КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1280
УДК 004.056.53:004.92

Ярема Олег Михайлович
аспірант кафедри кібербезпеки
Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна
ORCID: 0009-0009-8709-7813
yarema.oleh.m@gmail.com

Загородна Наталія Володимирівна
кандидат технічних наук, зав.каф.кафедри кібербезпеки
Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна
ORCID: 0000-0002-1808-835X
zagorodna_n@tntu.edu.ua

Деркач Марина Володимирівна
кандидат технічних наук, доцент кафедри кібербезпеки
Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна
ORCID: 0000-0001-8977-2776
m_derkach@tntu.edu.ua

Ревнюк Олександр Андрійович
PhD, асистент кафедри кібербезпеки
Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна
ORCID: 0009-0005-0511-5354
revo0708@gmail.com

Загородна Мирослава Василівна
м.н.с.
Інститут ветеринарної медицини НААН, Тернопіль, Україна
ORCID: 0009-0002-3258-4904
myroslavazagorodna@gmail.com

МОДИФІКАЦІЯ МЕТОДУ ЗАМІНИ НАЙМОЛОДШОГО БІТА У SVG ЗОБРАЖЕННЯХ

Анотація. У статті запропоновано та досліджено модифікацію методу заміни найменшого значущого біта (Least Significant Bit, LSB) для стеганографічного приховування даних у векторних SVG-зображеннях шляхом одночасного приховування в координатній та колірній складових. Також проведено комплексний порівняльний аналіз ефективності запропонованого методу вбудовування в векторний формат SVG з растровим форматом BMP. Аналіз останніх досліджень і публікацій демонструє науковий дефіцит у галузі стеганографічного використання векторних веб-ресурсів, які через свою архітектуру залишаються менш вивченими порівняно з звичними растровими зображеннями. Методика дослідження описує процес стандартизації вхідних графічних об'єктів та покроковий алгоритм, який реалізує як класичну модифікацію кольору шляхом заміни наймолодших бітів, так і запропоновану гібридну стратегію. Цей метод передбачає розщеплення потоку секретного повідомлення між текстовими шістнадцятковими кодами палітри кольорів та числовими координатами геометричних примітивів шляхів малювання. Основна частина та результати дослідження містять детальні експериментальні дані для різної кількості замінених бітів LSB. Продемонстровано, що ізольоване приховування по кольору в SVG має малу ємність через обмежену кількість тегів, але перехід до модифікації координат збільшує корисний простір ємності у десятки разів. Запропонований гібридний метод поєднання вбудовування секретних бітів і в колірну, і в координатну складову дозволив суттєво збільшити обсяг прихованих даних. За допомогою розрахунку метрик пікового відношення сигналу до шуму (PSNR) та індексу структурної подібності (SSIM) встановлено, що зі зростанням ємності вбудовування векторний формат демонструє стійкість до деградації якості: показник PSNR для SVG стабілізується на одному рівні незалежно від бітової глибини, тоді як якість BMP пропорційно падає і викликає появу візуальних артефактів.

Ключові слова: стеганографія; метод найменш значущого біта (LSB); гібридний метод; векторне зображення; растрове зображення; SVG; BMP; ємність стегоконтейнера; якість стегоконтейнера.

ВСТУП

Стеганографія є одним із напрямів захисту інформації, що полягає у приховуванні самого факту передачі секретної інформації . На відміну від криптографії, яка з використанням певних математичних перетворень приховує зміст повідомлення, стеганографія маскує існування секретної інформації шляхом її вбудовування у інші цифрові об’єкти, які називаються контейнерами [1]. Найчастіше у ролі контейнерів виступають зображення, хоча вбудовувати можна і у аудіо- та відео-файли, а також текстові документи.

Сьогодні методи стеганографії знаходять застосування у багатьох сферах, зокрема для захисту конфіденційних даних, прихованого обміну інформацією, цифрового маркування контенту, підтвердження авторських прав, забезпечення автентичності документів та передачі службових даних у відкритих мережах [2, 3, 4].

Загалом існує широкий спектр стеганографічних методів, але одним із перших і найвідоміших методів стеганографічного приховування інформації в растрових зображеннях є метод найменш значущого біта (Least Significant Bit, LSB) [5]. Його основна ідея полягає у вбудовуванні бітів секретного повідомлення в найменш значущі біти значень кольорових компонентів пікселів зображення-контейнера.

