Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності

На правах рукопису

Борзов Юрій Олексійович

УДК 004.832.3:519.711.2

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПІДВИЩЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ КРИТИЧНОГО ЗАСТОСУВАННЯ

05.13.06 – інформаційні технології

Дисертація на здобуття наукового ступеня
кандидата технічних наук

Науковий керівник
Рак Тарас Євгенович
доктор технічних наук, доцент

Львів – 2015

ЗМІСТ

ВСТУП

Актуальність роботи. Технологічний розвиток суспільства призвів до постійно зростаючого впровадження інформаційних технологій у найрізноманітніші області людської діяльності. У результаті новий поштовх отримала автоматизація управління функціонуванням та бізнес-діяльністю суб'єктів господарювання на основі впровадження інформаційних та інформаційно-управляючих систем. Одним із актуальних напрямів впровадження технологій таких систем є автоматизація діяльності об'єктів підвищеної небезпеки та потенційно небезпечних об'єктів, які, зазвичай, функціонують в online режимах чи режимах реального часу. Системи такої автоматизації отримали назву інформаційних або інформаційно-управляючих систем критичного застосування і до них, типово, відносять автоматизовані системи раннього виявлення надзвичайних ситуацій та оповіщення (АСРВО), медичні системи, системи SmartHouse, системи управління складними та небезпечними виробництвами і об'єктами, аварії на яких можуть привести до масштабних надзвичайних ситуацій тощо.

Визначальною характеристикою цих систем є те, що їх функціонування має значний вплив на ефективність забезпечення життєдіяльності людей. Це зумовлено тим, що процеси прийняття рішень щодо управління системами критичного застосування (локалізації, ліквідації надзвичайних ситуацій і ін.) включають передачу комунікаційними системами та аналіз персоналом або автоматизованими системами відеоінформації, спотворення якої може призвести до помилкових рішень.

До якісних атрибутів окремих видів систем критичного застосування, а це в першу чергу стосується систем управління безпекою соціальних об'єктів та систем управління безпекою, відносять функціональну безпеку, яка визначає у

широкому розумінні функціонування системи у відповідності до визначених наперед вимог. Під безпекою систем розуміють таке їх функціонування, при якому відсутні небезпечні відмови та недопустимі втрати. Причинами відмов можуть бути дефекти програм, даних, апаратури, впливи зовнішнього середовища.

Для забезпечення необхідного рівня функціональної безпеки при вирішення проблем передачі інформації в реальних системах критичного застосування необхідне комплексне використання різних методів. До таких методів можна віднести: завадостійке кодування, стиснення відеоінформації, криптографічне перетворення тощо. Завадостійке кодування виконується з метою захисту від випадкових завад та допомагає ефективно використовувати комунікаційні канали для надійної передачі інформації. Стиснення використовується для зменшення обсягу переданої інформації. Під стисненням розуміють кодування даних з метою представлення інформації в більш компактному вигляді.

Основною архітектурною особливістю окремих видів систем критичного застосування є їх розподіленість, а відтак існування комунікаційних каналів. При цьому важливою складовою інформаційних пакетів в комунікаційних сеансах дуже часто використовуються цифрові зображення різних типів. Відповідно, гарантування стійкого, надійного і захищеного передавання зображень комунікаційними каналами є елементом забезпечення безпеки обробки інформації в інформаційно-управляючих системах критичного застосування мережевої архітектури. У результаті підвищується рівень загальної функціональної безпеки та забезпечується живучість і збільшується ефективність функціонування інформаційно-управляючих систем критичного застосування.

Підвищенням рівня функціональної безпеки в системах, заснованих на комунікаційних сеансах, є використання інформаційних технологій на основі криптографічного кодування. Такі засоби вважаються найбільш ефективними на сьогодні.

Тобто основними категоріями забезпечення функціональної безпеки СППР (система підтримки прийняття рішень) на підставі відео зображень виступають стійкість, надійність та безпечність процесів технічної обробки та управління інформацією, що циркулює в автоматизованій системі. Стійкість та надійність забезпечуються методами стійкого та надійного кодування. А безпека – різноманітними криптографічними перетвореннями тощо.

Проблеми розробки інформаційних технологій підвищення надійності та безпеки даних, зокрема в комунікаційних сеансах, відображено в працях К. Шеннона, М. Діффі, М. Хеллмана, В. К. Задіраки, І. Д. Горбенка, В. Я. Чечельницького, М. П. Карпінського, Ю.М. Коростіля, О.А.Курченка. Серед існуючої великої кількості криптографічних перетворень особливе місце займає асиметрична система криптографічного кодування RSA. При великих значеннях ключів кодування та декодування ця криптосистема визначає високий рівень безпеки, що призвело до того, що алгоритм практичної реалізації криптосистеми став промисловим стандартом і визначає напрями розвитку інформаційних технологій забезпечення функціональної безпеки.

У випадку використання криптографічного кодування на основі стандарту RSA для цифрових зображень виникає проблема, яка полягає у тому, що на закодованому зображенні можуть зберігатись контури (флуктуації функції інтенсивності). У цьому випадку атака на об’єкт захисту може полягати не у зламі самого алгоритму, а у використанні методів цифрової обробки зображень (фільтрації, реконструкції) для отримання основної інформативності цього зображення.

Отримані на сьогодні результати теоретичних та практичних досліджень надають можливість уникнути появи контурів на закодованих зображеннях при достатньо малих значеннях ключів. Проте, вони характеризується або високою обчислювальною складністю, або значними інформаційними втратами, які

виникають в процесах забезпечення функціональної безпеки. Їх практичне використання є витратним з точки зору мінімізації ресурсів для забезпечення високого рівня функціональної безпеки.

Тому актуальною науковою задачею є розробка інформаційної технології підвищення функціональної безпеки інформаційно-управляючих систем критичного застосування, яка базується на комунікаційних процедурах із застосуванням універсальних засобів з метою мінімізації обчислювальних ресурсів в процесах забезпечення надійності, стійкості та безпеки функціонування цих систем.

Зв’язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи, її мета і основні завдання відповідають державній програмі забезпечення пожежної безпеки в Україні на 2012-2015 рр., державним науково-технічним програмам, сформульованим в Законі України "Про науково-технічну діяльність" та в Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки". Робота виконувалася у рамках науково-дослідних робіт “Створення навчального макету автоматизованої системи оперативно-диспетчерського управління для підготовки та перепідготовки диспетчерів та керівного складу ОДС” (0114U004183), “Розроблення методичних рекомендацій з організації служби оперативного зв’язку, телекомунікаційних систем та інформаційних технологій в системі ДСНС України” (0114U004185), “Розробка методів і моделей захисту інформаційно-комунікаційних систем і мереж у структурних підрозділах ДСНС України” (0114U004275).

Мета і задачі дослідження. Метою дисертаційної роботи є розроблення інформаційних технологій для забезпечення необхідного рівня функціональної безпеки інформаційно-управляючих систем критичного застосування та зменшенні витрат при передаванні зображень в комунікаційних сеансах.

Для досягнення мети в роботі необхідно розв'язати такі часткові задачі:

1) провести аналіз ефективності методів та засобів забезпечення функціональної безпеки при передаванні зображень комунікаційними каналами інформаційно-управляючих систем критичного застосування;

2) розробити метод забезпечення функціональної безпеки систем критичного застосування для випадку використання повноколірних зображень завдяки сумісному використанню криптосистем Ель-Гамаля і RSA;

3) удосконалити метод забезпечення необхідного рівня функціональної безпеки систем критичного застосування у випадку циркуляції в телекомунікаційних сеансах напівтонових зображень із глибиною кольору в 1-2 байти, який ґрунтується на інтегральному поєднанні елементів алгоритму криптографічного кодування RSA та операції зашумлення;

4) розробити метод забезпечення функціональної безпеки, який базується на використанні бінарних операцій в інтегральному поєднанні із елементами алгоритму RSA для побудови стійких алгоритмів забезпечення функціональної безпеки інформаційно-управляючих систем критичного застосування;

5) розробити інформаційну технологію підвищення функціональної безпеки для мережевих інформаційно-управляючих систем критичного застосування та програмно її реалізувати для забезпечення різних складових функціональної безпеки;

6) провести аналіз ефективності використання розроблених методів та інформаційної технології забезпечення функціональної безпеки у інформаційно-управляючих системах з комунікаційними каналами.

Об'єктом дослідження є процес обробки інформації для забезпечення функціональної безпеки в системах підтримки прийняття рішень в комунікайних сеансах інформаційно-управляючих систем критичного застосування на підставі цифрових зображень.

Предметом дослідження є методи, засоби та інформаційні технології

підвищення функціональної безпеки комунікаційних сеансів при передаванні зображень.

Методи дослідження. Результати дисертаційних досліджень отримані з використанням елементів інформаційних технологій, теорії інформаційних систем, цифрової обробки зображень, теорії безпеки інформації, теорії чисел, лінійної та булевої алгебр, дискретної математики, топології, математичного аналізу та комп'ютерного моделювання.

Наукова новизна одержаних результатів. На основі виконаних теоретичних та експериментальних досліджень отримано такі результати:

вперше розроблено:

- метод забезпечення необхідного рівня функціональної безпеки систем критичного застосування, який ґрунтується на сумісному використанні систем криптографічного кодування Ель-Гамаля і RSA, що дає можливість підвищити стійкість функціонування інформаційних систем при передаванні в комунікаційних процедурах цифрових зображень із глибиною кольору у 4 байти із зменшенням витрат;

отримав подальший розвиток:

- метод забезпечення необхідного рівня функціональної безпеки систем критичного застосування у випадку циркуляції в телекомунікаційних сеансах напівтонових зображень із глибиною кольору в 1-2 байти, який ґрунтується на інтегральному поєднанні елементів алгоритму криптографічного кодування RSA та операції зашумлення, що дало можливість збільшити рівень безпеки систем без інформаційних втрат;

- метод забезпечення функціональної безпеки на основі алгоритму RSA, який завдяки використанню бінарних операторів забезпечує необхідне значення стійкості та унеможливлює несанкціоноване відтворення методами цифрової оброки сигналів повноколірних зображень із глибиною кольору у 3-4 байти в

комунікаційних процесах систем критичного застосування;

удосконалено:

- інформаційну технологію забезпечення необхідного рівня функціональної безпеки для випадку передавання комунікаційними каналами напівтонових зображень із глибиною кольору в 1-2 байти, яка базується на використанні модифікованого методу RSA та порозрядних операцій, що дає можливість усунути контури на зображеннях та зменшує витрати обчислювальних ресурсів в програмній реалізації процедур забезпечення функціональної безпеки.

Практичне значення одержаних результатів. Отримані результати досліджень є основою розробленої програмної бібліотеки, яка призначена для забезпечення функціональної безпеки при передаванні зображень у комп'ютерних мережах на основі протоколів TCP, UDP та Http.

Усі розроблені методи, на відміну від існуючих підходів, характеризуються достатньою стійкістю і надійністю у порівнянні із криптографічним кодуванням RSA і дають змогу створювати інформаційні технології, які не вимагають для свого функціонування значних обчислювальних ресурсів.

Усунення контурів в розроблених методах здійснюється при малих значеннях ключів процедур криптографічного кодування, що гарантує невихід за межі розрядної сітки в обчислювальному процесі.

Підвищення функціональної безпеки у випадку передавання комунікаційними каналами напівтонових зображень із глибиною кольору в 1-2 байти забезпечується удосконаленою інформаційною технологією з високим значенням стійкості, яке рівна: $4 \cdot 16^4 \cdot (\varphi(\psi(n)) - 1) \cdot \Omega(n)$ (тут φ – функція Ейлера, а ψ– найменше спільне кратне чисел (P– 1) і (Q– 1), які, у свою чергу, визначають відкриту і закриту частину ключа, та число $n = PQ$, $\Omega(n)$ – стійкість криптографічного кодування).

Сумісне використання елементів криптографічних кодувань RSA та Ель-

Гамаля дозволило отримати метод забезпечення функціональної безпеки, який володіє стійкістю у $(P-3)^2$ разів більшою у порівнянні із базовим аглоритмом.

Програмно побудовано динамічну бібліотеку, яка реалізовує технологію захисту зображень. Особливістю цієї бібліотеки є можливість її використання як для персоніфікованої інформаційної безпеки, так і для забезпечення інформаційної безпеки у комунікаційних сеансах автоматизованих систем.

Результати дисертаційних досліджень використовувались в Головному управлінні ДСНС у Львівській області при розробці та впровадженні системи оперативно-диспетчерського управління (СОДУ) та Системи 112 (акт про використання результатів досліджень від 24 червня 2014 року).

Результати роботи використовуються у навчальному процесі Львівського державного університету безпеки життєдіяльності на кафедрі управління інформаційною безпекою при викладанні дисципліни «Безпека інформації в інформаційно-комунікаційних системах» тема «Протоколи передавання та захисту інформації, захист комп'ютерних мереж» (акт про використання результатів досліджень від 11 лютого 2015 року).

Особистий внесок здобувача. Основні положення та результати дисертаційної роботи автор отримав самостійно. У друкованих працях, опублікованих у співтоваристві, авторові належать: схема використання порозрядних операцій в модифікаціях алгоритму RSA за одним та двома рядками [12, 50, 53], метод використання бінарних операцій при криптографічному кодуванні кольорових зображень [54], реалізація оператора зашумлення в кодуванні напівтонових [73, 76, 92] та кольорових зображень [51], сумісне використання побітових операцій та оператора зашумлення при захисті кольорових зображень [52, 142], алгоритм сумісного використання криптосистем RSA та Ель-Гамаля при криптографічному кодуванні за одним та двома рядками [55, 118].

Апробація результатів дисертації. Результати дисертаційної роботи

доповідалися на таких науково-технічних конференціях:

- The VIth International Scientific and Technical Conference [“Computer Science and Information Technologies” (CSIT 2011)], (Lviv, November 16-19, 2011).
- Міжнародна наукова конференція [«Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту»], (Херсон, 16-20 травня 2011).
- Міжнародна наукова конференція [«Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту»], (Херсон, 27-31 травня 2012).

Публікації. Матеріали дисертації опубліковано в 12 наукових працях, з них: 8 – у фахових виданнях України з технічних наук (з них 6 входять до міжнародних наукометричних баз), 1 – у закордонному виданні, яке індексується міжнародними наукометричними базами та 3 – у матеріалах міжнародних науково-технічних конференцій.

Структура і обсяг роботи. Дисертація складається зі вступу, 4 розділів, висновків та додатків. Загальний обсяг роботи – 141 сторінок, з них основний текст – 107 сторінок. Робота містить 54 рисунків на 37 сторінках та 2 додатки на 17 сторінках. Список використаних літературних джерел складається із 144 найменувань і викладений на 17 сторінках.

РОЗДІЛ 1. АНАЛІЗ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

1.1. Класифікація автоматизованих систем критичного застосування

Сучасні автоматизовані системи критичного застосування визначаються критичними умовами функціонування і необхідності забезпечення функціональної безпеки комп'ютерними системами, на основі яких вони будуються. Визначальним для таких систем є обов'язкова підтримка двох режимів роботи – нормального і аварійного.

За [25] сучасна класифікація автоматизованих систем критичного застосування має вигляд наведений на рис.1.1. Вона включає в себе інформаційно-управляючі системи з дуже широкого спектру прикладного застовування

Системи критичного застосування, зазвичай, це системи реального часу. Але на відміну від звичайних інформаційних систем реального часу до них висуваються посилені вимоги високої надійності і живучості. Одним із факторів, які забезпечують високі показники цих характеристик є функціональна безпека. А тому основною вимогою до практично усіх систем критичного застосування є забезпечення функціональної безпеки (safety), яка за [45] визначає функціонування системи відповідно до існуючих (визначених наперед) вимог.

Основною складовою функціональної безпеки є інформаційна безпека, яка [45] визначає захищеність систем обробки і зберігання даних для забезпечення конфіденційності, доступності і цілісності інформації. За визначенням згідно державним стандарту [64], інформаційна безпека визначає заходи, спрямовані на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення. Отже, інформаційна безпека, а відтак, функціональна безпека

визначають захист від несанкціонованого доступу до даних і забезпечення надійності і стійкості до навмисних впливів. Усе це має безпосереднє відношення на ефективність функціонування інформаційних систем вцілому.

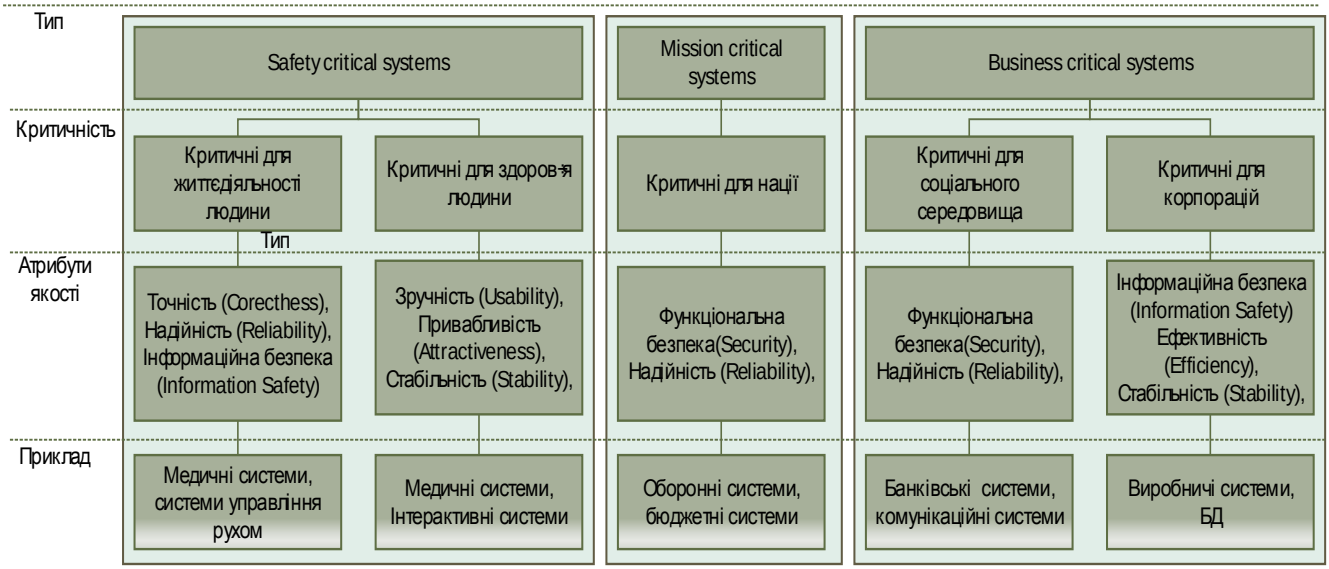


Рисунок 1.1 – Класифікація автоматизованих систем критичного застосування

У випадку систем критичного застосування проблеми забезпечення функціональної безпеки поглиблюються використання комп'ютерних мереж (завичай зовнішніми каналами) для організації комунікаційних сеансів. У відповідності до цього спектр завдань забезпечення безпеки доповнюється завданнями забезпечення максимально стійких до зовнішніх (атак) впливів комунікапційних процедур.

1.2. Характеристика проблеми забезпечення функціональної безпеки в автоматизованих системах критичного застосування

1.2.1. Проблема забезпечення функціональної безпеки

Задача забезпечення функціональної безпеки функціонування сучасних систем критичного застосування (тобто систем для управління критичною

інфраструктурою) є достатньо складною і розглядалась у багатьох дослідженнях. Підсумовуючи їх аналіз можна констатувати, що для організації ефективної функціональної безпеки автоматизованих систем критичного застосування в загальному випадку необхідне вирішення завдань, які можна об'єднати у 4 групи: нормативна, організаційна, технологічна та психологічна.

У дисертаційному дослідженні розглядались завдання лише технологічного характеру, оскільки вони безпесередньо пов'язані із надійністю функціонування програмно-апаратного забезпечення інформаційних систем. При цьому треба пам'ятати, що покращення розв'язання завдань навіть однієї групи може призвести до підвищення ефективності забезпечення функціональної безпеки вцілому.

Сучасний розвиток інформаційних технологій (в контексті програмно-апаратного забезпечення) і в першу чергу комунікаційних технологій (що є важливою складовою сучасних систем критичного застосування) створив надзвичайного сприятливі умови для роботи в середовищі цих систем у віддаленому режимі. При цьому вирішуються найрізноманітніші функціональні завдання: від управління виробничими процесами до адміністрування роботою самих систем. Це, у першу чергу, піднімає рівень ефективності функціонування систем і, по-друге, призводить, в окремих випадках, до значної економії різноманітних ресурсів (у першу чергу фінансових).

Проте породження сучасними інформаційними технологіями нових можливостей у функціонуванні систем критичного застосування призвели до появи нових загроз в області безпеки функціонування цих систем [25]. Аналіз описаних у літературі зловмисних впливів на функціонування систем критичного застосування дозволяє за характером і наслідками виділити їх ту три групи [25]:

• атака на конфіденційність - несанкціонований доступ або перехоплення інформації (втрата конфіденційності);

• несанкціонована зміна інформації, програмного забезпечення, обладнання і т.д. (втрата цілісності);

• блокування транзакцій та/або відключення системи (втрата готовності).

Архітектура сучасних систем критичного застосування має безпосередній вплив на характер атак на ці системи. Аналіз типових архітектур дозволяє стверджувати, що найбільш вразливим елементами систем критичного застосування є:

• сервери системи, які підтримують зовнішні комунікаційні канали (у першу чергу інтернет канали);

• робочі станції системи, які задіяні у комунікаційних сеансах і використовують типові користувацькі операційні середовища;

• спеціалізовані пристрої (автоматизовані чи керовані), які є елементами систем критичного застосування і функціонують у середовищі ком'ютерних мереж на основі загальновідомих протоколів;

• будь-які програмні апаратні елементи, які можуть бути використані у виді мостів для організації доступу у мережі для сторонніх пристроїв через відкриті інтерфейси (наприклад через відкритий порт USB).

Використання вказаних елементів визначє фізичний спосіб проникнення в систему. Проте цього недостатньо для фахової організації атаки. Відомі рзультати різномантіних досліджень в області функціональної безпеки констатують, що високий рівень атаки забезпечується поетапним виконанням таких дій [43, 45]: визначенням цілей, розвідкою, забезпеченням доступу до системи, безпосередньо реалізацією атаки, знищенням доказів про втручання.

Шляхів (методів і засобів) реалізації атаки існує велика кількість. Завдання, які розв'язувались в дисертаційній роботі, стосуються унеможливлення проведення атаки у випадку, коли інформаційним об'єктом в системі критичного застосування виступають цифрові зображення.

1.2.2. Загальний аналіз методів забезпечення функціональної безпеки

Для забезпечення необхідного рівня функціональної безпеки при вирішення проблем передачі інформації в реальних системах критичного застосування необхідне комплексне використання різних методів. До таких методів можна віднести: завадостійке кодування, стиснення відеоінформації, криптографічне перетворення тощо. Завадостійке кодування виконується з метою захисту від випадкових завад та допомагає ефективно використовувати комунікаційні канали для надійної передачі інформації. Стиснення використовується для зменшення обсягу переданої інформації. Під стисненням розуміють кодування даних з метою представлення інформації в більш компактному вигляді. На практиці дані методи, як правило, використовуються сумісно для надійного захисту інформації, яка передається в комунікаційних сеансах.

Ефективність систем критичного застосування з точки зору забезпечення функціональної безпеки необхідно оцінювати за допомогою комплексного показника – завадо захищеності. Завадозахищеність за [13] включає в себе поняття завадостійкості і прихованості.

Функція захисту інформації від помилок, які можуть виникати при передачі інформації комунікаційними каналами, здійснюється за допомогою завадостійкого кодування, що забезпечує можливість автоматичного формування допустимих кодових комбінацій (кодових слів). При порушенні кодової комбінації система здатна фіксувати і виправляти помилки, які виникають при передаванні інформації. Всі завадостійкі коди можна розділити на два основних класи: блокові і неперервні (рекурентні або ланцюгові). Як блокові, так і неперервні коди в залежності від методів внесення надмірності розділяються на роздільні і нероздільні. Більшість відомих роздільних кодів складають систематичні коди. У цих кодів перевіряючі символи визначаються в результаті проведення лінійних операцій над певними інформаційними символами.

Прихованість за [47] є показником, який характеризує здатність забезпечувати безпеку інформації при передаванні її комунікаційними каналами від несанкціонованого доступу чи спотворення.

Одним із найбільш поширених на сьогодні способів захисту від несанкціонованого доступу до інформації у системах критичного застосувння є використання криптоситем. А в окремих випадках використання криптосистем може бути бути обов'язковим і регламентуватись законодавчо, як наприклад в [34, 41].

Класифікація сучасних криптографічних систем передбачає існування трьох видів систем: симетричні, асиметричні та змішані. Симетричний вид кодування – це кодування, засноване на ідеї єдиного секретного ключа і поділяється, у свою чергу, на такі класи: потокові, блочні і змішані [35, 38, 36, 40, 43, 58]. Основною проблемою симетричних методів кодування є безпечний розподіл ключів між суб'єктами комунікаційної взаємодії. Асиметричний вид кодування базується на ідеї відкритого ключа. Він є більш ресурсовибагливим, але нівелює проблему безпечного розподілу ключів [15, 19, 49, 58].

Сучасні автоматизовані системи, особливо ті, що використовують комунікаційні сеанси, як правило, для забезпечення конфіденційності обміну інформації базуються на змішаному виді захисту [59, 62, 67, 65, 71].

Суть цього змішаного виду полягає в послідовному використанні, зазвичай, асиметричного, а потім симетричного алгоритму кодування. Наприклад, на початку комунікаційного сеансу секретні ключі симетричного алгоритму кодування передаються мережевими каналами у закодованому асиметричним алгоритмом виді. Такий підхід ускладнює процедуру кодування, але підвищує її стійкість вцілому.

Стисла характеристика симетричних криптосистем. Як вже відзначалось, симетричні криптосистеми визначаються використанням єдиного (секретного) ключа як для процедур кодування так і для процедур декодування (рис.1.2 [27]).

Найбільш відомими симетричними криптографічними алгоритмами є DES, AES, ГОСТ 28147-89 і ін. [42, 70, 71].

Типовий підхід у побудові симетричних методів кодування полягає у перестановках та порозрядних операціях у інформаційних блоках, які маються фіксовану довжину. У відповідності до цього стійкість до взлому симетричного алгоритму кодування визначається так: відкриті дані вважають захищеними, якщо парою секретний ключ і закриті дані неможливо отримати інформацію про відкриті дані.

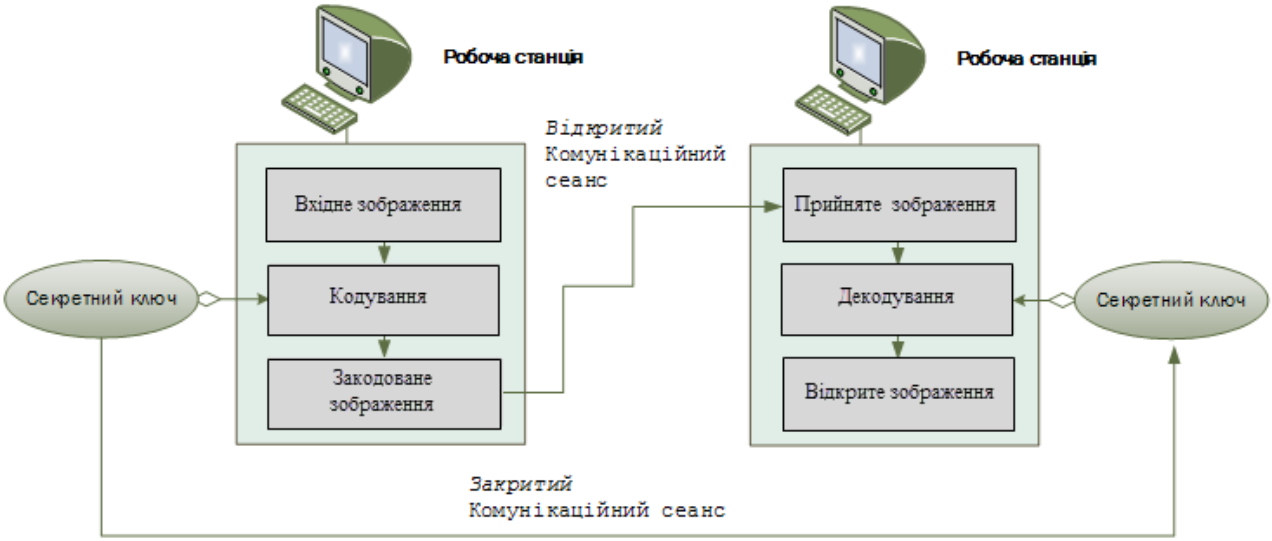


Рисунок 1.2 – Схема захищеної комунікації з використанням симетричних криптосистем

Оскільки математично доведено, що за умови меншого за розмір даних розміра секретного ключа, неможливо побудувати абсолютно стійкий симетричний алгоритм, то переваги сучасних найбільш використовуваних методів визначаються значенням обчислювальних ресурсів, які необхідні для атаки на закодоване повідомлення (зображення в контексті дисертаційної роботи).

Стисла характеристика асиметричних криптосистем

Новим напрямком у криптографії став винахід асиметричних криптосистем з відкритим ключем (рис. 1.3), таких, як RSA, DSA або Ель-Гамаль [2, 15, 31].

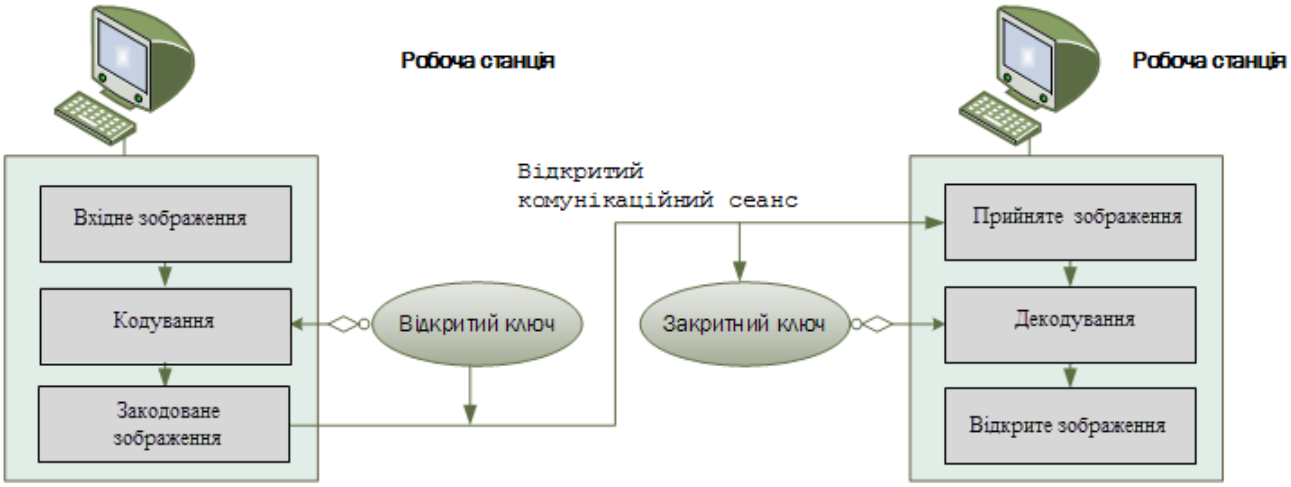


Рисунок 1.3 – Схема захищеної комунікації з використанням асиметричних криптосистем

Суть методу кодування в тому, що обчислення функції від закодованого повідомлення в прямому напрямку проходить з використанням відкритого ключа приймаючого абонента, а при розкодуванні (обчисленні зворотної функції) застосовується його секретний ключ. Як і слід було очікувати, математичних задач, що задовольняють перерахованим вимогам, відомо небагато, і лише на деяких з них були побудовані використовувані на практиці коди.

1.3. Методи криптографічного кодування для забезпечення функціональної безпеки системи критичного застовування для випадку цифрових зображень

1.3.1. Симетричні методи криптографічного кодування

Загальні принципи роботи симетричних методів забезпечення функціональної безпеки наведені у попередньому параграфі. До найбільш відомих на сьогодні

симетричних схем відносять такі традиційні алгорими як Lucifer, IDEAAES, Rijndael, ГОСТ 28147-89 і ін. [37] Проте використання цих методів в системах критичного застосування, зокрема для випадку зображень, не зовсім є виправданим, оскільки вони не забезпечують достатнього рівня стійкості і зашумленості зображень. Це призвело до появи новітніх симетричних схем, особливо це стосується випадку зображень. Фактично можна констатувати появу цілого напряму, а саме методів симетричного захисту цифрових зображень.

Серед усіх новітніх методів найбільшим рівнем стійкості характеризуються системи, які базуються на використанні хаотичних систем чи хаотичних полів [98, 100, 105, 108, 143,]. Популярність такого базису для організації функціональної безпеки пояснюється чутливістю криптосистем на основі хаотичних систем до вхідних значень та параметрів самої системи. Алгоритми забезпечення функціональної безпеки на основі хаотичних систем зазвичай є двоетапними: етап зашумлення та етап заміни [103, 140].

