МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ГО «АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ»

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Колективна монографія

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ГО «АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ»

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Колективна монографія

Київ
Європейський університет
2023

УДК [004.056(53+55):003(26+27)]+621.643.8
А 43

Рекомендовано до друку Вченою радою ПВНЗ «Європейський університет» (протокол № 3 від 28.09.2022)

Рецензенти:
В.А. Лахно – доктор технічних наук, професор
(Національний університет біоресурсів і природокористування України)
М.Г. Медведєв – доктор технічних наук, професор
(Таврійський національний університет імені В. І. Вернадського)
О.А. Чемерис – доктор технічних наук, старший науковий співробітник
(Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України)

А 43 Актуальні питання забезпечення кібербезпеки та захисту інформації: колективна монографія / за заг. наук. ред. А.М. Давиденко, Київ: Європейський університет, 2023. – 204 с.

ISBN 978-966-301-259-9

Монографія є результатом тривалих наукових досліджень і пошуків авторів у напрямі обґрунтування сучасних концепцій, моделей, механізмів, проблем та перспектив розвитку наукових засад забезпечення кібербезпеки та захисту інформації України та світу; узагальнено та висвітлено організаційно-технологічні аспекти функціонування та захисту об'єктів критичної інфраструктури; наведено теоретичні засади та розроблено практичні рекомендації щодо безпеки комп'ютерних мереж та інтернет ресурсів в умовах сучасних впливів; проаналізовано проблеми й обґрунтовано перспективи розвитку криптографічних та стеганографічних методів захисту інформації.

До монографії увійшли матеріали доповідей учасників VIII Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», що проходила 2-5 лютого 2022 року на базі «Едельвейс» Європейського університету.

УДК [004.056(53+55)::003(26+27)]+621.643.8

ISBN 978-966-301-259-9

ЗМІСТ

УДК 004.056.55:519.876.5

ОГЛЯД ОСНОВНИХ ЗАДАЧ, ЯКІ МОЖНА ВИРІШУВАТИ ЗА ДОПОМОГОЮ СТЕГАНОГРАФІЇ

Мартинюк Г.В.
к.т.н., доцент, доцент
кафедра засобів захисту інформації
Національний авіаційний університет
ganna.martyniuk@gmail.com

Мелешко Т.В.
старший викладач
кафедра засобів захисту інформації
Національний авіаційний університет
sorokunnet@ukr.net

Бичков В.В.
старший викладач
кафедра засобів захисту інформації
Національний авіаційний університет
volodymyr.bychkov@npp.nau.edu.ua

Анотація. У роботі наводяться особливості поширених методів стеганографії. Розглядаються вимоги до стеганосистем. Особлива увага приділяється основним задачам та областям застосування методів відкритої стеганографії.

Стеганографія – це наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі [1]. На відміну від криптографії, що приховує вміст секретного повідомлення, стеганографія приховує факт його існування. Як правило, повідомлення буде виглядати як щось інше, наприклад, як зображення, стаття, список покупок, аудіо- або відеофайл. Перевагою стеганографічних методів є те, що тільки цільові одержувачі стегоконтейнера можуть отримати приховане повідомлення [2]. Третя сторона не буде знати про наявність прихованих даних у повідомленні. Стеганографію зазвичай використовують разом із методами криптографії, в такий спосіб, доповнюючи її.

Перевага стеганографії над чистою криптографією у тому, що повідомлення не привертають до себе уваги. Криптографія захищає зміст повідомлення, а стеганографія захищає сам факт наявності будь-яких прихованих посилань.

Можливості стеганографії вражають. Так, наприклад, зміна у 1% оцифрованого звуку (частота дискретизації 44100 Гц, 8-бітний рівень відліку, стерео-режим) дозволяє приховати повідомлення у 10 Кбайт [1]. Причому, людина нічого не помітить при прослуховуванні.

