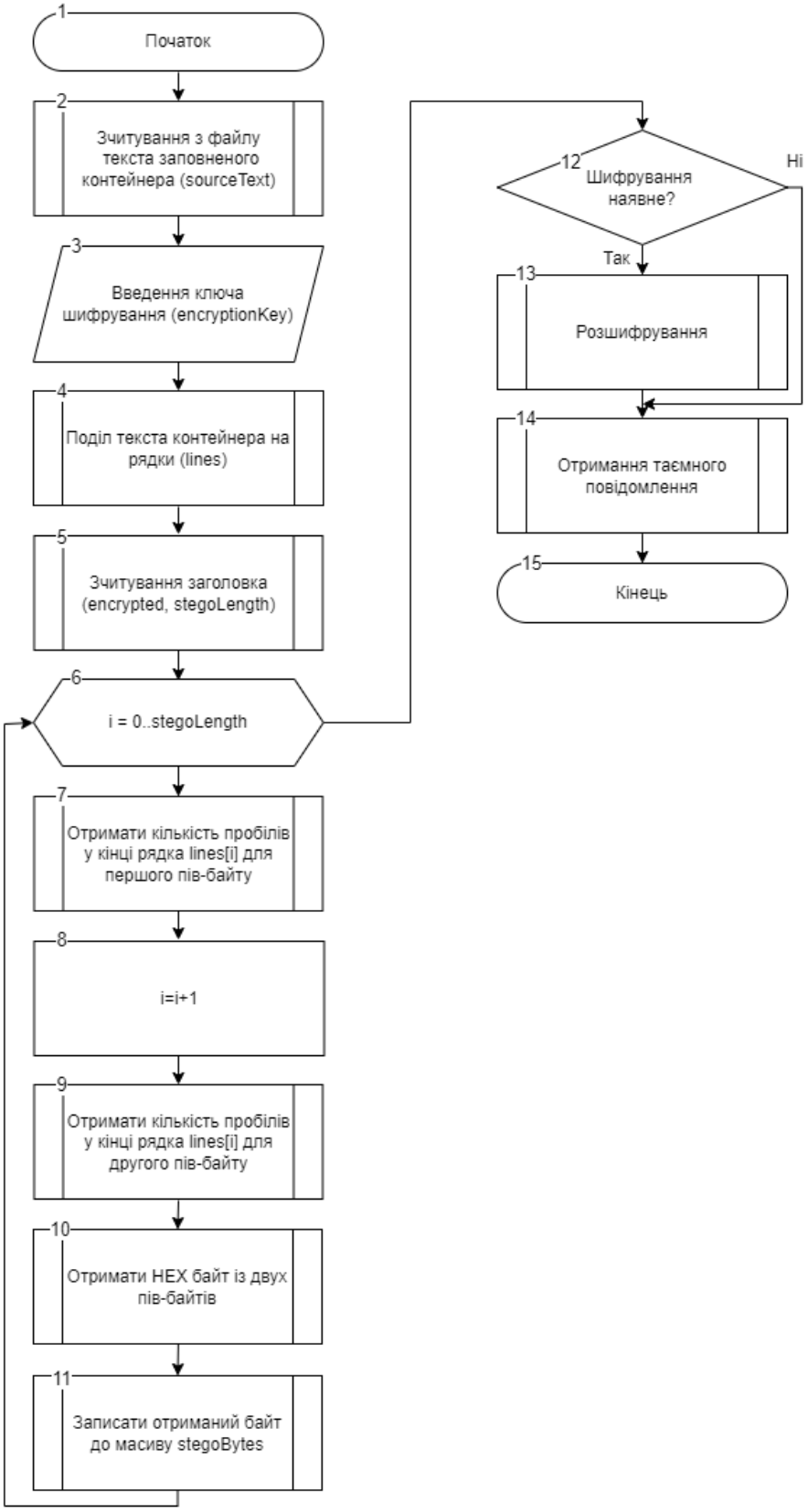


Рисунок 3.3 – Блок-схема узагальненого алгоритму виконання отримання таємного повідомлення методом хвостових пробілів

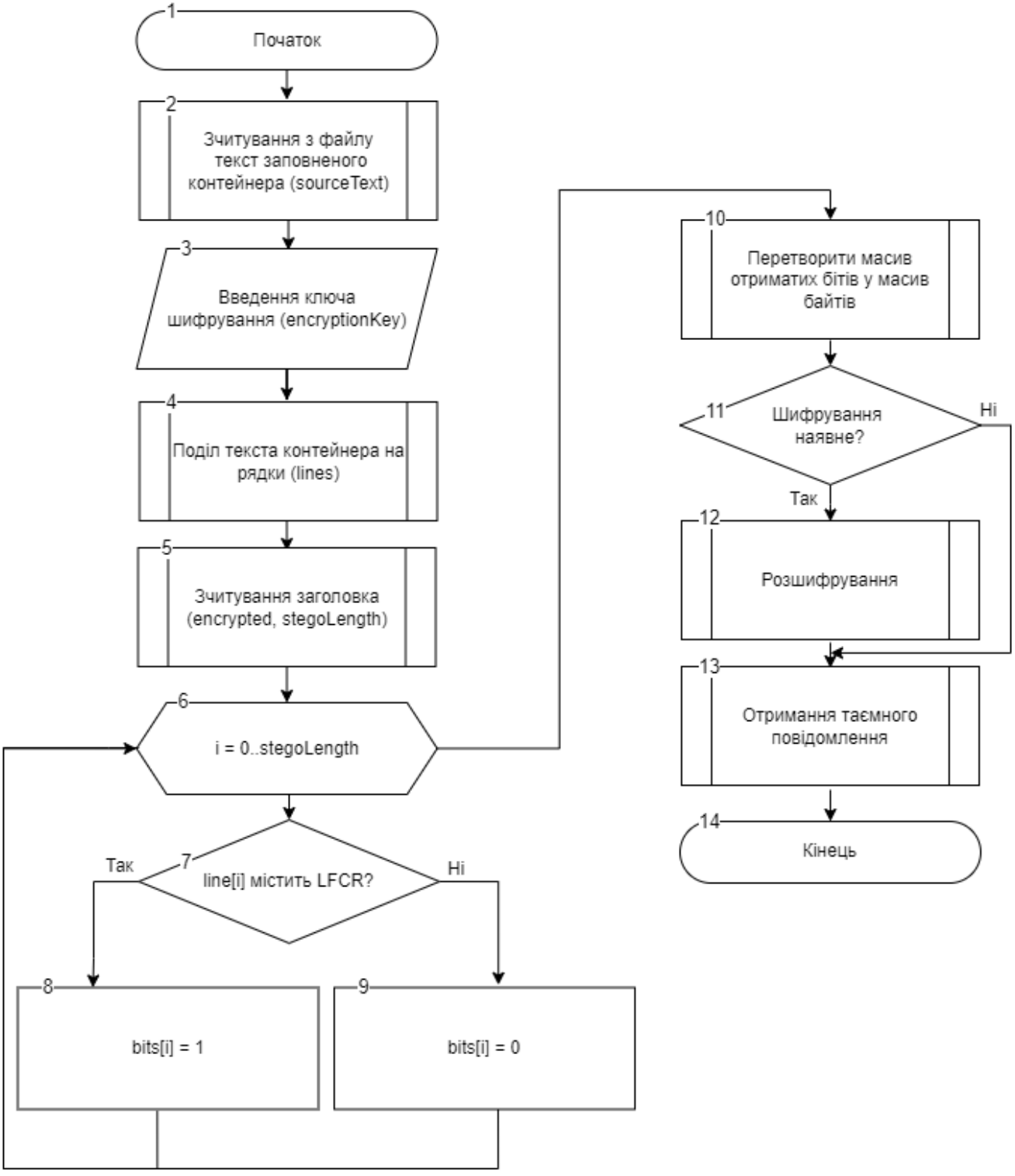


Рисунок 3.4 – Блок-схема узагальненого алгоритму виконання отримання таємного повідомлення методом зміни порядку проходження маркерів кінця рядка CR / LF

3.4 Перевірка працездатності програмного забезпечення

3.4.1 Перевірка модифікованого методу хвостових пробілів з наявним шифруванням.

У результаті вибору файлу з контейнером та файлу з таємним повідомленням, а також введення ключа шифрування, отримано заповнений контейнер (див. рис.3.5).

