РОЗРОБКА МЕТОДУ БАГАТОРІВНЕВОЇ СЕЛЕКТИВНОЇ ОБРОБКИ ВІДЕОІНФОРМАЦІЇ В МЕЖАХ КОНЦЕПЦІЇ ІНТЕРНЕТУ РЕЧЕЙ

Гаврилов Д.С., Рябуха Ю.Н., Баранник В.В., Баранник Н.В.

Вступ

Прийняття провідними країнами світу концепції Інтернету Речей значною мірою загострило питання надання користувачу можливості керування будь-яким предметом з будь-якого місця у будь-який час. При цьому, керування має бути максимально простим та захищеним для користувача. Під захистом в даній роботі розуміється неможливість несанкціонованого користувача з'єднатися та/чи керувати предметом в системі Інтернету Речей. Варто відмітити, що процес авторизації та застосування предметів має бути простим та непомітним для авторизованого користувача.

Аналіз останніх публікацій вказав, що концепція Інтернету Речей є масштабованою, що дозволяє використовувати її як в інтересах приватної особи, так і в інтересах компанії, організації чи відомчої структури. В великих організаціях та відомчих структурах в межах даної концепції використовують безпілотні літальні апарати (БПЛА) різних типів для моніторингу, транспортування ті ін.. При цьому, під час покладених на БПЛА задач на борту формується та обробляється відеоінформаційний ресурс, який містить конфіденційні відомості, тож, потребує криптографічного захисту [1-5].

Таким чином, мета роботи полягає в розробці методу підвищення безпеки відеоінформації в межах концепції Інтернету Речей на основі використання багаторівневої селективної обробки.

Для досягнення поставленої мети, необхідно вирішити такі завдання:

1. Розробити метод виявлення ключової інформації на різних етапах обробки.

2. Розробити метод підвищення безпеки відеоінформації в межах концепції Інтернету Речей при заданій якості дешифрування з використанням багаторівневої селективної обробки.

Основна частина

Інформаційну технологію багаторівневої селективної обробки даних пропонується, розробляти на основі JPEG – платформи. При цьому, кодування та криптозахист проводити з застосуванням інформаційних технологій в наступній послідовності (рис. 1):

