КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.677
УДК 004.056

Римчук Ірина Віторівна
магістр кафедри комп'ютерної інженерії та безпеки
Луцький національний технічний університет, Луцьк, Україна
rymchuk.i1209@lntu.edu.ua

Костючко Сергій Миколайович
к.т.н., доцент кафедри комп'ютерної інженерії та безпеки
Луцький національний технічний університет, Луцьк, Україна
ORCID ID: 0000-0002-1262-6268
s.kostiuchko@gmail.com

Поліщук Микола Миколайович
к.т.н., доцент кафедри комп'ютерної інженерії та безпеки
Луцький національний технічний університет, Луцьк, Україна
ORCID ID: 0000-0002-1218-5925
polishchuk.kolia@gmail.com

Гринюк Сергій Васильович
к.т.н., доцент кафедри комп'ютерної інженерії та безпеки
Луцький національний технічний університет, Луцьк, Україна
ORCID ID: 0000-0002-0080-3167
sergij.grunjuk@gmail.com

Конкевич Людмила Миколаївна
асистент кафедри комп'ютерної інженерії та безпеки
Луцький національний технічний університет, Луцьк, Україна
ORCID ID: 0000-0002-8279-3133
k.liudmilka@lutsk-ntu.com.ua

БЕЗПЕКА КОМУНІКАЦІЙНИХ ПРОЦЕСІВ З ВИКОРИСТАННЯМ ВІЗУАЛЬНОЇ КРИПТОГРАФІЇ

Анотація. Стаття присвячена дослідженню технологій шифрування даних із акцентом на візуальну криптографію, яка є сучасним і перспективним методом забезпечення конфіденційності інформації. Основна увага приділяється аналізу існуючих методів шифрування інформації та розробці рішень, що дозволяють забезпечити надійний захист комунікацій. Візуальна криптографія, як один із сучасних методів, є актуальною через зростання потреби у захисті конфіденційних даних в умовах посилення загроз кібербезпеки. У роботі описано основні принципи візуальної криптографії, її переваги та практичні можливості застосування у сферах, де конфіденційність інформації має вирішальне значення, таких як державна безпека, військова сфера, фінансові установи та системи охорони здоров'я. Описано переваги візуальної криптографії, що дозволяє передавати зашифровані повідомлення у вигляді зображень, які можна розшифрувати шляхом фізичного накладання частин. Це розширює потенціал технології у контексті систем аутентифікації та доступу. Крім того, стаття містить опис програмних засобів для реалізації шифрування та розшифрування інформації, а також детальний огляд можливостей використання мов програмування для вирішення таких задач. Розглянуто ключові алгоритми та методи шифрування, оцінюючи їх ефективність та можливості впровадження у реальні системи захисту інформації. Завдяки проведеним дослідженням було проаналізовано різні підходи до захисту даних і визначено переваги візуальної криптографії у порівнянні з іншими методами. Результати дослідження демонструють ефективність візуальної криптографії як методу захисту інформації, особливо у випадках, коли необхідно уникнути залежності від складних цифрових технологій. Перспективи подальших досліджень включають розробку більш досконалих алгоритмів візуального

шифрування, адаптивних до різних умов використання, а також впровадження технології для захисту критично важливих даних у різних галузях.

Ключові слова: криптографія; V-Crypt; симетричне шифрування; асиметричне шифрування; стеганографія.

ВСТУП

Дослідження та розробки у сфері візуальної криптографії залишаються актуальними через низку важливих факторів, які стосуються безпеки даних, особливо в контексті зростаючої цифрової комунікації. Візуальна криптографія забезпечує високий рівень конфіденційності за рахунок відсутності необхідності використання комп'ютерних алгоритмів для розшифрування. Це дозволяє передавати захищені дані у вигляді зображень, які можна розшифрувати лише шляхом фізичного накладення шарів. Це важливо для державних та військових структур, де потрібно забезпечити максимальну секретність даних. Оскільки для відновлення зашифрованого повідомлення необхідні фізичні компоненти (шари зображення), цей метод захищений від цифрових атак, таких як злом програмного забезпечення або перехоплення даних. Останні дослідження розширюють межі застосування візуальної криптографії в області біометричної ідентифікації. Використання цього методу для шифрування та захисту біометричних даних (відбитків пальців, зображень обличчя тощо) відкриває нові перспективи для безпечного доступу до систем. Візуальна криптографія доповнює традиційні методи шифрування. Простота реалізації, фізична природа шифрування та захист від цифрових атак роблять цей напрям важливим для розвитку безпечних комунікацій в умовах сучасних загроз кібербезпеці.

