Додаток А.

Комплект графічних матеріалів

Порівняльний аналіз алгоритмів генерування та вбудовування цифрових водяних знаків у 2D зображення

Актуальність роботи. Задача надійного захисту конфіденційних даних, які мають цифровий формат, від несанкціонованого доступу є однією з найстаріших і майже не вирішених досі проблем.

У зв'язку з інтенсивним розвитком та поширенням технологій, які дозволяють за допомогою комп'ютера інтегрувати, обробляти та синхронно відтворювати різні типи сигналів (так звані мультимедійні технології), питання захисту інформації, представленої у цифровому вигляді, є надзвичайно актуальним. Тому в усьому світі активно розробляються методи захисту інформації організаційного, методологічного та технічного характеру, серед них - і методи стеганографії.

Метою роботи є підвищення інформаційної безпеки систем електронного документообігу.

Для досягнення поставленої мети необхідно розв'язати наступні **задачі**:

1) провести аналітичний огляд сучасних рішень і технік застосування комп'ютерної стеганографії до створення ЦВЗ;

2) провести аналітичний огляд основних алгоритмів вбудовування ЦВЗ в файли-зображення;

3) провести експериментальні дослідження алгоритмів вбудовування ЦВЗ, що базуються на дискретних перетвореннях за критеріями візуальної непомітності вбудовування, прихованої пропускної здатності, стійкості до спотворень.

Сучасні алгоритми створення ЦВЗ для файлів-зображень

Характеристика ЦВЗ	Принцип роботи	Переваги	Недоліки
1 Адитивні алгоритми створення ЦВЗ			
1.1 Алгоритми на основі лінійного вбудовування ЦВЗ			
Послідовність псевдовипадкових чисел, розподілених за законом Гауса, довжиною 1000 чисел	Модифікація 1000 найбільших коефіцієнтів дискретного косинусного перетворення (ДКП)	Нечутливість ЦВЗ до стискання та інших видів обробки сигналу	Трудомісткість обчислення двовимірного ДКП
Послідовність бінарних псевдовипадкових чисел {-1,1}, довжина якої визначається розмірами первинного зображення	Модифікація всіх коефіцієнтів детальних піддіапазонів першого підрівня розкладання при виконанні чотирирівневого вейвлет-перетворення	Можливість виявлення ЦВЗ без первинного зображення. Візуальна непомітність ЦВЗ	Для відновлення ЦВЗ необхідно мати первинне зображення
Масив псевдовипадкових чисел, розподілених згідно із законом Гауса, розміром 1024 числа	Модифікація всіх коефіцієнтів LL піддіапазону вейвлет-перетворення зображення	Можливість модифікації алгоритму для використання секретного ключа	Для відновлення ЦВЗ необхідно мати первинне зображення
Послідовність псевдовипадкових дійсних чисел, розподілених за законом Гауса	Модифікація найбільших коефіцієнтів детальних піддіапазонів тривневої декомпозиції зображення	Добре візуальне маскування вбудованих даних. Для виявлення ЦВЗ не потрібна наявність первинного зображення	
Послідовність псевдовипадкових дійсних чисел, розподілених за законом Гауса, довжиною 1000 чисел	Модифікація перцептуально значущих коефіцієнтів тривневої декомпозиції зображення з використанням біортогональних вейвлет-фільтрів	Стійкість ЦВЗ до багатьох видів атак. Для виявлення ЦВЗ не потрібна наявність первинного зображення	
Послідовність псевдовипадкових дійсних чисел, розподілених за гауссівським законом	Модифікація найбільших коефіцієнтів кожного піддіапазону тривневої декомпозиції зображення	Для виявлення ЦВЗ не потрібна наявність первинного зображення	