У растрових зображеннях кожен піксель описується числовими значеннями кольорів. Наприклад, у форматі RGB (див.рис.1) кожен піксель містить три компоненти: червону (Red), зелену (Green) та синю (Blue), кожна з яких зазвичай кодується одним байтом (8 бітами).

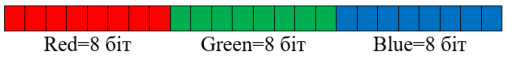

Рис. 1. Структура RGB формату

На рисунку 2 показано структуру байта, що складається з восьми бітів, де старші біти (Most significant bit, MSB) мають найбільшу вагу та найбільше впливають на значення числа, а молодші біти (Least significant bit, LSB) мають найменшу вагу. Саме найменш значущі біти використовуються для приховування інформації, оскільки вони мають найменший вплив на загальне значення кольору, тому їх зміна практично непомітна людському оку.

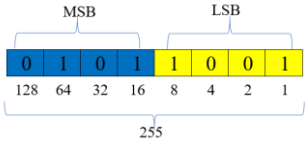

Рис. 2. Бінарне представлення байту

Процес приховування інформації за методом LSB складається з кількох етапів. Спочатку секретне повідомлення перетворюється у бінарну послідовність. Далі послідовно переглядаються пікселі зображення, а найменш значущі біти їхніх кольорових компонент замінюються бітами повідомлення. Існують чисельні модифікації методу заміни наймолодших бітів, описані в працях [6, 7, 8] та дослідження методів виявлення секретних повідомлень, вбудованих LSB методом [9, 10].

Традиційно метод LSB використовується переважно для растрових зображень, де контейнер представлений сукупністю пікселів. Растрова графіка забезпечує значну ємність для приховування даних завдяки великій кількості кольорових компонентів, зміни яких залишаються практично непомітними для людського ока, тож переважна більшість досліджень використовує саме цей тип зображень. Водночас кількість наукових праць, що розглядають особливості застосування цього методу до специфічних типів зображень і форматів, залишається обмеженою [11, 12].

Проте поряд із растровою графікою широкого поширення набула векторна графіка, яка використовується для створення логотипів, технічних креслень, картографічних матеріалів, інфографіки та вебконтенту. На відміну від растрових зображень, що складаються з пікселів, векторні зображення описуються математичними об'єктами – лініями, кривими, багатокутниками та іншими геометричними примітивами [13]. Основною перевагою векторної графіки є можливість масштабування без втрати якості та порівняно невеликий розмір файлів.

Зростання популярності форматів векторної графіки створює передумови для використання їх як контейнерів для приховування інформації. Використання лише растрових контейнерів обмежує сферу застосування стеганографічних методів, тоді як векторні зображення широко використовуються в сучасних інформаційних системах та часто передаються через мережу. Крім того, особливості структури векторної графіки відкривають нові можливості для вбудовування даних шляхом модифікації параметрів геометричних об'єктів без помітного погіршення візуальної якості зображення.

У [14] проведено порівняльний аналіз форматів SVG та PNG з огляду можливості вбудовування прихованих зображень. Водночас дослідження методів приховування інформації у векторній графіці залишається актуальним науковим напрямом, оскільки сприяє розширенню функціональних можливостей сучасної стеганографії та підвищенню різноманітності контейнерів для прихованого передавання даних.

Отже метою даної роботи є дослідження якості растрових та векторних зображень після стеганографічних перетворень та модифікація методу заміни наймолодшого біта в SVG-зображеннях.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

SVG (Scalable Vector Graphics) – це відкритий формат векторної графіки, розроблений консорціумом W3C, який базується на мові розмітки XML. На відміну від растрових форматів, SVG-зображення описується не набором пікселів, а сукупністю геометричних примітивів, їхніх властивостей та взаємного розташування.

Структурно SVG-файл являє собою текстовий документ XML, кореневим елементом якого є тег <svg>. Цей елемент визначає розміри полотна, систему координат та містить усі графічні об'єкти зображення [15]. Основними складовими SVG-документа є:

– графічні примітиви (<rect>, <circle>, <ellipse>, <line>, <polyline>, <polygon>, <path>), які описують геометричні фігури;

– текстові елементи (<text>), призначені для відображення текстової інформації;

– групи об'єктів (<g>), що забезпечують логічне об'єднання декількох елементів;

– стилі оформлення, які можуть задаватися безпосередньо в атрибутах елементів або за допомогою CSS;

– метадані та службові елементи (<metadata>, <defs>, <desc>), які містять додаткову інформацію про зображення або визначення об'єктів для повторного використання;

– трансформації (transform), що дозволяють виконувати масштабування, обертання, переміщення та інші геометричні перетворення.

