Ахмаметьєва Ганна Валеріївна
к.т.н., доцент, доцент кафедри кібербезпеки,
Національний університет «Одеська юридична академія»

СВІТОВІ ТЕНДЕНЦІЇ РОЗВИТКУ СТЕГАНОАНАЛІЗУ ЦИФРОВИХ ЗОБРАЖЕНЬ

DOI https://doi.org/10.36059/978-966-397-537-5-7

Широке застосування мультимедійних даних в мережі Internet призводить до швидкого розповсюдження спотворень цифрових зображень (ЦЗ), що полягають у ненавмисних пошкодженнях, таких як незначні похибки при передачі каналами зв'язку або результат фільтрації або стиснення при користуванні деякими додатками, або навмисних, зокрема цілеспрямоване пошкодження зображень, їх розмиття, клонування, фальсифікація (як авторства, так і самих даних), тощо. Через обмеження неконтрольованого застосування криптографічних засобів захисту в ряді країн світу набув розвиток стеганографії – наукового напряму, який займається розробкою та дослідженням методів організації прихованого каналу зв'язку через вбудовування конфіденційної інформації в цифровий контейнер. Найчастіше в якості контейнеру застосовуються ЦЗ через особливості їх структури, що містить достатній обсяг надлишкової інформації для приховування в них секретних даних.

На даний час існує величезна кількість стеганографічних методів, які дозволяють вбудувати повідомлення в просторову або частотну область ЦЗ. Просторові стеганографічні методи, такі як метод заміни найменшого значущого біту LSB (Least Significant Bit) та його варіації [1–4], численні модифікації методів PVD (Pixel Value Differencing) [5–7] забезпечують високу пропускну спроможність прихованого каналу зв'язку, тобто обсяг вбудованої інформації (payload) в біт/піксель (bpp), є простими в реалізації. Такі методи часто забезпечують високу візуальну якість заповненого контейнеру (стеганоповідомлення, СП, stego), однак є нестійкими до ряду атак, таких як просторова фільтрація, яскравісні перетворення, стиснення, які спричиняють повне або часткове руйнування вбудованих даних.

У сучасних дослідженнях, присвячених стеганоаналізу (основною задачею якого є виявлення і доведення факту існування прихованого повідомлення в цифровому контенті), серед просторових методів вбудовування широкого поширення набули методи HUGO [8], WOW [9], S-UNIWARD [10], MiPOD [11], Hill [12] через наявність їх програмних реалізації мовами програмування C++ (Windows, Linux) та MatLAB у відкритому доступі [13].

На відміну від просторових методів частотні застосовують різні перетворення, зокрема дискретне косинусне перетворення [14–16], Вейвлет-перетворення [17–18], перетворення Фур'є [19] та інші. Стеганографічні методи, побудовані на їх основі, більш складні в реалізації, в деякій мірі допускають можливість незначного спотворення прихованої інформації, проте забезпечують стійкість до атак стиснення та деяких інших, проти яких просторові методи стеганографії безсильні.

З метою протидії безконтрольного обміну злочинних та протизаконних повідомлень через приховані канали зв'язку необхідно розвивати та удосконалювати методи стеганоаналізу. Через те, що існує величезна кількість методів вбудовування секретної інформації та наявні різні параметри як самого алгоритму вбудовування/вилучення, також існує можливість варіювати пропускну спроможність або задавати стеганографічний ключ, який задає порядок вибору елементу контейнера, відновлення прихованого повідомлення – вкрай складна і на даний час нереалізована задача. Однак довести факт існування в цифровому контенті деякого секретного повідомлення, оцінити приблизну пропускну спроможність або визначити область або елементи, використані для вбудовування, на даний час не викликає певних труднощів.

Слід зазначити, що на ефективність виявлення вкладень в значній мірі впливає пропускна спроможність прихованого каналу зв'язку, адже незважаючи на можливість ЦЗ вмістити значний обсяг додаткової інформації, найчастіше її вбудовують з малим значенням payload: від 0,05 до 0,5 bpp, що забезпечує більш високу якість результуючого зображення та відсутність небажаних артефактів.

Серед стеганоаналітичних методів розрізняють спеціальні – спрямовані проти виявлення стеганоповідомлень, вбудованих конкретним

визначеним стеганографічним методом, та універсальні, що охоплюють широку групу методів вбудовування. Прийнято розрізняти універсальні методи, що здатні виявляти наявність секретної інформації, вбудованої в просторову область контейнера, та універсальні методи, спрямовані проти стеганографії в області перетворень. Останнім часом загально поширеною є тенденція застосування нейронних мереж для навчання на основі тестової вибірки та подальшого аналізу випадкових даних.

Метою дослідження є аналіз сучасних тенденцій в області стеганоаналізу з урахуванням ефективності виявлення вкладень в цифрових зображеннях, вбудованими поширеними стеганографічними алгоритмами при малих значеннях пропускної спроможності прихованого каналу зв'язку в просторову область та область перетворень контейнерів.

Для розв'язання поставленої мети необхідно:

– проаналізувати сучасні рішення стеганоаналізу для виявлення вкладень в ЦЗ, вбудованих в просторову область контейнера;

– навести порівняльний аналіз ефективності стеганоаналітичних методів, що виявляють вкладення на основі просторової області ЦЗ;

– порівняти ефективність раніше розробленого автором методу Color Triads з сучасними рішеннями стеганоаналізу;

– проаналізувати сучасні стеганоаналітичні методи для виявлення вкладень в ЦЗ, вбудованих в область перетворень контейнера;

– навести порівняльний аналіз ефективності стеганоаналітичних методів, що виявляють вкладення в області перетворень ЦЗ.

Об'єкт дослідження – процеси організації і виявлення стеганографічного каналу зв'язку.

Предмет дослідження – стеганоаналітичні методи для цифрових зображень.

Оцінювати ефективність виявлення наявності прихованих повідомлень будемо на основі показника точності детектування (Accuracy – *Acc*), який визначається на основі бінарної класифікації (табл. 1) за формулою:

$$Acc = \frac{TP + TN}{P + N}, \quad P = TP + FN, \quad N = FP + TN.$$

Таблиця 1 – Позначення бінарної класифікації в задачах стеганоаналізу

		Вірна гіпотеза	
		Контейнер	**Стегано-повідомлення**
Результат класифікації	Контейнер	*TN* – True Negative	*FP* – False Positive
	Стегано-повідомлення	*FN* – False Negative	*TP* – True Positive

Тобто, *TN* – деяке ЦЗ визначається як незаповнений контейнер, і це так насправді є; *FP* – незаповнений контейнер визначається як стеганоповідомлення (в літературі такі помилки називають помилки II роду); *FN* – стеганоповідомлення визначається як незаповнений контейнер (помилки I роду); *TP* – заповнене ЦЗ правильно визначається як стеганоповідомлення.

