забезпечують порівняно з відомими аналогами підвищення стійкості цифрового підписування, а також спрощення процедури перевірки підпису, що особливо важливо для клієнт-серверних задач.

Література: ***1.*** *Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. – CRC Press, 2001. – 816 p.* ***2.*** *Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. – М.: Горячая линия–Телеком, 2007. – 320 с.* ***3.*** *Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф, 2002. - 816 с.* ***4.*** *Романец Ю. В., Тимофеева П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.* ***5.*** *Введение в криптографию / Под общ. ред. В. Б. Ященко. – М.: МЦНМО: «ЧеРо», 2000. – 236 с.* ***6.*** *Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.* ***7.*** *Брассар Ж. Современная криптология. – М.: ПОЛИМЕД, 1999. – 176 с.* ***8.*** *Simmons G. J., Authentication theory/coding theory // Proc. CRYPTO'84, Lect. Notes in Comput. Sci. – V. 196, 1985. – Pp. 411–431.* ***9.*** *Яремчук Ю. Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем // Захист інформації. – № 4, 2012. – С. 120–127.* ***10.*** *Яремчук Ю.Є. Розробка алгоритмів прискореного обчислення елементів рекурентних послідовностей для криптографічних застосувань // Реєстрація, зберігання і обробка даних. – Т. 15, № 1, 2013. – С. 14–22.* ***11.*** *Яремчук Ю. Є. Метод автентифікації сторін взаємодії на основі рекурентних послідовностей // Сучасний захист інформації. – № 1, 2013. – С. 4–10.* ***12.*** *Маркушевич А. И. Возвратные последовательности. – М.: Наука, 1975. – 48 с.* ***13.*** *Кнут Д. Искусство программирования для ЭВМ, том 2. Получисленные алгоритмы. – М.: Вильямс, 2004. – 832 с.*

УДК: 004.056.5

ОЦІНЮВАННЯ СТІЙКОСТІ МЕТОДУ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНІ ЗОБРАЖЕННЯ ДО АКТИВНИХ ТА ПАСИВНИХ АТАК

Василь Карпінець, Юрій Яремчук, Кирило Безпалий
Вінницький національний технічний університет

Анотація: **Проведено аналіз стійкості методу вбудовування цифрових водяних знаків (ЦВЗ) у векторні зображення до активних та пасивних зловмисних атак, спрямованих на зчитування та ускладнення витягнення ЦВЗ правовласником. Для цього були розглянуті поширені атаки на основі афінних перетворень зображення, атака шляхом внесення додаткового шуму, а також пасивна атака для визначення місця розташування ЦВЗ. Результати аналізу показали високий рівень стійкості методу до цих атак завдяки особливостям вбудовування ЦВЗ і використаного двовимірного дискретного косинусного перетворення.**

Summary: **This paper analyzes the stability of the method of embedding digital watermarks (digital watermark) in vector images for active and passive malicious attacks aimed at reading and complications extract digital watermark owner. This was considered common attacks based on affine transformations of the image, the attack by introducing additional noise, and passive attack is to determine the location of digital watermark. The analysis showed a high level of resistance to this attack method by digital watermark embedding features and used two-dimensional discrete cosine transform.**

Ключові слова: **Стеганографія, цифровий водяний знак, захист авторського права, векторні зображення, стеганографічна стійкість.**

І Вступ

Задача захисту авторського права векторних зображень на сьогодні стає все більш актуальною. Особливу увагу привертають такі методи забезпечення захисту, для яких не потрібно наявності оригіналу для підтвердження авторства. На сьогодні запропоновано декілька таких методів вбудовування цифрових водяних знаків (ЦВЗ) у векторні зображення [1]. Проте недоліком таких методів є можливі значні спотворення зображення внаслідок вбудовування ЦВЗ. У роботі [2] запропоновано метод, який забезпечує збереження високого рівня якості зображення при вбудовуванні ЦВЗ [3].

Однак, актуальним залишається питання аналізу запропонованого методу щодо забезпечення стійкості до зловмисних атак. У роботах [4] та [5] було проведено дослідження стеганографічної стійкості методу до відомих активних і пасивних атак, спрямованих на зчитування, видалення або підміну ЦВЗ, а також на ускладнення витягування правовласником ЦВЗ шляхом додавання шуму, видалення/додавання точок

векторного зображення або геометричних перетворень векторних зображень. Проведено аналіз на теоретичному рівні, який показав достатньо високий рівень стійкості запропонованого методу до таких атак. При цьому актуальним залишається експериментальне оцінювання стійкості до активних та пасивних зловмисних атак на прикладах конкретних векторних зображень, ЦВЗ та різних значень параметрів методу.

II Дослідження стійкості запропонованого методу до активних та пасивних атак

Стійкість будь-якої системи вбудовування ЦВЗ полягає у можливості правильного розпізнавання самого ЦВЗ після навмисних спотворень. Для оцінювання стійкості запропонованого методу до зловмисних атак основним показником буде помилка розпізнавання бітів ЦВЗ, яка визначається як відношення неправильно розпізнаних біт ЦВЗ до розміру ЦВЗ.

Для аналізу стійкості запропонованого методу проведемо вбудовування ЦВЗ розміром 768 бітів у векторну карту, фрагмент якої показано на рис. 1. Після цього будемо її змінювати, імітуючи найпоширеніші зловмисні атаки.