Постановка проблеми полягає у забезпеченні надійного захисту даних під час їх передачі в умовах зростаючих загроз кібербезпеки та крадіжки інформації. З розвитком цифрових технологій і збільшенням обсягу переданих через Інтернет даних виникає потреба у впровадженні нових методів захисту, які були б ефективними і стійкими до сучасних атак.

Аналіз останніх досліджень і публікацій. Візуально-порогова схема, рекурсивне приховування секретів та зображення в градаціях сірого — це концепції, що можуть бути ефективно поєднані для створення складних та багаторівневих методів шифрування.

У пороговій схемі секретом може бути будь-який тип даних. Наприклад, це може бути зображення I, що складається з чорних і білих пікселів. Секретне зображення I може бути закодовано як двійковий рядок K = K(I), де 1 означає чорний піксель, а 0 — білий піксель. Використовуючи будь-яку зручну схему обміну секретами, можна створити спільні ресурси для K. Пізніше K буде реконструйовано за допомогою відповідного алгоритму для схеми обміну секретами. Зображення I перетворюється назад за допомогою отриманого двійкового рядка. Однак у цій основній схемі обміну секретами, криптографічні обчислення з використанням комп'ютера необхідні для спільного використання секрету та декодування секрету зі спільних даних. У всіх схемах обміну секретами необхідна значна складність для шифрування та декодування секрету, тому комп'ютери є важливими.

Кафрі та Керен [1] поставили наступне запитання: чи можливо створити схему спільного використання секретів, у якій секретне зображення I можна реконструювати візуально шляхом накладання випадкових сіток? Кожна сітка складатиметься з прозорості, що складається з чорних і білих пікселів. Пізніше Наор і Шамір [2] представили спеціальну реалізацію, яку назвали візуальним секретним обміном (VSS).

Цей метод може безпечно обмінюватися інформацією про зображення (друкованим текстом, рукописними нотатками, зображеннями тощо), а також можна декодувати спільні секрети за допомогою зорової системи людини. На основі секретного повідомлення (оригінального зображення) схема VSS генерує n зображень (відомих як спільні ресурси), які можна надрукувати на n прозорих плівках. У схемі k-out-of-n буде n прозорих плівок, і якщо буде накладено будь-яке k або більше k прозорих плівок, має з'явитися оригінальне секретне зображення I, але жодної інформації про вихідне зображення неможливо отримати, якщо менше ніж гранична кількість k прозорих плівок укладено (k-1 частка).

Основна відмінність між традиційною пороговою схемою та візуальною пороговою схемою полягає в тому, як секрет відновлюється. Традиційна порогова схема зазвичай передбачає обчислення в скінченному полі; у зоровій пороговій схемі обчислення виконується зоровою системою людини [8]. В обох типах схем умови безпеки однакові.

Рекурсивне приховування секретів було вперше представлено у [5] із застосуванням як до зображень, так і до друкованого тексту, щоб підвищити ефективність візуальної криптографії та зробити можливим включення додаткової секретної інформації, яка служить стеганографічним каналом. Ідея, пов'язана з рекурсивним приховуванням секретів, полягає в тому, що кілька повідомлень можуть бути приховані в одному з спільних ресурсів вихідного секретного зображення. Секретні зображення, які потрібно приховати, беруться відповідно до їхніх розмірів від найменшого до найбільшого (тобто секретний розмір подвоюється на кожному кроці). Найменше секретне зображення розділене на n часток за допомогою основної ідеї візуальної криптографії. Ці n часток розташовані одна під одною, і тепер вони представляють першу частку секретного зображення. Друга частка виконується таким чином, що якщо n часток накладаються, то розкривається секретне зображення, яке розглядається. Цей процес повторюється рекурсивно. Важливо зауважити, що частка вихідного секретного образу, яка містить рекурсивно приховану інформацію, також повинна містити обидві частки останнього прихованого секретного образу [5]. По відношенню до оригінального секретного зображення це накладає примус на розмір секретних зображень.

