«Дослідження і проектування систем прихованої передачі інформації в форматі JPG»

Виконав: Студент СП-509
Царинний Є. О.

Керівник: д.т.н., проф. Рудницький В.М.

МЕТА ПРОЕКТУ

Підвищення стійкості систем прихованої передачі інформації, в тому числі в форматі JPG.

Для досягнення даної мети необхідно:

- провести аналіз існуючих методів та засобів стеганографічного захисту інформації в МЗ;
- провести аналіз та адаптацію узагальненої математичної моделі та методів вбудовування даних у зображення;
- провести аналіз існуючих стеганографічних методів проектування систем прихованої передачі інформації,
- провести аналіз стандартів кодування зображень JPEG;
- провести аналіз стійкості систем прихованої передачі інформації на тлі зовнішніх впливів в форматі JPG;
- розробити програмні засобу для стеганографічного захисту інформації в МЗ та перевірити їх ефективності.

ОСНОВНІ ЗАВДАННЯ

- Провести огляд існуючих систем прихованої передачі інформації;
- Адаптувати математичну модель стеганосистеми як системи передачі прихованої інформації;
- Встановити критерії оцінки стеганосистем;
- Вибрати зображення для вбудовування;
- Провести огляд існуючих стеганографічних методів проектування систем прихованої передачі інформації;
- Зробити аналіз стандартів кодування зображень JPEG;
- Провести аналіз стійкості систем прихованої передачі інформації на тлі зовнішніх впливів в форматі JPG.

Об’єкт та предмет дослідження

- ***Об’єкт дослідження*** – процес обробки, захисту та прихованої передачі інформації в в форматі JPG.

- ***Предмет дослідження*** – математичні моделі, методи та засоби забезпечення стеганографічної стійкості системи прихованої передачі інформації

Методи дослідження

- Розробка математичної моделі процесу стеганографічних перетворень інформації з урахуванням дії завад в каналах зв’язку здійснювалася на основі методів теоретико-множинного підходу.
- Підготовка інформаційного сигналу та сигналу-контейнера для вбудовування прихованих даних проводилася з використанням методів цифрової обробки сигналів та зображень.
- Для підвищення завадостійкості інформації використовувались методи теорії кодування.
- Для вибору оптимального за зазначеними критеріями методу застосовувалися методи багатокритеріальної оптимізації.

У першому розділі дипломної роботи були отримані наступні результати:

- 1. Визначені основні сфери використання та характеристики стеганографії. Обґрунтована актуальність її використання для вирішення сучасних задач, пов’язаних з прихованою передачею інформації та захистом авторських прав.
- 2. Адаптована математична модель стеганосистеми як системи передачі інформації, що описує передачу повідомлення від відправника до отримувача, до вимог дипломної роботи, шляхом врахування навмисних атак та випадкових завад.
- 3. Наведено класифікацію показників, що дають кількісні та якісні оцінки для порівняльного оцінювання якості стеганографічних засобів. До кількісних оцінок, що оперують із зображеннями на рівні пікселів, відносяться співвідношення «сигнал/шум», нормована середня абсолютна різниця, якість зображення, середньоквадратична похибка та середня абсолютна різниця. До найважливіших якісних характеристик стеганографічних систем, утворених з використанням різних методів, відносяться: пропускна здатність, стійкість, невидимість, захищеність, складність вбудовування та вилучення.

