Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет кібербезпеки
(повна назва)

Кафедра інформаційно-мережної інженерії
(повна назва)

# КВАЛІФІКАЦІЙНА РОБОТА
# Пояснювальна записка

рівень вищої освіти другий (магістерський)

Дослідження методів селективного кодування в інформаційно-мережних системах

(тема)

Виконав:
здобувач 2 року навчання,
групи ІМІм-24-2
Тарас ПАНІБОГ
(власне ім'я, прізвище)

Спеціальність 172 Електронні комунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Інформаційно-мережна інженерія
( повна назва освітньої програми)

Керівник проф. Володимир БАРАННІК
(посада, власне ім'я, прізвище)

Допускається до захисту

Зав. кафедри _____ Микола МОСКАЛЕЦЬ.
(підпис) (власне ім'я, прізвище)

2026 р.

Не містить відомостей заборонених до відкритого публікування

Студент _____ / Панібог Т.М./

Керівник _____ / Бараннік В.В./

Харківський національний університет радіоелектроніки

Факультет кібербезпеки

Кафедра інформаційно-мережної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 172 Електронні комунікації та радіотехніка

Тип програми освітньо-наукова
(код і повна назва)

Освітня програма інформаційно-мережна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

# ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Панібогу Тарасу Миколайовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження методів селективного кодування в інформаційно-мережних системах

затверджена наказом університету від 23 березня 2026р . №232 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 20 травня 2026 р.

3. Вихідні дані до роботи
Проаналізувати архітектуру стандарту VVC та визначити перелік синтаксичних елементів CABAC, придатних для форматно-сумісної селективної обробки. Розробити алгоритм ідентифікації та кодування контейнерів у межах значень і знаків коефіцієнтів трансформації із забезпеченням постійного бітрейту. Оцінити вплив селективного кодування на ступінь візуальної деградації відео та обчислювальні витрати мережевих вузлів. Дослідити криптографічну стійкість запропонованого рішення до мережевих атак.

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Аналіз стану та тенденцій розвитку методів селективного кодування стандарту обробки відео даних HEVC
2. Математичний апарат та архітектура контекстно-адаптивного ентропійного кодування в системах стандарту VVC
3. Програмна реалізація та експериментальне дослідження методів селективного кодування у середовищі еталонної моделі VTM
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____

Слайди у форматі Power Point (назва та мета роботи, актуальність дослідження, аналіз існуючих підходів, виклики стандарту VVC, ентропійне кодування CABAC, математичні моделі бінаризації, кодування коефіцієнтів (TC), критерії безпеки маскування, запропонований селективний метод, експериментальне дослідження, деградація візуальної якості, стійкість та накладні витрати, загальні висновки)

**КАЛЕНДАРНИЙ ПЛАН**

| № | Назва етапів роботи | Терміни виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Ознайомлення із завданням. Уточнення ТЗ. | 23.03.2026 | вик. |
| 2 | Підбір літератури за темою роботи | 24.03 - 10.04.2026 | вик. |
| 3 | Аналіз стану та тенденцій розвитку методів селективного кодування стандарту обробки відео даних HEVC | 11.04 - 20.04.2026 | вик. |
| 4 | Математичний апарат та архітектура контекстно-адаптивного ентропійного кодування в системах стандарту VVC | 21.04 - 25.04.2026 | вик. |
| 5 | Програмна реалізація та експериментальне дослідження методів селективного кодування у середовищі еталонної моделі VTM | 26.04 - 18.05.2026 | вик. |
| 6 | Оформлення презентаційного матеріалу, підготовка до захисту у ЕК | 19.05 - 20.05.2026 | вик. |
| | | | |

Дата видачі завдання 23 березня 2026 р.

Здобувач _____
(підпис)

Керівник роботи _____ проф. Володимир БАРАННІК
(підпис) (посада, власне ім'я, прізвище

)

# РЕФЕРАТ

Пояснювальна записка: 67 с., 3 рис., 2 таблиці, 1 додаток, 70 джерел.

Об'єкт дослідження – процеси обробки, стиснення, захисту та розповсюдження мультимедійних потоків даних стандарту VVC (H.266) в умовах обмежених ресурсів інформаційно-мережних систем.

Мета роботи – дослідження можливості селективного кодування синтаксичних елементів ентропійного потоку для зниження обчислювальної складності, зменшення наскрізної затримки передачі та забезпечення форматно-сумісного захисту мультимедійного контенту в процесі функціонування інформаційно-мережних систем..

За результатами роботи розроблені: метод форматно-сумісного та постійно-бітрейтного селективного кодування синтаксичних елементів CABAC; алгоритм ідентифікації та захисту контейнерів у межах значень і знаків коефіцієнтів трансформації відеопотоку VVC та схема інтеграції селективного кодування в проміжні вузли телекомунікаційної мережі для безпечного транскодування трафіку.

СЕЛЕКТИВНЕ КОДУВАННЯ, ВИБІРКОВЕ ШИФРУВАННЯ, СУМІСНІСТЬ З ФОРМАТОМ, ПОСТІЙНИЙ БІТРЕЙТ, ІНФОРМАЦІЙНО-МЕРЕЖЕВІ СИСТЕМИ, CABAC, КОДЕР VVC, ОБЛАСТЬ ІНТЕРЕСУ (ROI), КОЕФІЦІЄНТИ ТРАНСФОРМАЦІЇ, МУЛЬТИМЕДІЙНИЙ КОНТЕНТ.

# THE ABSTRACT

Explanatory note: 67 p., 3 fig, 2 tables, 70 sources, 1 app.

The object of research processes of processing, compression, protection, and distribution of VVC (H.266) multimedia data streams under conditions of limited resources in information and network systems.

The purpose of this research is to investigate the possibility of selective coding of syntactic elements of the entropy stream to reduce computational complexity, decrease end-to-end transmission delay, and ensure format-compatible protection of multimedia content during the operation of information and network systems.

Based on the results of the research, the following were developed: a method for format-compatible and constant-bitrate selective encoding of CABAC syntactic elements; an algorithm for identifying and protecting containers within the range of values and signs of VVC video stream transformation coefficients; and a scheme for integrating selective coding into intermediate nodes of a telecommunications network for secure traffic transcoding.

SELECTIVE CODING, SELECTIVE ENCRYPTION, FORMAT COMPATIBILITY, CONSTANT BITRATE, INFORMATION AND NETWORK SYSTEMS, CABAC, VVC ENCODER, REGION OF INTEREST (ROI), TRANSFORMATION COEFFICIENTS, MULTIMEDIA CONTENT.

ЗМІСТ

# ПЕРЕЛІК СКОРОЧЕНЬ

AES (Advanced Encryption Standard) – розширений стандарт шифрування;

AES-CFB (Advanced Encryption Standard in Cipher Feedback mode) – розширений стандарт шифрування в режимі зворотного зв'язку за шифротекстом;

AES-CTR (Advanced Encryption Standard in Counter mode) – розширений стандарт шифрування в режимі лічильника;

ALF (Adaptive Loop Filter) – адаптивний петльовий фільтр;

AVC (Advanced Video Coding) – прогресивне кодування відео (стандарт H.264);

CABAC (Context-Adaptive Binary Arithmetic Coding) – контекстно-адаптивне бінарне арифметичне кодування;

CBR (Constant Bitrate) – постійний бітрейт;

CTC / CTCs (Common Test Conditions) – загальні тестові умови стандарту VVC;

EDR (Edge Differential Ratio) – коефіцієнт диференціації країв;

EGk (Exponential-Golomb k-th order) – код Експоненціального Голомба k-го порядку;

EQ (Encryption Quality) – якість шифрування;

FL (Fixed-Length Coding) – кодування фіксованої довжини;

GOP (Group of Pictures) – група кадрів;

HEVC (High Efficiency Video Coding) – стандарт високоефективного відеокодування (H.265);

IoT (Internet of Things) – інтернет речей;

IPM (Intra Prediction Mode) – режими внутрішнього прогнозування;

JPEG (Joint Photographic Experts Group) – стандарт стиснення зображень Об'єднаної групи експертів з фотографії;

LUT (Look-Up Table) – спеціалізований масив підстановок / таблиця пошуку;

MV (Motion Vectors) – вектори руху;

NPCR (Number of Pixels Change Rate) – швидкість зміни кількості пікселів;

OTT (Over-the-Top) – метод надання відеопослуг через мережу Інтернет;

PSNR (Peak Signal-to-Noise Ratio) – пікове співвідношення сигнал/шум;

QP (Quantization Parameter) – параметр квантування;

QTC (Quantized Transform Coefficients) – квантовані коефіцієнти перетворення;

ROI (Region of Interest) – область інтересу;

SAO (Sample Adaptive Offset) – фільтр адаптивного зміщення вибірки;

SHVC (Scalable High Efficiency Video Coding) – масштабоване розширення стандарту HEVC;

SSIM (Structural Similarity) – індекс структурної подібності;

SSS (Shamir's Secret Sharing) – схема розділення секрету Шаміра;

TB (Truncated Binary Coding) – урізане бінарне кодування;

TC / TCs (Transform Coefficients) – коефіцієнти трансформації;

TRp (Truncated Rice Coding) – укорочений код Райса з контекстом p;

TU (Truncated Unary Coding) – урізане унарне кодування;

U (Unary Coding) – унарне відображення / кодування;

UACI (Unified Average Changing Intensity) – уніфікована середня інтенсивність зміни;

VMAF (Video Multimethod Assessment Fusion) – інтегральний критерій суб'єктивного сприйняття / багатометодна оцінка відео;

VTM (VVC Test Model) – еталонне програмне забезпечення стандарту VVC;

VVC (Versatile Video Coding) – новітній стандарт відеокодування (H.266).

# ВСТУП

Актуальність теми. Стрімке зростання обсягів мультимедійного трафіку в сучасних інформаційно-мережних системах висуває жорсткі вимоги до балансу між конфіденційністю даних та ефективністю їхньої передачі. Традиційні підходи до захисту даних, що базуються на повному шифруванні відеопотоку (наприклад, алгоритмом AES на мережевому рівні), мають суттєві обмеження. До цих обмежень відносяться: висока обчислювальна складність, збільшення енергоспоживання кінцевих пристроїв та зростання наскрізної затримки (end-to-end latency). Крім того, повне шифрування руйнує синтаксичну структуру відеопотоку. Це унеможливлює проміжну обробку відео в мережевих вузлах (транскодування, адаптацію до смуги перепущення, додавання водяних знаків або моніторинг якості) без повного декодування, що створює серйозні ризики витоку секретних ключів на ненадійних проміжних серверах (Middleboxes).

Шляхом зменшення впливу викладених вище недоліків є застосування методи селективного кодування. З появою новітнього стандарту кодування відео VVC (Versatile Video Coding / H.266), який збільшує рівень стиснення до 40% порівняно з HEVC, задача селективного захисту ускладнюється через загрозу руйнування глибоких внутрішньопотокових залежностей. Саме тому наукові дослідження, спрямовані на розробку форматно-сумісних методів селективного кодування з постійним бітрейтом (Constant Bitrate) на рівні контекстно-адаптивного арифметичного енкодера (CABAC), є критично важливими для сучасних інформаційно-мережних систем. Вони дозволяють підвищити компресію даних від 15% до 26% із незначним збільшенням часових витрат на процес декодування до 6% часу, зберігаючи можливість безпечної маршрутизації та постобробки трафіку в мережі.

Мета дослідження полягає у дослідженні можливості селективного кодування синтаксичних елементів ентропійного потоку для зниження обчислювальної складності, зменшення наскрізної затримки передачі та

забезпечення форматно-сумісного захисту мультимедійного контенту в процесі функціонування інформаційно-мережних систем.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Проаналізувати архітектуру стандарту VVC та визначити перелік синтаксичних елементів CABAC, придатних для форматно-сумісної селективної обробки.

2. Розробити алгоритм ідентифікації та кодування контейнерів у межах значень і знаків коефіцієнтів трансформації (ТС) із забезпеченням постійного бітрейту.

3. Оцінити вплив селективного кодування на ступінь візуальної деградації відео та обчислювальні витрати мережевих вузлів.

4. Дослідити криптографічну стійкість запропонованого рішення до мережевих атак.

Об’єкт дослідження. Процеси обробки, стиснення, захисту та розповсюдження мультимедійних потоків даних стандарту VVC (H.266) в умовах обмежених ресурсів інформаційно-мережних систем.