Треба відзначити, що найпростішим зашумленням може бути звичайна компресія [96, 109] чи дія фрактальною функцією [106]. Проте в сучасних методах в основі процедури зашумлення лежить використання хаотичних послідовностей [130], матриць трансформації [108] (дуже часто матриць Арнольда) і ін. для зашумлення шляхом зміни позиції піксела із значенням функції інтенсивності. Такий підхід є швидкий в реалізації, але при цьому не змінюється саме значення функції інтесивності, а тому гістограма закодованого зображення є рівною гістограмі вхідного зображення. Усунення цього недоліку відбувається на етапі заміни, на якому використовують дію на значення пікселів хаотичних послідовностей. Тепер виникає нова проблема, яка полягає у тому, що хаотична послідовність генерується однією хаотичною картою [136]. Відповідно до цього використання лише однієї хаотичної карти призводить до вузького діапазону ключів, а тому понижує стійкість.

Першим розвитком методів, базованих на використанні хаотичних послідовностей, стало привнесення у процедури кодування елементів дисперсійного аналізу [112, 122, 123, 127, 128]. Це призвело до зростання рівня зашумленості, однак діапазон ключів кодування залишився вузьким.

Другим розвитком методів, базованих на використанні хаотичних послідовностей, стало використання багатовимірних хаотичних карт [117, 120, 121, 129] (наприклад стандартні хаотичні карти, хаотичні нейронні мережі, просторово-часові хаотичні системи [126]). Такий підхід підвищив рівень стійкості, проте збільшив також обчислювальні витрати.

Третім розвитком методів, базованих на використанні хаотичних послідовностей, стало використання наборів хаотичних карт [113, 137, 138, 139, 141]. Це дозволило розширити діапазон ключів кодування, підвищити чутливість до зміни ключів. Проте відомими є атаки нетрадиційними методами на такі алгоритми.

1.3.2. Асиметричні методи криптографічного кодування

Найпершим асиметричним методом криптографічного кодуванн для організації функціональної безпеки є алгоритм Діффі-Хеллмана [33]. В основі алгоритму лежить використання функції дискретного піднесення до степеня. В результаті вдалось досягти криптографічної стійкості, яка базується на прогнозованій складності задачі дискретного логарифмування. Проте на сьогодні отримано математичні методики взлому алгоритму Діффі-Хеллмана.

Достатньо популярним способом забезпечення інформаційної безпеки є використання алгоритму McEliece [62]. В основі цієї системи є елементи теорії алгебраїчного кодування і процедура рандомізації в процедурах кодування. Стійкість алгоритму McEliece визначається складністю задачі декодування повних лінійних кодів. Проте на сьогодні, подібно до алгоритму Діффі-Хеллмана,

існує достаня кількість методів успішної атаки на алгоритм McEliece.

Ще одним із достатньо відомих сучасних асиметричних методів забезпечення функціональної безпеки є алгоритм Ель-Гамаля [37]. Його криптостійкість визначається обчислювальною складністю задачі логарифмування цілих чисел на скінченних полях. Проблема алгоритму схеми Ель-Гамаля полягає у відсутності семантичної стійкості. Тому цей алгоритм дуже часто використовується у сумісних з іншими методами (зазвичай симетричними) забезпечення функціональної безпеки.

Наступним достатньо відомим асиметричним підходом до забезпечення безпеки є так звані еліптичні криптосистеми [10, 62, 94]. Вони базуються на використанні еліптичних кривих [68] над скінченними полями [3]. Стійкість еліптичної криптосистеми визначається складністю субекспоненціальних алгоритмів в задачах дискретного логарифмування в групах точок еліптичних кривих [3].

Найбільш відомим асиметричним методом забезпечення функціональної безпеки є алгоритм Ривеста-Шаміра-Адельмана, відомий як алгоритм RSA [83, 84]. В основі алгоритму RSA лежить використання функції Ейлера [14], хоча це і не обов’язково (достатньо часто використовуються інші функції, наприклад функція Кармайля). Стійкість алгоритму RSA, заснована на труднощі вирішення проблеми факторизації, базується на складності задачі розкладу чисел на прості множники [6-8, 16, 17] і детально описана у наступному параграфі. Висока стійкість алгоритму сприяла його популяризації, що привело до появи різноманітних промислових стандартів. Проте, як будь-який алгоритм, він має свої переваги і недоліки. Їх детальний аналіз наведено нижче.

1.4. Використання криптографічного кодування RSA для організації функціональної безпеки в автоматизованих системах критичного застосування

1.4.1.Загальна схема алгоритму RSA

За [125] RSA - криптографічний алгоритм з відкритим ключем, що грунтується на обчислювальній складності задачі факторизації великих простих чисел [19, 20]. В даному дослідженні алгоритм RSA розглядається на основі функції Ейлера.

Алгоритм RSA відноситься до несиметричних систем, або систем з відкритим ключем, тобто таких систем, у яких для кодування використовується відкритий ключ [59, 72], а для розкодовування – закритий (секретний). У криптографічній системі RSA кожен ключ складається з пари цілих чисел.

Використання криптосистеми RSA передбачає виконання двох процедур: генерації ключів та кодування/розкодовування.

Алгоритм генерації ключів складається із таких кроків [9, 60, 125]:

1. випадковим чином вибираються два простих числа p і q [39, 44];
2. визначається їх добуток (модуль): $n = p \cdot q$;
3. визначається значення функції Ейлера: $\varphi(n) = (p - 1)(q - 1)$ [104];
4. вибирається таке ціле число e (відкрита експонента), щоб виконувались умови:
   - $1 < e < \varphi(n)$;
   - e взаємно просте з $\varphi(n)$;
5. вибирається число d (секретна експонента), яке обернено мультиплікативне до числа e: $d \cdot e \equiv 1 \pmod{\varphi(n)}$;
6. утворюється пара (e, n), яка називається відкритим ключем;
7. утворюється пара (d, n), яка називається закритим ключем.

Процедура кодування повідомлення m реалізовується за допомогою відкритого ключа (e, n) за формулою

$$c = m^e \pmod{n}, \tag{1.1}$$

де c – закодоване повідомлення.

Процедура розкодування за допомогою закритого ключа (d, n) реалізовується за формулою

$$m = c^d \pmod{n}, \tag{1.2}$$

де m – декодоване повідомлення.

1.4.2. Проблема стійкості криптографічного кодування на основі алгоритму RSA

Алгоритм RSA відноситься до так званих несиметричних схем кодування експонентної часової складності – $O(c^{f(n)})$ [21, 82], де $c > 1$ – константа, $f(n)$ – поліноміальна функція від числа n, яке визначається добутком простих чисел p і q.

Стійкість кодування, заснованого на алгоритмі RSA, базується на складності вирішення задачі факторизації цього числа n [24, 32]. Суть задачі факторизації полягає у представлення натурального числа n у вигляді добутку двох простих чисел p і q [61]. На сьогодні невідомі поліноміальні алгоритми факторизації простих чисел [58, 82]. Проте вважається, що факторизація поліноміальної складності за алгоритмом Шора є можлива на квантовому комп'ютері [58].

Для підвищення стійкості процедури кодування основна рекомендація полягає у використанні так званих "стійких" простих чисел p і q для побудови модуля числа n [2]. Наприклад, така рекомендація є в стандарті ANSI X9.31. Стійкі числа характеризуються ускладненням процедури факторизації числа n методами факторингу. Зазвичай, це ускладнення полягає у забезпеченні існування

великих головних дільників чисел (p +1) та (p - 1) з метою ускладнення роботи таких методів розкладу на множники [91] як, наприклад, за алгоритмом Поларда [2] чи викладеними у [89, 99].

Проте отримані останнім часом теоретичні та практичні результати в розвитку методів факторингу, зокрема, наприклад, метод еліптичних кривих [3, 10], нівелюють використання стійких чисел. Тому простий вибір стійких чисел не гарантує безпеки кодування, а відтак треба або вибирати дуже великі (довгі) прості числа, або підвищувати стійкість алгоритмів кодування/декодування.

Отже важливою науково-практичною задачею є забезпечення підвищеного рівня безпеки при коротких простих числах p і q.

Існуючі на сьогодні мінімальні практичні рекомендації для надійного кодування при використанні алгоритму RSA полягають або у пропозиції вибору простих чисел з розрядністю в декілька сотень бітів, або у виборі довжини числа n, яка є не меншою за 2048 бітів ($n \approx 2 \cdot 10^{600}$) [66]. Проте за [5, 36] відомо про обмеження використання сучасних обчислювальних ресурсів при $n > 10^{145}$.

Отже, можна констатувати, що основною проблемою RSA в практичній реалізації є генерація і використання великих простих чисел. Це означає, що практична реалізація RSA вимагає значних обчислювальних ресурсів, зокрема машинного часу та потужних обчислювачів [29].

1.4.3 Аналіз атак на алгоритм RSA

Для атаки на інформаційну систему, безпека якої базується на алгоритмі RSA, найчастіше використовується чотири види атак. Перший вид атаки полягає у пошуку (відновленні) секретного ключа за відкритим. Така атака є успішною, якщо знайти головні (найбільші спільні) множники числа n – числа p і q. Володіючи значеннями p, q і e можна легко визначити значення d. Як вже відзначалось, з математичної точки зору задача відновлення секретного ключа є задачею

факторизації: з одного боку для пошуку спільних множників n можна використовувати d, а з іншого - для пошуку d можна використовувати n. Найбільш відомими реалізаціями цього виду атак є використання еліптичних кривих, методи Морісона-Брілхарта, квадратичного решета, узагальненого числового решета та атака Вінера. Еліптичні криві вже згадувались у п. 1.2. А ідея атаки Вінера [125] полягає у тому, що за поліноміальний час з використанням неперервних дробів існує можливість визначити d. Існування алгоритмів атаки першого виду поки що не вирішує універсально і однозначно задачу факторизації. Так, наприклад, на сьогодні успішно вирішена факторизація 512-бітного модуля [66]. А тому, принаймні на сьогодні, при правильному виборі довгих значень ключів можна протистояти атаці, які базуються на розв'язанні задачі факторизації.

Другий вид атаки не є факторизацією і полягає у пошуку алгоритму визначення кореня степеня e з (mod n) [88, 90, 97]. Оскільки функція кодування визначається за (1.1), то коренем степеня e з (mod n) є повідомлення m. А надалі за визначеним коренем можна розкодувати захищені повідомлення уже без секретного ключа. Тут варто відзначити, що на сьогодні не існує ефективних алгоритмів цього виду атак, які б характеризувались універсальним призначенням. Як правило, така атака здійснюється у випадку, коли за умови невеликого показника степеня кодується велика кількість зв'язаних повідомлень.

Суть третього виду атак полягає у визначенні секретного ключа через аналіз параметрів функціонування програмно-апаратних комплексів в процесах кодування/розкодовування [101, 102, 111, 124]. Найбільш відомими методами є визначення RSA ключів за різницею потенціалів та адаптивний метод аналізу звукового фону [63]. На сьогодні ці методи дають можливість достатньо легко розкривати ключі із довжиною 4096 бітів. Проте слабкість такого виду атаки полягає у необхідності контакту з апаратурою. Так для використання методу, який базується на різниці потенціалів, необхідним є фізичний контакт з нульовою фазою апаратного

забезпечення, наприклад, завдяки підключенню давача до корпусу комп'ютера.

Існують атаки, які не базуються на розкритті усіх повідомлень, які кодуються визначеним ключем. Їх ідея полягає у розкриті окремого повідомлення без визначення ключа.

Серед цих атак найбільш відомими є словникові атаки або, за іншими термінологіями, атаки по наперед передбачуваному тексту чи атаки єдиного повідомлення. Володіючи відкритим ключем і маючи вдало сформований словник, можна достатньо легко розкрити повідомлення. Основний метод захисту полягає у додатковому зашумлення, яке виражається у додаванні у повідомлення додаткових бітів. У випадку, коли одне і те ж повідомлення m посилаються декільком користувачам, які використовують однакове значення e, випадкові біти додаються перед кожним кодуванням.

Алгоритми, які використовують підхід з додатковим зашумленням, набули широкої популярності, внаслідок чого виник напрям імовірнісного кодування. Їх основна проблема полягає у можливості зростання розміру кодованого повідомлення і використанні окремої процедури зашумлення. Для випадку зображення словникова атака є в принципі неможливою, оскільки сформувати наперед словник є неможливим. А ось проблема зростання розміру кодованого повідомлення є актуальною, оскільки цифрові зображення містять дуже багато точок кодування і навіть незначне зростання розміру кодованого повідомлення може призвести до значного обсягу даних комунікаційного сеансу.

У випадку зображень існує окремий вид атак, який базується на фільтраційних методах виділення контурів [26, 30, 69, 74] з метою отримання інформації із закодованого зображення без повного його розкодування. При цьому, як правило, використовуються або ентропійні методи виділення країв або матричні фільтри виділення контурів, які базуються на диференціальних градієнтних операторах [48]. Основним способом захисту є додаткове зашумлення закодованого зобра-

ження чи зміна по відношенню до закодованого зображення значення ентропії. Проблеми додаткового зашумлення полягають у тому, щоб в процесі кодування не збільшився розмір кодованого повідомлення, а сам додатковий шум не можна було б визначити різноманітними детекторами. Остання проблема вирішується в інтеграції процедури зашумлення у сам алгоритм RSA. Більш детальніше проблема використання алгоритму RSA із повідомленнями, якими виступають цифрові зображення, описується у наступному розділі.

Інші види атак [66, 85], які націлені не на криптоситему, а на суб'єктів комунікаційних сеансів чи вразливість самої системи у даному аналізі не розглядаються.

Отже, підсумовуючи вцілому можна констатувати, що для безпечного комунікаціного сеансу із використанням зображень необхідно вибирати довгі значення ключів та захистити етапи управління ключами системи RSA, виконання алгоритму RSA і канали обміну повідомленнями інформаційної автоматизованої системи критичного застосування.

1.5. Проблема забезпечення функціональної безпеки при організації захисту зображень за алгоритмом RSA

Зображення в телекомунікаційних сеансах систем критичного застосування є одним із важливих інформаційних пакетів. Відповідно до цього актуальним є завдання забезпечення функціональної безпеки при використанні саме такого типу інформації. Саме цьому питанню присвячений даний параграф.

Відомо, що використання алгоритму RSA у порівнянні із симетричними алгоритмами призводить до зростання часових витрат. Для їх мінімазації намагаються число e вибирати невеликим. Зазвичай в діпазоні від до 1 до 2 байтів. Вибране у межах цього діапазону число e у двійкому представленні містить лише по дві одиниці. Це значно зменшує обчислювальні витрати (зокрема кількість

операцій множення) операції піднесення до степеня.

Використання малих значень числа *e* має ще одну перевагу – таке мале число забезпечує не вихід за межі розрядної сітки і мінімальні потреби в обчислювальних ресурсах (зокрема незначні обсяги оперативної пам'яті саме для процедур кодування/декодування). Ця перевага набуває особливої ваги при використанні малоресурсних обчислювачів, наприклад, мобільних пристроїв чи пристроїв категорії "вбудовувані системи".

Проте використання малого значення числа *e* несе загрози інформаційній безпеці зокрема, а відтак функціональній безпеці загалом автоматизованої системи, оскільки, як зазначалось у попередньому параграфі, вибір малого значення *e* дає усі можливості провести успішну криптографічну атаку, що може призвести до декодування закодованого зображення. Це особливо актуально для випадків, коли один і той же ключ використовувся для кодування різних зображень для різних адресатів. Типово на сьогодні ця проблема вирішувалась додатковим зашумленням у форматі доповнення повідомлень.

Основна проблема використання алгоритму RSA для випадку криптографічного кодування зображень полягає у тому, що при малих значення числа *e* на зображеннях із флуктуаціями функції інтенсивності на закодованому зображенні будуть зберігатись контури (рис. 1.4б). Такий ефект носить назву неповного зашумлення.

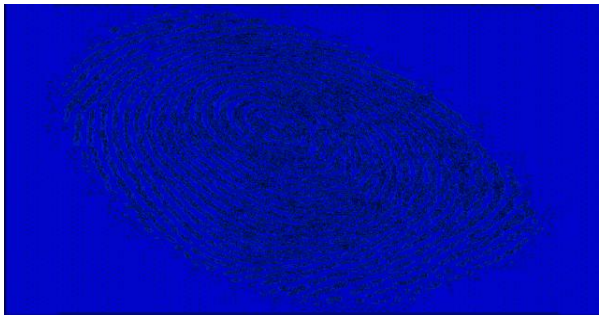
Поява цього ефекту пов'язана з логікою дії основної математичної функції, а саме функції mod, у процедурах кодування:

$$c'_{i,j} = c^{e}_{i,j} \bmod z. \qquad (1.3)$$

Тут $c'_{i,j}$ – закодоване значення яскравості або функції інтенсивності у точці (пікселі) з координатами (*i, j*); $c_{i,j}$ – вхідне значення яскравості або функції інтенсивності у точці (пікселі) з координатами (*i, j*); mod – математична функція

ділення за модулем числа z; z – операнд (ключ кодування) бінарної математичної функції mod.

а)



б) в)

Рисунок 1.4 – Приклад атаки на закодоване зображення методами фільтрації цифрових зображень: а – вихідне зображення; б – закодоване зображення; б – реконструйоване зображення

“Зашумленість” зображення (тобто кодування) в алгоритмі RSA дає математична операція mod. Функція mod є функцією двох аргументів $c_{i,j}$ і z. На рис. 1.5 наведено просторовий дискретний розподіл значень функції mod на областях визначення $z \in [1;100]$ та $c_{i,j} \in [1;50]$. При цьому крок дискретизації був рівним 1 у обох напрямах.

З наведеного на рис. 1.5 розподілу можна виділити визначальну властивість функції mod, яка полягає в існуванні значних однорідних областей при фіксованому значення операнда z. Площа, як геометрична характеристика цих областей, визначається співвідношенням z і $c_{i,j}$. У результаті існування однорідних

областей можна констатувати, що при близьких значеннях функції інтенсивності в результаті операції (1.3) закодовані значення $c'_{i,j}$ також будуть близькими. Саме ця близькість визначає рівень зашумленості на закодованому зображенні.

Проте окремі флуктуації значень функцій інтесивності $c_{i,j}$, а саме цією характеристикою визначаються контури, в результаті операції (1.3) даватимуть стрибки закодованих значень $c'_{i,j}$. Це означає, що при фіксованому значенні значенні операнда *z* на закодованому зображенні будуть зберігатись контури (через флуктуації закодованих значень функції інтенсивності). Як приклад добре ілюструє рис. 1.4б. Тому можна констатувати, що після роботи процедури кодування закодоване зображення не буде приховувати інформативність, яку несуть контури.

У цьому випадку загроза функціональній безпеці буде визначатись не методами взлому алгоритму RSA (атака на RSA математичними методами). Для видобування більшої інформативності із закодованого зображення будуть використовуватись методи цифрової обробки сигналів, наприклад фільтрації [1, 22, 75, 86, 95]. Як приклад, на рис 1.4в наведений результат фільтрації закодованого зображення (рис. 1.4б) найпростішим методом фільтрації, а саме матричним оператором Собеля. Із наведено на рис. 1.4в відфільтрованого зображення вже можна отримати практичну повну інформативність. При цьому витрати на взлом були мінімальними. Відзначимо, що використання спеціалізованих фільтраційних методів чи інших методів цифрової обробки зображень (наприклад реконструкції) дадуть можливість суттєво підняти отриманий рівень інформативності після такого способу взлому.

Одним із найбільш відомих розвинутих напрямів розв’язання проблеми уникнення контурів при малих значеннях простих числе полягає у використанні різноманітних топологічних підходів [115, 135], алгебраїчних форм, афінних чи матричних перетворень [23, 28, 76-81, 87, 92, 108, 114, 131, 132, 134]. Треба

відзначити, що з точки зору атаки методами цифрової обробки зображень рівень зашумленості закодованих зображень є дуже високим, а тому таку атаку провести фактично неможливо. Більше використання квадратичних форм або тернарних афінних перетворень суттєво підвищує стійкість до атаки математичними способами, описаними у п. 1.3.2. Проте проблема використання алгебраїчних форм і афінних перетворень полягає у тому, що різко зростають обчислювальні витрати, а тому використання алгоритмів, побудованих на основі цих методів не завжди є можливим. Особливо це стосується випадків, коли вимоги до часу мережевої транзакції є регламентованими і достатньо малими.

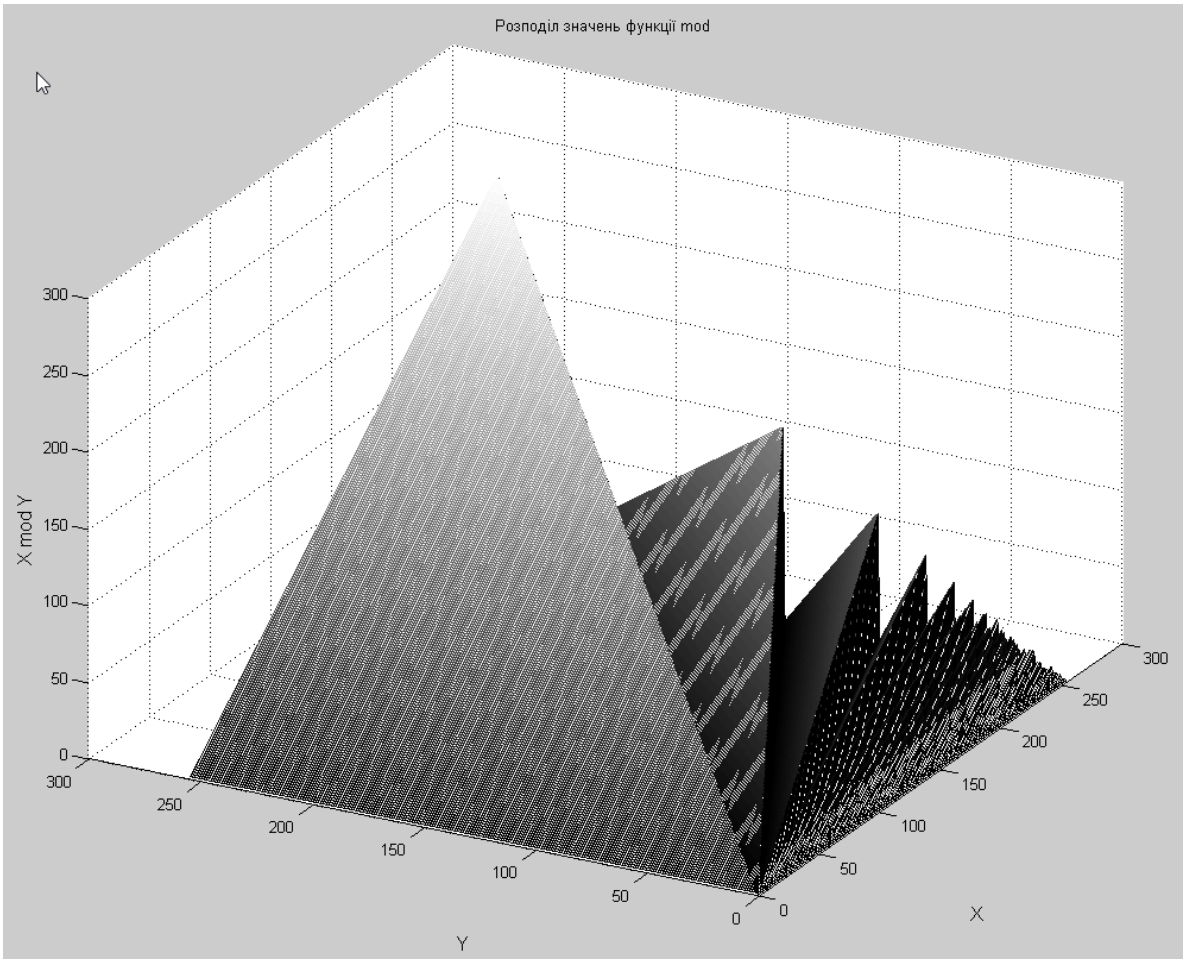


Рисунок 1.5 – Просторовий розподіл функції *mod*

Отже актуальною науково-прикладною задачею є розробка інформаційної технології забезпечення функціональної безпеки інформаційно-управляючих систем критичного застосування, які базуються на комунікаційних процедурах із застосуванням універсальних засобів з метою мінімізації обчислювальних ресурсів в процесах забезпечення надійності, стійкості та безпеки функціонування цих систем

Висновки до розділу 1

У першому розділі дисертаційного дослідження проведено аналіз сучасних автоматизованих систем обробки інформації критичного застосування. З цією метою досліджувались цільове призначення систем, їх характеристики та атрибути, які визначають ефективність їх функціонування в залежності від типу системи.

В процесі аналізу сучасних підходів до забезпечення функціональної безпеки показано, що одним із основних елементів є криптографічне кодування. Виявлено, що використання традиційних методів криптографічного кодування не завжди забезпечує необхідний рівень безпеки у випадку використання інформаційним об’єктом цифрового зображення.

Проаналізовано різні види криптографічних кодуваннь, які використо-вуються в організації функціональної безпеки. Наведено їх недоліки та переваги.

Результати аналізу сучасних завдань забезпечення функціональної безпеки підтведили важливість використання ефективних алгоритмів криптографічних кодувань в автоматизованих системах критичної обробки інформації на основі мережевої архітектури.

Для випадку цифрових зображень визначено основні наукові результати в області кодування, які доволяють нівелювати контури в процедурах кодування. В результаті аналізу виявлено, що існуючі на сьогодні методи не володіють необхідним значенням стійкості, а тому їх використання в автоматизованих системах обробки інформації критичного застосування може понизити загальний рівень функціональної безпеки

РОЗДІЛ 2. ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ У ВИПАДКУ ПЕРЕДАВАННЯ У ТЕЛЕКОМУНІКАЦІЙНИХ СЕАНСАХ НАПІВТОНОВИХ ЗОБРАЖЕНЬ

Як вже відзначалось у попередньому розділі, алгоритм RSA є одним із найбільш уживаних промислових стандартів кодування сигналів. Однак по відношенню до зображення існують певні проблеми його кодування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [96,107].

Тому актуальною задачею є розробка модифікації методу RSA такої, щоб

- зберегти стійкість;
- забезпечити повну зашумленість зображення з метою унеможливити використання методів візуальної обробки зображень.

Одним із шляхів вирішення цієї задачі є використання побітових операцій в алгоритмі RSA з додатковим зашумленням в програмній реалізації.

Основним об’єктом дослідження у цьому розділі є напівтонове цифрове зображення. Як відомо, цифрове зображення – це масив даних, отриманий шляхом дискретизації (аналого-цифрового перетворення) оригіналу. Напівтонове зображення визначається як масив даних, які є градаціями функції інтенсивності розміром 1 або 2 байти. Це визначає діапазон значень градацій функції інтесивності: [0;255] та [0; 65535] для кожного розміру відповідно.

На практиці розмір 1 байт є більш вживаним, а тому розглядатимуться напівтонові зображення із значеннями функції інтенсивності розміром 1 байт. Найбільш відомими такими зображеннями є так звані зображення у “відтінках сірого”, для значення 0 – це чорний колір, а 255 – білий колір (максимальна інтенсивність). Тут варто зазначити, що в загальному випадку діапазон значень може визначати будь-який колірний проміжок вибраної колірної палітри. Проте на практиці найчастіше використовується саме сегмент [чорний;білий].

2.1. Матричне представлення однотонового зображення

Нехай задано рисунок P з ширини l і висоти h. Його можна розглядати як матрицю пік селів

$$<pxl_{ij}>_{1\le i\le n,\ 1\le j\le m}, \tag{2.1}$$

де pxl_{ij} – піксел з координатами i та j;

n і m – число точок по висоті та ширині.

В загальному випадку n і m є залежними від l та h, а тому більш коректним є запис

$$n = n(l) \text{ і } m = m(h). \tag{2.2}$$

Матриці (2.1) у відповідність ставиться матриця значень функції інтенсивні (значення пікселів)

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}, \tag{2.3}$$

де c_{ij} – однобайтове значення функції інтенсивності піксела dtp_{ij} напівтонового зображення P.

Тобто має місце відповідність [4, 77]

$$P = \mathbf{P}_{l,h} = \left[\ pxl_{ij}\ \right]_{1\le i\le n(l),1\le j\le m(h)} \to \mathbf{C}=\left[\ c_{ij}\ \right]_{1\le i\le n(l),1\le j\le m(h)}. \tag{2.4}$$

Важливою характеристикою зображення є наявність в зображенні контурів. Задача виділення контура вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають області постійних рівнів яскравості, тобто, контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші

частини зображення залишаються темними [77].

Математично – ідеальний контур є розривом просторової функції рівнів яскравості в площині зображення. Тому виділення контура означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [69]. Це є однією з причин, через що контури залишаються в зображенні при кодуванні в системі RSA, оскільки кодування тут базується на піднесенні до степеня по модулю деякого натурального числа. При цьому на контурі і на сусідніх до контура пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

2.2. Поєднання алгоритму RSA і побітових операцій при кодуванні – декодуванні напівтонових зображень

Для підвищення стійкості RSA розроблено дві модифікації алгоритму RSA, які базуються на використанні побітових операцій [52, 53]. Модифікації відрізняються використанням одного чи двох послідовних рядків матриці напівтонового зображення.

2.2.1. Модифікації алгоритму RSA

Кодування і декодування по одному рядку матриці зображення.

Нехай задано P, Q - пара довільних простих чисел і число N, яке визначається так

$$N = PQ. \tag{2.5}$$

Кодування відбувається поелементно з використанням наступного перетворення елементів матриці зображення **C** (2.3):

1. Випадково вибирається натуральне число $e < \varphi(N)$ і знаходиться таке натуральне d, що виконується конгруенція

$$ed \equiv 1(\text{mod } \varphi(N)). \tag{2.6}$$

2. Будується число

$$A = (e << k) + (d << l) + (e << l) + (d << k), \tag{2.7}$$

де $k < 16$, $l < 16$ – натуральні числа, $k \neq l$, << – операція логічного зсуву вліво.

3. У кожному рядку виконується логічний зсув вліво значення інтенсивності i-го піксела, $i = 1, 2, \ldots, m$, m – число елементів у рядку, за наступним правилом:

- якщо $i \bmod 7 = 0$, то виконується логічний зсув вліво значення інтенсивності піксела на величину $i \bmod 3$,
- якщо $i \bmod 11 = 1$, то виконується логічний зсув вліво значення інтенсивності піксела на величину $i \bmod 4$.

Математично це правило можна представити так:

$$c_{i,j} = c_{i,j} << \begin{cases} i \bmod 3, \text{ якщо } i \bmod 7 = 0; \\ i \bmod 4, \text{ якщо } i \bmod 11 = 1. \end{cases} \tag{2.8}$$

4. Будується число B відніманням від отриманого значення інтенсивності піксела числа $(A - 3)$.

5. Закодованим значенням інтенсивності i-го піксела, $i = 1, 2, \ldots, m$, m –число елементів у рядку, вибирається число

$$C \equiv B^e \ (\text{mod } N). \tag{2.9}$$

Декодування проводиться в порядку, протилежному до кодування після отримання числа

$$C^d \equiv (B^e)^d \pmod{N}, \qquad (2.10)$$

виконанням протилежних операції до змісту пунктів 4), 3), 2), 1).

Кодування по двох рядках матриці.

Кодування відбувається з використанням елементів двох рядків за алгоритмом, який описано вище для кодування елементів одного рядка інтенсивнстей, за виключенням п. 5, причому кожний рядок з вибраних двох рядків кодується незалежно за своїм алгоритмом, для нього модифікованим п. 5.

Пункт 5) має вигляд:

1. Для першого рядка закодованим значенням інтенсивності i-го піксела, $i = 1, 2, \ldots, m$, m – число елементів у рядку, вибирається число

$$C \equiv B^e \pmod{N} \qquad (2.11)$$

2. Для другого рядка закодованим значенням інтенсивності i-го піксела, $i = 1, 2, \ldots, m$, m – число елементів у рядку, вибирається число

$$C \equiv B^d \pmod{N}. \qquad (2.12)$$

Декодування відбувається в протилежному порядку з урахуванням п. 1, 2.

2.2.2 Оцінка стійкості криптографічного кодування

Нехай $\psi(n)$ – найменше спільне кратне чисел P - 1 і Q - 1. Тоді, як відомо за Вербшцьким [21], стійкість алгоритму RSA визначається числом $\chi(n) = \varphi(\psi(n)) - 1$, яке означає, що за $\chi(n)$ ітерацій система RSA може бути розкрита.

Для оцінки стійкості розробленого алгоритму пропонується така методика За (2.7) будується число A. Таке число можна побудувати $\wp(A) = 4 \cdot 16^4$ способами. Це означає, що за $\wp(n)\chi(n)$ ітерацій можна розкрити закодоване повідомлення

вказаним методом, що більше, ніж в стандартному варіанті RSA.

2.2.3. Результати практичних експериментів

На основі описаних модифікацій RSA розроблено алгоритми захисту напівтонових зображень в телекомунікайціних системах. Ці алгоритми реалізовано в програмному рішенні, описаному у р. 4. Використовуючи це програмне рішення проведено практичні експерименти, результати яких наведено на рис. 2.1-2.6.

Рисунок 2.1 – Початкове зображення для кодування за одним рядком за п. 2.2.1

Так для випадку кодування за одним рядком матриці зображення отримано результати, наведені на рис. 2.1-2.3. Параметри зображення є такими: l = 699 пікселів; h = 476 пікселів; формат – напівтоновий однобайтний. Кодування здійснювалось при такій парі простих чисел P = 107, Q = 83.