Сфери застосування стеганографії

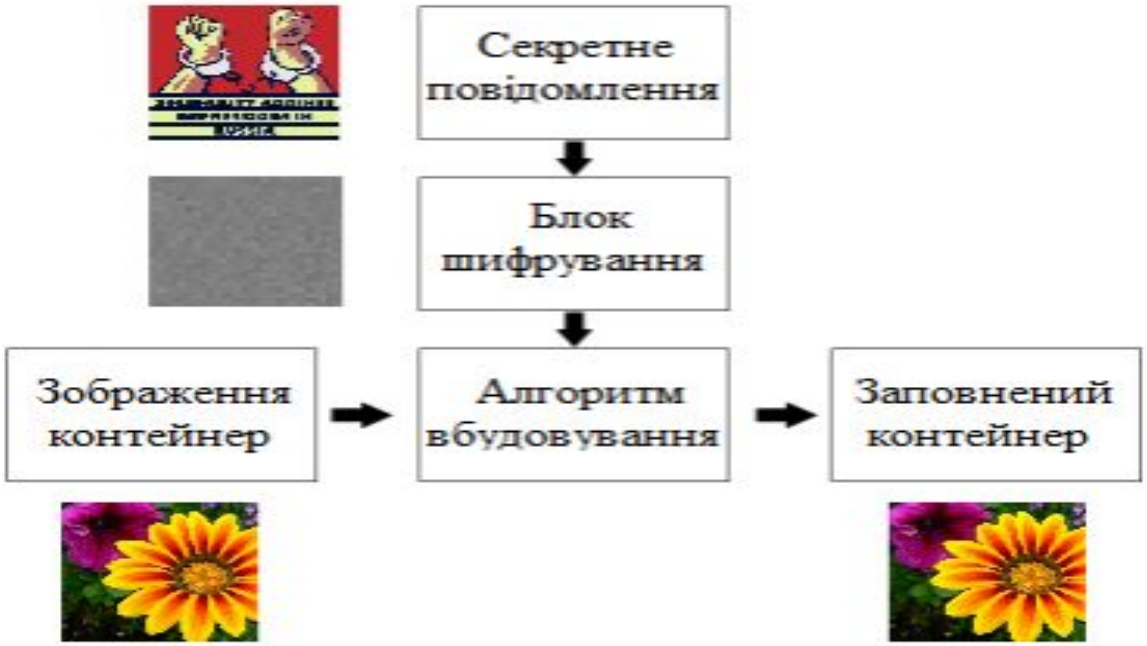


Рис. 1. Блок-схема процесу вбудовування повідомлення при прихованому зв’язку

Сфери застосування стеганографії

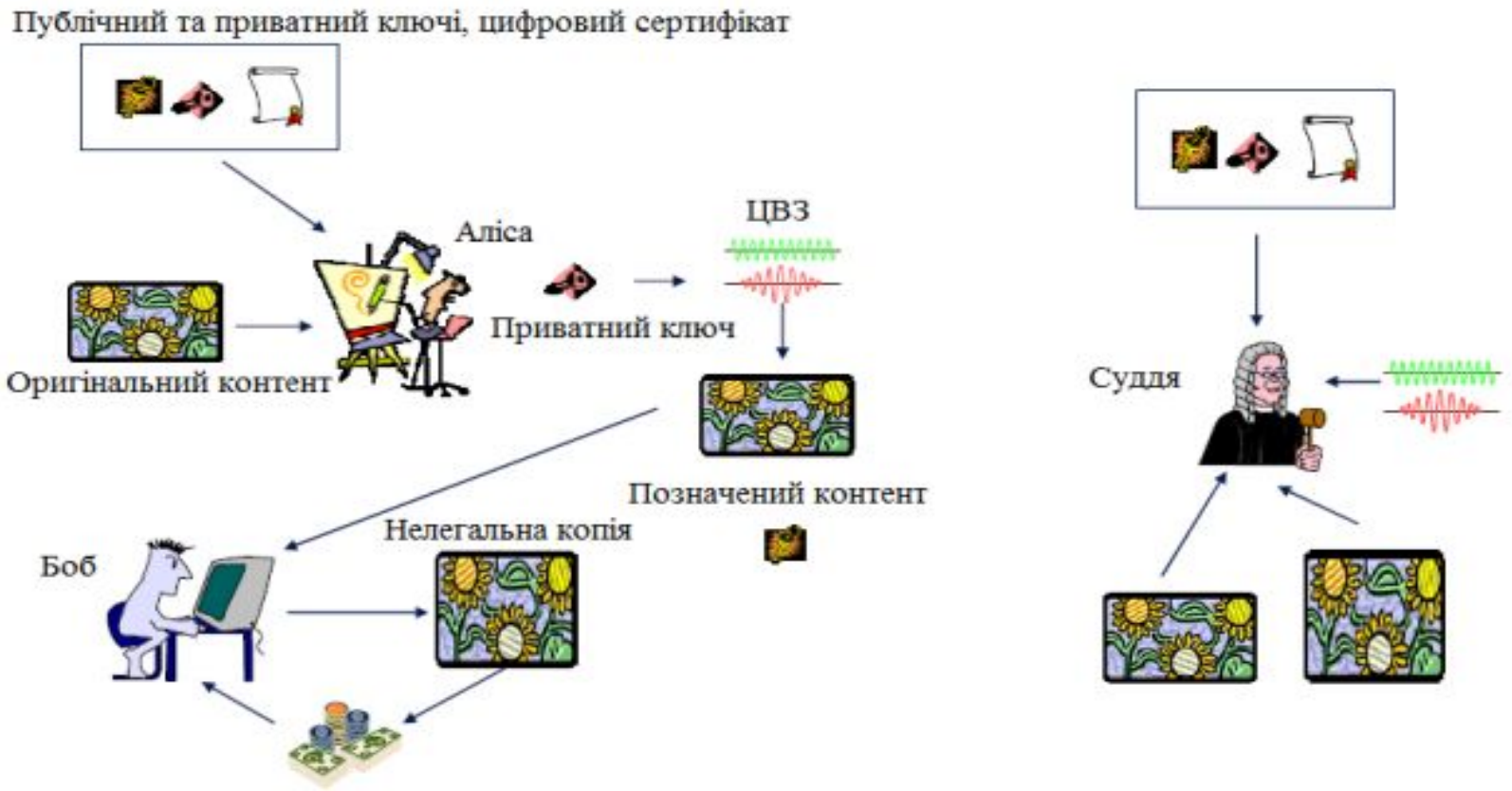


Рис. 2. Блок-схема процесу вбудовування ЦВЗ з метою захисту авторських прав

Сфери застосування стеганографії

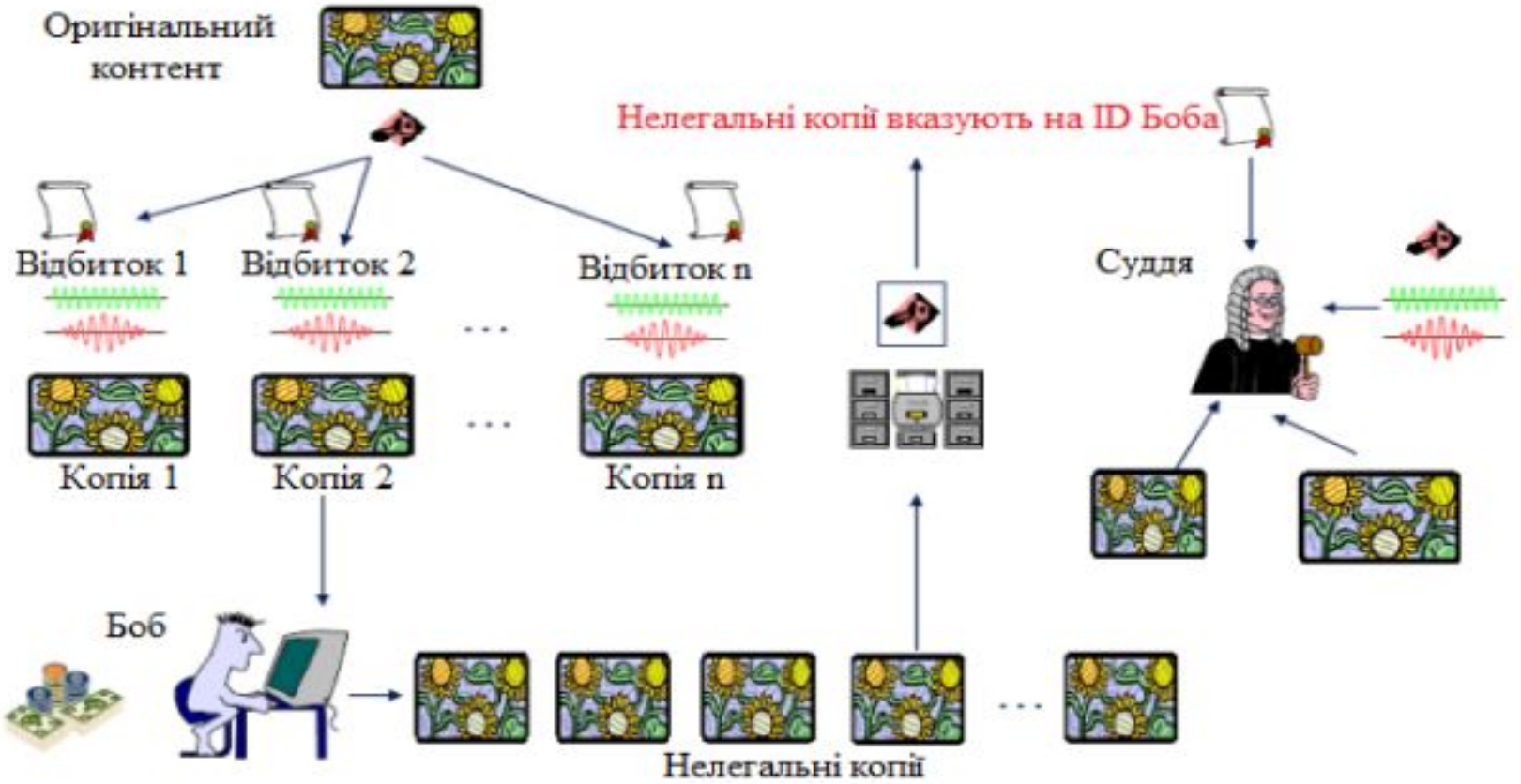


Рис. 3. Блок-схема процесу вбудовування ідентифікаційних номерів з метою відстеження порушника