Предмет дослідження Методи та алгоритми селективного (селективного) кодування і кодування синтаксичних елементів (знаків коефіцієнтів трансформації, векторів руху, режимів прогнозування) на рівні контекстно-адаптивного бінарного арифметичного кодування (CABAC) з дотриманням умов сумісності з форматом та незмінності бітрейту.

Методи дослідження. Для розв'язання поставлених у роботі задач використано:

- Теорію цифрової обробки сигналів та компресії зображень для аналізу структури синтаксичних елементів відеопотоку VVC та визначення зон криптографічного маскування.
- Теорію інформації та криптографії для побудови алгоритмів селективного симетричного кодування бінарних контейнерів CABAC.
- Методи математичного моделювання та обчислювального експерименту для програмної реалізації запропонованих методів на базі

еталонного програмного забезпечення стандарту VVC (VTM — VVC Test Model) під загальними тестовими умовами (CTC).

- Методи статистичного аналізу та теорії оцінки якості зображень для вимірювання ступеня викривлення та криптостійкості за метриками об'єктивної якості (PSNR, SSIM, VMAF), показниками візуальної деградації (EQ, EDR) та стійкості до диференційного аналізу (NPCR, UACI).

# 1 АНАЛІЗ СТАНУ ТА ТЕНДЕНЦІЙ РОЗВИТКУ МЕТОДІВ СЕЛЕКТИВНОГО КОДУВАННЯ СТАНДАРТУ ОБРОБКИ ВІДЕО ДАНИХ HEVC

Сучасний етап розвитку інформаційно-мережних систем характеризується експоненційним зростанням обсягів мультимедійного трафіку високої чіткості, що передається через відкриті канали зв'язку. Забезпечення безпеки та конфіденційності такого візуального контенту має першочергове значення у багатьох прикладних сферах, включаючи системи охоронного відеоспостереження, конфіденційний корпоративний зв'язок, хмарні сервіси розповсюдження медіа та медичні телекомунікаційні мережі. Прямим та найбільш очевидним технологічним рішенням для безпечної передачі цифрових відеоданих є тотальне шифрування всього сформованого бітового потоку на транспортному або мережевому рівнях за допомогою стійких криптографічних протоколів, таких як Advanced Encryption Standard (AES).

Проте застосування концепції повного шифрування до високоінтенсивних мультимедійних потоків у сучасних мережах супроводжується низкою критичних обмежень та суттєвих недоліків. По-перше, повне криптографічне перетворення всього масиву даних створює колосальне додаткове навантаження на обчислювальні тракти кінцевих пристроїв, що призводить до супутного збільшення їхнього енергетичного сліду та суттєвого зростання наскрізної затримки (end-to-end latency). Ця проблема стає особливо гострою для мобільних платформ та автономних вузлів інтернету речей (IoT), які функціонують в умовах дефіциту обчислювальних ресурсів, особливо коли відео кодується з високим цільовим бітрейтом. По-перече, тотальне шифрування повністю руйнує синтаксичну прозорість медіапотоку для проміжних елементів мережі. Сучасні архітектури розподілу контенту часто потребують виконання операцій постобробки на проміжних вузлах (middleboxes) безпосередньо в процесі маршрутизації. До таких операцій належать транскодування відео для адаптації до поточної смуги перепущення

каналу, динамічний моніторинг об'єктивної якості, додавання цифрових водяних знаків або сплайсинг сегментів. За умов повного шифрування проміжний вузол змушений виконувати дешифрування та повторне шифрування, що вимагає передачі секретних ключів стороннім серверам і створює серйозні ризики витоку інформації.

Ефективною альтернативою, що дозволяє розв’язати зазначені суперечності, є впровадження методів селективного (вибіркового) кодування та шифрування даних безпосередньо у стиснутому домені. Суть цього підходу полягає в тому, що криптографічному маскуванню піддається лише обмежений набір найбільш конфіденційних та інформаційно насичених синтаксичних елементів потоку. Це забезпечує дві фундаментальні властивості: сумісність із форматом стандарту (Format-compliance) та збереження постійного бітрейту (Constant Bitrate). Властивість сумісності з форматом гарантує, що захищений відеопотік може бути розібраний та декодований будь-яким стандартним декодером без ризику фатального збою, завдяки чому всі операції постобробки та пакування на проміжних серверах виконуються без доступу до секретного ключа. Також це дозволяє гнучко шифрувати лише просторові області інтересу (ROI), залишаючи фон чітким. Зі свого боку, властивість постійного бітрейту зберігає вихідну ефективність компресії кодера.

Технологія вибіркового захисту була широко досліджена для багатьох стандартів стиснення, включаючи JPEG, JPEG-2000, AVC, SVC, а також для стандарту HEVC та його масштабованого розширення SHVC. Проте у липні 2020 року було випущено стандарт відеокодування наступного покоління VVC (Versatile Video Coding / H.266), який завдяки новим інструментам перевершує HEVC до 50% за рівнем зниження бітрейту при аналогічній візуальній якості. Згідно з положеннями теорії інформації, підвищення ефективності стиснення неминуче додає більше внутрішніх залежностей у бітовий потік, що радикально ускладнює процес форматно-сумісного селективного кодування. Для вирішення цієї проблеми перспективним є виконання шифрування на рівні контекстно-адаптивного механізму бінарного арифметичного кодування (CABAC). Нижче

наведено детальний аналіз стану та тенденцій розвитку методів селективного кодування, який дозволить визначити оптимальні шляхи побудови систем захисту.

Shahid Z., Puech W. [35] запропонували підхід на основі візуального захисту та форматно-сумісного селективного шифрування бітових рядків (binstrings) стандарту HEVC на етапі ентропійного кодування CABAC. Для захисту вибраних синтаксичних елементів застосовано алгоритм AES у режимі зворотного зв'язку за шифротекстом (CFB). Результатом роботи є надійне приховування візуального вмісту без руйнування структури бітового потоку. Недоліком дослідження є те, що за рахунок використання попередньої (передрелізної) версії стандарту HEVC у моделі не було ідентифіковано та враховано повний спектр потенційно чутливих синтаксичних маркерів.

Farajallah M., Hamidouche W., Deforges O., Assad S. E. [10] запропонували алгоритм селективного кодування та захисту виділених областей інтересу (ROI) у відеопотоках HEVC, який спирається на концепцію прямокутних незалежних сегментів кадру (тайлів). Шифруванню підлягають лише тайли всередині ROI, а фон залишається відкритим. Досягненням роботи є те, що реалізовано форматно-сумісне маскування з постійним бітрейтом. Автори усунули ефект поширення помилок і спотворень за межі захищеної зони ROI на відкритий фон шляхом штучного обмеження векторів руху (MV) фонових тайлів, яким дозволено посилатися лише на аналогічні фонові області в опорних кадрах.

Boyadjis B., Bergeron C., Pesquet-Popescu B., Dufaux F. [5] створили розширений алгоритм селективного скремблювання для відеопотоків H.264/AVC та HEVC, спрямований на штучне збільшення рівня візуальної деградації контенту. Автори перевели процес селективного шифрування з режиму обходу (bypass) CABAC у звичайний контекстно-адаптивний режим, додавши до простору шифрування режими внутрішнього прогнозування (IPM) яскравості та залишкові коефіцієнти. Це суттєво підвищило стійкість до візуального аналізу, проте негативно вплинуло на ефективність стиснення, викликавши незначне зростання бітрейту.

Hamidouche W., Farajallah M., Sidaty N., El Assad S., Deforges O. [12] досліджували селективне кодування останньої версії HEVC та запропонували рішення для роботи в реальному часі для масштабованого розширення HEVC, яке отримало назву SHVC. Особливістю SHVC є використання нелінійних хаотичних динамічних систем. Результатом роботи є створення процесу аналізу та оптимізації всіх елементів синтаксису SHVC, що дозволило виконати форматно-сумісну обробку з постійним бітрейтом та мінімальною затримкою. Метод повністю зберіг функціональність масштабованості відео (layering) при зменшенні накладних витратах до 6% від загального часу роботи декодера.

Van Wallendael G., Boho A., Cock J. D., Munteanu A., Van De Walle R. [45] проводили дослідження щодо оцінки сукупності синтаксичних елементів кодера HEVC з метою створення гнучкого форматно-сумісного рішення, яке підтримує можливість подальшої адаптації та транскодування відео безпосередньо в мережевих вузлах. Досягненням роботи є знаходження оптимальних комбінація синтаксичних елементів шифрування яких забезпечує широкий діапазон рівнів скремблювання (від легкої зміни якості до повного руйнування) при мінімальному негативному впливі на криву ефективності швидкість-спотворення.

Memos V. A., Psannis K. E. [22] створено схему оптимізованої передачі медіаданих HEVC, яка передбачає шифрування виключно ключових кадрів (I-кадрів) алгоритмом AES-256 на основі ідеї, що P- та B-кадри не можуть бути декодовані без опорного кадру. Науковою новизною роботи є скорочення загального часу шифрування на 50% завдяки ефекту каскадного поширення спотворень по групі кадрів (GOP). Автори згрупували знакові біти коефіцієнтів трансформації для формування блоків під AES та інтегрували параметри схеми розділення секрету Шаміра (SSS) для захисту AC-коефіцієнтів. Недоліком запропонованого підходу є збільшення розміру бітового потоку щонайменше на 8%, за рахунок порушення умови щодо постійного бітрейту.

Long M., Peng F., Gong X. [21] Суть роботи полягає у двоетапній інтегрованій архітектурі форматно-сумісного захисту потоків HEVC,

адаптованої для безпечного обміну медіафайлами всередині мультимедійних соціальних мереж. Авторами запропоновано гібридний підхід: спочатку потоковий шифр маскує знаки коефіцієнтів трансформації (ТС) та реалізує приховування першого біта знака. На другому етапі, залежно від заданого коефіцієнта керування, вибірково шифруються параметри руху (індекс об'єднання, індекс прогнозування MV, знаки різниці MV, індекс опорного кадру). Система продемонструвала високу стійкість, але призвела до супутнього збільшення підсумкового бітрейту

Sallam A. I., El-Rabaie E.-S. M., Faragallah O. S. [33]. В роботі представлено метод низькоскладного селективного шифрування відео потоків HEVC для інформаційно-мережних систем реального часу, побудований на базі одновимірної хаотичної логістичної карти (Chaotic Logistic Map). Реалізовано швидкісне шифрування знакових бітів різниць векторів руху та коефіцієнтів трансформації безпосередньо на етапі ентропійного кодування. Метод підтвердив повну сумісність із форматом та нульовий вплив на бітрейт, забезпечуючи при цьому достатній (проміжний) рівень криптографічного захисту.

Peng F., Zhang X., Lin Z.-X., Long M. [27]. Основою роботи є настроювана дворангова схема селективного кодування HEVC, заснована на поєднанні режимів внутрішнього прогнозування хроматичного компонента (chroma IPM) та скремблювання коефіцієнтів трансформації. Розроблено механізм аналізу контурів (ребер) у кожному блоці перетворення. На першому рівні шифрується базовий набір елементів (IPM, суфікси ТС, знаки різниць MV тощо). На другому рівні, якщо блок містить ребра об'єктів, вмикається додаткове швидке скремблювання коефіцієнтів через операцію XOR із послідовністю генератора AES-CTR, що дозволяє динамічно адаптувати рівень безпеки до вмісту кадру.

Xu D. [52] запропонував метод стеганографічного приховування даних всередині частково зашифрованого бітового потоку HEVC шляхом модифікації квантованих коефіцієнтів перетворення (QTC). Забезпечено впровадження додаткової інформації в обхідному (bypass) режимі кодування без зміни

фізичного розміру даних, що гарантує збереження постійного бітрейту та форматної сумісності. Завдяки симетрії операцій XOR, процес вилучення прихованого повідомлення може виконуватися як на зашифрованому, так і на повністю відновленому відеопотоці при високій стійкості до атак заміни контенту.

Бараннік В. В., Бараннік Д. В. та ін. [23] запропонували метод маскування інформації в контурних областях відеозображень, інтегрований у процеси їхнього стиснення. Суть роботи полягає у контурно-орієнтованому селективному кодуванні, де криптографічному маскуванню піддаються структурні закономірності ребер та меж об'єктів у кадрі. Досягненням дослідження є забезпечення високої стійкості до візуального та семантичного аналізу при збереженні повної синтаксичної цілісності бітового потоку. Це дозволяє ефективно захистити виділені області інтересу (ROI) без залучення тотальних важких шифрів. Недоліком підходу є висока залежність ефективності маскування від алгоритмів просторової сегментації контурів, що робить систему вразливою до високочастотних шумів сенсора камери.