Для визначення подібності початкового і декодованого зображення використовувалась метрика [30]

$$\left\| P - P'' \right\| = \sum_{j=1}^{m} \sum_{i=1}^{n} \begin{cases} 1, c_{i,j} = c''_{i,j}, \\ 0, c_{i,j} \neq c''_{i,j} \end{cases}, \tag{2.13}$$

де P'' – декодоване зображення із значення функції інтенсивності $c''_{i,j}$.

Рисунок 2.2 – Закодоване зображення за методом з п. 2.2. Кодування здійснювалось за одним рядком. Початкове зображення наведене на рис. 2.1

Рисунок 2.3 – Декодоване зображення. Кодування здійснювалось за одним рядком за методом з п. 2.2. Початкове зображення наведене на рис. 2.1

Співвідношення сигнал/шум [30] між оригінальним та закодованим зображенням визначається за формулою

$$PSNR(P,P') = 20\log_{10}\left(\frac{255}{\sum_{j=1}^{m}\sum_{i=1}^{n}\left|c_{i,j}-c'_{i,j}\right|^2}\right). \qquad (2.14)$$

У випадку зображень наведених на рис. 2.1 і 2.2 маємо: $PSNR\,(P, P') = 6.69$.

Рівень зашумленості $L(P, P')$ оригінального P і закодованого зображень P' оцінювався падінням рівня ентропії

$$L\left(P,P'\right) = \frac{H_{256}\left(P\right) - H_{256}\left(P'\right)}{\log_2 255}100\%. \qquad (2.15)$$

де $H_{256}(P)$ – ентропія значень функції інтенсивності зображення P, яка визначалась так [31, 144]

$$H_{256}(P) = -\sum_{i=0}^{255} \frac{p_i}{256} \log_2 \left(\frac{p_i}{256} \right). \quad (2.16)$$

де p_i – відліки гістограми зображення P.

У випадку зображень, наведених на рис. 2.1 та 2.2 ентропія оригінального зображення становила – 7.13, закодованого – 4.53. Тобто $L(P, P') = -32.6$, що свідчить про падіння ентропії і зростання рівня зашумленості.

Падіння рівня ентропії означає, що закодоване зображення є більш вирівняним по контрасності ніж оригінальне. Тобто на закодованому зображені меншими є перепади функції інтенсивності, що є причиною виникнення контурів.

Загалом рівень зашумленості можна також визначати падінням рівня шуму, який визначається за формулою [56]

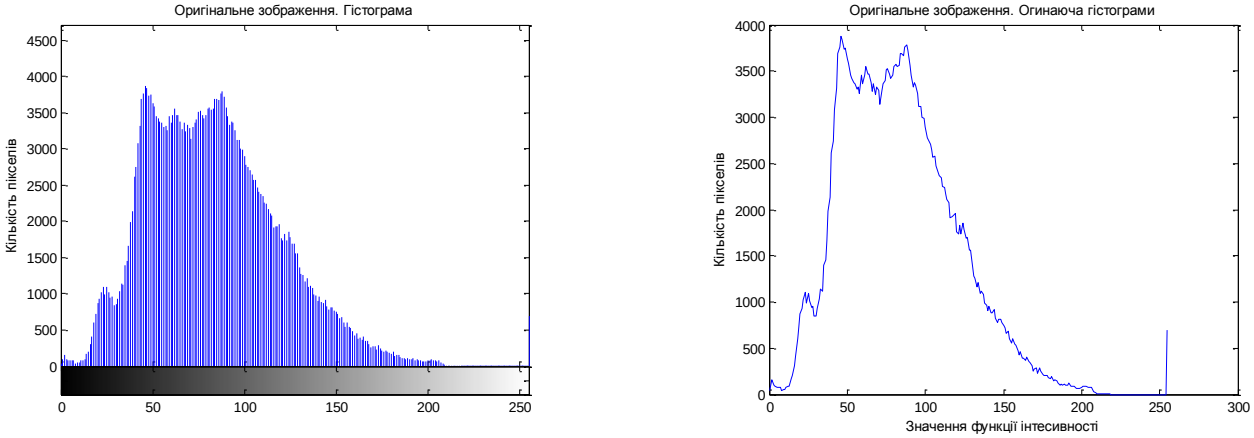
$$PSNR(P) = 20 \log_{10} \left(\frac{255}{\frac{1}{Z} \sum_{k=1}^{Z} \sigma_k^2} \right). \quad (2.17)$$

де Z – кількість проміжків гістограми зображення P; σ_k^2 – дисперсія функції інтенсивності на k-му проміжку.

У випадку зображень, наведених на рис. 2.1 і 2.2, маємо: $PSNR(P) = 8.94$, $PSNR(P') = 2.29$. Тобто падіння рівня $|PSNR(P) - PSNR(P')|$ шуму становить: 6.64.

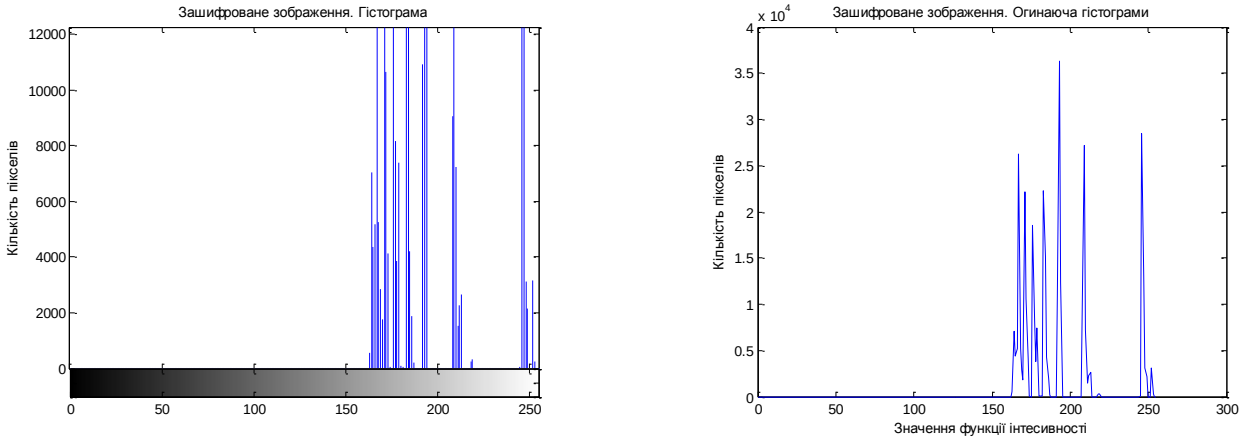
З порівняння гістограм оригінального та закодованого зображень можна побачити кардинальну зміну гістограми на закодованому зображенні. Проте на закодованому зображенні мінімальні контури все ж таки можна помітити. Це означає, що злам гістограми не гарантує розв’язання проблеми появи контурів.

Для їх уникнення треба підвищувати значення простих чисел *P* і *Q*. Інший шлях уникнення навіть мінімальних контурів – це використання кодування за двома рядками.



а) б)

Рисунок 2.4 – Гістограма та її огинаюча зображення наведеного на рис. 2.1



а) б)

Рисунок 2.5 – Гістограма та її огинаюча зображення наведеного на рис. 2.2

Для випадку кодування за двома рядками матриці зображення отримано результати, наведені на рис. 2.6-2.8. Параметри зображення є такими: *l* = 720 пікселів; *h* = 480 пікселів; формат – напівтоновий однобайтний. Кодування

здійснювалось при такій парі простих чисел $P = 107$, $Q = 83$.

З порівняння рис. 2.2 і 2.7 видно, що кодування по одному рядку матриці відрізняється від кодування по двох рядках цієї матриці. Контури у другому випадку є відсутні. Про це свідчать і чисельні характеристики процедури кодування, зокрема у випадку: $PSNR(P, P') = 8.8$, $L(P, P') = -39.6$, $PSNR(P) = 5.15$, $PSNR(P') = 2.38$. Порівнючи ці дані із даними, отриманими у випадку кодування за одним рядком, можна констатувати, що рівень зашумленості не дуже сильно, але все ж таки зріс. Цього виявилось достатньо для того, щоб повністю видалити контури на закодованому зображенні.

Початкові і декодовані зображення є ідентичними за метрикою (2.12).

Рисунок 2.6 – Початкове зображення для кодування за двома рядками п. 2.2.1

Гістограми рис. 2.6 та 2.7. наведені у додатках як рис. Д.1.1 та Д.1.2 відповідно. Порівнюючи гістограми, можна констатувати що, подібно до випадку кодування за одним рядком, маємо повний злам гістограми.

Обидві модифікації алгоритму RSA без жодних застережень можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення, може зрости розмір кодованого

зображення.

Запропоновані модифікації кодування/декодування грунтуються на використанні ідей базового алгоритму RSA. А тому їх стійкість до несанкціонованого декодування запропонованими потоковими модифікаціями забезпечується алгоритмом RSA.

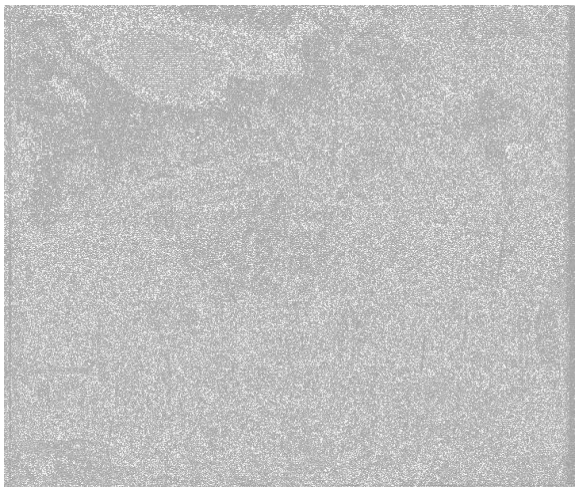


Рисунок 2.7 – Закодоване зображення за методом з п. 2.2. Кодування здійснювалось за двома рядками. Початкове зображення наведене на рис. 2.6

Рисунок 2.8 – Декодоване зображення. Кодування здійснювалось за двома рядками за методом з п. 2.2. Початкове зображення наведене на рис. 2.6.

2.3. Використання побітових операцій і додаткового зашумлення в алгоритмі RSA при кодуванні та декодуванні зображень

2.3.1. Модифікації алгоритму RSA

Наступні модифікації алгоритму RSA передбачають окрім використання побітових операцій в алгоритмі ще й привнесення додаткового зашумлення в криптографічний процес [51, 73, 142]. З цією метою, подібно до модифікації, наведеної у п. 2.1, також розроблено дві методології, а саме кодування та декодування за одним та двома рядками матриці зображення.

Кодування і декодування по одному рядку матриці зображення.

Нехай задано *P*, *Q* - пара довільних простих чисел і число для *N* для якого виконується рівність (2.5).

Кодування відбувається поелементно з використанням наступного перетворення елементів матриці зображення **C** (2.3):

1. Випадково вибирається натуральне число $e < \varphi(N)$ і знаходиться таке натуральне *d*, що виконується конгруенція (2.6).

2. Будується число *A* за (2.7).

3. В кожному рядку виконується логічний зсув вліво значення інтенсивності *i*-го піксела, $i = 1, 2, \ldots, m$, m – число елементів у рядку, за наступним правилом: виконується логічний зсув вліво значення інтенсивності піксела на величину $i \bmod n$, $n < 16$.

$$c_{i,j} = c_{i,j} << i \bmod n, n < 16. \qquad (2.18)$$

4. Будується число *B* відніманням від отриманого значення інтенсивності піксела числа $(A + e)$.

5. Закодованим значенням інтенсивності *i*-го піксела, $i = 1, 2, \ldots, m$, m –число елементів у рядку, вибирається число

$$C \equiv \mathrm{B}^{\mathrm{e}} \pmod N + f(i^2) . \qquad (2.19)$$

Декодування проводиться в порядку, протилежному до кодування після отримання числа

$$(C - f(i^2))^d \equiv (B^e)^d \pmod N, \qquad (2.20)$$

виконанням протилежних операції до змісту пунктів 4) – 1).

Кодування по двох рядках матриці.

Кодування відбувається з використанням елементів двох рядків за алгорит-

мом, який описано вище для кодування елементів одного рядка інтенсивностей, за виключенням п. 5, причому кожний рядок з вибраних двох рядків кодується незалежно за своїм алгоритмом, для нього модифікованим п. 5.

Пункт 5) має вигляд:

1. Для першого рядка закодованим значенням інтенсивності i-го піксела, $i = 1, 2, \ldots, m$, m – число елементів у рядку, вибирається число

$$C \equiv B^e \pmod{N} + g(i^2). \tag{2.21}$$

2. Для другого рядка закодованим значенням інтенсивності i-го піксела, $i = 1, 2, \ldots, m$, m – число елементів у рядку, вибирається число

$$C \equiv B^e \pmod{N} - g(i^2). \tag{2.22}$$

Декодування відбувається в протилежному порядку з урахуванням п. 1,2.

2.3.2. Результати практичних експериментів

На основі описаних модифікацій RSA розроблено алгоритми криптографічного кодування напівтонових зображень в телекомунікайціних системах, які також реалізовано в програмному рішенні, описаному у розділі 4. Використовуючи це програмне рішення, проведено практичні експерименти, результати яких наведено на рис. 2.9-2.14.

Для випадку кодування за одним рядком матриці (метод з п. 2.3.1) зображення отримано результати, наведені на рис. 2.9-2.11. Параметри зображення є такими: l = 667 пікселів; h = 332 пікселів; формат – напівтоновий однобайтний. Кодування здійснювалось при такій парі простих чисел $P = 79$, $Q = 89$.

Чисельні результати процедури кодування є такими: $PSNR(P, P') = 10.682$, $L(P, P') = -2.36$, $PSNR(P) = 7.87.15$, $PSNR(P') = 7.91$.

Гістограми зображень, наведених на рис. 2.9 та 2.10, приводяться у додатках

на рис. Д.1.3 та Д.1.4 відповідно.

Рисунок 2.9 – Початкове зображення для кодування за одним рядком за п. 2.3

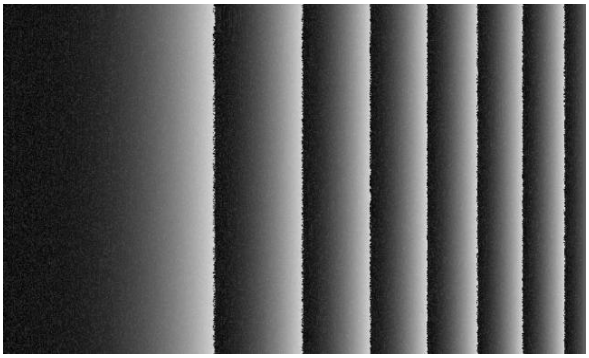


Рисунок 2.10 – Закодоване зображення за методом з п. 2.3. Кодування здійснювалось за одним рядком. Початкове зображення наведене на рис. 2.9

Рисунок 2.11 – Декодоване зображення. Кодування здійснювалось за одним рядком за методом з п. 2.3. Початкове зображення наведене на рис. 2.9

Зображення, які використовувались у п. 2.2, є близькими за своїми параметрами із зображенням, яке наведене на рис. 2.9. Тому приймаємо, що чисельні результати процедур кодування обидвох методів є співмірними між собою.

З порівняння чисельних значень, отриманих за методами з п. 2.2, з результатами, отриманими за методом з п. 2.3, можна констатувати, що рівень зашумленості $L(P, P')$ впав, проте значення метрики $PSNR(P, P')$ зросло. Гістограма у випадку використання методу з п. 2.3 “ламається” не дуже сильно. Проте візуаль-

на оцінка закодованого зображення свідчить про абсолютно повну відсутність контурів на закодованому зображенні. Більше того, закодоване зображення володіє візульною характеристикою гармонійності, що може бути використано як додаткове стеганографічне приховування інформації.

Для випадку кодування за двома рядками матриці зображення отримано результати, наведені на рис. 2 .12-2.14. Параметри зображення є такими: l = 640 пікселів; h = 386 пікселів; формат – напівтоновий однобайтний. Кодування здійснювалось при такій парі простих чисел P = 89, Q = 83.

Рисунок 2.12 – Початкове зображення для кодування за двома рядками методом з п. 2.3

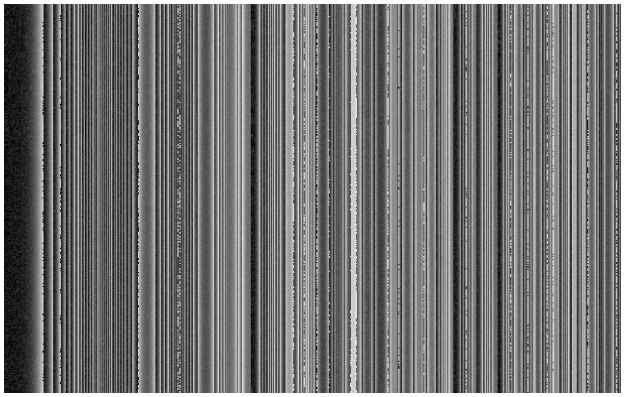


Рисунок 2.13 – Закодоване за методом з п. 2.3 зображення, рис. 2.12. Кодування здійснювалось за двома рядками.

Рисунок 2.14 – Декодоване зображення. Кодування здійснювалось за двома рядками за методом з п. 2.3.

Чисельні результати процедури кодування є такими: $PSNR(P, P') = 9.18$, $L(P, P') = 1.57$, $PSNR(P) = 4.54$, $PSNR(P') = 6.27$.

Гістограми зображень, наведених на рис. 2.12 та 2.13, приводяться у додатках на рис. Д.1.5 та Д.1.6 відповідно. Зміна гістограм у порівнянні із методами із п. 2.2 та, подібно до випадку використання одного рядка, також не є сильною.

У випадку використання двох рядків, на відміну від випадку використання одного рядка, бачимо зростання рівня зашумленості та падіння метрики $PSNR(P, P')$. Це свідчить про зростання рівня гармонійності закодованого зображення.

З порівняння рис. 2.10 і рис. 2.13 видно, що кодування по одному рядку матриці суттєво не відрізняється від кодування по двох рядках цієї матриці з точки зору нівелювання контурів. Контури в обох закодованих зображеннях є повністю відсутніми. Більше того, рівень зашумленості змінився несуттєво. Тому використання двох рядків є виправданим у тих випадках, коли незначний ріст рівня зашумлення, а також рівня гармонійності закодованого зображення, є суттєвимим.

Порівняння декодованих і оригінальних зображень в обидвох випадках за мірою подібності (2.12) засвідчує повну ідентичність оригінальних та декодованих зображень. Початкові і декодовані зображення є ідентичними за метрикою (2.12).

2.4. Використання функцій зашумлення в модифікаціях алгоритму RSA при кодуванні та декодуванні напівтонових зображень

2.4.1. Модифікації алгоритму RSA

Кодування і декодування по двох рядках матриці зображення [12, 54].

Нехай задано P, Q – пару довільних простих чисел і число для N, яке визначається так

$$N = PQ,\ \varphi(N) = (P - 1)(Q - 1)\ . \qquad (2.23)$$

Кодування відбувається поелементно з використанням наступного перетворення елементів матриці значень функції інтенсивності зображення **C** (2.3):

1. Випадково вибирається натуральне число $e < \varphi(N)$ і знаходиться таке натуральне d, що виконується конгруенція (2.6).

2. Будуються чотири числа

$$\begin{aligned} A \equiv \left(c_{k,i}\right)^e \left(\mathrm{mod}\, N\right), B \equiv \left(c_{k+1,i}\right)^e \left(\mathrm{mod}\, N\right), \\ E \equiv \left(c_{k,i+1}\right)^d \left(\mathrm{mod}\, N\right), D \equiv \left(c_{k+1,i+1}\right)^d \left(\mathrm{mod}\, N\right), \end{aligned} \tag{2.24}$$

тут $1 \le k < n, 1 \le i < m$.

3. Будується матриця закодованих значень інтенсивностей пікселів

$$\tilde{\mathbf{C}} = \begin{pmatrix} \tilde{c}_{1,1} & \ldots & \tilde{c}_{1,m} \\ \ldots & \ldots & \ldots \\ \tilde{c}_{n,1} & \ldots & \tilde{c}_{n,m} \end{pmatrix}, \tag{2.25}$$

де

$$\tilde{c}_{k,i} = A, \tilde{c}_{k+1,i} = B, \tilde{c}_{k,i+1} = E, \tilde{c}_{k+1,i+1} = D,\ 1 \le\ k < n,\ 1 \le i < m. \tag{2.26}$$

Декодування проводиться наступним чином. Декодовані значення інтенсивностей пікселів отримуються з наступних співвідношень:

$$\begin{aligned} c_{k,i} \equiv A^d \left(\mathrm{mod}\, N\right), c_{k+1,i} \equiv B^d \left(\mathrm{mod}\, N\right), \\ c_{k,i+1} \equiv E^e \left(\mathrm{mod}\, N\right), c_{k+1,i+1} \equiv D^e \left(\mathrm{mod}\, N\right), \end{aligned} \tag{2.27}$$

Кодування і декодування по двох рядках матриці зображення з додатковим зашумленням [54].

Нехай задано P, Q – пару довільних простих чисел і число для N, яке визначається рівністю (2.23).

Кодування відбувається поелементно з використанням наступного перетворення елементів матриці значень функції інтенсивності зображення **C** (2.3):

1. Випадково вибирається натуральне число $e < \varphi(N)$ і знаходиться таке натуральне d, що виконується конгруенція (2.6).

2. Будуються чотири числа

$$\begin{gathered} A \equiv \left(c_{k,i}\right)^e \left(\operatorname{mod} N\right), B \equiv \left(c_{k+1,i}\right)^e \left(\operatorname{mod} N\right), \\ E \equiv \left(c_{k,i+1} + i^2 / \left(ed\right)\right)^d \left(\operatorname{mod} N\right), D \equiv \left(c_{k+1,i+1} + k^2 / \left(ed\right)\right)^d \left(\operatorname{mod} N\right), \end{gathered} \tag{2.28}$$

тут $1 \le k < n, 1 \le i < m$.

3. Будується матриця закодованих значень інтенсивностей пікселів (2.25) елементи якої визначаються так

$$\begin{gathered} \tilde{c}_{k,i} = A + f\left(k,i\right), \tilde{c}_{k+1,i} = B + g\left(k,i\right), \\ \tilde{c}_{k,i+1} = E + F\left(k,i\right), \tilde{c}_{k+1,i+1} = D + G\left(k,i\right),\ 1 \le k < n, 1 \le i < m. \end{gathered} \tag{2.29}$$

Декодування проводиться наступним чином. Декодовані значення інтенсивностей пікселів отримуються з наступних співвідношень:

$$\begin{gathered} c_{k,i} \equiv \left(\tilde{c}_{k,i} - f\left(k,i\right)\right)^d \left(\operatorname{mod} N\right), c_{k+1,i} \equiv \left(\tilde{c}_{k+1,i} - g\left(k,i\right)\right)^d \left(\operatorname{mod} N\right), \\ c_{k,i+1} \equiv \left(\tilde{c}_{k,i+1} - F\left(k,i\right)\right)^e \left(\operatorname{mod} N\right) - i^2 / \left(ed\right), \\ c_{k+1,i+1} \equiv \left(\tilde{c}_{k+1,i+1} - G\left(k,i\right)\right)^e \left(\operatorname{mod} N\right) - k^2 / \left(ed\right), \\ f\left(k,i\right) = Pk^2 i^2, g\left(k,i\right) = Qk^2 i^2, F\left(k,i\right) = ek^2 i^2, G\left(k,i\right) = dk^2 i^2. \end{gathered} \tag{2.30}$$

Для оцінки стійкості розробленого методу скористаємось методикою описаною у п. 2.2.2. За цією методикою і за (2.23) побудуємо чотири числа *A*, *B*, *E*, *D*.

Ці числа можна побудувати $\wp(A) = ((n - 1) \cdot (m - 1))^4$ способами. Це означає, що за $\wp(n) \cdot \chi(n)$ ітерацій можна розкрити закодоване повідомлення вказаним

методом, що більше, ніж в стандартному варіанті RSA.

2.4.2. Результати практичних експериментів

На основі описаних модифікацій RSA розроблено алгоритми криптографічного кодування напівтонових зображень в телекомунікаційних системах, які, подібно до модифікацій, описаних у п. 2.2 та 2.3, також реалізовано в програмному рішенні, описаному у розділі 4. Використовуючи це програмне рішення, проведено практичні експерименти, результати яких наведено на рис. 2.15-2.21.

Рисунок 2.15 – Початкове зображення для кодування за двома рядками методом з п. 2.4

Для випадку кодування за двома рядком матриці (метод з п. 2.4.1) зображення отримано результати, наведені на рис. 2.15-2.17. Параметри зображення є такими: l = 469 пікселів; h = 700 пікселів; формат – напівтоновий однобайтний. Кодування здійснювалось при такій парі простих чисел P = 23, Q = 37.

Чисельні результати процедури кодування є такими: $PSNR(P, P') = 4.72$, $L(P, P') = -28.78$, $PSNR(P) = 3.73$, $PSNR(P') = 19.85$.

Гістограми зображень, наведених на рис. 2.15 та 2.16, приводяться у до-

датках на рис. Д. 1.7 та Д. 1.8 відповідно. Зміна гістограм, у порівнянні із методами із п. 2.2 та подібно до випадку використання одного рядка, також не є сильною.

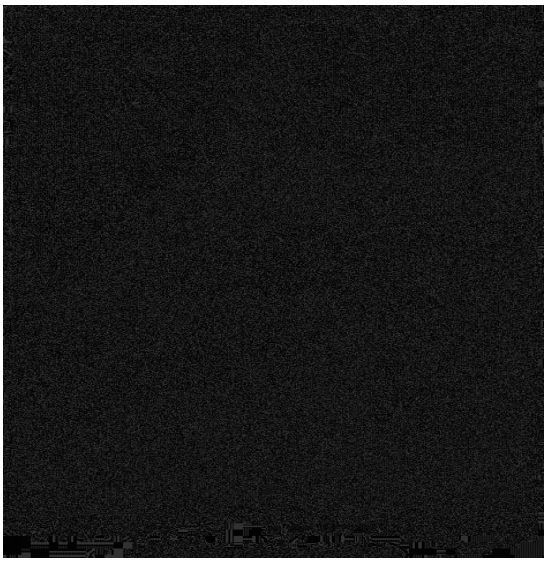


Рисунок 2.16 – Закодоване за двома рядками методом з п. 2.4 зображення, наведене на рис. 2.15.

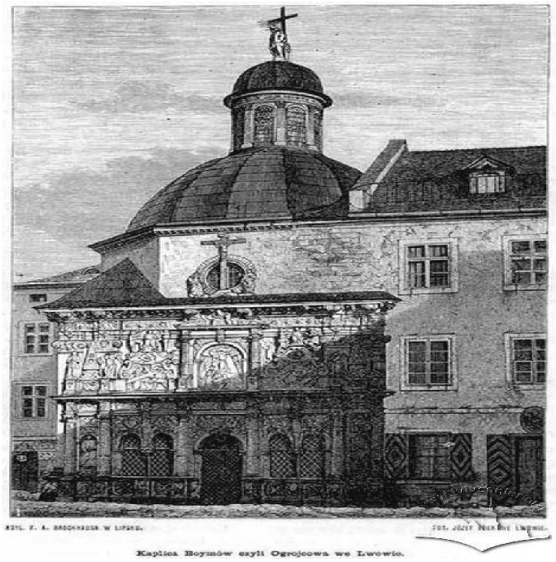


Рисунок 2.17 – Декодоване зображення. Кодування здійснювалось за двома рядками методом з п. 2.4.

З порівняння змін гістограм оригінального (рис. Д.1.7) та закодованого (рис. Д.1.8) випливає суттєва зміна останнього зображення, а ріст рівня зашумленості засвідчив відсутність гармонійності закодованого зображення. За відображенням дії процедури кодування метод, описаний у п. 2.4, є подібний до методів, які наводились у п. 2.2.

Для випадку кодування із додатковим зашумленням матриці зображення отримано результати, наведені на рис. 2.18-2.20. Параметри зображення є такими: l = 640 пікселів; h = 386 пікселів; формат – напівтоновий однобайтний. Кодування здійснювалось при такій парі простих чисел P = 13, Q = 97.

Чисельні результати процедури кодування є такими: $PSNR(P, P') = 9.3$,

$L(P, P') = -1.53$, $PSNR(P) = 6.59$, $PSNR(P') = 7.07$.

Рисунок 2.18 – Початкове зображення для кодування без додаткового зашумлення методом з п. 2.4

Гістограми зображень, наведених на рис. 2.18 та 2.19, приводяться у додатках на рис. Д. 1.9 та Д. 1.10 відповідно. Зміна гістограм, у порівнянні із випадком без зашумлення, вже не є настільки різкою. Це підтверджується появою деякої впорядкованості (гармонійності) на закодованому зображенні, а чисельно це підтвердження виражається зростанням значень $L(P, P')$ і $PSNR(P, P')$.

Стосовно появи впорядкованості на закодованому зображенні варто додати наступне.

При кодуванні з додатковим зашумленням структура і впорядкованість на закодованому зображенні візуально суттєво відрізняються в залежності від вибору структури зашумлення. Цей факт може бути використано в топологічній модифікації алгоритму кодування-декодування. На рис. 2.23 показано результати використання різних функцій зашумлення при таких значеннях простих чисел: $P = 43$, $Q = 67$. Види додаткового зашумлення, які використовувались у цьому експерименті наведене у табл. 2.1.

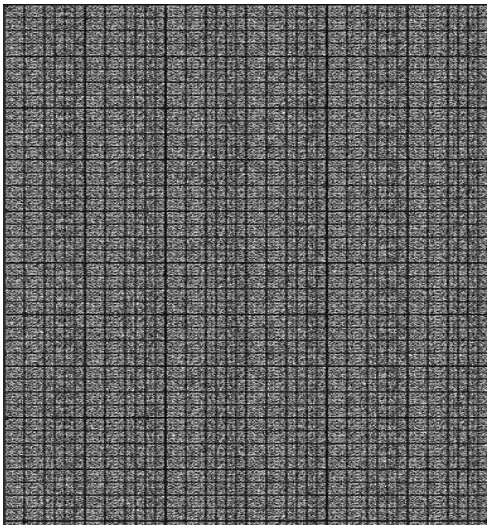


Рисунок 2.19 – Закодоване із додатковим зашумлення за п. 2.4 зображення, наведене на рис. 2.18

Рисунок 2.20 – Декодоване за методом з п. 2.4 зображення

Табл. 2.1. Види додаткового зашумлення

Позначення	Вид
#1	$f(k,i)=Pk^2i^2, g(k,i)=Qk^2i^2, F(k,i)=ek^2i^2, G(k,i)=Pk^2i^2$
#2	$f(k,i)=Pk^3i^2, g(k,i)=Qk^3i^2, F(k,i)=ek^2i^2, G(k,i)=Pk^2i^2$
#3	$f(k,i)=Pk^3i^2, g(k,i)=Qk^3i^2, F(k,i)=ek^3i^2, G(k,i)=Pk^3i^2$
#4	$f(k,i)=Pk^3i^4, g(k,i)=Qk^3i^4, F(k,i)=ek^3i^4, G(k,i)=Pk^3i^4$

Результати експериментів відображають графіки, наведені на рис. 2.21, 2.22. Як засвідчують результати експериментів, рівень зашумленості різко зростає при зміні функції (оператора) зашумленості (рис. 2.22). При цьому зростає відстань від оригінального зображення за метрикою PSNR (рис. 2.21). Очевидно, що степінь впорядкованості на закодованому зображенні також падає із ускладненням

оператора додаткової зашумленості.