Рисунок 1 – Фрагмент векторної географічної карти для вбудовування ЦВЗ

Проаналізуємо стійкість методу до атаки шляхом *повороту векторного зображення.* При цьому будемо визначати правильність розпізнавання бітів ЦВЗ після повороту векторної карти на різні кути за формулою:

$$[X',Y'] = [X,Y] \cdot \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}, \quad (1)$$

де X', Y' та X, Y – відповідно координати точок повернутого та оригінального зображення; α – кут повороту точок зображення.

Оскільки згідно з методом [3] для різних значень параметра відбору придатних матриць P_h можуть відповідати різні придатні матриці коефіцієнтів дискретного косинусного перетворення (ДКП) для вбудовування, їм будуть відповідати різні точки векторного зображення, зміна яких може по-різному вплинути на правильність розпізнавання бітів ЦВЗ. Тому для дослідження візьмемо декілька різних значень P_h, при яких кількість придатних матриць ДКП є достатньою.

Значення параметра P також впливає на спотворення зображення, тому ймовірно може впливати на правильність розпізнавання бітів ЦВЗ. Проте параметр P не впливає на визначення придатних матриць ДКП і є значно меншим від P_h, тому для дослідження параметр P оберемо таким, щоб був достатнім для відновлення 100 % бітів ЦВЗ у випадку оригінальної карти для кожного значення P_h. Після вбудовування ЦВЗ та повороту карти на різні кути отримаємо результати розпізнавання бітів ЦВЗ, які наведено в табл. 1.

Таблиця 1 – Результати розпізнавання бітів ЦВЗ після повороту векторної карти

Поворот, град	P_h = 0.005, P = 0.00004			P_h = 0.01, P = 0.0004			P_h = 0.0008, P = 0.00003		
	Правильно	Неправильно	Помилка, %	Правильно	Неправильно	Помилка, %	Правильно	Неправильно	Помилка, %
1	753	15	1,95	762	6	0,78	752	16	2,08

5	665	103	13,41	474	294	38,28	329	439	57,16
10	652	116	15,10	168	600	78,13	357	411	53,52
15	644	124	16,15	465	303	39,45	389	379	49,35
20	493	275	35,81	480	288	37,50	402	366	47,66
25	493	275	35,81	488	280	36,46	403	365	47,53
30	261	507	66,02	502	266	34,64	373	395	51,43
35	294	474	61,72	531	237	30,86	376	392	51,04
40	280	488	63,54	517	251	32,68	418	350	45,57
45	404	364	47,40	207	561	73,05	337	431	56,12
50	464	304	39,58	618	150	19,53	358	410	53,39
55	297	471	61,33	633	135	17,58	321	447	58,20
60	453	315	41,02	645	123	16,02	377	391	50,91
65	455	313	40,76	461	307	39,97	369	399	51,95
70	316	452	58,85	448	320	41,67	385	383	49,87
75	446	322	41,93	438	330	42,97	401	367	47,79
80	144	624	81,25	425	343	44,66	391	377	49,09
85	140	628	81,77	408	360	46,88	524	244	31,77
90	384	384	50,00	384	384	50,00	386	382	49,74

З табл. 1 видно, що помилка розпізнавання, в основному, зростає зі збільшенням кута повороту зображення. При цьому для різних P_h помилка розпізнавання є різною і змінюється не пропорційно до кута повороту.

Для кращого представлення результатів побудуємо графік залежності помилки розпізнавання бітів ЦВЗ від кута повороту для різних P_h та P, який показано на рис. 2.

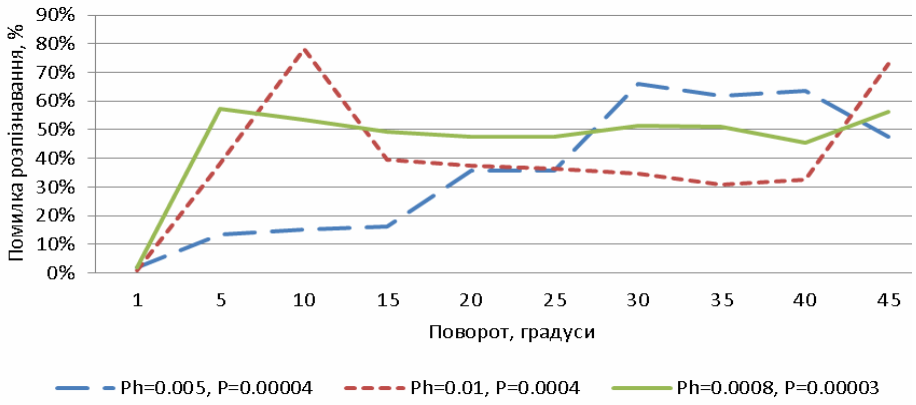

Рисунок 2 – Графік залежностей похибок розпізнавання бітів ЦВЗ від кута повороту векторної карти

На рис. 2 видно, що найменша похибка розпізнавання (до 16 %) при повороті до 15 градусів спостерігається для карти, в яку було вбудовано ЦВЗ при $P_h = 0{,}005$. При цьому похибка розпізнавання найменша при повороті зображення більше ніж на 20 градусів при $P_h = 0{,}01$. Такі результати показують пряму залежність похибки розпізнавання бітів ЦВЗ від вибраного значення P_h при вбудовуванні.