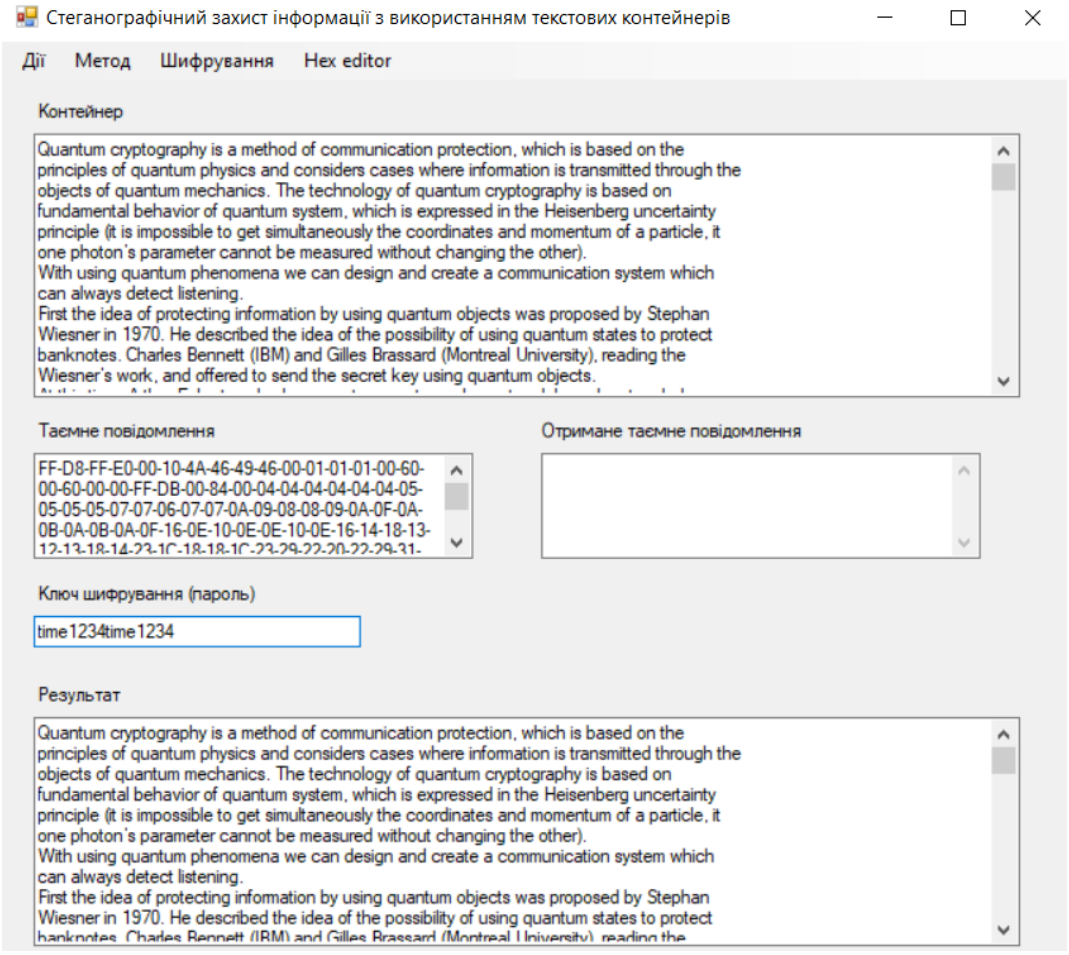


Рисунок 3.5 – Отримання заповненого контейнера методом хвостових пробілів

У результаті вибору файлу із заповненим контейнером та введенням ключа шифрування отримано таємне повідомлення (див.рис.3.6).

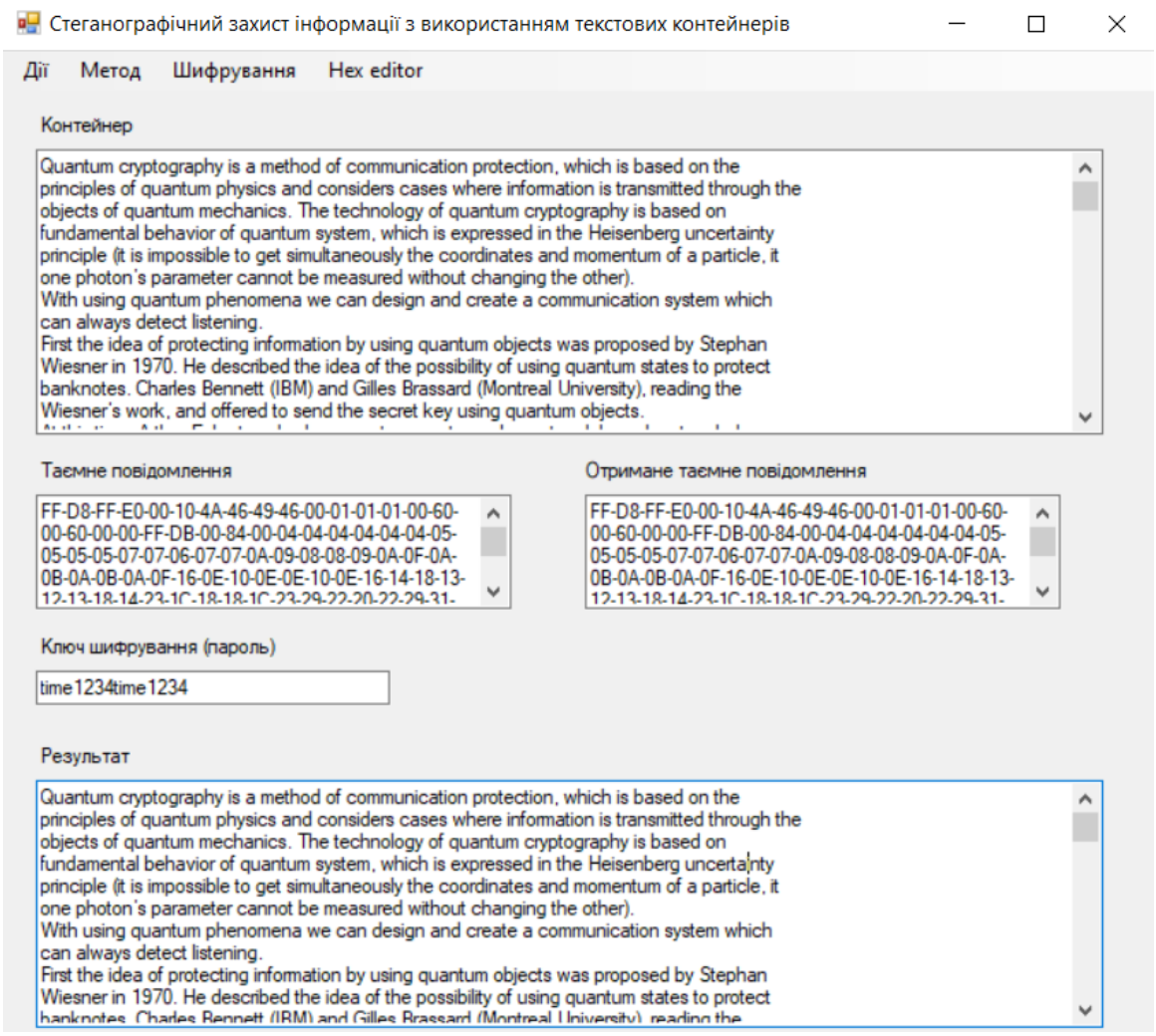


Рисунок 3.6 – Отримання таємного повідомлення методом хвостових пробілів

Для перегляду файлу із заповненим контейнером у вигляді байтів використовується додаток Hex Editor Neo [12]. Перший фрагмент заповненого контейнера відповідає заголовку таємного повідомлення (див. рис. 3.7). При виконанні даного методу для заголовка виділяється перші 6 рядків контейнера.

Розмір таємного повідомлення становить 1874 байт, але через особливості наявного шифрування його розмір збільшився до 1888 (дане число кратне 16). Тому в заголовку передається число 1888.