В сучасній обробці даних, зокрема цифрових зображень, поширено використання згорткових нейронних мереж (Convolutional Neural Networks, CNN), які побудовані на основі матричної структури та здатні автоматично і адаптивно виявляти та навчатися просторової ієрархії ознак, наприклад, просторові особливості перепадів яскравості, високочастотні, середньочастотні або низькочастотні характеристики на основі дискретного косинусного перетворення, перетворення Фур'є та інших. Часто CNN поєднують з технологією глибокого навчання (Deep Learning Networks, DNN), коли неможливо чітко визначити ті характеристики, які властиві, наприклад, лише стеганоповідомленням. В більшості випадків неможливо спрогнозувати, які саме характеристичні особливості будуть збурені тим чи іншим стеганографічним методом, оскільки велике значення в процесі стеганоперетворення має і обраний контейнер.

Розглянемо деякі сучасні методи стеганоаналізу, побудовані на основі нейронних мереж, та проаналізуємо, наскільки ефективно вони виявляють вкладення, вбудовані за умови малої пропускної здатності.

У роботі [20] автори пропонують стеганоаналіз зображень, сформованих з низькою пропускною спроможністю, побудований на основі згорткової нейронної мережі, що включає шар передобробки

(виділення характерних особливостей на основі 30 високочастотних фільтрів), транспонована згортка (Transposed convolutional layer – TC), звичайні згортки (Convolutional layer – Conv) та повнозв'язні згортки (Fully connected layer – FC). Дослідженні були проведені для ЦЗ в градаціях сірого при використанні стеганографічних методів S-UNIWARD [10], WOW [9] та HUGO [8] для пропускної спроможності прихованого каналу зв'язку 0,2, 0,1 та 0,05 bpp. В роботі наведено порівняння результатів детектування з [21–23].

Мережа, запропонована в роботі [21], відрізняється від вищезгаданої кількістю звичайних згорткових шарів при аналогічних інших параметрах, в роботах [22; 23] додатково використовується усереднююче об'єднання(Average Polling layer – AP), в [22] – чотири AP та три FC, в [23] – три AC та один FC при одному високочастотному фільтрі на шарі передоборобки. У всіх згорткових мережах [21–23] відсутній шар TC. Порівнюючи вищезгадані чотири нейронні мережі лише перші дві надають адекватні результати детектування: при пропускній здатності 0,2 bpp отримано середню точність детектування 89 % та 85 % відповідно для [20] і [21], точність детектування для [22; 23] для 0,2 bpp не перевищує 65 %.

В роботі [24] запропоновано стеганоаналітичну нейронну мережу, що містить п'ять звичайних згорткових шарів, п'ять FC шари та два шари підвищення частоти дискретизації. Особливістю підходу є аналіз всіх частотних складових вхідних зображень, не лише високочастотних, як в попередніх методах. В статті наведені результати виявлення стеганоповідомлень, сформованих алгоритмами S-UNIWARD [10], WOW [9] та MiPOD [11], для пропускної здатності 0,1, 0,2, 0,3, 0,4, 0,5 bpp, які є достатньо високими для ємності 0,4, 0,5 bpp, однак значно просідають при 0,1 bpp (від 66 до 78 % в залежності від стеганоалгоритму).

Стаття [25] пропонує складну нейронну мережу, яка складається зі звичайних згорток з різними згортковими ядрами, роздільних згорток (Separable convolution), які оперують з 30 та 60 фільтрами, функцій пакетної нормалізації, поканальних згорток (Deethwise convolution), AP шарів та кінцевої глобальної AP-згортки. Наведені результати детектування для різних стеганографічних методів, результати яких наведено нижче в таблицях порівняння. Незважаючи на складність

запропонованої нейронної мережі результати детектування навіть для пропускної спроможності 0,4 bpp не перевищують 90 %.

В [26] запропоновано мережу на основі компонентів, які містить мережа [25] з додаванням шару просторового відсіву (Spatial Dropout Layer). Наведена точність детектування стеганоповідомлень на основі алгоритмів S-UNIWARD [10], WOW [9] та MiPOD [11], найкращі результати для пропускної спроможності 0,2 bpp отримано при виявленні WOW-стеганоповідомлень: точність виявлення становить 92 %. При менших значеннях пропускної здатності результати не перевищують 76 %.

У роботі [27] автори пропонують відносно просту нейронну мережу, у складі якої є звичайні згортки, AP-згортки та кінцева FC-згортка. Додатковим елементом мережі є коваріаційний пул (Covariance Pool). Передобробка ЦЗ включає пошук характеристик на основі високочастотних фільтрів. Особливістю нейронної мережі є можливість виявляти наявність прихованої інформації, вкладеної як просторовими стеганографічними методами, так і методами, що використовують область перетворень.

Автори статті [28] пропонують ще один метод, спроможний виявляти вкладання, вбудовані як просторовими стеганографічними методами, так і вбудовуванням в область перетворень. Стеганоаналітичний метод базується на аналізі характеристичних особливостей пересічних блоків, причому розмір цих блоків може бути довільним. На основі виявлених характеристик проводиться тренування нейронної мережі та подальше виявлення наявності секретних повідомлень. Результати алгоритму наведені лише для стеганометодів S-UNIWARD [10] та PQ [29], найкраща точність детектування відповідно складає 88,64 % та 82,5 % при пропускної спроможності 0,4 bpp. Також наведено порівняння результатів детектування з роботами [30–33].

У статті [30] наведена нейронна мережа для відокремлення незаповнених контейнерів від стеганоповідомлень, сформованих стеганоалгоритмами S-UNIWARD [10], WOW [9] та Hill [12]. Однак за наведеними результатами мережа здатна виявляти вбудовані вкладення з точністю не вище 90 % при пропускній здатності 0,5 bpp.

У [31] для стеганографічних методів S-UNIWARD [10], WOW [9], MiPOD [11] та HUGO [8] наведені результати

стеганоаналізу нейронною мережею, точність виявлення вкладень не перевищує 90 % для пропускної спроможності 0,4 bpp.

В роботі [32] проводиться дослідження нейронної мережі для виявлення прихованих вкладень в залежності від комбінації складових згортки, наведено результати тестування для стеганографічних алгоритмів S-UNIWARD [10] та WOW [9]. Завдяки запропонованій мережі найкращий результат складає 90,2 % для пропускної здатності 0,2 bpp при виявленні стеганоповідомлень, вбудованих алгоритмом WOW.

