Роботу виконано за держбюджетною темою «Розвиток розподіленої енергетики в умовах ринку електричної енергії України з використанням технологій та систем цифровізації. Розділ 1. Організаційні та математичні моделі взаємодії учасників децентралізованого ринку електроенергії» (ЦИФРОВІЗАЦІЯ), КПКВК 6541230.

1. Evdokimov, V.; Kudin, A.; Chikhladze, V.; Artemchuk, V. A Blockchain Architecture for Hourly Electricity Rights and Yield Derivatives. FinTech. – 2026, 5(1), №2. https://doi.org/10.3390/fintech5010002
2. Pendle Finance Documentation. Available URL: https://docs.pendle.finance (application date 09.05.2026).

Гібридний метод приховування водяних знаків на основі конформних відображень та сингулярного розкладу матриць

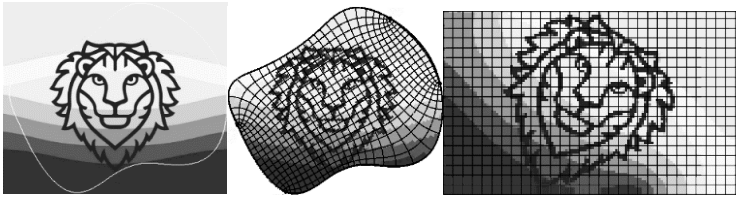
УДК 004.056.55 : 517.54

Андрій Бомба[1], Михайло Бойчура[2]

Національний університет водного господарства та природокористування, [2]m.v.boichura@nuwm.edu.ua

Традиційні методи вбудовування невидимих цифрових водяних знаків (ЦВЗ) в області є вразливими до геометричних атак, а використання частотних методів ускладнюється у випадку фігур складної геометрії. Метою роботи є підвищення захищеності зображень з криволінійною границею шляхом розроблення робастного методу вбудовування ЦВЗ, стійкого до топологічних деформацій.

Запропоновано підхід до накладання ЦВЗ на однозв'язну область (зображення) довільної форми. Він передбачає поєднання числових методів конформних відображень для перетворення досліджуваної області на прямокутник [1] та сингулярного розкладу матриць – для подальшого вбудовування прихованої інформації [2]. Окрім іншого, підхід передбачає побудову геометричного криптографічного ключа.



а) б) в)

Рис. 1. Початкове зображення (а), сітки фізичної області (б) та області комплексного потенціалу (в)

Алгоритм для вбудовування ЦВЗ складається з наступних кроків: визначаються межі криволінійної фігури, здійснюється відображення фізичної області на прямокутник, формується матриця яскравості пікселів, остання розбивається на блоки, до яких застосовуються сингулярні розклади,

модифікуються сингулярні числа блоків за допомогою бітової послідовності ЦВЗ, виконується зворотне відображення яскравості пікселів у фізичну область.

На рис.1, як приклад, зображено спеціальну схему: фігура – модельна область – область комплексного потенціалу.

Висновки. Запропонований підхід забезпечує високу робастність ЦВЗ до топологічних атак та стиснення JPEG. Використання конформної сітки як геометричного ключа забезпечує можливість надійно захищати приховану інформацію від вилучення.

1. Бомба А.Я., Бойчура М.В. Методи комплексного аналізу в задачах ідентифікації: монографія. Рівне: НУВГП, 2020. 188 с.
2. Liu R., Tan T. An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*. – 2002. – V. 4, №1. – P. 121-128.

Проблематика узагальненої оцінки методів криптографічного захисту інформації

УДК 004.056.55

Віра Тітова[1], Володимир Анікін[2]

Хмельницький національний університет,
[1]titovav@khmnu.edu.ua, [2]anikin_volodymyr@khmnu.edu.ua

Існує значна розбіжність в підходах до узагальненої оцінки методів криптографічного захисту інформації (КЗІ). Аналіз досвіду проведення як вітчизняних, так і зарубіжних криптографічних конкурсів, в межах яких очевидною була необхідність строгого критеріального порівняння запропонованих методів-претендентів між собою, показує неузгодженість підходів до такої порівняльної оцінки. Часто таке порівняння методів криптографічного захисту фактично зводиться до порівняння засобів КЗІ, оскільки у якості критеріїв порівняння обирається, як приклад, швидкодія роботи, чи інша фізична величина, що емпірично вимірюється на прототипі засобу КЗІ. Подібний підхід простежувався, зокрема, у конкурсних процедурах, пов'язаних із вибором стандарту ДСТУ 7624:2014 «Калина», де поряд із криптографічними властивостями враховувалися також показники ефективності реалізацій.

З одного боку, такий підхід може бути виправданий з точки зору прикладної спрямованості порівняння, де той чи інший метод КЗІ не несе жодного практичного сенсу у суто теоретичному вимірі. Проте, з іншого боку, коли необхідність узагальненого порівняння виникає в ході певних науково-дослідних робіт, в межах яких, наприклад, є необхідність підібрати методи КЗІ як компонент деякої більш глобальної системи, а об'єктом оцінювання виступають не готові засоби, чи навіть їх прототипи, а виключно теоретичні абстракції, узагальнені характеристики яких необхідно порівняти, то згаданий емпірично-орієнтований підхід не може бути застосований.

Одним із аргументів, щодо принципової розбіжності у підходах порівняння методів та засобів КЗІ є те, що при дослідженні кількох різних реалізацій засобів