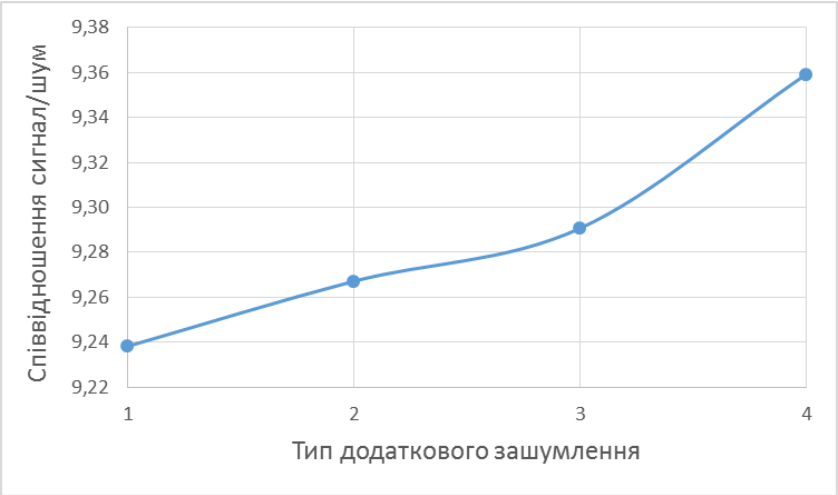


Рисунок 2.21 – Зміна значення $PSNR\,(P, P')$ в залежності від виду функції зашумлення

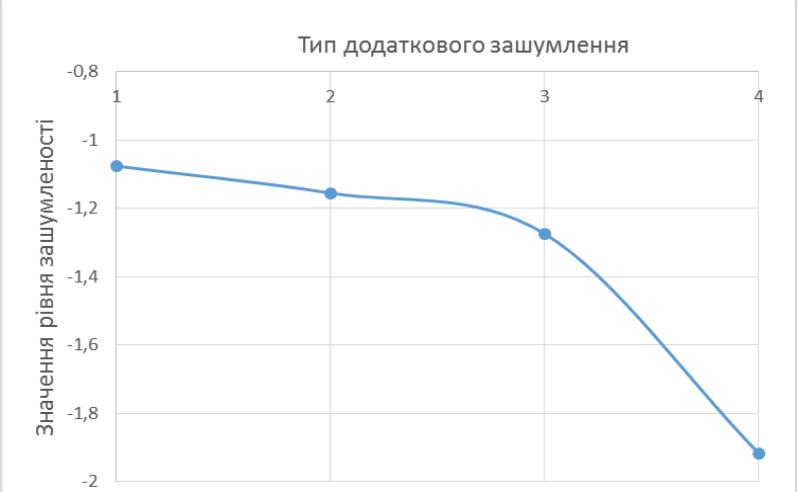
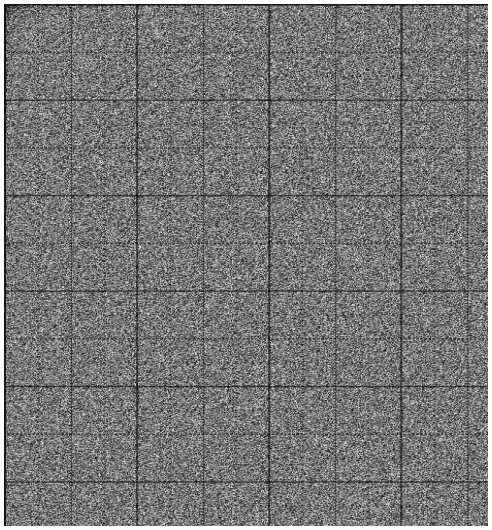
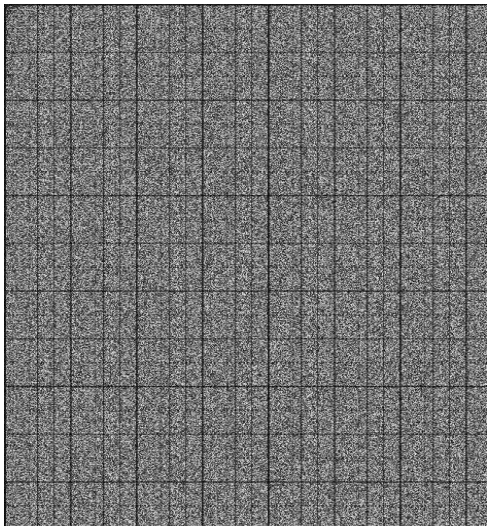


Рисунок 2.22 – Зміна значення $L(P, P')$ в залежності від виду функції зашумлення

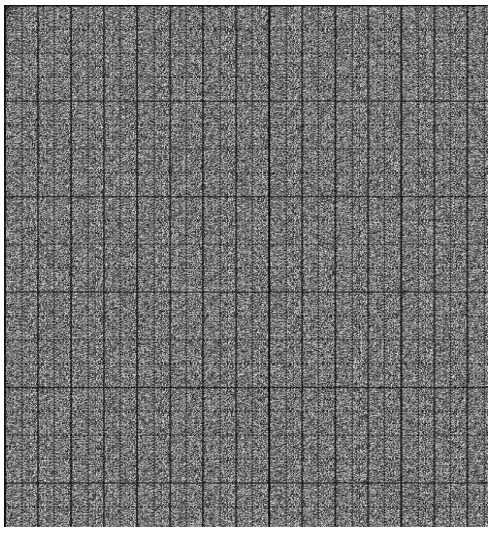
Модифіковані методи кодування з п. 2.4 побудовані так, що при малих значеннях ключа також можна досягти якісного кодування, але за умови вірного підбору параметрів кодування. При цьому досягається висока швидкість роботи алгоритму.



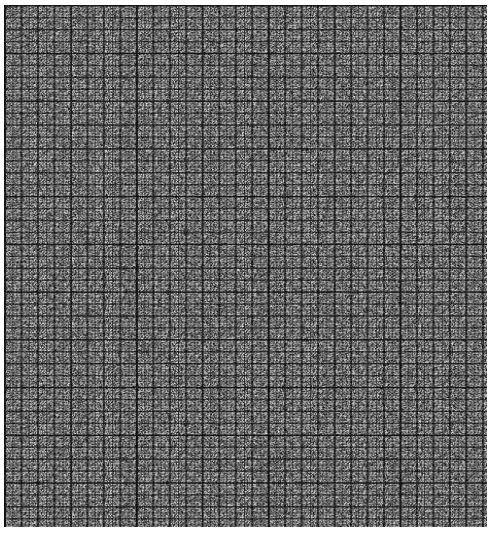
#1



#2



#3



#4

Рисунок 2.23 – Вплив функції зашумлення на результат кодування

Висновки до розділу 2

1. Наведені у другому розділі методи криптографічного кодування призначені для забезпечення функціональної безпеки в автоматизованих системах критичного застосування для випадку коли основним інформаційним об’єктом використовуються напівтонових цифрові зображення

2. Усі наведені у цьому розділі методи можуть бути використані стосовно будь-якого типу зображень, але найбільші переваги досягаються у випадку використання напівтонових зображень, які дозволяють чітко виділяти контури.

3. Без жодних модифікацій усі розроблені методи можна також використати і стосовно кольорових зображень. Однак, незалежно від типу кольорового зображення, пропорційно до розмірності вхідного зображення, може зрости розмір кодованого зображення і гарантовано втричі зростають витрати пам’яті в процедурах кодування та декодування на робочих станціях комунікаційних сеансів.

4. Модифікації методу RSA, які базуються на сумісному використанні побітових операцій і алгоритму RSA без додаткового зашумлення, є залежними від кількості рядків, які задіюються в процедурах кодування/декодування. Це означає, що рівень зашумленості у випадку використання двох рядків є суттєво більший від випадку використання одного рядка.

5. У випадку сумісного використання побітових операцій, алгоритму RSA та додаткового зашумлення залежність від вибору кількості рядків для процедур кодування/декодування є набагато меншою за випадок модифікації алгоритму RSA без додаткового зашумлення. Рівень зашумленості у випадку використання двох рядків несуттєво зростає від випадку використання одного рядка.

6. Використання додаткового зашумлення при сумісному використанні побітових операцій та алгоритму RSA дозволило понизити мінімальні значення простих чисел, які використовуються в алгоритмі і при яких контури вже не відображаються на закодованому зображенні.

7. Модифіковані методи кодування побудовані так, що при малих значеннях ключа також можна досягти якісного кодування, але за умови вірного підбору параметрів кодування. При цьому досягається висока швидкість роботи алгоритму.

8. Відзначимо, що стійкість усіх модифікацій забезпечується самим алгоритмом RSA. Тому реалізація (забезпечення) стійкості модифікованих алгоритмів з одночасним забезпеченням якості зображення не вимагають значних обчислювальних ресурсів.

РОЗДІЛ 3. ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ У ВИПАДКУ ПЕРЕДАВАННЯ В ТЕЛЕКОМУНІКАЦІЙНИМИ СЕАНСАХ ПОВНОКОЛІРНИХ ЗОБРАЖЕНЬ

3.1. Матричне представлення кольорового зображення

На відміну від розділу 2 у цьому розділі об’єктом дослідження є процеси криптографічного кодування цифрових кольорових зображень в телекомунікаційних системах. При цьому розглядатимуться такі кольорові зображення, у яких значення функції інтенсивності у кожному пікселі виражаються багатобайтним представленням [4]. За основу взято 4-и байтне представлення значення функції інтенсивності в системі ARGB. За цим представлення кожному пікселу зображення P відповідає тріада однобайтових чисел, які відповідають значенням функції інтенсивності по кожному каналу системи ARGB

$$pxl_{ij} \to (c_{i,j}^{\alpha}, c_{i,j}^{R}, c_{i,j}^{G}, c_{i,j}^{B}), 1 \le i \le n,\ 1 \le j \le m, \tag{3.1}$$

де $c_{i,j}^{\alpha}$ – значення α-складової значення функції інтенсивності системи ARGB; $c_{i,j}^{R}, c_{i,j}^{G}, c_{i,j}^{B}$ – значення функції інтенсивності по кожному каналу системи ARGB відповідно.

Представлення (3.1) визначає співвідношення кожному пікселу не одно- чи двобайтового цілого числа, а компонентного вектора розмірністю 4

$$\mathbf{c}_{i,j} \to (c_{i,j}^{\alpha}, c_{i,j}^{R}, c_{i,j}^{G}, c_{i,j}^{B}). \tag{3.2}$$

У відповідності до цього матричне представлення (2.3) у випадку кольорових зображень набирає такого виду

$$\mathbf{C}=\begin{pmatrix} \mathbf{c}_{1,1} & \dots & \mathbf{c}_{1,m} \\ \dots & \dots & \dots \\ \mathbf{c}_{n,1} & \dots & \mathbf{c}_{n,m} \end{pmatrix}, \tag{3.4}$$

Тобто елементами матриці C виступають вектори розмірності 4.

З іншого боку, якщо до уваги приймати число розміром 4-и байти, і кожен байт цього числа є елементом вектора $\mathbf{c}_{i,j}$, то можна знов перейти до аналізу кольорового зображення у цілих числах. Правда, на відміну від напівтонових зображень, по-перше, ці числа будуть великими, що має значення для вбудованих телекомунікаційних систем і по-друге – вони будуть від'ємними, оскільки, зазвичай, значення α-каналу є рівним 1. Оскільки це останній байт в 4-х байтовому представленні цілого числа, то він буде порозрядно визначати знак цього числа. У випадку трибайтового кольорового зображення (наприклад колірні системи RGB чи YUV, проблеми від'ємного значення не існує, оскільки усі елементи колірного вектора вибраного піксела задіюються у визначенні цілого числа, а 4-й байт є завжди нульовим.

Таке трактування елементів матриці (3.4) дає можливість використання матричного представлення (2.3) для аналізу 3-х чи 4-х байтових кольорових зображень.

3.2. Бінарні операції і елементи алгоритму RSA кодуванні та декодуванні кольорових зображень

3.2.1. Математична модель сумісного використання бінарних операцій та елементів алгоритму RSA для організації криптографічного кодування кольорових зображень

Кодування по одному рядку матриці зображення [50].

Нехай задано P, Q – пару довільних простих чисел і число N, яке

визначається за виразом (2.5).

Кодування відбувається поелементно з використанням наступного перетворення елементів матриці значень функції інтенсивності кольорового зображення **C** (2.3):

1. Випадково вибирається натуральне число $e < \varphi(N)$ і знаходиться таке натуральне d, що виконується конгруенція (2.6).
2. Якщо

$$i \equiv 0 \pmod 2, \quad 1 \le i \le l, \tag{3.5}$$

то випадково вибирається число

$$m \equiv (i + P) \pmod{31}+1, \tag{3.6}$$

і будуються числа

$$B \equiv m^e \pmod N, \quad X = i \cdot B \cdot P. \tag{3.7}$$

3. Якщо

$$i \equiv 1 \pmod 2, \quad 1 \le i \le l, \tag{3.8}$$

то випадково вибирається число

$$m \equiv (i + Q) \pmod{31}+1, \tag{3.9}$$

і будуються числа

$$B \equiv m^d \pmod N, \; X = i \cdot B \cdot Q. \tag{3.10}$$

4. З використанням бінарної операції ^ – порозрядного виключеного «АБО» – будується число

$$a_{i,j} = c_{i,j} \wedge X. \tag{3.11}$$

5. Виокремлюється кожний розряд числа $a_{i,j}$ за наступною схемою:

$$\begin{aligned}
&a_{1,i,j} = a_{i,j} \,\&\, 2^0; \quad a_{2,i,j} = a_{i,j} \,\&\, 2^1; \quad a_{3,i,j} = a_{i,j} \,\&\, 2^2; \quad a_{4,i,j} = a_{i,j} \,\&\, 2^3;\\
&a_{5,i,j} = a_{i,j} \,\&\, 2^4; \quad a_{6,i,j} = a_{i,j} \,\&\, 2^5; \quad a_{7,i,j} = a_{i,j} \,\&\, 2^6; \quad a_{8,i,j} = a_{i,j} \,\&\, 2^7;\\
&a_{9,i,j} = a_{i,j} \,\&\, 2^8; \quad a_{10,i,j} = a_{i,j} \,\&\, 2^9; \quad a_{11,i,j} = a_{i,j} \,\&\, 2^{10}; \quad a_{12,i,j} = a_{i,j} \,\&\, 2^{11};\\
&a_{13,i,j} = a_{i,j} \,\&\, 2^{12}; \quad a_{14,i,j} = a_{i,j} \,\&\, 2^{13}; \quad a_{15,i,j} = a_{i,j} \,\&\, 2^{14}; \quad a_{16,i,j} = a_{i,j} \,\&\, 2^{15};\\
&a_{17,i,j} = a_{i,j} \,\&\, 2^{16}; \quad a_{18,i,j} = a_{i,j} \,\&\, 2^{17}; \quad a_{19,i,j} = a_{i,j} \,\&\, 2^{18}; \quad a_{20,i,j} = a_{i,j} \,\&\, 2^{19};\\
&a_{21,i,j} = a_{i,j} \,\&\, 2^{20}; \quad a_{22,i,j} = a_{i,j} \,\&\, 2^{21}; \quad a_{23,i,j} = a_{i,j} \,\&\, 2^{22}; \quad a_{24,i,j} = a_{i,j} \,\&\, 2^{23};\\
&a_{25,i,j} = a_{i,j} \,\&\, 2^{25}; \quad a_{26,i,j} = a_{i,j} \,\&\, 2^{25}; \quad a_{27,i,j} = a_{i,j} \,\&\, 2^{26}; \quad a_{28,i,j} = a_{i,j} \,\&\, 2^{27};\\
&a_{29,i,j} = a_{i,j} \,\&\, 2^{28}; \quad a_{30,i,j} = a_{i,j} \,\&\, 2^{29}; \quad a_{31,i,j} = a_{i,j} \,\&\, 2^{30}; \quad a_{32,i,j} = a_{i,j} \,\&\, 2^{31},
\end{aligned} \tag{3.12}$$

де & – операція арифметичного «І».

6. Виконується циклічне заміщення $m + 1$ розрядів числа a за схемою:

$$a_{k,i,j} = a_{k,i,j} << m{+}1. \tag{3.13}$$

де << – бінарна операція зсуву «І».

7. Виконавши додавання отримаємо закодовані значення функції інтенсивності для кожного піксела

$$u_{i,j} = a_{1,i,j} \,|\, a_{2,i,j} \,|\, ... \,|\, a_{32,i,j}\,. \tag{3.14}$$

Тут | – операція порозрядного додавання.

Відповідно до (3.14) отримуємо закодоване зображення.

8. Всі числа, отримані за (3.14) записуються в наступну матрицю за формулою

$$\mathbf{V} = \begin{pmatrix} u_{1,1} & ... & u_{1,l} \\ ... & ... & ... \\ u_{h,1} & ... & u_{h,l} \end{pmatrix}. \tag{3.15}$$

Декодування по одному рядку матриці зображення.

Декодування проводиться при заданих числах $e < \varphi(N)$ і d, N, визначених за (2.5) і (2.6), наступним чином:

1. Якщо

$$i \equiv 0 \pmod 2, \ 1 \le i \le l, \tag{3.16}$$

то будується число

$$m \equiv B^d \pmod N \tag{3.17}$$

і число

$$X = i \cdot B \cdot P. \tag{3.18}$$

2. Якщо

$$i \equiv 1 \pmod 2, \ 1 \le i \le l, \tag{3.19}$$

то будується число

$$m \equiv B^e \pmod N \tag{3.20}$$

і число

$$X = i \cdot B \cdot Q. \tag{3.21}$$

3. Виокремлюється кожний розряд числа $a_{i,j}$ за схемою (3.12).

4. Виконується циклічне заміщення $m + 1$ розрядів числа $a_{i,j}$ за схемою (3.13)

5. З використанням бінарної операції ^ – порозрядного виключеного «АБО» – будується число

$$c_{i,j} = a \wedge X. \qquad (3.22)$$

6. Декодованим є зображення після 5-го кроку.

Для оцінки стійкості розробленого методу скористаємось методикою описаною у п. 2.2.2. В описаному алгоритмі для кодування використовуються два числа: або m, визначене за (3.6), або m визначене за (3.9). Ці два числа можна вибрати $\wp(m, n) = i \cdot 31^2$ способами. Це означає, що за $\wp(n) \cdot \chi(n)$ ітерацій можна розкрити закодоване повідомлення вказаним методом, що більше, ніж в стандартному варіанті RSA.

3.2.2. Результати практичних експериментів

На основі описаної модифікацій RSA розроблено алгоритми кодування кольорових зображень в телекомунікаційних системах, який, подібно до методів описаних у розділі 2, також реалізовано в програмному рішенні, описаному у розділі 4. Використовуючи це програмне рішення, проведено практичні експерименти, результати яких наведено на рис. 3.1-3.4.

Рисунок 3.1 – Початкове зображення для кодування за методом з п. 3.2

Рисунок 3.2 – Декодоване зображення, наведене на рис3.1. Кодування здійснювалось за методом з п. 3.2 при таких параметрах: $P = 71$, $Q = 83$

Параметри зображення є такими: $l = 640$ пікселів; $h = 386$ пікселів; формат – кольоровий в системі ARGB. Кодування здійснювалось при такій парі простих чисел $P = 71$, $Q = 83$.

З порівняння результатів, наведених на рис. 3.3 і 3.4 видно, що кодування при різних значеннях простих чисел P і Q, суттєво відрізняється. Проте в обидвох випадках контури в обох закодованих зображеннях відсутні повністю. Це означає, що для подолання проблеми збереження контурів на закодованому зображенні достатньо простих чисел із значеннями в околі 100.

Початкове (рис. 3.1) і декодоване (рис. 3.2) зображення за метрикою (2.12) є повністю ідентичними.

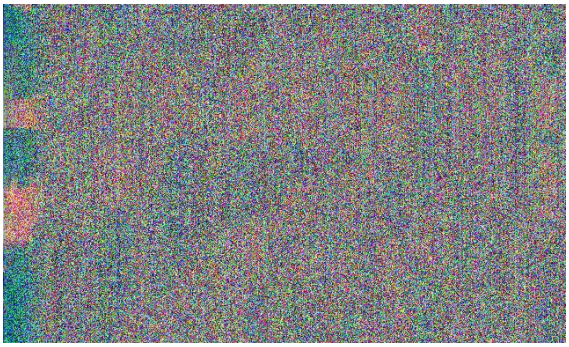


Рисунок 3.3 – Закодоване зображення за методом з п. 3.2. Кодування здійснювалось при таких параметрах: $P = 71$, $Q = 83$. Початкове зображення наведене на рис. 3.1

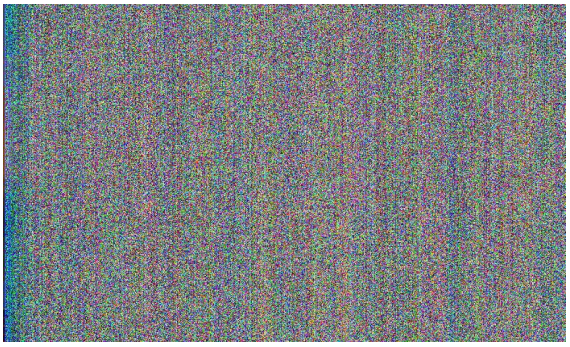


Рисунок 3.4 – Закодоване зображення за методом з п. 3.2. Кодування здійснювалось при таких параметрах: $P = 127$, $Q = 53$. Початкове зображення наведене на рис. 3.1

Чисельні результати процедури кодування при використанні пари значень: $P = 71$, $Q = 83$ є такими: $PSNR(P, P') = 9.9$, $L(P, P') = 3.23$, $PSNR(P) = 4.68$, $PSNR(P') = 5.45$.

Чисельні результати процедури кодування при використанні пари значень:

$P = 127$, $Q = 53$ є такими: $PSNR(P, P') = 10.46$, $L(P, P') = 8.1517$, $PSNR\ (P) = 4.68$, $PSNR\ (P') = 5.83$.

Окрім значень пари P і Q, результати використання яких наведені на рис 3.3 та 3.4, в практичних експериментах використовувалось ще значення $P = 59$, $Q = 67$. На рис. 3.5 та 3.6 наведено графіки залежності основних метрик від значень P і Q. З наведених графіків видно, що зміни величин метрик засвідчують зростання рівня зашумленості при збільшенні значень P і Q. Подібний характер залежності є властивим для алгоритму RSA. Тому графіки, наведені на рис. 3.5 та 3.6, є підтвердженням того, що розроблена модифікація зберегла усі базові характеристики базового методу, проте зменшила рівень мінімальних значень P і Q для нівелювання проблеми контурів на закодованому зображенні.

Практичний інтерес становить вплив значень P і Q на зміну гістограми оригінального зображення. Для зображень, наведених на рис. 3.1, 3.3 та 3.4, гістограми наведені в додатках на рис. Д.1.12 - Д.1.14 відповідно. З порівняння цих гістограм можна констатувати, що ріст значень P і Q в процедурах кодування призводить до стиску та нормалізації гістограми значень функції інтенсивності

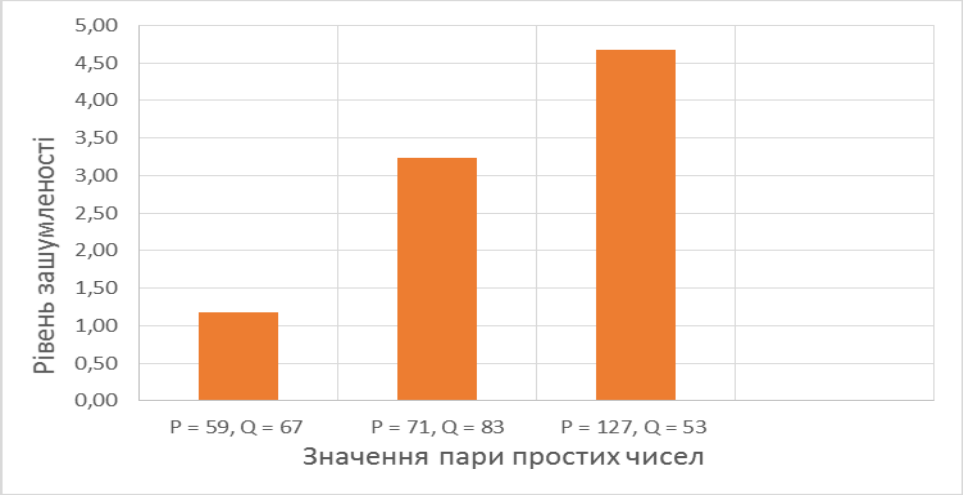


Рисунок 3.5 – Залежність рівня зашумленості від значень P і Q при використанні методу з п. 3.2. в процедурі кодування зображення, наведеного на рис. 3.1

Рисунок 3.6 – Залежність метрики $PSNR(P, P')$ від значень P і Q при використанні методу з п. 3.2. в процедурі кодування зображення, наведеного на рис. 3.1

На останок відзначимо, що розроблений у п. 3.2 метод кодування кольорових зображень може використовуватись для будь-яких зображень, значення функції інтенсивності яких має глибину в 1 байт і більше.

3.3. Використання бінарних операцій та матриці ключів при кодуванні кольорових зображень в модифікаціях алгоритму RSA

3.3.1. Модифікації алгоритму RSA

Процедура кодування [11, 52].

Нехай задано P, Q – пару довільних простих чисел і число N, яке визначається за виразом (2.5)

Кодування відбувається поелементно для кожного i-ого рядка з використанням наступних перетворень елементів матриці значень функції інтенсивності кольорового зображення $\mathbf{C}$ (2.3):

1. Якщо

$$j \bmod 2 \equiv 0, \tag{3.23}$$

то будується число:

$$jj = \text{random}(j + P) \bmod 31 \; + \; 1, \quad a_{i,j} \equiv jj^{e} \bmod N, \quad X = ja_{i,j}P. \tag{3.24}$$

2. Якщо

$$j \bmod 2 \equiv 1, \tag{3.25}$$

то будується число:

$$jj = \text{random}(j + Q) \bmod 31 \; + \; 1, \quad a_{i,j} \equiv jj^{d} \bmod N, \quad X = ja_{i,j}Q. \tag{3.26}$$

3. Будується число

$$K = c_{i,j} \wedge X. \tag{3.27}$$

4. Кодоване до $c_{i,j}$ значення $\tilde{c}_{i,j}$ отримується циклічним зсувом числа K на $(31 - jj)$ розрядів.

5. Результатом роботи є, подібно до (2.19), матриця кодованих значень інтенсивностей пікселів вхідної матриці (2.3) і матриця ключів

$$\mathbf{A} = \left[a_{i,j} \right]_{1 \le i \le n(l), 1 \le j \le m(h)}. \tag{3.28}$$

Процедура декодування.

Декодування проводиться при заданих числах $e < \varphi(N)$ і d, N, визначених за (2.5) і (2.6), наступним чином:

1. Якщо виконується конгруенція (3.23), то будується число:

$$jj = \text{random}(j + P) \bmod 31 \; + \; 1, \quad a_{i,j} \equiv jj^{d} \bmod N, \quad X = ja_{i,j}P. \tag{3.29}$$

2. Якщо виконується конгруенція (3.25), то будується число:

$$jj = \text{random}(j + Q) \bmod 31 + 1, \quad a_{i,j} \equiv jj^e \bmod N, \quad X = ja_{i,j}Q. \tag{3.30}$$

3. Виконується циклічний зсув закодованого значення функції інтенсивності $\tilde{c}_{i,j}$ на $(31 - jj)$ розрядів.

Результатом роботи є матриця (2.3) кодованих значень інтенсивностей пікселів, яка визначається так

$$\mathbf{C} = \tilde{\mathbf{C}} \wedge X \,. \tag{3.31}$$

3.3.2. Результати практичних експериментів

На основі описаної модифікацій RSA розроблено алгоритм кодування кольорових зображень в телекомунікаційних системах, який, подібно до методів описаних у п. 3.2, також реалізовано в програмному рішенні, описаному у розділі 4. Використовуючи це програмне рішення, проведено практичні експерименти, результати яких наведено на рис. 3.7-3.12.

Параметри зображення є такими: l = 552 пікселів; h = 575 пікселів; формат – кольоровий в системі ARGB. Кодування здійснювалось при такій парі простих чисел P = 61, Q = 59.

Результати практичного використання описаного методу наведені на рис 3.7.

Чисельні результати процедури кодування при використанні пари значень: P = 71, Q = 83 є такими: $PSNR(P, P')$ = 11.78, $L(P, P')$ = 11.46, $PSNR\ (P)$ = 4.17, $PSNR\ (P')$ = 5.7.

Гістограми оригінального (рис.3.7) та закодованого (рис.3.9) зображень наведені в додатках на рис. Д1.15 та Д1.16 відповідно. Порівняння цих гістограм свідчить про сильну нормалізацію гістограми при достатньо малих значеннях P і Q. Як можна побачити з рисунку закодованого зображення, досягнуто високого рівня шуму і повної відсутності контурів при менших, за випадок методу з п. 3.2, значеннях простих чисел P і Q.

Рисунок 3.7 – Початкове зображення для кодування за методом з п. 3.3

Рисунок 3.8 – Декодоване за методом з п. 3.3. зображення

Особливістю розробленого у п. 3.3 методу, є те, що він поєднує позитивні сторони двох криптографічних систем – симетричної та асиметричної. Негативна риса асиметричної системи – повільність виконання процедур кодування-декодування, при описаному поєднанні частково нейтралізовується швидкістю симетричної системи. Як видно з результатів, кодування при такому підході не втрачає того рівня стійкості, який притаманний для обох систем.

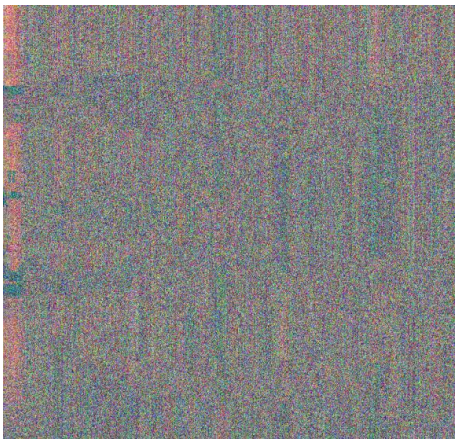


Рисунок 3.9 – Закодоване за методом з п. 3.3. зображення, наведене на рис. 3.7

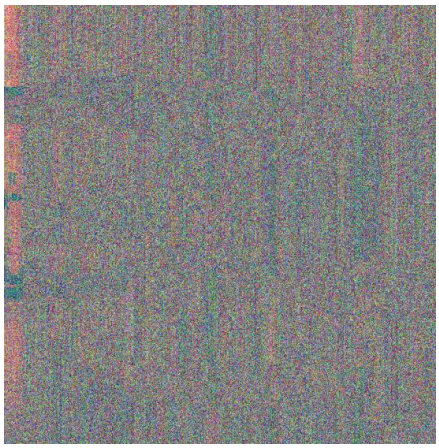


Рисунок 3.10 – Зображення матриці ключів для зображення, наведеного на рис. 3.9

Для порівняння із методом, описаним у п. 3.2, кодувалось теж саме зображення (рис. 3.1) при тих самих значеннях пари P і Q (п. 3.2.2). Результати кодування наведено на рис. 3.9.

Чисельні результати процедури кодування при використанні пари значень: $P = 71$, $Q = 83$ є такими: $PSNR(P, P') = 13.72$, $L(P, P') = 14.61$, $PSNR(P) = 10.02$, $PSNR(P') = 6.04$.

При порівнянні з результатом, наведеним на рис. 3.2, можна констатувати, що навіть при таких малих значеннях пари значень P і Q, які використовувались в процедурі кодування, вже починає суттєво зростати рівень зашумленості. Особливо це стосується випадку порівняння із методом, описаним у п. 3.2.

Гістограма закодованого зображення наведена у додатках на рис Д.1.17. При порівнянні із гістограмами, наведеними на рис. Д.1.13 та Д.1.14, тенденція нормалізації збереглась, але рівень нормалізації є меншим у порівнянні із використанням методу, описаним у п. 3.2. Але тут треба зазначити, що гістограма, наведена на рис. Д.1.17 отримана при значно менших значеннях P і Q, ніж гістограми наведені на рис. Д.1.13 та Д.1.14.

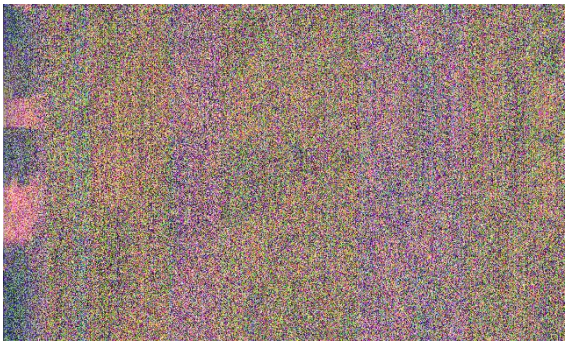


Рисунок 3.11 – Закодоване зображення, наведене на рис. 3.1, за методом з п. 3.3 при таких параметрах: $P = 71$, $Q = 83$

Рисунок 3.12 – Зображення матриці ключів для закодованого зображення, наведеного на рис. 3.11

Основним недоліком розробленого методу є те, що наведений у п. 3 метод є

орієнтований виключно на кольорові зображення із глибиною кольору 4-и байти. Застосування цього методу навіть для три байтових зображень потребує значної модифікації методу.

3.4. Сумісне використання криптосистем Ель-Гамаля і RSA для організації кодування повноколірних зображень

У результаті аналізу сучасних методів організації безпеки в телекомунікаційних системах з'ясовано ефективність і можливість використання криптосистеми Ель-Гамаля. Зокрема виявлено можливість сумісного використання криптосистем Ель-Гамаля і RSA [55, 118, 133].

В процесі дисертаційних досліджень отримано два ефективні способи сумісного використання цих криптосистем для організації криптографічного кодування кольорових зображень в телекомунікаційних сеансах.

3.4.1. Кодування і декодування по одному рядку матриці зображення

Нехай задано P, Q – пару довільних простих чисел і число N, яке визначається за виразом (2.5)

Кодування відбувається поелементно з використанням наступного перетворення елементів матриці значень функції інтенсивностей кольорового зображення **C** (2.3):

1. Випадково вибирається натуральне число $d < \varphi(N)$ і знаходиться таке натуральне d, що виконується конгруенція (2.6).

2. Випадково вибирається натуральне число x,

$$1 < x < P - 1, \tag{3.32}$$

і вибирається натуральне число k,

$$1 < k < P - 1. \tag{3.33}$$

3. Будуються чотири числа

$$\begin{aligned} a &\equiv Q\ , \\ b &\equiv \left(Q^x \left(\mathrm{mod}\, P\right)\right)^k , \\ a_{i,j} &\equiv i\left(i+j\right)^e \left(\mathrm{mod}\, N\right), \\ b_{i,j} &\equiv j\left(ij\right)^d \left(\mathrm{mod}\, N\right), \end{aligned} \tag{3.34}$$

де $1 \le i \le n$, $1 \le j \le m$.