Серед просторових стеганографічних методів зберігають актуальність методи заміни найменшого значущого біту (Least Significant Bit, LSB), з'являються його різновиди [34–37], найчастіше метод LSB застосовується при малих значеннях прихованої пропускної спроможності.

Серед стеганоаналітичних розробок, спрямованих на виявлення вкладень LSB-алгоритмами, можна відзначити роботи [38; 39]. В публікації [38] запропонована нейронна мережа для здійснення WS-стеганоаналізу, яка досліджувалась для трьох випадків: при застосуванні лінійного усереднюючого фільтру (AVG), при використанні вибірки KB-dropout, на основі мережевої структури U-Net, а також наведено порівняння з результатами стеганоаналізу B0 [40], ns-B0 [41] та ns/r-B0 [42].

Робота [39] пропонує стеганоаналіз п'яти варіантів методу LSB, зокрема LSB Replacement (LSBR) при заміні одного та двох молодших бітів, LSB Matching, LSBMR, що описується формулою:

$$LSBMR = LSBR\,(f\,(A, B)),$$

де $f(A, B)$ – функція над парою пікселів A, B; та LSBRmod5:

$$LSBR \bmod 5(X) = \arg\min_{Y \bmod 5 - M} |X - Y|,$$

де X, Y – значення пікселів, $X, Y \in [0, 255]$, M – секретне повідомлення в бітах.

Навчання та аналіз передбачають вилучення характерних наборів особливостей на основі кореляційних зв'язків та блокових пеатернів LDP, LFP (в статті наведені результати для трьох наборів, які

позначені як Set F1, Set F2 та SPAM). На основі проведеного огляду в табл. 2–7 зібрані результати виявлення вкладень, вбудованих стеганографічними методами S-UNIWARD, WOW, HUGO, MiPOD, Hill та LSB. В таблицях 2, 3, 5, 7 також наведені результати досліджень [43] розробленого автором стеганоаналітичного алгоритму Color Triads* [44], позначення * зазначає, що алгоритм не використовує в своїй основі нейронні мережі. Порівняння цього алгоритму з аналогами, що базуються на згорткових нейронних мережах або глибокому навчанні, обумовлено отриманими високими значеннями у якості виявлення вбудованих повідомлень. Жирним в табл. 2–7 позначені кращі результати детектування серед стеганоаналітичних методів, побудованих на основі нейронних мереж. Жирним з курсивом – результати стеганоаналізу Color Triads, якщо вони перевищують інші методи.

Таблиця 2 – Точність детектування стеганоповідомлень, сформованих алгоритмом S-UNIWARD, %

Стеганоаналітичний метод	**Payload, bpp**					
	0,5	**0,4**	**0,3**	**0,2**	**0,1**	**0,05**
HSDetect-Net (2025) [24]	94,22	89,36	83,32	81,87	66,78	–
TCSI-ECA-Transfer (2023) [20]	–	–	–	**91,60**	**84,00**	**74,20**
Net from [32] (2023)	–	93,10	–	79,30	–	–
Net from [26] (2023)	96,60	**94,80**	86,20	81,60	68,80	49,80
OBS (2023) [28]	–	88,64	79,50	74,25	66,70	–
Net from [27] (2022)	–	90,58	**86,85**	80,98	69,87	–
AG-Net (2022) [30]	89,27	85,49	80,66	–	–	–
Shen-Net (2021) [21]	–	–	–	88,17	78,90	69,17
GBRAS-net (2021) [25]	–	77,90	–	73,60	–	–
SFR-Net (2021) [31]	–	89,60	–	75,50	–	–
Yedroudj-Net (2018) [22]	–	–	–	56,01	–	–
SCA-TLU-CNN (2017) [33]	–	87,19	–	77,76	67,80	60,00
Xu-Net (2016) [23]	–	–	–	60,94	53,82	50,55
Color Triads* (2022) [43]	–	***99,67***	–	***99,43***	***97,70***	***92,53***

Якщо розглядати стеганоаналіз методу S-UNIWARD, то більшість нейронних мереж добре працюють при виявленні вкладень, вбудованих з пропускною спроможністю 0,3–0,5 bpp, серед них

можна визначити мережу [26; 27] та HSDetect-Net [24], які забезпечують точність детектування на рівні 83–87 % для 0,3 bpp, 92–98 % для 0,4 bpp та 99 % для 0,5 bpp. Для меншої пропускної спроможності серед нейронних мереж кращою є TCSI-ECA-Transfer [20], яка з високою точністю (91,2 %) виявляє стеганоповідомлення, сформовані з пропускною здатністю 0,2 bpp та 0,1 bpp (84 %).

Таблиця 3 – Точність детектування стеганоповідомлень, сформованих алгоритмом WOW, %

Стеганоаналітичний метод	**Payload, bpp**					
	0,5	**0,4**	**0,3**	**0,2**	**0,1**	**0,05**
HSDetect-Net (2025) [24]	99,07	**98,99**	88,44	82,09	76,92	–
TCSI-ECA-Transfer (2023) [20]	–	–	–	89,00	**79,84**	**69,73**
Net from [32] (2023)	–	94,40	–	90,20	–	–
Net from [26] (2023)	**99,60**	98,60	**94,00**	**92,00**	76,00	52,20
Net from [27] (2022)	–	92,09	89,22	84,61	75,70	–
AG-Net (2022) [30]	85,82	83,62	79,57	–	–	–
Shen-Net (2021) [21]	–	–	–	85,49	74,05	63,90
GBRAS-net (2021) [25]	–	89,80	–	80,30	–	–
SFR-Net (2021) [31]	–	87,90	–	76,80	–	–
Yedroudj-Net (2018) [22]	–	–	–	51,20	–	–
SCA-TLU-CNN (2017) [33]	–	90,41	–	83,09	75,58	65,50
Xu-Net (2016) [23]	–	–	–	65,43	55,86	50,76
Color Triads* (2022) [43]	–	***99,51***	–	***99,35***	***97,87***	***94,09***

Для виявлення стеганоповідомлень, сформованих стеганоаналітичним методом WOW з пропускною спроможністю 0,2–0,5 bpp, гарну точність детектування (більше 92 % для заданих значень payload) надає мережа [26], непогані результати спостерігаються також для мережі HSDetect-Net [24], особливо при значеннях payload 0,3–0,5 bpp: точність виявлення заповнених зображень і пустих контейнерів перевищує 88 %. Також можна відзначити мережу [32], що за умови пропускної здатності 0,2 bpp забезпечує 90,2 % точно виявлених стеганоповідомлень і незаповнених контейнерів. З малою пропускною спроможністю 0,05–0,1 bpp впорається мережа TCSI-ECA-Transfer [20], однак все ж таки відсоток помилкових детектувань залишається значним (21 % та 31 % відповідно для 0,1 bpp та 0,05 bpp).