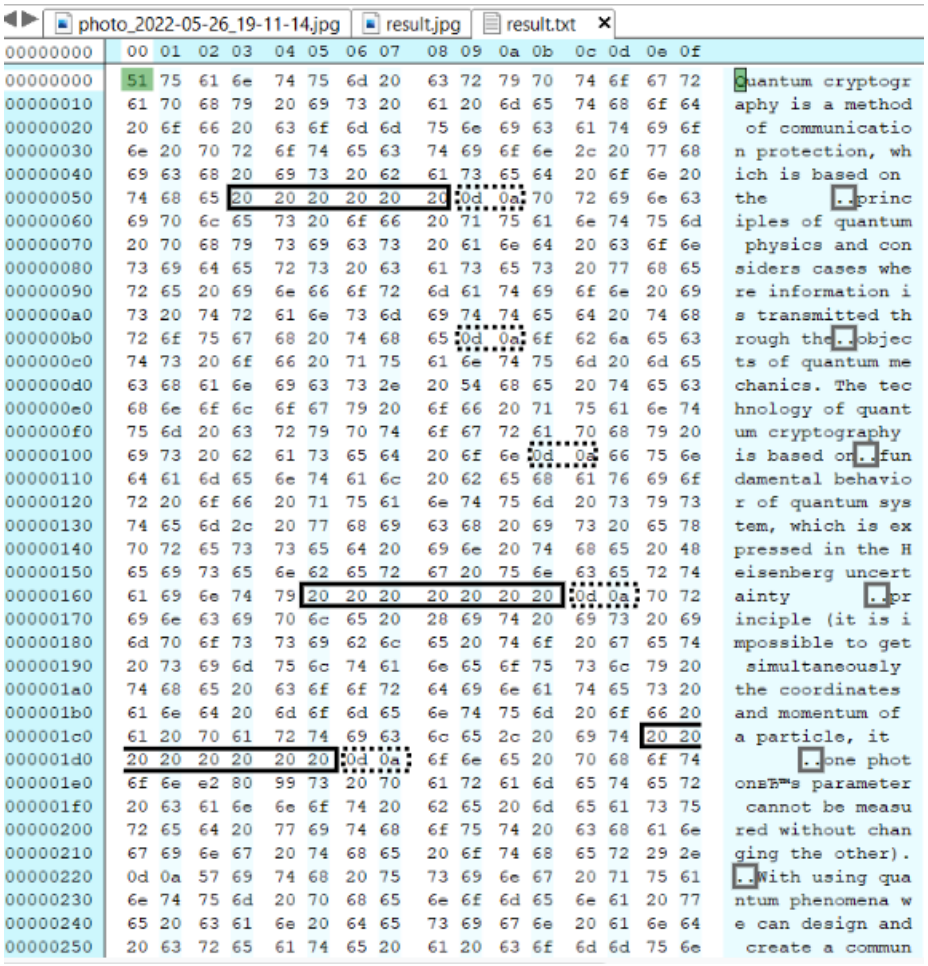


Рисунок 3.7 – Скріншот заповненого заголовком контейнера при приховуванні повідомлення методом хвостових пробілів

На рисунку хвостові пробіли (20) виділені чорною лінією та розташовані перед символами, які позначають кінець рядка (0d, 0a) та виділені пунктирною лінією. У тексті дані символи позначені двома крапками та обведені сірою лінією.

У рядках заголовка наявна така послідовність кількостей хвостових пробілів – 6 0 0 7 8 0, що відповідає даній довжині таємного повідомлення (1888 байт) та наявності шифрування.

Другий фрагмент заповненого контейнера відображає приховування перших трьох байтів зашифрованого таємного повідомлення (див. рис. 3.8).

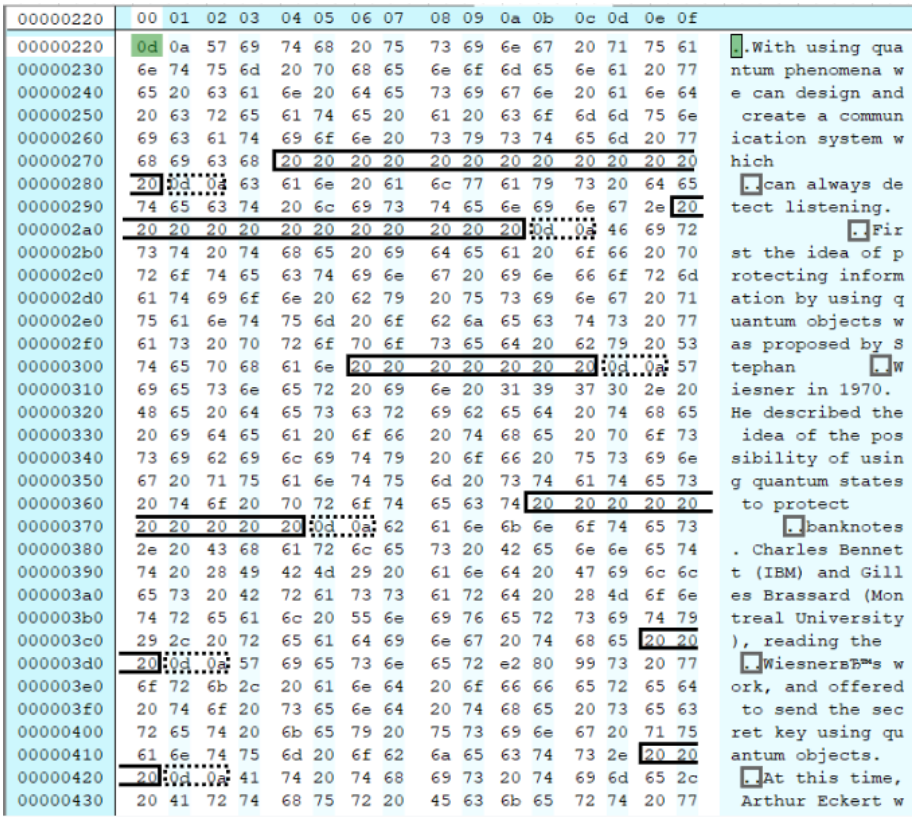


Рисунок 3.8 – Скріншот заповненого контейнера при приховуванні повідомлення методом хвостових пробілів

На рисунку хвостові пробіли (20) виділені чорною лінією та розташовані перед символами, які позначають кінець рядка (0d, 0a) та виділені пунктирною лінією. У тексті дані символи позначені двома крапками та обведені сірою лінією.

У рядках даного фрагменту наявна така послідовність кількостей хвостових пробілів – 13 12 7 10 3 3, що відповідає значенням перших трьох байтів зашифрованого таємного повідомлення – dc 7a 33.

3.4.2 Перевірка методу зміни порядку проходження маркерів кінця рядка CR / LF з відсутнім шифруванням.

У результаті вибору файлу з контейнером та файлу з таємним повідомленням отримано заповнений контейнер (див. рис.3.9).

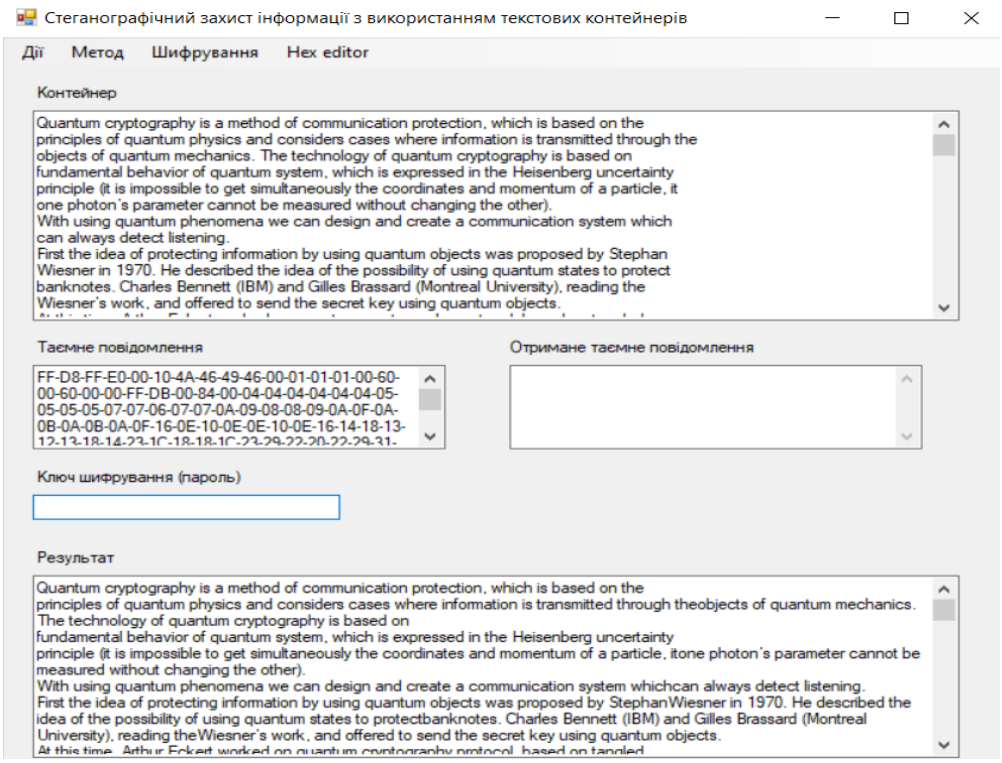


Рисунок 3.9 – Отримання заповненого контейнера методом CR / LF

У результаті вибору файлу із заповненим контейнером отримано таємне повідомлення (див.рис.3.10).