Бабенко Ю. М., Гаврилов Д. С. [2] дослідили особливості практичного застосування методів арифметичного кодування в системах криптографічного захисту інформації для підвищення доступності та семантичної цілісності відеоресурсів критичної інфраструктури. Суть дослідження полягає у розробці комбінованих алгоритмів інтеграції шифрування безпосередньо у статистичний ентропійний тракт кодера. Головним досягненням роботи є доведення можливості одночасного виконання компресії та захисту даних за рахунок спрямованої модифікації робочих інтервалів арифметичного енкодера, що мінімізує обчислювальні затримки у реальному часі. Особливістю запропонованої схеми крипто-компресії є підвищена чутливість до похибок передачі бітів у каналах зв'язку інформаційно-мережних систем, оскільки будь-яка мережева завада викликає незворотну каскадну десинхронізацію всього наступного масиву даних на стороні декодера.

Узагальнюючи результати проведеного аналізу стану та тенденцій розвитку методів селективного кодування мультимедійних даних, можна сформулювати наступні висновки:

Забезпечення конфіденційності та безпеки візуального контенту в сучасних інформаційно-мережних системах вимагає відходу від методів повного шифрування потоків (наприклад, AES) через їхню високу обчислювальну складність, затримки та неможливість проміжної обробки даних (транскодування, масштабування) без дешифрування. Технологія селективного (вибіркового) шифрування у стиснутому домені визначена як ефективна апаратна та алгоритмічна альтернатива.

Проаналізовано світовий досвід розробки методів вибіркового захисту для стандарту компресії HEVC (H.265). Встановлено, що найбільш технологічно доцільним є виконання криптографічного маскування безпосередньо на етапі ентропійного кодування CABAC. Це дозволяє маніпулювати специфічними синтаксичними елементами (знаками коефіцієнтів трансформації TC, векторами руху MV, режимами внутрішнього прогнозування IPM) для досягнення балансу між швидкістю роботи та рівнем візуальної деградації зображення.

Систематизовано основні архітектурні підходи до побудови селективних кодерів HEVC та виявлено їхні ключові компроміси:

- використання стандартних симетричних шифрів (AES-CFB, AES-CTR) забезпечує високу криптостійкість, але вимагає точного визначення простору синтаксичних маркерів, щоб уникнути руйнування структури потоку;

- впровадження концепції незалежних прямокутних сегментів (тайлів) дозволяє ефективно реалізувати захист виділених областей інтересу (ROI) без поширення спотворень на фонові області;

- застосування нелінійних хаотичних динамічних систем (одновимірних та багатовимірних логістичних карт) мінімізує обчислювальні витрати декодера (менше 6%), що є критично важливим для систем реального часу та масштабованого кодування (SHVC);

- інтеграція додаткових функцій, таких як стеганографічне приховування даних (Data Hiding) через модифікацію квантованих коефіцієнтів (QTC), розширює функціонал систем без збільшення фізичного обсягу файлу.

Виявлено загальний недолік багатьох існуючих методів для HEVC — це нездатність одночасно забезпечити сумісність із форматом (Format-compliance) та збереження постійного бітрейту (Constant Bitrate). Переведення шифрування з bypass-режиму CABAC у регулярний контекстний режим, або некоректне групування бітів знаків без урахування CABAC-контексту призводить до збільшення розміру бітового потоку (від незначного зростання до ), що порушує криву ефективності «швидкість-спотворення» та знижує продуктивність компресії.

Обґрунтовано наукову проблему та напрям подальшого дослідження магістерської роботи. З появою новітнього стандарту кодування відео наступного покоління VVC (Versatile Video Coding / H.266), який підвищує ефективність стиснення до 50% порівняно з HEVC, пряме перенесення існуючих алгоритмів шифрування стає неможливим. Збільшення щільності компресії додає значну кількість внутрішньопотокових залежностей та ускладнює процес форматно-сумісної обробки.

Висновки за розділом 1

Задача дослідження та розробки нових методів селективного кодування, адаптованих до специфіки алгоритмів binarization (TRp, Limited_EGk) та багатопрохідного кодування коефіцієнтів трансформації стандарту VVC, з жорстким дотриманням умов незмінності бітрейту та мінімальної обчислювальної складності, є актуальною науково-практичною задачею, яка вирішуватиметься у наступних розділах роботи.

# 2 МАТЕМАТИЧНИЙ АПАРАТ ТА АРХІТЕКТУРА КОНТЕКСТНО-АДАПТИВНОГО ЕНТРОПІЙНОГО КОДУВАННЯ В СИСТЕМАХ СТАНДАРТУ VVC

## 2.1 Математичний аналіз методів бінаризації коефіцієнтів трансформації

Процес функціонування арифметичного кодера CABAC у рамках стандарту VVC базується на триетапній схемі послідовної обробки:

- первинна двійкова декомпозиція (бінаризація);
- динамічне оцінювання контекстних моделей;
- фінальне стиснення сформованих бінарних послідовностей.

Математичний зміст першого етапу полягає в ін'єктивному відображенні множини багатозначних синтаксичних елементів у простір бінарних символів (бінів), що дозволяє звести задачу кодування складних алфавітів до обробки елементарних двійкових послідовностей.

Для оптимізації структурної надлишковості трафіку в архітектурі VVC впроваджено шість базових математичних методів бінаризації. Розглянемо їх формалізований опис, внутрішню суть та крипто-компресійні властивості.

1. Метод унарного відображення (U - Unary Coding). Це метод нерівномірного побітового представлення чисел, де кожна одиниця скалярної величини відображається еквівалентною довжиною двійкової серії. Застосовується для джерел із геометричним розподілом ймовірностей, де малі значення мають найвищу частоту появи. Перетворення кодує число $\xi$ як послідовність бінів, що завершується термінальним символом. Довжина підсумкового бітового рядка $L_U$ для заданого невід'ємного цілого числа $\xi$ визначається як:

$$L_U = \xi + 1 \tag{2.1}$$

При цьому бінарний потік формується у вигляді комбінації $\xi$ бінів зі значенням «1», за якими слідує один маркерний бін «0»:

$$\mathrm{Str}_U(\xi) = \{\underbrace{1,1,\ldots,1}_{\xi},0\} \tag{2.2}$$

де Str - це оператор формування підсумкового бінарного рядка (двійкової послідовності бінів);

$U$ - нижній індекс, який ідентифікує застосування саме унарного (Unary) алгоритму двійкового відображення;

$\xi$ - поточне скалярне невід'ємне ціле значення синтаксичного елемента відеопотоку, яке підлягає процедурі бінаризації;

1 - двійковий символ (бін) із логічним значенням «одиниця», що виступає базовим компонентом кодового слова;

$\underbrace{\ldots}_{\xi}$ - математичний оператор нижнього групування, який задає потужність підмножини і вказує на те, що символ «1» має повторитися у вихідному рядку точну кількість разів, яка дорівнює значенню змінної $\xi$;

0 - термінальний (маркерний) двійковий символ із логічним значенням «нуль», який додається в кінець рядка і сигналізує декодеру про завершення зчитування поточного кодового слова.

Головною перевагою є гранично низька обчислювальна складність та відсутність операцій множення/ділення. Ключовий недолік це катастрофічне лінійне зростання довжини коду при збільшенні значення $\xi$, що призводить до втрати ефективності стиснення.

2. Метод урізаного унарного кодування (TU - Truncated Unary Coding). Модифікація унарного алгоритму з фіксованим обмеженням максимальної потужності алфавіту джерела. Метод адаптує унарний код під умови, коли простір значень обмежений відомою верхньою межею $\Psi$.

Відображення розгалужується на дві умови залежно від співвідношення поточного сигналу та границі:

$$\mathrm{Str}_{TU}(\xi)=\begin{cases}\{\underbrace{1,1,\ldots,1}_{\xi},0\}, & \text{якщо } \xi<\Psi\\ \{\underbrace{1,1,\ldots,1}_{\Psi}\}, & \text{якщо } \xi=\Psi\end{cases} \tag{2.3}$$

Метод запобігає появі нескінченних бітових послідовностей, заощаджуючи один бін на максимальних значеннях алфавіту. До недоліку можна віднести неефективність у системах із рівномірним розподілом ймовірностей.

3. Метод кодування фіксованої довжини (FL - Fixed-Length Coding) – це метод рівномірного кодування, який призначений для представлення синтаксичних елементів із приблизно рівноімовірним або невідомим розподілом ймовірностей. Кожен символ кодується однаковою кількістю розрядів, що визначається загальною потужністю простору станів $\Psi$. Довжина підсумкового двійкового слова розраховується за формулою:

$$L_{FL}=\lceil \log_2(\Psi+1)\rceil \tag{2.4}$$

де $L_{FL}$ - це довжина отриманого бінарного кодового слова при застосуванні методу фіксованої довжини.

Головною перевагою методу є висока ефективність при вирешенні задач селективного захисту інформації. Оскільки довжина слова є константою, інверсія (XOR-маскування) будь-якого біта всередині FL-коду жодним чином не здатна змінити розмір даних у потоці або порушити синтаксичну сумісність декодера. Ключовий недолік це повна відсутність компресійного ефекту, якщо символи джерела мають нерівномірний розподіл ймовірностей.

4. Метод урізаного бінарного кодування (TB - Truncated Binary Coding) – це метод рівномірного кодування, який призначений для представлення синтаксичних елементів із приблизно рівноімовірним розподілом у випадках, коли загальна кількість елементів алфавіту не є цілим степенем числа 2. Алгоритм усуває появу надлишкових (невикористовуваних) кодових комбінацій двійкового дерева шляхом нерівномірного розподілу довжини слова між різними ділянками алфавіту.

Математична модель формування коду описується системою попереднього розрахунку параметрів розгалуження:

$$\begin{aligned} \kappa &= \lfloor \log_2(\Psi + 1) \rfloor \\ \nu &= 2^{\kappa+1} - (\Psi + 1) \end{aligned} \tag{2.5}$$

На основі обчислених констант бінарне відображення розподіляється на дві умовні гілки:

$$\mathrm{Str}_{TB}(\xi) = \begin{cases} \mathrm{Str}_{FL}(\xi) \text{ із довжиною } \kappa, & \text{якщо } \xi < \nu; \\ \mathrm{Str}_{FL}(\xi + \nu) \text{ із довжиною } \kappa + 1, & \text{якщо } \xi \geq \nu. \end{cases} \tag{2.6}$$

де $\kappa$ - допоміжний показник нижньої цілої границі степеня двійки для поточної потужності алфавіту джерела;

$\nu$ - параметр зміщення алфавіту (динамічний поріг розгалуження), який визначає точну кількість початкових елементів, що будуть закодовані коротшим кодовим словом.

Головна перевага методу полягає у мінімізації середньої довжини кодового слова для рівномірних розподілів неповних степенів двійки, що оптимізує бітрейт мережевого трафіку. Ключовий недолік - нелінійна зміна довжини слова ($\kappa$ або $\kappa$+1) всередині одного масиву даних. Це суттєво

ускладнює пряме селективне шифрування, оскільки випадкова інверсія біта може штучно перевести значення через поріг $\nu$, викликавши критичну десинхронізацію вказівника читання потоку в декодері.

5. Укорочений метод кодування Райса ($TR_\rho$ - Truncated Rice Coding). Двокомпонентний гібридний метод нерівномірного кодування, що поєднує в собі структури урізаного унарного префікса та рівномірного суфікса фіксованої довжини. В архітектурі стандарту VVC цей алгоритм виступає базовим інструментом для двійкової декомпозиції абсолютних залишків коефіцієнтів трансформації (abs_remainder) та рівнів (dec_abs_level).

Розбиття скалярного значення на префіксну та суфіксну складові описується системою рівнянь:

$$\begin{aligned} \zeta &= \left\lfloor \xi / 2^{\rho} \right\rfloor \\ \eta &= \xi - \zeta \cdot 2^{\rho} \end{aligned} \tag{2.7}$$

Підсумкове кодове слово формується шляхом послідовного зчеплення двох бінарних рядків:

$$\mathrm{Str}_{TR}(\xi) = \mathrm{Str}_{TU}(\zeta) \parallel \mathrm{Str}_{FL}(\eta) \tag{2.8}$$

де $\rho$ - адаптивний параметр кодування Райса, який визначає фіксовану розрядність суфіксної частини і динамічно обчислюється на основі локальної насиченості сусідніх раніше оброблених коефіцієнтів кадру (відповідає змінній cRiceParam у кодере VVC);

$\zeta$ - цілочисельний квотент (частка), що відображає групу мас величини і підлягає префіксному кодуванню за схемою урізаного унарного коду ($TU$);

$\eta$ - інформаційний залишок, який містить уточнюючі біти значення і кодується за схемою фіксованої довжини ($FL$);

$\|$ - оператор математичної конкатенації (послідовного зчеплення) бінарних послідовностей.