Зважаючи на те, що поворот зображення більше ніж на 15 градусів для більшості зображень буде явно помітним, а також може призвести до явного спотворення зображення, значення $P_h = 0{,}005$ в цьому випадку є оптимальним, враховуючи те, що воно також впливає на рівень спотворення векторного зображення.

З таких результатів можна зробити висновок, що запропонований метод є достатньо стійким до зловмисних атак через поворот векторного зображення.

Для проведення аналізу стійкості методу до *масштабування векторного зображення* також будемо визначати помилку розпізнавання бітів ЦВЗ після масштабування зображення.

Спочатку проаналізуємо стійкість запропонованого методу після збільшення в масштабі векторної карти. Масштабування векторної карти будемо проводити за формулою:

$$[X', Y'] = [X, Y] \cdot \begin{bmatrix} Kx & 0 \\ 0 & Ky \end{bmatrix}, \quad (2)$$

де Kx , Ky – масштабні коефіцієнти.

Згідно з формулою (2) для збільшення зображення коефіцієнти Kx , Ky мають бути більшими за 1 і для пропорційного масштабування рівні між собою.

Для аналізу візьмемо значення масштабних коефіцієнтів з діапазону $Kx = Ky$ = 1,01...2, що відповідають збільшенню зображення від 1 до 100 % відносно оригіналу. Результати проведеного аналізу показані в табл. 2.

Таблиця 2 – Результати розпізнавання бітів ЦВЗ після масштабування (збільшення) векторної карти

Масштаб		P_h= 0,005, P = 0,00004			P_h = 0,01, P = 0,0004			P_h = 0,0008, P = 0,00003		
Збільшення	Kx , Ky	Правильно	Неправильно	Помилка, %	Правильно	Неправильно	Помилка, %	Правильно	Неправильно	Помилка, %
1	1,01	767	1	0,13	768	0	0,00	767	1	0,13
2	1,02	502	266	34,64	768	0	0,00	438	330	42,97
3	1,03	502	266	34,64	768	0	0,00	59	709	92,32
4	1,04	502	266	34,64	608	160	20,83	59	709	92,32
5	1,05	163	605	78,78	608	160	20,83	58	710	92,45
10	1,1	258	510	66,41	610	158	20,57	285	483	62,89
20	1,2	254	514	66,93	279	489	63,67	445	323	42,06
30	1,3	360	408	53,13	279	489	63,67	321	447	58,20
40	1,4	337	431	56,12	240	528	68,75	370	398	51,82
50	1,5	393	375	48,83	588	180	23,44	334	434	56,51
60	1,6	331	437	56,90	265	503	65,49	450	318	41,41
70	1,7	452	316	41,15	264	504	65,63	341	427	55,60
80	1,8	401	367	47,79	250	518	67,45	412	356	46,35
90	1,9	300	468	60,94	287	481	62,63	372	396	51,56
100	2	368	400	52,08	288	480	62,50	414	354	46,09

З табл. 2 видно, що при масштабуванні зображення виникає помилка розпізнавання бітів ЦВЗ. При цьому для різних значень P_h і P вона є різною.

Для кращого представлення результатів побудуємо графік залежності помилки розпізнавання бітів ЦВЗ від коефіцієнта масштабування зображення для різних P_h та P , який показано на рис. 3.

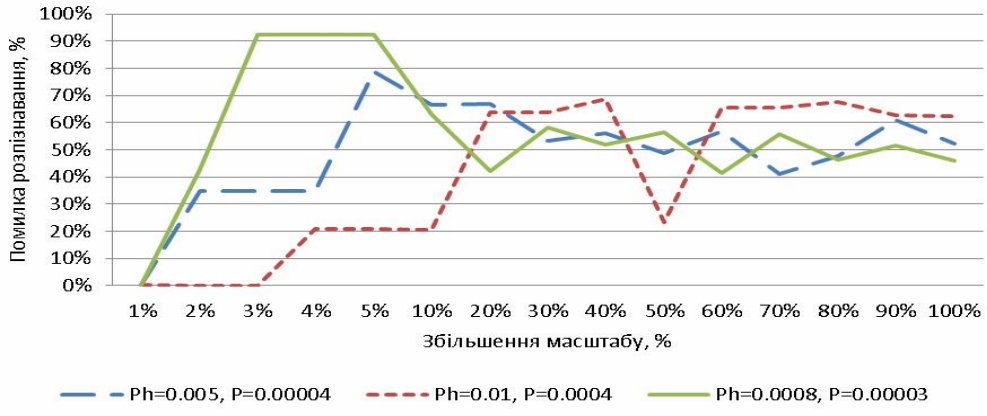

Рисунок 3 – Графік залежності помилки розпізнавання бітів ЦВЗ від рівня масштабування зображення

На рис. 3 видно, що при $P_h = 0{,}01$ при збільшенні масштабу до 3 % помилка розпізнавання бітів рівна 0, що забезпечує розпізнавання усіх бітів ЦВЗ. В цілому, при збільшенні масштабу зображення на 100 %, тобто у два рази, помилка розпізнавання бітів для різних значень P_h та P в середньому не перевищує 55 %. Це свідчить про те, що половину бітів ЦВЗ можна розпізнати при значних перетвореннях зображення.