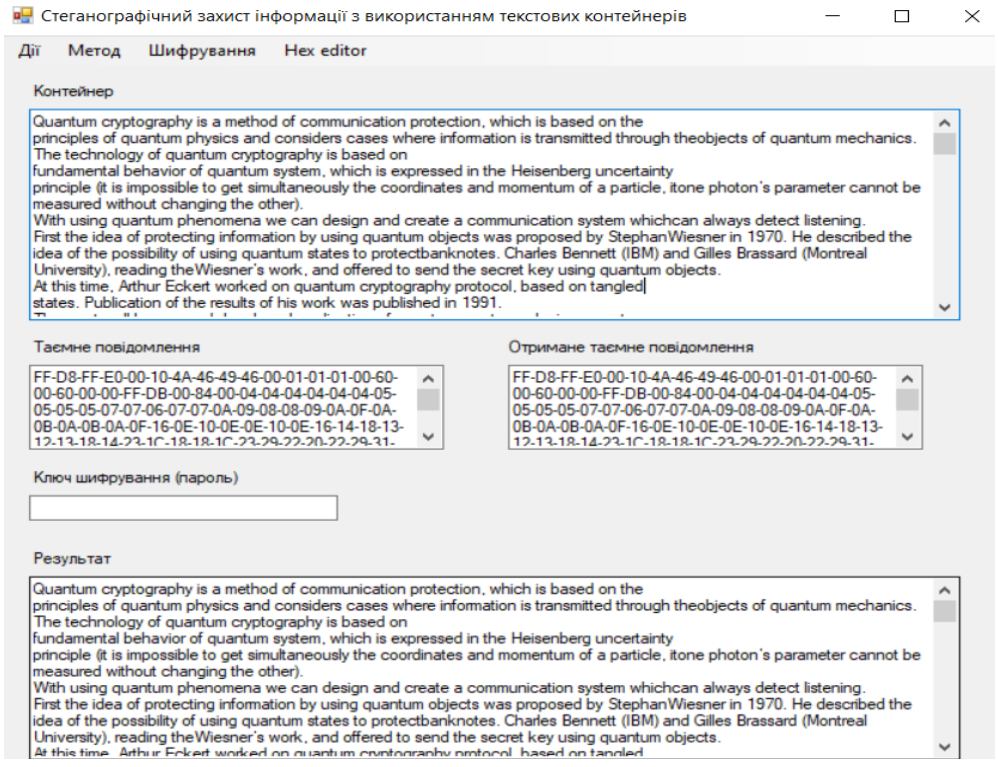


Рисунок 3.10 – Отримання таємного повідомлення методом CR / LF

При виконанні даного методу для заголовка виділяється перші 24 рядки контейнера. У заголовку передається число 1874, що відповідає розміру таємного повідомлення. Його представлення у двійковій системі числення - 0000 0000 0000 0111 0101 0010.

На рисунках 3.11-3.13 символам переведення рядка (CR) і повернення каретки (LF) відповідають символи 0d та 0a відповідно. Вони виділені пунктирною лінією, а у тексті дані символи позначені двома крапками та обведені сірою лінією.

Звичайний порядок проходження CR / LF (0d 0a) відповідає нулю, а інвертований LF / CR (0a 0d) – одиниці.

Перший фрагмент заповненого контейнера відповідає 8 молодшим бітам (0101 0010) заголовку таємного повідомлення (див. рис. 3.11).

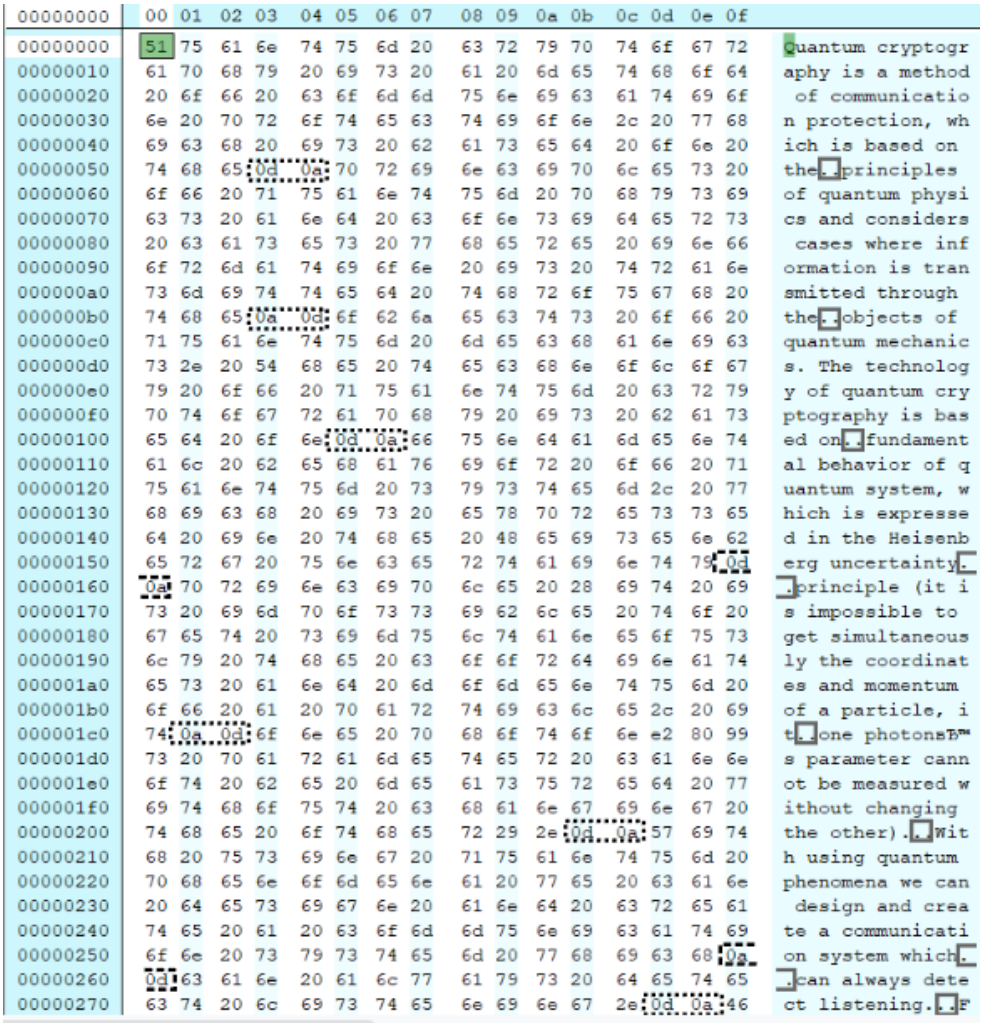


Рисунок 3.11 – Перший скріншот заповненого заголовком контейнера при приховуванні методом CR / LF

Другий фрагмент заповненого контейнера відповідає 8 середнім бітам (0000 0111) заголовку таємного повідомлення (див. рис. 3.12).