У сірому зображенні значення кожного окремого пікселя містить інформацію про інтенсивність. Зображення такого типу також називаються чорно-білими. Вони складаються виключно з сірих відтінків і, таким чином, відрізняються від однобітових чорно-білих зображень. Найтемнішим можливим відтінком є чорний, що означає повну відсутність прохідного або відбитого світла, а найсвітлішим можливим відтінком є білий.

Метою статті є розробка нових методів та дослідження існуючих для забезпечення захищеної передачі інформації у вигляді візуальних даних.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

У сучасному світі, де обсяг інформації, що передається через Інтернет, зростає експоненціально, а загрози кіберзлочинності й крадіжки даних стають дедалі складнішими та витонченішими, постає необхідність у впровадженні більш надійних методів захисту інформації. Візуальна криптографія пропонує інноваційний підхід, який ґрунтується на фізичних властивостях шифрування і не вимагає застосування складних алгоритмів для розшифровки. Цей метод дозволяє передавати інформацію у вигляді зображень, які можуть бути розкриті тільки шляхом фізичного накладення заздалегідь

визначених шарів, що надає йому унікальну перевагу порівняно з традиційними цифровими методами захисту.

Один з основних аспектів, який робить цей метод привабливим, полягає в тому, що він забезпечує винятковий рівень захисту, що особливо важливо для таких секторів, як державна безпека, військова сфера та розвідувальні організації. У цих сферах висока конфіденційність та секретність є ключовими вимогами. Використання фізичних компонентів для відновлення зашифрованої інформації мінімізує ризики, пов'язані з цифровими загрозами, такими як злом програмного забезпечення або перехоплення даних. Ця властивість робить візуальну криптографію надзвичайно надійним інструментом, оскільки вона забезпечує захист навіть у тих випадках, коли інші методи шифрування можуть виявитися вразливими.

Окрім цього, сучасні наукові дослідження значно розширюють потенційні сфери застосування візуальної криптографії, зокрема в галузі біометричної ідентифікації. Це відкриває нові горизонти для захисту особливо чутливих даних, таких як відбитки пальців, зображення обличчя та інші біометричні параметри, які все частіше використовуються для ідентифікації особистості. Застосування візуальної криптографії для шифрування таких даних дозволяє суттєво підвищити рівень безпеки доступу до різноманітних систем та сервісів, що є надзвичайно важливим у зв'язку зі збільшенням ролі біометричних методів аутентифікації.

Ця технологія володіє значним потенціалом для застосування в різних галузях, зокрема у фінансовому секторі, системах охорони здоров'я, телекомунікаціях і сфері електронної комерції, де захист персональних і конфіденційних даних є одним з основних пріоритетів. Простота реалізації, фізична основа шифрування і висока стійкість до цифрових загроз роблять візуальну криптографію перспективним інструментом для впровадження нових стандартів безпеки в умовах зростання кіберзагроз. Розвиток цієї технології має потенціал суттєво змінити підхід до забезпечення інформаційної безпеки у майбутньому, пропонуючи альтернативні або додаткові методи захисту, які здатні ефективно підсилювати або навіть заміняти традиційні криптографічні рішення.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Огляд криптографічних методів

В процесі розробки програмного забезпечення для візуальної криптографії важливим етапом став огляд і аналіз існуючих методів та засобів, які можуть бути використані для ефективного вирішення задачі шифрування і передачі інформації. З огляду на специфіку задачі, розглянуто кілька ключових методів шифрування, а також програмні засоби, що забезпечують їх реалізацію. Це охоплює як симетричні, так і асиметричні методи шифрування, кожен з яких має свої переваги і недоліки.

Симетричне шифрування

Симетричні алгоритми, такі як AES (Advanced Encryption Standard) і DES (Data Encryption Standard), широко використовуються завдяки своїй високій швидкості. Для шифрування та розшифрування використовується один і той самий ключ (рис. 1). Це робить процес дуже швидким, що є критичним для систем, де потрібно обробляти великі обсяги даних у реальному часі. Однак одним з основних викликів є забезпечення надійного зберігання цього ключа, адже компрометація ключа призведе до розкриття зашифрованої інформації.