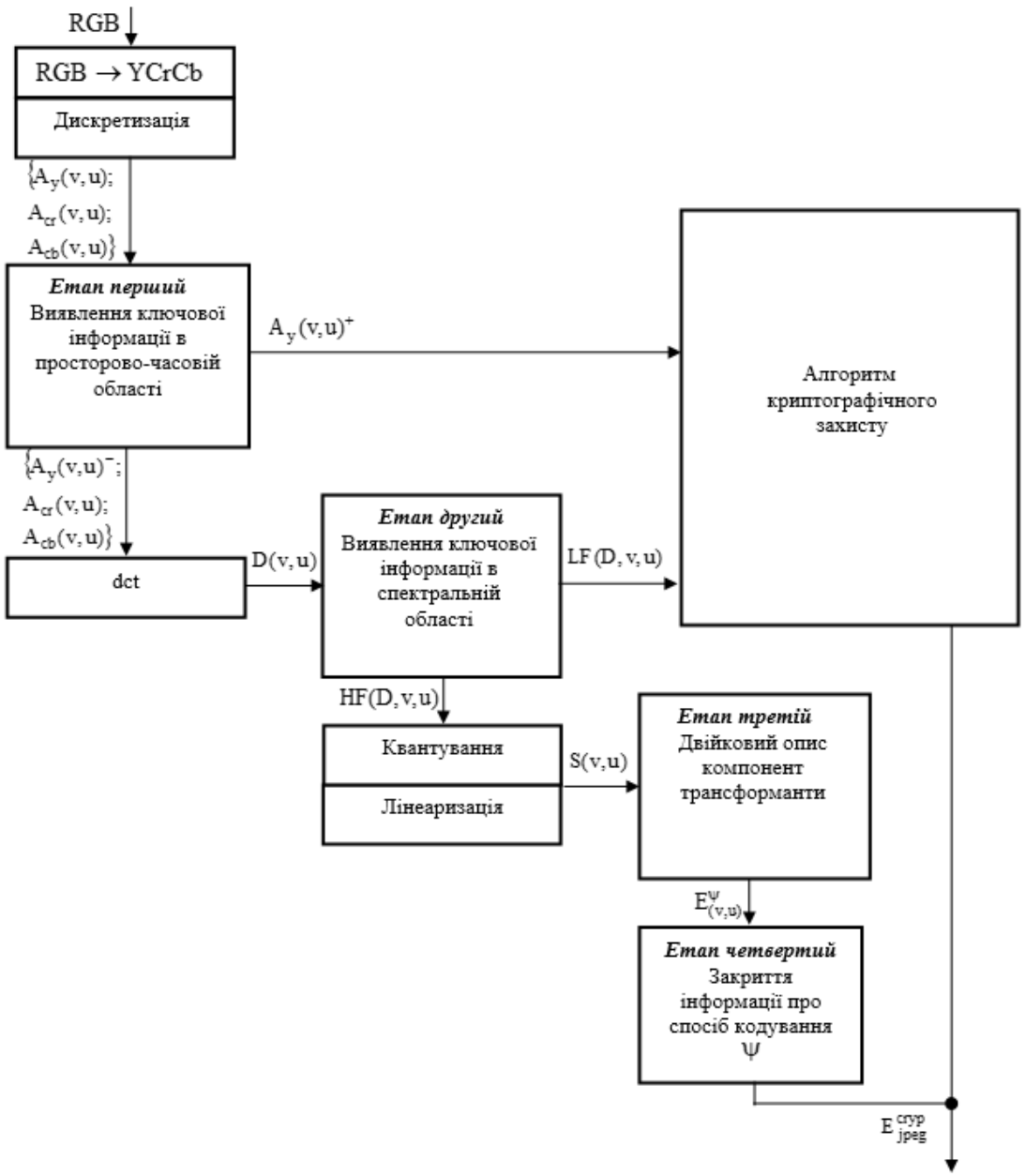


Рис. 1. Блок-схема інформаційної технології багаторівневої селективної обробки на основі JPEG – платформи

1. Інформаційна технологія виявлення та криптозахисту ключової інформації в просторово-часовій області:

– колірне перетворення та дискретизація кадру;

– виявлення та криптозахист ключової інформації в просторово-часовій області;

2. Інформаційна технологія виявлення та криптозахисту ключової інформації в спектральній області:

– дискретне косинусне перетворення та квантування вихідних відкритих даних;

– виявлення та криптозахист ключової інформації в спектральній області;

3. Інформаційна технологія криптографічного захисту інформації про спосіб кодування даних, що залишилися після попередніх етапів обробки даних:

– лінеаризація відкритих компонент квантованої трансформанти;

– двійковий опис компонент квантованої трансформанти;

– захист інформації про спосіб кодування.

Для вирішення задачі виявлення контурної інформації пропонується використовувати інформаційну технологію перевищення порогів (рис. 2). Емпіричним шляхом було виведена залежність між максимальним ($y_{v,u}^{(max)}$) та мінімальним ($y_{v,u}^{(min)}$) значенням елемента компоненти яскравості A_y з координатами блока (v, u), після чого перевіряється умова на перевищення порога (G) при цьому:

$$\begin{cases} y_{v,u}^{(max)} - y_{v,u}^{(min)} \geq G, \text{ то } A_y(v,u) \in A_{kon} \Rightarrow F_{kon}^{(y)} : A_{kon} \to \lambda; \\ y_{v,u}^{(max)} - y_{v,u}^{(min)} < G, \text{ то } A_y(v,u) \in A_{bk} \Rightarrow F_{bk}^{(y)} : A_{bk} \to E, \end{cases} \quad (1)$$

де A_{kon} - множина елементів кадру A, що містять контурну інформацію; A_{bk} - множина елементів кадру A в яких відсутня контурна інформація; $F_{kon}^{(y)}$ - функціонал, який перетворює множину A_{kon} елементів кадру, що складають контурну інформацію, в множину λ зашифрованих даних на етапі колірного перетворення за рахунок використання алгоритму криптографічного захисту «Калина».

