УДК 004.056.53

Н. В. Копайгородська
В. В. Карпінець

ЗАХИСТ ЦИФРОВИХ ЗОБРАЖЕНЬ КОРИСТУВАЧІВ ОНЛАЙН-РЕСУРСІВ СТЕНАГОГРАФІЧНИМИ ЗАСОБАМИ

Вінницький національний технічний університет

Анотація.
Досліджено методи захисту цифрового контенту від несанкціонованого копіювання та використання в онлайн-ресурсах. Запропоновано комбінований стеганографічний метод вбудовування цифрового водяного знаку..
Ключові слова: Цифровий водяний знак (ЦВЗ), дискретне перетворення Фур'є (ДПФ), дискретне косинусне перетворенням (ДКП).

Abstract
Methods of protection of digital content from unauthorized copying and use in online resources are investigated. A combined steganographic method of digital watermark embedding is proposed.
Keywords: Digital Watermark (DWC), Discrete Fourier Transform (DFT), Discrete Cosine Transformation (DCT).

У сучасному інформаційному суспільстві велика кількість послуг забезпечується за допомогою комп’ютерних мереж та інформаційних технологій. Інформація, що представлена в цифровому вигляді, має бути надійно захищена від багатьох загроз: несанкціонованого доступу та використання, знищення, підробки, витоку, порушення ліцензійних угод, відмови від авторства. Захист інформації є вкрай важливим як в комерційній, так і в державній сферах.

Здійснено детальний огляд стаганографічних методів а саме: дискретне перетворення Фур’є та дискретне косинусне перетворення .

Дискретне косинусне перетворення (ДКП) є одним із відомих методів перетворення, який перетворює зображення із просторової області в частотну [1]. Він широко застосовується в обробці зображень, використовуючи як властивості декорреляції, так і енергетичного ущільнення. Як правило, підходи для водяних знаків ДКП використовували квадратну матрицю 8 × 8 як розмір блоку [2].

Дискретне перетворення Фур'є зображення веде до представлення величини та фази. Це перетворення має кілька характеристик. Важливою властивістю ДПФ є його незмінність щодо перетворення. Насправді просторові зсуви впливають не на величину, а на фазову складову [2]. ДПФ також надійний для обрізання. Насправді, коли водяний знак вбудований у величину, навіть якщо спектр розмитий, синхронізація не потрібна.

Запропонований комбінований метод полягає в вбудовуванні ЦВЗ в величину-ампілутуди дискретного перетворення Фур’є та застовуванням до неї дискретного косинусного перетворення. Вибір лише амплітуди ДПФ, а не фази зумовлений перевагою з точки зору непомітності. Тим не менше, схема показує слабку стійкості, коли використовується лише амплітуда ДПФ.

Оскільки ДКП дуже надійне проти атак обробки сигналів, ми вважаємо, що це відмінне рішення для вирішення поставленої задачі. Крім того, для підвищення безпеки запропонованого способу використовується перетворення Арнольда для шифрування водяного знаку

Причиною такого вибору є той факт, що величина ДПФ показує здатність забезпечувати високу непомітність, тоді як ДКП може покращити стійкість запропонованої техніки до загальних атак обробки сигналів.

Ідея використання алгоритму скремблювання полягає в підвищенні безпеки водяного знаку, щоб уникнути несанкціонованого доступу, щоб його підробити або видалити. Отже, це гарантує більшу безпеку та надійність зображення в процесі передачі. Перетворення Арнольда широко використовується у водяних знаках цифрових зображень завдяки своїй простоті та періодичності.

Для того, щоб оцінити непомітність запропонованої схеми, ми обчислюємо PSNR та SSIM між вихідним зображенням та зображенням з водяним знаком відповідно. Більше того, абсолютна різниця між зображеннями з водяними знаками та оригінальними зображення розраховано для всіх тестових зображень.

Індекс структурної подібності (SSIM) проводить вимірювання подібності за допомогою комбінації трьох евристичних факторів порівняння яскравості, порівняння контрасту та порівняння структури. Це найбільш впливова оцінки якості сприйняття [4].

Коефіцієнт пікового сигналу до шуму (PSNR) найбільш широко використовуваною оцінки у літературі з водяних знаків для вимірювання відстані між вихідним зображенням та водяним знаком [5].

Таблиця 1 – Порівняння непомітності між запропонованим методом та ДПФ

	Методи нанесення водяних знаків			
Зображення	ДПФ		Запропонований метод	
	PSNR	SSIM	PSNR	SSIM
Мандрил	45,58	0,9871	61,28	1,0
Перець	48,21	0,9745	65,97	1,0
Оператор	46,15	0,9803	63,54	0,9999
Лена	47,31	0,9785	61,97	0,9998
Gold Hill	49,73	0,9762	66,37	0,9999
Середній	47,396	0,9793	63,82	0,9999

З таблиці 1 видно, що поєднання двох перетворень ДПФ-ДКП дає кращі результати з точки зору непомітності, ніж підхід на основі ДПФ для всіх тестових зображень.

Для того, щоб оцінити стійкість запропонованої схеми, ми обчислюємо нормоване співвідношення (NC) між вихідним водяним знаком та вилученим.