Графічні примітиви, в свою чергу, містять такі атрибути як fill чи stroke, які задають колір для ліній чи заливки геометричних фігур. Колір подається у шістнадцятковому форматі або у форматі трьох чисел від 0 до 255, тобто RGB [15].

Елемент <path> є одним із найбільш універсальних та функціонально насичених графічних примітивів формату SVG. Він призначений для опису складних геометричних контурів за допомогою послідовності команд та координат, що визначають траєкторію побудови зображення [16].

Структура елемента <path> визначається атрибутом d, який містить набір команд керування побудовою контуру. Кожна команда задає певну графічну операцію, зокрема переміщення поточної точки, побудову відрізків прямих або замикання контуру. Загальний вигляд елемента можна подати таким чином:

```
<path d="M x1,y1 L x2,y2 C x3,y3 x4,y4 x5,y5 Z"/>
```

Атрибут d даного елементу може мати наступні елементи [16]:

– M (Move To) встановлює початкову точку контуру;
– L (Line To) створює відрізок прямої до заданої точки;
– H та V задають горизонтальні та вертикальні лінії відповідно;
– C (Cubic Bezier Curve) будує кубічну криву Безьє;
– Q (Quadratic Bezier Curve) будує квадратичну криву Безьє;
– A (Arc) формує дугу еліпса;
– Z (Close Path) замикає контур.

В подальшому саме атрибути кольорових гам та координат будуть використовуватися для реалізації методу найменш значущого біта у зображеннях формату SVG.

МЕТОДИКА ДОСЛІДЖЕННЯ

Методика дослідження побудована на порівняльному аналізі аспектів алгоритмів стеганографії найменшого значущого біта у векторному форматі Scalable Vector Graphics (SVG) та растровому форматі Bitmap (BMP). Для забезпечення об'єктивності експерименту початковим етапом є стандартизація вхідних даних, яка буде передбачати створення пар ідентичних графічних об'єктів. Тестовий зразок розробляється як оригінальне векторне зображення у форматі SVG, після чого воно перетворюється в нестиснуте растрове зображення BMP із фіксованою глибиною кольору 24 біти на піксель, тобто по 8 бітів на один з каналів кольору RGB.

Процедура приховування інформації в растровому зображенні BMP використовує класичний підхід до приховування інформації шляхом заміни наймолодшого біта. Алгоритм зчитує бінарний потік повідомлення, який доповнюється позначкою кінця даних, і здійснює побітну заміну визначеної кількості наймолодших бітів у колірних каналах RGB кожного пікселя. Модифікація виконується безпосередньо з байтовим масивом зображення, що дозволяє визначати кількість бітів для заміни на один колірний канал, відповідно збільшуючи місткість контейнера ціною потенційного спотворення зображення артефактами.

У векторному зображенні SVG методика дещо змінена, оскільки замість піксельної матриці об'єктом модифікації виступає текст XML-файлу. Програмний алгоритм здійснює обхід дерева елементів документа за допомогою синтаксичного парсера. Запропонований нами алгоритм пропонує гібридну стратегію стеганографічного приховування найменшого значущого біта, яка базується на уже існуючих поокремих методах [17], і полягає в розділенні бінарного потоку приховуваного повідомлення між значеннями кольорів (які теж розбиваються на три кольорові канали) та числовими координатами геометричних примітивів. Для колірних атрибутів заливки `<… fill=″ ″>` та контуру `<… stroke=″ ″>` застосовується аналогічна до растрового варіанту побітна заміна найменших значущих бітів у колірних каналах. Для координатних атрибутів застосовується алгоритм, що базується на принципі механізму чисел з плаваючою комою. Цей алгоритм пропонує інтеграцію бітів повідомлення у найменш значущі біти числового значення після коми, яке конвертується в двійкову форму, а потім назад в десяткову. Це забезпечує мінімальне зміщення геометричних точок на соті і тисячні частки пікселя.