4. Будується матриця закодованих значень інтенсивностей пікселів (2.19), елементи якої визначаються так

$$\begin{aligned} \tilde{c}_{i,j} &= ac_{i,j} - bc_{i,j+1} + a_{i,j} + f\left(i,j\right); \\ \tilde{c}_{i,j+1} &= ac_{i,j} + bc_{i,j+1} + b_{i,j} + g\left(i,j\right), \end{aligned} \tag{3.35}$$

де $f(i, j)$, $g(i, j)$ – деякі функції зашумлення, $1 \le i \le n$, $1 \le j < m$.

Декодування відбувається наступним чином:

1. Декодовані значення інтенсивностей пікселів отримуються з співвідношень (3.35):

$$\begin{aligned} ac_{i,j} - bc_{i,j+1} &= \tilde{c}_{i,j} - a_{i,j} - f\left(i,j\right); \\ ac_{i,j} + bc_{i,j+1} &= \tilde{c}_{i,j+1} - b_{i,j} - g\left(i,j\right),\ 1 \le i < n,\ 1 \le j < m \end{aligned} \tag{3.36}$$

2.Тоді визначаються декодовані значення функції інтенсивності матриці **C**

$$\begin{aligned} c_{i,j} &= \frac{\left(a\left(\tilde{c}_{i,j} - a_{i,j} - f\left(i,j\right)\right) + b\left(\tilde{c}_{i,j+1} - b_{i,j} - g\left(i,j\right)\right)\right)}{\delta}; \\ c_{i,j+1} &= \frac{\left(a\left(\tilde{c}_{i,j+1} - b_{i,j} - g\left(i,j\right)\right) - b\left(\tilde{c}_{i,j} - a_{i,j} - f\left(i,j\right)\right)\right)}{\delta}, \end{aligned} \tag{3.37}$$

де $\delta = a^2 + b^2$.

Для оцінки стійкості розробленого методу скористаємось методикою, описаною у п. 2.2.2. За цією методикою визначимо два числа x і k, які використовуються у розробленому методі.

Ці два числа можна вибрати $\wp(x, k) = (P - 3)^2$ способами. Це означає, що за $\wp(n)\cdot\chi(n)$ ітерацій можна розкрити закодоване повідомлення з сумісним використанням криптосистем Ель-Гамаля і RSA.

3.4.2. Кодування і декодування по двох рядках матриці зображення з додатковим зашумленням

Нехай задано P, Q – пару довільних простих чисел і число N, яке визначається за виразом (2.5).

Кодування відбувається поелементно з використанням наступного перетворення елементів матриці інтенсивностей кольорів зображення **C** (2.3):

1. Випадково вибирається натуральне число $d < \varphi(N)$ і знаходиться таке натуральне e, що виконується конгруенція (2.6).

2. Випадково вибирається натуральне число x, і k за умовами (3.32) і (3.33) відповідно.

3. За виразами (3.34) будуються чотири числа a, b, $a_{i,j}$, $b_{i,j}$.

4. Будується матриця закодованих значень інтенсивностей пікселів

5. Будується матриця закодованих значень інтенсивностей пікселів (2.19), елементи якої визначаються так

$$\begin{aligned} \tilde{c}_{i,j} &= ac_{i,j} - bc_{i+1,j} + a_{i,j} + f(i,j); \\ \tilde{c}_{i+1,j} &= ac_{i,j} + bc_{i+1,j} + b_{i,j} + g(i,j), \end{aligned} \tag{3.38}$$

де $f(i, j)$, $g(i, j)$ – деякі функції зашумлення, $1 \le i \le n$, $1 \le j < m$.

Декодування відбувається наступним чином:

Декодовані значення інтенсивностей пікселів отримуються з (3.38):

$$\begin{aligned} ac_{i,j} - bc_{i+1,j} &= \tilde{c}_{i,j} - a_{i,j} - f(i,j); \\ ac_{i,j} + bc_{i+1,j} &= \tilde{c}_{i+1,j} - b_{i,j} - g(i,j),\ 1 \le i < n,\ 1 \le j < m \end{aligned} \tag{3.39}$$

Тоді визначаються декодовані значення функції інтенсивності матриці **C** за виразами:

$$\begin{aligned} c_{i,j} &= \frac{\left(a\left(\tilde{c}_{i,j} - a_{i,j} - f(i,j)\right) + b\left(\tilde{c}_{i+1,j} - b_{i,j} - g(i,j)\right)\right)}{\delta}; \\ c_{i,j+1} &= \frac{\left(a\left(\tilde{c}_{i+1,j} - b_{i,j} - g(i,j)\right) - b\left(\tilde{c}_{i,j} - a_{i,j} - f(i,j)\right)\right)}{\delta}, \end{aligned} \tag{3.40}$$

де δ визначається подібно до (3.37).

3.4.3. Результати практичних експериментів

На основі описаних модифікацій RSA розроблено алгоритм кодування кольорових зображень в телекомунікаційних системах, який, подібно до методів описаних у п. 3.2, також реалізований в програмному рішенні, описаному у розділі 4. Використовуючи це програмне рішення, проведено практичні експерименти, результати яких наведено на рис. 3.13-3.17.

Рисунок 3.13 – Початкове зображення для кодування методом з п. 3.4

Параметри зображення є такими: l = 552 пікселів; h = 575 пікселів; формат – кольоровий в системі ARGB. Кодування здійснювалось при такій парі простих чисел P = 23, Q = 19.

На рис. 3.14-3.15 наведено результати використання практичної реалізації сумісного використання криптосистем RSA і Ель-Гамаля при кодуванні та декодуванні за одним рядком матриці інтенсивностей кольорового зображення (п. 3.4.1) , наведеного на рис. 3.13. Чисельні результати процедури кодування при використанні пари значень: P = 71, Q = 83 є такими: $PSNR(P, P')$ = 8.06, $L(P, P')$ = -22.06, $PSNR\ (P)$ = 14.64, $PSNR\ (P')$ = 6.38.

Порівняння початкового (рис. 3.13) і декодованого (рис. 3.15) зображення за метрикою (2.12) засвідчили відсутність інформаційних втрат в процедурі кодування/декодування (п. 3.4.1). Рівень зашумленості $L(P, P')$ та значення метрики $PSNR(P, P')$ є достатньо високими. Варто відзначити слабку появу структуризації (гармонійності) зображення, подібно до методу з п. 2.3.2.

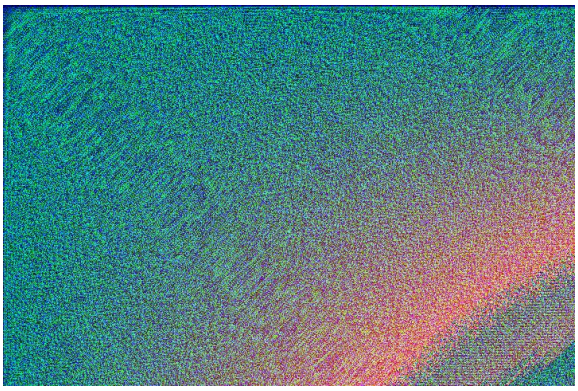


Рисунок 3.14 – Закодоване за одним рядком методом з п. 3.4.1 зображення, наведене на рис. 3.13

Рисунок 3.15 – Декодоване за одним рядком методом з п. 3.4.1 зображення

Гістограми оригінального (рис. 3.13) та закодованого (рис 3.14) зображень наведені в додатках на рис. Д1.18 та Д1.19 відповідно. З порівняння гістограм

отримуємо висновок про те, що сумісне використанні криптосистем Ель-Гамаля та RSA має стискуючу дію на гістограму. Визначальним для розробленого методу є те, що повна зашумленість зображення (рис. 3.12) досягається при дуже малих значення пари простих чисел чисел P і Q.

На рис. 3.16, 3.17 наведено результати використання практичної реалізації сумісного використання криптосистем RSA і Ель-Гамаля при кодуванні та декодуванні вже за двома рядком матриці інтенсивностей кольорового зображення (п. 3.4.2), наведеного на рис. 3.13.

Чисельні результати процедури кодування при використанні пари значень: $P = 71$, $Q = 83$ є такими: $PSNR(P, P') = 8.67$, $L(P, P') = -22.07$, $PSNR\ (P) = 14.64$, $PSNR\ (P') = 6.44$.

Використання метрики (2.12) засвідчили, що й у випадку методу, описаного у п. 3.4.2, відсутні інформаційні втрати.

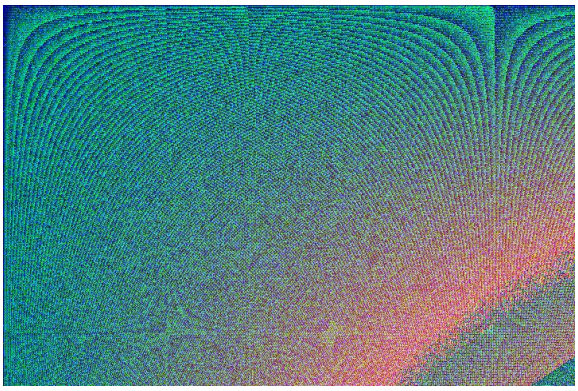


Рисунок 3.16 – Закодоване за двома рядками методом з п. 3.4.2 зображення, наведене на рис. 3.13

Рисунок 3.17 – Декодованеза двома рядками методом з п. 3.4.2 зображення

Значення пари P і Q були навмисно вибрані ті самі, що й у випадку методу з п. 3.4.1. При порівняння результатів, наведених на рис. 3.12 і 3.14, можна побачити у чисельному вимірі не суттєве зростання рівня зашумленості $L(P, P')$ та

значення метрики $PSNR(P, P')$ методу, описаного у п. 3.4.3, у порівнянні з методом описаним у п. 3.4.2. Але тут треба брати до уваги те, що у в останньому випадку використовувались меньші значення P і Q. При цьому контури повністю зникали. Тобто властивість додаткого зашумлення привносить у чисельному розумінні вищий рівень зашумленості при однакових значеннях P і Q. Отже, використання додаткового зашумлення в методі, що базується на поєднанні криптосистем Ель-Гамаля та RSA, дає можливість забезпечити нівелювання контурів на закодованому зображенні при менших значеннях P і Q.

Зауважимо, що при кодуванні з додатковим зашумленням (метод з п. 3.4.2) структурна характеристика (гармонійність, фрактальність) закодованого зображення суттєво зростає в залежності від вибору структури оператора зашумлення і порядку вибору пікселів вхідного зображення. Ця властивість може бути використана в топологічній модифікації алгоритму кодування/декодування.

Основним недоліком використання додаткової зашумленості є зростання операційних витрат (зокрема оперативної пам’яті) в процедурах кодування зображень.

Обидві запропоновані модифікації криптографічного кодування зображень, засновані на сумісному використанні криптосистем RSA і Ель-Гамаля, призначені для кодування кольорових зображень. Проте вони можуть бути використані для організації захисту будь-яких зображень, у тому числі і напівтонових.

На відміну від спеціалізованих для напівтонових зображень методів, які описані у розділі 2, у випадку використання методів, описаних у п. 3.4, будуть більшими обчислювальні витрати, але меншими витрати оперативної пам’яті.

Реалізація стійкості модифікованих і описаних у п. 3.4 алгоритмів визначається стійкістю двох використаних алгоритмів - Ель-Гамаля та RSA і з одночасним забезпеченням якості зображення не вимагають значних обчислювальних ресурсів.

Висновки до розділу 3

1. Запропоновані у розділі 3 методи криптографічного кодування призначені для забезпечення функціональної безпеки в автоматизованих системах критичного застосування, у яких основним інформаційним об'єктом виступають кольорові зображення. Їх визначальною характеристикою є високий рівень криптографічного кодуванняає при незначному зростанні часових та обчислювальних витрат в процедурах забезпечення безпеки функціонування автоматизованих систем.

2. Запропоновані методи можуть бути використані стосовно будь-якого типу зображень, але найбільші переваги досягаються у випадку використання кольорових зображень, які дозволяють чітко виділяти контури.

3. Мінімальна стійкість до несанкціонованого декодування у розроблених модифікаціях забезпечується алгоритмом RSA.

4. Використання бінарних операцій забезпечує нівелювання проблеми контурів на закодованому зображенні вже при значення простих чисел в околі 100. При цьому цей алгоритм при мінімальних видозмінах може бути використаний стосовно будь-якого типу зображень.

5. Використання побітових операцій дало можливість в задачі організації захисту кольорових 3-х та 4-х байтових зображень поєднати симетричні та асиметричні схеми кодування та декодування. Завдяки цьому поєднанню вдалось понизити мінімальний рівень значень простих чисел, при якому повністю зберігаються повна зашумленість і рівень криптозахисту системи RSA.

6. Сумісне використання криптосистем Ель-Гамаля і RSA забезпечило при мінімальних значеннях простих чисел стійке криптографічне кодування і повну зашумленість будь-яких кольорових зображень. Основною характеристикою цієї модифікації є повна інваріантність процедур кодування/декодування від типу зображення при несуттєвому зростанні обчислювальної складності.

РОЗДІЛ 4. ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДВИЩЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ЇЇ ПРОГРАМНА РЕАЛІЗАЦІЯ ДЛЯ ПРОЕКТУВАННЯ ТА ПОБУДОВИ АВТОМАТИЗОВАНИХ СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ

Четвертий розділ дисертаційних досліджень присвячений розробленню інформаційних технологій підвищення функціональної безпеки [46] при передаванні вмережевими каналами напівтонових та кольорових зображень та реалізації цих технологій в мережевому програмному рішенні.

4.1. Структура інформаційної технології підвищення рівня функціональної безпеки в автоматизованих системах управління критичного застосування

Загальна структура інформаційної технології забезпечення підвищення функціональної безпеки для випадку напівтонових та кольорових зображень наведена на рис. 4.1.

Структура технології подається у вигляді таких послідовних етапів:

#Зображення – етап введення в систему зображення. Джерелом зображення може бути будь-який інформаційний контейнер: файл, цифровий фотоапарат, відеокамера, порт мережі.

#Визначення типу зображення – етап, який призначений для визначення параметрів вибору найбільш оптимального алгоритму кодування. Параметрами вибору алгоритму виступають: вид зображення і параметри обчислювального та мережевого середовищ.

#Вибір алгоритму – етап, який призначений для вибору найбільш ефективного алгоритму (практичної реалізації методу) кодування вхідного зображення. Результати вибору алгоритму повинні бути відомі приймаючій стороні. Саме для цього на схемі (рис. 4.1) відображений окремий комунікаційний

сеанс, який зазвичай здійснюється відкритими каналами. Треба відзначити, що вибір методу може стати додатковим засобом захисту, але у цьому випадку результати вибору алгоритму повинні передаватись приймаючій стороні у спосіб, захищений від несанкціонованого доступу.

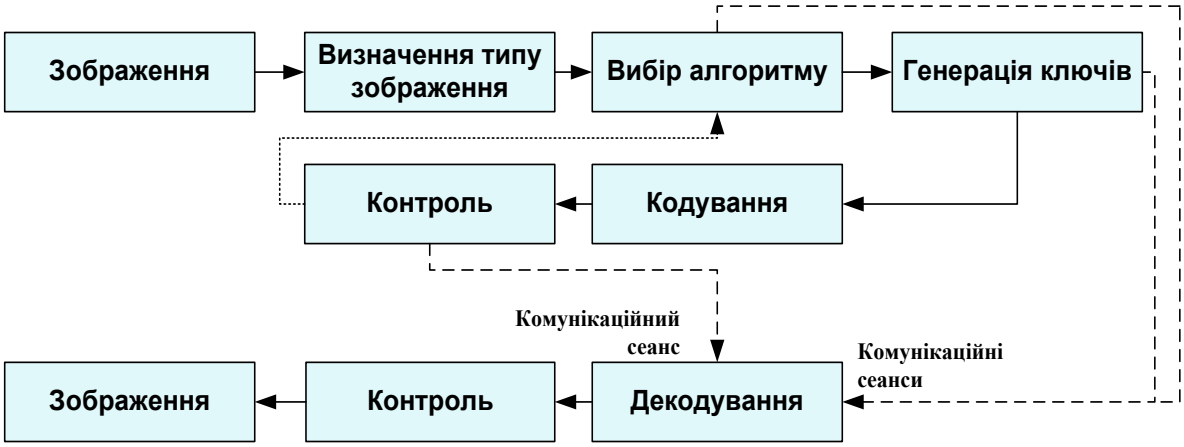


Рисунок 4.1 – Загальна структура інформаційної технології підвищення рівня функціональної безпеки для випадку передавання мережевими каналами автоматизованих системах критичного застосування напівтонових та кольорових зображень

#Генерація ключів – етап, який призначений генерації параметрів процедури кодування, зокрема ключів кодування та операторів додаткового зашумлення, якщо останні за обраним алгоритмом присутні у цій процедурі. Окрім генерації ключів на цьому етапі реалізовується обмін відкритими ключами між обчислювальними клієнтами мережевого середовища. Параметри мережевого сеансу для обміну ключами може відрізнятись від сеансу обміну закодованими повідомленнями. Найбільш типовим є обмін ключами по відкритому протоколу, оскільки відкриті ключі зазвичай не використовуються як засоби криптографічної атаки.

#Кодування – етап, на якому практично реалізовується процедура кодування за обраними алгоритмом та параметрами.

#Контроль – етап, на якому здійснюється перевірка результатів кодування на предмет збереження контурів. Така перевірка може здійснюватись візуально, або програмними детекторами контурів. У випадку збереження контурів на закодованому зображенні необхідно повернутись на етап #Вибір алгоритму або #Генерація ключів. Якщо результати контролю є задовільними, тобто контури не проявились на закодованому зображення, то розпочинається відкритий комунікаційний сеанс. У цьому сеансі закодоване зображення передається приймаючій стороні.

#Декодування – це етап приймаючої сторони, на якому за закритим ключем і вибраним алгоритмом кодування відбувається процедура декодування.

#Зображення – це також етап приймаючої сторони, на якому декодоване зображення розміщується у інформаційному контейнері приймаючої сторони.

Характерною особливістю описаної технології є наявність принаймні трьох комунікаційних сеансів. Мережі процедури забезпечення комунікаційних сеансів у наведеній технології не описуються, оскільки пропонується використовувати стандартні мережеві протоколи сім'ї TCP/IP.

Усі комунікаційні сеанси можуть реалізовуватись відкритими каналами, оскільки стійкість розроблених алгоритмів до несанкціонованого доступу є достатньою. Проте використання захищених каналів лише підвищить стійкість до атаки на зображення, яке захищається.

Але тут треба відзначити наступне. Комунікаційні сеанси є одним із найбільш вразливих з точки зору атаки місць в процесах захисту зображень, оскільки у кожному з них (а насамперед у перших двох) може бути витік інформації для атаки на сам процес. Відповідно зменшення сеансів призводить до мінімізації витоків інформаційних даних для організації атаки. Для цього пропонується варіант технології із двома телекомунікаційними сеансами, який наведено на рис. 4.2.

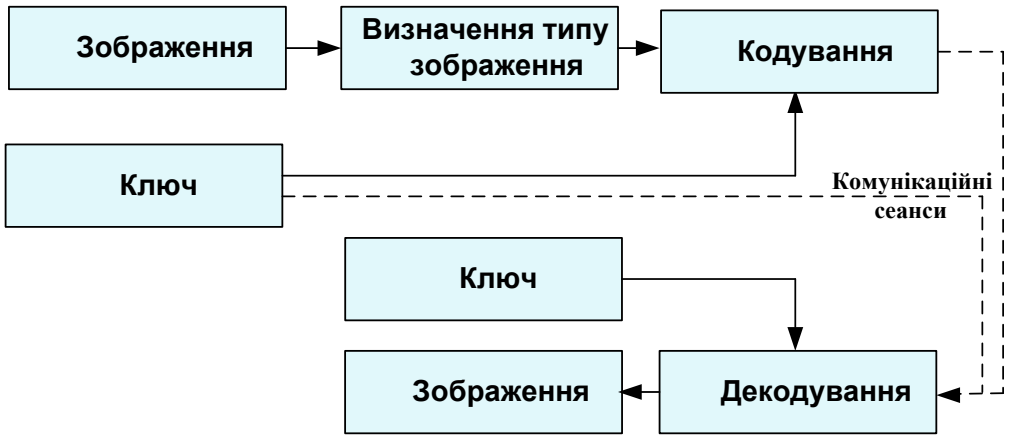


Рисунок 4.2 – Структура спрощеної інформаційної технології підвищення рівня функціональної безпеки для випадку передавання мережевими каналами автоматизованих системах критичного призначення напівтонових та кольорових зображень

У цій технології відсутній етап вибору алгоритму, оскільки сам алгоритм може бути обраний наперед, або тип алгоритму може передаватись у закодованому зображенні прихованими способами (записаний стеганографічними засобами). Тут треба пам’ятати, що використання приховування, у більшості випадків, призведе до інформаційних втрат різного ступеня. А це може бути неприйнятним для автоматизованих систем, що базуються на інтелектуальному аналізі зображень. Для таких систем навіть мінімальні інформаційні втрати можуть бути критичними для успішного їх функціонування.

4.2. Архітектура програмного рішення

У рамках дисертаційних досліджень розроблено два програмних рішеннях. Перше з них – це дві бінарні динамічні бібліотеки (crypto# та image determination), які, відповідно, містять набори функцій, що реалізовують:

- алгоритми криптографічного кодування, побудовані на основі розроблених в

дисертації методів (бібілотека – crypto#);

- алгоритми автоматичного детектування параметрів зображень, контурів, оцінки защумленості та різноманітні метрики (бібліотека – image determination).

Друге програмне рішення – це мережевий додаток, який є побудований як примітив системи, архітектура якої наведена на рис. 4.3.1 і використовується для ілюстрації та оцінки роботи алгоритмів захисту зображень в комунікаційних сеансах автоматизованих систем.

Обидва програмні рішення практично реалізовані для операційної платформи Windows. Але основним фреймворком розробки використовувалось інструментальний засіб QT Creator з використаннями технологій програмування [119]. Тому можна вважати, що кросплатформеність на рівні вихідного коду є забезпечена.

Практичний інтерес для розробки автоматизованих систем критичного застосування становить бібліотека, яка містить функції реалізації алгоритмів захисту. Тому основна увага в описі програмного рішення буде зосереджена на бібліотеці crypto.dll.

4.2.1. Структура бібліотеки криптографічного кодування

Як вже відзначалось, процедури криптографічного кодування зображень в телекомунікаційних сеансах автоматизованих систем реалізовані у форматі динамічної бібілотеки за інструментальними засобами і технологіями, описаними у [18, 93]. Такий підхід забезпечує простоту:

- оновлення програмних реалізацій розроблених алгоритмів криптографічного кодування;
- розширення набору бібліотеки функціями, які є реалізаціями нових методів криптографічного кодування.

Для забезпечення цього усі функції бібліотеки мають єдиний інтерфейс, який складається із

- вказівника на зображення у форматі цілочисельної матриці виду (2.3) або (3.4).
- вказівника на область даних, які є параметрами процедур кодування та декодування.

Програмно бібліотека crypto# складається із набору dll файлів, ім'я яких починається із слова crypto, а символ # визначає номер процедури кодування та відповідної їй процедури декодування.

Усі dll-файли реалізовують багатопотокову архітектуру, наведену на рис. 4.3. Мінімальний набір функцій, які реалізовують цю архітектуру, наведено у табл. 4.1. При цьому, імена функцій у всіх файлах бібліотеки є однаковими, що забезпечує існування єдиного програмного інтерфейсу. Такий інтерфейс дає можливість організовувати підтримку технології plug-in в автоматизованих системах, які будуть використовувати цю бібліотеку.

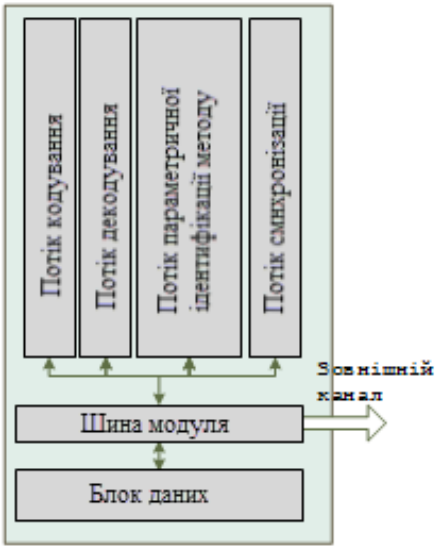


Рисунок 4.3 – Багатопотокова архітектура періоду виконання модулів криптографічного кодування бібліотеки crypto#

Особливістю обраної архітектури є можливість незалежного функціо-

нування потоків кодування та декодування. Усе інформаційне забезпечення цих процедур надається потоком параметричної ідентифікації.

Таблиця 4.1.

Мінімальні набори функцій, які реалізовують функціонали паралельних потоків архітектури, наведеної на рис. 4.3.

Потік кодування		**Потік декодування**	
Базова функція потоку	`thread_encrypt`	Базова функція потоку	`thread_decrypt`
Кодування	`encrypt#`	ДеКодування	`decrypt#`
Внутрішня міжпотокова комунікація	`set_message`	Внутрішня міжпотокова комунікація	`set_message`
	`get_message`		`get_message`
Потік параметричної ідентифікації		**Потік синхронізації**	
Базова функція потоку	`thread_ident`	Базова функція потоку	`thread_sync`
Визначення додаткових параметрів кодування/декодування	`encrypr_ident`	Внутрішня та зовнішня синхронізації	`internal_sync`
	`decrypr_ident`		`external_sync`
Внутрішні комунікаційні функції	`set_message`	Внутрішні комунікаційні функції	`set_message`
	`get_message`		`get_message`

Узгоджене функціонування потоків dll-бібілотеки забезпечується потоком синхронізації, спільною комунікаційною шиною та глобальним блоком даних.

Комунікаційна шина реалізована у вигляді черги повідомлень з пріоритетом. Внесення повідомлень в чергу та їх вибірка здійснюється потоками через функції `set_message/get_message`, використовуючи механізм користувацького атомарного доступу до черги.

Усі синхронізаційні дії з використанням комунікаційної шини виконує потік синхронізації. Він же забезпечує зовнішню комунікацію, яка складається із:

- приймання із зовнішніх програмних модулів зображень та параметрів

процедур кодування/декодування;

- передавання зовнішнім модулям результатів роботи процедур кодування/декодування.

4.2.2. Архітектура програмного примітиву однорангової автоматизованої системи

Система будувалась на основі модульного принципу. Кількість модулів є фіксованою. Їх структура, за винятком модуля захисту, є подібною.

Модуль захисту призначений для реалізації прикладних задач. Його спроектовано і розроблено за схемою динамічного наповнення функціональностями, реалізованими у форматі бінарного коду.

Така структура визначає програмне рішення як деяку оболонку для підмикання та реалізацій процедур кодування та декодування цифрових зображень, які визначені у форматах jpeg, tiff, gif, pcx та bmp. Зазначимо, що у загальному випадку вхідним може бути будь-який файл. Система дасть змогу здійснити над ним процедури кодування та мережеві транзакції.

Програмний засіб має вигляд зовнішньої програми, яка виконується в середовищі операційної системи окремим процесом. Така організація програмного засобу має свої переваги і недоліки. Перевагами є те, що:

- програмий модуль є незалежним від графічного середовища користувача, що дає змогу відлагоджувати програмний модуль незалежно від середовища;
- можна під’єднати один програмний модуль до декількох середовищ (програм) різного призначення;
- організовувати обробку в командному режимі без спеціально інтегрованого середовища;

Крім переваг, організація програми у вигляді окремого програмного модуля має і недоліки:

- ускладнений обмін між інтегрованим середовищем та програмою – обмін відбувається переважно через файли або мережеві канали;
- слабкий зв'язок інтегрованого середовища та тематичної програми ускладнює керування. Керування зводиться до запуску програми, передавання їй параметрів та аналізу результатів роботи.

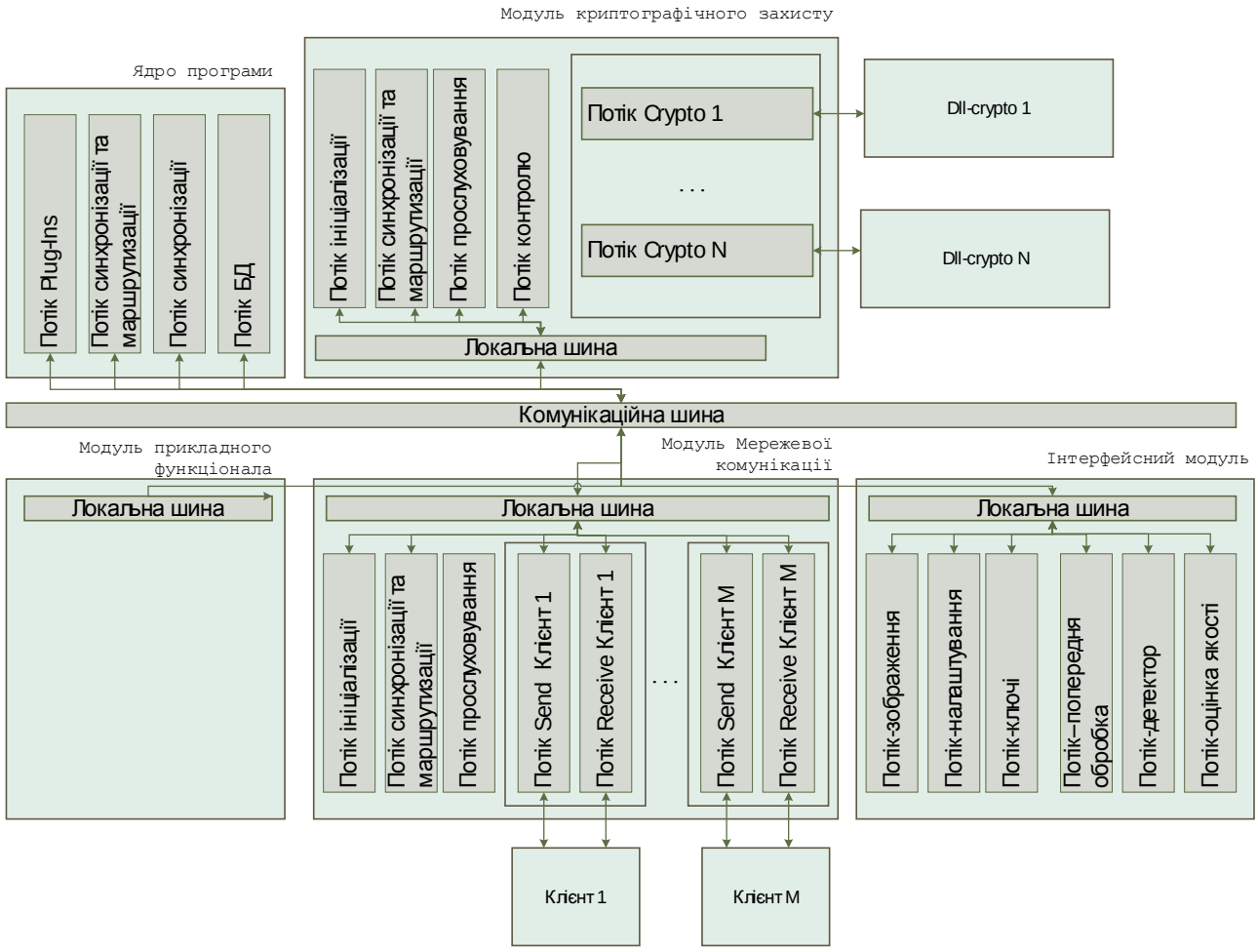


Рисунок 4.4 – Архітектура програмного засобу реалізації примітиву однорангової автоматизованої системи із захищеною комунікацією

Зазначимо, що система дає змогу працювати з багатьма вікнами одночасно (MDI-архітектура) та має дружній інтерфейс для управління всіма модулями.

Робота програмного забезпечення відбувається в режимі часу, наближеного

до реального. Витрати на роботу процедур кодування та декодування визначаються насамперед справжніми розмірами зображень та пропускною здатністю мережевих сеансів на фізичному рівні комунікаційних каналів.

Можливість візуалізації кінцевого результату дає змогу контролювати обчислення в процесі роботи.

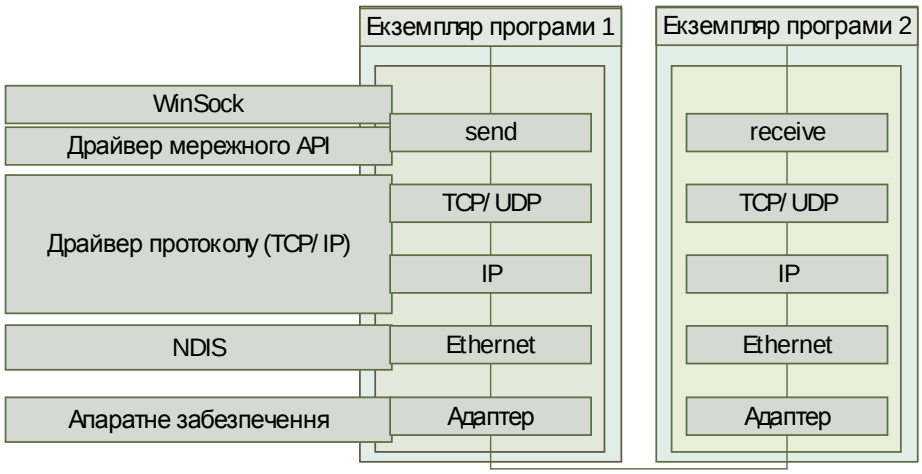


Рисунок 4.5 – Архітектура мережевої підтримки та схема мережевої взаємодії екземплярів програми. Позначення: send, receive – мережеві примітиви; TCP, UDP – мережеві протоколи обміну інформації; IP – транспортний драйвер; NDIS (Network Driver Interface Specification) – специфікація інтерфейсу мережевого драйвера

Структурно програмне забезпечення складається з ядра програми та трьох модулів: модуля кодування, комунікаційного модуля та модуля введення-виведення й користувацьких інтерфейсів.