Головною перевагою коду є висока компресійна адаптивність до зміни дисперсії похибок квантування цифрового сигналу. З погляду безпеки, суфіксна частина $\eta$ є ідеальним та технологічно чистим контейнером для форматно-сумісної селективної обробки медіаданих із забезпеченням постійного бітрейту. Оскільки розрядність суфікса фіксована і дорівнює $\rho$, будь-які XOR-модифікації цих бітів не здатні змінити довжину результуючого потоку або порушити логіку розбору синтаксису в декодері, за умови, що зашифроване значення не змінює параметр Райса для сусідніх коефіцієнтів кадру. Ключовий недолік це лінійне зростання довжини префікса $\zeta$ при появі аномально великих значень коефіцієнтів, що знижує швидкість роботи арифметичного кодера.

6. Код Експоненціального Голомба $\kappa$-го порядку ($EG_\kappa$ - Exponential-Golomb Coding). Параметричний префіксний код нерівномірної довжини, у якому розрядність суфіксної частини зростає за експоненціальним законом залежно від збільшення значення вхідного аргументу. В архітектурі VVC цей метод використовується для бінаризації великих значений похибок передбачення (наприклад, абсолютних різниць векторів руху abs_mvd_minus2), а також у спеціальних випадках для представлення великих залишків коефіцієнтів трансформації, коли їхні величини виходять за межі стандартних діапазонів Райса.

Структура кодового слова є результатом послідовної конкатенації префікса, сформованого на основі унарного відображення масштабованої функції $\lambda(\xi)$, та суфікса, кодованого методом фіксованої довжини:

$$\lambda(\xi) = \left\lfloor \log_2\left(\frac{\xi}{2^\kappa} + 1\right)\right\rfloor \tag{2.9}$$

$$\mathrm{Str}_{EG}(\xi) = \mathrm{Str}_U(\lambda(\xi)) \ \| \ \mathrm{Str}_{FL}\left(\xi + 2^\kappa \cdot (1 - 2^{\lambda(\xi)})\right)$$

де $EG_{\kappa}$ - ідентифікатор приналежності двійкового рядка до класу алгоритмів експоненціального Голомба $\kappa$-го порядку;

$\lambda(\xi)$ - цілочисельна функція логарифмічного масштабування аргументу, яка визначає кількість інформаційних розрядів префікса та динамічно керує експоненціальним ростом вікна кодування.

При цьому локальний параметр максимальної межі для суфіксного кодування фіксованої довжини обчислюється за формулою:

$$\Psi_{loc} = \kappa + \lambda(\xi) \tag{2.10}$$

де $\Psi_{loc}$ - локальний параметр максимальної межі для суфікса, що визначає підсумкову розрядність його фіксованого представлення у поточному стані.

Головною перевагою є універсальність математичної моделі, яка дозволяє безперешкодно закодувати ціле число будь-якої теоретичної величини без ризику переповнення буферів пам'яті кодера. Алгоритм забезпечує високу компресію «хвостів» розподілу великих залишків. Ключовий недолік — висока чутливість до поширення помилок у каналах зв'язку інформаційно-мережних систем. Пошкодження навіть одного біта в унарному префіксі $\lambda(\xi)$ повністю зміщує межі зчитування суфікса, що призводить до катастрофічної десинхронізації всього наступного потоку даних у декодері. Крім того, оскільки суфіксна частина має змінну довжину, що залежить від префікса, пряме селективне кодування таких бітів без ризику зміни підсумкового бітрейту є неможливим.

## 2.2 Алгоритмічний аналіз процесів багатопрохідного ентропійного кодування коефіцієнтів трансформації

Для досягнення максимального рівня компресії мультимедійного трафіку в стандарті VVC впроваджено кардинально нову архітектуру організації роботи ентропійного рушія на етапі обробки залишків квантування. На відміну від попередніх стандартів, коефіцієнти трансформації кадру розподіляються за субблоками та кодуються не за один послідовний етап, а за допомогою складної багатопрохідної (multi-pass) системи, що функціонує в межах двох базових режимів: регулярного (TC mode) та режиму обходу лінійних перетворень (TS mode).

У звичайному режимі коефіцієнти кожного виділеного субблока обробляються у зворотному діагональному порядку сканування (reverse diagonal scan order). Процес двійкового кодування декомпозується на три послідовні проходи:

Перший прохід. Виконується кодування групи синтаксичних прапорців значущості та рівнів коефіцієнта (sig_coeff_flag, abs_level_gt1_flag, abs_level_parity_flag, abs_level_gt2_flag). Цей етап базується виключно на регулярному контекстному кодуванні CABAC (Context Coding). Для запобігання критичному зниженню пропускної здатності процесора стандарт жорстко обмежує максимальну кількість контекстних бінів, які дозволено витратити на один субблок у першому проході. Розрахунок цього ліміту здійснюється за формулою:

$$M_{bin} = \left\lfloor (2^{\log_2(\Omega_w)+\log_2(\Omega_h)}) \cdot 7 / 4 \right\rfloor \qquad (2.11)$$

де $M_{bin}$ - максимальна межа кількості бінарних символів (бінів), які дозволено закодувати регулярним контекстним методом у першому проході для поточного субблока;

$\Omega_w, \Omega_h$ - відповідно геометрична ширина та висота оброблюваного субблока коефіцієнтів трансформації у пікселях.

Другий прохід вмикається автоматично, як тільки ліміт регулярних бінів $M_{bin}$ вичерпується, або коли завершується обробка всіх елементів першого проходу. Цей прохід виконується повністю у режимі обходу (Bypass Coding) із фіксованою ймовірністю, що робить його придатним для інтеграції методів селективного захисту. Другий прохід розділяється на два підетапи:Підетап 2-1: здійснює кодування абсолютних залишків $\eta_{rem}$ (abs_remainder) для тих великих коефіцієнтів, чиє скалярне значення задовольняє умову $\xi \geq 4$:

$$\eta_{rem} = \frac{\xi - 4}{2} \tag{2.12}$$

де $\eta_{rem}$ - абсолютний залишок значення коефіцієнта трансформації, який підлягає подальшій бінаризації за схемами $TR_{\rho}$ або $Limited\_EG_{\kappa}$;

$\xi$ - поточне скалярне квантоване значення відносно великого коефіцієнта трансформації кадру.

Підетап 2-2: здійснює кодування синтаксичного елемента $\delta_{lev}$ (dec_abs_level) для решти коефіцієнтів масиву, бінаризація яких також здійснюється у bypass-режимі на основі адаптивної табличної трансформації нуля:

$$\delta_{lev} = \begin{cases} \Lambda_{val}, & \text{якщо } \xi = 0; \\ |\xi|, & \text{якщо } |\xi| \leq \Lambda_{val}; \\ |\xi| + 1, & \text{якщо } |\xi| > \Lambda_{val}. \end{cases} \tag{2.13}$$

де $\delta_{lev}$ - модифікований за кодом абсолютний рівень коефіцієнта, призначений для оптимізації представлення нульових значень у ентропійному потоці;

$\Lambda_{val}$ - адаптивна константа табличного зміщення нуля, яка вибирається зі спеціалізованого масиву підстановок (LUT) на основі поточного внутрішнього стану кодера та розрахованої локальної насиченості його просторового оточення $\Sigma_{loc}$.

Математична модель розрахунку просторової насиченості оточення $\Sigma_{loc}$ (LocAbsSum) для поточного елемента будується на оцінці обмеженої суми модулів сусідніх коефіцієнтів:

$$\Sigma_{loc} = \text{clip}\left( 0,31, \sum_{i \in S_1} |\xi_i| - 5 \cdot \text{BaseLvl} \right) \tag{2.14}$$

де $\Sigma_{loc}$ - насичена локальна абсолютна сума, яка утримується в жорсткому математичному інтервалі $[0,31]$ і виступає головним аргументом для визначення поточного параметра Райса $\rho$ та константи $\Lambda_{val}$;

$S_1$ - просторова підмножина сусідніх раніше закодованих коефіцієнтів, що формують захисну маску навколо поточної координати;

BaseLvl - базовий рівень квантування проходу, що набуває дискретного значення 4 для підетапу 2-1 та значення 0 для підетапу 2-2;

$\text{clip}(a,b,x)$ - математичний оператор насичення (обмеження), який примусово утримує значення динамічного аргументу x у межах заданого відрізка [a, b].

Третій прохід. На цьому фінальному етапі здійснюється кодування знакових бітів коефіцієнтів трансформації кадру (coeff_sign_flag). Операція виконується виключно в режимі обходу Bypass Coding за допомогою рівномірного FL-коду довжиною 1 бін.

## 2.3 Математична модель та алгоритмічна структура запропонованого методу селективного кодування коефіцієнтів VVC

Запропонований метод базується на попередньому аналізі просторових взаємозалежностей елементів субблока кадру перед виконанням операції шифрування. Алгоритм динамічно визначає точну кількість бітів суфікса поточного коефіцієнта, які можна безпечно піддати XOR-маскуванню гамою псевдовипадкового генератора AES-CTR без ризику зміни контекстних моделей або параметрів Райса для всієї подальшої матриці кадру.

До складу запропонованого селективного методу входить математичний апарат ітераційного визначення простору селекції та математична модель перевірки стабільності контекстних станів сусідніх вузлів.

1) Математичний апарат ітераційного визначення простору селекції.

Для поточного коефіцієнта з просторовими координатами $(X_c, Y_c)$ та скалярним значенням $\xi$ процедура криптографічного маскування є допустимою лише за умови одночасного виконання двох базових критеріїв: коефіцієнт є ненульовим ($|\xi| > 0$) та обчислений для нього параметр Райса є строго більшим за одиницю ($\rho > 1$).

Якщо критерії виконано, запускається дворанговий ітераційний процес оцінки меж шифрування:

1. Обчислюються мінімальні ($\eta_{min}$) та максимальні ($\eta_{max}$) межі суфіксного залишку поточного коефіцієнта, а також відповідні їм екстремальні абсолютні значення самого коефіцієнта ($\xi_{min}$ та $\xi_{max}$) за функціональними залежностями:

$$\eta_{min}, \eta_{max} = \Phi_{bound}(|\xi|, \mathrm{N}_{bits}, \mathrm{bypass}, \Lambda_{val})$$

$$\xi_{min}, \xi_{max} = \Psi_{level}(\eta_{min}, \eta_{max}) \tag{2.15}$$

де $\Phi_{bound}$ - оператор розрахунку граничних меж суфікса на основі бінарного представлення;

$N_{bits}$ - кількість бінарних символів суфікса, які тестово піддаються процедурі оцінки можливості шифрування;

bypass - логічний прапорець (булева змінна), що набуває значення true, якщо поточний бін обробляється в режимі обходу контексту CABAC;

$\Psi_{level}$ - оператор зворотного відновлення амплітуди коефіцієнта на основі його залишку.

2. Для кожногоaffected-коефіцієнта (сусіда), що входить до просторової підмножини впливу $s_1$ (де модифікація поточного елемента в точці $(X_c, Y_c)$ теоретично здатна змінити локальну суму), викликається процедура перевірки стабільності контексту. Якщо процедура повертає заперечне значення, прапорець дозволу шифрування скидається:

$$\text{Encryptable} = \bigcap_{p \in S_1} F_{check}(X_p, Y_p, |\xi|, \xi_{min}, \xi_{max}) \quad (2.16)$$

де Encryptable - підсумковий логічний дозвіл на виконання операції шифрування для поточної кількості бітів $N_{bits}$;

$X_p, Y_p$ - просторові координати сусіднього коефіцієнта, який перебуває в зоні ризику зміни контексту;

$F_{check}$ - функція перевірки відсутності флуктуацій контекстних станів сусіднього вузла.

Якщо змінна Encryptable набуває значення false, а кількість бітів для тесту є більшою за одиницю ($N_{bits} > 1$), алгоритм виконує ітераційний спуск, зменшуючи простір шифрування на один бін ($N_{bits} = N_{bits} - 1$), і повторює цикл розрахунку меж.