Оскільки масштабування зображення передбачає і зменшення розміру, проаналізуємо стійкість запропонованого методу до такого перетворення.

Масштабування векторної карти будемо проводити за формулою (2), згідно з якою для зменшення зображення коефіцієнти Kx, Ky мають бути меншими за 1 і для пропорційного масштабування рівня між собою.

Для аналізу візьмемо значення масштабних коефіцієнтів з діапазону $Kx = Ky = 0{,}5...0{,}99$, що відповідають зменшенню зображення від 1 до 50 % відносно оригіналу (табл. 3).

Таблиця 3 – Результати розпізнавання бітів ЦВЗ після масштабування (зменшення) векторної карти

Масштаб		$P_h = 0{,}005$, $P = 0.00004$			$P_h = 0{,}01$, $P = 0{,}0004$			$P_h = 0{,}0008$, $P = 0{,}00003$		
Зменшення	Kx, Ky	Правильно	Неправильно	Помилка, %	Правильно	Неправильно	Помилка, %	Правильно	Неправильно	Помилка, %
–1	0,99	768	0	0,00	768	0	0,00	397	371	48,31
–2	0,98	768	0	0,00	768	0	0,00	230	538	70,05
–3	0,97	768	0	0,00	440	328	42,71	331	437	56,90
–4	0,96	768	0	0,00	441	327	42,58	587	181	23,57
–5	0,95	768	0	0,00	441	327	42,58	413	355	46,22
–10	0,9	414	354	46,09	440	328	42,71	460	308	40,10
–20	0,8	393	375	48,83	712	56	7,29	396	372	48,44
–30	0,7	302	466	60,68	371	397	51,69	356	412	53,65
–40	0,6	452	316	41,15	675	93	12,11	400	368	47,92
–50	0,5	542	226	29,43	676	92	11,98	386	382	49,74

З табл. 3 видно, що при різних значеннях рівня масштабування виникають різні помилки розпізнавання бітів ЦВЗ. При цьому для однакових значень масштабних коефіцієнтів помилка розпізнавання є різною для векторних карт з вбудованим ЦВЗ з різними значеннями P_h і P.

Для кращого представлення результатів побудуємо графік залежності помилки розпізнавання бітів ЦВЗ від коефіцієнта масштабування зображення для різних P_h та P, який показано на рис. 4.

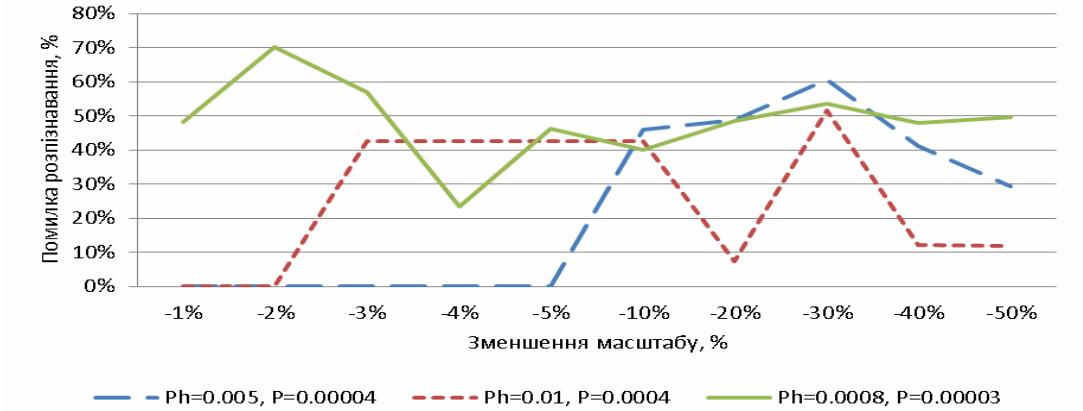

Рисунок 4 – Графік залежності помилки розпізнавання бітів ЦВЗ від рівня масштабування зображення

На рис. 4 видно, що при $P_h = 0{,}005$ та зменшенні масштабу до 5 % помилка розпізнавання бітів рівна 0, що забезпечує розпізнавання усіх бітів ЦВЗ. При цьому при зменшенні зображення у 2 рази помилка розпізнавання приблизно рівна 30 %, тобто 70 % відсотків бітів ЦВЗ можна відновити.

Ще однією з найпоширеніших активних зловмисних атак є *внесення додатково шуму* в зображення з метою ускладнення розпізнавання бітів ЦВЗ.

Для аналізу стійкості запропонованого методу до такого типу атаки потрібно штучно промоделювати дії зловмисника. Фактично метою зловмисника є зміна значень коефіцієнтів матриць ДКП з вбудованими бітами ЦВЗ таким чином, щоб при витягуванні ЦВЗ вони не відповідали умовам придатності матриць та/або неправильно відповідали формулі розпізнавання бітів.

Згідно з методом параметр P_h визначає матриці для вбудовування бітів ЦВЗ і є секретною інформацією, що має бути невідомою зловмиснику. Також частиною секретного ключа можуть бути позиції ВЧ-коефіцієнтів, що беруть участь у вбудовуванні бітів ЦВЗ. Якщо зловмисник не володіє цими даними, він не може визначити, які саме точки векторного зображення або відповідні їм коефіцієнти містять ЦВЗ.