Сфери застосування стеганографії

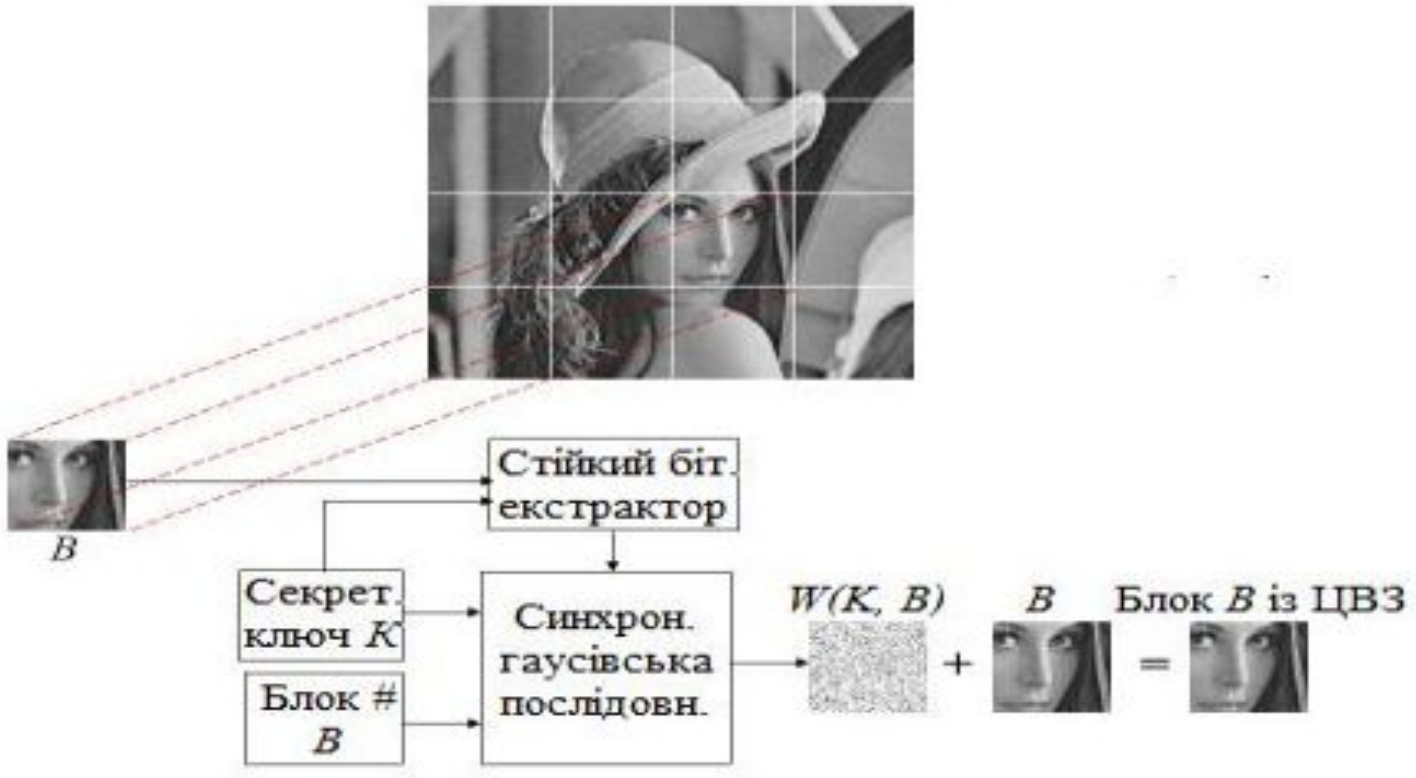


Рис. 4. Блок-схема процесу вбудовування ЦВЗ для захисту цілісності зображення

Сфери застосування стеганографії

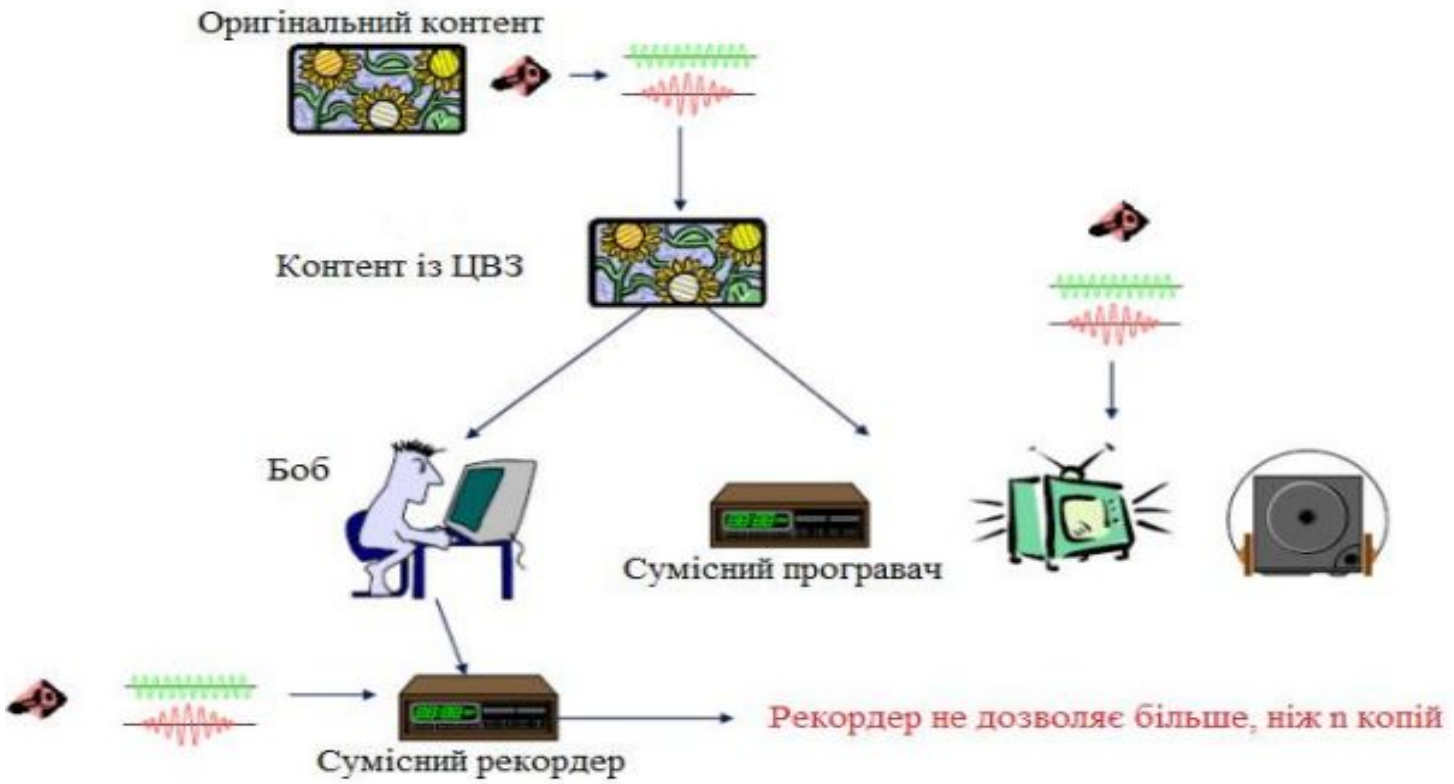


Рис. 5. Блок-схема процесу вбудовування ЦВЗ для управління копіюванням при записі DVD

