Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Кафедра МБІС

Магістерська кваліфікаційна робота

на тему:

“Підвищення стійкості цифрових водяних знаків до геометричних перетворень у системах безпеки на основі визначення особливих точок зображення ”

Керівник : к.т.н., доцент кафедри МБІС **Карпінець В.В.**
Виконала: ст. гр., УБ -17м, **Юдіна Г.М**.

Вінниця 2019

Актуальність теми дослідження

На сьогоднішній день існує багато методів вбудовування ЦВЗ в зображення, проте переважна більшість з них є нестійкими до певних видів атак. Як результат – можливість спотворення зображення-контейнера чи самого цифрового водяного знаку, а також до геометричних атак, зокрема повороту та масштабування. Цей вид атак може призвести до спотворення зображення, втрати чи зміни положення цифрового водяного знаку. Більшість методів вбудовування ЦВЗ є нестійкими до таких атак, тому досить актуальним є розроблення методу вбудовування ЦВЗ, що буде стійким до геометричних атак (поворот зображення та масштабування).

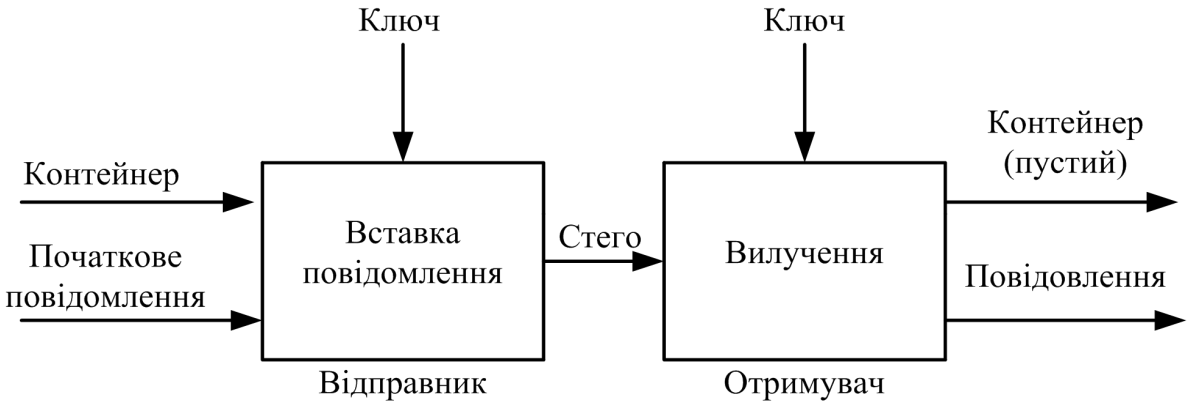


Рисунок 1 – Узагальнена модель стегосистеми

Мета і задачі дослідження

Метою роботи є розроблення стеганографічного методу підвищення стійкості ЦВЗ зображення-контейнера до геометричних перетворень у системах безпеки.

Для досягнення заданої мети в роботі **пропонується розв'язати такі задачі**:
- проаналізувати існуючі стеганографічні методи захисту зображень;
- проаналізувати види атак зловмисників на зображення;
- розробити алгоритм вбудовування ЦВЗ в зображення-контейнер, що буде стійким до геометричних атак.
- алгоритм видобування прихованого ЦВЗ з зображення контейнера.
- розробити метод підвищення стійкості ЦВЗ до геометричних перетворень зображення-контейнера;
- провести оцінювання запропонованого методу, з точки зору успішного відновлення прихованого повідомлення після атак на контейнер;
- виконати програмну реалізацію розробленого методу.

Об'єктом дослідження є процес підвищення стійкості ЦВЗ до геометричних перетворень зображень контейнера.

Предмет дослідження є методи і засоби вбудовування цифрових водяних знаків у зображення для захисту інформації в системах безпеки.

Наукова новизна отриманих результатів полягає в тому, що:
- розроблено стеганографічний метод підвищення стійкості ЦВЗ до геометричних перетворень зображення-контейнера у системах безпеки;
- вдосконалено метод визначення особливих точок зображення-контейнера шляхом встановлення оптимального значення коефіцієнтів функції відгуку зображення.

Аналіз можливості розробки методу вбудовування ЦВЗ стійких до геометричних перетворень

Розглянемо проблему десинхронізації на прикладі графічних контейнерів. Позначимо через *f(x,y)* цифрове зображення розміром N×M пікселів.

