УДК 535.42

КЛЮЧОВІ ВЛАСТИВОСТІ ОПТИЧНОГО ШИФРУВАННЯ НА БАЗІ САМОАСОЦІАТИВНОЇ СХЕМИ ФУР'Є-ГОЛОГРАФІЇ

А. А. Козловський[1, a], Л. М. Кохтич[1], Л. А. Держипольська[2]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут*

[2] *Інститут фізики НАН України*

Анотація

Оптичне шифрування – альтернативний метод захисту інформації, що використовує голографічні методи для кодуванню та декодування інформації. В статті розглядається самоасоціативна схема Фур'є голографії, в якій ключем дешифрування є частка початкового зображення, що поєднана з випадковим фазовим дифузором. Така схема дозволяє одночасно реалізувати оптичне шифрування інформації та асоціативне відновлення, тобто пошук інформації, що відрізняє дану схему від інших оптичних схем, які побудовані на ПВФШ. Також схема, в залежності від юстування, дозволяє отримати асоціативне відновлення, тобто зображення відновлюється з однаковою засвіткою по всій поверхні, або фантомне, в якому буде підсвіченно та частинка дифузору, яка використовувалася при відновленні.

Ключові слова: оптичне шифрування, голографічні методи захисту інформації, Фур'є-голографія, самоасоціативна схема Фур'є-голографії

Вступ

Найбільш поширеними методами захисту інформації на сьогоднішній день є методи математичного шифрування, які в той самий час демонструють слабкість перед спрямованими атаками на бази даних, які вони захищають. Тому, багато досліджень ведеться в напрямку альтернативних методів захисту інформації.

Наприклад, проводиться активне дослідження методів шифрування, які побудовані не на суто математичних моделях. Такими є голографічні методи захисту інформації. Це пояснюється тим, що ці методи працюють миттєво й володіють можливостями паралельної обробки масивів даних, одночасно з обробкою неоцифрованих даних.

В оптичному шифруванні, лінза є ключовим інструментом, адже вона фізично виконує перетворення Фур'є. Прості сферичні лінзи здатні створювати Фур'є-образ початкового зображення [1]. Завдяки цьому, вони використовуються в оптичному шифруванні.

Якщо розглядати голограми в контексті об'єкту дослідження, то створення самої голограми виступає як запис інформації (якогось зображення). Це відповідає кодуванню – якщо подивитись на голограму, яку ми створили при записі деякої інформації, буде неможливо зрозуміти, що дійсно зображено на голограмі, окрім шуму.

Одним з перших методів оптичного шифрування була схема подвійного випадкового фазового шифрування (ПВФШ), запропонована в 1995 році Філіпом Рефріджером та Бахрамом Джавіджі [2]. В схемі ПВФШ, що показана на Рис. 1, зображення, яке будуть шифрувати, вмонтовано в амплітудний дифузор.

На вхідне зображення діють лінзами. Зашифрованою інформацією вважається зображення, отримане після проходження другої лінзи. Відновлення інформації початкового зображення можливо тільки якщо в наявності є оригінальний ключ шифрування. Нажаль, у такій схемі наявна лінійна залежность між простим текстом і шифрованим. Після більш детального аналізу цієї проблеми, були розроблені різні методи криптоаналізу, побудовані на алгоритмах пошуку фаз, що забезпечують знаходження ключів до системи за допомогою наявної інформації по невеликій кількості пар простого тексту [3][4][5].

Не дивлячись на присутні проблеми лінійності в ПВФШ, активно ведеться пошук більш надійно захищених алгоритмів шифрування зображення, які створять можливісті використання індивідуальних ключів декодування для різного рівня персонального допуску.

1. Опис самоасоціативної схеми з однаковим опорним і предметним пучками як частинний випадок узагальненої схеми Фур'є-голографії

В роботах [6] [7] було показано теоретично, що якщо ми розглянемо голограму, в якій опорне та предметне зображення є однаковими, то будемо бачити утворення асоціативного зв'язка зображення з самим собою, що при відновленні такої голограми буде створювати відгук в певних порядках дифра-