Узагальнена структурна схема стеганосистеми як системи передачі інформації

«Магічний трикутник» ключових характеристик стеганосистем

Додаткові характеристики:
- **Захищеність**
- **Складність вбудовування/вилучення**

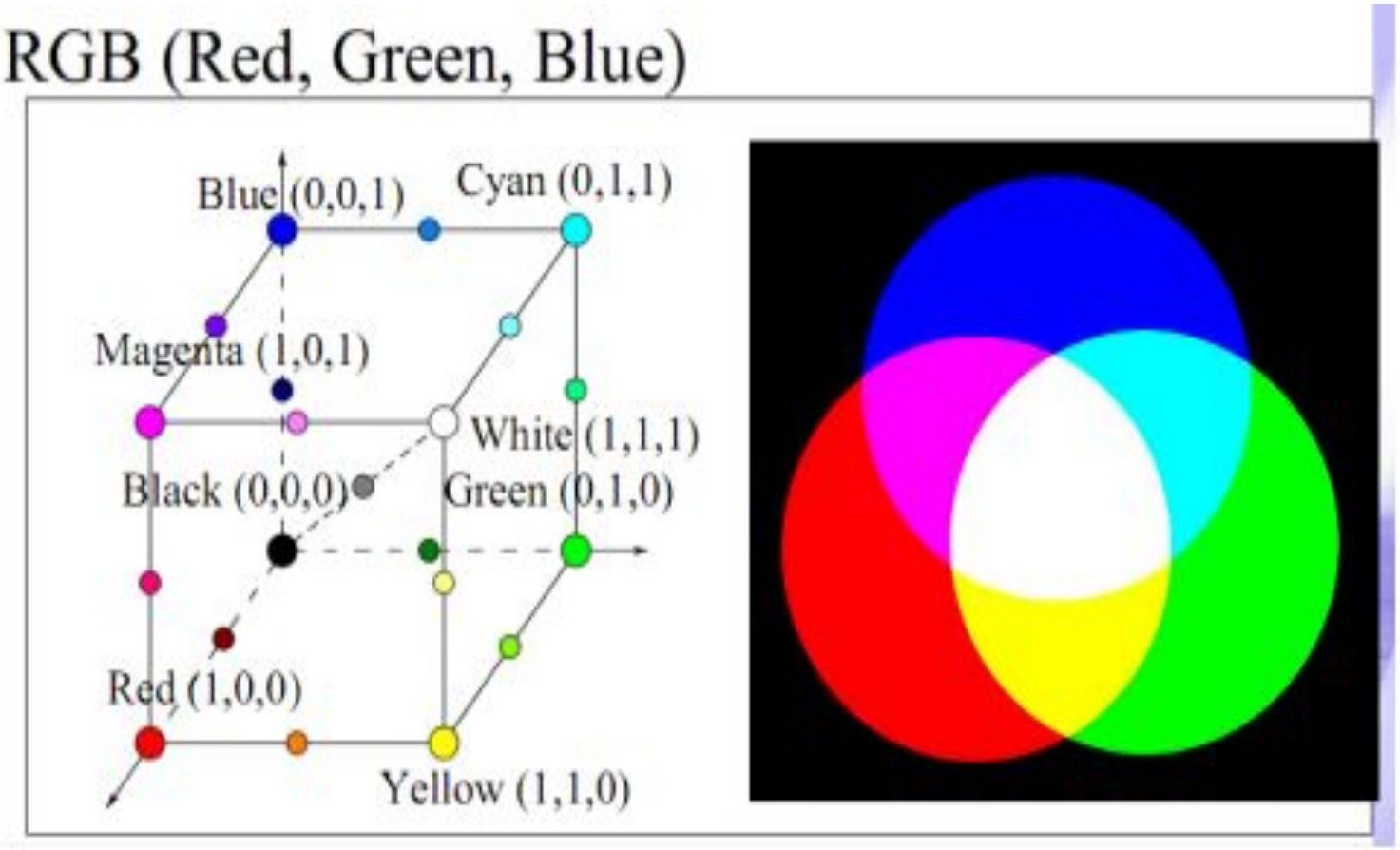
У другому розділі дипломної роботи були отримані наступні результати:

- 1. Визначені основні методи прихованої передачі інформації, в тому числі в форматі JPG. Обґрунтована актуальність їх використання для вирішення сучасних задач, пов’язаних з прихованою передачею інформації та захистом авторських прав.
- 2. Виконано обґрунтування вибору типу зображень для досліджень. Були обрані кольорові bmp зображення з глибиною кольору 24 біти та розміром *1024x1024* пікселів. Акцент робиться на групі кольорових зображень без різких переходів між текстурними областями, що мають достатню кількість мілких деталей.
- 3. Для досліджень були обрані та коротко охарактеризовані наступні методи: найпоширеніший метод заміни найменш значущого біту, метод Куттера-Джордана-Боссена, як один з кращих в просторової області, модифікований метод Коха-Жао, як один з основних в частотній області, метод Бенгама, що є вдосконаленням попереднього, метод, заснований на ДВП та методи із розширенням спектра сигналу тощо.

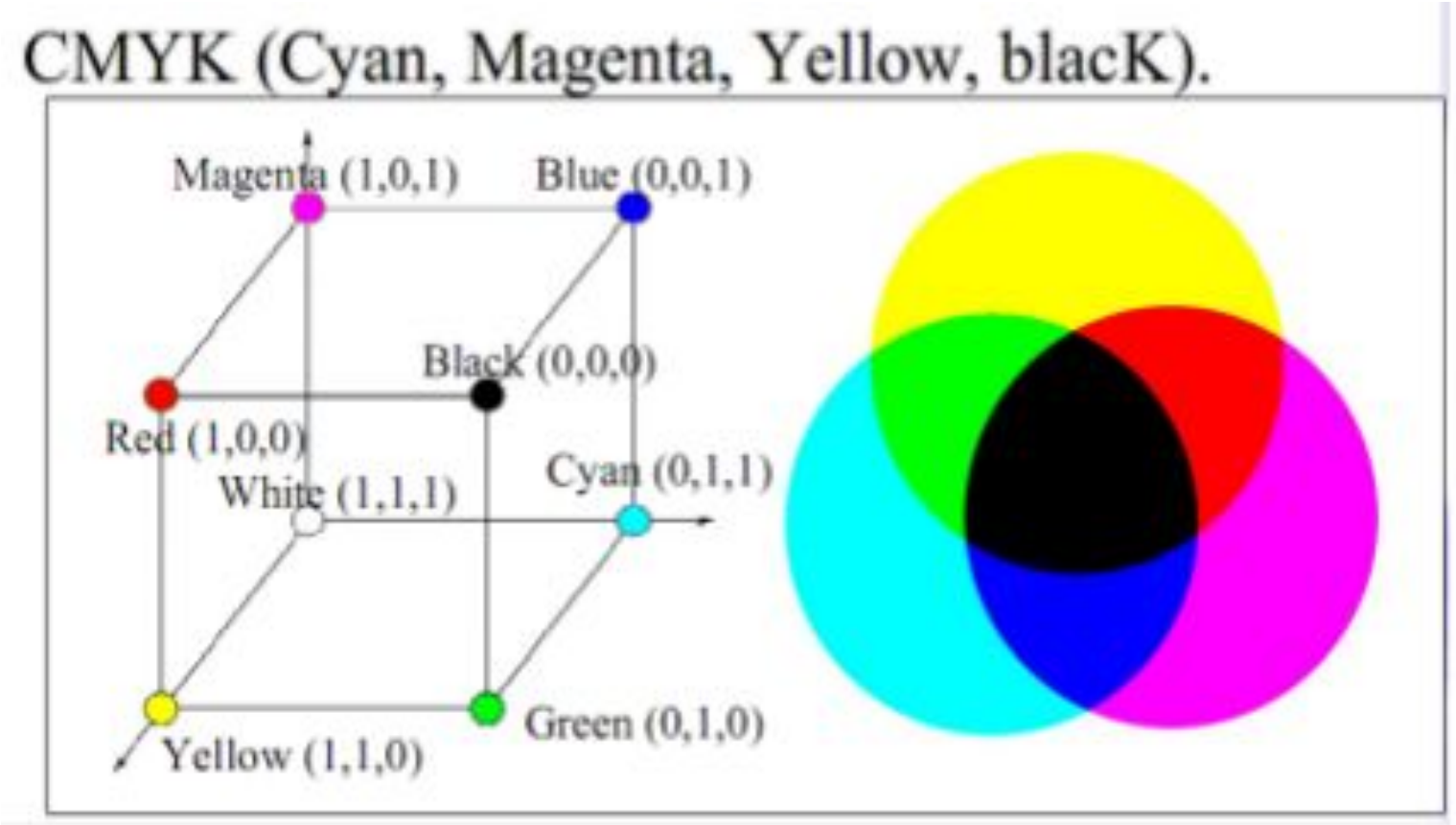
Приклад растрового (а) та векторного (б) зображень