Розглянемо поворот зображення $x_k^{'} = x_k \cos\varphi + y_k \sin\varphi, y_k^{'} = -x_k \sin\varphi + y_k \cos\varphi,$

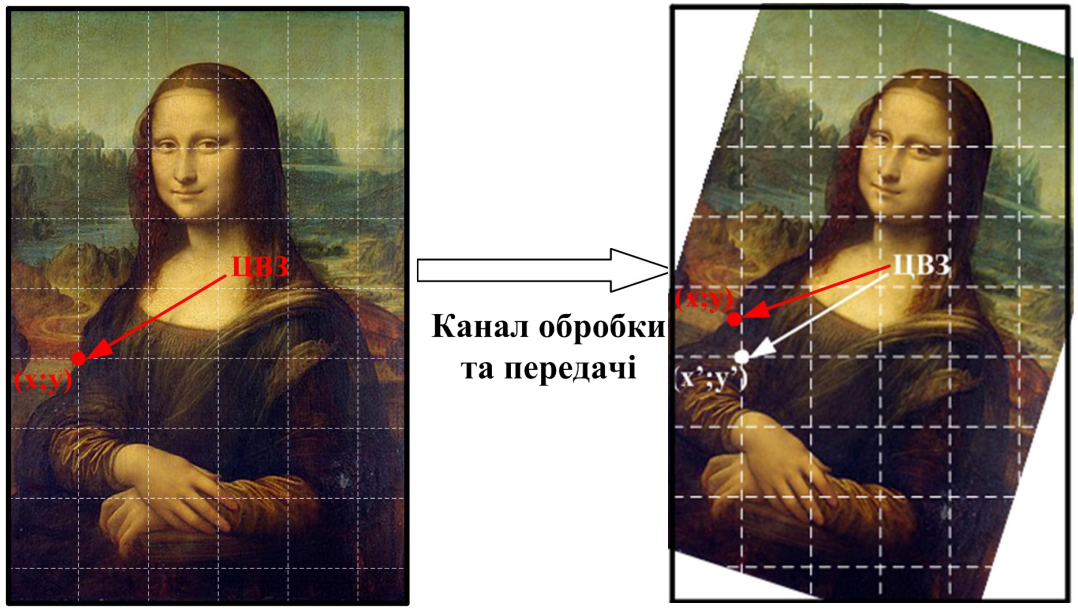


Рисунок 5.1 – Приклад геометричного спотворення (повороті) зображення при його передачі

Після дослідження та порівняльного аналізу вище перелічених методів для подальшого використання було обрано метод за особливими точками, оскільки використовують оригінальні дані контейнера і не вносять в нього додаткових даних для синхронізації.

Метод детектування особливих точок зображення

Особлива точка (характерна) - точка зображення, що володіє високою локальною інформативністю.

Розглянемо фрагмент зображення *U* зображення *I(x,y)* з центром в точці *(u,v),* і його копії, зміщенні на величину *(x,y).* Для кожної точки фрагменту можна порахувати зважений квадрат різниці між зміщеним і вихідним фрагментом зображення, та розглянути функцію:

$$S(x,y)=\sum_{(u,v)\in U} w(u,v)\left(I(u+x,v+y)-I(u,v)\right)^2. \qquad (1)$$

Функцію, I(u+x,v+y) можна розкласти в ряд Тейлора в межах центру (u,v), що дозволить перейти від (1) до наступного виразу:

$$S(x,y)\approx\sum_{(u,v)\in U} w(u,v)\left(I_x(u,v)x+I_y(u,v)y\right)^2. \qquad (2)$$

де I_x та I_y – частинні похідні яскравості в горизонтальному і вертикальному напрямках

Вираз (2) можна записати в матричні формі:

$$S(x,y)\approx(xy)\sum_{(u,v)\in U} w(u,v)\begin{bmatrix} I_x^2 & I_xI_y \\ I_xI_y & I_y^2 \end{bmatrix}$$

де $M=\sum_{(u,v)\in U} w(u,v)\begin{bmatrix} I_x^2 & I_xI_y \\ I_xI_y & I_y^2 \end{bmatrix}$ – матриця локальної структури.

Вдосконалення методу детектування особливих точок зображень

Виходячи з цього можна зробити ряд висновків:
– Якщо власні числа матриці λ_1 та λ_2 прямують до нуля, то піксель *(x,y)*, не є особливою точкою.
– Якщо $\lambda_1 \approx 0$ та λ_2 приймає більше по модулю значення, то піксель *(x,y)*, належить до краю області придатності точки до особливої.
– Якщо (λ_1 та λ_2) >> 0, тоді піксель можна вважати особливою точкою.

Харрсіом запропоновано використовувати міру відгуку кута (точки) – порогове значення.

$$z(x,y) = \det(M) - k \cdot tr(M)^2,$$

де k – встановлений емпіричним чином параметр, змінюється від 0.04 до 0.6. det(M) та tr(M)– визначник і слід матриці, що залежить від кількості особливих точок в зображенні і визначається для кожного зображення окремо (рис.7.1).

Апроксимувавши дану залежність і взявши по ній першу похідну можна відносно просто визначити чутливість зміни кількості особливих точок від зміни параметра k.