Таблиця 4 – Точність детектування стеганоповідомлень, сформованих алгоритмом HUGO, %

Стеганоаналітичний метод	Payload, bpp			
	0,4	**0,2**	**0,1**	**0,05**
TCSI-ECA-Transfer (2023) [20]	–	**89,15**	**79,30**	**69,19**
Shen-Net (2021) [21]	–	51,32	72,93	62,78
GBRAS-net (2021) [25]	**84,50**	74,60	–	–
SFR-Net (2021) [31]	83,60	75,40	–	–
Yedroudj-Net (2018) [22]	–	84,66	–	–
Xu-Net (2016) [23]	–	66,79	59,49	52,83

Менш поширеним для вбудовування додаткової інформації є стеганографічний алгоритм HUGO, і найкраще визначає наявність вкладень мережа TCSI-ECA-Transfer [20], і хоч для неї не проводились дослідження щодо пропускної спроможності 0,4 bpp, з урахуванням 89 % вірних класифікацій при 0,2 bpp, можна очікувати точність детектування не менше 92–93 %.

Таблиця 5 – Точність детектування стеганоповідомлень, сформованих алгоритмом MiPOD, %

Стеганоаналітичний метод	Payload, bpp					
	0,5	**0,4**	**0,3**	**0,2**	**0,1**	**0,05**
HSDetect-Net (2025) [24]	95,68	89,99	87,80	84,77	**78,90**	–
Net from [26] (2023)	**97,20**	**96,40**	**89,00**	**86,80**	70,90	50,60
GBRAS-net (2021) [25]	–	81,40	–	68,30	–	–
SFR-Net (2021) [31]	–	84,10	–	75,20	–	–
Color Triads* (2022) [43]	–	***99,59***	**–**	***99,09***	***95,41***	***92,69***

Стеганографічні алгоритми MiPOD та Hill реалізовані лише мовою математичного середовища MatLAB, чим обумовлено їх менше поширення, тим не менш нейронні мережі [26] та HSDetect-Net [24] непогано визначають наявність вкладень, вбудованих з пропускною спроможністю 0,2–0,5 bpp.

Найкращі результати детектування стеганографічних вкладень, вбудованих методом Hill, визначає нейронна мережа [27], точність детектування складає 86 % для пропускної спроможності 0,4 bpp, очікуване значення *Acc* для 0,5 bpp має перевищувати 90 %.

Таблиця 6 – Точність детектування стеганоповідомлень, сформованих алгоритмом Hill, %

Стеганоаналітичний метод	Payload, bpp				
	0,5	**0,4**	**0,3**	**0,2**	**0,1**
Net from [27] (2022)	–	**86,23**	**82,75**	**77,50**	68,61
AG-Net (2022) [30]	84,60	81,95	77,96	–	–
GBRAS-net (2021) [25]	–	81,90	–	68,50	–

Таблиця 7 – Точність детектування стеганоповідомлень, сформованих алгоритмом LSB, %

Стеганоаналітичний метод		Payload, bpp							
		0,5	**0,4**	**0,3**	**0,25**	**0,2**	**0,1**	**0,05**	**0,01**
B0 [40] (2019)		–	–	–	–	83,10	81,60	78,50	62,90
ns-B0 [41] (2021)		–	–	–	–	88,60	88,60	86,60	**78,00**
ns/r-B0 [42] (2019)		–	–	–	–	91,80	89,80	86,80	73,40
[38] (2024)	AVG	–	–	–	–	91,50	81,60	76,40	57,10
	KB	–	–	–	–	98,90	95,30	87,00	61,90
	U-Net	–	–	–	–	**99,70**	**97,70**	**90,60**	64,20
[39] (2024)	Set F1	87,19	83,29	78,39	75,25	70,49	54,44	–	–
	Set F2	86,8	83,71	80,01	76,50	72,25	57,69	–	–
	SPAM	86,24	78,35	72,50	68,98	63,92	40,05	–	–
Color Triads* (2022) [43]		***100***	***100***	***100***	***100***	***100***	***99,9***	***95,9***	–

З таблиці 7 видно, що найкращий з нейромережевих стеганоаналітичних методів [38] у варіації U-Net забезпечує високу якість виявлення вбудованих повідомлень навіть за умови малих значень прихованої пропускної спроможності (для значень *payload* 0,2, 0,1 та 0,05 bpp досягається точність 99,7 %, 97,9 % та 90,6 % відповідно. Також статті [38, 40–42] приділяють увагу пропускній здатності 0,01 bpp, для якої найкращий результат детектування отриманий алгоритмом ns-B0 [41] і становить 78 % вірно класифікованих стеганоповідомлень та незаповнених контейнерів.

Щодо стеганоалгоритму Color Triads для значень *payload* 0,05–0,5 bpp досягаються максимальні значення точності детектування, які перевищують 95 % вірно класифікованих ЦЗ.

Щодо стеганоаналізу Color Triads слід зазначити важливу його особливість: він може приймати на вхід лише кольорові ЦЗ, представлені колірною схемою RGB. Алгоритм Color Triads побудований так, що для визначення прихованого повідомлення, яке може бути вбудовано в одну, дві або всі три колірні складові [45], аналізується кількість Red-, Green- та Blue-тріад, що утворюються послідовними групами колірних триплетів, тобто кольорів, які описуються схемою (*R*, *G*, *B*), де *R* – яскравість червоної колірної складової, *G* – яскравість зеленої колірної складової, *B* – яскравість синьої колірної складової. Наведені в таблицях 2, 3, 5 і 7 результати детектування ЦЗ властиві випадку заповнення однієї довільної колірної складової, притому досягається висока точність виявлення повідомлень навіть за малих значень пропускної здатності (значення *Acc* не менше 92 % навіть при *payload*=0,05 bpp). Методи, побудовані на основі нейронних мереж, аналізують зображення в градаціях сірого, а тому також здатні виявляти вкладення в кольорових контейнерах, аналізуючи кожну колірну складову незалежно від інших.

Серед стеганографічних методів, що вбудовують додаткову інформацію в область перетворень ЦЗ можна відзначити J-UNIWARD [46], nsF5 [47], UED [48], UERD [49] та PQ [29], зокрема вони використовуються дослідниками при розробці і тестуванні методів виявлення прихованих повідомлень.