Інтерес до стеганографії відродився в останнє десятиліття і був викликаний широким поширенням технологій мультимедіа, що цілком закономірно, беручи

до уваги проблеми, пов’язані із захистом інформації. Не менш важливим стала поява нових типів каналів передачі інформації, що в сукупності з першим фактором дало новий імпульс розвитку та удосконаленню стеганографії, сприяло виникненню нових стеганографічних методів, в основу яких були покладені особливості подання інформації в комп’ютерних файлах, обчислювальних мережах і т. д. Це, у свою чергу, дає можливість говорити про становлення нового напряму у сфері захисту інформації – комп’ютерної стеганографії.

Нижче наведено основні терміни стеганографії.

Стеганографія – це сукупність методів, з допомогою яких додаткова інформація вбудовується в основний, приховуючий об’єкт – контейнер, зі збереженням його належної якості [1].

Контейнер – це деяка інформація, або файл, в який можна вбудувати додаткову інформацію, що не призначена для використання сторонніми користувачами.

Належна якість контейнера після вбудовування – це збереження тих його основних характеристик, до зміни котрих чутливі органи відчуттів людини.

Типовими варіантами контейнерів є: нерухоме зображення, відеозаписи, потокове відео, аудіозаписи, змістовний друкований текст, Інтернет-протоколи, програмне забезпечення.

У більшості стеганосистем для вбудовування та витягнення повідомлень використовується ключ, що визначає секретний алгоритм, який визначає порядок внесення повідомлення в контейнер. За аналогією із криптографією, тип ключа спричиняє існування двох типів стеганосистем:

- з секретним ключем – використовується один ключ, що визначається до початку обміну стеганограмою або передається захищеним каналом;
- з відкритим ключем – для пакування та розпакування повідомлення використовуються різні ключі, які відрізняються таким чином, що за допомогою обчислень неможливо одержати один ключ із іншого, тому один із ключів (відкритий) може вільно передаватися по незахищеному каналу.

Ще одним розповсюдженим методом стеганографії є метод використання цифрових водяних знаків (ЦВДЗн). Цифрові водяні знаки забезпечують захист авторських прав на цифровий IP, який включає програмування, зображення, звукозаписи та відео. Цифрові водяні знаки не можна виявити неозброєним оком, але служать сигналами під час завантаження чи відтворення матеріалів, захищених авторським правом.

Найбільш надійні цифрові водяні знаки випадковим чином поширюють бітові дані в захищеному захищеним авторським правом матеріалі. Для досягнення оптимального ефекту цифрові водяні знаки повинні бути неперетворюваними та підтримувати зміни, включаючи скорочення алгоритму або переформатування файлів.

Процес вбудовування ЦВДЗн проілюстровано на рисунку 1.