Вибір даного симетричного блочного алгоритму обумовлено прийняттям його як національного стандарту України ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блочного перетворення», що дає право використовувати даний алгоритм у відомчих структурах:

$$F_{kon}^{(y)} : A_{kon} \to \lambda;$$

де $F_{bk}^{(y)}$ - функціонал, який перетворює множину A_{bk} елементів кадру, де відсутня контурна інформація в множину закодованих елементів E на етапі колірного перетворення за рахунок використання алгоритмів компресії:

$$F_{bk}^{(y)} : A_{bk} \to E.$$

Дана залежність було виведена з міркувань, що блок, який не містить контурну інформацію, складається з близьких між собою значень елементів в колірний площині. З урахуванням прийнятих допущень емпіричним шляхом було отримано значення порогу, перевищення якого однозначно визначає наявність контурної інформації в блоці.

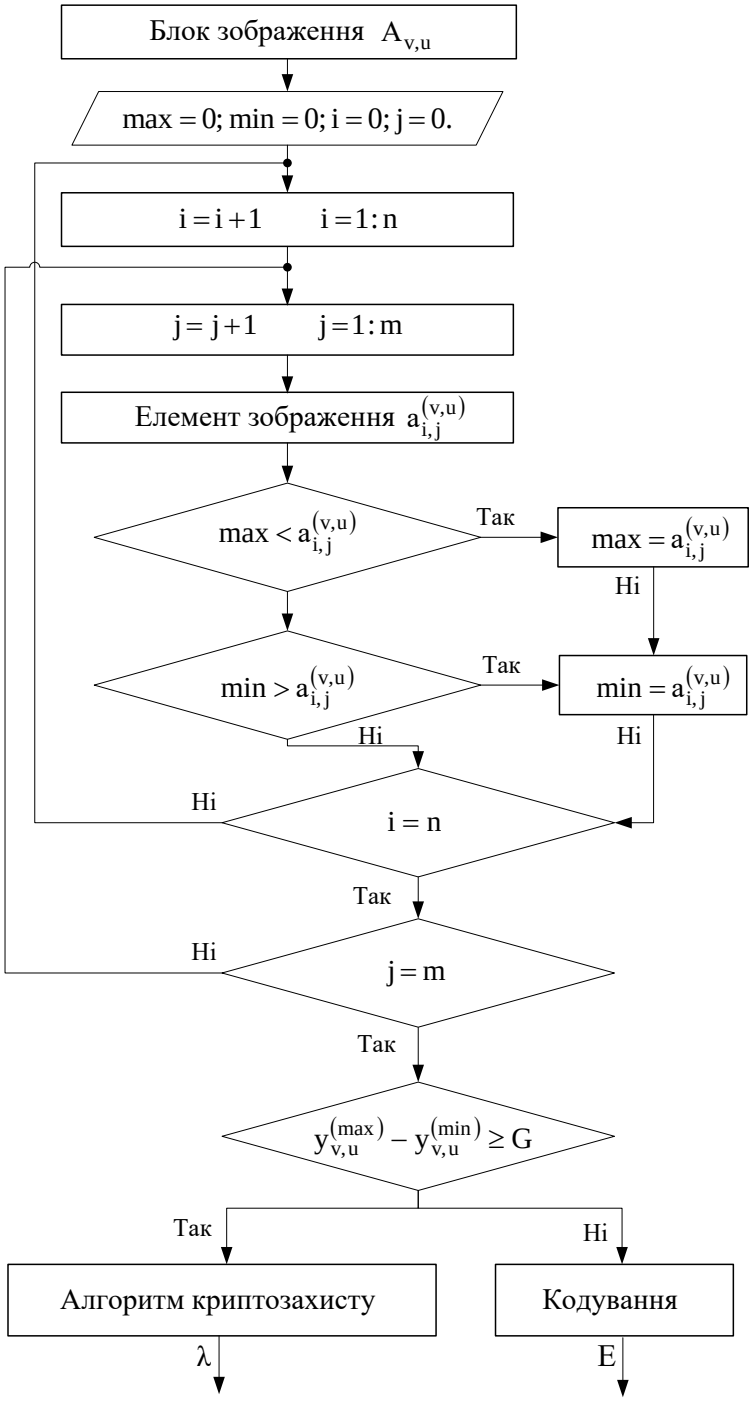


Рис. 2. Загальний вигляд алгоритму захисту контурної інформації інформаційною технологією перевищення порогів