Заключний етап методики присвячено збору та обчисленню метрик якості та ємності та проведенню порівняльного аналізу. Візуальна якість растрових стегозображень вимірюється за допомогою метрик візуальної відповідності, а саме через розрахунок пікового відношення сигналу до шуму (PSNR) та індексу структурної подібності (SSIM). Для оцінки аналогічних метрик векторних файлів SVG проводиться їх апаратний рендеринг у растрове зображення та фіксується абсолютна місткість контейнерів в бітах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На першому етапі ми досліджували вплив кількості вбудованих бітів LSB на якість зображення. Потрібно зазначити, що під час цієї ітерації стеганографічна модифікація обмежувалася лише атрибутами колірних палітр без залучення інших компонентів XML-коду. Візуальне зіставлення вихідного порожнього та заповненого стегоконтейнерів, де було здійснено заміну п’яти наймолодших бітів, для растрового формату представлено на рисунку 3, тоді як відповідні результати порівняння для векторного формату відображено на рисунку 4.

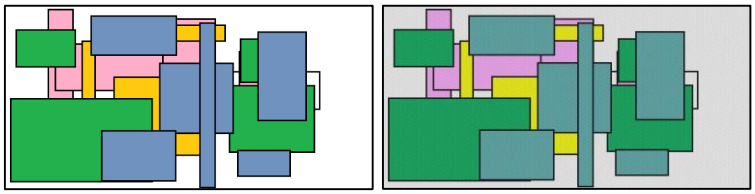

Рис. 3. Порожнє та заповнене растрові зображення

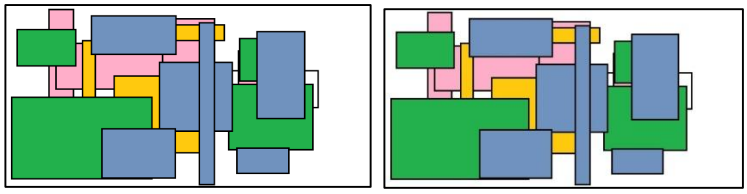

Рис. 4. Порожнє та заповнене векторні зображення

Візуальна оцінка зображень свідчить, що за однакової кількості замінюваних бітів растрове зображення зазнає відчутної деградації (особливо це можна помінити по зміні білого фону) з появою цифрових артефактів, тоді як векторний аналог зберігає стабільність структури і залишається, фактично, без видимих змін. Для підтвердження цієї гіпотези та отримання точних кількісних характеристик у таблиці 1 наведено розраховані метрики візуальної відповідності.

Таблиця 1

Метрики візуальної відповідності

К-ть замінюваних бітів LSB	SVG PSNR, дБ	BMP PSNR, дБ	SVG SSIM, %	BMP SSIM, %
1	61.4036	52.2294	99.9964	99.9129
3	53.6425	41.5010	99.9791	99.0077
5	44.0601	31.2085	99.7495	93.3497

Результати представлені у таблиці 1, демонструють обернено пропорційну залежність між кількістю замінюваних бітів LSB та метриками якості для обох графічних форматів, проте в різних масштабах. При збільшенні глибини вбудовування прихованих бітів з 1 до 5 спостерігається прогнозоване зниження показників PSNR та SSIM, що зумовлено зростанням колірних та координатних відхилень у стегоконтейнерах. Векторний формат SVG демонструє вищу стійкість до деградації зображення порівняно з растровим BMP, і навіть при максимальному навантаженні у 5 бітів показник PSNR для SVG залишається на високому рівні (більше 40 дБ), тоді як якість BMP стрімко падає нижче критичного порогу сприйняття (критичний поріг зазвичай приймається за 30 дБ).

Також важливою характеристикою для оцінки ефективності стеганографічного підходу є корисна ємність стегоконтейнера. Результати дослідження ємності інформації, яку можливо приховати виключно за рахунок колірних палітр, наведено в таблиці 2.