ISSN 2663 - 4023

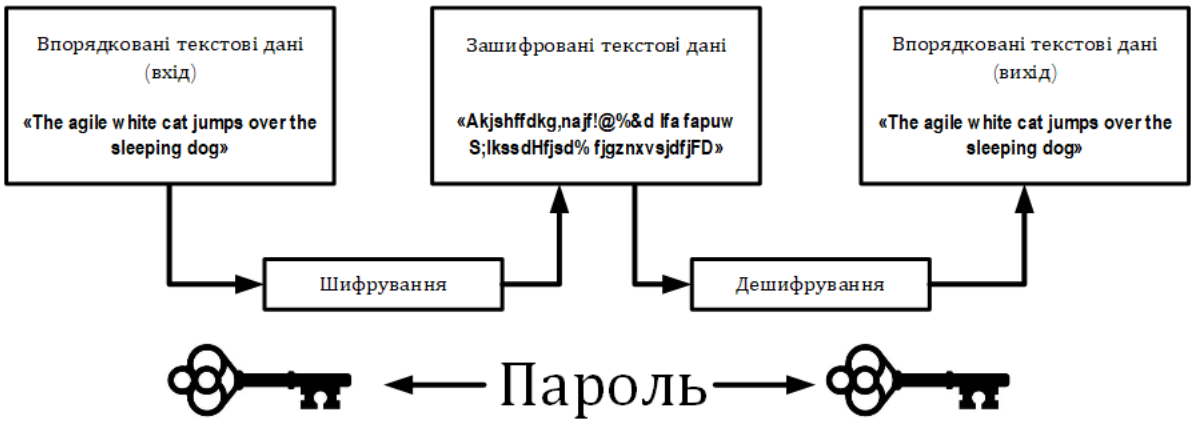

Рис. 1. Симетричне шифрування

Асиметричне шифрування

Асиметричні методи, такі як RSA (Rivest–Shamir–Adleman) та ECC (Elliptic Curve Cryptography), використовують дві пари ключів: публічний для шифрування і приватний для розшифрування (рис. 2). Це дозволяє безпечно обмінюватися інформацією навіть без попередньої зустрічі для передачі ключа. Хоча ці методи менш ефективні з точки зору швидкості в порівнянні з симетричними алгоритмами, вони є більш надійними для обміну ключами та забезпечення конфіденційності.

Візуальна криптографія зосереджена на передачі зашифрованих зображень або графічної інформації. Для цієї задачі важливо вибрати методи шифрування, які забезпечують баланс між швидкістю, безпекою та можливістю інтеграції з графічними форматами даних.

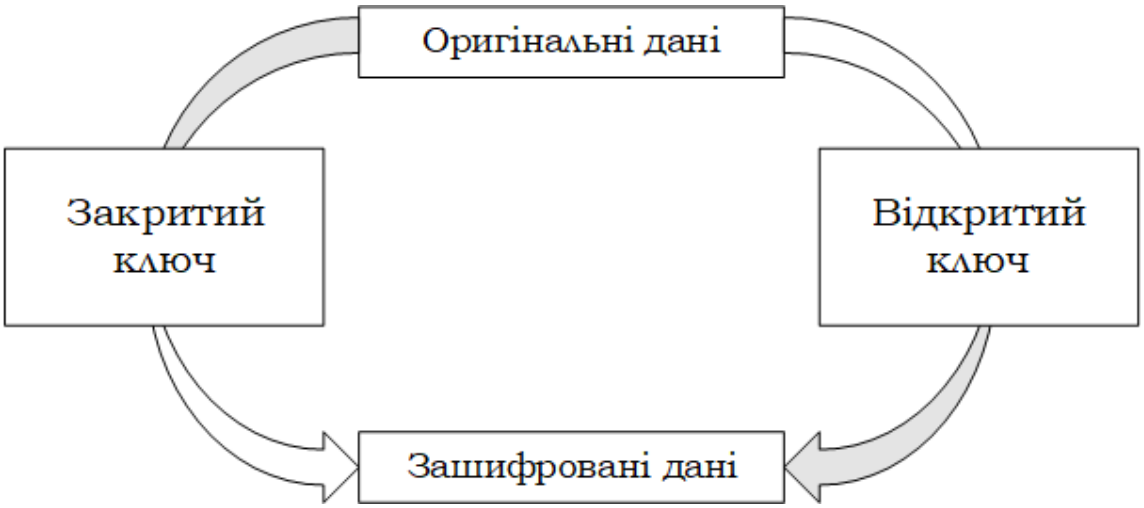

Рис.2. Асиметричне шифрування

Основи візуальної криптографії

Візуальна криптографія, запропонована Наором і Шаміром у 1994 році, є унікальним методом шифрування, де секретна інформація (наприклад, текст або зображення) розділяється на кілька візуальних частин або шарів (так званих «shares»). Окремо ці частини не містять зрозумілої інформації, однак при їх накладанні один на одного відновлюється оригінальне повідомлення (рис. 3).