Кожен з трьох модулів програми відповідає за виділені для нього задачі, зокрема кодування/декодування, відображення, збереження та мережевого передавання/приймання.

На рис. 4.6 наведено схему етапів роботи програмної системи для реалізації

процедур криптографічного кодування в телекомунікаційному сеансі. Зазначимо, що за наведеною схемою кодування зображень передбачає функціонування користувацьких потоків відокремлених модулів системи. В окремих випадках, наприклад, на етапі криптографічних обчислень, завдання виконується декількома користувацькими потоками.

Схему синхронізації роботи потоків, які реалізують етапи, що наведені на рис. 4.6, переважно виконують механізми повідомлень системи та об'єкти ядра операційного середовища. Останній спосіб доволі поширений і визначається потребами забезпечення повторного використання потоку. Це означає, що користувацький потік завершує свою роботу лише за командою ядра програмного рішення.

Повторне використання потоків дає можливість мінімізувати обчислювальні витрати, пов'язані із системними процедурами створення та знищення потоків та програмними – формування структур даних і підмиканням процедур синхронізації.

Потік, який очікує на повторне виконання, відмикається від планування потоковим менеджером операційної системи, а тому не витрачає жодних ресурсів до моменту його повторного запуску. Повторний запуск за допомогою об'єкта ядра повторно підмикає потік до планування, що допомагає активізувати потік і вирішувати специфічні для нього завдання.

У випадку розпаралелювання процедур кодування роботу потоків синхронізують за технологією спін-блокування на основі функцій атомарного доступу операційної системи Windows.

На кожному етапі здійснюється повна діагностика результатів математичних обчислень і стану потоку виконання. Усі діагностичні та критичні результати агрегує ядро програми для вироблення реакції на них. Такий підхід забезпечує реалізацію механізму, стійкого до технічних, алгоритмічних і функціональних

збоїв функціонування програмного рішення на етапі виконання програми.

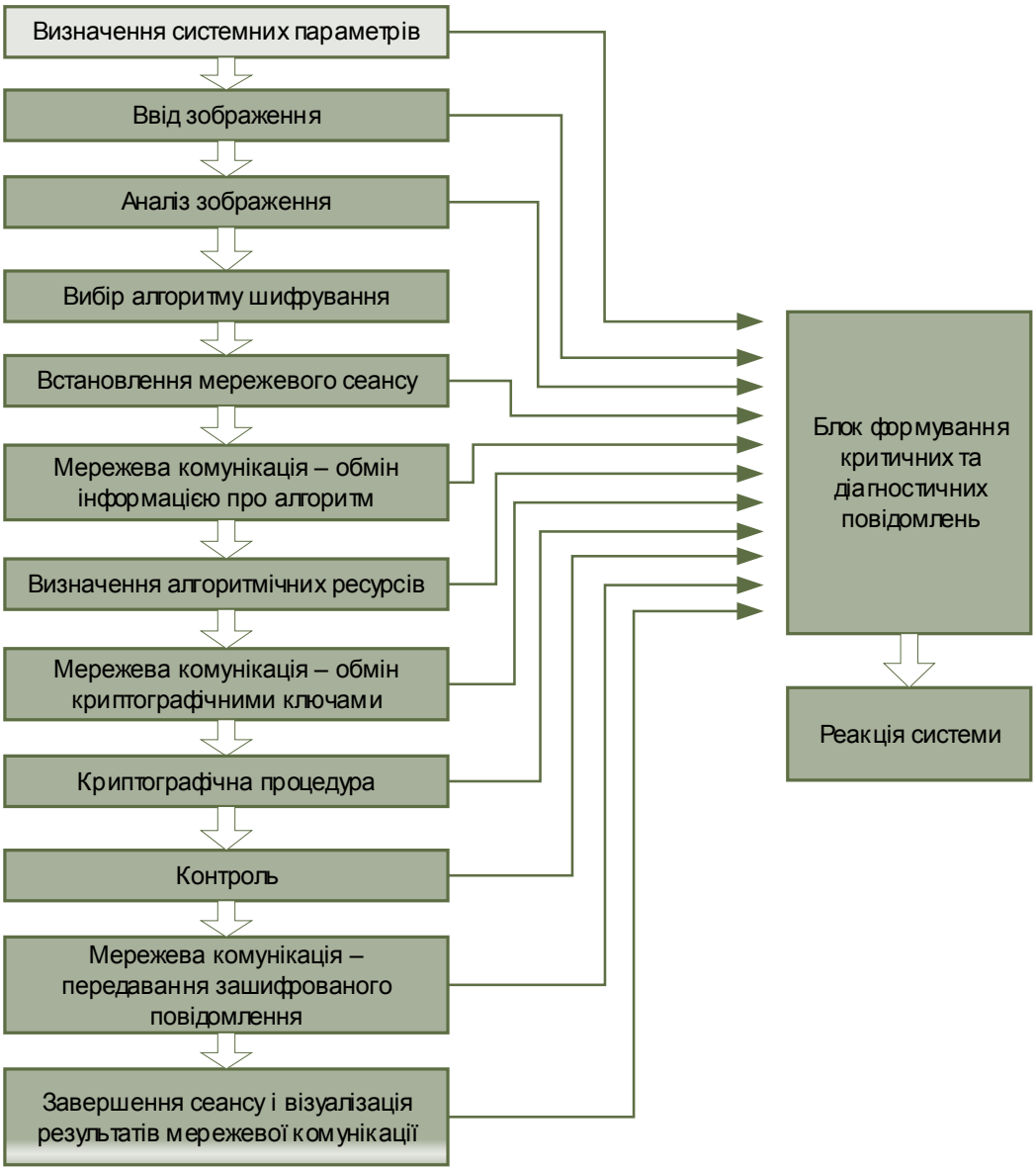


Рисунок 4.6 – Архітектура програмного засобу реалізації примітиву однорангової автоматизованої системи із захищеною комунікацією

4.3. Архітектура автоматизованих систем управління критичного застосування з реалізацією інформаційної технології підвищення рівня функціональної безпеки

Розроблене у вигляді мережевого прикладного додатку з використанням

технології plug-ins програмне рішення призначене для організації:

- персоніфікованого захисту зображень;
- захищеного обміну зображення в телекомунікаційних сеансах.

Проте використання формату динамічної бібліотеки надає можливість використання програмної реалізації криптографічних алгоритмів в процесах розроблення і експлуатації складніших обчислювальних структур, а саме автоматизованих систем, і у першу чергу, критичного призначення.

Підсистема захисту інформаційних потоків є складовою усіх сучасних автоматизованих систем. Проте, у випадку використання телекомунікаційних сеансів небезпека несанкціонованого витоку інформації зростає завдяки можливості атаки в процесах мережевих транзакцій. Відповідно зростає актуальність завдання забезпечення безпеки функціонування мережевих автоматизованих систем.

4.3.1. Системи без виділеного сервера

На рис. 4.7 наведено схема реалізації технології захисту зображень в автоматизованій системі без виділеного сервера. Типовим прикладом таких систем є медичні інофрмаційно-управляючі системи реалізовані в рамках технології Smart House. Визначальним в архітектурі таких систем є їх автономне функціонування без зовнішніх виділених керуючих систем. Мережеві транзакції в таких системах здійснюються лише у випадках виклику зовнішніх дій, синтезу зворотних реакцій та при виконанні синхронізаційних дій.

Автономність функціонування автономних однорангових систем визначає наявність персональних БД на кожному обчислювальному пристрої. Відповідно до цього стає актуальною задача персоніфікованого захисту зображень (наприклад зображень людини для віддаленого діагностування та визначення критичних ситуацій) на окремому комп’ютері. Так задача, у першу чергу, розв’язується засобами авторизації локальної БД. Використання засобів криптографічного

кодування дає змогу суттєво посилити цей захист, оскільки у файлах з бази даних будуть зберігатись закодовані зображення. У випадку, якщо у якості локальної БД не використовується система із авторизованим доступом, то криптографічне кодування залишається єдиним способом захисту від несанкціонованого витоку інформації. На рис. 4.7 персоніфікований захист відображено лише позначенням “Персоніфікована БД”.

Більшість сучасних однорангових автоматизованих системи з різних причин використовують мережеві комунікаційні засоби. Серед цих причин, у першу чергу, може бути необхідність використання зовнішніх систем:

- віддаленого глибокого інтелектуального аналізу;
- протоколювання і трекінгу;
- управління і прийняття рішень.

У випадках використання таких зовнішніх систем неминуче виникає задача передавання зображення. Оскільки, зазвичай, існує лише комунікаційний канал, то у більшості випадків мережеві транзакції здійснюються відкритими каналами. Відповідно криптографічне кодування залишається єдиним засобом захисту від мережевого перехоплення конфіденційної інформації.

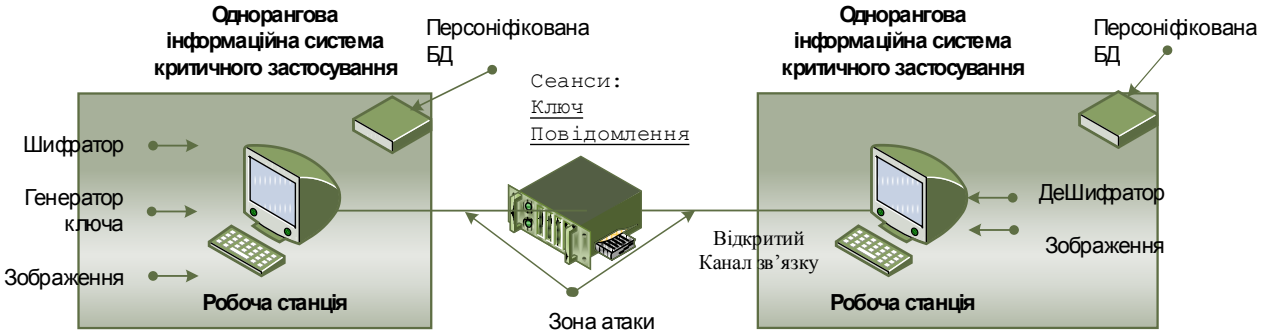


Рисунок 4.7 – Схема реалізації технології захисту в одноранговій мережевій автоматизованій системі

Розроблене програмне рішення разом із бібліотекою захисту є прототипом саме однорангових автоматизованих систем. Бібліотека функцій захисту може бути використана для розробки програмного модуля мережевого захисту і кодувати усі повідомлення, що передаватимуться в комунікаційні порти.

Особливістю цього підходу є відокремленість агента від самої системи. Це має свої переваги, оскільки такий модуль є стійким до збоїв самої системи і забезпечує захист для будь-яких комунікаційних сеансів.

Недоліком відокремленого програмного модуля є складність забезпечення персоніфікованого захисту в локальній БД системи. Тому пропонується криптографічний програмний модуль імплементовувати в саму систему і відокремлювати від решти задач (в тому числі і мережевих), які вирішуються в системі. Такий підхід забезпечуватиме максимальну незалежність роботи модуля, а також можливість оновлення алгоритмів захисту без необхідності перебудови системи вцілому.

4.3.2. Системи з виділеним сервером

На противагу від однорангових системи із виділеним сервером визначаються зовнішнім управлінням і будуються в рамках архітектури “клієнт-сервер”. У відповідності до цієї архітектури існують дві типові реалізації таких систем.

За першою реалізацією клієнтські машини характеризуються достатньо вузьким прикладним функціоналом на основі рішень, які виробляються керуючою машиною.

За другою реалізацією керуюча машина відіграє роль типового файл сервера. Усі керуючі рішення виробляються на машинах-клієнтах при мінімальних експертних оцінках, здійснених на керуючій машині.

Обидві реалізації породжують достатньо інтенсивний мережевий трафік, що, у свою чергу, робить залежним ефективне функціонування систем від стійкості роботи мережевих підсистем і збільшує вразливість самих систем до

зовнішніх атак.

На рис. 4.8. наведено загальну схему реалізації інформаційної технології захисту зображень в системах, побудованих за архітектурою “клієнт-сервер”.

На відміну від випадку однорангових, у системах, побудованих за архітектурою “клієнт-сервер”, може існувати єдина віддалена БД. Така БД розміщується на керуючій машині і повинна використовуватись у якості сховища даних для уже закодованих зображень.

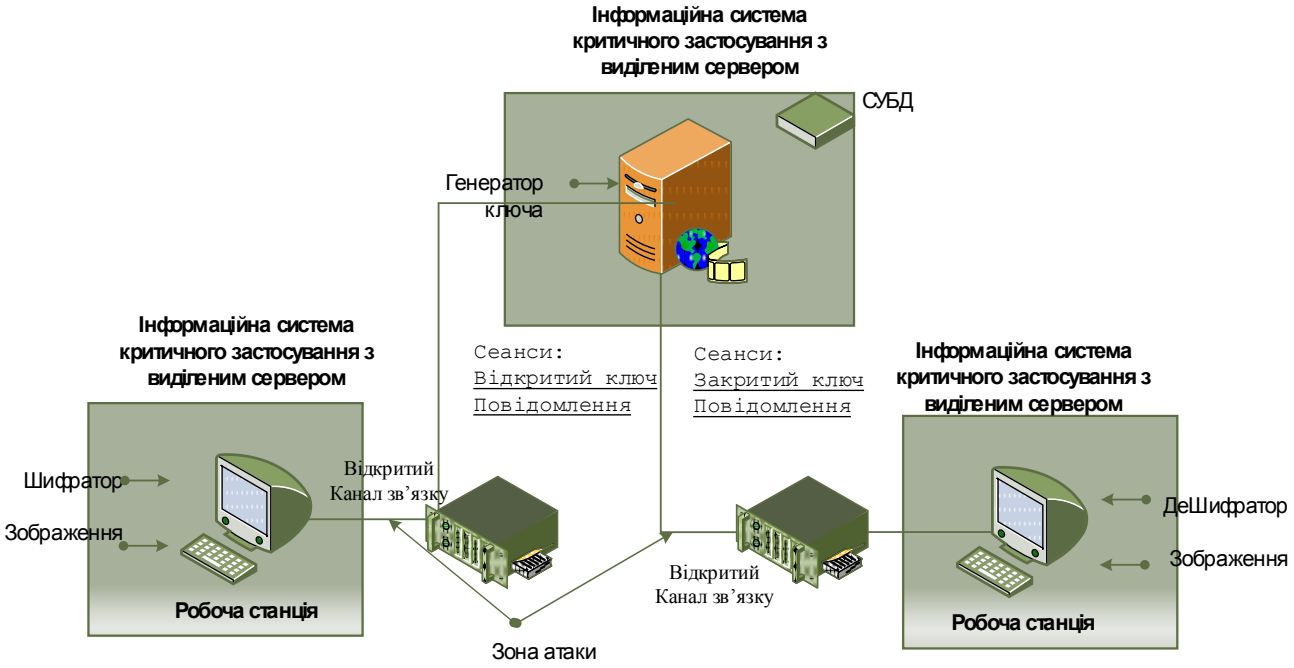


Рисунок 4.8 – Схема реалізації технології кодування зображень в мережевій автоматизованій системі з виділеним сервером

Процедури кодування та декодування повинні відбуватись на машинах-клієнтах і по відкритих комунікаційних каналах повинні передаватись результати їх роботи. Це означає, що програмні модулі криптографічного кодування повинні бути інтегровані в саму систему, зокрема у ту її частину, яка встановлюється на машинах-клієнтах.

Криптографічний програмний модуль, окрім процедур кодування та декоду-

вання, повинен реалізувати вибір алгоритму кодування та контроль результатів його роботи.

Серед завдань забезпечення функціональної безпеки керуючої машини є підтримка процедури генерації та обміну ключів процедур кодування. Такий підхід дозволяє централізувати інформацію, яка необхідна для успішного декодування зображення на будь-якій клієнтській машині.

Розвитком систем, архітектура яких наведена рис. 4.8, є розподілені автоматизовані системи. Для використання програмного модуля криптографічного захисту пропонується схема система, яка наведена рис. 4.9.

Визначальною характеристикою розподілених систем є не наявність зовнішньої керуючої машини, а масштабованість системи вцілому. Для забезпечення цієї масштабованості в розподіленій системі може існувати декілька зовнішніх управляючих машин. Усі вони призначені для виконання різних задач: від розподіленого зберігання інформації до вироблення і виконання вузько спеціалізованого прикладного функціоналу.

Однією із таких машин пропонується зробити сервер, криптогафічного кодування. Його основним завданням є забезпечення безпеки циркулювання інформації в цілій системі. Для вирішення основного завдання сервер повинен розв’язувати задачі:

- авторизації;
- сертифікації;
- генерації ключів;
- інформаційного забезпечення процедур декодування при розподіленому зберігання інформації.

Для забезпечення успішного розв’язання наведених задач цей сервер повинен бути відокремлений від прямого доступу з машин-клієнтів. Таке архітектурне рішення дає можливість зменшити витрати на закриті комунікаційні канали

і централізувати інформаційне забезпечення для успішного декодування зображення на будь-якому клієнті системи.

Централізація інформації на так званих серверах ресурної концентрації є необхідним завданням, оскільки, зазвичай, розподілене сховище даних вирішує лише завдання зберігання і забезпечення цілісності даних. У відповідності до цього необхідним для повноцінного функціонування системи є виокремлене існування сервісів захисту.

Сегментація системи, наведеної на рис. 4.9, передбачає існування окремих мережевих ділянок системи. З одного боку, ці ділянки повинні бути максимально самодостатні з точки зору прикладного функціоналу. З іншого – ці ділянки є складовими усієї системи, в яких будуть існувати міжсегментні комунікації. Тому до завдань криптографічного програмного модуля на сервері концентрації буде відноситись забезпечення стійкості до несанкціонованої атаки не тільки у внутрішньо сегментних комунікаціях, а й в комунікаційних сеансах між сегментами. В окремих системах розв’язання останнього завдання може мати більшу вагу за розв’язання першого. Це пояснюється тим, що комунікаційні канали в межах одного сегменту системи можуть бути захищені сторонніми засобами. Наприклад, засобами мережевої комунікації. В межах цілої розподіленої системи забезпечити такий тип каналів по усіх ділянках системи майже ніколи не вдається. Особливо це стосується тих розподілених систем, сегменти яких територіально рознесені на великому масштабі. У цьому випадку криптографічний програмний модуль залишається єдиним засобом захисту інформації в мережевих транзакціях по відкритих каналах.

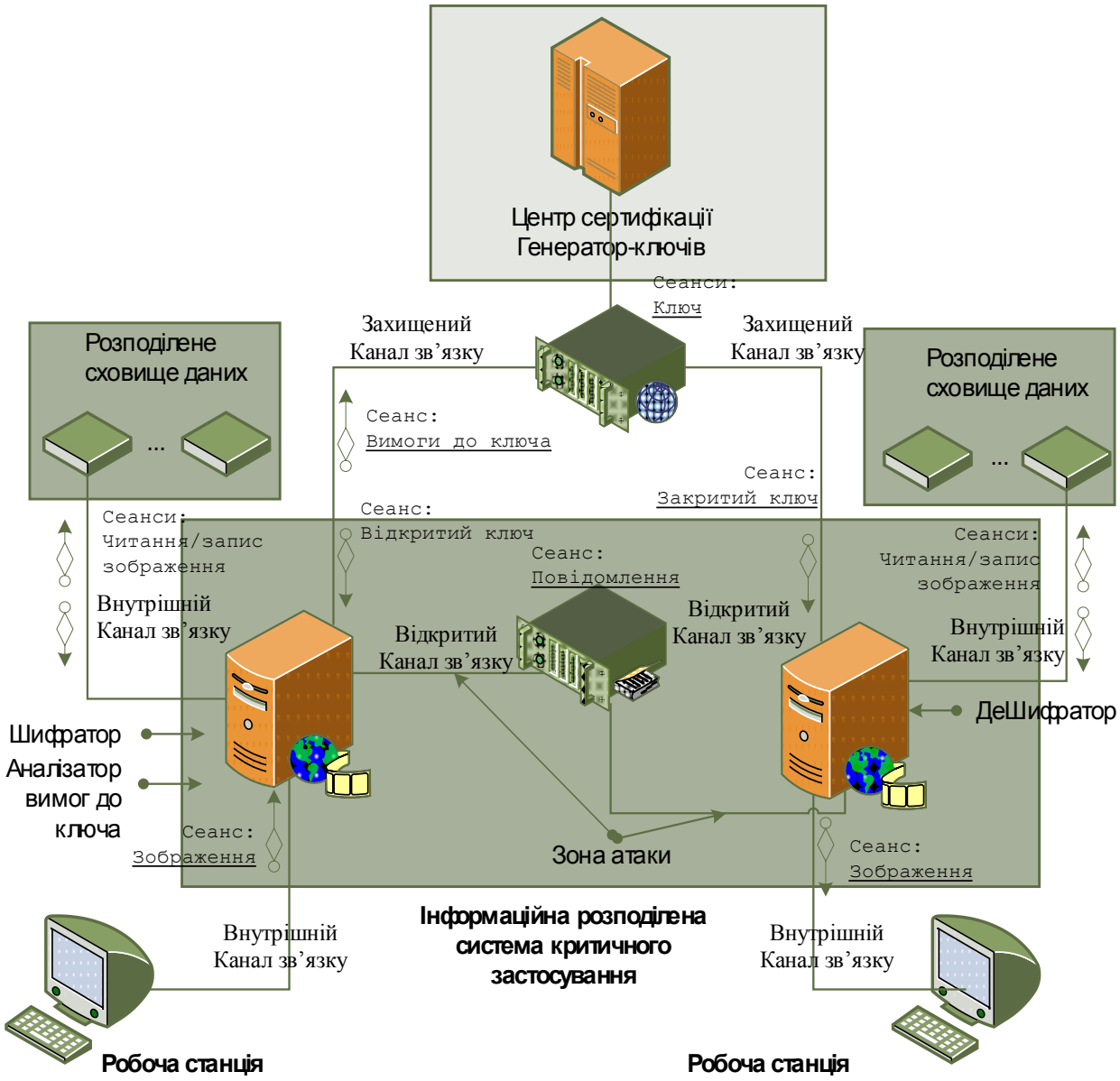


Рисунок 4.9 – Схема реалізації технології кодування зображень в розподіленій автоматизованій системі

У розподілених автоматизованих системах програмне забезпечення серверів є строго спеціалізованим за функціоналом системи і дуже рідко надає програмні сервіси, які не пов'язані із цим функціоналом. Тому жодної переваги немає форма реалізації криптографічного програмного модуля. Іншими словами - не має

принципового значення реалізація агента у формі окремого сервісу операційного середовища, який контролює мережеві ресурси комп'ютера, чи у вигляді модуля автоматизованої системи, який контролює мережеві порти лише автоматизованої системи. В обидвох випадках і з однаковою ефективністю криптографічний програмний модуль зможе вирішити основні завдання. Але тут треба зазначити, що у першому випадку кількість ресурсів контролю теоретично може бути набагато більшою, ніж у другому випадку. Відповідно обчислювальна завантаженість агента, реалізованого у вигляді сервісу операційного середовища, може бути набагато більшою, ніж у реалізації його у формі сервісу автоматизованої системи.

Висновки до розділу 4

1. Розроблено інформаційну технологію прогрманого модуля, який призначений для криптографічного кодування напівтонових та кольорових зображень телекомунікаційних сеансах автоматизованих систем критчного призначення.

2. Розроблене у форматі динамічної бібліотеки програмне рішення криптографічного кодування зображень, може бути використане як для організації персонального захисту, так і для модульних систем забезпечення функціональної безпеки, які інтегруються в автоматизовані системи обробки інформації критичного застосування.

3. Використання формату динамічної бібілотеки і єдиних програмних інтерфейсів дає можливість динамічно розширювати набір функцій криптографічного кодування новими алгоритмами без необхідності перероблення систем вцілому.

4. Виокремлені класи мережевих автоматизованих систем можуть мати захищені комунікаційні сеанси для передавання будь-якої інформації, у тому числі зображень.

ВИСНОВКИ

У дисертаційній роботі розв’язано актуальну науково-прикладну задачу, яка полягає у розробці інформаційної технології підвищення функціональної безпеки інформаційно-управляючих систем критичного застосування, які базуються на комунікаційних процедурах із застосуванням універсальних засобів з метою мінімізації обчислювальних ресурсів в процесах забезпечення надійності, стійкості та безпеки функціонування цих систем.

При цьому отримано такі науково-практичні результати:

1. На підставі опрацювання літературних джерел проаналізовано відомі інформаційні технології забезпечення функціональної безпеки при передаванні потоків даних у форматі цифрових зображень комунікаційними каналами інформаційно-управляючих систем критичного застосування. Функціональна безпека систем, що розглядаються забезпечується низкою засобів, кожен з яких використовує певні часові, обчислювальні ресурси тощо. Науково-методичні підходи застосування універсальних засобів, що поєднують у собі декілька функцій на даний час є не достатньо розвинутими.

2. Сумісне використання для кодування систем Ель-Гамаля і RSA дозволило отримати метод підвищення функціональної безпеки систем критичного застосування при передаванні в комунікаційних процедурах цифрових зображень із глибиною кольору до 4 байт, що дає можливість підвищити стійкість функціонування інформаційних системв $(P-3)^2 \cdot (\varphi(\psi(n))-1)$.

3. Використання елементів криптографічного кодування RSA та операції зашумлення дало можливість удосконалити метод забезпечення необхідного рівня функціональної безпеки в процедурах захисту напівтонових зображень із глибиною кольору в 1-2 байти, що дало можливість збільшити рівень безпеки систем без інформаційних втрат в комунікаційних процедурах автоматизованих

систем критичного застосування.

4. Інтегрування бінарних операторів в схему криптографічного кодування дало можливість підвищити загальний рівень функціональної безпеки систем оброки і комунікаційного обміну повноколірних зображень в автоматизованих системах критичного застосування.

5. Удосконалена інформаційна технологія підвищення функціональної безпеки для випадку передавання комунікаційними каналами напівтонових зображень із глибиною кольору в 1-2 байти завдяки використанню елементів алгоритму RSA та порозрядних операцій, що дає можливість забезпечити повну зашумленість зображень і зменшує межі розрядності обчислювальних процедур.

6. Розроблене на основі отриманих теоретичних результатів дисертаційного дослідження програмне рішення забезпечує збереження інформації не лише при передаванні її комунікаційними каналами, а й у випадку організації стійкого персоніфікованого захисту.

7. Модифіковані архітектури для виділених основних класів автоматизованих систем завдяки імплементації розробленої інформаційної технології забезпечують автоматизацію процедур забезпечення функціональної безпеки передавання інформації комунікаційними каналами інформаційно-управляючих систем критичного застосування.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Абламейко С. В. Обработка изображений: технология, методы, применение / С. Абламейко, Д. Лагуновский. – Минск: Ин-т техн. кибернетики НАН Беларуси, 1999. – 300 с.
2. Алгоритм шифрования RSA - описание и общие вопросы/ Електронний ресурс. [Електронний ресурс]. Режим доступу: http://kiev-security.org.ua/box/1/81.shtml.
3. Алгоритмические основы эллиптической криптографии / `Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.] . – М.: МЭИ, 2000. – 100 с.
4. Александров В. В. Представление и обработка изображений. Рекурсивный подход / В. В. Александров, Н. Д. Горский. – Ленинград: Наука, 1985. – 189 с.
5. Анісімов А. В. Алгоритмічна теорія великих чисел. Модулярна арифметика великих чисел / Анатолій Васильович Анісімов – К.: Видавничий дім «Академ періодика», 2001. – 153 с.
6. Березовский А. И. О тестировании быстродействия алгоритмов и программ выполнения основных операций для ассиметричной криптографии / А. И. Березовский, В. К. Задирака, Л. Б. Шевчук // Кибернетика и системный анализ. – 1999. – № 5. – с. 56–66.
7. Березовський А. І. Деякі резерви оптимізації обчислень для множення багаторозрядних чисел / А. І. Березовський, В. К. Задірака, С. С. Мельникова, Л. Б. Шевчук // Зб. «Теорія обчислень». – К., 1999. – с. 325-329.
8. Березовський А. І. Про оптимізацію за швидкодією алгоритмів виконаня операцій над багаторозрядними числами / А. І. Березовський, М. П. Бесараб, В. К. Задірака, Л. Б. Шенчук // Вісник державного увіверситету «Львівська політехніка» “Прикладна математика”. – Львів. – 1998. – Т. 2. № 337. – с. 297

– 300.

9. Бернет С. Криптография. Официальное руководство RSA Security / С. Бернет, С. Пэйн – М.: Бином–Пресс, 2002. – 384 с.
10. Бессалов А. В. Криптосистемы на эллиптических кривых: Учеб. Пособие / Бессалов А. В., Телиженко А. Б. – К.: ІВЦ «Вадавництво «Політехніка», 2004. – 224 с.
11. Бінарні операції в алгоритмі шифрування RSA. Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту: матеріали міжнародної наукової конференції: Матеріали міжнародної наукової конференції [“Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту (ISDMCI'2011)], (Євпаторія, 16-20 травня 2011) / ХНТУ. – Херсон, 2011. – Т1. – с. 358-360.
12. Борзов Ю.Ю. Модифікація алгоритму RSA: шифрування та дешифрування за одним рядком матриці зображення / Ю.О. Борзов, А.М. Ковальчук, Д.Д. Пелешко // Науковий вісник НЛТУ України: зб. наук.-техн. праць. – 2012. – Вип. 22.6. – С. 336 – 340.
13. Борисов В.И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты /В.М. Зинчук, А.Е. Лимарев и др.; под ред. В.М. Борисова. – М.: Радио и связь, 2000. – 384 с.
14. Бородін О. І. Теорія чисел / О. І. Бородін. – К.: Вища школа, 1970. – 275 с.
15. Брюс Шнайдер. Прикладная криптография / Брюс Шнайдер. – М.: Триумф, 2003. – 815 с.
16. Василенко О. Н. Современные способы проверки простоты чисел / О. Н. Василенко // Кибернетический Сборник. – 1988. – №2. – с. 162-188.
17. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О. Н.

Василенко – М.: МЦНМО, 2003. – 328 с.

18. Вельшенбах М. Криптография на Си и С++ в действии. Учебное пособие / М. Вельшенбах. – М.: Издательство Триумф, 2004. – 464 с.
19. Венбо Мао. Современная криптография. Теория и практика / Венбо Мао. – Минск: Издательство Вильямс, 2005. – 768 с.
20. Венков Б.А. Исследования по теории чисел / Б. А. Венков. –Ленинград: Наука, 1981. – 448 с.
21. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів: Видавницгво науково-технічної літератури, 1998. – 247 с.
22. Визильтер Ю.В. Обработка и анализ цифровых изображений с примерами на LabVIEW и IMAQ Vision / Ю.В. Визильтер, С.Ю. Желтов, В.А. Князь, А.Н. Ходарев, А.В. Моржин. – Москва, 2008. – 463 с.
23. Використання кубічних форм для підвищення стійкості шифрування тернарними афінними перетвореннями: Матеріали міжнародної наукової конференції [“Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту (ISDMCI'2013)], (Євпаторія, 20-24 травня 2013) / ХНТУ. – Херсон, 2013. – Т1. – с. 175-177.
24. Виноградов И.М. Основы теории чисел. Изд. 2, переработ. / И. М. Виноградов. – М. – Л.: ОНТИ, 1938. – 88 с.
25. Волкова С.О. Дослідження існуючих підходів підвищення якості програмного забезпечення критичного застосування/ С.О.Волкова, О.М.Трунов// Радіоелектронні і комп’ютерні системи. – 2008. – №6(33) . – с.202-208.
26. Воробель Р. А. Підвищення точності реконструкції зображень за критерієм мінімуму енергії / Р. А. Воробель, І. Б. Івасенко // Відбір і обробка інформації. – 2005. – № 23(99). – С.112 – 116.

27. Гарбарчук В. Кибернетический подход к проектированию систем защиты информации / В. Гарбарчук, З. Зинович, А, Свиц. – Луцк: Волынская обласная друкарня, 2003. – 659 с.
28. Голубева Е. П. Представление больших чисел тернарными квадратичными формами / Е. П, Голубева // Математический сборник. – 1986. – №129(171):1. – 40–54 с.
29. Гомес Ж. Мир математики. Т.2: Математики, шпионы и хакеры. Кодирование и криптография/ Ж. Гомес - М.: Де Агостини, 2014. - 144 с.
30. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; [пер. с англ. П. А. Чочиа]. –М.: Техносфера, 2005. – 1072 с
31. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – М.: Яхтсмен, 1996. – 192 с.
32. Делоне Б.Н. Петербургская школа теории чисел / Б. Н. Делоне. – М.: АН СССР, 1947. – 419 с.
33. Дж. Макконелл. Основы современных алгоритмов. 2-е дополненное издание / Дж. Макконелл. – М.: Техносфера, 2006. – 368 с.
34. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства // Офіційний журнал L 013. – 19/01/2000. – с. 0012–0020.
35. Диффи У. Защищенность и имитостойкость. Введение в криптографию / У. Диффи, М. Э. Хеллмен. – ТИИЭР, том 67, № 3, 1979.
36. Дубчак О.В., Лисенко Т.О, Сось В.С. Порівняльний аналіз криптографічних методів. [Електронний ресурс]. Режим доступу: http://www.rusnauka.com/12_KPSN_2009/Informatica/44807.doc.htm.
37. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БАК, 2003. – 144 с.