Таблиця 2

Ємності стегоконтейнерів в різних ітераціях LSB по кольору

К-ть замінюваних бітів LSB	Ємність бітів для приховування в SVG зображенні	Ємність бітів для приховування в BMP зображенні	Загальна кількість бітів в SVG зображенні	Загальна кількість бітів в BMP зображенні
1	9220	2190144	8400008	17521152
3	27660	6570432		
5	46100	10950720		

Згідно з представленими в таблиці 2 даними, традиційне використання LSB модифікації лише для колірних атрибутів у форматі SVG демонструє низькі показники абсолютної ємності, які суттєво поступаються растровому аналогу. Такий значний розрив у цифрах пояснюється структурними відмінностями форматів. У той час як нестиснутий файл BMP надає для маніпуляцій великий масив колірних байтів кожної піксельної точки, SVG-файл містить обмежену кількість тегів заливки (fill) та контуру (stroke), які можна використати для тієї ж мети. З огляду на це, базова місткість векторного контейнера, що використовує для заміни лише колірну гаму, є недостатньою для приховування великих обсягів даних. Це обґрунтовує необхідність розширення стеганографічного простору SVG шляхом інтеграції додаткових структурних елементів для приховування, а саме – модифікації числових параметрів координат. Результати вимірювання ємності стегоконтейнерів при переході на координатні атрибути SVG порівняно з класичним колірним методом у BMP наведено в таблиці 3.

Таблиця 3

Ємності стегоконтейнерів в різних ітераціях LSB по координатах в SVG, кольору в BMP

К-ть замінюваних бітів LSB	Ємність бітів для приховування в SVG зображенні	Ємність бітів для приховування в BMP зображенні	Загальна кількість бітів в SVG зображенні	Загальна кількість бітів в BMP зображенні
1	566158	2190144	8400008	17521152
3	1698474	6570432		
5	2830790	10950720		

Як демонструють дані таблиці 3, перенесення процесу приховування інформації в координати дозволило суттєво збільшити стеганографічний потенціал SVG, збільшивши ємність у 60 разів. Цей стрибок зумовлений високою щільністю числових значень у векторах шляхів малювання. Але попри зростання, чиста координатна місткість все ще залишається меншою за потенціал растрових зображень. З метою досягнення максимально можливого ефекту та використання всіх доступних структурних

компонентів XML-коду було протестовано запропонований раніше гібридний підхід. Повні результати дослідження місткості векторних контейнерів за умов одночасного використання обох каналів приховування (як колірних атрибутів, так і координатних) відображено в таблиці 4.

Таблиця 4

Ємності стегоконтейнерів в різних ітераціях LSB – гібридний в SVG, по кольору в BMP

К-ть замінюваних бітів LSB	Ємність бітів для приховування в SVG зображенні	Ємність бітів для приховування в BMP зображенні	Загальна кількість бітів в SVG зображенні	Загальна кількість бітів в BMP зображенні
1	575378	2190144	8400008	17521152
3	1726134	6570432		
5	2876890	10950720		

Аналіз даних таблиці 4 підтверджує, що запропонований гібридний метод, який інтегрує бінарний потік одночасно в колірні значення та геометричні координати SVG, забезпечує найвищі показники місткості серед усіх ітерацій. Хоча сумарна ємність гібридного SVG-контейнера через загальний розмір текстового файлу математично не наздоганяє растрову матрицю BMP, розроблений метод все ж вирішує проблему дефіциту стеганографічного простору векторних об'єктів. Створена комбінована схема дозволяє передавати великі масиви інформації всередині векторних зображень в форматі тексту, що робить SVG повноцінним середовищем для побудови прихованих каналів зв'язку.

Останнім етапом оцінки ефективності гібридного підходу є дослідження його впливу на артефакти візуального відображення, оскільки одночасне навантаження на два канали приховування може спровокувати помітніший ефект спотворення. Зведені дані розрахунку метрик пікового відношення сигналу до шуму та індексу структурної подібності для інтегрованого методу наведено в таблиці 5.

Таблиця 5

Метрики візуальної подібності гібридного методу LSB для SVG

К-ть замінюваних бітів LSB	SVG PSNR, дБ	BMP PSNR, дБ	SVG SSIM, %	BMP SSIM, %
1	30.14227717	52.2294067	0.9506906132	0.9991297207
3	30.13928957	41.50101418	0.9504849462	0.9900777021
5	30.09975461	31.20853824	0.9487428316	0.9334971513