[a] kozlovskyy.artur@gmail.com

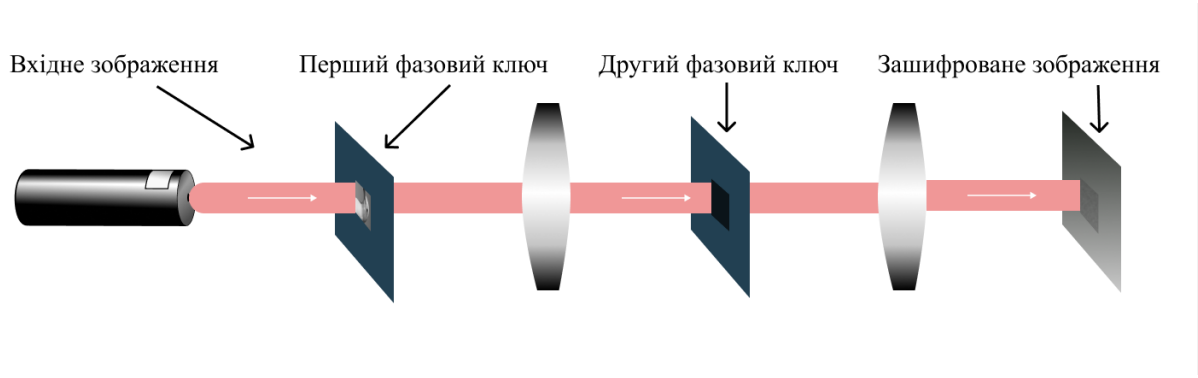

Рис. 1. Схема подвійного випадкового фазового шифрування

кції. Практично було доведено, що відгук буде мати вигляд оригінального зображення [8].

В роботі [9] була запропонована оригінальна самоасоціативна схема Фур'є-голографії, продемонстрована на Рис. 2. Застосовуючи таку схему для запису голограм при відновленні голограми, будемо мати відновлення зображення ідентичне записаному. Варто додати, що при відновленні за даною схемою, якщо ми використовуємо в схемі пучок, який несе не повну первинну інформацію (маємо не цілий первинний дифузор, яким записувалась голограма, а лише його частинку), то у відновленому зображення ми отримаємо все одно повну інформацію про первинне зображення (буде відновлюватися цілий первинний дифузор). В залежності від юстування схеми (наскільки гарно зведені пучки при записі голограми, ми можемо отримати асоціативне відновлення – в якому зображення відновлюється з однаковою засвіткою по всій поверхні, або ж фантомне – буде підсвічено та частинка дифузору, яка використовувалася при відновленні).

Фізично така схема досягається за допомогою отримання двох однакових пучків та розділу їх на два по амплітуді. Для такої схеми необхідно проводити юстування, за допомогою поворотного дзеркала, яке допомагає фокусувати пучки в площині голограми.

Коли промінь лазеру в установці проходить через первинний транспарант, що є спряженим з фазовим дифузором, він також отримує певну інформацію, що знаходиться в транспаранті. Після цього, ми розділяємо наш пучок на два за допомогою світлоподільника. Наступним етапом роботи схема є запис голограми. Вона записується в фокусній площині першої лінзи Фур'є двома ідентичними пучками, які ми отримали поділивши первинний світлоподільником.

При відновлення початкового зображення, нам необхідно використати один з променів, що буде проходити через частину початкового зображення. Даний пучок також має бути спряженим з відповідною частиною фазового дифузора. Після освітлення таким пучком голограми, будемо мати відновлений транспарант в Фур'є області другої Фур'є лінзи в +1 порядку дифракції.

Така самоасоціативна схема працює та має всі ознаки системи шифрування та дешифрування інформації. В ній, як і в звичних криптографічних системах, присутні алгоритми роботи, наприклад, на шифрування, та дешифрування. Перше представлено в схемі записом голограми, в той час як друга – її відновленням.

2. Основні властивості та переваги самоасоціативної схеми Фур'є-голографії при оптичному шифруванні та дешифруванні

Одної з особливостей самоасоціативної схеми є те, що вона дозволяє одночасно реалізувати оптичне шифрування інформації та асоціативне віднолення, тобто пошук інформації. Це відрізняє дану схеми від інших оптичних схем, які побудовані на ПВФШ [10].

За допомогою цієї особливісті, ми можемо проводити асоціативний пошук в масиві зашифрованих даних, або проводити шифрування даних в системі з асоціативним відгуком. Це відкриває широкий спектр нових можливостей завдяки поєднанню механізмів та властивостей шифрування та асоціативного відновлення зображень.

2.1. Обґрунтування двохкомпонентності ключа

В даній схемі ключем дешифрування є частка початкового зображення, що поєднана з випадковим фазовим дифузором. У результаті відновлення в зображення буде входити комплексна амплітуда пучка, яку ми використовували під час дешифрування зображення. Наведемо вираз для цього пучка.

$$b = |b|e^{-i\varphi d}$$

Тут $|b|$ – амплітудна частка ключа, яка містить інформацію про частинку початкового зображення ключа, φd – фазова частка. Остання несе в собі інформацію про зміну фази випадковим фазовим дифузором. Завдяки такій двокомпонентності ключа наша система дешифрування стає більш стійкою. Якщо спробувати використати ключ, в якому не вистачає одної з компонент, нехай то буде фазова чи амплітудна, відновлення первинного зображення не відбудеться, що показано на Рис. 3.