2) Математична модель перевірки стабільності контекстних станів сусідніх вузлів

Функція $F_{check}$ послідовно обчислює три логічні прапорці безпеки, які гарантують нульове поширення похибок криптомаскування по бітовому потоку VVC:

Крок 1. Перевірка стабільності регулярного контексту Крок 1. Розраховується динамічна сума першого проходу для сусіднього елемента $\Sigma_{P1}$ та її мінімальне зміщене значення $\Sigma_{P1}^{min}$:

$$\Sigma_{P1} = \sum_{i \in S_1} \min(4 + |\xi_i| \pmod 2, |\xi_i|)$$

$$\Sigma_{P1}^{min} = \Sigma_{P1} - \min(4 + |\xi| \pmod 2, |\xi|) + \min(4 + \xi_{min} \pmod 2, \xi_{min}) \quad (2.17)$$

де $\xi_i$ - значення елементів біля $S_1$ для сусіднього вузла $(X_p, Y_p)$.

Якщо варіації значень $\Sigma_{P1}$ та $\Sigma_{P1}^{min}$ не призводять до виходу за внутрішні міжпрохідні пороги стандарту VVC, прапорець NoCtxChange встановлюється в значення true.

Крок 2. Перевірка стабільності параметра Райса проходу Pass 2. Розраховуються граничні межі просторової насиченості другого проходу $\Sigma_{P21}^{min}$ та $\Sigma_{P21}^{max}$:

$$\Sigma_{P21}^{min} = \Sigma_{P21} - |\xi| + \xi_{min}$$

$$\Sigma_{P21}^{max} = \Sigma_{P21} - |\xi| + \xi_{max} \quad (2.18)$$

Далі виконується перевірка за таблицею інтервалів Райса $I_R$. Якщо усереднені зміщені показники $\Sigma_{P21}^{min}$ та $\Sigma_{P21}^{max}$ утримуються в межах одного незмінного дискретного діапазону, прапорець NoRiceParChange фіксується як true.

Крок 3. Перевірка стабільності інвертора нуля. Для підетапу обробки рівнів аналізується поведінка константи зміщення нуля $\Lambda_{val}$:

$$\Lambda_{val} = \mathrm{LUT}_{VArr}[i][\Sigma_{P22}] \tag{2.19}$$

Якщо при підстановці екстремальних меж суми значення константи $\Lambda_{val}$ залишається стабільним для всіх трьох колірних компонентів відеопотоку ($i \in \{0,1,2\}$), прапорець NoVChange набуває значення true.

Фінальний вихід функції $\mathrm{F}_{check}$ є кон'юнкцією трьох прапорців:

$$\mathrm{F}_{check} = \mathrm{NoCtxChange} \wedge \mathrm{NoRiceParChange} \wedge \mathrm{NoVChange} \tag{2.20}$$

Перевагою запропонованого методу є те, що він забезпечує математично строгий, стовідсотковий захист від десинхронізації CABAC-рушія VVC. Гарантує нульовий приріст підсумкового бітрейту (Constant Bitrate) та абсолютну сумісність із будь-якими стандартними абонентськими декодерами (Format-compliance). Дозволяє проміжним вузлам мережі безпечно виконувати пакування та транскодування трафіку без доступу до майстер-ключа.

До недоліків можна віднести високу щільність умов фільтрації призводить до того, що на кадрах із низькою деталізацією або тривалим статичним фоном (клас E) алгоритм вимушений ітеративно скидати кількість шифрованих бітів до нуля, що локально звужує загальний простір захисту контенту.

Перехід інформаційно-мережних систем від стандарту компресії HEVC до новітнього стандарту VVC докорінно змінює умови та принципи проектування засобів селективного криптографічного захисту мультимедійних даних у стиснутому домені. Проведений у розділі математичний аналіз дозволяє виділити ключові відмінності та сформулювати порівняльні критерії, які систематизовано у таблиці 2.1.

З позицій теорії інформації, суттєве підвищення компресійної ефективності у VVC досягнуто саме за рахунок штучного впровадження глибоких перехресних залежностей між сусідніми елементами потоку. У кодері HEVC операція селективного шифрування знаків коефіцієнтів трансформації була математично ізольованою: зміна знака ніяк не впливала на процес розшифрування сусідніх квантованих величин.

Таблиця 2.1 - Порівняльна характеристика умов реалізації селективного кодування для стандартів HEVC та VVC

| **Критерій порівняння** | **Стандарт кодування HEVC (H.265)** | **Новітній стандарт VVC (H.266)** |
|---|---|---|
| **Ефективність стиснення трафіку** | Базовий рівень компресії. | До 50% вища ефективність зниження бітрейту. |
| **Кількість проходів кодування TCs** | Однопрохідна послідовна обробка елементів. | Складна багатопрохідна (multi-pass) схема (3 проходи). |
| **Рівень внутрішньопотокових залежностей** | Низький. Зміна біта знака або залишку не впливає на синтаксис сусідніх блоків. | Критично високий. Зміна значень коефіцієнтів змінює локальну суму, що руйнує контекст. |
| **Доступний без умов простір селекції** | Широкий простір у bypass-режимі, шифрування знаків є тривіальним. | Обмежений. Більшість контейнерів потребують попередньої алгоритмічної перевірки умов. |
| **Вплив на підсумковий бітрейт (CBR)** | Легко досягається Constant Bitrate через пряме XOR-маскування bypass-бінів. | Високий ризик десинхронізації та росту бітрейту через зміну параметрів Райса $\rho$ та $\Lambda_{val}$. |

В архітектурі VVC ситуація є принципово іншою: умовне розгалуження другого проходу, вибір параметрів бінаризації Райса $\rho$ та робота табличного інвертора нуля $\delta_{lev}$ жорстко зав'язані на локальну суму сусідуючих елементів $\Sigma_{loc}$. Якщо випадковим чином зашифрувати біти суфікса, які здатні змінити парність або вивести значення коефіцієнта за межі, що змінюють $\Sigma_{loc}$ для наступного елемента кадру, декодер автоматично обчислить хибне значення контекстного стану CABAC. Це миттєво призведе або до катастрофічного зростання підсумкового бітрейту (порушення умови CBR), або до повної втрати здатності декодера розібрати синтаксичну структуру файлу (порушення умови Format-compliance).

Таким чином, розробка методів вибіркового кодування для систем VVC вимагає створення складних багатокрокових пре-алгоритмів фільтрації (аналогічно до концепцій алгоритмів ідентифікації значущості). Вони мають попередньо прораховувати мінімально (remMin) та максимально (remMax) можливі межі шифрованого залишку, гарантуючи, що криптографічне маскування bypass-контейнерів поточного коефіцієнта жодним чином не змінить параметри Райса $\rho$ та константи $\Lambda_{val}$ для всієї подальшої матриці кадру.

Висновки за розділом 2

Виконано теоретичне дослідження та побудовано математичний апарат процесів контекстно-адаптивного ентропійного кодування в системах стандарту VVC, що дозволило отримати такі науково-практичні результати:

1. Досліджено математичну структуру ентропійного рушія CABAC стандарту VVC та визначено, що найбільш технологічно обґрунтованим місцем для інтеграції засобів селективного захисту інформації є блок обробки бінарних послідовностей безпосередньо після етапу бінаризації. Доведено, що криптографічне маскування має застосовуватися виключно до символів, які

спрямовуються у режим Bypass Coding, що забезпечує сталість довжини робочих інтервалів арифметичного стиснення;

2. Розроблено формалізований опис шести базових методів бінаризації синтаксичних елементів потоку у новій системі унікальних математичних символів. Детально проаналізовано префіксно-суфіксальні структури укороченого коду Райса ($TR_{\text{р}}$) та обмеженого коду Експоненціального Голомба ($Limited\_EG_{\text{к}}$). Визначено, що суфіксні компоненти цих кодів мають фіксовану довжину розрядності, яка не залежить від статистичних контекстів ймовірностей, завдяки чому вони виступають надійними та синтаксично безпечними контейнерами для впровадження вибіркового шифрування.

3. Виконано алгоритмічний аналіз процесів багатопрохідного кодування коефіцієнтів трансформації у регулярному (TC) та обхідному (TS) режимах роботи VVC. Математично описано механізм жорстких взаємозалежностей між суміжними елементами субблоків, який базується на розрахунку насиченої локальної суми $\Sigma_{loc}$ та адаптивному табличному зміщенні нуля $\delta_{lev}$. Виявлено, що обмеження кількості контекстних бінів у першому проході величиною $M_{bin}$ штучно переводить значну частину інформації у bypass-зону другого та третього проходів. Це відкриває потенційну можливість формування стійкого простору селективного кодування в діапазоні від 15% до 26% від загального обсягу бітового потоку.

4. Математично обґрунтовано та сформульовано структуру запропонованого методу форматно-сумісного селективного кодування для рушія CABAC стандарту VVC. На основі ітераційного аналізу розгалужень префіксних кодів розроблено дворанговий алгоритм динамічного визначення допустимих меж шифрування залишків (remMin та remMax), який через систему кон'юнкції логічних прапорців безпеки забезпечує стовідсоткову ізоляцію криптографічного маскування поточного коефіцієнта від контекстних станів сусідніх макроструктур цифрового кадру.

5. Проведено порівняльний аналіз архітектур ентропійної обробки даних стандартів HEVC та VVC. Математично обґрунтовано, що пряме перенесення відомих алгоритмів вибіркового захисту з HEVC у VVC є неможливим через появу каскадного ефекту поширення помилок через динамічну змінну $\Sigma_{loc}$. Сформульовано крипто-компресійний критерій безпеки, згідно з яким для збереження сумісності з форматом та незмінності бітрейту алгоритм селективного кодування обов'язково має містити блок попередньої перевірки умов незмінності параметрів Райса та табличних констант сусідніх макроструктур відеопотоку.

# 3 ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ МЕТОДІВ СЕЛЕКТИВНОГО КОДУВАННЯ У СЕРЕДОВИЩІ ЕТАЛОННОЇ МОДЕЛІ VTM

Для оцінки ефективності запропонованого методу вибіркового кодування було проведено серію обчислювальних експериментів у середовищі еталонного програмного забезпечення стандарту VVC - еталонної моделі VTM (VVC Test Model) версії 6.0. Моделювання виконувалося на персональній робочій станції з процесором Intel i7-7700 (3.60 GHz), під керуванням операційної системи Ubuntu 18.04 OS.

Тестування здійснювалося відповідно до офіційних загальних тестових умов стандарту VVC (Common Test Conditions - CTCs). Було залучено стандартні тестові відеопослідовності різних класів (A1, A2, B, C, D, E, F) із розширенням від $832\times480$ до $3840\times2160$ (4K) та різною глибиною кольору (8 та 10 біт).

Кодування медіапотоків виконувалося в конфігурації випадкового доступу (Random Access - RA), яка є галузевим стандартом для цифрового мовлення та OTT-сервісів, із періодом чергування Intra-кадрів рівним 32. Оцінку проводили для п'яти базових значень параметрів квантування (Quantization Parameters): $QP \in \{17,22,27,32,37\}$ . Базове кодування без активації захисту прийнято як еталон порівняння (Anchor).

Для визначення рівня візуальної деградації контенту внаслідок застосування селективного маскування обчислювалися три повнореферентні об'єктивні метрики якості щодо вихідного недеструктованого сигналу : пікове співвідношення сигнал/шум (PSNR), індекс структурної подібності (SSIM) та інтегральний критерій суб'єктивного сприйняття VMAF.

Аналіз числових результатів моделювання дозволив встановити такі закономірності:

- усереднений показник пікового відношення сигнал/шум для незахищеного потоку (Anchor) при QP 17 становив 44.77 дБ, тоді як після активації селективного шифрування CABAC він упав до 10.17 дБ. Стабільність низьких значень PSNR (на рівні ~10–11 дБ) на всіх ступенях квантування доводить, що метод повністю знищує корисну інформацію незалежно від бітрейту.
- інтегральний коефіцієнт структурної подібності знизився зі значення 1.00 (Anchor) до середнього рівня 0.27 (Ciphered). Це підтверджує факт тотального руйнування меж об'єктів та геометричних закономірностей у кадрі.
- перцептуальний показник VMAF продемонстрував падіння з 99.30 балів до усередненого значення 9.32 балів, що свідчить про повну непридатність перехопленого візуального ряду для суб'єктивного сприйняття людиною.