При негативному відгуку точка класифікується як потрапила на край;
при відгуку, близькому до нуля, точка вважається потрапила в «плоску» область;
при великих позитивних значеннях z(x,y) вважається, що точка є кутом, так як в ній яскравість сильно змінюється в усіх напрямках. Описаний детектор знаходять будь-які ділянки зображення, в яких є велика зміна градієнта в усіх напрямках при заданому масштабі.

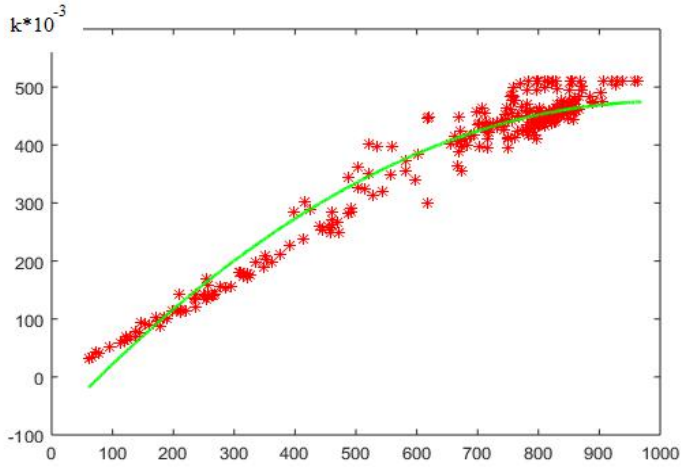
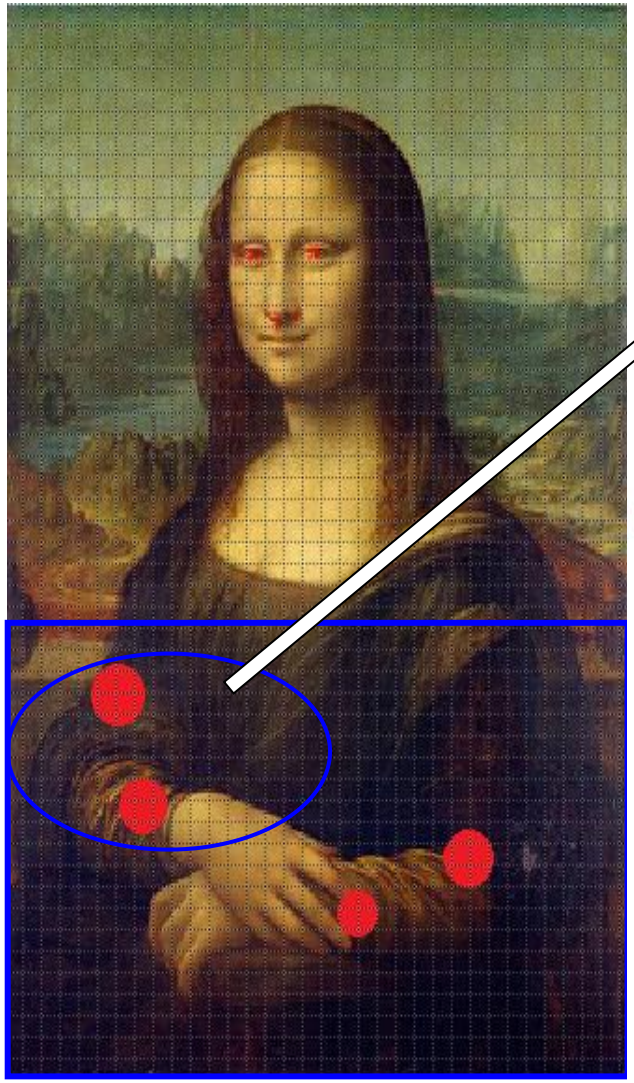


Рисунок 7.1 – Залежність k-від кількості особливих точок в зображенні

Розробка методу вбудовування ЦВЗ стійкого до геометричних спотворень зображення–контейнера

Існуючі методи синхронізації ЦВЗ в контейнері-зображенні мають один суттєвий недолік, а саме невисоку стійкість до геометричних перетворень. Найбільше переваг мають методи синхронізації на базі особливих точок. Ці методи принципово відрізняються від інших тим, що вони використовують оригінальні дані зображення і, як наслідок, створюють для кожного зображення свій унікальний набір точок.