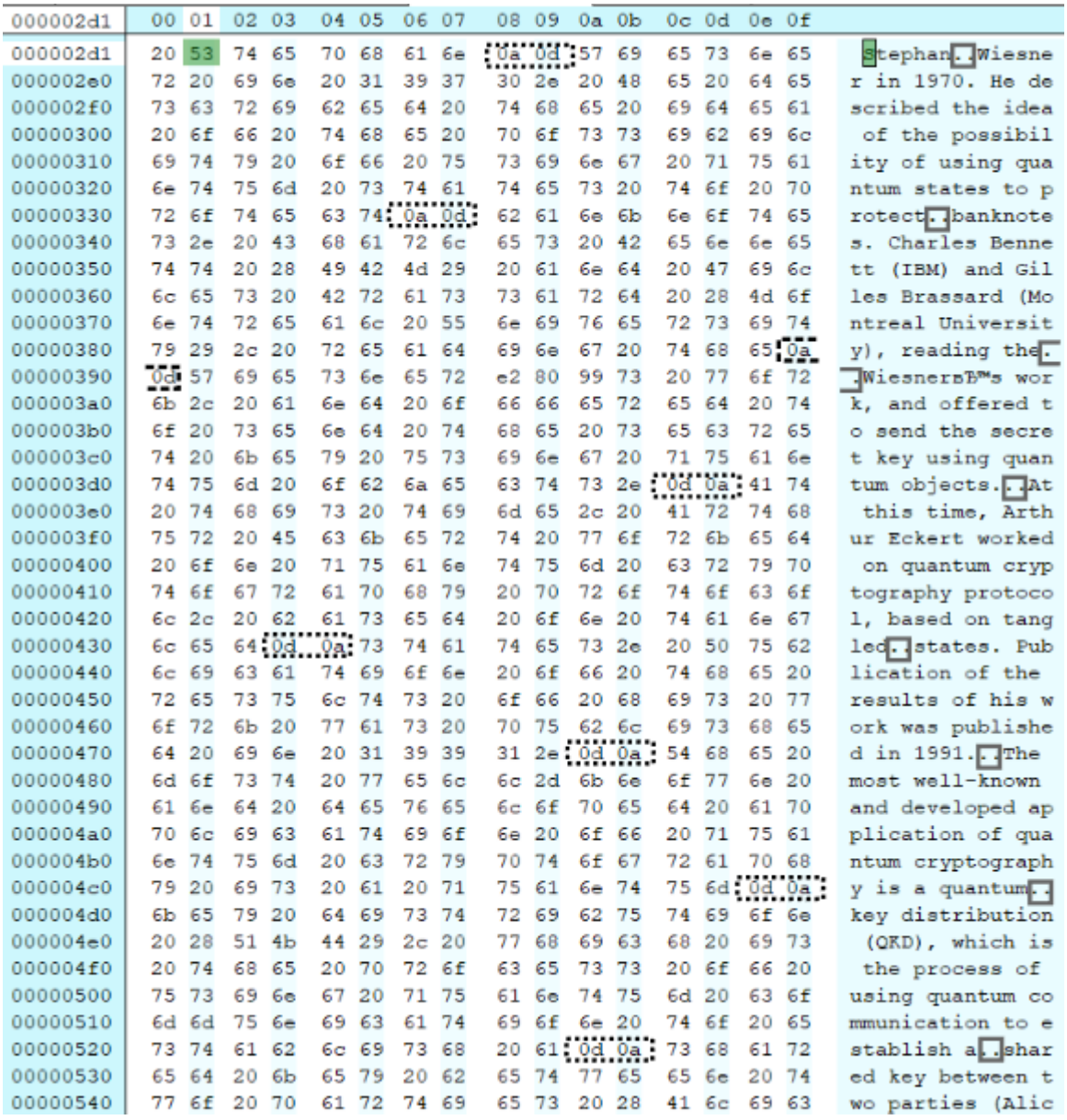
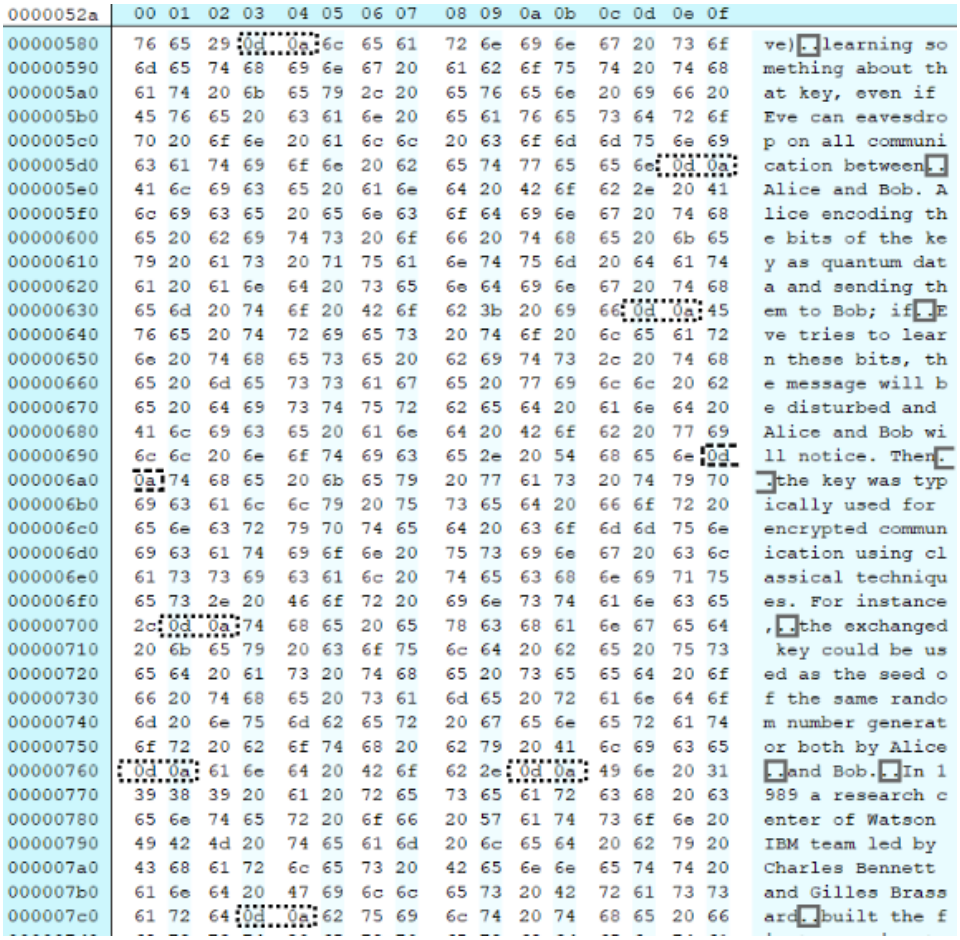


Рисунок 3.12 – Другий скріншот заповненого заголовком контейнера при приховуванні методом CR / LF