Аналіз обчислених значень у таблиці 5 демонструє специфічний характер деградації якості векторних зображень у разі застосування гібридного алгоритму. На відміну від растрового формату BMP, де показники PSNR та SSIM плавно знижуються пропорційно до зростання кількості вбудованих бітів, гібридний метод для SVG фіксує знижене значення PSNR незалежно від бітової глибини. Така стабілізація показника, вочевидь, зумовлена тим, що основний внесок у геометричне спотворення робить сам факт впровадження даних у координати (зсув точок), тоді як збільшення кількості замінюваних бітів майже не погіршує візуальну картину. З огляду на це, стає очевидним стеганографічний компроміс, в якому гібридний метод забезпечує хорошу місткість, проте вимагає пошуку балансу між обсягом секретних даних та візуальною якістю, оскільки значення PSNR нижче 30 дБ є критичним для збереження прихованості вбудованого повідомлення.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження було запропоновано та протестовано гібридний метод стеганографічного приховування даних шляхом заміни наймолодших бітів для формату SVG, який базується на одночасному використанні колірних та координатних атрибутних просторів XML коду. Проведений порівняльний аналіз із растровим форматом BMP показав, що ізольоване використання колірних атрибутів у SVG не забезпечує достатньої місткості для передачі масивів інформації через обмежену кількість тегів заливки та контуру в структурі XML. Додавання додаткового простору за рахунок модифікації числових параметрів координат за принципом механізму чисел з плаваючою комою дозволило розширити ємність векторного стегоконтейнера у десятки разів.

Оцінка якості вбудованих контейнерів за допомогою обчислення метрик візуальної подібності також підтвердила високу стійкість до спотворень векторного формату навіть зі зростанням кількості вбудованих біт. Геометричне спотворення SVG зображення, зумовлене зсувом координат на мінімальні частки пікселя під час модифікації координатного простору, Завдяки зміні наймешш значущих розрядів

після коми збільшення кількості замінюваних бітів практично не впливає на фінальний рендеринг зображення.

Перспективи подальших досліджень у цьому напрямі полягають у розширенні спектрів дослідження ефективності розробленого гібридного методу вбудовування інформації в SVG зображеннях. Окремим потенційним вектором розвитку може стати дослідження способів штучного збільшення ємності в SVG файлах. Окрім цього, науковий інтерес становить інтеграція інтелектуальних засобів криптографічного шифрування, що забезпечить додатковий рівень безпеки та захистить приховане повідомлення від декодування у разі його виявлення сучасними автоматизованими системами стегоаналізу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kumar, A., & Pooja, K. (2010). Steganography: A data hiding technique. *International Journal of Computer Applications, 9*(7), 19-23. https://doi.org/10.5120/1398-1887
2. Beridze, B., & Donadze, M. (2025). Steganography and its application prospects in information protection. In *Proceedings of the International Scientific-Practical Conference "Modern Challenges and Achievements in Information and Communication Technologies"* (Vol. 4, pp. 39-45). https://papers.4science.ge/index.php/mcaaict/article/view/361
3. Rusu, M. (2023). (Simple) applications of steganography for images. *Scientific Bulletin of Naval Academy, 26*(2), 94-99. https://doi.org/10.21279/1454-864X-23-I2-011
4. Megías, D., Mazurczyk, W., & Kuribayashi, M. (2021). Data hiding and its applications: Digital watermarking and steganography. *Applied Sciences, 11*(22), 10928. https://doi.org/10.3390/app112210928
5. Sakshi, S., Verma, S., Chaturvedi, P., & Yadav, S. (2022). Least significant bit steganography for text and image hiding. In *Proceedings of the 3rd International Conference on Intelligent Engineering and Management (ICIEM 2022)* (pp. 415-421). IEEE. https://doi.org/10.1109/ICIEM54221.2022.9853052
6. Aljughaiman, A., & Alrawashdeh, R. (2025). Content-adaptive LSB steganography with saliency fusion, ACO dispersion, and hybrid encryption with ablation study. *Scientific Reports*. https://doi.org/10.1038/s41598-025-33920-9
7. Patel, A., & Vekariya, D. (2026). An efficient image steganography method using block-based indexing and LSB substitution. *Journal of Innovative Image Processing, 8*, 536-557. https://doi.org/10.36548/jiip.2026.2.006
8. Abu Zaher, M. (2010). Modified least significant bit (MLSB). *Computer and Information Science, 4*(1), 60-67. https://doi.org/10.5539/cis.v4n1p60
9. Watters, P., Martin, F., & Stripf, H. S. (2008). Visual detection of LSB-encoded natural image steganography. *ACM Transactions on Applied Perception, 5*(1), 1-12. https://doi.org/10.1145/1279640.1328775
10. Fridrich, J., Goljan, M., & Du, R. (2002). Reliable detection of LSB steganography in color and grayscale images. In *Proceedings of the ACM Workshop on Multimedia and Security* (pp. 27-30). ACM. https://doi.org/10.1145/1232454.1232466
11. Koptyra, K., & Ogiela, M. R. (2024). Steganography in QR codes: Information hiding with suboptimal segmentation. *Electronics, 13*(13), 2658. https://doi.org/10.3390/electronics13132658
12. Gao, M., & Sun, B. (2011). Blind watermark algorithm based on QR barcode. In Y. Wang & T. Li (Eds.), *Foundations of Intelligent Systems* (Vol. 122, pp. 431-438). Springer. https://doi.org/10.1007/978-3-642-25664-6_52
13. Almutairi, B. (2019). A new steganography method for scalable vector graphics (SVG) images based on an improved LSB algorithm. *Journal of Computer Science and Network Security, 19*(10), 99-104. http://paper.ijcsns.org/07_book/201910/20191016.pdf
14. Almutairi, A. (2018). A comparative study on steganography digital images: A case study of scalable vector graphics (SVG) and portable network graphics (PNG) image formats. *International Journal of Advanced Computer Science and Applications, 9*(1), 170-175. https://doi.org/10.14569/IJACSA.2018.090123
15. Eisenberg, J., & Eisenberg, J. D. (2002). *SVG essentials*. O'Reilly Media. https://theswissbay.ch/pdf/Gentoomen%20Library/Misc/O'Reilly%20SVG%20Essentials.pdf
16. Libby, A. (2018). *Beginning SVG*. Apress. https://doi.org/10.1007/978-1-4842-3760-1
17. Securing information for commercial file sharing by combining raster graphic and vector graphic steganographies. (2019). *International Journal of Engineering and Advanced Technology, 8*(6), 788-795. https://doi.org/10.35940/IJEAT.F8005.088619