Перший етап багаторівневої селективної обробки, який полягає у виявленні та криптозахисті блоків $A_y(v,u)^+$, які по формулі 1 визначені як «блоки, які містять контурну інформацію». При цьому, аналізується тільки компонента яскравості A_y кадру. Структурно-функціональна схема даного етапу приведена на рис 3.

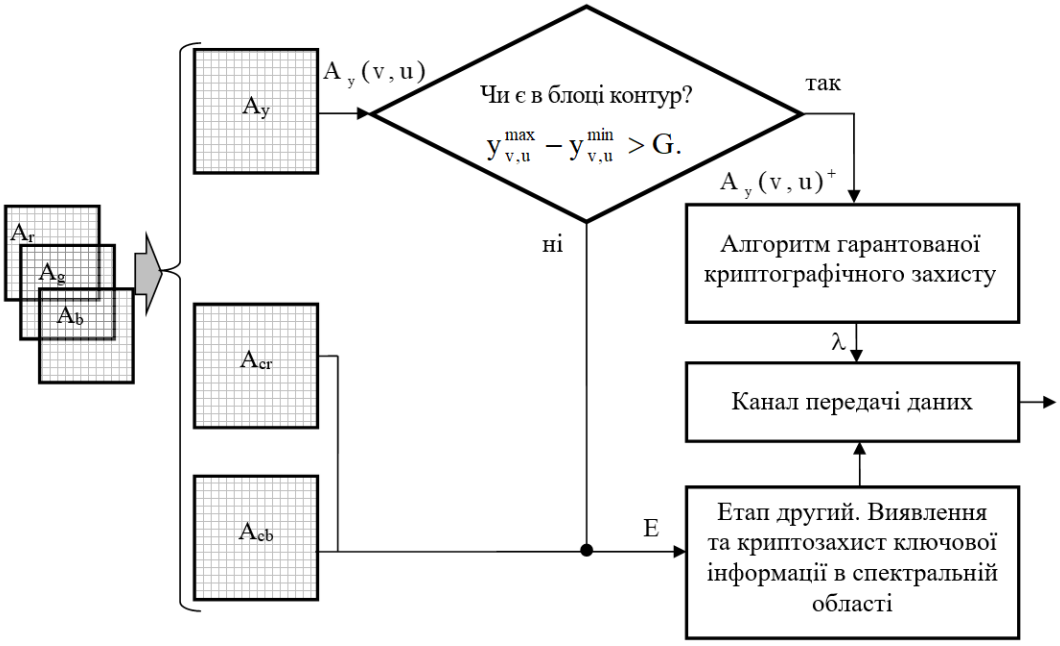


Рис. 3. Структурно-функціональна схема етапу виявлення ключової інформації в просторово-часовій області

В результаті того, що виявлення контурної інформації в просторовій області має ефект пропуску ключової інформації пропонується проводити додаткову фільтрацію в спектральній області, а саме на етапі дискретного косинусного перетворення (dct). Запропоновано підхід визначення рівня насиченості блоком контурною інформацією в залежності від кількості елементів в блоці, значення яких дорівнює «1». При цьому, оцінка насиченості блоком контурною інформацією PCI визначається формулою:

$$PCI = \frac{n_1}{n_0} \cdot 100\%, \qquad (2)$$

де PCI - показник, який визначає рівень насиченості блоку контурною інформацією; n_1 - кількість елементів, представленої в двійковому вигляді компоненти трансформанти, значення яких рівно «1»; n_0 - кількість елементів, представленої в двійковому вигляді компоненти трансформанти, значення яких рівно «0».

