ПРЕЗЕНТАЦІЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА ТЕМУ:

ПІДВИЩЕННЯ ЗАХИСТУ ЦИФРОВИХ ЗОБРАЖЕНЬ ЗА РАХУНОК ДОДАТКОВОЇ ІДЕНТИФІКАЦІЇ ЗА ВИКОРИСТАННЯМ ВОДЯНИХ ЗНАКІВ ТА ПЕРЕВІРКИ ВІДДАЛЕНИМ СЕРВЕРОМ

КУЛІШ ДАРИНИ
УБ-16м
Науковий керівник:
к.т.н., доцент Карпінець В.В.

ПОСТАНОВКА ЗАДАЧІ

- Мета роботи: підвищення рівня захисту цифрових зображень.
- Основні завдання: проаналізувати, спроектувати та розробити.
- Об’єкт дослідження: процес підвищення захисту зображень шляхом додаткової ідентифікації за використанням ЦВЗ та перевірки на унікальність (ідентичність) віддаленим сервером.
- Предмет дослідження: стеганографічні та криптографічні методи захисту, методи хешування даних задля захисту зображення.

АКТУАЛЬНІСТЬ РОБОТИ

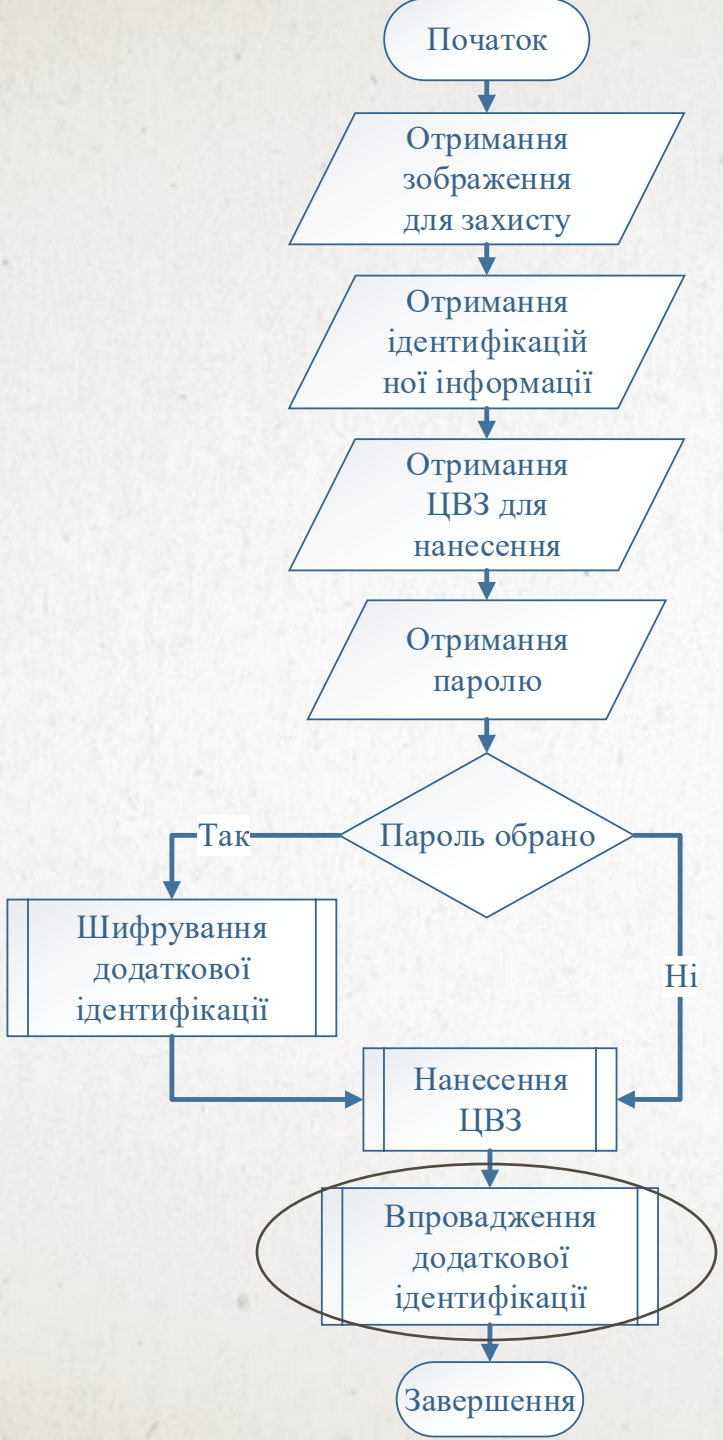
В даний час широко поширена передача цифрових зображень від авторів споживачам або посередникам засобами Internet. Легкість копіювання таких зображень призводить до того, що постійно зростає число порушень авторських прав на графічні роботи, в зв'язку з незаконним використанням цих робіт, зокрема, шляхом їх несанкціонованого розміщення в інтернет-галереях. Таким чином, актуальною є проблема захисту зображень та прав авторів цифрових графічних робіт.