При стеганоаналізі ЦЗ в форматі JPEG окрім пропускної спроможності також враховується якісь стиснення результуючих зображень (Quality Factor, QF), найчастіше розглядають значення QF, що дорівнюють 75 та 95.

В роботі [50] автори пропонують нейронну мережу, побудовану за структурою SRNet, причому до характеристичних ознак додаються додаткові, які базуються на стратегії редукції, включаючи max, min и mean, об'єднання яких може створювати додаткові ознаки, зокрема max_mean, min_mean, max_min та max_min_mean. Експериментальні дослідження проводились для чотирьох алгоритмів J-UNIWARD [46], nsF5 [47], UED [48], UERD [49] при значеннях *payload* 0,1–0,4 bpp та значеннях QF 75 та 95. Також в статті наводиться порівняння з мережею SRNet [51], яка стала основою для удосконалення поточного методу, та [52].

У статті [53] запропонований стеганоаналітичний метод, в основі якого відокремлення низькочастотної складової ЦЗ на основі вейвлет-перетворення, для якої за допомогою глибокої згорткової нейронної мережі вилучаються ознаки вмісту зображення. На попередньому етапі отримані характеристики кластеризуються для отримання міток відповідного класу, після чого стеганоаналітична мережа навчається окремо за допомогою зразків в кожному підкласі. В роботі наведені результати експериментів для стеганографічного методу J-UNIWARD [46] при значеннях *payload* 0,1–0,4 bpp та значенні $QF = 75$.

Робота [54] пропонує для стеганоаналізу схему автоматичного зіставлення розподілів, що базується на консенсусної кластеризації CADM. Наводяться результати досліджень при виявленні стеганографічних вкладень методами J-UNIWARD [46], nsF5 [47], UERD [49] та J-MiPOD [55] за умови пропускної здатності 0,2–0,3 bpp. Зокрема точність виявлення вкладень, сформованих алгоритмом J-MiPOD [55] при $QF = 75$ та 0,2 bpp складає 94,3 % та 87,2 % відповідно для 0,3 bpp та 0,2 bpp.

Стаття [56] пропонує стеганоаналітичний алгоритм виявлення вкладень, вбудованих стеганографічними методами J-UNIWARD [46] та UED [48] при $QF = 75$ та 95, а також пропускної спроможності 0,1–0,5 bpp. Стеганоаналіз базується на навчанні нейронної мережі з урахуванням графа, який попереджує глобальну втрату ознак через локальне навчання ознак згортковою нейронною мережею, та модуля покращення ознак, який запобігає ослабленню стеганографічної інформації через накладання згорткових шарів. Це дозволяє знизити кількість помилкових класифікацій, зокрема при пропускній здатності 0,5 bpp спостерігається лише 1,05 % та 6,23 % помилок виявлення вкладень стеганоалгоритмом UED та 4,42 % та 10,83 % помилок виявлення вкладень стеганоалгоритмом J-UNIWARD відповідно при $QF = 75$ та $QF = 95$.

У вищезгаданих роботах [27; 28] наводяться результати експериментів для запропонованих стеганоаналітичних мереж: в [27] на основі стеганографії J-UNIWARD [46] та UED [48], в [28] на основі стеганографії nsF5 [47] та PQ [29], дослідження яких були проведені для $QF = 75$, зокрема точність стеганоаналізу PQ-алгоритму

становить 55,45 %, 60,45 %, 67,04 % та 73,18 % для значень payload 0,1 bpp, 0,2 bpp, 0,3 bpp, 0,4 bpp відповідно. В статті [27] також наведено порівняння точності детектування з [51, 57, 58].

На основі описаних вище стеганоаналітичних методів та наведених в публікаціях порівняння з аналогами, сформовано узагальнені табл. 8–11, які містять точність детектування стеганоповідомлень, отриманих вбудовуванням додаткової інформації стеганографічними алгоритмами J-UNIWARD [46], nsF5 [47], UED [48], UERD [49]. Жирним в таблицях 8–11 позначені кращі результати детектування серед наведених стеганоаналітичних методів.

Таблиця 8 – Точність детектування стеганоповідомлень, сформованих алгоритмом J-UNIWARD, %

Стегано-аналітичний метод	Payload, bpp							
	0,4		0,3		0,2		0,1	
	QF 75	QF 95	QF 75	QF 95	QF 75	QF 95	QF 75	QF 95
[51] (2018)	92,71	81,19	88,43	74,10	80,94	65,13	67,65	55,76
[52] (2019)	–	–	–	–	–	–	56,20	59,60
[57] (2019)	92,05	80,87	87,18	73,48	79,11	65,57	67,14	55,84
[58] (2019)	91,61	77,41	85,40	69,47	77,66	61,79	64,20	54,98
[27] (2022)	**93,18**	81,09	89,08	73,92	81,89	65,71	67,88	57,03
[50] (2023)	90,75	79,05	85,20	69,53	76,60	62,27	66,40	56,49
[53] (2023)	85,56	–	79,70	–	71,39	–	61,13	–
[54] (2023)	–	–	72,40	69,50	–	–	–	–
[56] (2023)	90,99	**84,05**	**89,51**	**76,13**	**85,08**	**69,50**	**69,86**	59,79

Порівнюючи результати класифікації і відокремлення стеганоповідомлень від незаповнених контейнерів, можна спостерігати, що незалежно від стеганографічного методу кращі значення точності детектування характерні для якості стиснення $QF = 75$, тобто чим вище якість збережених заповнених зображень, тим складнішим буде стеганоаналіз.

За результатами аналізу стеганографічного алгоритму J-UNIWARD [46] (табл. 8) можна відзначити нейронні мережі [27; 51; 57], які мають порівняний відсоток вірно класифікованих зображень.

Однак найкраща ефективність досягається методом [56], результати якого перевищують аналоги майже за всіма випадками, окрім $QF = 75$ при 0,4 bpp, де кращим виявився метод [27], який за цих умов досягає значення 93,18 %.