В такому випадку зловмисник може додати шум в зображення шляхом зміни значень координат точок або відповідних їм коефіцієнтів ДКП.

Для моделювання такої атаки будемо вносити додатковий шум у векторну карту з вбудованим ЦВЗ шляхом зміни координат усіх його точок на певну величину. Для того, щоб краще уявити рівень внесеного шуму, будемо змінювати значення координат точок шляхом зміни відповідних їм коефіцієнтів ДКП. Оскільки стійкість до такої атаки теоретично залежить від параметрів P_h та P, то для визначення та представлення рівня величини шуму найкраще скористатися одним з цих параметрів, наприклад, P_h.

В роботі [5] зазначено, що запропонований метод абсолютно стійкий до атаки через зміщення зображення, яке забезпечується збільшенням або зменшенням усіх координат точок на певне значення. Тому для більшої правдоподібності такої атаки будемо змінювати усі коефіцієнти ДКП шляхом додавання або віднімання псевдовипадкової величини з певного діапазону $\{0..k_n \cdot P\}$, де k_n – коефіцієнт, який визначає рівень додаткового шуму. Таким чином ми забезпечимо додавання нерівномірного шуму по всьому зображенні.

Дослідження будемо проводити з точки зору правильності розпізнавання бітів ЦВЗ після зміни векторної карти шляхом додавання шуму різного рівня. Основним показником будемо вважати помилку розпізнавання бітів ЦВЗ. При цьому будемо визначати рівень спотворень, які буде спричиняти така атака. Для цього визначимо сумарну похибку та максимальне відхилення координат точок векторної карти.

Для аналізу візьмемо векторну карту (рис. 1), ЦВЗ розміром 768 бітів, $P = 0{,}00003$, $P_h = 0{,}003$. Для k_n оберемо діапазон $\{0...100\}$.

Після проведення внесення додаткового шуму різного рівня отримаємо результати експерименту, які показано в табл. 4

Таблиця 4 – Результати розпізнавання бітів ЦВЗ після внесення додаткового шуму

k_n	Сумарна похибка	Максимальне відхилення	Відновлено	Неправильно	Помилка, %
0	1,26448	0,00057	768	0	0,00
0,1	1,26535	0,00057	768	0	0,00
0,2	1,30683	0,00058	762	6	0,78
0,3	1,36118	0,00058	758	10	1,30
0,4	1,40712	0,00058	759	9	1,17
0,5	1,45309	0,00059	753	15	1,95
0,6	1,50081	0,00059	735	33	4,30
0,7	1,54551	0,00059	743	25	3,26
0,8	1,59128	0,00059	713	55	7,16
0,9	1,64333	0,00059	724	44	5,73
1	1,69167	0,0006	705	63	8,20
2	2,22244	0,00063	646	122	15,89
3	2,79076	0,00072	600	168	21,88
4	3,37877	0,00074	591	177	23,05
5	3,98173	0,00076	557	211	27,47
6	4,61449	0,00073	562	206	26,82
7	5,25861	0,00077	548	220	28,65

8	5,89809	0,00084	536	232	30,21
9	6,57405	0,00086	530	238	30,99
10	7,1982	0,00094	511	257	33,46
100	68,04526	0,00763	216	552	71,88

З результатів табл. 4 видно, що збільшення значення k_n, тобто рівня додаткового шуму, прямопропорційно впливає на збільшення сумарної похибки відхилення координат точок. Для кращого представлення побудуємо графік залежності сумарної похибки відхилення координат точок від рівня шуму, який показано на рис. 5.

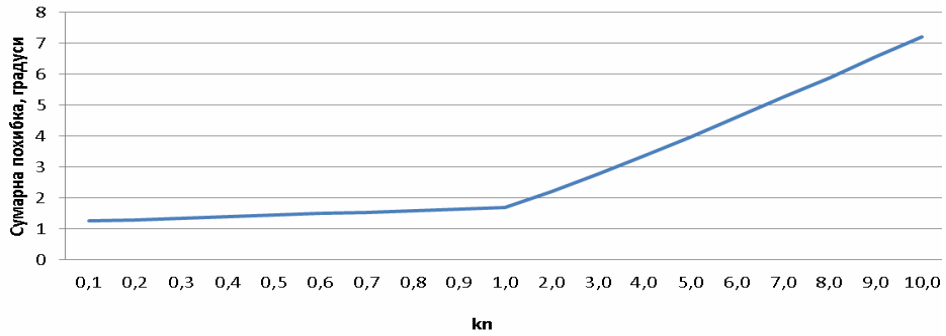

Рисунок 5 – Графік залежності сумарної похибки відхилення координат точок від рівня шуму

На рис. 5 видно, що при $k_n > 1$ сумарна похибка починає суттєво збільшуватись відносно початкового значення. Наприклад, при $k_n = 3$ сумарна похибка відхилення координат точок є більшою від початкового значення при $k_n = 0$ більше ніж у 2 рази, що може призвести до видимої деградації зображення. При цьому величина помилки розпізнавання бітів складає всього 22 %. Навіть при $k_n = 10$, коли сумарна похибка є більшою від початкового значення у 5,7 разів і збільшення максимального відхилення точок майже у 2 рази, що призведе до повної деградації зображення, помилка розпізнавання бітів ЦВЗ складає 33,46 %.