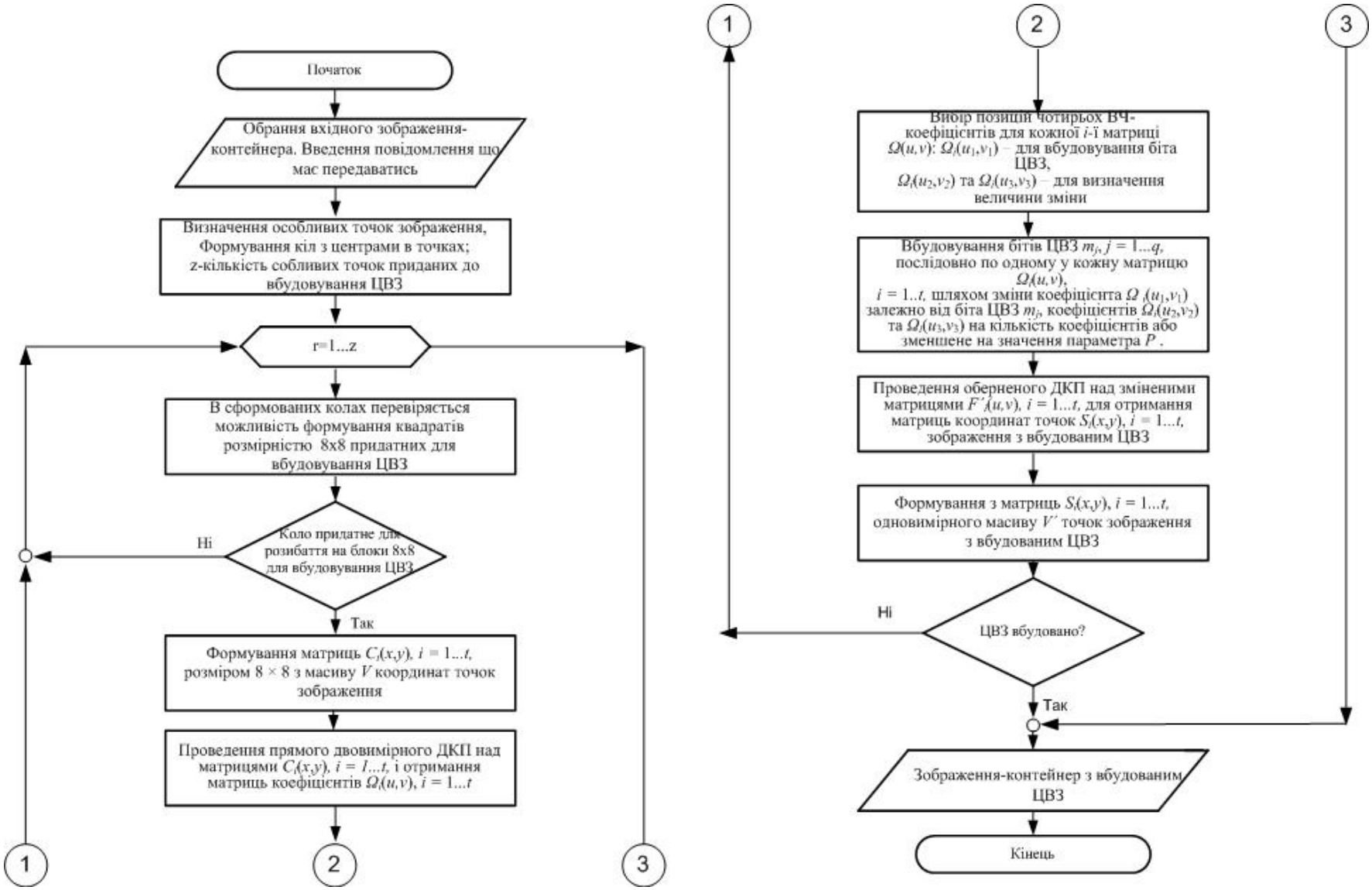
	0	1	2	3	4	5	6	7
0	630	-67	-1	15	5	0	0	1
1	153	-27	-38	24	-5	1	2	-7
2	63	-18	-3	9	0	-1	-1	-1
3	27	-8	-11	11	-6	1	-1	6
4	13	-9	0	6	0	1	-1	0
5	14	-5	-1	7	0	1	-1	0
6	6	-7	-1	1	-1	1	0	0
7	0	0	1	1	1	0	0	-1