Таблиця 9 – Точність детектування стеганоповідомлень, сформованих алгоритмом UED, %

Стегано-аналітичний метод	Payload, bpp							
	0,4		0,3		0,2		0,1	
	QF 75	QF 95	QF 75	QF 95	QF 75	QF 95	QF 75	QF 95
[51] (2018)	98,16	92,12	**97,14**	87,63	94,12	80,34	86,77	69,69
[52] (2019)	–	–	–	–	–	–	57,75	59,50
[57] (2019)	98,20	**92,22**	97,11	87,99	94,21	80,70	87,22	70,46
[58] (2019)	97,97	89,90	96,27	84,75	92,76	76,64	83,52	65,35
[27] (2022)	**98,34**	91,87	96,97	87,21	**94,71**	79,95	**88,16**	69,91
[50] (2023)	96,63	90,65	95,50	83,65	91,88	75,82	85,53	65,55
[56] (2023)	94,79	91,96	92,72	**88,78**	89,97	**81,85**	82,61	70,50

Застосування стеганоаналізу проти UED-стеганографії [48] (табл. 9) є більш ефективним при застосуванні нейромереж [51; 57; 27; 56], трохи відстають за показниками методи [50; 58], причому при збереженні стеганоповідомлень з якістю $QF = 75$ краще визначає наявність вбудованої інформації мережа [27], особливо при значеннях пропускної здатності 0,1 та 0,2 bpp (88,16 % та 94,71 % відповідно).

У випадку якості $QF = 95$ найбільш ефективним при значеннях *payload* 0,1, 0,2, 0,3 bpp є [56], де точність виявлення складає 70,5 %, 81,85 % та 88,78 % відповідно.

За умови більш високої пропускної спроможності прихованого каналу зв'язку можна відзначити методи [51] (97,14 % при $QF = 75$, 0,3 bpp), [57] (92,22 % при $QF = 95$, 0,4 bpp) та [27] (98,34 % при $QF = 75$, 0,4 bpp).

При виявленні стеганоповідомлень, сформованих методом nsF5 [47] (табл. 10) фаворитом є нейронна мережа [50], причому якість детектування зображень, збережених з QF=95 навіть трохи перевищує якість $QF = 75$, де різниця у точності детектування при однакових значеннях пропускної здатності не перевищує 1,25 %.

Таблиця 10 – Точність детектування стеганоповідомлень, сформованих алгоритмом nsF5, %

Стегано-аналітичний метод	Payload, bpp							
	0,4		0,3		0,2		0,1	
	QF 75	QF 95	QF 75	QF 95	QF 75	QF 95	QF 75	QF 95
[51] (2018)	85,62	82,79	76,25	72,50	67,68	63,96	55,35	52,59
[52] (2019)	–	–	–	–	–	–	58	57,15
NOBS [28] (2023)	82,75	–	73,50	–	66,20	–	58,72	–
[50] (2023)	**97,12**	**98,37**	**92,63**	**93,55**	**82,98**	**83,40**	**68,72**	**68,95**
[54] (2023)	–	–	–	–	81,40	76,90	–	–

Таблиця 11 – Точність детектування стеганоповідомлень, сформованих алгоритмом UERD, %

Стегано-аналітичний метод	Payload, bpp							
	0,4		0,3		0,2		0,1	
	QF 75	QF 95	QF 75	QF 95	QF 75	QF 95	QF 75	QF 95
[51] (2018)	80,87	75,15	79,19	71,94	75,28	66,71	62,63	57,76
[50] (2023)	**96,32**	**88,68**	**93,48**	83,55	**88,41**	75,82	**80,27**	**67,55**
[54] (2023)	–	–	92,90	**93,80**	79,20	**79,30**	–	–

Також нейронна мережа [50] добре зарекомендувала себе при виявленні вкладень на основі UERD-стеганографії [49] (табл. 11), однак за умови $QF = 95$ при значеннях *payload* 0,2 та 0,3 bpp точність методу [54] перевищує і складає 79,3 % та 93,8 % відповідно.

Висновки. Отже, проведений огляд сучасних методів стеганографічного аналізу показав, що все більшого поширення набувають нейронні мережі, побудовані на основі згорткової структури та глибокого навчання з виявленням численних ознак ЦЗ як на основі просторової області, так і в області перетворень на основі низьких, середніх та високих частот зображення.

Розглянуті мережі забезпечують високу ефективність виявлення вкладень за умови пропускної спроможності прихованого каналу зв'язку 0,4–0,5 bpp, однак за менших значеннях пропускної

здатності результати залишають бажати кращого. Особливо цей факт підтверджує порівняння алгоритму Color Triads [43] з аналогами, що працюють в просторовій області, який використовує в своїй основі лише три подібні характеристики, а саме кількість Red-, Green- та Blue-тріад, за якими визначається факт наявності вкладень. Отже точність детектування цього алгоритму свідчить про те, що точковий аналіз може дати набагато вищі результати, ніж навчання на основі великої кількості характеристичних ознак.

При цьому розвиток стеганоаналізу не припиняється, оскільки постійно з'являються нові методи стеганографії, спрямовані на ускладнення процесу виявлення вкладень, в сучасних дослідженнях автори охоплюють все більший спектр стеганографічних алгоритмів при урахуванні малих значень пропускної спроможності прихованого каналу зв'язку, що особливо актуально, оскільки саме такі вкладення набагато складніше.

Дослідники удосконалюють структуру нейронних мереж, комбінуючи різні функції та елементи аналізу і вилучення характеристичних ознак, що вносить значний вклад в посилення інформаційної безпеки та захисту інформації.

Список використаних джерел

1. J. Mielikainen. LSB matching revisited. *Signal Processing Letters, IEEE*. 2006. Vol. 13. P. 285–287.

2. Muhammad K., Sajjad M., Mehmood, I. A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. *Multimed Tools Appl*. 2016. No. 75. P. 14867–14893. DOI: https://doi.org/10.1007/s11042-015-2671-9

3. Soukaena H. Hashem, Eman Taleb Zghaer. Review Study among Traditional LSB, Proposed Modified LSB and DWT Steganography Algorith. *Al-Mansour Journal*. 2017. Issue (27). P. 37–56.

4. Rahman S., Uddin J., Hussain H. et al. A novel and efficient digital image steganography technique using least significant bit substitution. *Scientific Reports*. 2025. Vol. 15, Is. 107. DOI: https://doi.org/10.1038/s41598-024-83147-3

5. Wu D. C., Tsai W. H. A Steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*. 2003. Vol. 24. P. 1613–1626.

6. Da-Chun Wu, Zong-Nan Shih. Image Steganography by Pixel-Value Differencing Using General Quantization Ranges. *Computer Modeling in Engineering & Sciences*. August 2024. Vol. 141 (1). P. 1–10. DOI: 10.32604/cmes.2024.050813

7. Monalisa Sahu, Neelamadhab Padhy, Sasanko Sekhar Gantayat. Multi-directional PVD steganography avoiding PDH and boundary issue. *Journal of King Saud University – Computer and Information Sciences*. November 2022. Vol. 34 (10), Part A. P. 8838–8851. DOI: https://doi.org/10.1016/j.jksuci.2021.10.007

8. Filler T., Fridrich J. Gibbs Construction in Steganography. *IEEE Transactions on Information Forensics and Security*. 2010. Vol. 4 (5). P. 705–720.