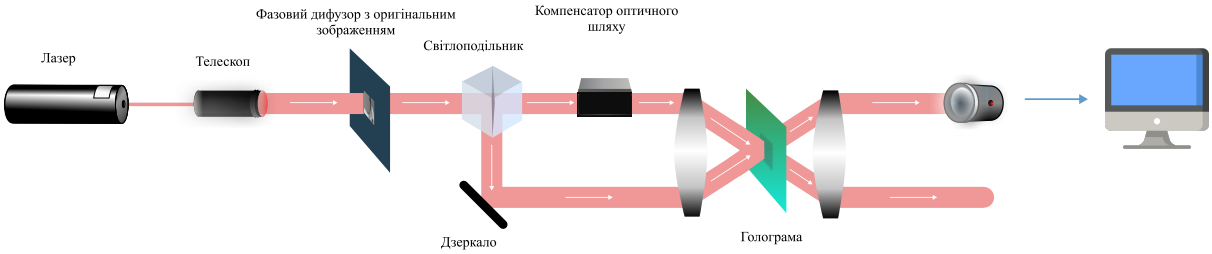

Рис. 2. Самоасоціативна схема Фур'є голографії

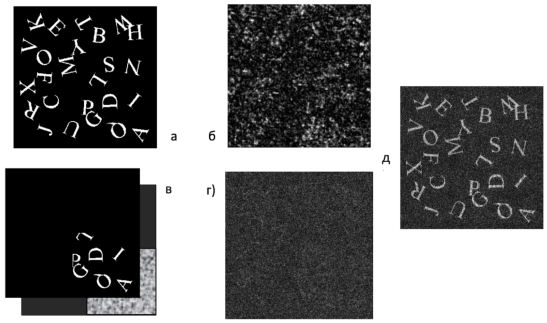

Рис. 3. Робота самоасоціативної схеми з використанням різних ключів дешифрування. а)оригінальне зображення; б) цілий ключ (амплітудна і фазова частини); в) дешифроване зображення за використання тільки фазової частини ключа; г) дешифроване зображення за використання тільки амплітудної частини ключа; д) дешифроване зображення цілим ключем.

2.2. Аналіз надлишковості ключа

Загальна якість відновленого зображення визначається як середній контраст, на який впливали два параметри – величина самого ключа, що визначається як відношення площі частини зображення використаного для дешифрування й щільність початкового зображення, тобто його середня інтенсивність.

$$\bar{V} = \frac{\bar{I}_{\max} - \bar{I}_{\min}}{\bar{I}_{\max} + \bar{I}_{\min}}$$

Тут $I_{\max}$ та $I_{\min}$ відповідають за значення інтенсивності в найясравіших та найтемніших ділянках зображення відповідно.

Для нас буде більш корисно ввести новий критерій якості зображення, який буде брати за основу ймовірність правильного виявлення частинок даних – бітів.

У бінарно-відновленому зображення світлі ділянки містять сигнал та шум, а темні ділянки – тільки шум, оскільки сигналу на них немає. Тому нам також варто розгялнути критерій якості зображення в контексті сигнал/шум. Тому розглянемо наступні вирази.

$$\bar{I}_{\max} = S + N, \quad \bar{I}_{\min} = N, \quad SNR = \frac{S}{N}$$

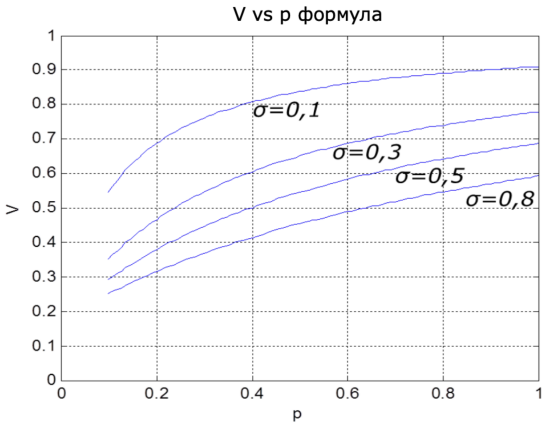

Рис. 4. Залежності якості зображення від розміру ключа для різної щільності зображення

Тут S, N і SNR – шум, сигнал та співвідношення шум/сигнал. Використовуючи дві попередні формули запишемо такі співвідношення.

$$\bar{V} = \frac{SNR}{SNR + 2}, \quad SNR = \frac{2\bar{V}}{1 - \bar{V}}$$

Також можна записати таким чином.

$$SNR = 2(p/\sigma + 0,21)$$

З даної формули ми бачимо, що при зменшенні площі ключа дешифрування, а також при збільшенні щільності зашифрованого зображення, співвідношення шум/сигнал буде зменшуватись.