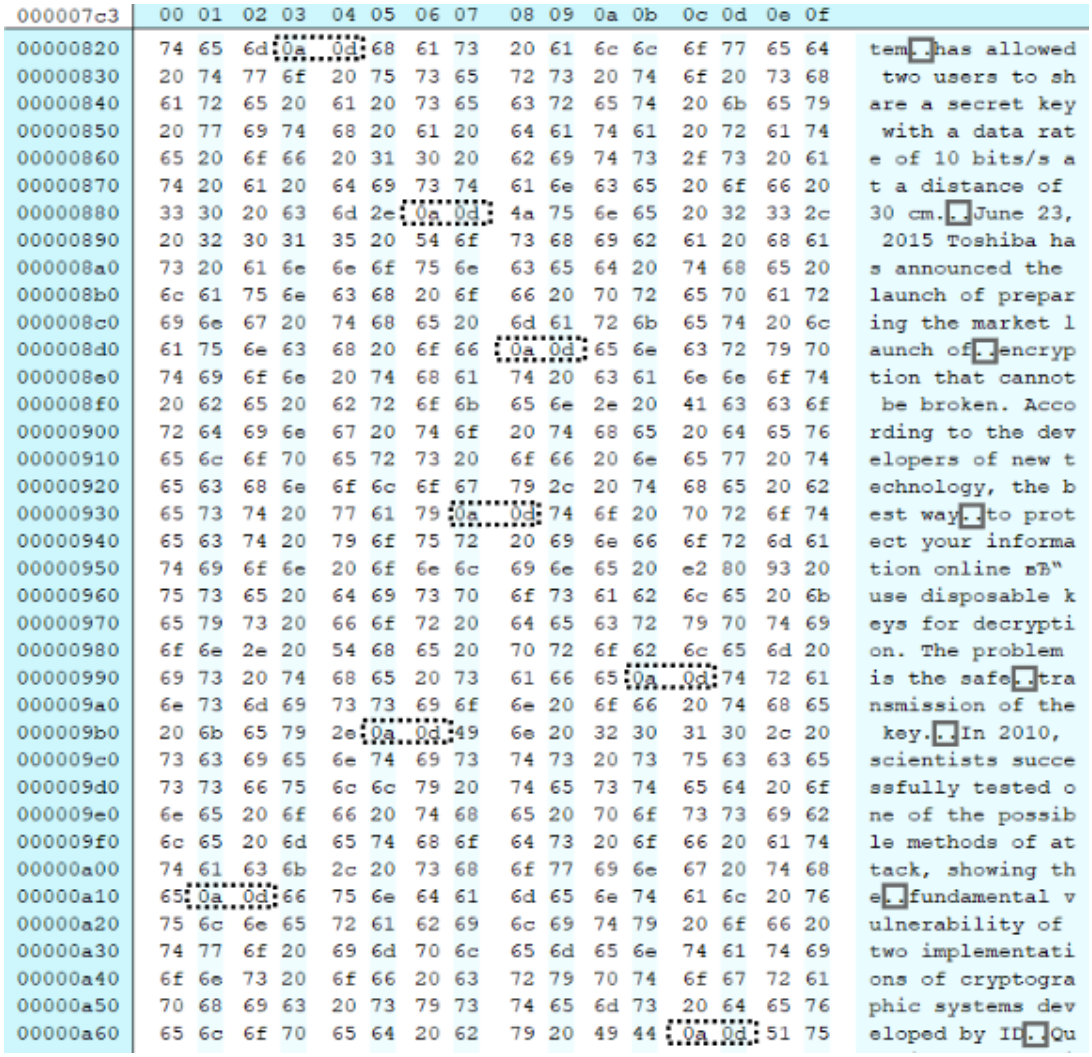
Третій фрагмент заповненого контейнера відповідає 8 старшим бітам (0000 0000) заголовку таємного повідомлення (див. рис. 3.13).



```
0000052a  00 01 02 03  04 05 06 07  08 09 0a 0b  0c 0d 0e 0f
00000580  76 65 29 0d  0a 6c 65 61  72 6e 69 6e  67 20 73 6f  ve).·learning so
00000590  6d 65 74 68  69 6e 67 20  61 62 6f 75  74 20 74 68  mething about th
000005a0  61 74 20 6b  65 79 2c 20  65 76 65 6e  20 69 66 20  at key, even if
000005b0  45 76 65 20  63 61 6e 20  65 61 76 65  73 64 72 6f  Eve can eavesdro
000005c0  70 20 6f 6e  20 61 6c 6c  20 63 6f 6d  6d 75 6e 69  p on all communi
000005d0  63 61 74 69  6f 6e 20 62  65 74 77 65  65 6e 0d 0a  cation between··
000005e0  41 6c 69 63  65 20 61 6e  64 20 42 6f  62 2e 20 41  Alice and Bob. A
000005f0  6c 69 63 65  20 65 6e 63  6f 64 69 6e  67 20 74 68  lice encoding th
00000600  65 20 62 69  74 73 20 6f  66 20 74 68  65 20 6b 65  e bits of the ke
00000610  79 20 61 73  20 71 75 61  6e 74 75 6d  20 64 61 74  y as quantum dat
00000620  61 20 61 6e  64 20 73 65  6e 64 69 6e  67 20 74 68  a and sending th
00000630  65 6d 20 74  6f 20 42 6f  62 3b 20 69  66 0d 0a 45  em to Bob; if··E
00000640  76 65 20 74  72 69 65 73  20 74 6f 20  6c 65 61 72  ve tries to lear
00000650  6e 20 74 68  65 73 65 20  62 69 74 73  2c 20 74 68  n these bits, th
00000660  65 20 6d 65  73 73 61 67  65 20 77 69  6c 6c 20 62  e message will b
00000670  65 20 64 69  73 74 75 72  62 65 64 20  61 6e 64 20  e disturbed and
00000680  41 6c 69 63  65 20 61 6e  64 20 42 6f  62 20 77 69  Alice and Bob wi
00000690  6c 6c 20 6e  6f 74 69 63  65 2e 20 54  68 65 6e 0d  ll notice. Then·
000006a0  0a 74 68 65  20 6b 65 79  20 77 61 73  20 74 79 70  ·the key was typ
000006b0  69 63 61 6c  6c 79 20 75  73 65 64 20  66 6f 72 20  ically used for
000006c0  65 6e 63 72  79 70 74 65  64 20 63 6f  6d 6d 75 6e  encrypted commun
000006d0  69 63 61 74  69 6f 6e 20  75 73 69 6e  67 20 63 6c  ication using cl
000006e0  61 73 73 69  63 61 6c 20  74 65 63 68  6e 69 71 75  assical techniqu
000006f0  65 73 2e 20  46 6f 72 20  69 6e 73 74  61 6e 63 65  es. For instance
00000700  2c 0d 0a 74  68 65 20 65  78 63 68 61  6e 67 65 64  ,··the exchanged
00000710  20 6b 65 79  20 63 6f 75  6c 64 20 62  65 20 75 73  key could be us
00000720  65 64 20 61  73 20 74 68  65 20 73 65  65 64 20 6f  ed as the seed o
00000730  66 20 74 68  65 20 73 61  6d 65 20 72  61 6e 64 6f  f the same rando
00000740  6d 20 6e 75  6d 62 65 72  20 67 65 6e  65 72 61 74  m number generat
00000750  6f 72 20 62  6f 74 68 20  62 79 20 41  6c 69 63 65  or both by Alice
00000760  0d 0a 61 6e  64 20 42 6f  62 2e 0d 0a  49 6e 20 31  ··and Bob.··In 1
00000770  39 38 39 20  61 20 72 65  73 65 61 72  63 68 20 63  989 a research c
00000780  65 6e 74 65  72 20 6f 66  20 57 61 74  73 6f 6e 20  enter of Watson
00000790  49 42 4d 20  74 65 61 6d  20 6c 65 64  20 62 79 20  IBM team led by
000007a0  43 68 61 72  6c 65 73 20  42 65 6e 6e  65 74 74 20  Charles Bennett
000007b0  61 6e 64 20  47 69 6c 6c  65 73 20 42  72 61 73 73  and Gilles Brass
000007c0  61 72 64 0d  0a 62 75 69  6c 74 20 74  68 65 20 66  ard··built the f
```

Рисунок 3.13 – Третій скріншот заповненого заголовком контейнера при приховуванні методом CR / LF

Наступний фрагмент заповненого контейнера відображає приховування першого байту зашифрованого таємного повідомлення (див. рис. 3.14). У рядках даного фрагменту наявна така послідовність бітів – 1111 1111, що відповідає значенню першого байту таємного повідомлення – ff.



```
000007c3  00 01 02 03  04 05 06 07  08 09 0a 0b  0c 0d 0e 0f
00000820  74 65 6d 0a  0d 68 61 73  20 61 6c 6c  6f 77 65 64  tem..has allowed
00000830  20 74 77 6f  20 75 73 65  72 73 20 74  6f 20 73 68   two users to sh
00000840  61 72 65 20  61 20 73 65  63 72 65 74  20 6b 65 79  are a secret key
00000850  20 77 69 74  68 20 61 20  64 61 74 61  20 72 61 74   with a data rat
00000860  65 20 6f 66  20 31 30 20  62 69 74 73  2f 73 20 61  e of 10 bits/s a
00000870  74 20 61 20  64 69 73 74  61 6e 63 65  20 6f 66 20  t a distance of
00000880  33 30 20 63  6d 2e 0a 0d  4a 75 6e 65  20 32 33 2c  30 cm...June 23,
00000890  20 32 30 31  35 20 54 6f  73 68 69 62  61 20 68 61   2015 Toshiba ha
000008a0  73 20 61 6e  6e 6f 75 6e  63 65 64 20  74 68 65 20  s announced the
000008b0  6c 61 75 6e  63 68 20 6f  66 20 70 72  65 70 61 72  launch of prepar
000008c0  69 6e 67 20  74 68 65 20  6d 61 72 6b  65 74 20 6c  ing the market l
000008d0  61 75 6e 63  68 20 6f 66  0a 0d 65 6e  63 72 79 70  aunch of..encryp
000008e0  74 69 6f 6e  20 74 68 61  74 20 63 61  6e 6e 6f 74  tion that cannot
000008f0  20 62 65 20  62 72 6f 6b  65 6e 2e 20  41 63 63 6f   be broken. Acco
00000900  72 64 69 6e  67 20 74 6f  20 74 68 65  20 64 65 76  rding to the dev
00000910  65 6c 6f 70  65 72 73 20  6f 66 20 6e  65 77 20 74  elopers of new t
00000920  65 63 68 6e  6f 6c 6f 67  79 2c 20 74  68 65 20 62  echnology, the b
00000930  65 73 74 20  77 61 79 0a  0d 74 6f 20  70 72 6f 74  est way..to prot
00000940  65 63 74 20  79 6f 75 72  20 69 6e 66  6f 72 6d 61  ect your informa
00000950  74 69 6f 6e  20 6f 6e 6c  69 6e 65 20  e2 80 93 20  tion online вЂ“
00000960  75 73 65 20  64 69 73 70  6f 73 61 62  6c 65 20 6b  use disposable k
00000970  65 79 73 20  66 6f 72 20  64 65 63 72  79 70 74 69  eys for decrypti
00000980  6f 6e 2e 20  54 68 65 20  70 72 6f 62  6c 65 6d 20  on. The problem
00000990  69 73 20 74  68 65 20 73  61 66 65 0a  0d 74 72 61  is the safe..tra
000009a0  6e 73 6d 69  73 73 69 6f  6e 20 6f 66  20 74 68 65  nsmission of the
000009b0  20 6b 65 79  2e 0a 0d 49  6e 20 32 30  31 30 2c 20   key...In 2010,
000009c0  73 63 69 65  6e 74 69 73  74 73 20 73  75 63 63 65  scientists succe
000009d0  73 73 66 75  6c 6c 79 20  74 65 73 74  65 64 20 6f  ssfully tested o
000009e0  6e 65 20 6f  66 20 74 68  65 20 70 6f  73 73 69 62  ne of the possib
000009f0  6c 65 20 6d  65 74 68 6f  64 73 20 6f  66 20 61 74  le methods of at
00000a00  74 61 63 6b  2c 20 73 68  6f 77 69 6e  67 20 74 68  tack, showing th
00000a10  65 0a 0d 66  75 6e 64 61  6d 65 6e 74  61 6c 20 76  e..fundamental v
00000a20  75 6c 6e 65  72 61 62 69  6c 69 74 79  20 6f 66 20  ulnerability of
00000a30  74 77 6f 20  69 6d 70 6c  65 6d 65 6e  74 61 74 69  two implementati
00000a40  6f 6e 73 20  6f 66 20 63  72 79 70 74  6f 67 72 61  ons of cryptogra
00000a50  70 68 69 63  20 73 79 73  74 65 6d 73  20 64 65 76  phic systems dev
00000a60  65 6c 6f 70  65 64 20 62  79 20 49 44  0a 0d 51 75  eloped by ID..Qu
```