Сучасні алгоритми створення ЦВЗ для файлів-зображень

Характеристика ЦВЗ	Принцип роботи	Переваги	Недоліки
Масив біполярних псевдовипадкових чисел	Модифікація1000 найбільших коефіцієнтів комплексного вейвлет-перетворення (ЦВЗ також піддається перетворенню)	Для виявлення ЦВЗ не потрібна наявність первинного зображення	
Послідовність псевдовипадкових дійсних чисел, розподілених за гауссівським законом	Модифікація найбільших коефіцієнтів тривівневого вейвлет-перетворення (коефіцієнти відбираються відповідно до заданого порогу)	Робастність ЦВЗ до деяких видів атак	Для відновлення ЦВЗ необхідно мати первинне зображення
Послідовність псевдовипадкових дійсних чисел, довжина якої залежить від пропускної здатності зображення, що обчислюється на основі моделі людського зору	Модифікація коефіцієнтів чотирирівневого вейвлет-перетворення, відібраних з урахуванням заданого порога	Висока робастність вбудованого ЦВЗ	Для відновлення ЦВЗ необхідно мати первинне зображення
Послідовність псевдовипадкових дійсних чисел, розподілених за гауссівським законом	Модифікація найбільших коефіцієнтів з високочастотного та середньо частотного діапазонів перетворення Хаара	Висока робастність до атак із зміною масштабу.	Для відновлення ЦВЗ необхідно мати первинне зображення
Послідовність псевдовипадкових дійсних чисел, розподілених за гауссівським аконом (довжина відповідає кількості модифікованих коефіцієнтів)	Модифікація значимих коефіцієнтів всіх піддіапазонів п'ятирівневого вейвлет-перетворення	Можливість модифікації алгоритму для використання стегоключа	Для відновлення ЦВЗ необхідно мати первинне зображення
Послідовність псевдовипадкових дійсних чисел, розподілених за гауссівським законом (довжина відповідає кількості модифікованих коефіцієнтів)	Алгоритм є модифікованим варіантом попереднього алгоритму, зі сліпим відновленням ЦВЗ	Для виявлення ЦВЗ не потрібна наявність первинного зображення	Сильно знижена завадостійкість в порівнянні з попереднім алгоритмом

Сучасні алгоритми створення ЦВЗ для файлів-зображень

Характеристика ЦВЗ	Принцип роботи	Переваги	Недоліки
1.2 Алгоритми на основі злиття ЦВЗ та контейнера			
Чорно-білий логотип розміром до 25% від первинного зображення	Модифікація всіх коефіцієнтів однорівневої декомпозиції первинного зображення	Великий розмір ЦВЗ, що приховується (до чверті розміру первинного зображення)	Для відновлення ЦВЗ необхідно мати первинне зображення
Чорно-білий логотип	Модифікація всіх коефіцієнтів детальних піддіапазонів вейвлет перетворення первинного зображення	Для виявлення ЦВЗ не потрібна наявність первинного зображення	
2 Алгоритми створення ЦВЗ на основі квантування			
2.1 Алгоритми з використанням скалярного квантування			
Послідовність ±1	Модифікація високочастотних коефіцієнтів зображення після цілого вейвлет-перетворення	Для виявлення ЦВЗ не потрібна наявність первинного зображення	
Бінарне зображення розміром 1/2 від первинного зображення	Модифікація ВЧ-НЧ та НЧ-ВЧ областей дворівневого вейвлет-перетворення первинного зображення	Великий розмір ЦВЗ, що приховується	Для вилучення ЦВЗ необхідно мати первинне зображення; низька стійкість алгоритму по відношенню до операцій обробки сигналу
2.2 Алгоритми з використанням векторного квантування			
Послідовність символів, отримана з логотипу розміром 25% від первинного зображення	Модифікація n мірного вектора коефіцієнтів дискретного вейвлет-перетворення первинного зображення	Великий розмір ЦВЗ, що приховується Можливо контролювати робастність, рівень спотворень і якість вбудованого зображення	Для відновлення ЦВЗ необхідно мати первинне зображення