а *б*

Колірна модель RGB



Колірна модель CMYK

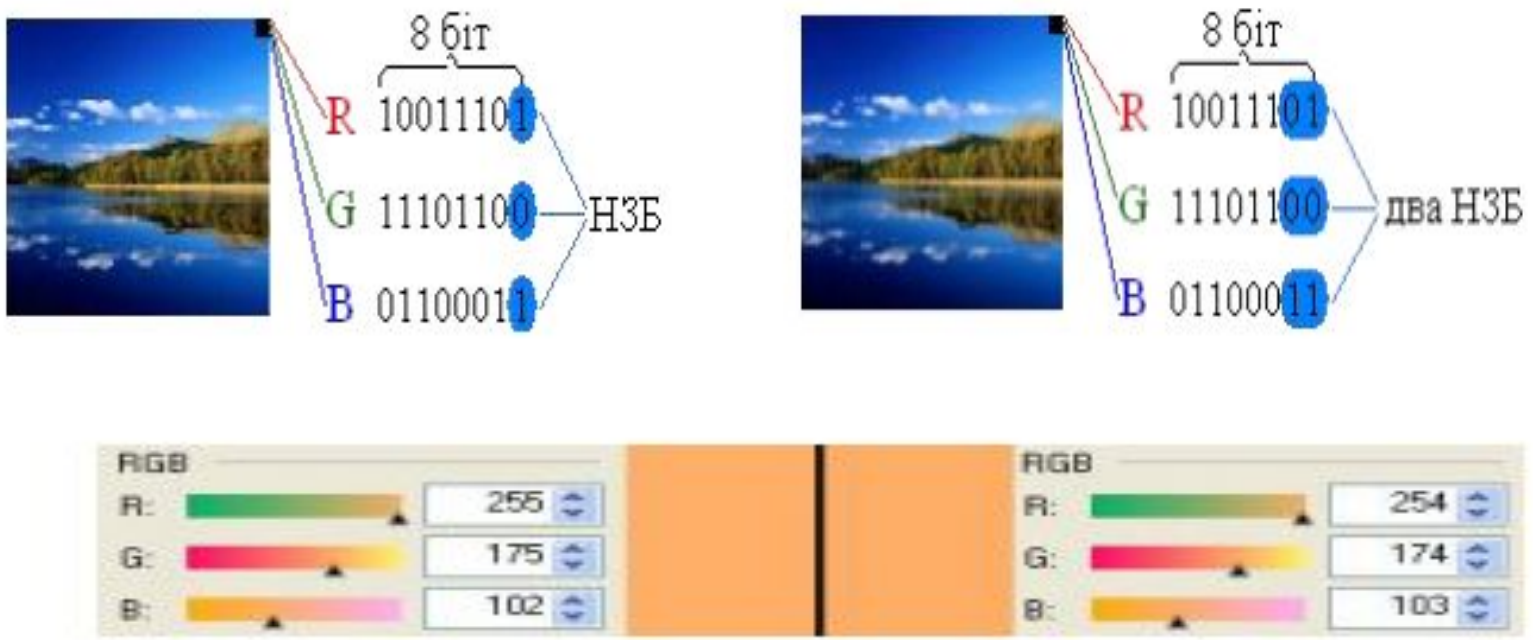


Приклади зображень для досліджень

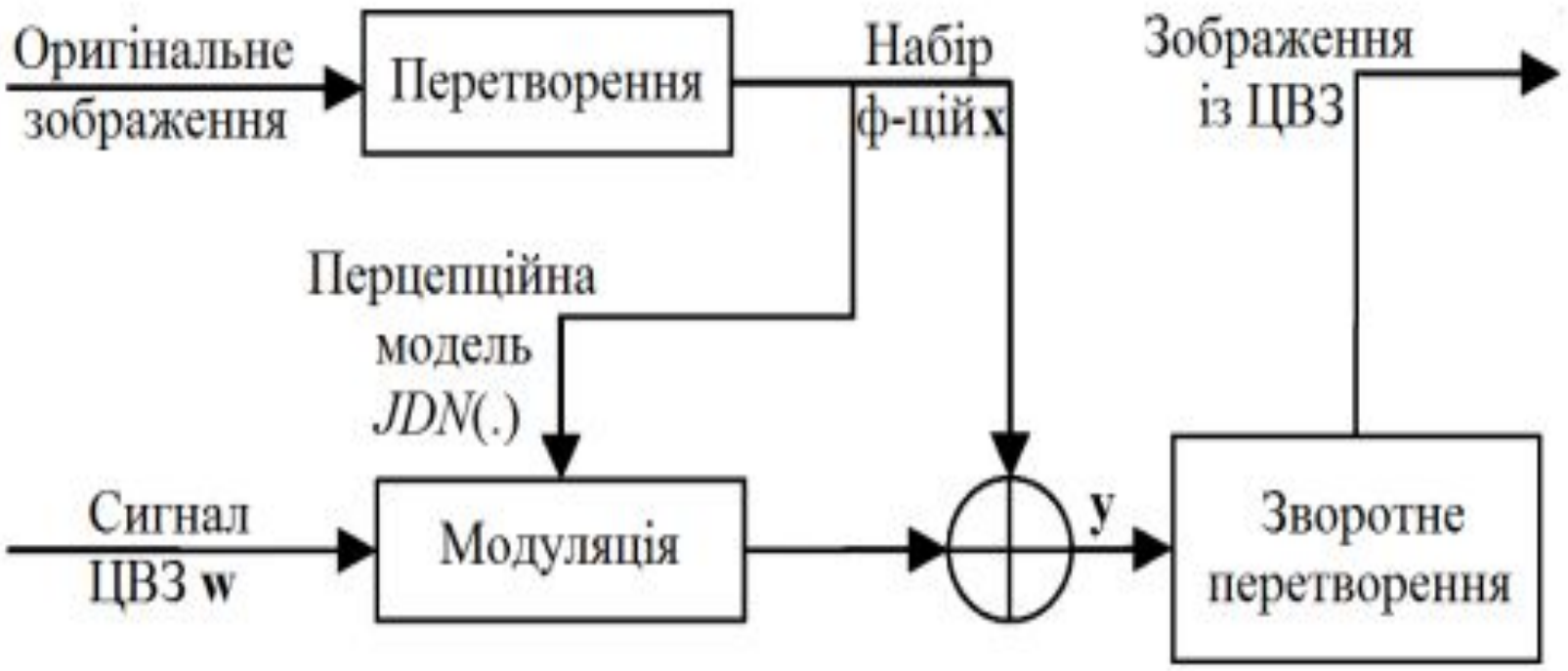





Приховування інформації методом НЗБ та зміна кольору при заміні НЗБ



Принцип методів з розширенням спектру



Основні стандарти кодування зображень JPEG, розглянуті в третьому розділі

- JPEG XT,
- JPEG-LS,
- JPEG 2000,
- JPEG XR,
- JBIG,
- JPEG AIK,
- JPSearch,
- JPEG XS,
- JPEG Pleno

У четвертому розділі дипломної роботи були отримані наступні результати:

- 1. Визначені, класифіковані та досліджені атаки на системи прихованої передачі інформації. Отримані кількісні оцінки стійкості до атак проти вбудованого повідомлення та стеганогдетектора, реалізовані на основі афінних перетворень, стисненні та переформатуванні маркованих зображень. За результатами визначено, що при наявності активного порушника, найефективнішим способом приховування даних є методи на основі вейвлет-перетворення.
- 2. Реалізований програмний комплекс, що імітує канали зв’язку. Що дозволяє дослідити можливість стеганографічних методів адаптуватись до реальних каналів передачі. Були отримані порогові значення спотворень стеганосистем, для яких ще можливе відновлення прихованої інформації. Для різних методів максимально допустиме значення помилки у каналах із стиранням та мультиплікативною завадою становило 0,03-1 %. В той чай, як для каналів із адитивним білим гаусовим шумом помилка не має перевищувати для всіх досліджуваних методів.

У четвертому розділі дипломної роботи були отримані наступні результати:

- 3. Були розраховані мінімальні значення SNR для кожного з методів, при якому можливе правильне вилучення прихованої інформації, і максимальні показники NAD відповідно. Загалом найпростіші методи, що оперують із просторовою областю зображення, виявилися найбільш стійкими до обраних завад у комунікаційних каналах. Вони потребують всього 122-126 дБ для значення SNR. Метод дискретного вейвлет-перетворення показав значення на рівні найкращих – 286 дБ. В той час, як частотні методи потребують значно вищого рівня SNR (264- 12431 дБ) для детектування прихованого повідомлення, та мають нижчі граничні показники допустимих спотворень.
- 4. Вдосконалено метод попередньої підготовки інформації до прихованої передачі телекомунікаційними системами, де застосування завадостійкого кодування дозволяє збільшити ймовірність безпомилкового прийому повідомлення до 66% при негативному впливі адитивного білого гаусового шуму в каналі зв’язку
- 5. Вдосконалено метод адаптації телекомунікаційних систем передачі прихованої інформації до зовнішніх впливів, де застосування м'якого детектування дозволяє у 1,7 рази зменшити співвідношення сигнал/шум, при якому спрацює детектор, та підвищити ймовірність вилучення прихованої інформації.

Реалізація атак на вбудоване повідомлення і стеганодетектор (а – оригінальне зображення, б – зміна контрастності, в – зміна яскравості, г – масштабування, д – поворот, е – відсічення)