Рисунок 3.14 - Скріншот заповненого контейнера при приховуванні повідомлення методом CR / LF

3.5 Інструкція з використання комплексу

Розроблюваний комплекс може використовуватись як засіб стеганографічного захисту інформації та як навчальна програма. Головне вікно програми містить усі необхідні поля та кнопки (див. рис.3.15).

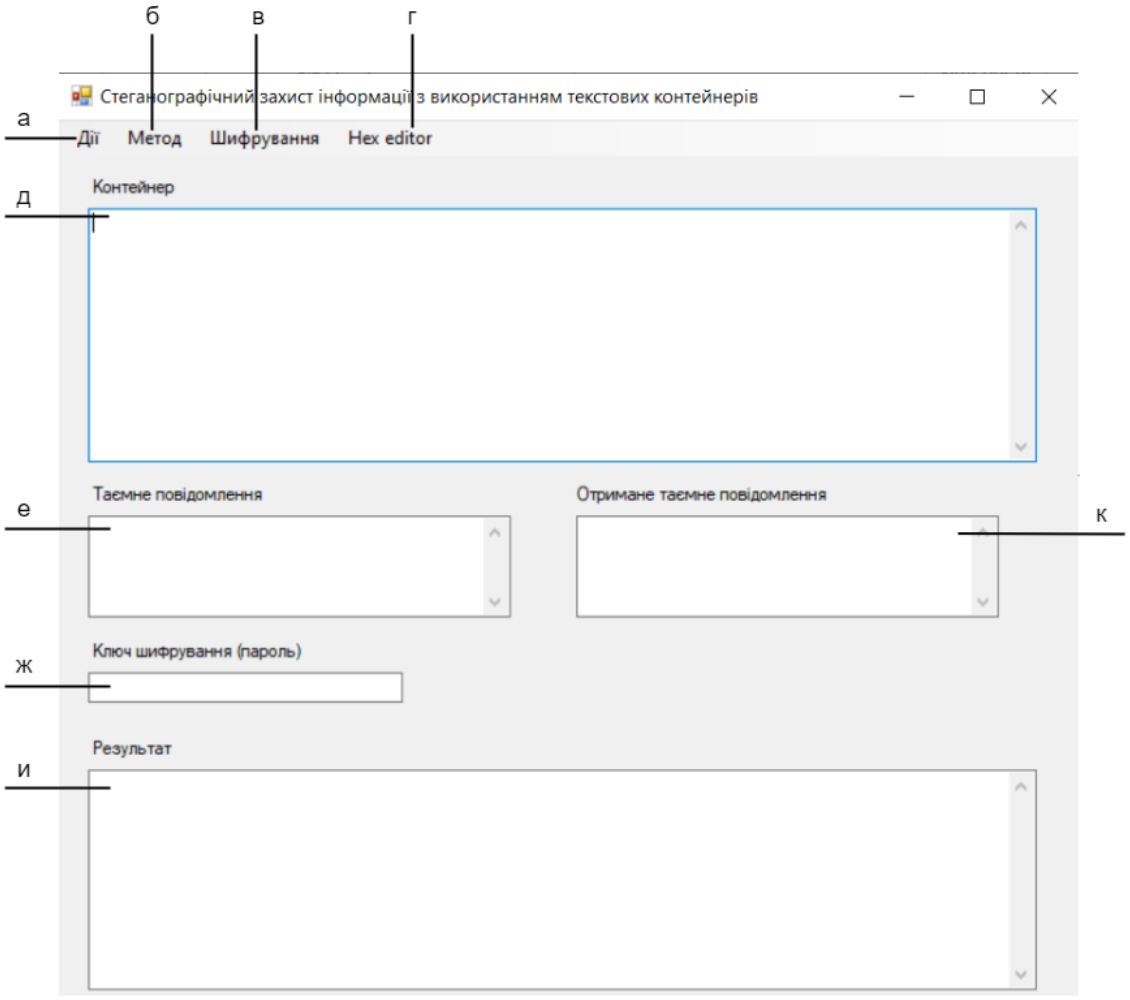


Рисунок 3.15 - Головне вікно програми

Головне вікно програми поділяється на такі частини:

а) Пункт меню «Дії»

Містить такі підпункти меню (див Рис. 3.16):

1) Обрати контейнер - дозволяє зчитати з файлу текстовий файл та відобразити його користувачеві. Використовується для зчитування звичайного, або заповненого контейнера.

2) Обрати таємне повідомлення - дозволяє обрати файл як таємне повідомлення, зчитує файл у вигляді байтів та відображає користувачеві у HEX форматі.
3) Отримати заповнений контейнер - виконує приховування обраного таємного повідомлення в обраному контейнері. Відображає заповнений контейнер користувачеві у полі «Поле змісту заповненого контейнеру» (див. п. № и).
4) Отримати таємне повідомлення – виконує отримання таємного повідомлення із обраного заповненого контейнера. Виводить отримане повідомлення у поле «Поле змісту таємного повідомлення у HEX форматі, отриманого із заповненого контейнера» (див п. № к)
5) Записати у файл заповнений контейнер – дозволяє зберегти отримане таємне повідомлення у вигляді файлу. Розширення файлу вводить сам користувач.

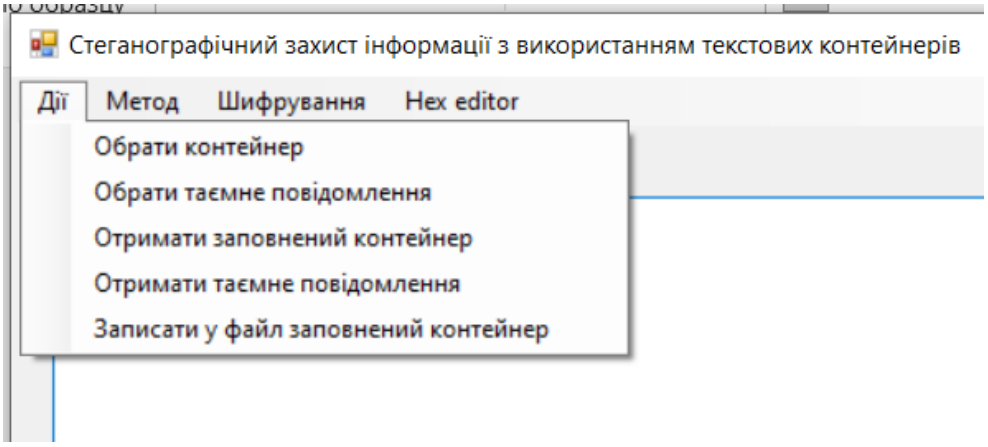


Рис 3.16 - Підпункти меню «Дії»

б)Пункт меню «Метод»

Містить такі підпункти меню(див. Рис. 3.17):

1) Метод CR/LF - приховування та отримання таємного повідомлення відбувається методом заміни символів переносу рядка та повернення каретки.
2) Метод хвостових пробілів(модифікований) – приховування та отримання таємного повідомлення відбувається методом додавання кінцевих пробілів до рядків контейнера.