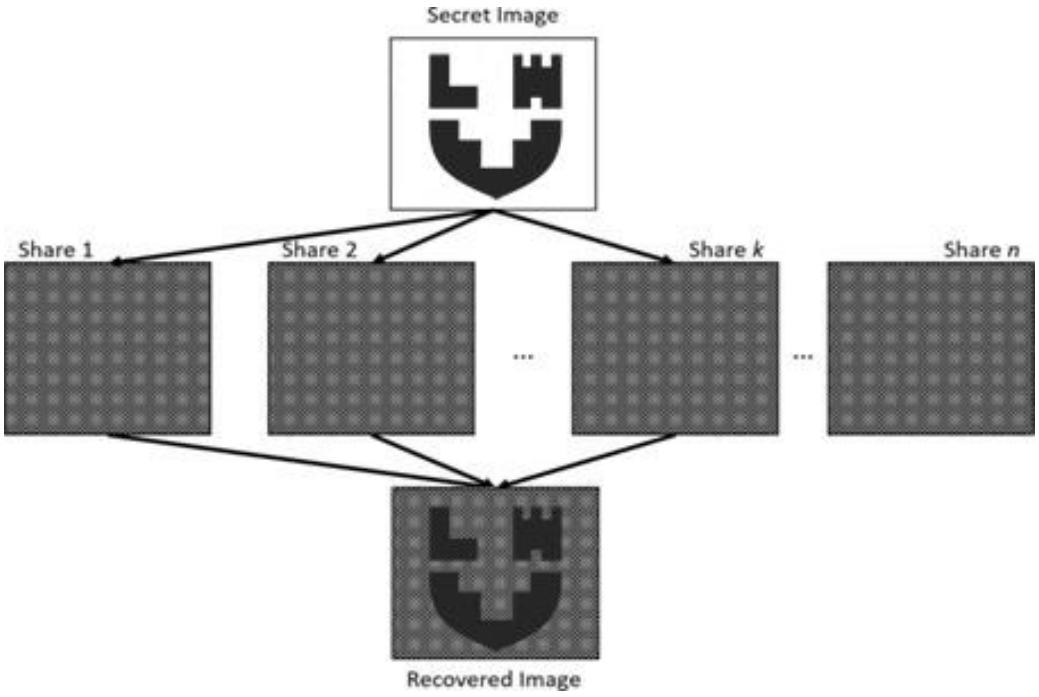

Рис. 3. Принцип роботи візуальної криптографії

Основна концепція методу полягає у використанні бінарного зображення (чорно-білих пікселів) для представлення секретної інформації. Кожен піксель секретного зображення ділиться на кілька підпікселів у двох або більше шарах. Ці шари виглядають як випадковий шум і не мають жодного сенсу окремо, проте при правильному накладанні вони утворюють оригінальне зображення. Це робить метод ефективним для захисту інформації, оскільки без усіх частин неможливо відновити вихідні дані.

Програмні засоби для реалізації візуальної криптографії

Окрім вибору мови програмування та відповідних бібліотек, важливим етапом було проектування архітектури самої програми. Основною метою було створення системи, яка б дозволила користувачам легко шифрувати і розшифровувати повідомлення, використовуючи принципи візуальної криптографії. Це вимагало розробки інтуїтивно зрозумілого алгоритму, який би забезпечував мінімальну взаємодію з користувачем для виконання складних математичних операцій шифрування.

Основною мовою програмування для реалізації алгоритмів візуальної криптографії було обрано Python через його універсальність, доступність та потужні бібліотеки для роботи з графічними зображеннями й інтерфейсами користувача. Python дозволяє швидко та ефективно реалізовувати складні алгоритми шифрування з мінімальними витратами часу на написання коду, що робить його ідеальним вибором для проектів, де важлива швидкість та легкість в розробці.