ВІЗУАЛІЗАЦІЯ ЗАХИСТУ

- Просторовий метод нанесення
- Захист від НСК
- Можливість обирати зображення для вбудовування

- Вбудовування ідентифікаційної інформації
- Можливість встановлення паролю
- Шифрування даних AES-шифром

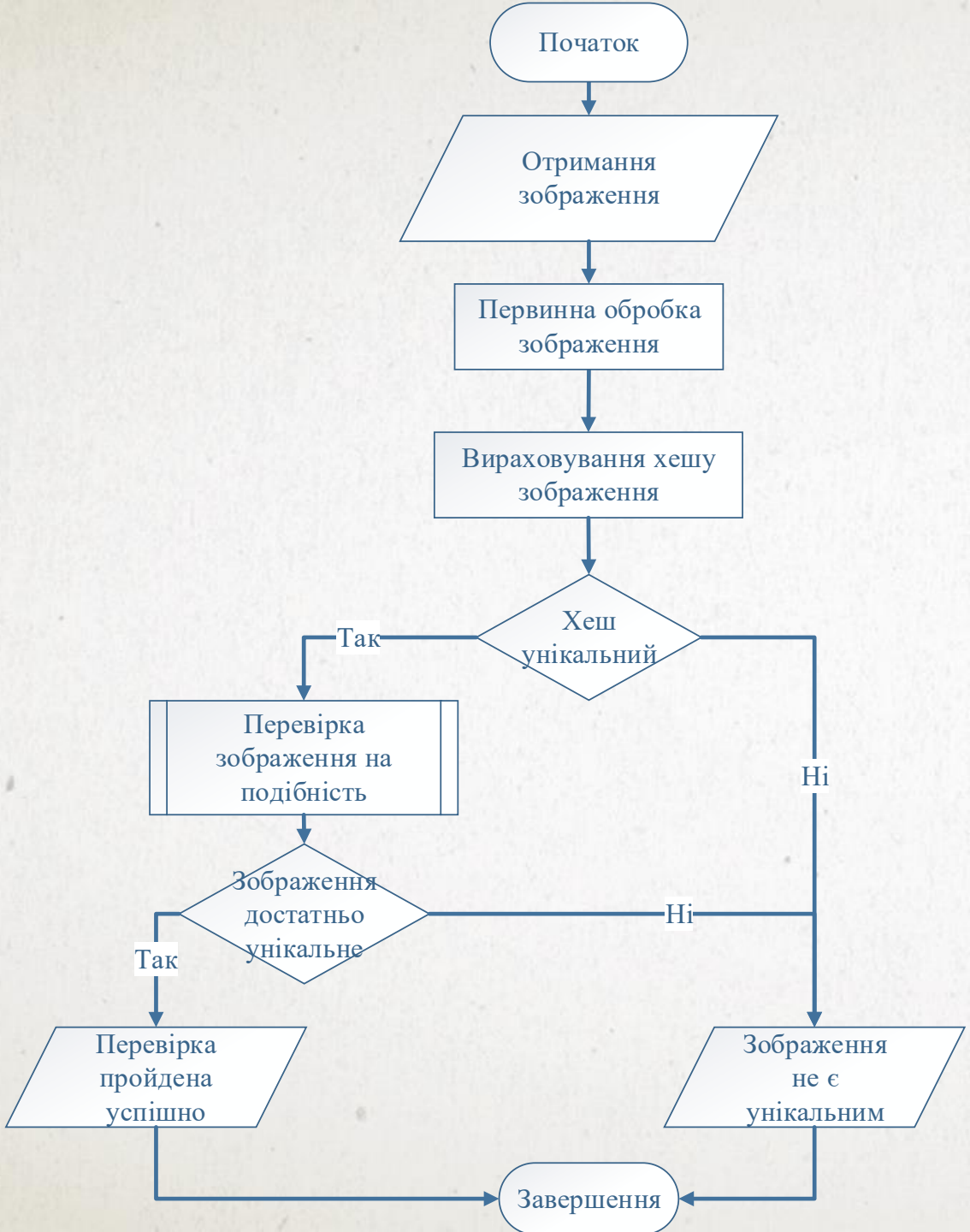
- Перевірка зображення на унікальність
- Підтвердження на автентичність
- Порівняння хеш-сум (MD5 алгоритм) в якості оптимізації порівняння