Як видно з табл. 4, помилка розпізнавання бітів ЦВЗ теж залежить від рівня додаткового шуму. На рис. 6 показано графік залежності помилок розпізнавання бітів ЦВЗ від рівня шуму.

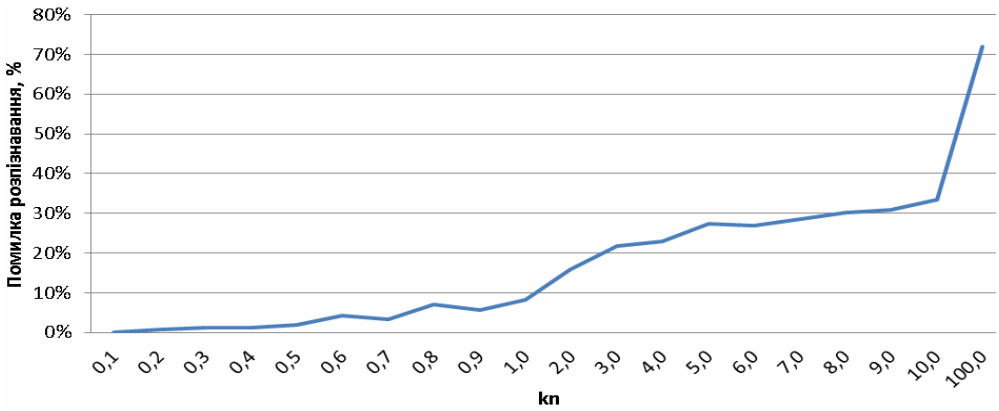

Рисунок 6 – Графік залежності помилок розпізнавання бітів ЦВЗ від рівня шуму

На рис. 6 видно, що помилка розпізнавання бітів також збільшується при збільшенні рівня шуму, хоча збільшення не таке прямолінійне, як у випадку сумарної похибки. Це пояснюється тим, що запропонований метод може забезпечити правильне розпізнавання бітів ЦВЗ при зміні значень трьох коефіцієнтів матриць ДКП, що беруть участь у вбудовування бітів ЦВЗ на певну величину. Тобто збільшення рівня шуму може не вплинути на ознаку придатності матриці при витягуванні ЦВЗ, а також на правильність розпізнавання вбудованого в неї біта ЦВЗ.

З табл. 4 та на рис. 6 також видно випадки, коли при збільшенні рівня шуму помилка розпізнавання бітів ЦВЗ зменшується. Це пояснюється тим, що величина додаткового шуму для кожної матриці ДКП є не

константою, а псевдовипадковим числом з діапазону $\{0..k_n \cdot P\}$. Тому в цьому випадку навіть для однакового значення величини шуму кожного разу ми можемо отримати різні результати.

Отже, виходячи з результатів табл. 4 та рис. 5 – 6 можна сказати, що запропонований метод є достатньо стійким до внесення додаткового шуму.

Окрім активних атак, важливим є оцінювання стійкості запропонованого методу *до пасивних атак, спрямованих на визначення місця розташування ЦВЗ* для їх подальшого зчитування, підміни чи видалення.

В загальному випадку стійкість існуючих стеганографічних методів вбудовування ЦВЗ до такого роду атак забезпечується вбудовуванням ЦВЗ тільки у певні місця зображення. Для цього використовується ключ, який і визначає місця розташування бітів ЦВЗ. Виходячи з цього, стійкість методів до таких атак визначається кількістю можливих варіантів місць розташування ЦВЗ, які потрібно перевірити зловмиснику для того, щоб визначити де вбудовано ЦВЗ.

Згідно із запропонованим методом вбудовування бітів ЦВЗ проводиться лише у визначені матриці ДКП, тобто стійкість, в першу чергу, забезпечується як і у відомих методів. Крім цього зловмисник може шукати місце розташування ЦВЗ через параметр P_h, який визначає ті матриці, в які можуть бути вбудовані біти ЦВЗ. Але, оскільки розмір ЦВЗ може бути меншим від кількості придатних матриць ДКП, який згідно з методом невідомий зловмиснику, то для визначення місць розташування бітів ЦВЗ зловмиснику необхідно буде перевіряти усі можливі варіанти.

Виходячи з цього, визначимо максимально можливу кількість комбінацій матриць ДКП, в які можуть бути вбудовані біти ЦВЗ. Для цього використаємо формулу для визначення комбінацій без повторень C_t^q, яка дорівнює відомому біноміальному коефіцієнту [6]. Для запропонованого методу вона матиме такий вигляд:

$$C_t^q = \frac{t!}{(t-q)!\,q!} = \binom{t}{q}, \tag{3}$$

де t – кількість матриць ДКП; q – кількість бітів ЦВЗ.

Вираз (3) визначає кількість можливих комбінацій розміщення бітів ЦВЗ для певного значення кількості бітів ЦВЗ q. Оскільки значення q невідоме зловмиснику, для перебору діапазону усіх можливих q потрібно визначити суму усіх C_t^q для кожного значення q в діапазоні від 0 до t.