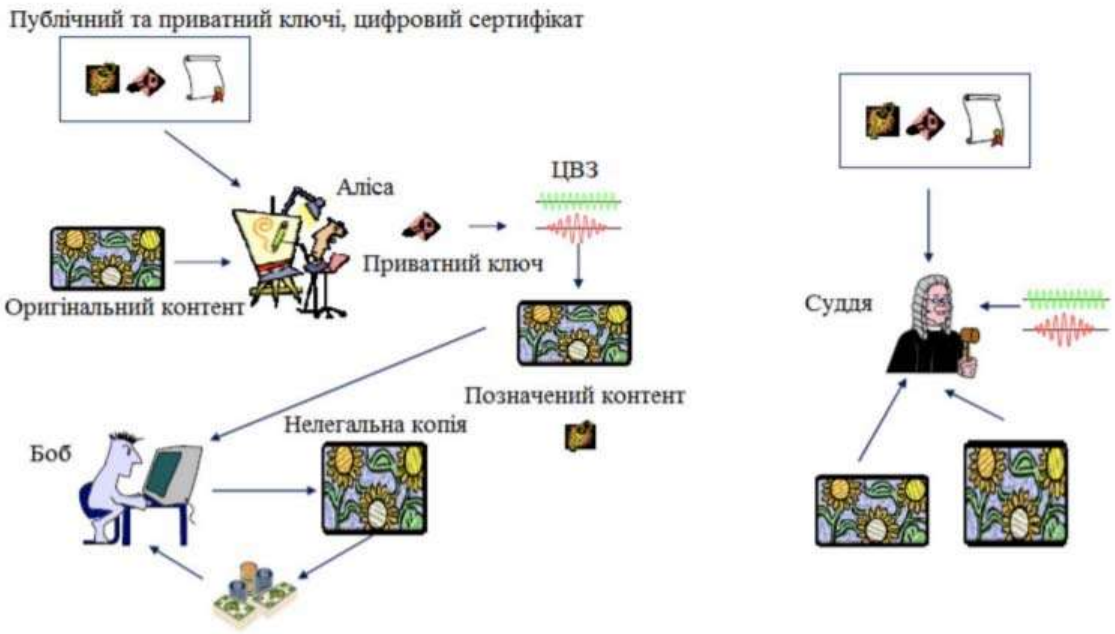

Рис. 1. Блок-схема процесу вбудовування ЦВДЗн
з метою захисту авторських прав.

Яким б різними не були напрями стеганографії, пропоновані ними вимоги багато в чому збігаються. Найбільш істотна відмінність постановки завдання прихованої передачі даних від постановки завдання вбудовування цифрового водяного знаку (ЦВДЗн) полягає в тому, що в першому випадку зловмисник повинен виявити приховане повідомлення, тоді як у другому випадку про його існування всі знають. Більше того, у зловмисника на законних підставах може бути пристрій виявлення ЦВДЗн.

Отже, у стеганосистемі відбувається об’єднання двох типів інформації таким чином, щоб вони по-різному сприймалися принципово різними детекторами. У якості одного з детекторів виступає система виділення прихованого повідомлення, у якості іншого – людина.

Алгоритм вбудовування повідомлення в найпростішому випадку складається із двох основних етапів:

- Вбудовування в стегакодері секретного повідомлення в контейнероригінал.
- Виявлення (виділення) у стеганодетекторі (декодері) прихованого зашифрованого повідомлення з контейнера-результату.

Виходячи із цього, слід розглянути математичну модель стеганосистеми. Процес тривіального стеганографічного перетворення описується залежностями:

$$E : C \times M \tag{1}$$

$$D : S \rightarrow M, \tag{1}$$

де $S = \{(c_1, m_1), (c_2, m_2), ..., (c_n, m_n), ..., (c_q, m_q)\} = \{s_1, s_2, ..., s_q\}$ – множина контейнерів-результатів (стеганограм).

Залежність (1) описує процес приховання інформації, залежність (1) – витягнення прихованої інформації. Необхідною умовою при цьому є відсутність "перетинання", тобто, якщо $m_a \neq m_b$, причому $m_a , m_b \in M$, а $(c_a , m_a),(c_b , m_b) \in S$, то $E(c_a , m_a) \cap E(c_b , m_b) = \varnothing$.

Крім того, необхідно, щоб потужність множини $|C| \geq |M|$. При цьому обидва адресати (відправник і одержувач) повинні знати алгоритм прямого (E) і зворотного (D) стеганографічних перетворень.

Отже, у загальному випадку стеганосистема – це сукупність $\Sigma = (C,M,S,E,D)$ контейнерів (оригіналів і результатів), повідомлень і перетворень, які їх пов'язують.

Для більшості стеганосистем множина контейнерів *C* вибирається таким чином, щоб у результаті стеганографічного перетворення (1) заповнений контейнер і контейнер-оригінал були подібні.

На сьогоднішній день існує велика кількість стеганографічних методів [1-5], проте, необхідно відмітити, що майже всі такі методи реалізовані тільки при використанні двох контейнерів: зображення та аудіосигналу.