низькочастотні коефіцієнти

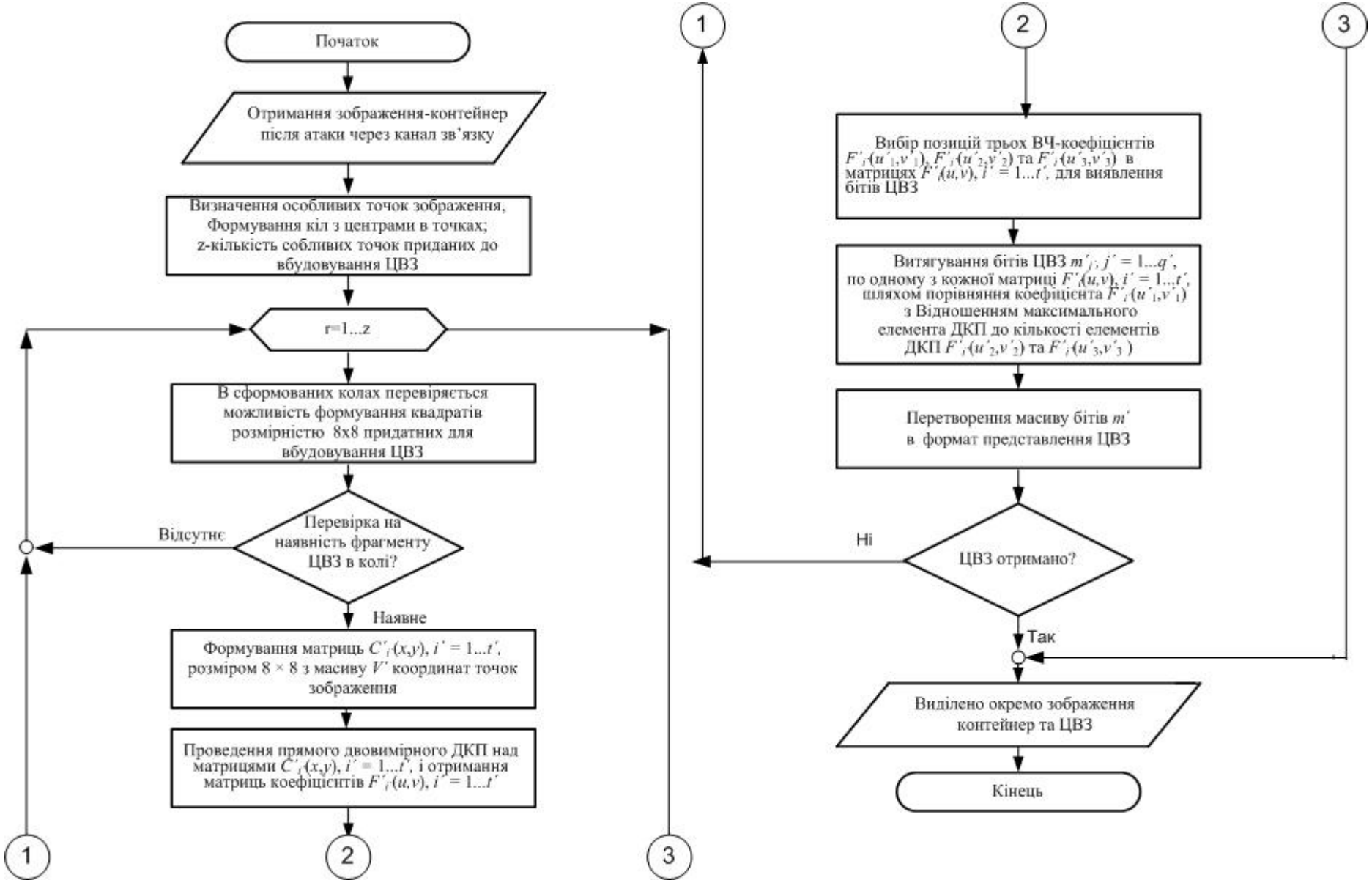
середньочастотні коефіцієнти

високочастотні коефіцієнти

Структурна схема алгоритму вбудовування ЦВЗ в зображення



Структурна схема алгоритму вилучення ЦВЗ з зображення



Оцінювання якості розробленого методу вбудовування ЦВЗ в зображення

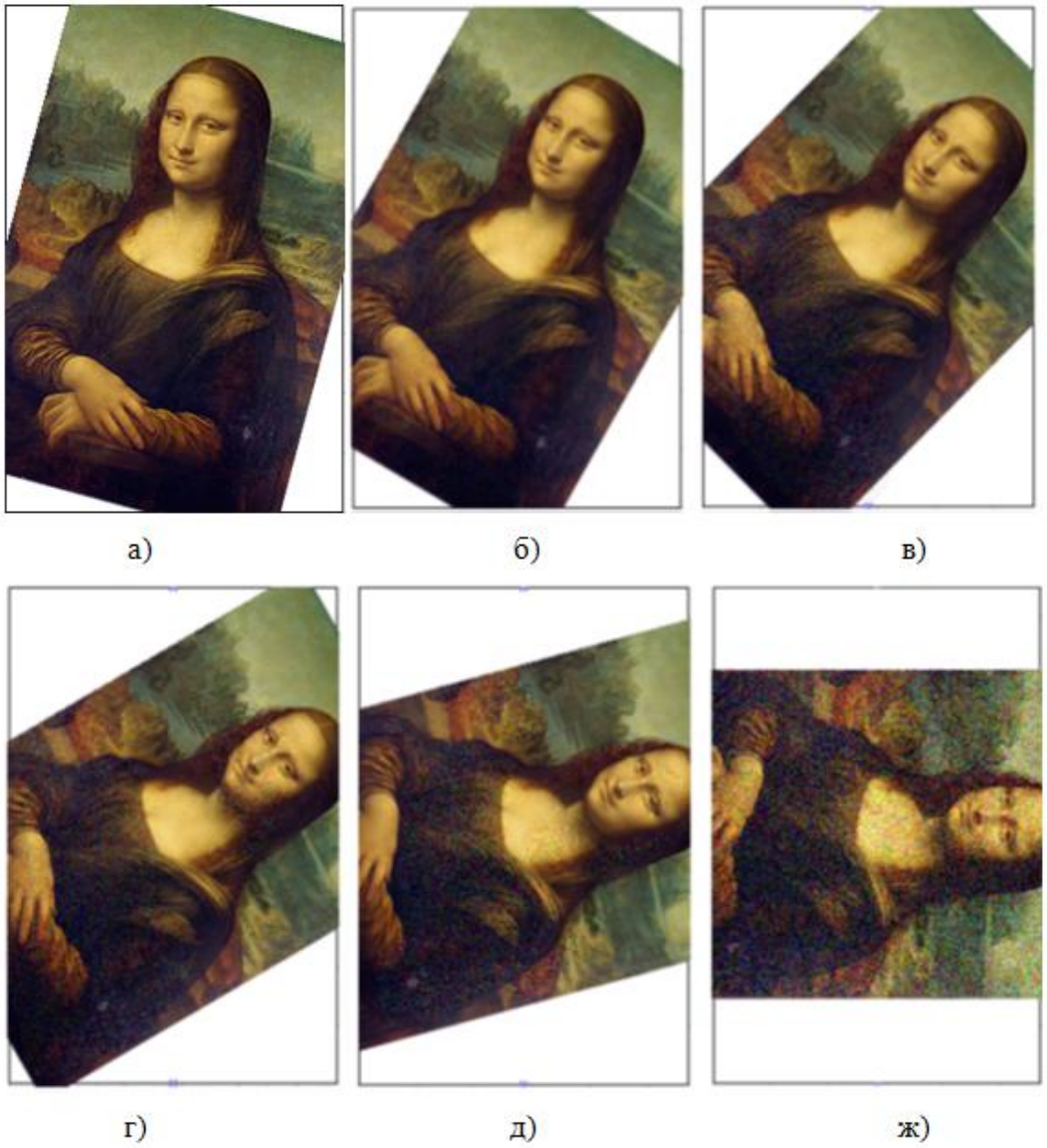


Рисунок 1 – Зміна якості зображення під час геометричної атаки на нього: а)15˚, б)30˚, в)45˚, г)60˚, д)75˚, ж)90˚

Параметри оцін-я	а)	б)	в)	г)	д)	ж)
Максимальна відмінність	17,5	33,4	54,5	68,4	84,5	101
Середня абсолютна відмінність	7,15	25,4	38,5	54,4	60,04	71,1
Нормована середня абсолютна відмінність	0,12	0,81	5,75	11,2	14,3	17,5
Відношення «сигнал-шум»	$8,7 \cdot 10^{11}$	$11,3 \cdot 10^{4}$	$3,3 \cdot 10^{2}$	810	$110 \cdot 10^{-2}$	$4,7 \cdot 10^{-5}$
Якість зображення	0,99	0,87	0,73	0,45	0,38	0,18
Нормована взаємна кореляція	0,98	0,90	0,84	0,54	0,48	0,34
Якість кореляції	0,87	0,71	0,65	0,41	0,33	0,1

Програмна реалізація методу вбудовування ЦВЗ стійкого до геометричних перетворень зображення

Оскільки розроблений метод вбудовування ЦВЗ досить добре зарекомендував себе з точки зору стійкості до геометричних перетворень та кількісних та якісних показників оцінювання методів, було вирішено виконати його програмну реалізацію. Для її здійснення обрано об'єктно-орієнтовну мову програмування C# та Microsoft .NET Framework 4.6.1.