Позначимо кількість комбінацій без повторень для матриць ДКП як $C_{матр.}$ та використаємо одну з тотожностей для біноміального коефіцієнта [6]:

$$C_{матр.} = \sum_{q=0}^{t} \frac{t!}{(t-q)!\,q!} = \sum_{q=0}^{t} \binom{t}{q} = 2^t. \tag{4}$$

З виразу (4) видно, що кількість комбінацій матриць ДКП з вбудованими бітами ЦВЗ залежить від кількості матриць ДКП, а її збільшення підпорядковується експоненціальному закону.

Згідно з виразом (4) кількість комбінацій обчислюється для діапазону $q = 0...t$. Однак слід зазначити, що для запропонованого методу при вбудовуванні ЦВЗ розміром з цього діапазону не завжди буде забезпечуватись достатня стійкість до виявлення місця його розташування. Це пояснюється тим, що згідно з формулою (3) у випадку, коли q приймає граничне значення діапазону, наприклад, при $q = 0$ та $q = t$, кількість комбінацій $C_{матр.} = 1$, тобто стійкість для таких випадків буде низькою. При цьому максимальна стійкість буде забезпечуватись тоді, коли розмір ЦВЗ q буде дорівнювати половині усіх матриць ДКП, тобто при $q = t/2$.

Виходячи з цього, для забезпечення достатнього рівня стійкості запропонованого методу пропонується вибирати ЦВЗ з дещо вужчого діапазону, при якому кожному значенню q буде відповідати достатня кількість комбінацій матриць ДКП $C_{матр.}$, наприклад, $q = \frac{1}{4}t...\frac{3}{4}t$.

Сумарна кількість комбінацій матриць ДКП з вбудованими бітами ЦВЗ для такого діапазону буде визначатись таким чином:

$$C_{матр.} = \sum_{q=t/4}^{\frac{3}{4}t} \frac{t!}{(t-q)!\ q!}. \quad (5)$$

Також слід зазначити, що окрім матриць ДКП та розміру ЦВЗ зловмиснику невідомі позиції трьох коефіцієнтів ВЧ-діапазону в матрицях ДКП, що створює додаткову складність при визначенні місць розташування ЦВЗ та забезпечує вищу стійкість запропонованого методу.

Для визначення кількості комбінацій трьох коефіцієнтів $C_{коеф.}$ з ВЧ-діапазону для матриць ДКП також скористаємось формулою (3). До ВЧ-діапазону відносять 21 коефіцієнт з 64, тому кількість комбінацій трьох ВЧ-коефіцієнтів для кожної матриці ДКП буде дорівнювати

$$C_{коеф.} = \frac{21!}{(21-3)!\ 3!} = 1330.$$

Отже, враховуючи додаткову складність для зловмисника завдяки невідомим позиціям ВЧ-коефіцієнтів, загальна кількість комбінацій розміщення бітів ЦВЗ у зображенні $C_{метод}$ для діапазону $q = \frac{1}{4}t...\frac{3}{4}t$ буде визначатись таким чином:

$$C_{метод} = \sum_{q=t/4}^{\frac{3}{4}t} \frac{t!}{(t-q)!\ q!} \cdot 1330. \quad (6)$$

Для кращого представлення стійкості запропонованого методу виконаємо обчислення кількості комбінацій позицій розміщення бітів ЦВЗ, які потрібно проаналізувати зловмиснику для визначення місця розташування ЦВЗ для випадку типової векторної карти з середніми рівнем деталізації, кількістю точок та розміром.

Для прикладу візьмемо типову географічну векторну карту одного з міст України з 64 000 точок та розміром файла – 1,5 Мб. При цьому кількість матриць ДКП буде $t = 1000$.

Для кращого розуміння впливу діапазону значень q на загальну кількість комбінацій $C_{метод}$ для запропонованого методу виконаємо обчислення для максимального діапазону $q = 0...t$ та для рекомендованого $q = \frac{1}{4}t...\frac{3}{4}t$. В результаті отримаємо:

$$C_{метод.} = \sum_{q=0}^{t} \frac{t!}{(t-q)!\ q!} \cdot 1330 = 1{,}42 \cdot 10^{304} \approx 2^{1010} \text{ , при } q = 0...t;$$

$$C_{метод} = \sum_{q=\frac{t}{4}}^{\frac{3}{4}t} \frac{t!}{(t-q)!\ q!} \cdot 1330 = 1{,}42 \cdot 10^{304} \approx 2^{1010} \text{ , при } q = \frac{1}{4}t...\frac{3}{4}t.$$

Отримані результати показують достатньо велику кількість комбінацій розміщення бітів ЦВЗ, які потрібно перевірити зловмиснику для виявлення місця розташування ЦВЗ, що забезпечує достатній рівень стійкості запропонованого методу для карти з вказаними параметрами. Також слід зазначити, що запропонований діапазон значень q для розміру ЦВЗ незначно зменшує кількість варіантів розміщення бітів ЦВЗ у зображенні порівняно з загальною кількістю (для розглянутого прикладу різниця складає 2^{816}, що у $2{,}45 \cdot 10^{55}$ разів менше від загальної кількості операцій 2^{1010}).