Дотримуючись даних міркувань, різні типи блоків 8x8 після dct були проаналізовані по формулі 2. Результати дослідження з представниками кожного класу представлені в табл. 1.

Основуючись на набрану статистику, класифікація по критерію наявності контурної інформації PCI в залежності від кількості «1» в блоці прийняла наступний вид:

1) в разі відсутності в блоці контурної інформації PCI_{bk}:

$$PCI_{bk} < 10\%, \qquad (3)$$

2) в разі плавного колірного переходу PCI_{pp} в блоці:

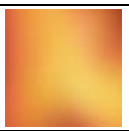
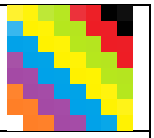
$$10\% \le PCI_{pp} < 40\%, \qquad (4)$$

3) в разі наявності контурної інформації PCI_{kon} в блоці:

$$40\% \le PCI_{kon} < 100\%, \quad (5)$$

Таблиця 1

Результат експериментального дослідження трансформант

					
розмір блоку	8 x 8	8 x 8	8 x 8	8 x 8	8 x 8
ймовірність появи «1» в трансформанті	0,0059	0,2928	0,2749	0,4668	0,4761
ймовірність появи «0» в трансформанті	0,9941	0,7072	0,7251	0,5332	0,5239
відношення "1" к "0" (К), %	0,5935	41,4027	37,912	87,5468	90,8761
клас блоку	без контурної інформації	з плавним переходом		з контурною інформацією	

Виходячи з приведеної класифікації, пропонується шифрувати відповідну кількість низькочастотних компонент DC, так як дані частоти несуть в собі ключову інформацію. Так, наприклад, однотонні блоки не містять в собі об’єкти інтересу та не потребують захисту, в той час як блоки з плавним колірним переходом та блоки з контурною інформацією можуть дати криптоаналітикам можливість отримати конфіденційні дані.

Правило обрання виду та об’єму обробки згідно з запропонованою класифікацією прийме вигляд:

Для блоку, який ідентифіковано за правилом (2) як «блок без контурної інформації» $PCI_{bk} < 10\%$, (рис. 4):

$$PCI = PCI_{bk} \Rightarrow \quad E = F_{bk}^{(ac)}(D(v,u)); \quad (6)$$

де $F_{bk}^{(ac)}$ - функціонал, який перетворює множину високочастотних AC елементів в множину закодованих елементів E.

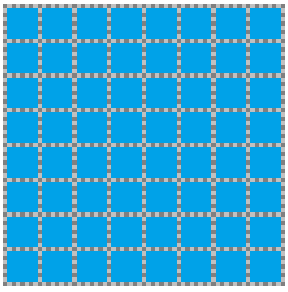


Рис. 4 Вихідний блок 8x8 без контурної інформації

Для блоку, який ідентифіковано за правилом (2) як «блок з плавним колірним переходом» $10\% \le PCI_{pp} < 40\%$ (рис. 5):

$$PCI = PCI_{pp} \Rightarrow \begin{cases} F_{kon}^{(dc)} : d_{x,i}^{(v,u)} \to \lambda, & \text{при } i = [1;4], \quad x = [1,4]; \\ F_{bk}^{(ac)} : d_{x,i}^{(v,u)} \to E, & \text{при } i = [1;8], \quad x = [5,15]; \end{cases} \quad (7)$$

де $F_{kon}^{(dc)}$ - функціонал, що перетворює множину низькочастотних DC елементів в множину зашифрованих елементів λ; $d_{x,i}^{(v,u)}$ – і-й елемент на х-й діагоналі трансформанти $D(v,u)$.