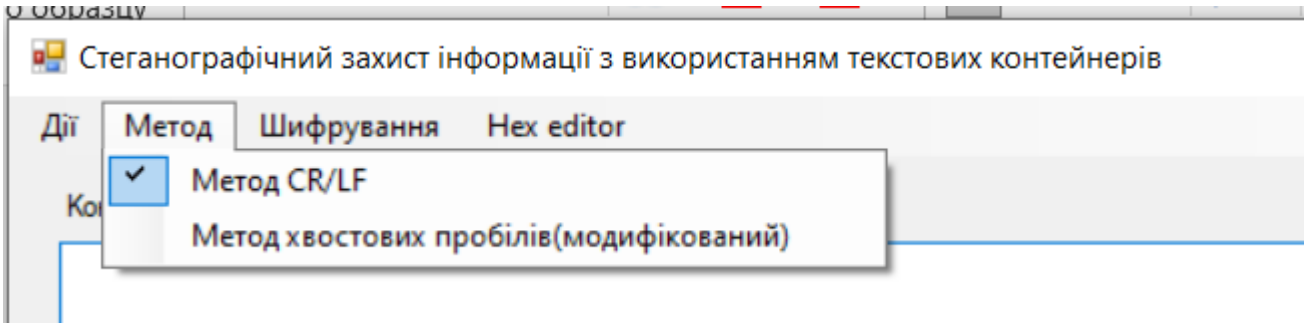


Рисунок 3.17 - Підпункти меню «Метод»

в) Пункт меню «Шифрування»

Має такі підпункти (див. Рис. 3.18):

1) Наявне – при наявному шифруванні перед приховуванням відбувається шифрування таємного повідомлення ключем, введеним у полі «Поле ключа шифрування, введеного користувачем» (див. п. ж) методом AES128. Після отримання таємного повідомлення відбувається дешифрування.
2) Відсутнє – шифрування та дешифрування таємного повідомлення не відбувається.

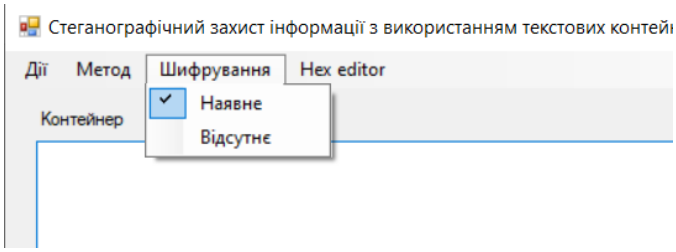


Рисунок 3.18 - Підпункти меню «Шифування»

г) Пункт меню «Hex Editor»

Після проведення операцій приховування та отримання таємного повідомлення дозволяє відкрити додаткове програмне забезпечення «Hex Editor», у якому наявно відображається таємне повідомлення та заповнений контейнер у вигляді байтів.

д) Поле тексту контейнера, зчитаного з файлу або введеного користувачем

Використовується користувачем для вводу звичайного або заповненого контейнера.

е)Поле змісту таємного повідомлення у HEX форматі, зчитується з файлу

Використовується користувачем для вводу таємного повідомлення. Заповнити це поле можливо тільки через пункт меню «Обрати таємне повідомлення» (див. п. а.2).

ж) Поле ключа шифрування, введеного користувачем

Використовується користувачем для вводу ключа шифрування якщо воно наявне, повинно містити 16 символів. Якщо шифрування не є наявним, заповнювати це поле непотрібно.

и) Поле змісту заповненого контейнеру

Це поле використовується для відображення заповненого контейнера після приховування таємного повідомлення.

к) Поле змісту таємного повідомлення у HEX форматі, отриманого із заповненого контейнера

Це поле заповнюється після отримання таємного повідомлення із заповненого контейнера.

3.6 Висновки за розділом

Середовищем розробки обрано Visual Studio 2022, мовою розробки обрано C#. Технологія Windows Forms.NET була обрана задля створення графічного інтерфейсу даного комплексу. Розроблено програмне забезпечення комплексу в режимах приховування та отримання таємного повідомлення, створені відповідні блок-схеми. Проведена перевірка працездатності програмного забезпечення у двох режимах: перевірка модифікованого методу хвостових пробілів з наявним шифруванням та перевірка методу зміни порядку проходження маркерів кінця рядка CR / LF з відсутнім шифруванням. Створена інструкція з використання даного комплексу.

ВИСНОВКИ

У даній роботі розроблено програмний комплекс, який демонструє методи стеганографічного захисту інформації, реалізуючи приховування таємного повідомлення в текстовий контейнер та його отримування.

Наведено загальні відомості в галузі стеганографії. Описано та створено порівняльну характеристику методів текстової стеганографії. Вирішено використовувати метод зміни порядку проходження маркерів кінця рядка CR / LF та модифікований метод хвостових пробілів для реалізації в роботі.

Описано функціонування даного комплексу у двох режимах: приховування та отримання таємного повідомлення. Для посилення захисту інформації вирішено використовувати шифрування AES128. Створено структуру даних, приведено структуру заголовка таємного повідомлення.

Обрано середовище розробки, мову програмування та технологію для створення графічного інтерфейсу комплексу. Розроблено програмне забезпечення комплексу та створені відповідні блок-схеми узагальнених алгоритмів методів в режимах приховування та отримання таємного повідомлення. Проведена перевірка працездатності програмного забезпечення. Створена інструкція з використання даного комплексу.

Розроблений комплекс може бути використаний у навчальному процесі студентів відповідних спеціальностей при проведенні лабораторних і практичних робіт.

ПЕРЕЛІК ПОСИЛАНЬ

1. Грибунин В. Г. Цифровая стеганография [Електронний ресурс]: електронна книга / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев /- 2013, - 80 с. - Режим доступу до книги: https://booksonline.com.ua/view.php?book=161356
2. Шелест М. Є., Комп'ютерна стеганографія та її можливості [Електронний ресурс]: науково-практичний журнал/ М. Є. Шелест, В. І. Андреев – Сучасна спеціальна техніка №1(24), 2011. – Режим доступу до журн.: http://elar.naiau.kiev.ua/bitstream/123456789/2200/1/%D0%A8%D0%B5%D0%BB%D0%B5%D1%81%D1%82%20%D0%9C.%20%D0%84..pdf
3. Ross Anderson. Information Hiding: First International Workshop, (Cambridge, U.K., May 30 - June 1, 1996.) Proceedings, Том 1, PH
4. Бондаренко Л.Л., Пархоменко І.І.. Види атак на стеганографічні системи [Електронний ресурс]: – Режим доступу до ресурсу: http://www.rusnauka.com/25_SEN_2015/Informatica/4_198994.doc.htm
5. Кузнецов О. О. Стеганографія [Електронний ресурс]: навч. посібник/ О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків: ХНЕУ, 2011. – Режим доступу до посібника: https://studfile.net/preview/16435716/
6. Сопронюк Ф. А. Информационные технологии и защита информации в информационно-коммуникационных системах [Електронний ресурс]: монографія/ Ф. А. Сопронюк, Н. М. Кораблев, В. В. Хома. – Харьков, 2015. – Режим доступу до монографії: https://docplayer.com/42516646-Informacionnye-tehnologii-i-zashchita-informacii-v-informacionno-kommunikacionnyh-sistemah.html
7. Advanced encryption standard (AES) [Електронний ресурс]: Federal Information Processing Standards Publication 197. – November 26, 2001. – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf
8. What's new in Visual Studio 2022 [Електронний ресурс]: Microsoft Documentation. – 2022. – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/visualstudio/ide/whats-new-visual-studio-2022?view=vs-2022
9. A tour of the C# language [Електронний ресурс]: Microsoft Documentation. –2022. – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/dotnet/csharp/tour-of-csharp/
10. Desktop Guide (Windows Forms .NET) [Електронний ресурс]: Microsoft Documentation. –2021. – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/dotnet/desktop/winforms/overview/?view=netdesktop-6.0
11. Aes Class [Електронний ресурс]: Microsoft Documentation. – Режим доступу до ресурсу: https://docs.microsoft.com/enus/dotnet/api/system.security.cryptography.aes?view=net-6.0
12. Скачать Hex Editor [Електронний ресурс]: softportal. – Режим доступу до ресурсу: https://www.softportal.com/get-4031-hex-editor.html