Таким чином, результати оцінювання показали, що запропонований метод забезпечує достатній рівень стійкості до атак, спрямованих на визначення місця розташування ЦВЗ.

III Висновки

В роботі проведено аналіз стійкості запропонованого методу до активних зловмисних атак, спрямованих на ускладнення витягнення ЦВЗ правовласником, зокрема до атак на основі афінних перетворень та атаки внесенням шуму. Метод забезпечує достатньо високий рівень стійкості до повороту та масштабування зображення, зокрема при повороті зображення на 15 градусів похибка розпізнавання становить до 16 %

неправильно розпізнаних бітів, а при масштабуванні зображення на 3 % і 100 % помилка розпізнавання становить 0 % та 55 % бітів відповідно.

Аналіз стійкості запропонованого методу до атаки шляхом внесення додаткового шуму показав, що при внесенні шуму такого рівня, при якому сумарна похибка відхилень координат є більшою від початкової у 5,7 разів, що призводить до повної деградації зображення, помилка розпізнавання становить усього 33,46 % неправильно розпізнаних бітів.

Проведено оцінювання стійкості запропонованого методу до пасивних атак, спрямованих на визначення місця розташування ЦВЗ. Результати оцінювання показали забезпечення достатнього рівня стійкості, наприклад, для типової векторної географічної карти, яка складається з 64 тис. точок розміром близько 1,5 Мб, кількість комбінацій розміщення бітів ЦВЗ становить приблизно 2^{1010}.

Література: ***1.*** *Zheng L. Research on Vector Map Digital Watermarking Technology / L. Zheng, Y. Jia, Q. Wang. // First International Workshop on Education Technology and Computer Science – 2009. – P. 303 – 307.* ***2.*** *Карпінець В. В. Зменшення відхилень координат точок внаслідок вбудовування цифрових водяних знаків у векторні зображення / В. В. Карпінець, Ю. Є. Яремчук // Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні – 2010. – № 2(21). – С.101 – 109.* ***3.*** *Карпінець В. В. Аналіз впливу цифрових водяних знаків на якість векторних зображень / В. В. Карпінець, Ю. Є. Яремчук // Сучасний захист інформації. – 2011. – №1. – С.72 – 82 .* ***4.*** *Карпінець В. В. Дослідження стеганографічної стійкості методу вбудовування цифрових водяних знаків у векторні зображення / В. В. Карпінець, Ю. Є. Яремчук // ВІСНИК Вінницького політехнічного інституту. – 2011. - №3. – С. 200-205.* ***5.*** *Карпінець В. В. Аналіз стійкості методу вбудовування цифрових водяних знаків у векторні зображення до зловмисних атак / В. В. Карпінець, Ю. Є. Яремчук // ВІСНИК Вінницького політехнічного інституту. – 2011. - №4. – С. 154-159.* ***6.*** *Холл М. Комбинаторика / М. Холл // Издательство «МИР». Москва. — 1970. 424 с.*

УДК 512

РЕКУРЕНТНІ АЛГОРИТМИ ОБЧИСЛЕННЯ КОРЕНЯ ДОВІЛЬНОГО СТЕПЕНЮ У КІЛЬЦІ ЛИШКІВ

Людмила Ковальчук, Олексій Беспалов, Павло Огнєв
Физико-технічний інститут НТУУ "КПІ"

Аннотация: **Побудовано поліноміальні рекурентні алгоритми добування кореню довільного степеню у кільці лишків.**
Annotation: **Polynomial algorithms are constructed for obtaining the roots of arbitrary powers in a residue ring.**
Ключові слова: **Кільця лишків, добування кореня, еліптичні криві.**

І Вступ

У даній роботі будуть побудовані алгоритми добування кореня кубічного та коренів вищих степенів у кільцях лишків.

Питання розв'язку степеневих рівнянь у кільцях лишків є цікавим як з точки зору власне теорії чисел, так і з точки зору її застосувань у криптології. В першу чергу у криптології застосовуються алгоритми розпізнавання квадратичності та добування квадратного кореня як за простим модулем, так і за складеним, що є добутком двох простих чисел. Слід зазначити, що такі алгоритми є повністю описаними (наприклад, у [1, 2]). Вони поліноміальні (у окремих випадках – імовірнісні). Ці алгоритми мають застосування як при побудові криптосистем (наприклад, криптосистема Блюма), так і при криптоаналізі (поліноміальна еквівалентність задачі добування кореня за складеним модулем та задачі факторизації), а також при побудові криптографічно сильних генераторів (наприклад, BBS).

Побудова зручних поліноміальних алгоритмів добування кубічного кореня та кореня більш високого степеню також є цікавою задачею теорії чисел, хоча й не такою прикладною, як добування квадратного кореня. Проте деякі застосування все ж таки можна навести. По-перше, як і у випадку з квадратним коренем, задача добування кореня (будь-якого степеню) за складеним модулем поліноміально еквівалентна задачі факторизації, тобто може використовуватись у криптоаналізі алгоритмів, що базуються на складності задачі факторизації. По-друге, задача добування саме кубічного кореня може мати застосування при побудові криптосистем на еліптичних кривих, що задані над кільцями лишків (за складеним модулем). На таких еліптичних кривих можна побудувати як RSA-подібні криптосистеми, так і Ель-Гамале-подібні.