

МЕТОДИ ПРИХОВУВАННЯ ДАНИХ У ЗОБРАЖЕННЯХ НА ОСНОВІ АСИМЕТРИЧНОГО ШИФРУВАННЯ ТА АДАПТИВНОЇ СТЕГАНОГРАФІЇ

Вінницький національний технічний університет

Анотація

Досліджено поєднання асиметричного шифрування та адаптивної стеганографії для підвищення конфіденційності й прихованості інформації у цифрових зображеннях. Проаналізовано сучасні методи вбудовування зашифрованих даних у графічні контейнери та їх стійкість до стиснення і стегоаналізу. Розглянуто використання асиметричних криптосистем для безпечного розподілу ключів і попереднього шифрування повідомлення. Обґрунтовано доцільність поєднання криптографічних і стеганографічних підходів для підвищення рівня захисту інформації під час передавання даних відкритими каналами зв'язку. Визначено основні переваги підходу для забезпечення надійності та стійкості системи захисту.

Ключові слова: асиметричне шифрування, адаптивна стеганографія, захист інформації, цифрові зображення, криптографія, приховування даних, інформаційна безпека.

Abstract

The combination of asymmetric encryption and adaptive steganography to increase the confidentiality and concealment of information in digital images is studied. Modern methods of embedding encrypted data into graphic containers and their resistance to compression and steganalysis are analyzed. The use of asymmetric cryptosystems for secure key distribution and pre-encryption of messages is considered. The feasibility of combining cryptographic and steganographic approaches to increase the level of information protection during data transmission over open communication channels is substantiated. The main advantages of the approach for ensuring the reliability and stability of the protection system are identified.

Keywords: asymmetric encryption, adaptive steganography, information protection, digital images, cryptography, data hiding, information security.

Вступ

Зростання обсягів передавання цифрових зображень у мережевому середовищі потребує надійних засобів захисту конфіденційної інформації. Криптографічні методи забезпечують захист змісту даних, однак не приховують факту їх передавання, тоді як стеганографія дозволяє маскувати інформацію у мультимедійних контейнерах. Найбільш ефективним підходом є поєднання асиметричного шифрування та адаптивної стеганографії, що забезпечує одночасно конфіденційність і прихованість передачі даних.

Результати дослідження

Шифрування таємної інформації із застосуванням алгоритму AES з наступним вміщенням зашифрованих даних у зображення способом кластеризації найближчого центру. Проте зберігання ключа шифрування поряд із зашифрованими відомостями в одному носії суттєво зніжує ступінь надійності системи. Втілено подвійне стеганографічне перетворення, що передбачає вкладення одного носія в інший, але застосування методу LSB та брак чітко окреслених систем керування ключами обмежують фактичну стійкість представленого вирішення. Підходи ґрунтуються на використанні алгоритмів DES, Blowfish та SHA-256, проте використання застарілих криптографічних засобів або носіїв зі стисненням контейнера може спричинити втрату чи пошкодження прихованих даних [1].

Зростання витривалості адаптивної стеганографії під час передачі візуальних об'єктів у форматах JPEG та PNG, особливо з огляду впливу процедур ущільнення, які часто

впроваджують додаткову обробку медіа. Адаптивний стеганографічний метод, який протистоїть JPEG компресії, через аналіз втрачених при стисненні відомостей та виокремлення незмінних текстурних ознак ділянок із високою спроможністю до реставрації прихованого змісту після обробки. Вкладення реалізується у ці стійкі зони, що дає змогу покращити витягання секрету та збільшити якість зображень навіть після повторного ущільнення порівняно з класичними підходами, такими як LSB чи методи на базі автоенкодерів [2].

Напрям, котрий також націлений на пристосування до типових змін коефіцієнтів DCT при JPEG ущільненні, є спосіб адаптивного визначення простору вкладення з динамічним виправленням помилок, де вибір області залежить від статистичних характеристик певного зображення, а код корекції неточностей калібрується динамічно для зниження надмірності та забезпечення міцності до зовнішніх трансформацій. Дослідні результати засвідчили збільшену несприйнятливість до стегоаналізу після ущільнення, що є визначальним для практичних застосувань у відкритих шляхах комунікації [3].