Графік залежності якості відновленого зображення різної щільності від розміру ключа наведено на Рис. 4.

Найкращу якість відновленого зображення ми отримаємо, якщо будемо мати зображення з низькою щільністю. Зображення, які мають високу щільність, бажано інвертувати для збільшення їх якості відновлення. Наприклад, якщо необхідно зашифрувати фотографію тексту, бажано її перетворити в таку, в якій літери будуть білими, а простір навколо них – чорний. Так вдасться відновити текст більш якісно.

Звернемо увагу на те, що схема, яку ми розглядаємо, володіє високою гнучкістю завдяки своїй асоціативності. Так, ми можемо регулювати розмір ключа дешифрування, а також вибрати бажану частку початкового зображення, що ми використовуємо для відновлення, й це буде впливати на результат деши-

фрування. Основною вимогою до ключа є те, щоб він містив в собі частку оригінального зображення.

Ми вже отримали залежність якості відновленого зображення від розміру використаного ключа, тому ми можемо обрати такий ключ, який нам потрібно, знаючи його передбачувану стійкість до пошкоджень.

Оскільки на відміну від тексту, для дешифрування якого необхідне високоточне відтворення, для дешифрування зображення набагато більшу вагу має його впізнаваність, аніж точність відтворення. Так, ми можемо зробити ключ мінімальним, тобто таким що несе мінімальну кількість інформації для того, щоб розкодоване зображення було впізнаваним.

Визначимо параметр гарантованого відтворення даних, що будуть мати контраст не нижче певного рівня $V_{\min}$, й йому буде відповідати певний мінімальний розмір ключа $p_{\min}$. Якщо ми втратимо якусь частину такого ключа, ми все ще зможемо відновити зображення, але його якість буде менше за допустиму, яку ми визначили як $V_{\min}$. Візьмемо ключ з розміром вдвічі більшим за $p_{\min}$, і якщо ми втратимо 50% відсотків такого ключа, то ми зможемо гарантовано відновити наше зображення з задовільною якістю. Ці додаткові 50% є надлишковими. Чим більше буде ключ, тим більш захищеним він буде від втрат.

Висновки

Дана робота присвячена дослідженню оптичного шифрування на прикладі самоасоціативної схеми Фур'є-голографії. Були показані алгоритми оптичного шифрування та дешифрування, які використовуються під час роботи самоасоціативної схеми Фур'є-голографії. Було обґрунтувано двокомпонентность ключа шифрування, що складається з фазової та амплітудної частин.

В ході роботи встановлено, що найкращу якість зображення, яке відновлюється, можна отримати за умови шифрування зображення з низькою щільністю. Було доведено, що зображення з високою щільністю бажано інвертувати, задля покращення результату відновлення.

Було показано, що дана схема дає можливість зробити ключ шифрування надлкишковим, що підвищить захищеність й вбереже результат дешифрування, якщо ключ зазнає пошкоджень.

Перелік використаних джерел

1. Goodman Joseph W. Introduction to Fourier Optics. — 1996. — P. 491 c.
2. Refregier Philippe, Javidi Bahram. Optical image encryption based on input plane and Fourier plane random encoding. — 1995.
3. Carnicer A., Usategui. M. M. Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys. — 2005.
4. Guo C., Liu S., Sheridan J. T. Iterative phase retrieval algorithms. I: Optimization // Appl. Opt., 54(15). — 2015. — P. 4698–4708.
5. Guo C., Liu S., Sheridan J. T. Iterative phase retrieval algorithms. Part II: Attacking optical encryption systems // Appl. Opt., 54(15). — 2015. — P. 4709–4719.
6. Heerden P. J. Van. A new optical method of storing and retrieving information // Applied Optics. . Vol.2. No4. — 1963. — P. 387–392.
7. Heerden P. J. Van. Theory of optical information storage in solids // Applied Optics. Vol.2. No4. — 1963. — P. 393– 400.
8. K.S.Pennington, R.J.Collier. Hologram-generated ghost image experiment // Applied physics letters. Vol.8. No 14. — 1966. — P. 14–16.
9. Г. Держипольський А. Кореляційні перетворення оптичних полів та обробка інформації в самоасоціативній схемі Фур'є - голографії. — 2021. — С. 137 с. — Режим доступу: http://www.iop.kiev.ua/assets/files/dissertations/derzypolskyiDis.pdf.
10. Derzhypolskyi A., Derzhypolska L., Gnatovskyi O. Optical encryption based on self-associative Fourier holographic scheme and its Walsh- Hadamard generalization in virtual optics domain.