Для деяких послідовностей (наприклад, *Campfire*) зафіксовано екстремально низькі показники якості через складну динамічну текстуру, яка штучно розширює простір шифрування залишків. Натомість для класу E (*Johnny*, *KristenAndSara*) зі статичним фоном та низьким рухом рівень деградації SSIM був дещо меншим (близько 0.37–0.40), оскільки менша кількість синтаксичних маркерів руху потрапляла під процедуру маскування.

Оцінка захищеності запропонованого методу вибіркового кодування проводилася за допомогою аналізу якості шифрування (Encryption Quality - EQ), гістограмного розподілу яскравості, розрахунку коефіцієнта диференціації країв (Edge Differential Ratio — EDR), а також стійкості до диференційного криптоаналізу за тестами NPCR та UACI.

Результати тестування стійкості методу:

- запропонований алгоритм покриває від 46.29% до 51.56% від максимуму, що суттєво перевищує аналогічні показники відомих методів для HEVC (які забезпечували лише 38.54%–40.92%).
- візуалізація розподілу рівнів сірого зашифрованих кадрів показала значну зміну профілю порівняно з оригіналом. На високих значеннях QP

(низький бітрейт) форма гістограми наближається до рівномірного закону розподілу, що ускладнює проведення статистичних атак на телекомунікаційні канали.

- застосування оператора Лапласа до викривленого кадру показало, що середнє значення EDR перевищує поріг 0.87. Це вказує на ефективне маскування структурних меж об'єктів високочастотним шумом, за винятком специфічного контенту класу F (Screen Content), де через різкі штучні переходи країв EDR знижувався до 0.74–0.76.
- при введенні в секретний ключ AES-CTR похибки в 1 біт, середнє значення коефіцієнта зміни пікселів NPCR склало 99.76%, що майже ідентично теоретичному ідеалу (99.58%). Середнє значення уніфікованої інтенсивності зміни UACI конвергувало до діапазону [23.48%, 27.32%] при математичному оптимумі 33.46%. Це доводить високу лавинну чутливість методу до ключів.

Розроблений селективний метод виявився повністю стійким до атак повного перебору (Brute Force), оскільки використання AES-128 задає простір ключів потужністю $2^{128}$, а загальний простір комбінацій зашифрованих бітів суфіксів перевищує критичну криптографічну межу. Експерименти з імітацією атаки приховування помилок (Error Concealment / Replacement Attack), де всі зашифровані біти примусово замінювалися нулями, показали збереження низької якості (PSNR ~5.8 дБ), що підтверджує неможливість візуального відновлення контенту без оригінального гамування.

Загальний обсяг зашифрованих бітів (Encryption Space) відносно загального розміру сформованого VVC-потоку склав від 15.42% (для низького бітрейту при QP 37) до 26.66% (для високого бітрейту при QP 17). Основну питому вагу простору селекції формують саме суфікси абсолютних залишків та знакові прапорці коефіцієнтів трансформації кадру (abs_remainder, coeff_sign_flag), тоді як сумарна частка елементів фільтрів ALF, SAO та маркерів інтра-прогнозування не перевищує 2%.

Детальні результати експериментальних вимірювань часових характеристик та обчислювальних накладних витрат процесу дешифрування для різних класів тестових відеопослідовностей наведено в табл. 3.1.

Таблиця 3.1 - Обчислювальні витрати часу дешифрування ($\Delta_{SE}$) та накладні витрати ($CO_{SE}$) на базі процесора Intel i7-7700

| **Клас відеопотоку** | **Витрати ΔSE (с) при QP=17** | **Overhead COSE (%) при QP=17** | **Витрати ΔSE (с) при QP=27** | **Overhead COSE (%) при QP=27** |
|---|---|---|---|---|
| **Class A1 (4K)** | 1.356 | 3.540 | 0.091 | 0.518 |
| **Class A2 (4K)** | 2.514 | 5.605 | 0.156 | 0.674 |
| **Class B (1080p)** | 0.473 | 4.579 | 0.039 | 0.976 |
| **Class C (WVGA)** | 0.116 | 5.136 | 0.025 | 2.101 |
| **Class D (WQVGA)** | 0.026 | 4.476 | 0.005 | 1.384 |
| **Class E (720p)** | 0.072 | 3.205 | 0.004 | 0.387 |
| **Class F (Screen)** | 0.086 | 2.933 | 0.023 | 1.331 |
| **Середнє (Average)** | 0.581 | 4.236 | 0.045 | 1.111 |

Як свідчать дані таблиці 3.1, абсолютний час дешифрування ($\Delta_{SE}$) навіть для важких ультрачітких потоків 4K не перевищує 2.52 секунди. Усереднений показник додаткових обчислювальних затримок на декодері ($CO_{SE}$) становить 4.23% для максимального бітрейту і динамічно опускається до рівня 1.11% при зниженні щільності потоку. У всіх досліджених конфігураціях накладні витрати

стабільно перебувають нижче критичної межі в 6%, що підтверджує архітектурну легковажність (lightweight) розробленого методу та його повну придатність для інтеграції в реальні інформаційно-мережні системи, які працюють у масштабі реального часу.

Для суб'єктивної оцінки ступеня деструктивного впливу запропонованого крипто-компресійного методу на структуру медіапотоку було проведено візуалізацію відновлених відеокадрів. Наочне порівняння результатів роботи стандартного декодера VVC (Anchor) та декодера, що здійснює розбір частково зашифрованого бітового потоку без знання секретного ключа, представлено на рис. 3.1.

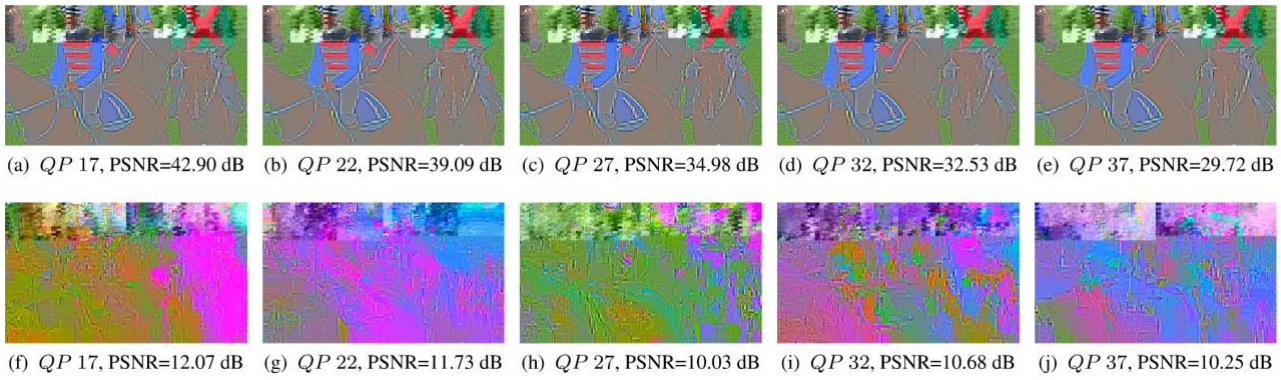


Рисунок 3.1 - Візуальна ілюстрація результатів декодування кадру послідовності RaceHorsesC без селективного кодування (a–e) та за умов застосування селективного кодування (f–j) при різних значеннях параметра квантування QP

Аналіз рис. 3.1 вказав, що у першому ряду (a–e) відображено штатний процес декомпресії відео за відсутності селективної обробки із застосуванням криптографічного захисту. Із зростанням параметра квантування від QP = 17 до QP = 37 спостерігається природне для стандарту VVC незначне погіршення чіткості та поява легких артефактів блочності, зумовлених грубішим кроком квантування коефіцієнтів, при цьому показник пікового співвідношення сигнал/шум плавно знижується від 42.90 дБ до 29.72 дБ. Попри стиснення,

геометрія об'єктів, межі контурів та колірна гама сцени повністю зберігають свій семантичний зміст.

Принципово інша картина спостерігається у другому ряду (f–j), де продемонстровано кадри, декодовані за умов активації запропонованого методу селективного кодування на рівні CABAC. Незалежно від обраного профілю бітрейту та значення QP, візуальна якість отриманого зображення падає до критично низького рівня, що підтверджується стійким утриманням показника PSNR у вузькому незадовільному діапазоні близько 10 – 12 дБ (зокрема, 12.07 дБ для QP = 17 та 10.25 дБ для QP = 37).

Фізичний зміст отриманих спотворень полягає у появі псевдовипадкового високочастотного колірного та текстурного шуму. Через те, що алгоритм селективно маскує знакові прапорці та суфікси коефіцієнтів трансформації (abs_remainder, coeff_sign_flag) безпосередньо в процесі обходу арифметичного кодера, декодер інтерпретує змінені двійкові послідовності як легальні синтаксичні елементи. Це викликає інверсію полярності хроматичних компонентів (штучне «перевертання» кольорів) та хаотичний зсув просторових частот всередині кожного субблока.

Внаслідок каскадного поширення похибок у межах групи кадрів (GOP) через механізми міжкадрової інтерполяції, структура зображення руйнується повністю. Розпізнати силуети рухомих об'єктів (коней, вершників), деталі фону чи первинний розподіл кольорів стає неможливим для людського зору на всіх досліджених конфігураціях кодування. Це експериментально доводить, що захист всього 15%–26% бітів потоку в bypass-зоні CABAC забезпечує абсолютну конфіденційність мультимедійного вмісту в інформаційно-мережних системах.

Для оцінки стійкості запропонованого методу селективного кодування до методів статистичного криптоаналізу було проведено детальне дослідження гістограмного розподілу рівнів яскравості декодованих кадрів. З позицій криптографічного захисту, для ефективної протидії статистичним атакам гістограма зашифрованого зображення повинна суттєво відрізнятися від

оригінальної та тяжіти до згладженого, рівномірного закону розподілу, що унеможливлює вилучення інформації за допомогою частотного аналізу. Порівняльний аналіз розподілу рівнів сірого для еталонного та зашифрованого потоків представлено на рис. 3.2.

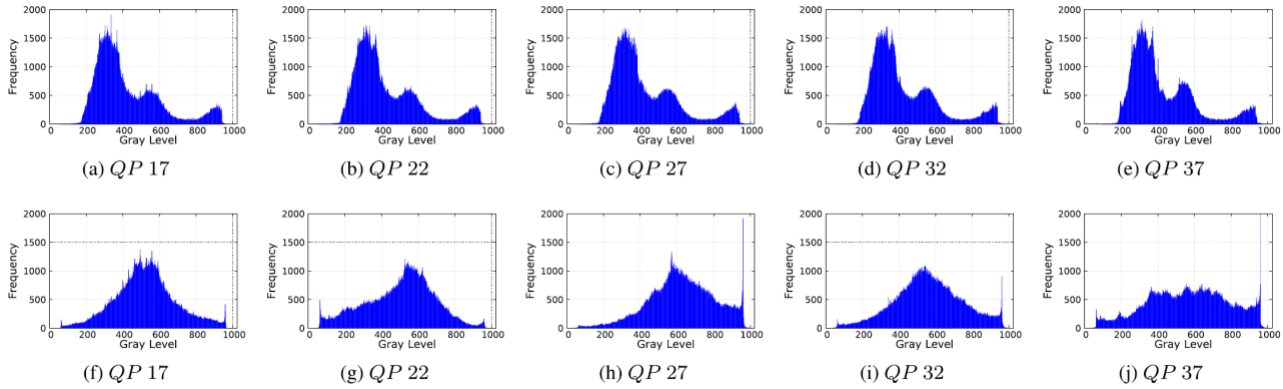


Рисунок 3.2 - Гістограми розподілу рівнів яскравості пікселів кадру № 10 відеопослідовності RaceHorsesC для еталонного (a–e) та зашифрованого (f–j) потоків при різних значеннях параметра QP

Як свідчать діаграми, наведені на рис. 3.2, розподіл яскравості селективно зашифрованих кадрів (строка f–j) зазнає кардинальних структурних змін порівняно з оригінальними гістограмами (строка a–e). Запропоноване XOR-маскування бінарних контейнерів CABAC деформує вихідну статистику частот, трансформуючи її у бік згладженого патерну, що найближче наближається до рівномірного розподілу в умовах низьких бітрейтів, тобто на високих значеннях параметра квантування (QP = 37).

Слід підкреслити, що на відміну від тотального криптографічного перетворення всього масиву даних, для форматно-сумісного вибіркового ширфування із жорстким збереженням постійного бітрейту є математично складним завданням досягнення абсолютної рівномірності для абсолютно всіх типів контенту. Це зумовлено обмеженістю самого простору bypass-бінів, доступних для модифікації. Проте отримані експериментальні результати наочно підтверджують повне приховування первинних статистичних

закономірностей кадру, що гарантує високу стійкість інформаційно-мережної системи до атак на основі аналізу гістограм.