Сучасні алгоритми створення ЦВЗ для файлів-зображень

Характеристика ЦВЗ	Принцип роботи	Переваги	Недоліки
3 Алгоритми створення ЦВЗ, що використовують фрактальне перетворення			
Формується з первинного зображення (до 15 різних ЦВЗ)	Модифікація декількох «особливих» точок з використанням методу фрактального кодування Харріса. Для кожної особливої точки виконують зміну доменного блоку тієї ж позиції так, щоб він був більш схожий на ранговий блок	Для виявлення ЦВЗ не потрібна наявність первинного зображення	
Рядок бітів	Модифікація обраного відповідно до ключа рангового блоку в доменному пулі. Якщо треба вбудувати «1», пошук виконується в одній частині пулу, якщо «0» в іншій частині	Наявність секретного ключа; стійкість до стиснення JPEG	
Рядок бітів	Модифікація вручну вибраних двох квадратних областей на зображенні, що не перекриваються (так звані рангова та доменна області)	Наявність секретного ключа	Можливе помітне погіршення якості зображення при вбудовуванні ЦВЗ

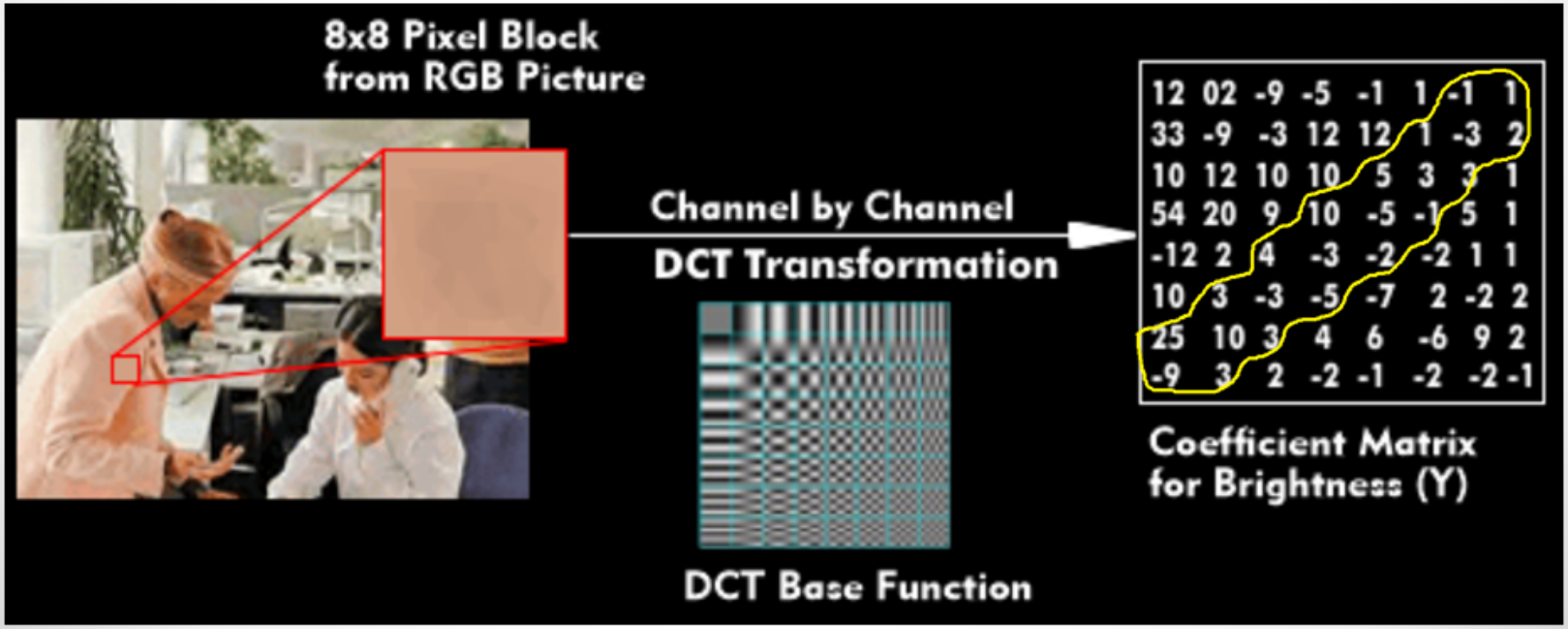
Дискретне косинусне перетворення зображення