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Oleh Yarema
PhD student of the Cybersecurity Department
Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine
ORCID: 0009-0009-8709-7813
yarema.oleh.m@gmail.com

Nataliya Zagorodna
PhD (Technical Sciences), Head of the Cybersecurity Department
Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine
ORCID: 0000-0002-1808-835X
zagorodna_n@tntu.edu.ua

Maryna Derkach
PhD (Technical Sciences), Associate Professor of the Cybersecurity Department
Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine
ORCID: 0000-0001-8977-2776
m_derkach@tntu.edu.ua

Oleksandr Revniuk
PhD, Assistant Professor of the Cybersecurity Department
Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine
ORCID: 0009-0005-0511-5354
revo0708@gmail.com

Myroslava Zagorodna
Junior Research Scientist
Institute of Veterinary Medicine of NAAN, Ternopil, Ukraine
ORCID: 0009-0002-3258-4904
myroslavazagorodna@gmail.com

A MODIFICATION OF THE LEAST SIGNIFICANT BIT STEGANOGRAPHY METHOD IN SVG IMAGES

Abstract. This paper proposes and investigates a modification of the least significant bit (LSB) replacement method for steganographic data hiding in SVG images by simultaneously hiding data in both the coordinate and color components. A comprehensive comparative analysis of the effectiveness of the proposed method of embedding data into the vector SVG format versus the raster BMP format is also conducted. An analysis of recent publications reveals a research gap in the field of steganographic use of vector web resources, which, due to their architecture, remain less studied compared to raster images. The research methodology describes the process of standardizing input graphic objects and a step-by-step algorithm that implements both the classical color modification by replacing the least significant bits and the proposed hybrid strategy. This method involves splitting the secret message stream between the text-based hexadecimal codes of the color palette and the numerical coordinates of the geometric primitives of the drawing paths. The results of the study contain detailed experimental data for various numbers of replaced LSBs. It is demonstrated that isolated color-based hiding in SVG has low capacity due to the limited number of tags. Switching to coordinate modification increases the usable capacity almost by ten. The proposed hybrid method, which combines the embedding of secret bits into both the color and coordinate components allowed significantly increase the amount of hidden data. Using Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index (SSIM), it was found that the vector format demonstrates resistance to quality degradation as number of hidden bits increases: the PSNR value for SVG remains stable regardless of bit depth, whereas BMP quality decreases proportionally and leads to the appearance of visual artifacts.