Однією з ключових бібліотек, що я використовувала для роботи із зображеннями, стала Pillow (Python Imaging Library). Ця бібліотека відкриває безліч можливостей, дозволяючи працювати з різними форматами графічних файлів, такими як JPEG, PNG та іншими. Pillow надає зручні інструменти для маніпулювання пікселями, зміни розміру зображень, а також збереження результатів у потрібному форматі. Вона стала ідеальним вибором для реалізації процесу шифрування, адже забезпечує необхідні функції для генерації та збереження візуальних частин зашифрованого зображення, що значно спрощує процес.

Для створення зручного та зрозумілого інтерфейсу користувача обрано бібліотеку Tkinter. Це стандартний інструмент для створення графічних інтерфейсів у Python, який дозволяє легко додавати інтерактивні елементи, такі як кнопки, поля для введення тексту, діалогові вікна для вибору файлів і кольорів. Використання Tkinter забезпечує простоту роботи з програмою для кінцевого користувача, що особливо важливо для проєктів, які орієнтовані на широку аудиторію. Завдяки цій бібліотеці, було створено інтерфейс, який не тільки функціональний, а й інтуїтивно зрозумілий, що підвищує загальну ефективність роботи з програмою.

Щоб реалізувати алгоритм, я використано можливості Python для роботи з числовими і логічними операціями. Наприклад, використання бібліотеки NumPy значно прискорило обробку даних, оскільки вона забезпечує високошвидкісні обчислення з масивами, що стало важливим для роботи з великими зображеннями. NumPy дозволила ефективно працювати з матрицями, представляючи пікселі як числові значення, що дало можливість швидко виконувати операції з їхнім розподілом між різними шарами.

Порівняння альтернативних методів

У процесі дослідження також розглядалися кілька інших підходів до шифрування інформації за допомогою зображень. Один із них — стеганографія, техніка приховування інформації в цифрових зображеннях. У цьому методі дані вбудовуються в малопомітні деталі зображення, наприклад, у найменш значущі біти пікселів. Хоча стеганографія дозволяє приховати повідомлення, її основним недоліком є те, що навіть незначні зміни у файлі зображення можуть вплинути на цілісність прихованої інформації.

На відміну від стеганографії, візуальна криптографія не залежить від збереження цілісності самого зображення. Цей метод використовує розподіл повідомлення на кілька окремих шарів (зображень), кожен з яких сам по собі не несе жодної інформації. Лише накладання цих шарів дає можливість розшифрувати повідомлення, що робить візуальну криптографію стійкою до модифікацій та змін.

Аналіз цих методів показав, що для задачі безпечної передачі повідомлень візуальна криптографія є оптимальним вибором завдяки своїй здатності захищати інформацію через поділ на кілька візуальних частин. Використання програмних засобів, таких як Python, Pillow та Tkinter, забезпечило ефективність розробки програмного забезпечення, оскільки ці інструменти надали всі необхідні ресурси для реалізації алгоритмів шифрування і створення зручного інтерфейсу користувача. Враховуючи специфіку завдання, було визначено, що візуальна криптографія є практичним та надійним рішенням для забезпечення конфіденційності переданої інформації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У ході дослідження було проаналізовано можливості візуальної криптографії для забезпечення безпеки комунікаційних процесів. Використання візуальної криптографії дозволяє передавати зашифровані повідомлення у вигляді зображень, які можуть бути розкриті лише за умови фізичного накладання частин, що забезпечує високий рівень конфіденційності даних. Такий підхід має переваги перед традиційними методами шифрування, оскільки не потребує додаткових обчислювальних ресурсів для декодування і є стійким до цифрових атак.

Розроблені програмні рішення показали ефективність у забезпеченні захисту даних, що особливо актуально для галузей, де конфіденційність має критичне значення, зокрема в державних та військових структурах. На основі проведених тестувань було виявлено можливі напрями для вдосконалення, зокрема розширення функціональних можливостей для підтримки різних типів зображень та алгоритмів покращення якості розшифрованого зображення.