Застосування полярних кодів, які дозволяють оминати зміни «чутливих» коефіцієнтів при високих коефіцієнтах якості JPEG та гарантують безпомилкову стійкість до повторного стиснення, чим розв'язують одну з найважливіших труднощів стеганографії у частотній області [4].

Використання асиметричного шифрування у стеганографічних системах зумовлене необхідністю усунення проблеми безпечного розподілу ключів, що є характерною для симетричних алгоритмів. На відміну від підходів, де секретний ключ зберігається разом із контейнером або передається тим самим каналом зв'язку, асиметричні криптосистеми передбачають застосування пари ключів відкритого для шифрування та закритого для розшифрування. Модель дозволяє здійснювати попереднє шифрування перед його вбудовуванням у зображення без ризику компрометації ключового матеріалу навіть у випадку перехоплення контейнера. Найпоширенішими алгоритмами в цьому контексті є RSA та криптографія на еліптичних кривих, що забезпечують високий рівень криптостійкості на основі складності задач великих чисел [5].

У системах застосовується ECC, оскільки менша довжина ключів забезпечує зменшення обсягу шифротексту, що безпосередньо впливає на зниження навантаження на контейнер. Важливим для адаптивних методів у форматах JPEG та PNG, де надлишкове вбудовування може призвести до статистичних викривлень або зміни якості. Асиметричне шифрування дозволяє формувати компактні криптограми, які надалі розміщуються в обраних текстурно стійких або частотно стабільних ділянках зображення, визначених за допомогою адаптивного аналізу ентропії [6]. Подальший розвиток отримали гібридні криптостеганографічні схеми, у яких асиметричний алгоритм застосовується для захисту симетричного ключа, а основний масив даних шифрується швидкодіючими блочними алгоритмами. Він поєднує переваги високої швидкості симетричного шифрування та безпечного управління ключами асиметричної криптографії. Поєднанні з адаптивним вибором областей вбудовування він забезпечує багаторівневий захист навіть у разі виявлення факту приховування або часткового пошкодження контейнера відсутність приватного ключа, запобігає відновленню змісту повідомлення [7].

Асиметричне шифрування та адаптивна стеганографія формує багаторівневу модель захисту інформації, у якій криптографічна складова забезпечує конфіденційність змісту повідомлення, а стеганографічна приховування самого факту його існування. Принцип розділення функцій безпеки навіть у разі виявлення вбудованих даних зловмисник стикається з необхідністю подолання криптографічного захисту, що значно підвищує загальну стійкість системи. Адаптивний вибір областей вкладення, заснований на аналізі статистичних та текстурних характеристик зображення, мінімізує ймовірність стегоаналізу, тоді як асиметричні алгоритми усувають проблему компрометації ключів під час передачі контейнера відкритими каналами зв'язку [8].

Теоретична модель взаємодії зазначених технологій передбачає попереднє шифрування інформаційного повідомлення відкритим ключем отримувача з подальшим перетворенням отриманої криптограми у форму, придатну для адаптивного вбудовування. Внаслідок цього структура зашифрованих даних набуває властивостей псевдовипадковості, що додатково ускладнює статистичне виявлення прихованого вмісту. Використання ентропійного аналізу,

частотних характеристик або оцінки стабільності коефіцієнтів перетворення дозволяє оптимізувати процес розміщення криптограми, щоб забезпечити баланс між місткістю контейнера, непомітністю змін та стійкістю до повторного стиснення або цифрової обробки [9].

Інформаційна безпека системи може розглядатися як незалежний захисний механізм, рівень надійності яких визначається найстійкішим компонентом. Асиметричне шифрування гарантує криптографічну незламність повідомлення навіть у випадку повного вилучення прихованих даних, тоді як адаптивна стеганографія знижує імовірність їх виявлення.