ЕТАПИ ЗАХИСТУ ЗОБРАЖЕНЬ: НАНЕСЕННЯ ЦВЗ ТА ВПРОВАДЖЕННЯ ДОДАТКОВОЇ ІДЕНТИФІКАЦІЇ

ЕТАПИ ЗАХИСТУ ЗОБРАЖЕНЬ:

ПІДПРОЦЕС ВПРОВАДЖЕННЯ ДОДАТКОВОЇ ІДЕНТИФІКАЦІЇ



ЕТАПИ ПЕРЕВІРКИ ВІДДАЛЕНИМ СЕРВЕРОМ

ПРОЦЕС ПОРІВНЯННЯ ЗОБРАЖЕННЯ

ГРАФІК ЗАЛЕЖНОСТІ ЧАСУ ВИКОНАННЯ ВІД КІЛЬКОСТІ СИМВОЛІВ

Кількість символів, які можна сховати в зображення, обчислюються за формулою: $I = \frac{x*y*l*3}{8}$

РЕЗУЛЬТАТИ РОБОТИ

- Завдяки методу вбудовування інформації LSB візуально неможливо виявити факт наявності прихованого повідомлення:

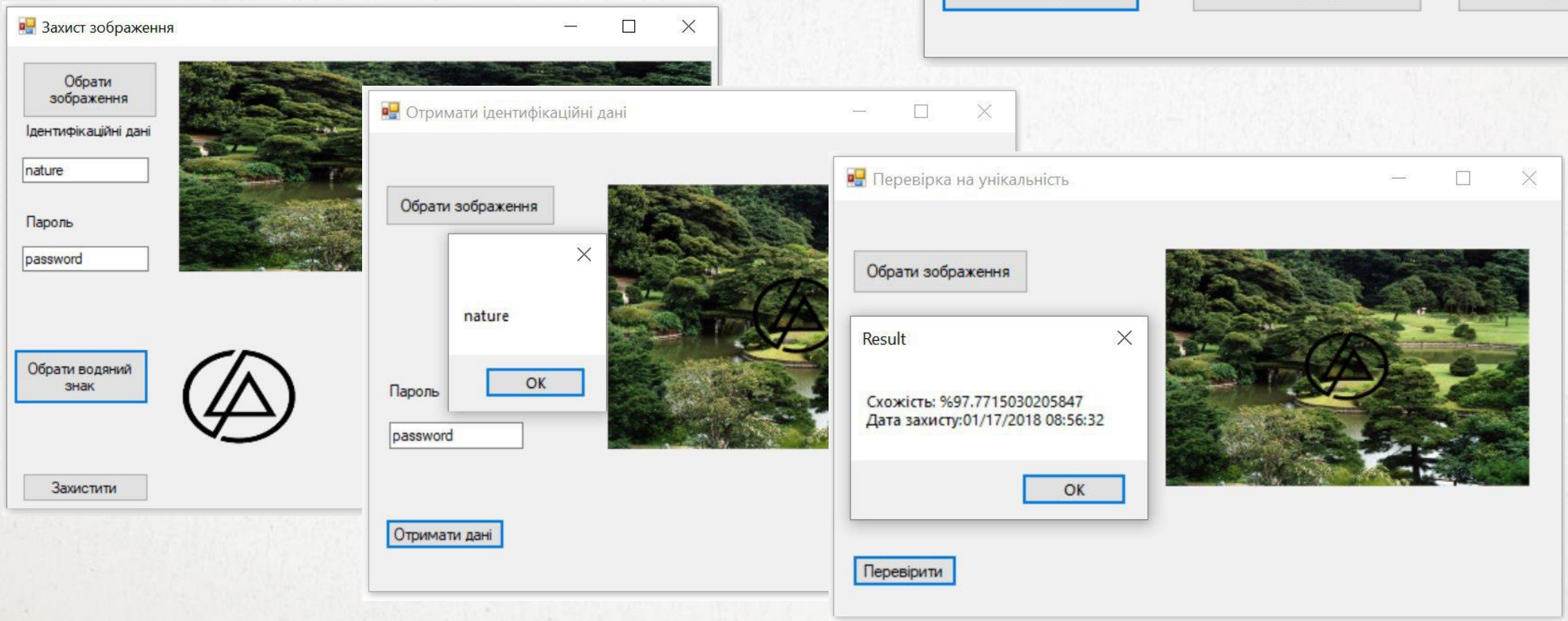
ПЕРЕВАГИ ЗАПРОПОНОВАНОГО КОМПЛЕКСНОГО ЗАХИСТУ

- Запропоновано ускладнення методу LSB шляхом перестановки параметрів кольору RGB у випадковому порядку і зберігається цей порядок у базі даних.
- При вилученні даних обчислюється хеш зображення та співставлений відносно нього необхідний порядок для бітів, таким чином отримуємо підвищену надійність, як і у випадку матриці сплутування, але при оригінальному розмірі зображення, що є важливим параметром для серверу.

ПЕРЕВАГИ ПРОГРАМИ

- Для підвищення надійності від зламу користувач не тільки власноруч вводить текст, який буде вбудовано в зображення, але й придумує пароль.
- Можливість користування як у вигляді клієнт-серверного додатку з локальною базою, так і у вигляді мобільного додатку. Можна розгорнути додаток в мережі Інтернет.
- Невелика кількість кроків для вбудовування/вилучення інформації; інтуїтивно зрозумілий інтерфейс.
- Прийнятна обчислювальна складність реалізації стеганосистеми. При тому, можна додавати інші алгоритми вбудовування інформації, шифрування та хешування.

СКРІНШОТИ ПРОГРАМИ



ОБЛАСТІ ЗАСТОСУВАННЯ

- Функція нанесення ЦВЗ може бути використана в особистих цілях фотографами, власниками інтернет-галерей.
- На підприємствах як спосіб захисту зображень та впровадження даних для відновлення.
- Програма може виступати додатком для підтвердження авторських прав (на підставі перевірки серверу, можна стверджувати що зображення вже було захищене), і завдяки цифровим міткам і єдиній базі, бути впевненим хто є автором. Додатковою підставою будуть слугувати ідентифікаційні дані та ЦВЗ.

ДЯКУЮ ЗА УВАГУ!