Перспективи подальших досліджень полягають у розробці більш досконалих алгоритмів, які забезпечуватимуть точнішу візуалізацію та можливість адаптивного налаштування під різні умови шифрування. Окрім того, можливим є впровадження візуальної криптографії для захисту біометричних даних, що сприятиме підвищенню безпеки в системах ідентифікації та доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kafri, O., & Keren, E. (1987). Encryption of pictures and shapes by random grids. *Optics Letters, 12(6)*. https://doi.org/10.1364/ol.12.000377
2. Naor, M., & Shamir, A. (1995). Visual cryptography. *Advances in Cryptology – EUROCRYPT'94*, 1–12. https://doi.org/10.1007/bfb0053419
3. Shamir, A. (1979). How to share a secret. *Communications of the ACM, 22(11),* 612–613. https://doi.org/10.1145/359168.359176
4. Horng, G., Chen, T., & Tsai D.-S. (2006). Cheating in Visual Cryptography. *Designs, Codes and Cryptography, 38(2),* 219–236. https://doi.org/10.1007/s10623-005-6342-0
5. Gnanaguruparan, M., & Kak, S. (2002). Recursive hiding of secrets in visual cryptography. *Cryptologia, 26(1),* 68–76. https://doi.org/10.1080/0161-110291890768
6. Parakh, A., & Kak, S. (2010). A Tree Based Recursive Information Hiding Scheme. *ICC 2010 - 2010 IEEE International Conference on Communications.* https://doi.org/10.1109/icc.2010.5502430
7. Yang C.-N., Chen T.-S. (2005). Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. *Pattern Recognition Letters. 26(2),* 193–206. https://doi.org/10.1016/j.patrec.2004.08.025
8. Cryptography: Theory and practice. (1995). *Computers & Mathematics with Applications, 30(9)*. https://doi.org/10.1016/0898-1221(95)90225-2
9. Katoh, T., & Imai, H. (1998). An extended construction method for visual secret sharing schemes. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science), 81(7),* 55–63. https://doi.org/10.1002/(sici)1520-6440(199807)81:7%3C55::aid-ecjc7%3E3.0.co;2-#
10. Verheul, E. R., & van Tilborg, H. C. A. (1997). Constructions and Properties of k out of n Visual Secret Sharing Schemes. *Designs, Codes and Cryptography, 11(2),* 179–196. https://doi.org/10.1023/a:1008280705142
11. Hryniuk, S., & Polishchuk, M. (2020). Use information encryption technology for secure network transmission. *Computer-integrated technologies: education, science, production, 39,* 122–126. https://doi.org/10.36910/6775-2524-0560-2020-39-21
12. Polishchuk, M., Semenyuk, O., Polishchuk, L., & Lomakin, M. (2023). Possibilities of authorization and protection of user data during the development of cloud web applications for IoT. *Computer-integrated technologies: education, science, production, (52),* 94–103. https://doi.org/10.36910/6775-2524-0560-2023-52-12
13. Cherniashchuk, N., & Kostiuchko, S. (2022). Detection of attacks based on compromise marks. *12th International Conference on Dependable Systems, Services and Technologies (DESSERT).* https://doi.org/10.1109/dessert58054.2022.10018583

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Iryna Rymchuk
Master of Computer Engineering and Security Department
Lutsk National Technical University, Lutsk, Ukraine
rymchuk.i1209@lntu.edu.ua

Serhii Kostiuchko
Ph.D., Associate Professor of Computer Engineering and Security Department
Lutsk National Technical University, Lutsk, Ukraine
ORCID ID: 0000-0002-1262-6268
s.kostiuchko@gmail.com

Mykola Polishchuk
Ph.D., Associate Professor of Computer Engineering and Security Department
Lutsk National Technical University, Lutsk, Ukraine
ORCID ID: 0000-0002-1218-5925
polishchuk.kolia@gmail.com

Serhii Hryniuk
Ph.D., Associate Professor of Computer Engineering and Security Department
Lutsk National Technical University, Lutsk, Ukraine
ORCID ID: 0000-0002-0080-3167
sergij.grunjuk@gmail.com

Liudmyla Konkevych
Assistant of Computer Engineering and Security Department
Lutsk National Technical University, Lutsk, Ukraine
ORCID ID: 0000-0002-8279-3133
k.liudmilka@lutsk-ntu.com.ua