Висновки

Ефективний захист конфіденційних даних у цифрових зображеннях досягається шляхом поєднання асиметричного шифрування та адаптивної стеганографії. Адаптивні методи вбудовування забезпечують стійкість прихованої інформації до стиснення та цифрової обробки зображень, тоді як асиметрична криптографія вирішує проблему безпечного розподілу ключів і гарантує конфіденційність повідомлення. Поєднання зазначених підходів формує багаторівневий механізм захисту, що підвищує прихованість, цілісність і криптографічну стійкість передавання даних у відкритих каналах зв'язку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. В. В. Лукічов Ю. В. Баришев Н. Р. Кондратенко В. І. Маліновський. МЕТОД АДАПТИВНОГО БАГАТОШАРОВОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ СТЕГANOГРАФІЇ ТА КРИПТОГРАФІЇ. Інформаційні технології та комп'ютерна інженерія. URL: <https://itce.vntu.edu.ua/index.php/itce/article/view/966/628>.
2. Adaptive Image Steganography Against JPEG Compression – DOAJ. Directory of Open Access Journals – DOAJ. URL: https://doaj.org/article/2243d95aa5914e08b07a42853c0d3823?utm_source.
3. О. С. КРАВЧЕНКО. ЗАГАЛЬНА ТЕХНОЛОГІЯ ШИФРУВАННЯ ТА ВБУДОВУВАННЯ ДАНИХ В РАСТРОВІ ЗОБРАЖЕННЯ, ЩО Є СТІЙКИМ ДО СТИСНЕННЯ JPEG. Національний технічний університет «Харківський політехнічний інститут», Україна. URL: <https://doi.org/10.20998/2220-4784.2021.02.04>.
4. Jimin Zhang Xiaolei He1, Yun Cao1 Errorless robust JPEG steganography using steganographic polar codes - Journal on Information Security. SpringerLink. URL: https://link.springer.com/article/10.1186/s13635-024-00173-4?utm_source.
5. І.А Терейковський С.О Гнатюк. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського». ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ Навчальний посібник. URL: <https://ela.kpi.ua/server/api/core/bitstreams/0dbba7ac-40e4-4a83-80b7-f729109cfe9a/content>.
6. Zhe Miao. Elliptic curve cryptography: Theory, security, and applications in modern network security. Southeast University Nan Jing. URL: <https://doi.org/10.54254/2753-8818/51/2024CH0183>.
7. Ganavi M. Prabhudeva S. Hemanth Kumar N. P. An Efficient Image Steganography Scheme Using Bit-plane Slicing with Elliptic Curve Cryptography and Wavelet Transform. URL: <https://doi.org/10.5815/ijcnis.2022.04.04>.
8. Ковтун, В. Ю., Гнатюк, С. О., & Кінзерявий, О. М. (2013). Modern methods of computer steganography systematization. Ukrainian Scientific Journal of Information Security, 19(3), 209–217. <https://doi.org/10.18372/2225-5036.19.5628>
9. Казміді, І. Д. Сучасний стан стеганографії цифрових зображень / Казміді І. Д., Зубок В. Ю. // Theoretical and Applied Cybersecurity : Матеріали III Всеукраїнської науково-практичної конференції (TACS-2025), [Київ], 29 травня 2025 р. / НН ФТІ, КПІ ім. Ігоря Сікорського. - Київ, 2025. - С. 42-48.

Оболонська Яна Олександрівна – студентка групи 1БС-226, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vn.oyana@gmail.com

Науковий керівник: **Лукічов Віталій Володимирович** – доцент, кафедри захисту інформації, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: lukichov.vitaliy@vntu.edu.ua

Бондаренко Павло Якович – старший викладач кафедри військової підготовки Вінницький національний технічний університет, Вінниця, e-mail: pavlobondarenko1970@gmail.com

Obolonska Yana Oleksandrivna - student of group 1BS-22b, faculty of information technologies and computer engineering, citizen of the Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: vn.oyana@gmail.com

Research supervisor: **Lukichov Vitaliy Volodymyrovych** – associate professor, Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University,

Vinnytsia, e-mail: lukichov.vitalyi@vntu.edu.ua

Pavlo Bondarenko – Senior Lecturer, Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: pavlobondarenko1970@gmail.com