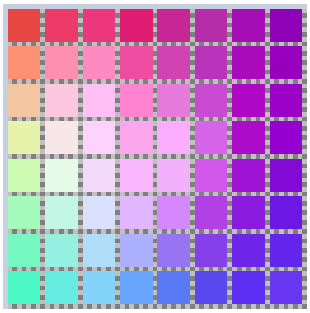


Рис. 5 Вихідний блок 8х8 з плавним колірним переходом

Для блоку, який ідентифікований за правилом (2) як «блок з контурною інформацією» $40\% \le PCI_{kon} < 100\%$ (рис. 6)

$$PCI = PCI_{kon} \Rightarrow \begin{cases} F_{kon}^{(dc)}: d_{x,i}^{(v,u)} \to \lambda, & \text{при } i=[1;7], \quad x=[1,7]; \\ F_{bk}^{(ac)}: d_{x,i}^{(v,u)} \to E, & \text{при } i=[1;8], \quad x=[8,15]. \end{cases} \frac{n!}{r!(n-r)!} \qquad (8)$$

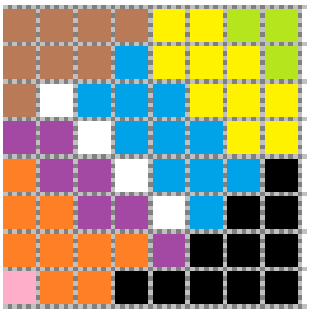


Рис. 6 Вихідний блок 8х8 з контурною інформацією

Таким чином, розроблено другий етап інформаційної технології багаторівневої селективної обробки даних, який полягає в криптозахисті низькочастотних DC компонент трансформанти D(v,u) в кількості, що залежить від класу блоку. Мета даної інформаційної технології полягає в захисті від пропуску ключової інформації на попередньому етапі. Структурно-функціональна схема даного етапу приведена на рис. 7.

Підхід, запропонований на рис. 7, дозволить усунути недолік попереднього етапу, який полягає у можливому пропуску ключової інформації. При цьому, трансформанта буде класифікована по одному з трьох видів представлених на рис. 8.

Рис. 7. Блок-схема інформаційної технології виявлення ключової інформації в спектральній області

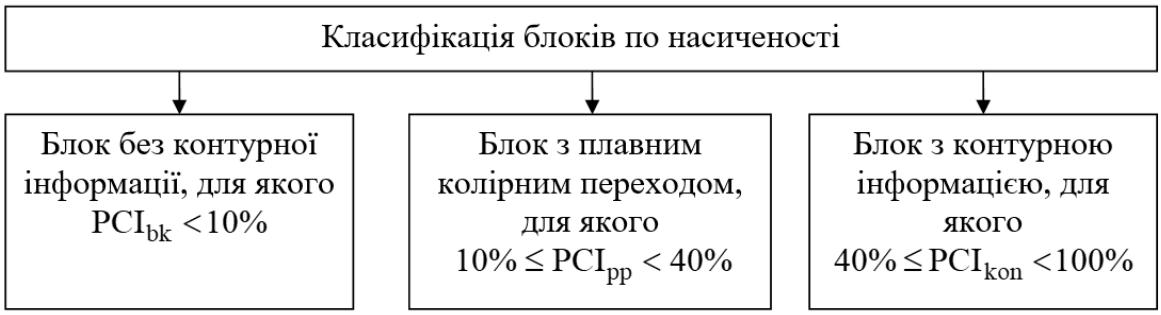


Рис. 8. Класифікація блоку по насиченості

В залежності від класу блоку пропонується шифрувати відповідну кількість низькочастотних DC компонент в трансформанті $D(v, u)$.

Інформаційна технологія загального криптографічного захисту інформації про спосіб кодування даних, що залишилися після попередніх етапів обробки полягає у використанні різних алгоритмів кодування (рис. 9) в залежності від ймовірності P_1 появи «1». Внаслідок чого ймовірність P_1 появи «1» стає конфіденційною інформацією і потребує захисту.