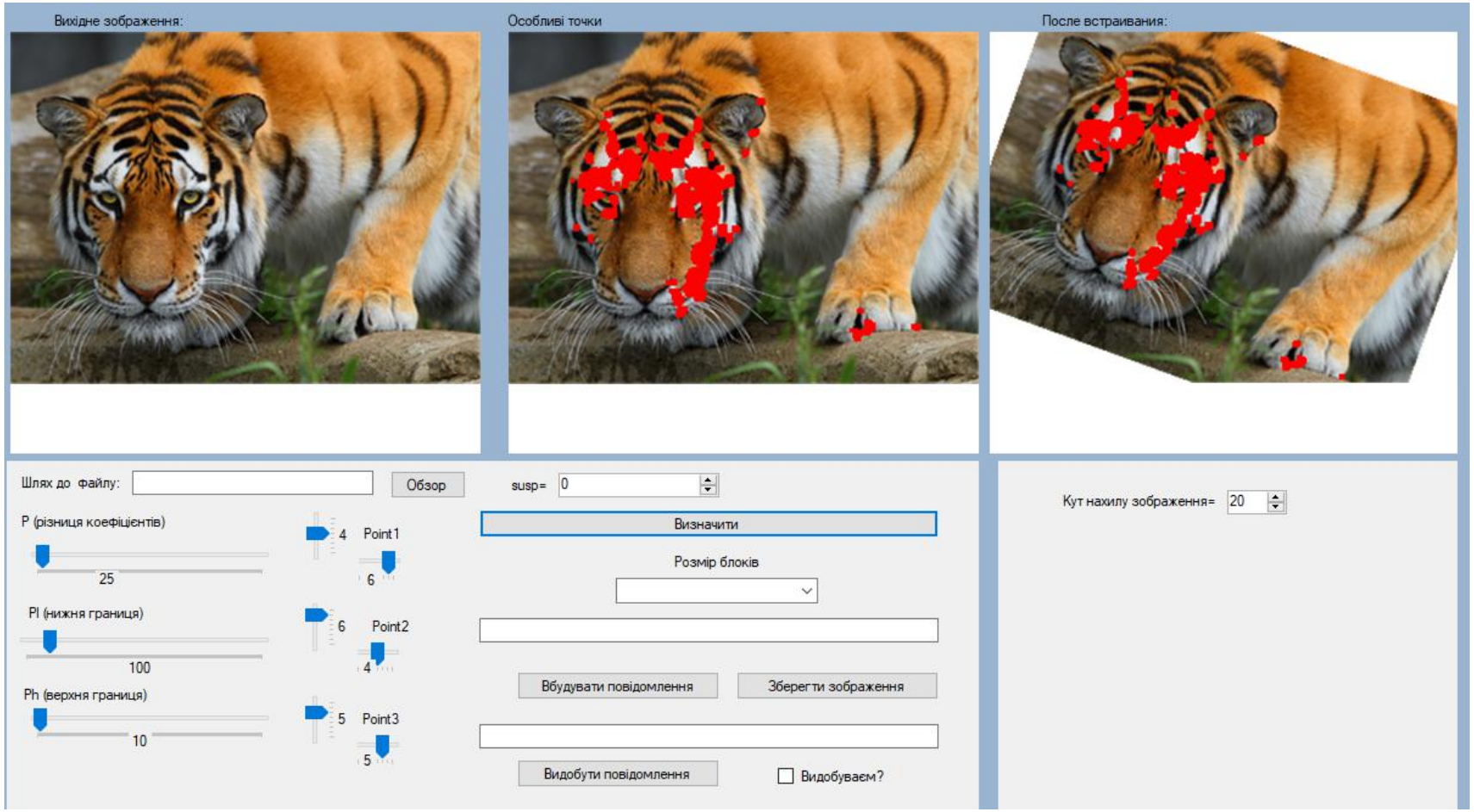


Рисунок1 – Загальний вигляд інтерфейсу програмного засобу

Програмна реалізація методу вбудовування ЦВЗ стійкого до геометричних перетворень зображення

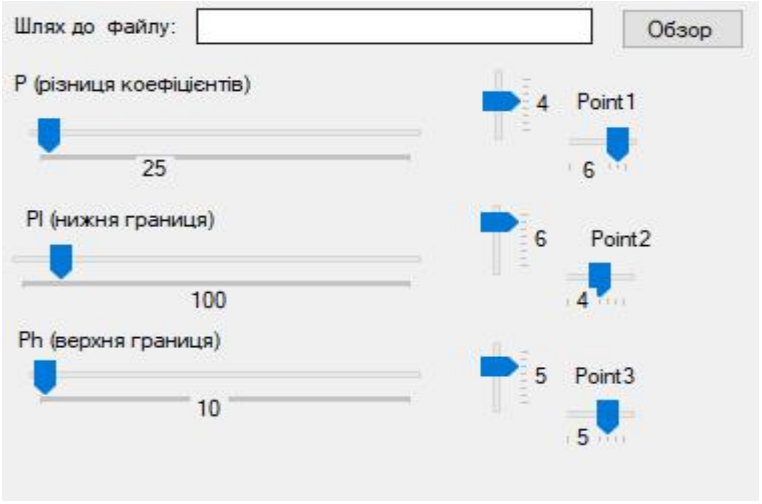


Рисунок 1 – Інтерфейс налаштування параметрів методу вбудовування ЦВЗ.

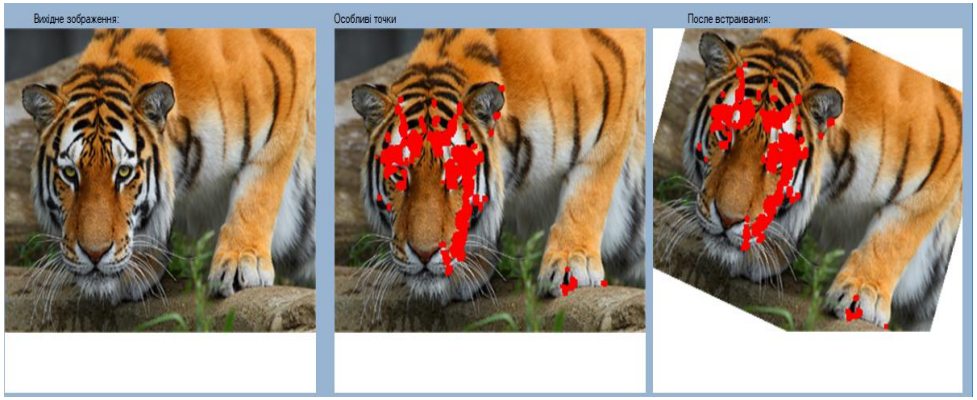


Рисунок 2 - Вхідне зображення з вбудованим прихованим повідомленням.