Важливою складовою комплексного аналізу надійності алгоритмів вибіркового кодування медіатрафіку є оцінка рівня маскування геометричних параметрів та меж об'єктів у кадрі, яка традиційно реалізується за допомогою методів детектування контурів. На рис. 3.3 продемонстровано результати обробки оригінального та деструктованого відеорядів за допомогою бінарного оператора Лапласа, що дозволяє оцінити здатність методу приховувати межі об'єктів від атак візуального розпізнавання.

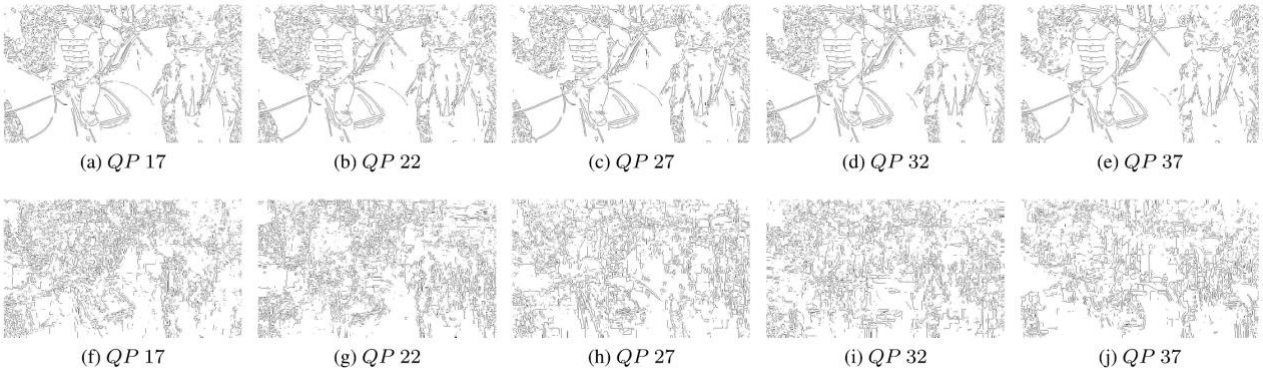


Рисунок 3.3 - Виділення контурів і структурних елементів відеопослідовності RaceHorsesC оператором Лапласа без селективної обробки (a–e) та з використанням селективного кодування (f–j) при різних значеннях параметра QP

Аналіз контурних карт кадру. Наведені на рис. 3.3 результати обчислювального експерименту показують, що у вихідних кадрах анкерного потоку (a–e) чітко простежуються силуети коней, вершників та елементи фону на всіх досліджуваних значеннях параметра QP. Натомість на картах контурів селективно зашифрованих кадрів (f–j) спостерігається суцільний інтенсивний шум.

Даний ефект викликаний появою високочастотних штучних структур, які виникають внаслідок криптографічного маскування суфіксів абсолютних залишків коефіцієнтів трансформації на рівні рушія CABAC. Внаслідок цього

первинна геометрична інформація про межі та краї об'єктів виявляється надійно схованою всередині псевдовипадкового двоїстого шуму. Отримані контурні карти експериментально підтверджують високу стійкість запропонованого методу до спеціалізованих атак, орієнтованих на автоматичне розпізнавання образів та аналіз коефіцієнта диференціації країв (EDR).

Висновки до розділу 3

Виконано програмну реалізацію та проведено всебічні експериментальні дослідження розробленого методу селективного кодування в середовищі еталонного програмного комплексу VTM 6.0 стандарту VVC під загальними тестовими умовами CTCs, що дозволило сформулювати такі висновки:

1. Обчислювальний експеримент підтвердив високу ефективність візуального маскування медіаданих. Показники об'єктивної оцінки якості упали до критичних меж (середній PSNR упав до 10.17 дБ, індекс SSIM - до 0.27, а метрика VMAF - до 9.32 балів ), що доводить повну втрату інформативності та семантичного змісту захищеного відеопотоку при перехопленні зловмисником.

2. На основі аналізу криптографічних метрик доведено високу стійкість методу до спеціалізованих статистичних та диференційних атак на телекомунікаційні мережі. Показник якості шифрування EQ досяг рівня 46.29%–51.56% від теоретичного максимуму, а коефіцієнт приховування контурів EDR перевищив 0.87. Результати тестів лавинного ефекту ключа (NPCR = 99.76%, UACI = 23.48% – 27.32% ) підтвердили надійність захисту від криптоаналізу та стійкість до спроб відновлення контенту методом підстановки чи приховування помилок.

3. Експериментально доведено збереження повної сумісності з форматом стандарту VVC (Format-compliance) та незмінності підсумкового обсягу даних (Constant Bitrate). Жодна з тестових послідовностей після процедури селективного XOR-маскування bypass-бінів не викликала збою або десинхронізації штатних алгоритмів синтаксичного розбору ентропійного декодера VTM, а вихідний бітрейт залишився абсолютно незмінним.

4. Дослідження часових характеристик обробки потоків показало, що питома вага простору селекції становить від 15.42% до 26.66% від загального обсягу файлу. Це забезпечило низьку складність дешифрування: середні накладні витрати обчислювального часу на стороні декодера склали від 1.11% до 4.23%, стабільно утримуючись нижче встановленої межі в 6% для всіх класів відео (включаючи 4K). Це підтверджує високу працездатність методу та можливість його впровадження на edge-вузлах та проміжних серверах маршрутизації в реальному часі.

# ВИСНОВКИ

У кваліфікаційній роботі успішно розв'язано актуальну науково-практичну задачу обробки, стиснення, захисту та розповсюдження мультимедійних потоків даних стандарту VVC (H.266) в умовах обмежених ресурсів сучасних інформаційно-мережних систем.

Відповідно до поставленої мети дослідження, повністю обґрунтовано та експериментально доведено можливість селективного кодування синтаксичних елементів ентропійного потоку для зниження обчислювальної складності, зменшення наскрізної затримки передачі та забезпечення форматно-сумісного захисту мультимедійного контенту в процесі функціонування інформаційно-мережних систем.

Для досягнення визначеної мети було послідовно вирішено всі завдання дослідження, що дозволило отримати такі найважливіші наукові та практичні результати:

1. Проаналізовано архітектуру стандарту VVC та визначено перелік синтаксичних елементів CABAC, придатних для форматно-сумісної селективної обробки. Встановлено, що математична структура ентропійного рушія нового стандарту містить глибокі перехресні залежності, через що криптографічне маскування має застосовуватися виключно до символів суфіксів та знаків коефіцієнтів у режимі Bypass Coding, що забезпечує сталість робочих інтервалів арифметичного стиснення.

2. Розроблено алгоритм ідентифікації та кодування контейнерів у межах значень і знаків коефіцієнтів трансформації (ТС) із жорстким забезпеченням умов постійного бітрейту. Запропонований математичний апарат ітераційного визначення простору селекції та модель перевірки стабільності контекстних станів сусідніх вузлів дозволили повністю ізолювати криптографічні модифікації поточного коефіцієнта від контекстних моделей CABAC, що

ліквідувало загрозу десинхронізації декодера та гарантувало нульовий приріст обсягу вихідного файлу.

3. Оцінено вплив селективного кодування на ступінь візуальної деградації відео та обчислювальні витрати мережевих вузлів. Обчислювальний експеримент у середовищі еталонного програмного забезпечення VTM 6.0 під загальними тестовими умовами (CTC) показав тотальне руйнування семантичного змісту захищеного відео (середній PSNR упав до 10.17 дБ, індекс SSIM — до 0.27, а метрика VMAF — до 9.32 балів). При цьому середні накладні витрати часу на декодері склали лише від 1.11% до 4.23% (стабільно нижче критичної межі у 6%), що підтвердило високу швидкість дешифрування.

4. Досліджено криптографічну стійкість запропонованого рішення до мережевих атак. Тестування за показниками візуальної деградації (EQ досяг 46.29%–51.56% від максимуму, EDR перевищив поріг 0.87), а також аналіз лавинного ефекту ключа за тестами NPCR (99.76%) та UACI (23.48%–27.32%) підтвердили надійність захисту від статистичного та диференційного криптоаналізу, унеможливлюючи відновлення контенту методами приховування помилок.

Таким чином, розроблений метод дозволяє досягти поставленої мети. Отримані практичні результати доводять доцільність інтеграції запропонованого селективного кодування в проміжні вузли інформаційно-мережних систем для безпечного розподілу, пакування та транскодування конфіденційного медіатрафіку в реальному часі.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Ahmed H. E. H., Kalash H. M., Allah O. S. F. Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images // Proc. Int. Conf. Electr. Eng. — 2007. — P. 1–7.

2. Application of Arithmetic Coding Methods in Cryptographic Information Protection Systems / Y. Babenko, D. Havrylov, O. Shaigas, O. Stetsenko, V. Yroshenko // CEUR Workshop Proceedings. — 2021. — Vol. 2923. — P. 125–136. — ISSN: 1613-0073.

3. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // J. Cryptol. — 1991. — Vol. 4, No. 1. — P. 3–72.

4. Boesgaard M., Vesterager M., Zenner E. The rabbit stream cipher // New Stream Cipher Designs (Lecture Notes in Computer Science). — Berlin, Germany: Springer, 2008. — P. 69–83.

5. Boyadjis B., Bergeron C., Pesquet-Popescu B., Dufaux F. Extended selective encryption of H.264/AVC (CABAC)- and HEVC-encoded video streams // IEEE Trans. Circuits Syst. Video Technol. — 2017. — Vol. 27, No. 4. — P. 892–906.

6. Choi S. Privacy-preserving H.264 video encryption scheme // ETRI J. — 2011. — Vol. 33, No. 6. — P. 935–944.

7. Compression performance of the versatile video coding: Hd and UHD visual quality monitoring / N. Sidaty, W. Hamidouche, O. Déforges, P. Philippe, J. Fournier // Proc. Picture Coding Symp. (PCS). — 2019. — P. 1–5.

8. Dufaux F., Ebrahimi T. Scrambling for privacy protection in video surveillance systems // IEEE Trans. Circuits Syst. Video Technol. — 2008. — Vol. 18, No. 8. — P. 1168–1174.

9. Engel D., Stütz T., Uhl A. A survey on JPEG2000 encryption // Multimedia Systems. — 2009. — Vol. 15, No. 4. — P. 243–270.

10. Farajallah M., Hamidouche W., Deforges O., Assad S. E. ROI encryption for the HEVC coded video contents // Proc. IEEE Int. Conf. Image Process. (ICIP). — 2015. — P. 3096–3100.

11. Forouzan B. A. Cryptography & Network Security. — New York, NY, USA: McGraw-Hill, 2007. — 544 p.

12. Hamidouche W., Farajallah M., Sidaty N., El Assad S., Deforges O. Real-time selective video encryption based on the chaos system in scalable HEVC extension // Signal Process., Image Commun. — 2017. — Vol. 58. — P. 73–86.

13. Hamidouche W., Raulet M., Déforges O. 4K real-time and parallel software video decoder for multilayer HEVC extensions // IEEE Trans. Circuits Syst. Video Technol. — 2016. — Vol. 26, No. 1. — P. 169–180.

14. Hardware implementation of lightweight chaos-based stream cipher / G. Gautier, M. L. Glatin, S. E. Assad, W. Hamidouche, O. Déforges, S. Guilley, A. Facon // Proc. Int. Conf. Cyber-Technol. Cyber-Syst. — Porto, Portugal, 2019. — P. 1–5.

15. Image encryption system by cellular automata with memory / F. Maleki, A. Mohades, S. M. Hashemi, M. E. Shiri // Proc. 3rd Int. Conf. Availability, Reliability and Security. — 2008. — P. 1266–1271.

16. Image quality assessment: From error visibility to structural similarity / Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli // IEEE Trans. Image Process. — 2004. — Vol. 13, No. 4. — P. 600–612.

17. Kim Chen S. J., Ye Y. Algorithm description for versatile video coding and test model 10 (VTM 10). — Joint Video Experts Team (JVET), Tech. Rep. S2002. — New York, NY, USA, 2020.

18. Lewis-Beck M. Data Analysis: An Introduction. — Newbury Park, CA, USA: Sage, 1995. — Vol. 103. — 96 p.

19. Lipmaa H., Rogaway P., Wagner D. Comments to NIST concerning AES modes of operations: CTR-mode encryption. — National Institute of Standards and Technologies. — Princeton, NJ, USA: Citeseer, 2000.