а

б

в

г

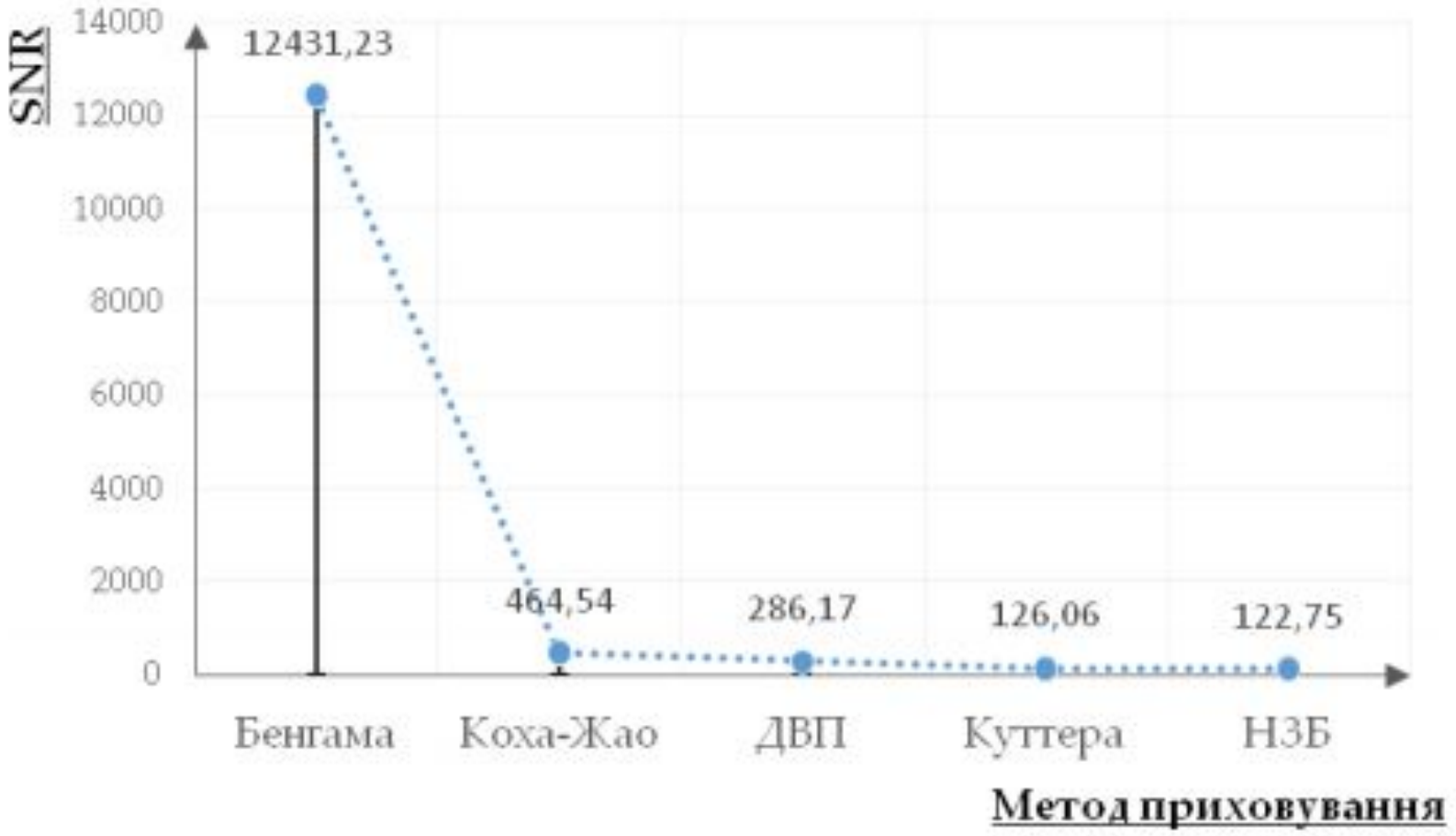
д

е

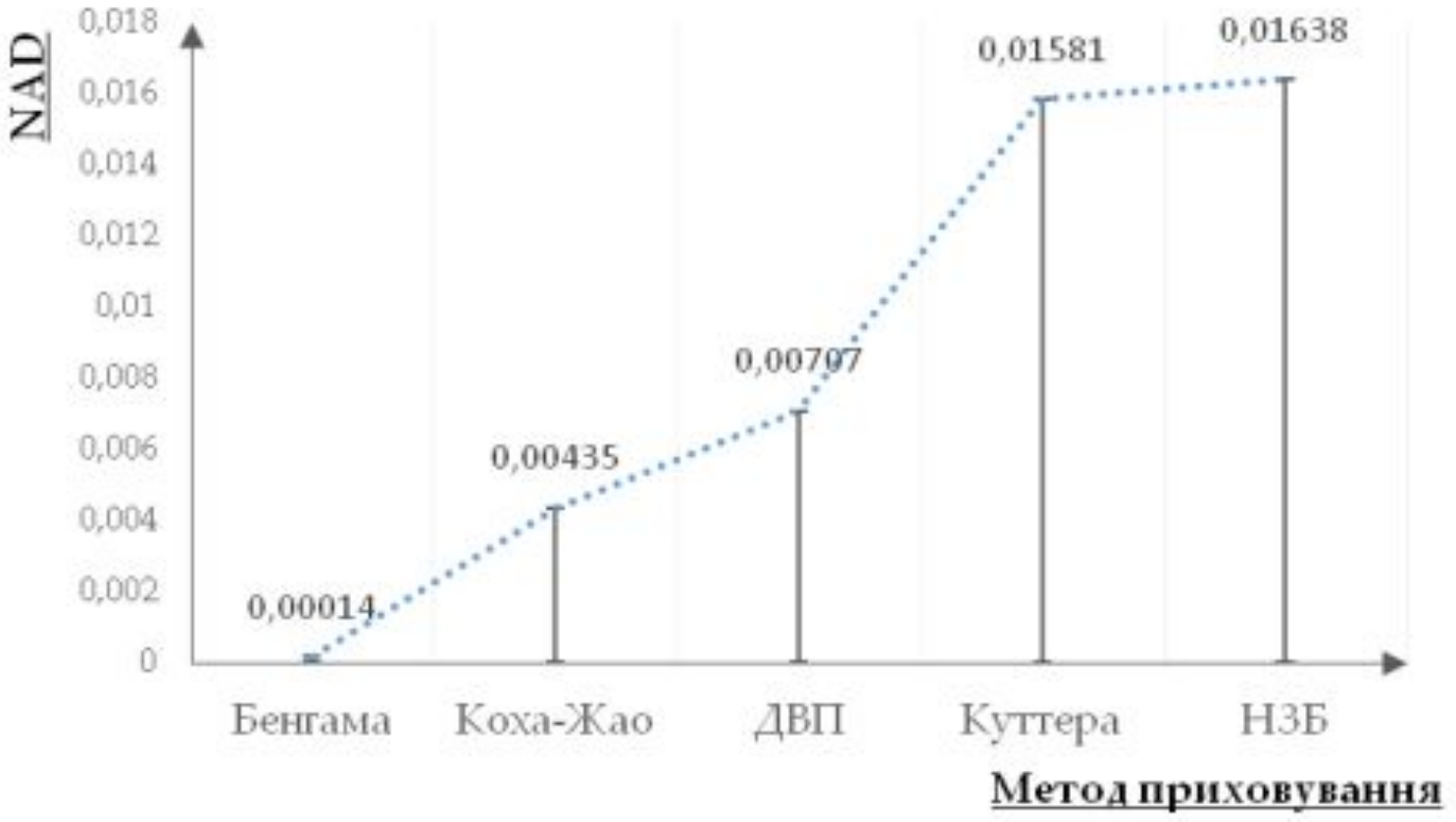
Аналіз стійкості до атак проти вбудованого повідомлення

Переформатув. / стиснення	в просторовій обл.		в частотній обл.				в обл. перетв.
	НЗБ	КДБ	КЖ		БМЕЮ		ДВП
Розмір зображення:	640× 640	640× 640	2048× 2048	640× 640	2048× 2048	640× 640	640× 640
bmp-png	+	+	+	+	+	+	+-
bmp-tiff	+	+	+	+	+	+	+
bmp-jpeg(rgb)/0%	-	-	+	+	+	+	+
bmpjpeg(rgb)/25%	-	-	+	+	+	+	+
bmpjpeg(rgb)/50%	-	-	+	+	+	+	+
bmpjpeg (Ycbcr)/0%	-	-	+	-	+	-	+
bmp-jpeg (Ycbcr)/25%	-	-	+	-	-	-	+
bmp-jpeg (CMYK)/0%	-	+	+	+	+	+	+
bmp-jpeg (CMYK)/25%	-	-	+	+	+	+	+

SNR для порогових значень спотворень для кожного з методів



NAD для порогових значень спотворень для кожного з методів



ДЯКУЮ ЗА УВАГУ