Маючи завантажене вхідне зображення, проводимо визначення особливих точок, після визначення особливих точок, отримуємо їх координати і формуємо окружності з центром в шуканих точках. Відбудувавши квадратичні блоки заданої розмірності, в даному випадку мова йде про розмір 8x8, починає роботу алгоритм вбудовування ЦВЗ Бенгама-Мемона-Ео-Юнга з подальшою перевіркою блоків на придатність.

Перед початком роботи методу вбудовування формується файл розширенням *.txt, в якому зберігається повідомлення, що планується вбудувати. Слід зауважити, що запропонований метод обмежений розміром зображення контейнера та для підтримання відповідної якості зображення, встановлюємо обмеження на величину повідомлення, що шифрується. Воно повинно бути не більше 15% від величини контейнера.

Економічна частина. Розрахунок ефективності вкладених інвестиції та періоду їх окупності

Абсолютна ефективність $E_{абс}$ вкладених інвестицій розраховується за формулою:

$$E_{абс} = (ПП - PV),$$

де *ПП* – приведена вартість всіх чистих прибутків, що їх отримає підприємство від реалізації результатів наукової розробки, грн; *PV* – теперішня вартість інвестицій *PV=ЗВ*, грн.

У свою чергу, приведена вартість всіх чистих прибутків ПП розраховується за формулою:

$$ПП = \sum_{t=1}^{m} \frac{\Delta П_i}{(1+\tau)^t},$$

де П – збільшення чистого прибутку у кожен із років, протягом яких виявляються результати НДР, грн.;

τ– ставка дисконтування (0,1);

t – період часу в роках, від моменту отримання прибутку до точки «0».

т – період часу, протягом якого виявляються результати впровадження.

$$ПП = \frac{32880}{(1+0,1)^1} + \frac{210750}{(1+0,1)^4} + \frac{297000}{(1+0,1)^5} + \frac{386250}{(1+0,1)^6} = 576276(грн)$$

Тоді абсолютна ефективність становить:

$$576276 - 32880 = 543396(грн)$$

Оскільки $E_{абс}>0$, то вкладання коштів на виконання та впровадження результатів НДДКРП буде доцільним.

Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $E_в$ за формулою:

$$E_в = \sqrt[T_ж]{1+\frac{E_{абс}}{PV}} - 1 \qquad E_в = \sqrt[6]{1+\frac{576276}{32880}} - 1 = 0,62$$

Виходячи з отриманих вище показників, розрахуємо термін окупності проекту

$$T_{ок} = \frac{1}{E_в}, \qquad T_{ок} = \frac{1}{0,62} = 1,61 роки$$

Очікуваний термін окупності інвестицій – 1,61 роки.

Висновки

В роботі досліджується актуальне питання розробки методу вбудовування ЦВЗ, що буде стійким до геометричних перетворень зображення-контейнера. Запропонований метод вбудовування ЦВЗ на базі особливих точок зображення, виділених за допомогою детектора кутів Харріса. Метод потребує однорідного розподілу виділених точок. Для його одержання необхідно розбивати зображення на блоки в центрі окружності яких знаходяться особливі точки.

Оскільки запропонований метод є стійким до геометричних перетворень, а саме повороту зображення, було виконано його програмну реалізацію. У третьому розділі дипломної роботи було здійснено розробку програмного засобу, що грунтується на визначенні особливих точок зображення контейнера. Відбудувавши квадратичні блоки заданої розмірності, в центах особливих точок починає роботу алгоритм вбудовування ЦВЗ з подальшою перевіркою блоків на придатність.

Визначені, класифіковані та досліджені атаки на стеганографічні системи. Отримані кількісні оцінки стійкості до атак проти вбудованого повідомлення та стеганогдетектора, реалізовані на основі афінних перетворень, повороту зображення-контейнера з ЦВЗ.

За результатами визначено, що при наявності активного порушника, найефективнішим способом приховування даних є методи на побудовані на основі особливих точок.

Виходячи з результатів проведеного маркетингового дослідження на розрахунок показників економічної ефективності, можна зробити висновок, що дана робота має високу інвестиційну привабливість. Очікуваний термін окупності інвестицій – 1,61 роки.

Дякую за увагу!!!