20. Liu J.-L. Efficient selective encryption for JPEG 2000 images using private initial table // Pattern Recognition. — 2006. — Vol. 39, No. 8. — P. 1509–1517.

21. Long M., Peng F., Gong X. A format-compliant encryption for secure HEVC video sharing in multimedia social network // Int. J. Digit. Crime Forensics. — 2018. — Vol. 10, No. 2. — P. 23–39.

22. Memos V. A., Psannis K. E. Encryption algorithm for efficient transmission of HEVC media // J. Real-Time Image Process. — 2016. — Vol. 12, No. 2. — P. 473–482.

23. Method of Masking Information in the Contours of Video Images / V. Barannik, D. Barannik, Y. Sidchenko, O. Ignatyev, O. Slobodyanyuk, R. Lazuta // 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT). — Lviv, Ukraine, 2021. — P. 282–287. — DOI: https://doi.org/10.1109/AICT52120.2021.9628973.

24. Overview of the versatile video coding (VVC) standard and its applications / B. Bross, Y.-K. Wang, Y. Ye, S. Liu, J. Chen, G. J. Sullivan, J.-R. Ohm // IEEE Trans. Circuits Syst. Video Technol. — 2021. — Vol. 31, No. 10. — P. 3736–3764.

25. Pareek N. K., Patidar V., Sud K. K. Diffusion-substitution based gray image encryption scheme // Digit. Signal Process. — 2013. — Vol. 23, No. 3. — P. 894–901.

26. Park S.-W., Shin S.-U. Efficient selective encryption scheme for the H.264/scalable video Coding (SVC) // Proc. 4th Int. Conf. Netw. Comput. Adv. Inf. Manage. — 2008. — P. 371–376.

27. Peng F., Zhang X., Lin Z.-X., Long M. A Tunable Selective Encryption Scheme for H.265/HEVC Based on Chroma IPM and Coefficient Scrambling. *IEEE Transactions on Circuits and Systems for Video Technology*. 2020. Vol. 30, No. 8. P. 2765–2780. DOI: https://doi.org/10.1109/TCSVT.2019.2924910.

28. Perceptual quality assessment of HEVC and VVC standards for 8K video / C. Bonnineau, W. Hamidouche, J. Fournier, N. Sidaty, J.-F. Travers, O. Deforges // IEEE Trans. Broadcast. — 2022. — Vol. 68, No. 1. — P. 1–8.

29. Privacy protection in real time HEVC standard using chaotic system / M. A. Taha, W. Hamidouche, N. Sidaty, M. Viitanen, J. Vanne, S. El Assad, O. Deforges // Cryptography. — 2020. — Vol. 4, No. 2. — P. 18.

30. Qumsieh R., Farajallah M., Hamamreh R. Joint block and stream cipher based on a modified skew tent map // Multimedia Tools Appl. — 2019. — Vol. 78, No. 23. — P. 33527–33547.

31. Rassool R. VMAF reproducibility: Validating a perceptual practical video quality metric // Proc. IEEE Int. Symp. Broadband Multimedia Syst. Broadcast. (BMSB). — 2017. — P. 1–2.

32. Said A. Measuring the strength of partial encryption schemes // Proc. IEEE Int. Conf. Image Process. — 2005. — P. 1126.

33. Sallam A. I., El-Rabaie E.-S. M., Faragallah O. S. Efficient HEVC selective stream encryption using chaotic logistic map // Multimedia Systems. — 2018. — Vol. 24, No. 4. — P. 419–437.

34. Shahid Z., Chaumont M., Puech W. Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames // IEEE Trans. Circuits Syst. Video Technol. — 2011. — Vol. 21, No. 5. — P. 565–576.

35. Shahid Z., Puech W. Visual protection of HEVC video by selective encryption of CABAC binstrings // IEEE Trans. Multimedia. — 2014. — Vol. 16, No. 1. — P. 24–36.

36. Shamir A. How to share a secret // Commun. ACM. — 1979. — Vol. 22, No. 11. — P. 612–613.

37. Shannon C. E. Communication theory of secrecy systems // Bell Labs Tech. J. — 1949. — Vol. 28, No. 4. — P. 656–715.

38. Specification for the Advanced Encryption Standard (AES) / National Institute of Standards and Technology (NIST). — FIPS Working Group, Standard 197. — Federal Information Process, 2001. — 51 p.

39. Stütz T., Uhl A. On JPEG2000 error concealment attacks // Proc. Pacific-Rim Symp. Image Video Technol. — Cham, Switzerland: Springer, 2009. — P. 851–861.

40. Sze V., Budagavi M. High throughput CABAC entropy coding in HEVC // IEEE Trans. Circuits Syst. Video Technol. — 2012. — Vol. 22, No. 12. — P. 1778–1791.

41. Taneja N., Raman B., Gupta I. Chaos based partial encryption of SPIHT compressed images // Int. J. Wavelets, Multiresolution Inf. Process. — 2011. — Vol. 9, No. 2. — P. 317–331.

42. Taneja N., Raman B., Gupta I. Selective image encryption in fractional wavelet domain // AEU-Int. J. Electron. Commun. — 2011. — Vol. 65, No. 4. — P. 338–344.

43. Tunable selective encryption scheme for H.265/HEVC based on chroma IPM and coefficient scrambling / F. Peng, X. Zhang, Z.-X. Lin, M. Long // IEEE Trans. Circuits Syst. Video Technol. — 2020. — Vol. 30, No. 8. — P. 2765–2780.

44. Van Droogenbroeck M. Partial encryption of images for real-time applications // Proc. IEEE Signal Process. Symp. — 2004. — Vol. 1, No. 2. — P. 11–15.

45. Van Wallendael G., Boho A., Cock J. D., Munteanu A., Van De Walle R. Encryption for high efficiency video coding with video adaptation capabilities // IEEE Trans. Consum. Electron. — 2013. — Vol. 59, No. 3. — P. 634–642.

46. Versatile video coding standard: A review from coding tools to consumers deployment / W. Hamidouche, T. Biatek, M. Abdoli, E. Francois, F. Pescador, M. Radosavljevic, D. Menard, M. Raulet // IEEE Consum. Electron. Mag. — 2022. — DOI: https://doi.org/10.1109/MCE.2022.3144545.

47. Vijayalakshmi V., Varalakshmi L., Sudha G. F. Efficient encryption of intra and inter frames in MPEG video // Proc. Int. Conf. Netw. Secur. Appl. — Chennai, India: Springer, 2010. — P. 93–104.

48. Winkler S., Mohandas P. The evolution of video quality measurement: From PSNR to hybrid metrics // IEEE Trans. Broadcast. — 2008. — Vol. 54, No. 3. — P. 660–668.

49. Wu H. The stream cipher HC-128 // New Stream Cipher Designs (Lecture Notes in Computer Science). — Berlin, Germany: Springer, 2008.

50. Wu Y., Noonan J. P., Agaian S. NPCR and UACI randomness tests for image encryption // Cyber J., Multidisciplinary J. Sci. Technol., J. Select. Areas Telecommu. — 2011. — Vol. 1, No. 2. — P. 31–38.

51. Wu Y., Noonan P. J., Agaian S. NPCR and UACI randomness tests for image encryption // Cyber J., Multidisciplinary J. Sci. Technol. — 2011. — Vol. 1, No. 2. — P. 31–38.

52. Xu D. Data hiding in partially encrypted HEVC video // ETRI J. — 2020. — Vol. 42, No. 3. — P. 446–458.

53. Alimpiev A., Barannik V., Podlesny S., Suprun O. and Bekirov Ali. (2017) The video information resources integrity concept by using binomial slots, 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH). Lviv, Ukraine, pp. 193-196, doi: 10.1109/MEMSTECH.2017.7937564.

54. Barannik, V., Yudin, O., Boiko, Y., Ziubina, R., Vyshnevska, N. (2019). Video Data Compression Methods in the Decision Support Systems. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computing, vol 754. Springer, Cham. https://doi.org/10.1007/978-3-319-91008-6_30

55. Баранник В.В. Рельефное представление изображений пирамидальным кодированием . Інформаційно- керуючи системи на залізничному транспорті. 2001. № 1. С. 17 – 25.

56. Баранник В.В. Основы теории структурно-комбинаторного стеганографического кодирования: монография / Баранник В.В., Баранник Д.В., Бекиров А.Е. – Х.: Издательство «Лидер», 2017. – 256 с.

57. Barannik V.V., Hahanova A.V., Krivonos V.N. Coding tangible component of transforms to provide accessibility and integrity of video data. East-West Design & Test Symposium (EWDTS 2013), 2013, pp. 1-5, doi: 10.1109/EWDTS.2013.6673179.

58. Barannik V., Shiryaev A. Quadrature compression of images in polyadic space. Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science, 2012, pp. 422-422. INSPEC Accession Number: 12713484.

59. A. Krasnorutsky, R. Onyshchenko, D. Barannik and V. Barannik.The Methods of Intellectual Processing of Video Frames in Coding Systems in Progress Aeromonitor to Increase Efficiency and Semantic Integrity. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 53-56, doi: 10.1109/ATIT58178.2022.10024208.

60. V. Barannik, S. Shulgin, N. Barannik and V. Barannik. Method of Coding Subbands of Non-Homogeneous Spectrum of Video Segments in Uneven Diagonal Space. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 72-75, doi: 10.1109/ATIT58178.2022.10024236.

61. Barannik V. et al.: The method of masking overhead compaction in video compression systems , Radioelectronic and Computer Systems, 2(2021), 2021, 51 – 63 https://doi.org/10.32620/reks.2021.2.05 .

62. Barannik V., Krasnorutsky A., Kolesnyk V., Barannik V., Pchelnikov S., Zeleny P. Method of compression and ensuring the fidelity of video images in infocommunication networks. Radioelectronic and computer systems, 2022, vol. 4, pp. 129-142. DOI: https://doi.org/10.32620/reks.2022.4.10 .

63. Бараннік Д.В. Технологія приховування інформативного контенту в динамічному потоці відеосегментів // Наукоємні технології. – 2023. №4. – С. 408-415. DOI: https://doi.org/10.18372/2310-5461.60.18270 .

64. Barannik, V., Lytvinenko, M., Okladnoy, D., Suprun, O. Description of the OFDM symbol with the help of mathematical laws. Analysis of technologies that were used in this case (2017) 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017 - Proceedings, art. no. 8020095, pp. 183-187. doi: 10.1109/AIACT.2017.8020095.

65. Barannik, V., Barannik, D., Babenko, M., Prokopenko, R., Akimov, O., & Petrukha, N. (2026). Devising a method for complex steganographic embedding of information in the structural-psychovisual space. Eastern-European Journal of Enterprise Technologies, 1(9 (139), 19–30. https://doi.org/10.15587/1729-4061.2026.351181.

66. Barannik, V., Sidchenko, S., Barannik, D., Barannik, V., Datsun, A. (2021). Devising a conceptual method for generating cryptocompression codograms of images without loss of information quality . Eastern-European Journal of Enterprise Technologies, 4 (2 (112)), 6–16. doi: https://doi.org/10.15587/1729-4061.2021.237359 .

67. Barannik, V. et al. (2023). Processing Marker Arrays of Clustered Transformants for Image Segments. In: Klymash, M., Luntovskyy, A., Beshley, M., Melnyk, I., Schill, A. (eds) Emerging Networking in the Digital Transformation Age. TCSET 2022. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham. https://doi.org/10.1007/978-3-031-24963-1_25 .

68. Баранник В. В. Метод сжатия изображений на основе неравновесного позиционного кодированиябитовых плоскостей / В. В. Баранник, Н. К. Гулак, Н. А. Королева // Радіоелектронні і комп'ютерні системи . 2009. - № 1. - С. 84–92. - Режим доступу: http://nbuv.gov.ua/UJRN/recs_2009_1_13.

69. A. Krasnorutsky, V. Kolesnyk, A. Berchanov, V. Barannik, N. Kharchenko and O. Malko, "Method of Structural-Statistical Coding of Video Segments in Spectral-Cluster Space," 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 32-37, doi:10.1109/ATIT58178.2022.10024240.

70. V. Barannik, Y. Babenko, V. Barannik, V. Kolesnyk and D. Zhuikov, "Method Taking into Account Level of Structural and Statistical Saturation of Video Segments in the Coding Process," 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 66-71, doi:10.1109/ATIT58178.2022.10024193.