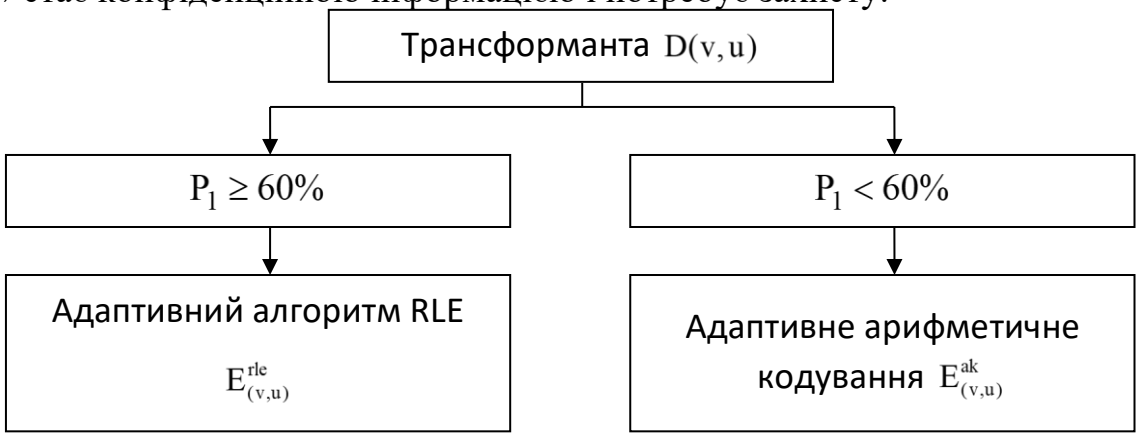


Рис. 9. Блок - схема вибору алгоритму кодування в залежності від ймовірності появи елементів

Таким чином, розроблено третій і четвертий етапи багаторівневої селективної обробки які полягають у виборі способу кодування даних, що надходять і криптозахисті інформації про обраний спосіб кодування. Структурно-функціональна схема даних етапів наведено на рис. 10.

Процес декодування полягає в зворотному алгоритмі, так як даний інформаційна технологія симетричний. Обробка здійснюється по біполярному принципом для авторизованого користувача і зловмисника (неавторизований користувач).