9. Holub V., Fridrich J. Designing Steganographic Distortion Using Directional Filters. In: *2012 IEEE International Workshop on Information Forensics and Security* (WIFS 2012). IEEE, Tenerife, Canary Islands, 2012. P. 1–6.

10. Holub V., Fridrich J., Denemark T. Universal Distortion Function for Steganography in an Arbitrary Domain. *EURASIP Journal on Information Security* (Section: SI: Revised Selected Papers of ACM IH and MMS 2013). 2014. P. 1–13.

11. Sedighi V., Cogranne R., Fridrich J. Content-Adaptive Steganography by Minimizing Statistical Detectability. *IEEE Transactions on Information Forensics and Security*. 2016. Vol. 11, Is. 2. P. 221–234.

12. Shuliang Sun, Yongning Guo. A Novel Image Steganography Based on Contourlet Transform and Hill Cipher. *Journal of Information Hiding and Multimedia Signal Processing*. 2015. Vol. 6 (5). P. 889–897.

13. Steganographic Algorithms. DDE Lab at Binghamton University. [Electronic resource]. URL: https://dde.binghamton.edu/download/stego_algorithms/

14. Khalaf Ashraf A. M., Fouad, Osama, Hussein Aziza, Hamed, Hesham, Kelash Hamdy, Ali, Hanafy. Hiding data in images using DCT steganography techniques with compression algorithms. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2019. Vol. 17 (3). P. 1168–1175. DOI: 10.12928/telkomnika.v17i3.

15. Ritonga Ramadani, Rosnelly Rika, Wanayumini, Wanayumini. Implementation of SLT-DCT Steganography Method on Images

to Improve the Quality of Steganography Images. *Proceeding of International Conference on Science and Technology UISU*. 2024. P. 264–271. DOI: 10.30743/qad1k130.

16. Tamer Rabie, Mohammed Baziyad, Ibrahim Kamel. High-Fidelity Steganography: A Covert Parity Bit Model-Based Approach. *Algorithms*. 2024. Vol. 17 (8). P. 328. DOI: https://doi.org/10.3390/a17080328

17. Tian Wu, Xuan Hu, Chunnian Liu, Yizhe Wang, Yiping Zhu. An efficient steganography scheme based on wavelet transformation for side-information estimation. Journal of King Saud University – Computer and Information Sciences. July 2024. Vol. 36, Is. 6, 102109. P. 1–12. https://doi.org/10.1016/j.jksuci.2024.102109

18. Alobaidi T., Mikhael W. An adaptive steganography insertion technique based on wavelet transform. *Journal of Engineering and Applied Science*. 2023. Vol. 70, P. 144. DOI: https://doi.org/10.1186/s44147-023-00300-x

19. Yujie Jiang, Jing Dong, Shutiao Luo. Robust Generative Image Steganography based on Frequency Domain using Fourier Transform. *BDICN '25: Proceedings of the 2025 4th International Conference on Big Data, Information and Computer Network*. 2025. P. 290–295. DOI: https://doi.org/10.1145/3727353.3727402

20. Shouyue Liu, Chunying Zhang, Liya Wang, Pengchao Yang, Shaona Hua, Tong Zhang. Image Steganalysis of Low Embedding Rate Based on the Attention Mechanism and Transfer Learning. *Electronics*. 2023. Vol. 12. P. 969. DOI: https://doi.org/10.3390/electronics12040969

21. Shen J., Liao X., Qin Z., Liu X.-C. Spatial Steganalysis of Low Embedding Rate Based on Convolutional Neural Network. *J. Softw.* 2021. Vol. 32. P. 2901–2915.

22. Yedroudj M., Comby F., Chaumont M. Yedroudj-net: An efficient CNN for spatial steganalysis. In Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, Canada, 15–20 April 2018. P. 2092–2096.

23. Xu G., Wu H., Shi Y. Structural design of convolutional neural networks for steganalysis. IEEE Signal Process. *Lett*. 2016. Vol. 23. P. 708–712. DOI: https://doi.org/10.1109/LSP.2016.2548421

24. Ntivuguruzwa Jean De La Croix, Tohari Ahmad, Fengling Han, Royyana Muslim Ijtihadie. HSDetect-Net: A Fuzzy-Based Deep

Learning Steganalysis Framework to Detect Possible Hidden Data in Digital Images. *IEEE Access*. 2025. Vol. 13. P. 43013–43027. DOI: 10.1109/ACCESS.2025.3546510

25. Reinel T.-S., Brayan A. H., Alejandro B. M., Alejandro M.-R., Daniel A.-G., Alejandro A. J., B. A. Buenaventura, Simon O.-A., Gustavo I., Raúl R.-P. GBRAS-net: A convolutional neural network architecture for spatial image steganalysis. *IEEE Access.* 2021. Vol. 9. P. 14340–14350. DOI: 10.1109/ACCESS.2021.3052494

26. Croix N. J. D. L., Ahmad T., Han F. Enhancing secret data detection using convolutional neural networks with fuzzy edge detection. *IEEE Access.* 2023. Vol. 11. P. 131001–131016. DOI: 10.1109/ACCESS.2023.3334650

27. Deng X.-Q., Chen B.-L., Luo W.-Q., Luo D.. Universal image steganalysis based on convolutional neural network with global covariance pooling. *J. Comput. Sci. Technol.*, 2022. Vol. 37 (5). P. 1134–1145. DOI: 10.1007/s11390-021-0572-0

28. Sabeti V. An improved approach to blind image steganalysis using an overlapping blocks idea. *J. Electr. Comput. Eng. Innovations*. 2023. Vol. 11 (2). P. 563–276. DOI: 10.22061/jecei.2022.9241.592

29. Fridrich J., Goljan M., Soukal D. Perturbed quantization steganography. *ACM Multimedia System Journal*, 2005. Vol. 11 (2). P. 98–107.

30. Zhang H., Liu F., Song Z., Zhang X., Zhao Y. AG-Net: An advanced general CNN model for steganalysis. *IEEE Access*. 2022. Vol. 10. P. 44116–44122.

31. Xu G., Xu Y., Zhang S., Xie X. SFRNet: Feature extraction-fusion steganalysis network based on squeeze-and-excitation block and RepVgg Block. *Secur. Commun. Networks*. 2021. P. 1–10.