38. Жуков А.Е. Системы блочного шифрования. Пособие по курсу «Криптографические методы защиты информации» / А. Е. Жуков. –М.: Московский Государственный Технический Университет им. Н.Э. Баумана, Кафедра ИУ-8. – 49 с.
39. Завадская Л. А. Криптографичски сильные генераторы псевдослучайных последовательностей / Л. А. Завадская, А. М. Фаль // Безопасность информации – 1997– № 1. – с. 7–11.
40. Задірака В. К. Комп'ютерна криптологія: Підручник / В. К. Задірака, О. С. Олесюк. – К., 2002. – 504с.
41. Закон України про електронний цифровиий підпис. – К., 22 травня 2003р., № 852-IV.
42. Зензин С. О. AES (Advanced Encryption Standart). Конечные поля / О. С. Зенин, М. А. Иванов. – М.: КУДИЦ-Образ, 2002. – 176 с.
43. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М.: КУДИЦ-ОБРАЗ. 2001. – 368 с.
44. Иванов М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2001. – 368с.
45. Інформаційна безпека. [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0.
46. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма: ГОСТ 34.310-94.

47. Каневский З. М. Теория скрытности / З. М. Каневский, В.П. Литвиненко – Воронеж : ВГУ, 1991. – 144 с.
48. Катыс Г. П. Методы и вычислительние средства обработки изображений / Г. П. Катыс. – Кишинев.: Истинца, 1991. – 209 с.
49. Коваленко И. Н. Асимметричные криптографические алгоритмы / И. Н. Коваленко, А. И. Кочубинский // Кибернетика и системный анализ. – 2003. – № 4. – С. 95-102.
50. Ковальчук А. М. Бінарні операції в алгоритмі шифрування RSA / А. М. Ковальчук, Д. Д. Пелешко, Ю. О. Борзов // [Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту], Матеріали міжнародної наукової конференції (Євпаторія, 16-20 травня, 2011) / ХНТУ. – Херсон, 2011. – С. 358-360.
51. Ковальчук А. Використання побітових операцій і додаткового зашумлення в алгоритмі RSA при шифруванні-дешифруванні зображень / А.Ковальчук, Д. Пелешко, Ю. Борзов. // Вісник НУ ЛП “Комп’ютерні науки та інформаційні технології”. – 2012. – №744. – С. 132–136.
52. Ковальчук А. Використання побітових операцій при шифруванні-дешифруванні кольорових зображень у модифікаціях алгоритму RSA / А.Ковальчук, Д. Пелешко, М. Навитка Ю. Борзов. // Вісник НУ ЛП “Комп’ютерні науки та інформаційні технології”. – 2011. – №719. – С. 133–136.
53. Ковальчук А. Поєднання алгоритму RSA і побітових операцій при шифруванні-дешифруванні зображень / А.Ковальчук, Д. Пелешко, М. Хомин, Ю. Борзов. // Вісник НУ ЛП “Комп’ютерні науки та інформаційні технології”. – 2011. – №694. – С. 309–312.
54. Ковальчук А. Бінарні операції та елементи алгоритму RSA при шифруванні-дешифруванні кольорових зображень/ А.Ковальчук, Д. Пелешко, Ю. Борзов.

// Комп’ютерні науки та інформаційні технології. Вісник НУ ЛП – 2013. – №771. – С. 121-125.

55. Ковальчук А.М. Сумісне використання криптосистем Ель-Гамаля І RSA в захисті графічної інформації / А.М. Ковальчук, Д.Д. Пелешко, Ю.О.Борзов. // Вісник НУ ЛП “Комп’ютерні науки та інформаційні технології”. – 2013. – №751. – С. 178–182.
56. Кодирование и обработка изображений / [под. ред. Зяблова В. В., Лебедева Д. С.]. – М.: Наука, 1988. – 180 с.
57. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. / С. Коутинхо. – М.: Постмаркет, 2001. – 328 с.
58. Криптографические методы защиты информации. [Електронний ресурс]. Режим доступу: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema8#p84.
59. Лебедев А.Н. Криптография с «открытым ключом» и возможности её практического применения / А. Н. Лебедев // Защита информации, выпуск 2, 1992. – с. 129-147.
60. Леммер Д. Н. Таблицы простых чисел от 2 до 10006721 / Д. Н. Леммер. – М., 1967.
61. Ляпин Е.С., Евсев А.Е. Алгебра и теория чисел. Часть I. Числа / Е. С. Ляпин, А. Е. Евсев. – Москва: Просвещение, 1974. – с. 383.
62. Мінгальова Ю. Новітні криптографічні методи захисту інформації. [Електронний ресурс]. Режим доступу: http://eprints.zu.edu.ua/13902/1/Mingaleva3.pdf.
63. Метод определения RSA-ключей через анализ изменения разности потенциалов. [Електронний ресурс]. Режим доступу: http://www.opennet.ru/opennews/art.shtml?num=40359

64. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Електронний ресурс]. Режим доступу: http:// http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41650.
65. Нильс Фергюсон. Практическая Криптография / Нильс Фергюсон, Брюс Шнайдер. – М.: Вильямс, 2005, 416 с.
66. Обзор методов вскрытия криптосистемы RSA. [Електронний ресурс]. Режим доступу: http://turboreferat.ru/information/obzor-metodov-vskrytiya-kriptosistemy-rsa/236910-1196384-page4.html.
67. Основы криптографии / [Алферов В. А., Зубов Н. Р., Кузьмин О. В, Черемушкин А. В.]. – К.: Изд. Гелиос АРВ, 2005. – 480 с.
68. Острик В. В. Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые / В. В. Острик, М. А. Цфасман. – М.: МЦНМО, 2001. – 48 с.
69. Павлидис Т. Алгоритмы машиной графики и обработки изображений / Т. Павлидис. – М.: Радио и связь, 1986. – 399 с.
70. Панасенко Сергей. Алгоритмы шифрования. Специальный справочник. / Сергей Панасенко. – Санкт-Петербург: «БХВ-ПЕТЕРБУРГ», 2009. – 564 с.
71. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – М.: ДМК, 2000. – 448 с.
72. Полянская О.Ю. Основы технологии PKI / О. Ю. Полянская, В. С. Горбатов. – М.: Горячая Линия-Телеком, 2004. – 248 с.
73. Про одну модифікацію алгоритму RSA шифрування-дешифрування півтонових зображень / А. Ковальчук, Д. Пелешко, М. Навитка, Ю. Борзов // Комп’ютерні науки та інформаційні технології. Вісник НУ ЛП – 2012. – №732.– С. 225-229.
74. Прэтт У. К. Цифровая обработка изображений / У. К. Прэтт; [пер. с англ.]. –

М.: Мир. – 1982. – 790 с.

75. Путятин Е. П. Обработка изображений в робототехнике / Е. П. Путятин, С. И. Аверин. – М.: Машиностроение, 1990. – 320 с.
76. Рак Т.Є. Лінійні форми з елементами алгоритму RSA і додаткове зашумлення в захисті півтонових зображень/ Т.Є Рак, Ю.О. Борзов // Науковий вісник НЛТУ України: зб. наук.-техн. праць. – 2015. – Вип. 25.3. – С. 336 – 340.
77. Рашкевич Ю. Модифікація алгоритму RSA для деяких класів зображень. / Ю. Рашкевич, Д. Пелешко, А. Ковальчук //«Технічні вісті», 2008. – №1(27), 2(28). – с. 59-62 .
78. Рашкевич Ю. Шифрування і дешифрування зображень дробово-лінійними формами з використанням алгоритму RSA / Ю. Рашкевич, А. Ковальчук, Д. Пелешко // Вісник НУ ЛП "Комп'ютерні науки та інформаційні технології". – 2009. – №650. – с. 185-190.
79. Рашкевич Ю.М. Шифрування та дешифрування зображень тернарними афінними формами з елементами алгоритму RSA. / Ю.М. Рашкевич, А.М. Ковальчук, Д.Д. Пелешко // Науковий вісник Національного лісотехнічного університету України. – 2009. –№ 19.6. – с. 259-262.
80. Рашкевич Ю. Ю. Потокова модифікація алгоритму RSA з використанням проективних та афінних перетворень для деяких класів зображень / Ю. Ю. Рашкевич, А. М. Ковальчук, Д. Д. Пелешко, М. Л. Навитка // Вісник Національного університету «Львівська політехніка». – 2011. – № 694. – с. 35-40.
81. Рашкевич Ю.М. Афінні перетворення в модифікаціях алгоритму RSA шифрування зображень / Ю. М. Рашкевич, А. М. Ковальчук, Д. Д. Пелешко // «Автоматика, Автоматизація, Електротехнічні комплекси та системи». – 2009. – №2(24). – с.59-66.

82. Ростовцев А. Г. Теоретическая криптография / А. Г. Ростовцев, Е. Б. Маховенко. – М.: Профессионал, 2005. – 490 с.
83. Рябко Б. Я. Криптографические методы защиты информации / Б. Я. Рябко, А. Н. Фионов. – М.: Горячая линия – Телеком, 2005. – 229 с.
84. Рябко Б. Я. Основы современной криптографии для специалистов в информационной технологии/ Б. Я. Рябко, А. Н. Фионов. – М.: Научн. мир. 2004. – 172 с.
85. Смит Р. Э. Аутентификация: от паролей до открытых ключей / Р. Э. Смит [пер. с англ.]. – М.: Издательский дом «Вильямс», 2002. – 432 с.
86. Сойфер В. А. Компьютерная обработка изображений, Ч. 1 / В. А. Сойфер // Соровский образовательный журнал. – 1996. – № 2. – с. 118-124.
87. Тернарні афінні перетворення в шифруванні і дешифруванні трьох зображень без додаткового зашумлення: Матеріали міжнародної наук. конф. [“Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту (ISDMCI'2011)], (Євпаторія, 16-20 травня 2011) / ХНТУ. – Херсон, 2011. – Т1. – с. 360-362.
88. Х. К. А. ван Тилборг. Основы Криптологии. Профессиональное руководство и интерактивный учебник / Х.К.А ван Тилборг. – М.: Мир, 2006. – 471 с.
89. Черемушкин А. В. Лекции по арифметическим алгоритмам и криптографии / А. В. Черемушкин. – М.: МЦИМО, 2002. – 104 с.
90. Чмора А. Л. Современная прикладная криптография/ А. Л. Чмора. – М.: Гелиос АРВ, 2001. – 256 с.
91. Шенахаге А. Быстрое умножение больших чисел / А. Шенахаге, В. Штрассен // Кибернет. Сб. – 1973. Вып. 10. – с. 87-98.
92. Шифрування-дешифрування напівтонових зображень модифікаціями алгоритму RSA: Матеріали міжнародної наукової конференції [“Інтелектуальні

системи прийняття рішень та проблеми обчислювального інтелекту (ISDMCI'2012)], (Євпаторія, 27-31 травня 2012) / ХНТУ. – Херсон, 2012. – С. 447-449.

93. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайдер. – М.: Изд-во ТРИУМФ. – 816 с.
94. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. / [Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.]. – М.: Изд. КомКнига, 2006. – 328 с.
95. Яне Б. Цифровая обработка изображений / Б. Яне. – М.: Техносфера, 2007. – 583 с.
96. Яншин В. В. Анализ и обработка изображений: принципы и алгоритмы / В. В. Яншин. – М.: Машиностроение, 1995. – 112 с.
97. Ященко В.В. Введение в криптографию / В. В. Ященко, Н. П, Варновский, Ю. В. Нестеренко. – М.: ЧеРо, 1999. – 272 с.
98. Alireza Jolfaei and Abdolrasoul Mirghadri,“An image Encryption approach using Chaos and Stream Cipher”, Journal of Theoretical and Applied Information Technology, Vol. 19, No. 2, September 2010,pp. 117-123.
99. Adleman L. On distinguishing prime numbers from composit numbers / L. Adleman, C. Pomerance, R. S. Rumaly // Ann.V-fth/ – 1983. – V.117. – p. 173-206.
100. Ahmed A. Abd El-Latif. A hybrid chaotic system and cyclic elliptic curve for image encryption / Ahmed A. Abd El-Latif, Xiamu Niu // AEU – International Journal of Electronics and Communications. – 2013. –Vol. 67, Issue 2. – p. 136-143.
101. Ahmed A. Abd El-Latif. A new image cipher in time and frequency domains / Ahmed A. Abd El-Latif, Xiamu Niu, Mohamed Amin // Optics Communications. – 2012. – Vol. 285, Issue 21-22. – p. 4241-4251.

102. Banerjee S. Synchronization of time delayed semiconductor lasers and its applications in digital cryptography / S. Banerjee, L. Rondoni, S. Mukhopadhyay // Optics Communications. – 2011. – Vol. 284, Issue 19. – p. 4623-4634.

103. Chong Fu. A novel chaos-based bit-level permutation scheme for digital image encryption / Chong Fu, Bin-bin Lin, Yu-sheng Miao, Xiao Liu, Jun-jie Chen // Optics Communications. – 2011. – Vol. 284, Issue 23. – p. 5415-5423.

104. Cohen H. Primality testing and Jacobi sums / H. Cohen, H. W. Lenstra // Math. Comp. –1984. – V.42(165). – p. 297-330.

105. Emad Mosa. Chaotic encryption of speech signals / Emad Mosa, Nagy W. Messiha, Osama Zahran, Fathi E. Abd El-Samie // International Journal of Speech Technology. – 2011. –Vol. 14, Issue 4. – p. 285-296.

106. Encryption and decryption of images using fractional-rational form of n degree with the elements of the RSA algorithm: Матеріали 1-ї міжнародної науково-технічної конференції ["Захист інформації і безпека інформаційних систем"], (Львів, 31 травня – 1 червня)/ НУ ЛП. – Львів, 2012. – с. 152.

107. Ercan Solak. Algebraic break of image ciphers based on discretized chaotic map lattices / Ercan Solak, Cahit Çokal // Information Sciences. – 2011. – Vol. 181, Issue 1. – p. 227-233.

108. Han Shuihua and Yang Shuangyan, "An Asymmetric Image Encryption Based on Matrix Transformation," ECTI Transactions on C omputer and Information Technology, Vol. 1, No. 2, November 2005, pp. 126-133.

109. Howard Cheng and Xiaobo Li, "Partial Encryption of Compressed Images and Videos," IEEE Transaction on Signal Processing, Vol. 48, No. 8, August 2000, pp. 2439- 2451.

110. Geng Zhao. Block Cipher Design, Issue Generalized Single-Use-Algorithm Based on Chaos / Geng Zhao, Guanrong Chen, Jingqing Fang, Gang Xu Tsinghua

// Science & Technology. – 2011. – Vol. 16, Issue 2. – p. 194-206.

111. GnuPG is NOT vulnerable to -Get Your Hands Off My Laptop. [Електронний ресурс]. Режим доступу: http://lists.gnupg.org/pipermail/gnupg-announce/2014q3/000349.html.

112. Guodong Ye. An efficient chaotic image encryption algorithm based on a generalized Arnold map / Guodong Ye, Kwok-Wo Wong // Nonlinear Dynamics. – 2012. – Vol. 69, Issue 4. – p. 2079-2087.

113. Guoji Zhang. A novel image encryption method based on total shuffling scheme / Guoji Zhang, Qing Liu // Optics Communications. – 2011. – Vol. 284, Issue 12. – p. 2775-2780.

114. Images protection by using projective and binary affine transformations with elements of RSA algorithm: Proceedings of the 11 International Conference ["The experience of designing and application of CAD systems in microelectronics" (CADSM 2011)], (Lviv – Polyana, February 23 – 25, 2011)/ Lviv Polytechnik National University. – Lviv: Publishing House Vezha&Co, 2011. – p. 321.

115. Jolly Shah and Dr. Vikas Saxena. Performance Study on Image Encryption Schemes. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, 2011. P.349-355.

116. Kamlesh Gupta. Novel Approach for fast Compressed Hybrid color image Cryptosystem / Kamlesh Gupta, Sanjay Silakari // Advances in Engineering Software. – 2012. – Vol. 49. – p. 29-42.

117. Kanso A. A novel image encryption algorithm based on a 3D chaotic map / A. Kanso, M. Ghebleh // Communications in Nonlinear Science and Numerical Simulation. – 2012. – Vol. 17, Issue 7. – p. 2943-2959.

118. Kovalchuk A. A blend of algorithms RSA and bit, additive-difference operations and algorithms in El-Gamal images / [A. Kovalchuk, Y. Borzov, D.

Peleshko та ін.]. // Journal of Global Research in Computer Science. – 2013. – P.1-7.

119. Lenstra H. W. Primality testing algorithms / H. W. Lenstra // Bourbaki Seminar. – 1981. –V.1980/81. – p. 243-257.

120. Maciej P. Wojtkowski. On the Real Baker Map / Maciej P. Wojtkowski // Reports on Mathematical Physics. – 2012. – Vol. 69, Issue 2. – p. 235-242.

121. Omid Mirzaei. A new image encryption method, Issue parallel sub-image encryption with hyper chaos / Omid Mirzaei, Mahdi Yaghoobi, Hassan Irani // Nonlinear Dynamics. – 2012. – Vol. 67, Issue 1. – p. 557-566.

122. Osama S. Faragallah. An enhanced chaotic key-based RC5 block cipher adapted to image encryption / Osama S. Faragallah // International Journal of Electronics. – 2012. – Vol. 99, Issue 7. – p. 925-943.

123. Qiaolun Gu. A novel reversible robust watermarking algorithm based on chaotic system / Qiaolun Gu, Tiegang Gao // Digital Signal Processing. – 2013. – Vol. 23, Issue 1. – p. 213-217.

124. Rebollo-Neira L. Self-contained encrypted image folding / L. Rebollo-Neira, J. Bowley, A.G. Constantinides, A. Plastino // Issue Statistical Mechanics and its Applications. – 2012. – Vol. 391, Issue 23. – p 5858-5870.

125. RSA. [Електронний ресурс]. Режим доступу: http://www.wikiwand.com/ru/RSA.

126. Ruisong Ye. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism / Ruisong Ye // Optics Communications. – 2011. – Vol. 284, Issue 22. – p. 5290-5298.

127. Seyed Mohammad Seyedzadeh. A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map / Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki // Signal Processing. – 2012. –Vol. 92, Issue 5. –

p. 1202-1215.

128. Seyyed Mohammad Reza Farschi. A novel chaotic approach for information hiding in image / Seyyed Mohammad Reza Farschi, H. Farschi // Nonlinear Dynamics. – 2012. –Vol. 69, Issue 4. – p. 1525-1539.

129. Shiguo Lian. Traceable content protection based on chaos and neural networks / Shiguo Lian, Xi Chen // Applied Soft Computing. – 2011. – Vol. 11, Issue 7. – p. 4293-4301.

130. Subba Rao Y.V., Abhijit Mitra, Mahadeva Prasanna S.R. "A Partial Image Encryption Method with Pseudo Random Sequences", In Proceedings of International Conference on Information System Security, Kolkata, India, December 19-21, 2006, Springer LNCS 4332, pp. 315-325.

131. The use of conjunctive partitioning of images to increase strength of the RSA algorithm: Proceedings of the VIII International Scientific and Technical Conference ["Perspective Technologies and Methods in MEMS Design " (MEMSTECH 2012)], (Lviv-Polyana, April 18-21, 2012) / Lviv Polytechnik National University. – Lviv: Publishing House Vezha&Co., 2012 – p. 138-139.

132. The Use of Disjunctive Covering of Images to Increase Strength of the RSA Algorithm: Proceeding of the VII International Conference ["Perspective Technologies and Methods in MEMS Design " (MEMSTECH 2011)], (Lviv-Polyana, May 11-14, 2011) / Lviv Polytechnik National University. – Lviv: Publishing House Vezha&Co, 2011. – p. 168-169.

133. Use of the bitwise operations for colorimages encryption and decryptionin the RSA algorithm modification/ A.Kovalchuk, D.Peleshko, Y.Borzov, M.Navytka // Proceeding sof the VII International Scientific and Technical Conference ["Computer Science and Information Technologies" (CSIT 2011)], (Lviv, 16-19 November 2011) / Lviv Polytechnic National University. – Lviv: Lviv

Polytechnic, 2011. – P. 17-18

134. The use of quadratic forms to increase strength of the encryption of binary affine loop transformation: Proceedings of the V International Scientific and Technical Conference ["Computer Science And Information Technologies" (CSIT 2010)], (Lviv, October 14-16, 2010) / Lviv Polytechnik National University. – Lviv: Publishing House Vezha&Co., 2010. – p. 19-21.

135. Van Droogenbroeck M., Benedett R. Techniques for a selective encryption of uncompressed and compressed images, "in Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS), Ghent, Belgium, September 9-11,2002,pp. 90-97.

136. Volos Ch. K. Image encryption process based on chaotic synchronization phenomena / Ch.K. Volos, I.M. Kyprianidis, I.N. Stouboulos // Signal Processing. – 2013. – Vol. 93, Issue 5. – p. 1328-1340.

137. Wei Zhang. A symmetric color image encryption algorithm using the intrinsic features of bit distributions / Wei Zhang, Kwok-wo Wong, Hai Yu, Zhi-liang Zhu // Communications in Nonlinear Science and Numerical Simulation. 2013 . – Vol. 18, Issue 3. – p. 584-600.

138. Wei Zhang. An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion / Wei Zhang, Kwok-wo Wong, Hai Yu, Zhi-liang Zhu // Optics Communications. – 2012. – Vol. 285, Issue 9. – p. 2343-2354.

139. Wei Zhang. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion / Wei Zhang, Kwok-wo Wong, Hai Yu, Zhi-liang Zhu // Communications in Nonlinear Science and Numerical Simulation. – 2013. – Vol. 18, Issue 8. – p. 2066–2080.

140. Xiaoling Huang. Image encryption algorithm using chaotic Chebyshev generator / Xiaoling Huang // Nonlinear Dynamics. – 2012. –Vol. 67, Issue 4. – p.

2411-2417.

141. Xingyuan Wang. Chaotic encryption algorithm based on alternant of stream cipher and block cipher / Xingyuan Wang, Xiaojuan Wang, Jianfeng Zhao, Zhenfeng Zhang // Nonlinear Dynamics. – 2011. – Vol. 63, Issue 4. – p. 587-597.

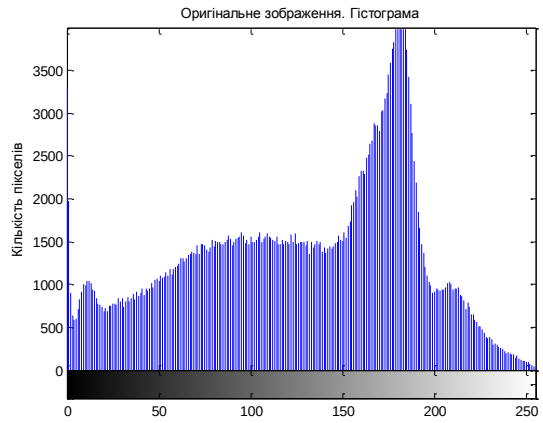
142. Use of the bitwise operations for color images encryption and decryption in the RSA algorithm modification: Proceedings of the VI International Scientific and Technical Conference ["Computer Science And Information Technologies" (CSIT 2011)], (Lviv, November 16-19, 2011) / Lviv Polytechnik National University. – Lviv: Publishing House Vezha&Co., 2011. – p. 17-18.

143. Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, Guanrong Chen. (2011) A new chaos-based fast image encryption algorithm. Applied Soft Computing. Vol. 11, Issue 1, 2011, Pages: 514-522.

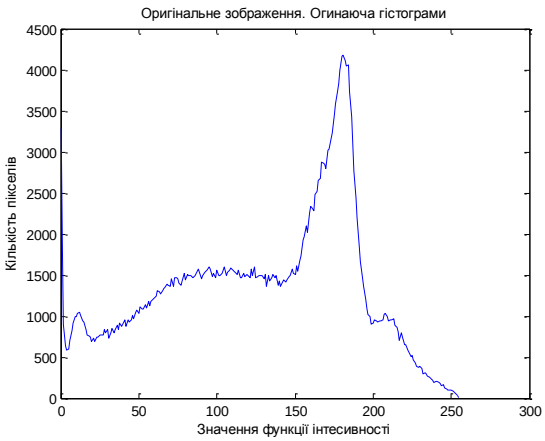
144. Yue Wu. Local Shannon entropy measure with statistical tests for image randomness / Yue Wu, Yicong Zhou, George Saveriades, Sos Agaian, Joseph P. Noonan, Premkumar Natarajan // Information Sciences. – 2013. – Vol. 222. – p. 323-342.

ДОДАТКИ

Д1. ГІСТОГРАМИ ЗОБРАЖЕНЬ

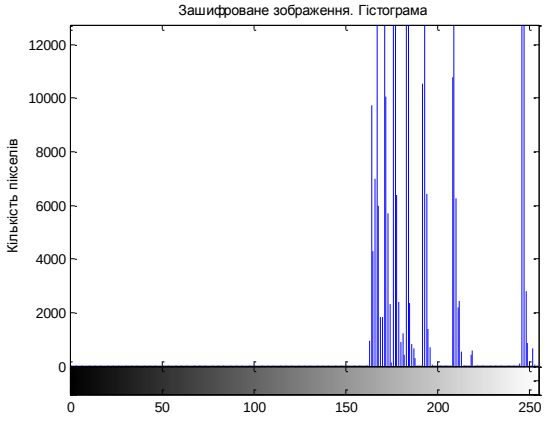


а)

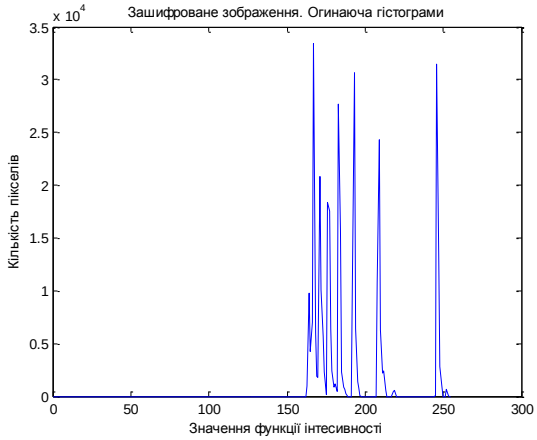


б)

Рисунок Д.1.1 – Гістограма та її огинаюча зображення, наведеного на рис. 2.6

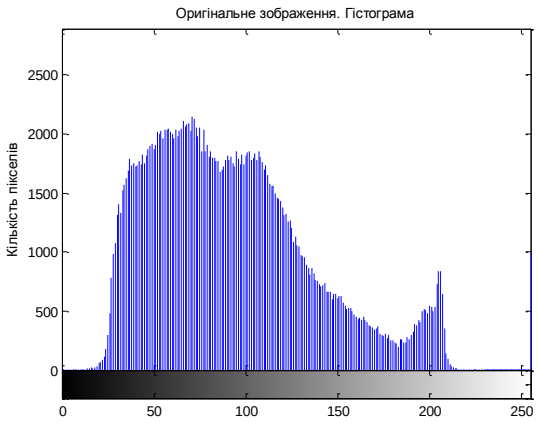


а)

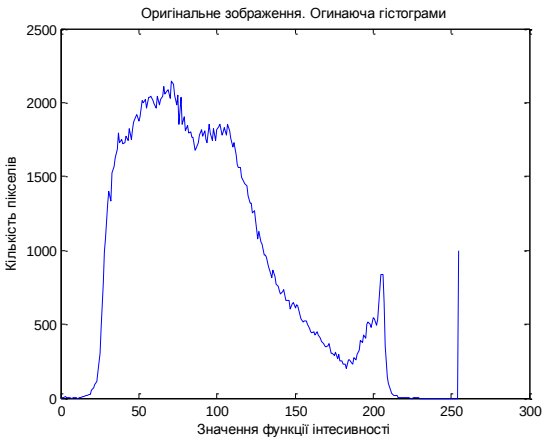


б)

Рисунок Д.1.2 – Гістограма та її огинаюча зображення, наведеного на рис. 2.7

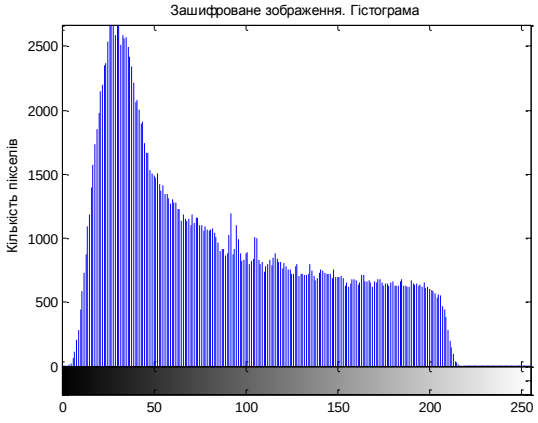


а)

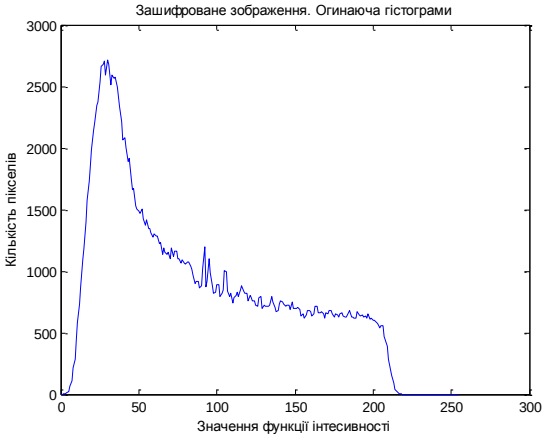


б)

Рисунок Д.1.3 – Гістограма та її огинаюча зображення, наведеного на рис. 2.9

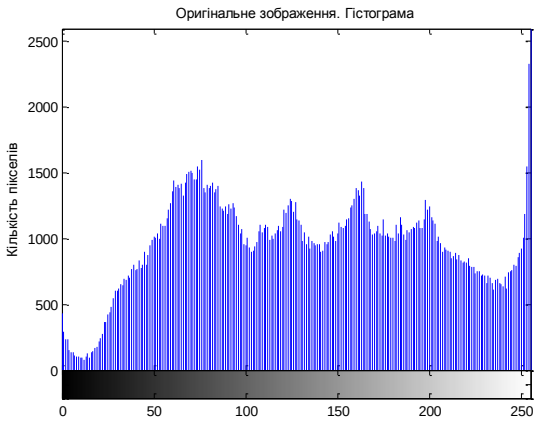


а)



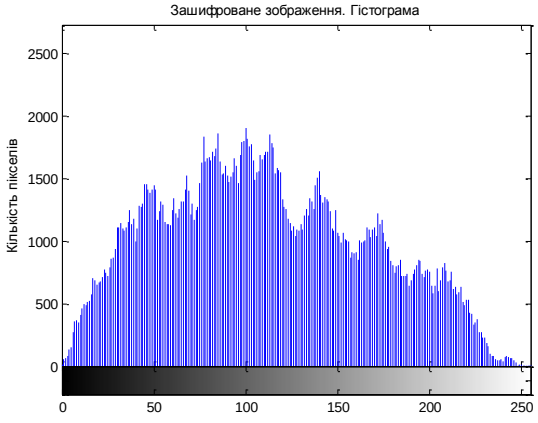
б)

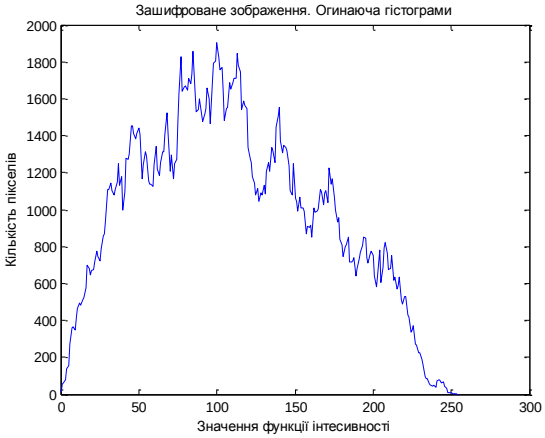
Рисунок Д.1.4 – Гістограма та її огинаюча зображення, наведеного на рис. 2.10



а) б)

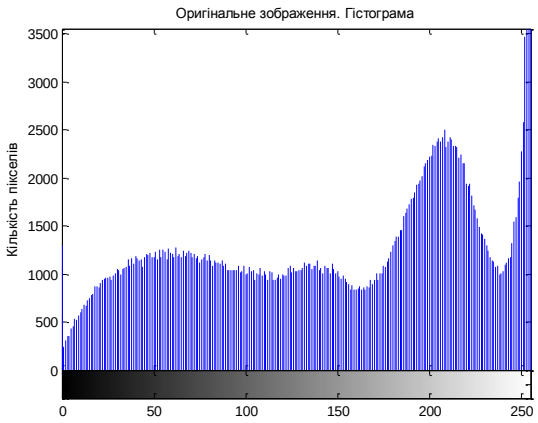
Рисунок Д.1.5 – Гістограма та її огинаюча зображення, наведеного на рис. 2.12