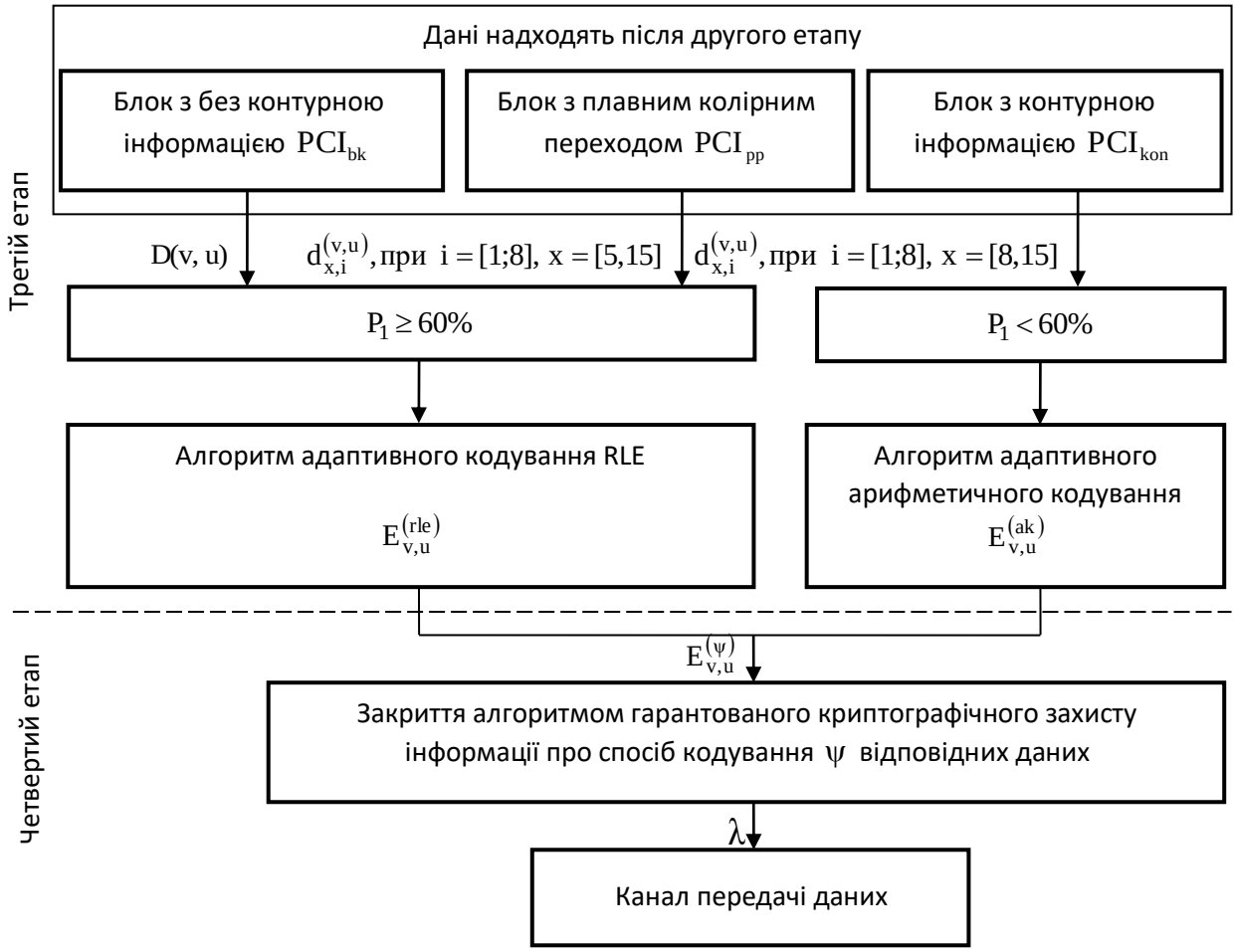


Рис. 10. Третій і четвертий етапи багаторівневої селективної обробки даних

Висновки

Розроблено інформаційну технологію багаторівневої селективної обробки відеоінформації в межах концепції Інтернету Речей.

Наукова новизна.

1) Вперше розроблено інформаційну технологію багаторівневої селективної обробки відеоінформації в межах концепції Інтернету Речей. На відміну від інших селективних інформаційних технологій забезпечується одночасне кодування і шифрування ключової компоненти на просторово-часовому та спектральному етапах обробки, що забезпечує оперативне, дозоване шифрування інформації.

2) Вперше розроблено класифікацію насиченості блоку в залежності від частоти появи одиниці. На відміну від інших інформаційних технологій визначення класу блоку розроблена класифікація не вимагає додаткових перетворень. Це дозволяє знизити час на обробку, що позитивно впливає на оперативність передачі даних.

Створено правило дозованої обробки (кодування і шифрування) трансформанти в залежності від класу даних, що надходять.

Література

1. Бараннік В.В. Кодування трансформованих зображень в інфокомунікаційних системах / В.В. Бараннік, В.П. Поляков – Х. : ХУПС, 2010. – 212 с.

2. Бараннік В.В. Метод кластеризації фрагментів аерофотознімків у спектрально–частотному просторі // Бараннік В.В., Мусієнко О.П., Ялівець К.С. // Наукоємні технології. – 2016. – Т. 9, № 1. – С. 23 – 30.

3. Бараннік В.В.. Аналіз методів виявлення меж об'єктів на зображеннях і їх класифікація / В.В. Бараннік, А.В. Власов, А.В. Яковенко // Сучасна спеціальна техніка. – 2012. – вип. 3 (30). – С. 17 – 27.

4. Гонсалес Р.С., Вудс Р.Э. Цифровая обработка изображений/ Р.С. Гонсалес, Р.Э. Вудс. М.: Тех-носфера, 2006. – 1072 с.

5. Гаврилов Д.С. Метод забезпечення безпеки відеоінформаційного ресурсу на основі багато-рівневої селективної обробки в телекомунікаційних / Д.С. Гаврилов, О.Г. Оксіюк, П.М. Гуржій, Б.О. Демідов // Наука і техніка. № 26. – 2017. – С. 46-48.