В результаті двовимірного прямого дискретного косинусного перетворення блоку зображення з індексом b можна отримати матрицю розміром $N \times N$ коефіцієнтів ДКП, які позначаються $\Omega_b(v,\nu)$:

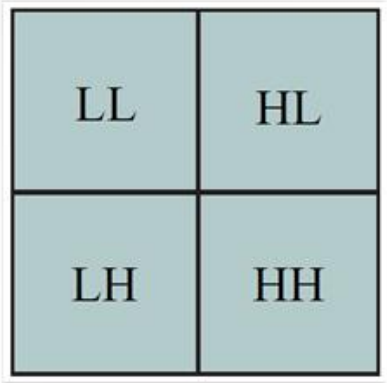
$$\Omega_b(v,\nu) = \frac{\zeta(v)\cdot\gamma(\nu)}{\sqrt{2N}} \times \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C_b(x,y)\cos\left[\frac{\pi\cdot v\cdot(2x+1)}{2N}\right]\cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right]$$

$$\zeta(v) = \begin{cases} 1/\sqrt{N}, v = 0, \\ \sqrt{2}/\sqrt{N}, 0 < v < N-1. \end{cases}, \quad \gamma(\nu) = \begin{cases} 1/\sqrt{N}, \nu = 0, \\ \sqrt{2}/\sqrt{N}, 0 < \nu < N-1. \end{cases}$$

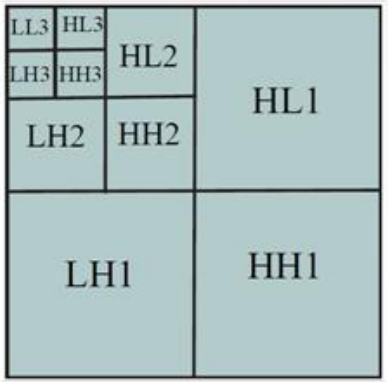
де $C_b(x,y)$ – значення пікселя блоку b в позиції (x,y); (v,ν) – позиція коефіцієнту ДКП в блоці b.



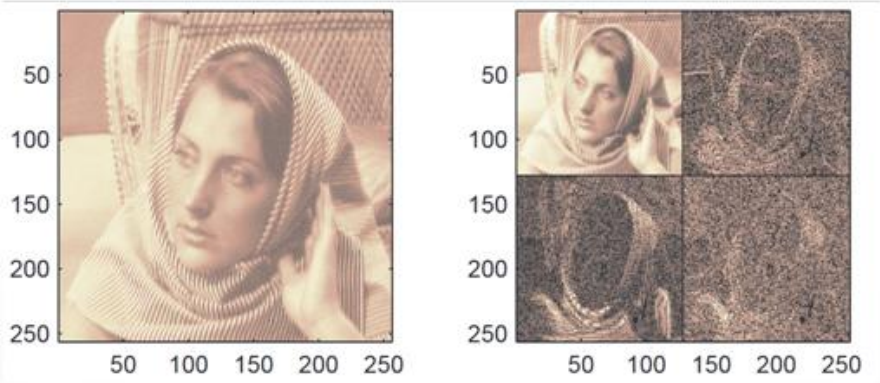
Дискретне вейвлет-перетворення зображення



Однорівневе двовимірне вейвлет-перетворення квадратного зображення



Трирівневе двовимірне вейвлет-перетворення квадратного зображення



Двовимірне вейвлет-перетворення зображення

Початкові умови експериментального дослідження

Castle.jpg

Universe.tiff

Snap.jpg

Tiffany.bmp

Lemur.jpg

Lego.png

ЦВЗ: Test Watermark Algorithm Message
ACSII binary format:

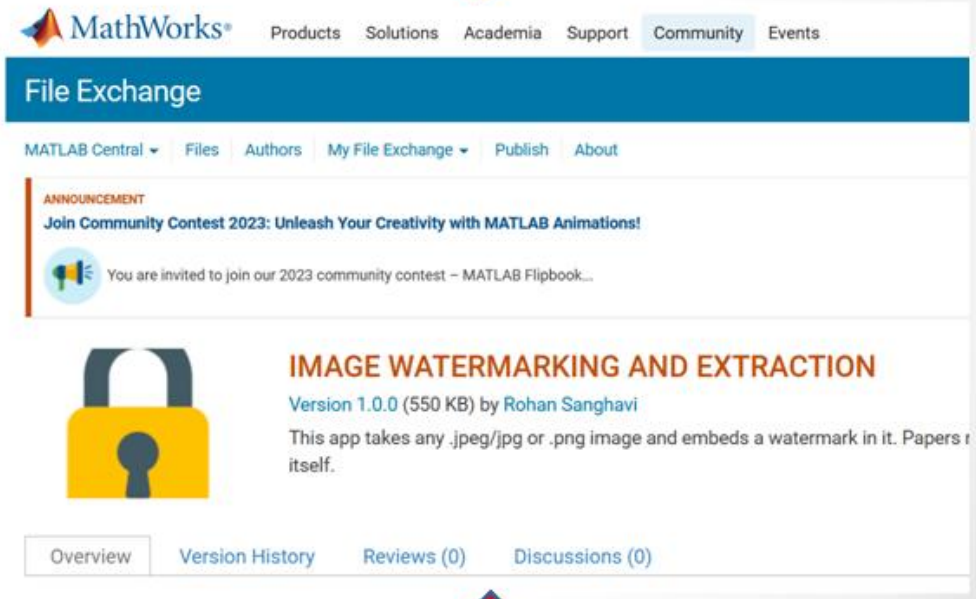
01010100 01100101 01110011 01110100 00100000 01010111 01100001 01110100
01100101 01110010 01101101 01100001 01110010 01101011 00100000 01000001
01101100 01100111 01101111 01110010 01101001 01110100 01101000 01101101
00100000 01001101 01100101 01110011 01110011 01100001 01100111 01100101

Початкові умови експериментального дослідження

Алгоритм Коха-Жао
Параметр вбудовування
P=16

Алгоритм Пунам-Арора
Параметр вбудовування
a=0.03

Алгоритм Патідара
Параметр вбудовування
γ=0.11



Алгоритм Сангхаві

Дослідження візуальних спотворень зображень, що виникають під час використання дослідних алгоритмів

Показник спотворення	Формула для розрахунку
Середня абсолютна різниця (Average Absolute Difference – AD)	$AD = \frac{1}{XY}\sum_{x,y}\lvert C_{x,y} - S_{x,y}\rvert$
Нормована середня абсолютна різниця (Normalized Average Absolute Difference – NAD)	$NAD = \frac{\sum_{x,y}\lvert C_{x,y} - S_{x,y}\rvert}{\sum_{x,y}\lvert C_{x,y}\rvert}$
Відношення сигнал/шум (Signal to Noise Ratio – SNR)	$SNR = \frac{\sum_{x,y}(C_{x,y})^2}{\sum_{x,y}(C_{x,y} - S_{x,y})^2}$
Максимальне значення відношення сигнал/шум (Peak Signal to Noise Ratio – PSNR)	$PSNR = XY\frac{\max_{x,y}(C_{x,y})^2}{\sum_{x,y}(C_{x,y} - S_{x,y})^2}$
Якість зображення (Image Fidelity – IF)	$IF = 1 - \frac{\sum_{x,y}(C_{x,y} - S_{x,y})^2}{\sum_{x,y}(C_{x,y})^2}$

Зображення/ Алгоритм	Коха-Жао	Сангхаві	Пунам-Арора	Патідара
Castle.jpeg	2	1	3	4
Lemur.jpeg	2	1	3	4
Snap.jpeg	1	2	3	4
Tiffany.bmp	1	2	4	3
Lego.png	1	2	3	4
Universe.tiff	0	0	3	4
Підсумок	7	8	22	27

Дослідження стійкості алгоритмів до різних видів атак

Атака / Алгоритм	Коха-Жао	Сангхаві	Пунам-Арора	Патідара
Масштабування	0	0	0	0
Поворот	5	0	0	0
Контрастність	5	1	3	5
Підвищення яскравості	5	0	4	5
Зниження яскравості	5	0	2	5
Видалення частини зображення	5	4	5	5
Стиснення JPEG з коефіцієнтом якості 0.7	5	0	0	5
Стиснення JPEG з коефіцієнтом якості 0.5	5	0	0	0

Дослідження пропускної здатності алгоритмів

До найважливіших якісних характеристик стеганографічних систем відносять пропускну здатність – кількість бітів прихованого повідомлення, що можуть бути передані за допомогою вказаного алгоритму в зображенні розміру M×N.