Keywords: steganography; least significant bit (LSB) method; hybrid method; vector image; raster image; SVG; BMP; steganographic container capacity; steganographic container quality.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Rahmati, M. (2025, February). *Federated learning driven cybersecurity framework for IoT networks with privacy-preserving and real-time threat detection capabilities*. arXiv. https://arxiv.org/abs/2502.10599
2. Wu, J., Wang, Y., Dai, H., Xu, C., & Kent, K. B. (2023, March). *Adaptive bi-recommendation and self-improving network for heterogeneous domain adaptation assisted IoT intrusion detection*. arXiv. https://arxiv.org/abs/2303.14317
3. Lai, T., Farid, F., Bello, A., & Sabrina, F. (2023, July). *Ensemble learning-based anomaly detection for IoT cybersecurity via Bayesian hyperparameters sensitivity analysis*. arXiv. https://arxiv.org/abs/2307.10596
4. Mehedi, S. T., Anwar, A., Rahman, Z., Ahmed, K., & Islam, R. (2022, April). *Dependable intrusion detection system for IoT: A deep transfer learning-based approach*. arXiv. https://arxiv.org/abs/2204.04837
5. Haidur, H. I., Shulimova, D. D., Boyko, A. O., & Postnikov, Y. I. (2024). Model zabezpechennia kiberbezpeky Internetu rechei. *Telecommunication and Information Technologies*. https://tit.dut.edu.ua/index.php/telecommunication/article/view/2524
6. Zhydka, O. V., & Andriychenko, T. R. (2024). Informatsiina bezpeka system IoT. *Communication (Zhurnal)*. https://doi.org/10.31673/2412-9070.2024.046569
7. Merzlikin, Y., & Babeshko, Y. (2023). Analiz kiberbezpeky weboriientovanykh industrialnykh IoT-system. *ITSSI Journal, 24*. https://www.itssi-journal.com/index.php/ittsi/article/view/397
8. Dudykevych, V., Mykytyn, H., & Murak, T. (2025). Intehralna model bezpeky Internetu rechei u prostori intelektualizatsii obiektiv infrastruktury. *Cybersecurity: Education, Science, Technology*. https://csecurity.kubg.edu.ua/index.php/journal/article/view/848
9. Hlybovets, A., Shcherbyna, S., & Kiriienko, O. (2024). Vrazlyvosti bezpeky ta rishennia dlia zakhystu v systemakh Internetu rechei. *Naukovi zapysky NaUKMA*. https://doi.org/10.18523/2617-3808.2024.7.89-97
10. Zayats, V. (2024). Intehratsiia shtuchnoho intelektu v protokoly bezpeky Internetu rechei. *Kiberbezpeka ta kompiuterno intehrovani tekhnolohii*. https://conference.wunu.edu.ua/index.php/kbkit/article/view/733
11. Pedan, S. I., Melnyk, M. V., & Alekseyev, M. O. (2024). Pidvyshchennia bezpeky ziednannia IoT-prystroiv shliakhom analizu bezdrotovykh syhnaliv. In *Proceedings of the International Conference "Perspektyvy telekomunikatsii"*. https://conferenc-journal.its.kpi.ua/article/view/307418
12. Shabala, Y., & Korniichuk, B. (2024). Metodolohiia otsiniuvannia bezpeky IoT na promyslovykh obiektakh. *Upravlinnia rozvytkom skladnykh system*. https://doi.org/10.32347/2412-9933.2024.60.146-155
13. Klyap, M., Lyakh, I., Shumylo, N., & Tsipinyo, A. (2025). Bezpeka IoT protokoliv yak vyklyk dlia mizhnarodnoho spivrobitnytstva. *Nauka i tekhnika sohodni*. https://dspace.uzhnu.edu.ua/items/2dfa3e55-9e32-4e78-a328-5c5c5a502c3f
14. Pavlenko, K. Y., & Sribna, I. M. (2025). *Modeliuvannia zahroz bezpetsi v IoT systemakh okhorony: Pidkhody do minimizatsii ryzykiv* (Master's thesis). https://conf.ztu.edu.ua/wp-content/uploads/2025/01/103.pdf
15. Shabala, Y. (2025). *Model hibrydnoi IoT systemy z pidvyshchenym rivnem informatsiinoi bezpeky* (Qualification work). https://ir.library.knu.ua/entities/publication/c6919d27-5039-4948-857f-f0463f305ae1

Отримано редакцією журналу / Received: 05.03.26
Прорецензовано / Revised: 15.03.26
Схвалено до друку / Accepted: 25.06.26