Для перевірки стійкості алгоритму зображення з водяними знаками піддаються різним атакам [6]:

- шумова атака: гауссовий шум (GN) та сіль і перець шум (SPN);
- атака стиснення формату: стиснення JPEG та JPEG2000;
- атака обробки зображень: Гаусова фільтрація низьких частот (LPGF), згладжування Гауса (GS) та вирівнювання гістограм (HE);
- геометричні спотворення: обрізка (Cropp) та обертання.
- комбіновані атаки.

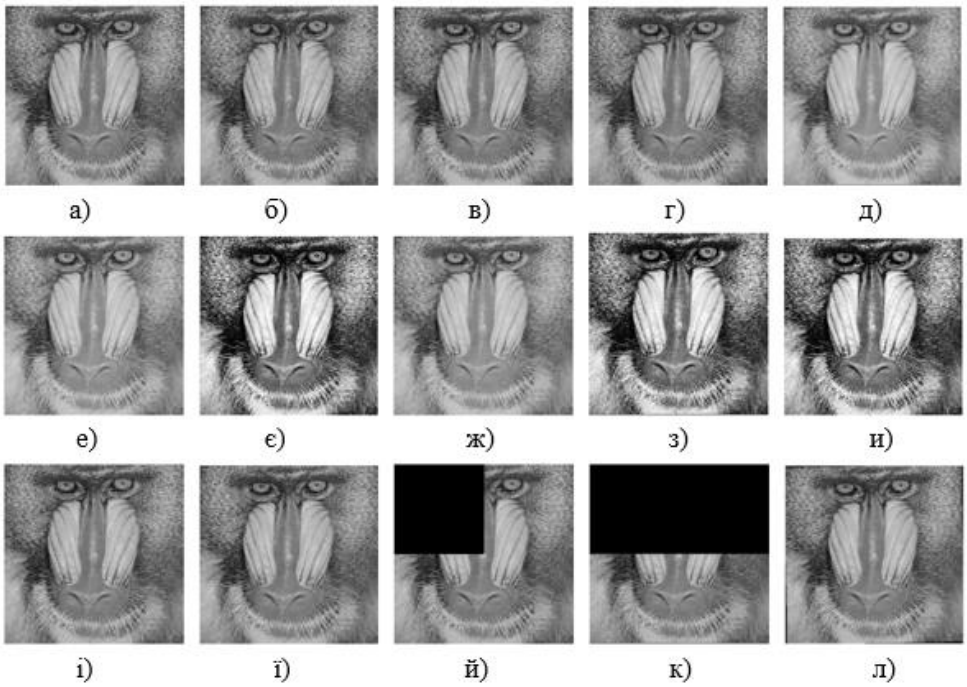

Рисунок 1 - Зразок зображень із вбудовуваними водяними знаками та застосуванням атак.

Запропонований метод забезпечує добру здатність витягувати водяні знаки проти кількох видів атак незалежно від природи зображення. Це ілюструє отримане значення NC, розраховані між вихідним водяним знаком та вилученим той, який перевищує 0,9694.

Більше того, незалежно від типу атаки, можна зробити висновок, що отримані результати з точки зору NC методу ДПФ-ДКП перевершує показники методу ДПФ.

Отже, запропонована схема вбудовування цифрового водяного знаку у зображення, що поєднує добре відомі перетворення ДПФ та ДКП для захисту авторських прав. Водяний знак вбудований в коефіцієнти ДКП середньої смуги амплітуди ДПФ зображення обкладинки за допомогою двох секретних ключів для підвищення безпеки. Перший використовується для генерації послідовностей PN, що вставляються у вбудовування водяного знаку тоді як другий - зашифрувати водяний знак за допомогою перетворення Арнольда.

Беручи отримані результати показують переваги об'єднання перетворень ДПФ та ДКП що запропонована схема забезпечує хорошу стійкість до найрізноманітніших атак для зображеннь, зберігаючи високу непомітність.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Хорошко В.О. Комп'ютерна стеганографія: [навчальний посібник] / В. О. Хорошко, Ю. Є. Яремчук, В. В. Карпінець. – Вінниця : ВНТУ, 2017. – 155 с.
2. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. – М.: Солон-Пресс, 2009. – 272 с
3. Коханович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Коханович, А. Ю. Пузиренко. – Київ: МК-Пресс, 2006. – 288 с.
4. Щєглов А.Ю. Захист компютерної інформації від несанкціонованого доступу. –спб.: Наука і техніка 2004. – 384 с.
5. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с
6. Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004) Image quality assessment: from error visibility to structural similarity. IEEE transactions on image processing, 13(4)
7. Азарова А.О. Методичні вказівки до проведення практичних занять та до виконання самостійної індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 – «Менеджмент» та 6.170103 – «Управління інформаційною безпекою» / Азарова А.О., Карпінець В.В. – Вінниця: ВНТУ, 2013. – 44 с.

Копайгородська Наталія Василівна — студентка групи УБ-19м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail:natali4ka16@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** — кандидат технічних наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця.

Kopaihorodska Nataliia Vasylivna — student, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnytsia

Supervisor: ***Karpinets Vasyl V.*** — Ph. D., assistant professor, Head of the Department of Management and Security of Information Systems, Vinnitsa National Technical University, Vinnytsia.