Під прихованою пропускною здатністю розуміють максимальну кількість інформації, яка може бути вбудована в контейнер, при цьому повідомлення, що приховуються, повинні бути безпомилково передані адресату і захищені від атак зловмисника.

Алгоритм	Контейнер Castle.jpg	Контейнер Tiffany.bmp	Контейнер Lego.png	Контейнер Universe.tiff
Коха-Жао	0.446	1	1	0.563
Сангхаві	0.203	0.212	0.323	0.117
Пунам-Арора	0.308	0.287	0.395	1
Патідара	1	1	1	0.401

Висновки

1. Розглянуто способи застосування комп'ютерної стеганографії до створення ЦВЗ. Зазначено, що використання ЦВЗ для підтвердження автентичності цифрових документів в наш час набувають все більшої популярності.

2. Докладно розглянуто основні алгоритми створення ЦВЗ для файлів-зображень. Зазначено, що основною проблемою при реалізації технологій створення ЦВЗ є збереження якості маркованих при вбудовуванні ЦВЗ файлів при їх використанні за основним призначенням у поєднанні з достовірністю подальшого відновлення ЦВЗ.

3. Проведено експериментальні дослідження чотирьох алгоритмів вбудовування ЦВЗ, що базуються на дискретних перетвореннях. В якості критерії при порівнянні було обрано: візуальну непомітність вбудовування, приховану пропускна здатність, стійкість до спотворень. Результати порівняльного аналізу представлені в таблицях та графіках.

Результати експериментів показали, що алгоритми, засновані на дискретному косинусному перетворенні (зокрема, найпопулярніший у цій групі алгоритм Коха-Жао), мають дуже високу стійкість до атак, але візуальна непомітність роботи алгоритму недостатня. Крім того, даний алгоритм показав низькі результати за обраними критеріями у випадку вбудовування в нестиснуті зображення.

Більш кращі показники мали алгоритми, побудовані на застосуванні дискретного вейвлет-перетворення. Загальним недоліком цієї групи методів є порівняно низька стійкість до атак (алгоритм Сангхаві). Головною ж перевагою є висока прихована пропускна здатність та непомітність вбудованого ЦВЗ.

Номер документу	Позначення	Найменування	Прим.
		Текстові документи	
1		Пояснювальна записка	104 с.
		Графічний матеріал	
2		Порівняльний аналіз алгоритмів	А4 ел.ф.
		генерування та вбудовування цифрових	
		водяних знаків у 2D зображення	
3-6		Сучасні алгоритми створення ЦВЗ	4хА4 ел.ф.
		для файлів-зображень	
7		Дискретне косинусне перетворення	А4 ел.ф.
		зображення	
8		Дискретне вейвлет-перетворення	А4 ел.ф.
		зображення	
9-10		Початкові умови експериментального	2хА4 ел.ф.
		дослідження	
11		Дослідження візуальних спотворень	А4 ел.ф.
		зображень, що виникають під	
		час використання дослідних алгоритмів	А4 ел.ф.
12		Дослідження стійкості алгоритмів	А4 ел.ф.
		до різних видів атак	
13		Дослідження пропускної здатності	А4 ел.ф.
		алгоритмів	
14		Висновки	А4 ел.ф.

Из	Лист	№ докум.	Підпис	Дата				
Розроб.		Мосолов			*Порівняльний аналіз алгоритмів генерування та вбудовування цифрових водяних знаків у 2D зображення*	Літера	Лист	Листів
Перев.		Василенко				Д		
						ХНУРЕ Кафедра КРіСТЗІ		
Н.контр.		Милютченко			Відомість кваліфікаційної роботи магістра			
Затв.		Антіпов						