COMMUNICATION PROCESSES SECURITY USING VISUAL CRYPTOGRAPHY

Abstract. The article is devoted to the study of data encryption technologies with an emphasis on visual cryptography, which is a modern and promising method of ensuring information confidentiality. The main attention is paid to the analysis of information encryption existing methods and the solutions development that allow to ensure reliable communications protection. Visual cryptography, as one of the modern methods, is relevant due to the growing need for protecting confidential data in the face of increasing cybersecurity threats. The paper describes the basic principles of visual cryptography, its advantages and application practical possibilities in areas where information confidentiality is of crucial importance, such as state security, the military, financial institutions and healthcare systems. The visual cryptography advantages are described, which allows transmitting encrypted messages in the form of images that can be decrypted by physically superimposing parts. This expands the potential of the technology in the authentication context and access systems. In addition, the article contains a software tools description for implementing information encryption and decryption, as well as a detailed overview of the possibilities of using programming languages to solve such problems. Key encryption algorithms and methods are considered, assessing their effectiveness and implementation possibilities in real information protection systems. Thanks to the conducted research, various approaches to data protection were analyzed and the visual cryptography advantages compared to other methods were identified. The results of the study demonstrate the visual cryptography effectiveness as a information protection method, especially in cases where it is necessary to avoid dependence on complex digital technologies. Prospects for further research include the development of more advanced visual encryption algorithms, adaptive to different conditions of use, as well as the implementation of technology for protecting critical data in various industries.

Keywords: cryptography; V-Crypt; symmetric encryption; asymmetric encryption; steganography.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kafri, O., & Keren, E. (1987). Encryption of pictures and shapes by random grids. *Optics Letters, 12(6).* https://doi.org/10.1364/ol.12.000377
2. Naor, M., & Shamir, A. (1995). Visual cryptography. *Advances in Cryptology – EUROCRYPT'94*, 1–12. https://doi.org/10.1007/bfb0053419
3. Shamir, A. (1979). How to share a secret. *Communications of the ACM, 22(11),* 612–613. https://doi.org/10.1145/359168.359176
4. Horng, G., Chen, T., & Tsai D.-S. (2006). Cheating in Visual Cryptography. *Designs, Codes and Cryptography, 38(2),* 219–236. https://doi.org/10.1007/s10623-005-6342-0
5. Gnanaguruparan, M., & Kak, S. (2002). Recursive hiding of secrets in visual cryptography. *Cryptologia, 26(1),* 68–76. https://doi.org/10.1080/0161-110291890768
6. Parakh, A., & Kak, S. (2010). A Tree Based Recursive Information Hiding Scheme. *ICC 2010 - 2010 IEEE International Conference on Communications.* https://doi.org/10.1109/icc.2010.5502430
7. Yang C.-N., Chen T.-S. (2005). Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. *Pattern Recognition Letters. 26(2),* 193–206. https://doi.org/10.1016/j.patrec.2004.08.025
8. Cryptography: Theory and practice. (1995). *Computers & Mathematics with Applications, 30(9).* https://doi.org/10.1016/0898-1221(95)90225-2
9. Katoh, T., & Imai, H. (1998). An extended construction method for visual secret sharing schemes. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science), 81(7),* 55–63. https://doi.org/10.1002/(sici)1520-6440(199807)81:7%3C55::aid-ecjc7%3E3.0.co;2-#
10. Verheul, E. R., & van Tilborg, H. C. A. (1997). Constructions and Properties of k out of n Visual Secret Sharing Schemes. *Designs, Codes and Cryptography, 11(2),* 179–196. https://doi.org/10.1023/a:1008280705142
11. Hryniuk, S., & Polishchuk, M. (2020). Use information encryption technology for secure network transmission. *Computer-integrated technologies: education, science, production, 39,* 122–126. https://doi.org/10.36910/6775-2524-0560-2020-39-21
12. Polishchuk, M., Semenyuk, O., Polishchuk, L., & Lomakin, M. (2023). Possibilities of authorization and protection of user data during the development of cloud web applications for IoT. *Computer-integrated technologies: education, science, production, (52),* 94–103. https://doi.org/10.36910/6775-2524-0560-2023-52-12
13. Cherniashchuk, N., & Kostiuchko, S. (2022). Detection of attacks based on compromise marks. *12th International Conference on Dependable Systems, Services and Technologies (DESSERT).* https://doi.org/10.1109/dessert58054.2022.10018583