а) б)

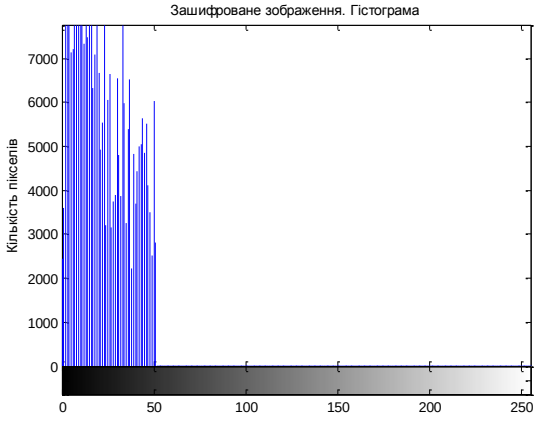
Рисунок Д.1.6 – Гістограма та її огинаюча зображення, наведеного на рис. 2.13



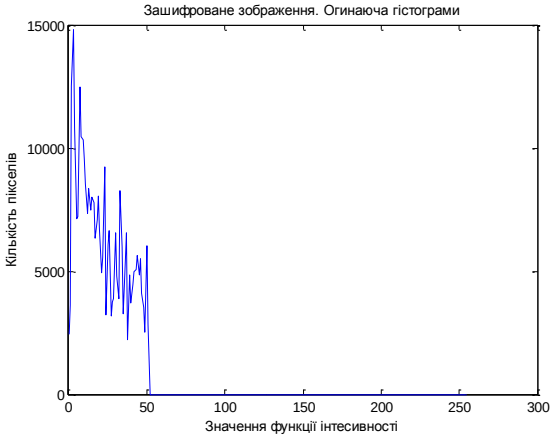
а)

б)

Рисунок Д.1.7 – Гістограма та її огинаюча зображення, наведеного на рис. 2.15

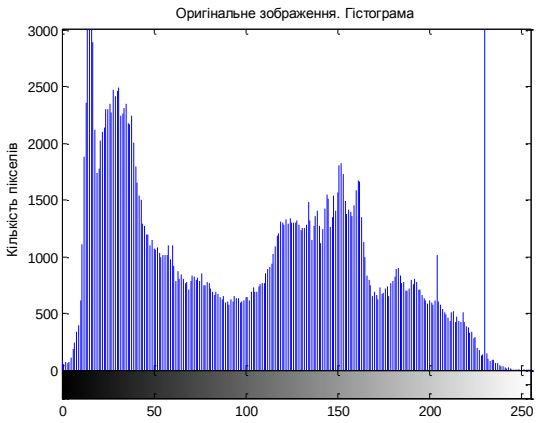


а)



б)

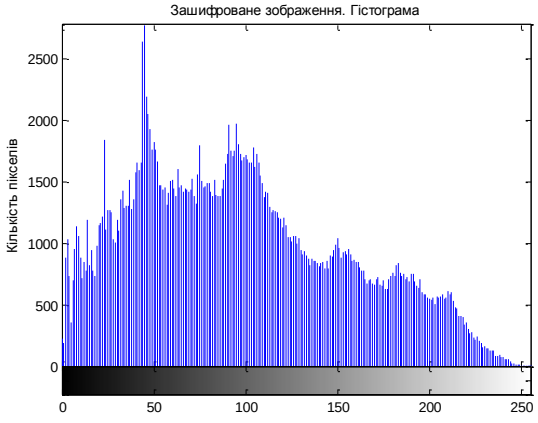
Рисунок Д.1.8 – Гістограма та її огинаюча зображення, наведеного на рис. 2.16



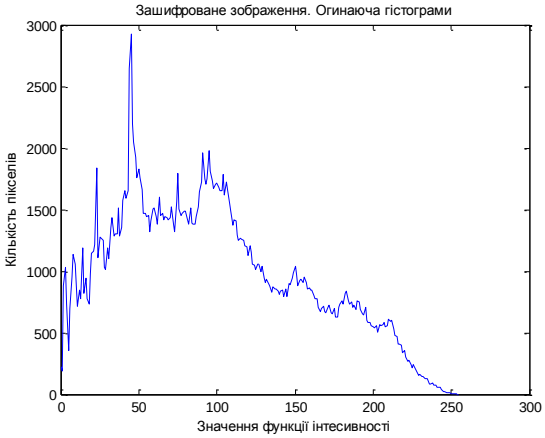
а)

б)

Рисунок Д.1.9 – Гістограма та її огинаюча зображення, наведеного на рис. 2.18



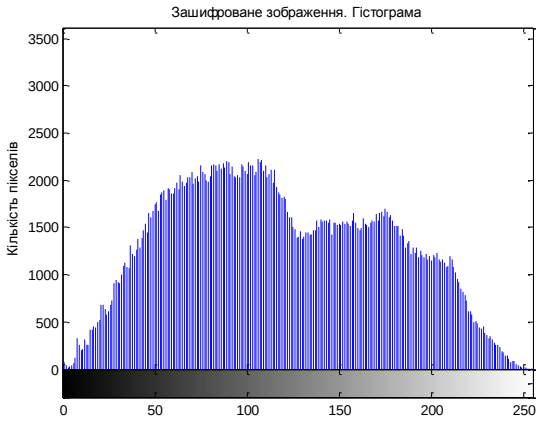
а)

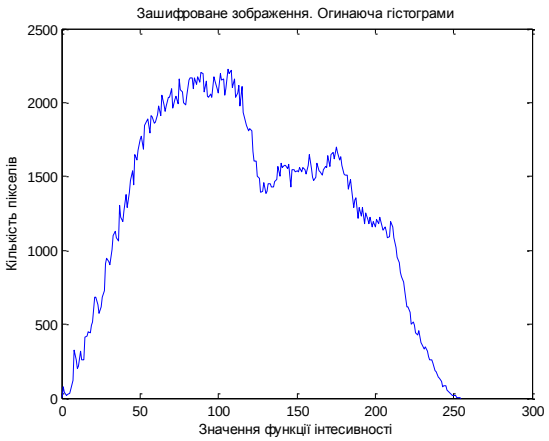


б)

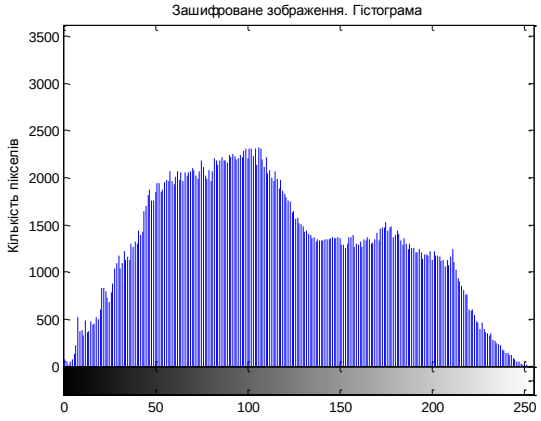
Рисунок Д.1.10 – Гістограма та її огинаюча зображення, наведеного на рис. 2.19

а)

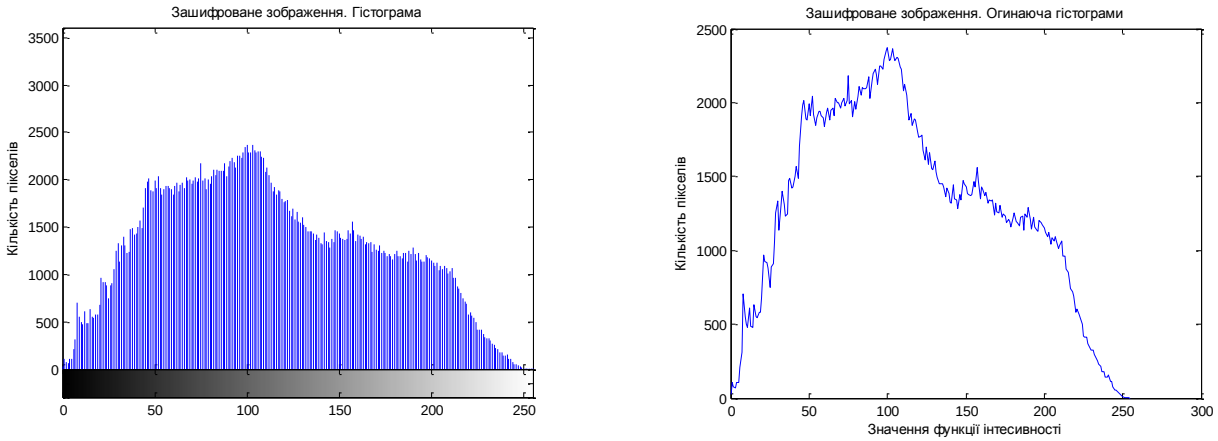

Зашифроване зображення. Гістограма
Кількість пікселів
0
500
1000
1500
2000
2500
3000
3500
0
50
100
150
200
250


Зашифроване зображення. Огинаюча гістограми
Кількість пікселів
0
500
1000
1500
2000
2500
0
50
100
150
200
250
300
Значення функції інтесивності

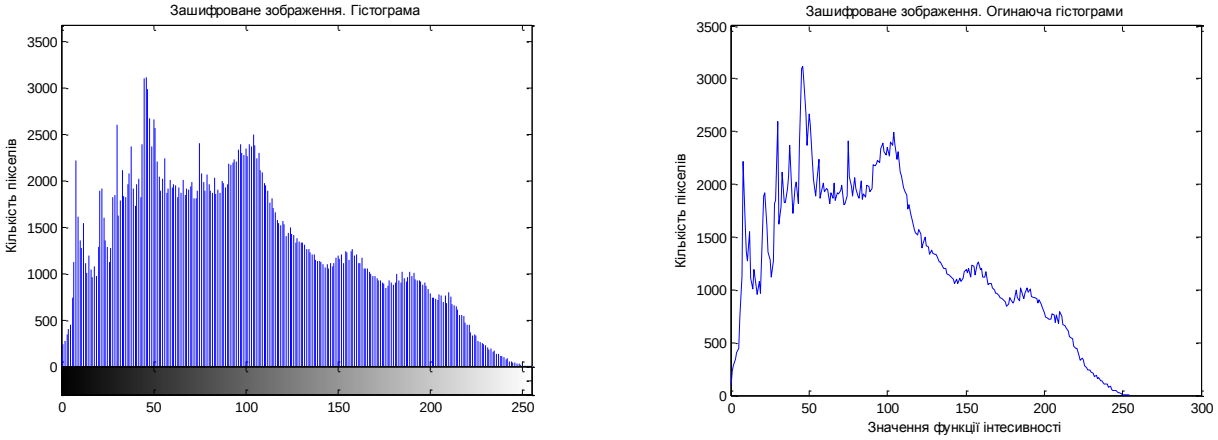
б)


Зашифроване зображення. Гістограма
Кількість пікселів
0
500
1000
1500
2000
2500
3000
3500
0
50
100
150
200
250


Зашифроване зображення. Огинаюча гістограми
Кількість пікселів
0
500
1000
1500
2000
2500
0
50
100
150
200
250
300
Значення функції інтесивності



в)



г)

Рисунок Д.1.11 – Гістограма та її огинаюча зображення, наведеного на рис. 2.23

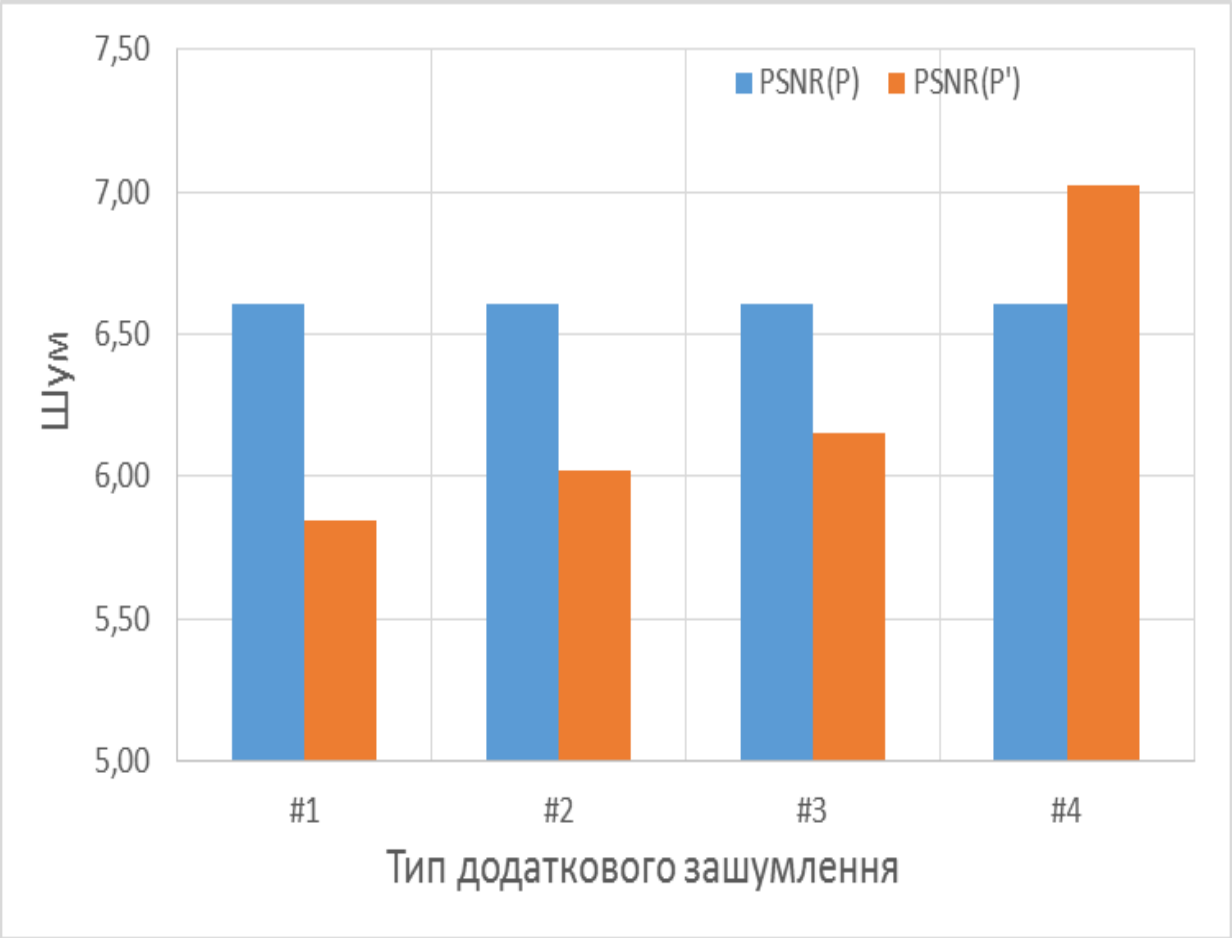
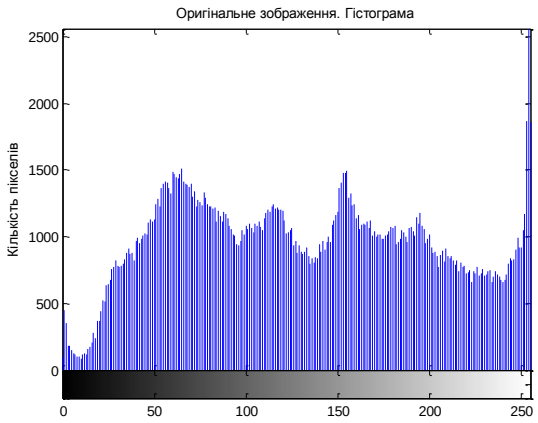


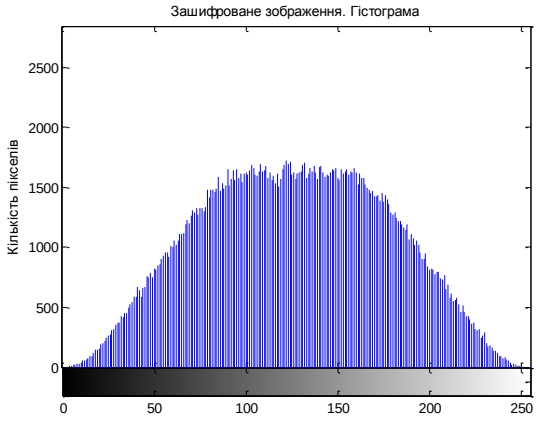
Рисунок Д.1.11 – Значення шуму на закодованому зображенні при використанні методу із п. 2.4. із різними значеннями оператора зашумленості, наведеними у табл. 2.1



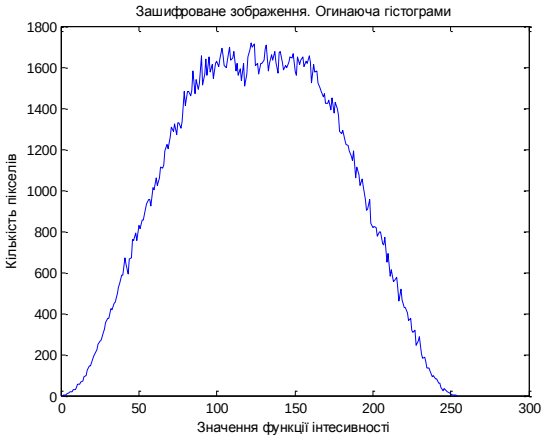
а)

б)

Рисунок Д.1.12 – Гістограма та її огинаюча зображення, наведеного на рис. 3.1

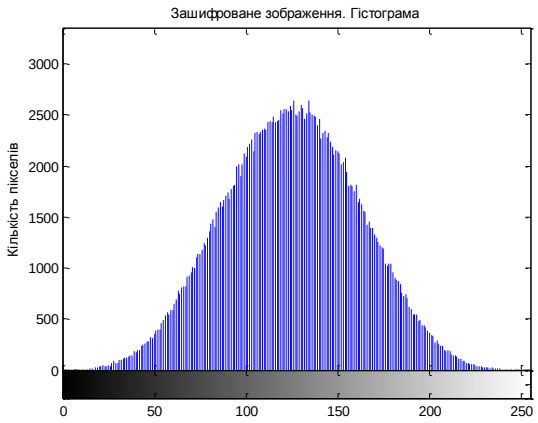


а)

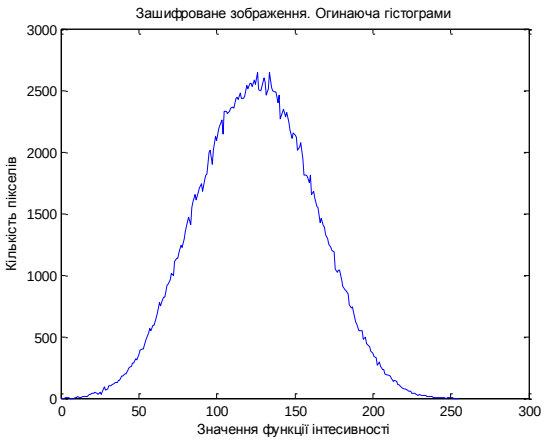


б)

Рисунок Д.1.13 – Гістограма та її огинаюча зображення, наведеного на рис. 3.3

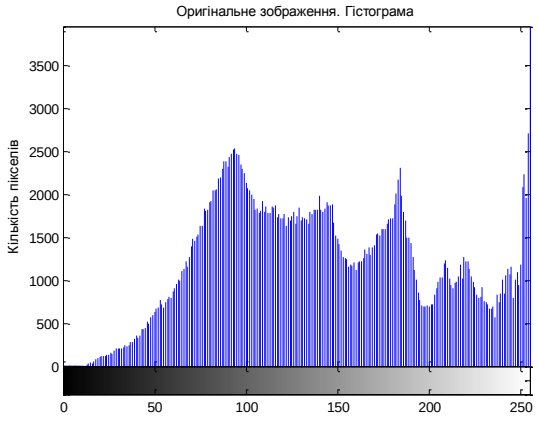


а)



б)

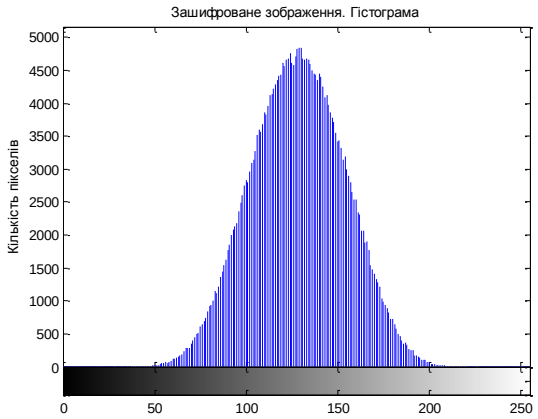
Рисунок Д.1.14 – Гістограма та її огинаюча зображення, наведеного на рис. 3.5



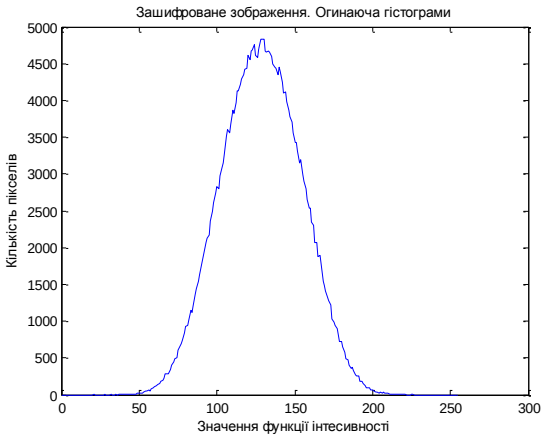
а)

б)

Рисунок Д.1.15 – Гістограма та її огинаюча зображення, наведеного на рис. 3.7

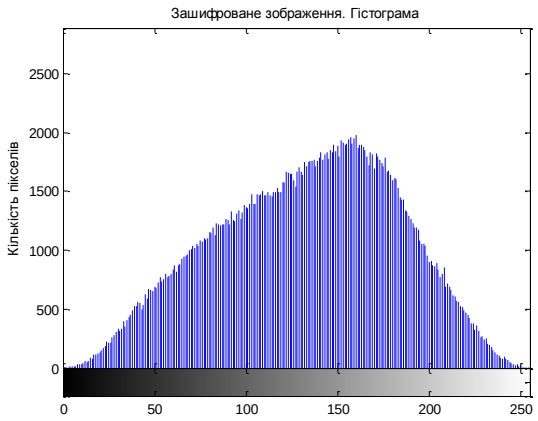


а)

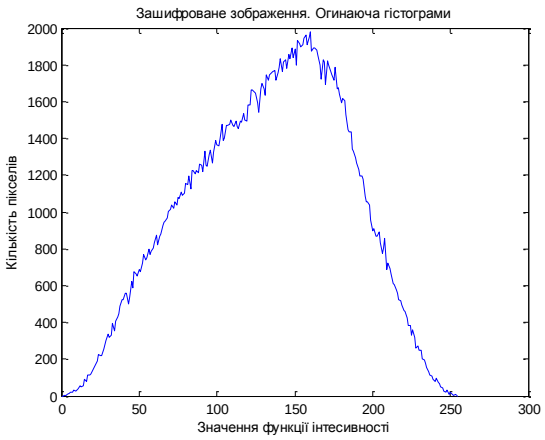


б)

Рисунок Д.1.16 – Гістограма та її огинаюча зображення, наведеного на рис. 3.9

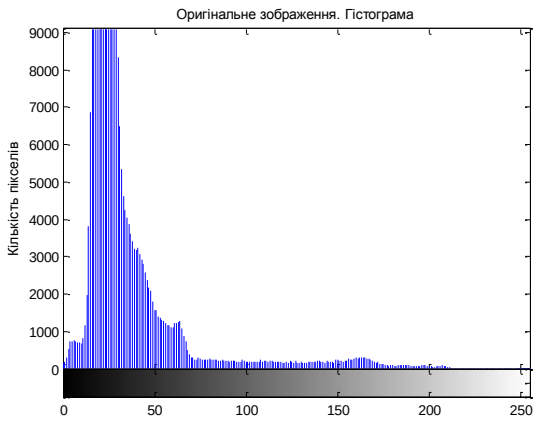


а)

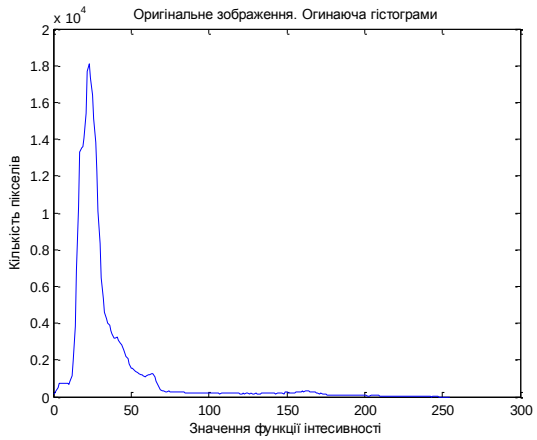


б)

Рисунок Д.1.17 – Гістограма та її огинаюча зображення, наведеного на рис. 3.11

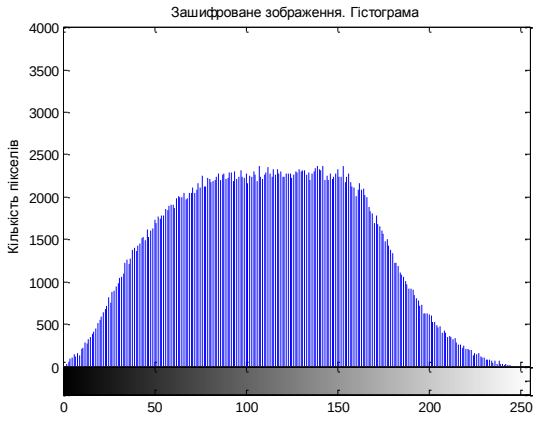


а)

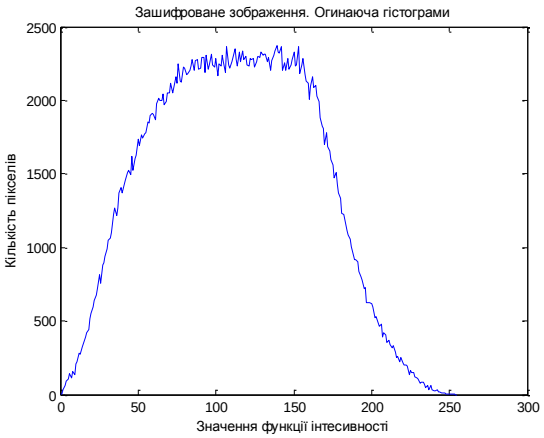


б)

Рисунок Д.1.18 – Гістограма та її огинаюча зображення, наведеного на рис. 3.13

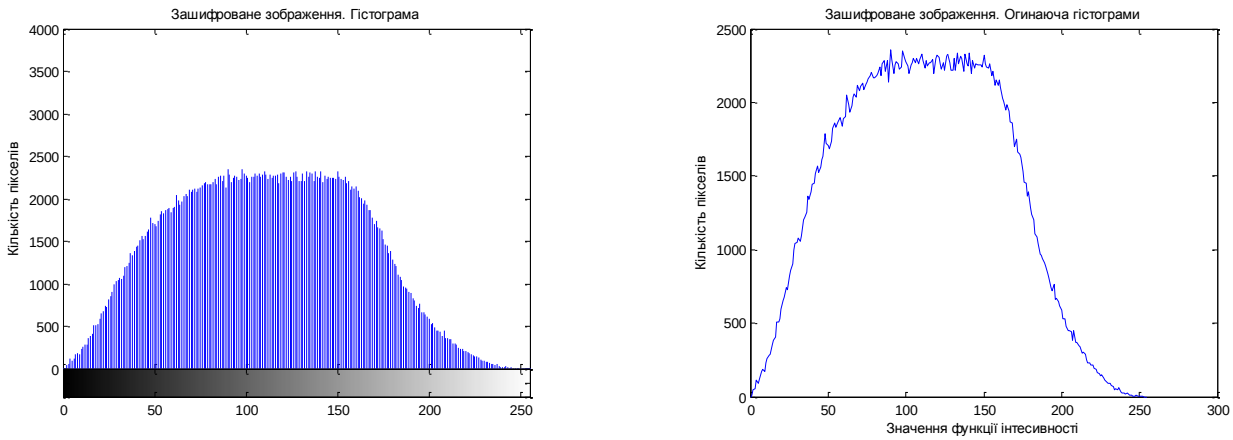


а)



б)

Рисунок Д.1.19 – Гістограма та її огинаюча зображення, наведеного на рис. 3.14



а) б)

Рисунок Д.1.20 – Гістограма та її огинаюча зображення, наведеного на рис. 3.16

Д2. АКТИ ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНИХ ДОСЛІДЖЕНЬ

ЗАТВЕРДЖУЮ
Перший заступник начальника
Головного управління
ДСНС України у Львівській області
Дідух І.М.
«17» червня 2014 р.

АКТ
про використання результатів дисертаційної роботи
Борзова Юрія Олексійовича
«Інформаційні технології підвищення функціональної безпеки систем обробки інформації критичного застосування»

Комісія в складі начальника відділу телекомунікацій, інформаційних технологій та системи 112 Конанця М.Д., головного фахівця відділу телекомунікацій, інформаційних технологій та системи 112 Хана В.О., начальника центру оперативного зв'язку, телекомунікаційних систем та інформаційних технологій ГУ підполковника служби цивільного захисту Купчака Ю.С. засвідчує, що при розробці та впровадженні системи оперативно-диспетчерського управління (СОДУ) підрозділами служби цивільного захисту Головного управління ДСНС України у Львівській області використано результати дисертаційних досліджень Борзова Ю.О., зокрема: метод шифрування та дешифрування напівтонових зображень із глибиною кольору в 1-2 байти, який ґрунтується на поєднанні елементів методу RSA та операції зашумлення, що дало можливість збільшити криптографічну стійкість без інформаційних втрат в процедурах захисту зображень в комунікаційних сеансах. Нівелювання контурів в розробленому методі здійснюється при малих значеннях ключів, що гарантує невихід за межі розрядної сітки в обчислювальному процесі.

Використання формату динамічної бібліотеки і єдиних програмних інтерфейсів в системі оперативно-диспетчерського управління дає можливість динамічно розширювати набір функцій криптографічного захисту новими алгоритмами без необхідності перероблення систем в цілому.

Розроблене у форматі динамічної бібліотеки програмне рішення захисту зображень може бути використане як для створення відокремленого, тобто виключно мережевого агента, так і для створення агента, інтегрованого в автоматизовану систему.

Начальник відділу телекомунікацій,
інформаційних технологій та системи 112
ГУ ДСНС України у Львівській області М.Д. Конанець

Головний фахівець відділу телекомунікацій,
інформаційних технологій та системи 112
ГУ ДСНС України у Львівській області В.О. Хан

Начальник центру оперативного зв'язку,
телекомунікаційних систем та інформаційних технологій
ГУ ДСНС України у Львівській області
підполковник служби цивільного захисту Ю.С. Купчак

ЗАТВЕРДЖУЮ
Перший проректор Львівського
державного університету
безпеки життєдіяльності
полковник служби цивільного захисту
Коваль М.С.
«17» лютого 2015 р.

АКТ

про впровадження результатів дисертаційної роботи Борзова Юрія Олексійовича
«Інформаційні технології підвищення функціональної безпеки систем обробки інформації критичного застосування»

Комісія в складі голови – начальника інституту цивільного захисту Львівського державного університету безпеки життєдіяльності, к.т.н., доцента Ренкаса А.Г. та членів: заступника завідувача кафедри управління інформаційною безпекою, к.т.н., доцента Лагуна А.Е., доцента кафедри управління проектами, інформаційних технологій та телекомунікацій к.т.н. Мальця І.О. склали цей акт про те, що основні результати дисертаційної роботи старшого викладача кафедри управління проектами, інформаційних технологій та телекомунікацій Борзова Юрія Олексійовича за темою «Інформаційні технології підвищення функціональної безпеки систем обробки інформації критичного застосування» впроваджені у навчальний процес Львівського державного університету безпеки життєдіяльності, зокрема: забезпечення криптографічної стійкості при передаванні зображень в комунікаційних сеансах автоматизованих систем критичного застосування. В основі технологій забезпечення захисту від несанціонованого доступу до інформації (цифрових зображень) використовуються криптографічні методи підвищеної стійкості, які базуються на сумісному використанні алгоритму RSA та Ель-Гамаля, а також використанню додаткових операцій зашумлення. Завдяки цьому вирішується основна проблема використання алгоритму RSA при захисті зображень в інформаційних системах критичного застосування, яка полягає у збереженні контурів на зображеннях із різкими флуктуаціями функції інтенсивності.

Технології захисту, засновані на використанні алгоритму RSA, використовуєтюся при викладанні дисципліни «Основи криптографічного захисту інформації», тема «Алгоритми шифрування з відкритим ключем, потокові системи шифрування, використання регістрів зсуву в криптографії», та при викладанні дисципліни «Безпека інформації в інформаційно-комунікаційних системах» тема «Протоколи передавання та захисту інформації, захист комп'ютерних мереж».

Голова комісії: А.Г. Ренкас
Члени комісії: А.Е. Лагун
І.О. Малець