32. Jean De La Croix Ntivuguruzwa, Tohari Ahmad. A convolutional neural network to detect possible hidden data in spatial domain images. *Cybersecurity*. 2023. Vol. 6 (23). DOI: https://doi.org/10.1186/s42400-023-00156-x

33. Jian Ye, Jiangqun Ni, Yang Yi. Deep Learning Hierarchical Representations for Image Steganalysis. *IEEE Transactions on Information Forensics and Security*. 2017. Vol. 12 (11). P. 2545–2557.

34. Mielikainen J. LSB matching revisited. *Signal Processing Letters, IEEE*. 2006. Vol. 13. P. 285–287.

35. Muhammad K., Sajjad M., Mehmood I. A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. *Multimed Tools Appl.* 2016. Vol. 75. P. 14867–14893. DOI: https://doi.org/10.1007/s11042-015-2671-9

36. Soukaena H. Hashem, Eman Taleb Zghaer. Review Study among Traditional LSB, Proposed Modified LSB and DWT Steganography Algorith. *Al-Mansour Journal.* 2017. Vol. 27. P. 37–56.

37. Marwa M. Emam, Abdelmgeid A. Aly, Fatma A. Omara. A Modified Image Steganography Method based on LSB Technique. International Journal of Computer Applications (0975 – 8887). September 2015. Vol. 125 (5). P. 12–17.

38. Martin Beneš, Rainer Böhme. Exploring Diffusion-Inspired Pixel Predictors for WS Steganalysis. In *Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '24)*, June 24–26, 2024, Baiona, Spain. P. 75–86. DOI: https://doi.org/10.1145/3658664.3659645

39. Veena Sivasamy Thanasekaran, Arivazhagan Selvaraj. Low Dimensional Multi Class Steganalysis of Spatial LSB based Stego Images Using Textural Features. *The International Arab Journal of Information Technology.* March 2024. Vol. 21 (2). P. 233–242. DOI: https://doi.org/10.34028/iajit/21/2/6

40. Mingxing Tan, Quoc Le. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. In *International Conference on Machine Learning (ICML)*. 2019. PMLR, P. 6105–6114.

41. Yassine Yousfi, Jan Butora, Jessica Fridrich, Clément Fuji Tsang. Improving Efficient-Net for JPEG Steganalysis. *In Workshop on Information Hiding and Multimedia Security (IH&MMSec)*. 2021. ACM, P. 149–157.

42. Mo Chen, Mehdi Boroumand, Jessica Fridrich. Reference Channels for Steganalysis of Images with Convolutional Neural Networks. *In Workshop onbInformation Hiding and Multimedia Security (IH&MMSec)*. 2019. ACM, P. 188–197.

43. Akhmametieva H. Universal approach to the identification of steganographic transformation of the spatial domain of digital images.

International Science Journal of Engineering & Agriculture. 2022. Vol. 1 (3). P. 133–142.

44. Anna Akhmametieva. Steganalysis of digital contents, based on the analysis of unique color triplets. *Annales Mathematicae et Informaticae*. 2017. Vol. 47. P. 3–18.

45. Akhmametieva A. V., Bwabwa M. C. Steganalysis of Digital Images under Different Content Fullness. *Telecommunications and Radio Engineering*. 2019. Vol. 78. P. 671–681. DOI: 10.1615/TelecomRadEng.v78.i8.30

46. Holub V., Fridrich J., Denemark T. Universal Distortion Function for Steganography in an Arbitrary Domain. *EURASIP Journal on Information Security* (Section:SI: Revised Selected Papers of ACM IH and MMS 2013). 2014 (1). P. 1–13.

47. Fridrich, J. Pevný T., Kodovský J. Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities. In J. Dittmann and J. Fridrich, editors, *Proceedings of the 9th ACM Multimedia & Security Workshop*, Dallas, TX, September 20–21, 2007. P. 3–14.

48. L. Guo, J. Ni, Y. Q. Shi. Uniform embedding for efficient JPEG steganography. *IEEE Transactions on Information Forensics and Security*. 2014. Vol. 9 (5). P. 814–825.

49. Guo L., Ni J., Su W., Tang C., Shi Y. Q. Using statistical image model for JPEG steganography: Uniform embedding revisited. *IEEE Transactions on Information Forensics and Security.* 2015. Vol. 10 (12). P. 2669–2680.

50. Yuchen Li, Baohong Ling, Donghui Hu, Shuli Zheng, Guoan Zhang. A Deep Learning Driven Feature Based Steganalysis Approach**.** *Intelligent Automation & Soft Computing*. 2023. Vol. 37 (2). P. 2213–2225. DOI: 10.32604/iasc.2023.029983

51. Boroumand M., Chen M., Fridrich J. Deep residual network for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*. 2019. Vol. 14 (5). P. 1181–1193.

52. Xue Y., Yang L., Wen J., Niu S., Zhong P. A subspace learning-based method for JPEG mismatched steganalysis. *Multimedia Tools and Applications*. 2019. Vol. 78 (7). P. 8151–8166.

53. Mo Chengyu, Liu Fenlin, Zhu Ma, Yan Gengcong, Qi Baojun, Yang Chunfang. Image Steganalysis Based on Deep Content Features

Clustering. *Computers, Materials and Continua*. 2023. Vol. 76 (3). P. 2921–2936. DOI: https://doi.org/10.32604/cmc.2023.039540

54. Ju Jia, Meng Luo, Siqi Ma, Lina Wang, Yang Liu. Consensus-Clustering-Based Automatic Distribution Matching for Cross-Domain Image Steganalysis. *IEEE Transactions on Knowledge and Data Engineering*. June 2023. Vol. 35 (6). P. 5665–5679.

55. Cogranne R., Giboulot Q., Bas P. Steganography by minimizing statistical detectability: The cases of JPEG and color images. *In Proc. Workshop Informat. Hiding Multimedia Secur*. 2020. P. 161–167.

56. Qiyun Liu, Zhiguang Yang, Hanzhou Wu. JPEG Steganalysis Based on Steganographic Feature Enhancement and Graph Attention Learning. *Journal of Electronic Imaging.* 2023. P. 1–10. DOI: https://doi.org/10.48550/arXiv.2302.02276

57. Huang J., Ni J., Wan L., Yan J. A customized convolutional neural network with low model complexity for JPEG steganalysis. In Proc. the ACM Workshop on Information Hiding and Multimedia Security, July 2019. P. 198–203. DOI: 10.1145/3335203.3335734

58. Deng X., Chen B., Luo W., Luo D. Fast and effective global covariance pooling network for image steganalysis. In Proc. the ACM Workshop on Information Hiding and Multimedia Security, July 2019, P. 230–234. DOI: 10.1145/3335203.3335739