Зображення чи аудіофайли вибирають в якості контейнера по ряду причин:

- великий обсяг цифрового представлення контейнера, що дозволяє приховувати повідомлення великого обсягу або підвищувати стійкість впровадження;
- наперед відомий розмір контейнера, відсутність обмежень, що накладаються вимогами реального часу;
- наявність у більшості реальних зображень текстурних областей, що мають шумову структуру і добре підходять для вбудовування інформації;
- слабка чутливість людського ока до незначних змін кольорів зображення чи незначних змін в аудіосигналі.

Нижче буде надано більш детальну інформацію про використання такого виду контейнерів.

Аудіосигнали. Для впровадження інформації в аудіосигнали, необхідно визначити вимоги, які можуть бути пред'явлені до стеганосистем, які застосовуються для вбудовування інформації в аудіосигнали:

- інформація, що приховується, повинна бути стійкою до наявності різних пофарбованих шумів, стиснення з втратами, фільтрування, аналоговоцифрового та цифро-аналогового перетворень;
- інформація, що приховується, не повинна вносити в сигнал спотворення, що сприймаються системою слуху людини;
- спроба видалення інформації, що приховується, повинна призводити до помітного пошкодження контейнера (для ЦВДЗ);
- інформація, що приховується, не повинна вносити помітних змін до статистики контейнера.

Для впровадження інформації в аудіосигнали можна використовувати методи, що застосовуються в інших видах стеганографії.

Наприклад, можна впроваджувати інформацію, заміняючи найменш значні біти (всі або деякі). Або можна будувати стеганосистеми, ґрунтуючись на особливостях аудіосигналів та системи слуху людини.

Систему слуху людини можна уявити, як аналізатор частотного спектра, який може виявляти і розпізнавати сигнали діапазоні 10 – 20000 Гц. Систему слуху людини можна змоделювати, як 26 фільтрів, що пропускають, смуга пропускання, яких збільшується зі збільшенням частоти.

Система слуху людини розрізняє зміни фази сигналу слабше, ніж зміни амплітуди чи частоти.

Аудіосигнали можна розділити на три класи:

- розмова телефонної якості, діапазон 300 – 3400 Гц;
- широкосмугове мовлення 50 - 7000 Гц;
- широкосмугові аудіосигнали 20 – 20 000 Гц.

Зображення. Ефект маскування в просторовій множині може бути пояснений шляхом побудови стохастичних моделей зображення. При цьому зображення представляється у вигляді марківського випадкового поля.

Таким чином, можна запропонувати таку узагальнену схему впровадження даних у зображення:

1. Виконати фільтрацію зображення за допомогою орієнтованих смугових фільтрів. При цьому одержимо розподіл енергії по частотнопросторових компонентах.

2. Обчислити поріг маскування на основі знання локальної величини енергії.

3. Масштабувати значення енергії впроваджуваного ЦВДЗ у кожному компоненті так, щоб воно було менше порога маскування.

Високорівневі властивості зорової системи людини (ЗСЛ) поки рідко враховуються при побудові стеганоалгоритмів. Їх відмінністю від низькорівневих є те, що ці властивості проявляються «удруге», обробивши первинну інформацію від ЗСЛ, мозок видає команди на її «підстроювання» під зображення.

З огляду на це, нижче наведено основні властивості зорової системи людини:

1. Чутливість до контрасту. Висококонтрастні ділянки зображення, перепади яскравості привертаються до себе значну увагу.

2. Чутливість до розміру. Більші ділянки зображення «помітніші» менших за розміром. Причому, існує поріг насичення, коли подальше збільшення розміру не істотне.

3. Чутливість до форми. Довгі й тонкі об’єкти привертають більшу увагу, ніж круглі однорідні.

4. Чутливість до кольору. Деякі кольори (наприклад, червоний) «помітніші» інших. Цей ефект підсилюється, якщо тло заднього плану відрізняється від кольору фігур на ньому.

5. Чутливість до місця розташування. Людина схильна в першу чергу розглядати центр зображення.

6. Люди звичайно уважніше до зображень переднього плану, ніж заднього.

7. Якщо на зображенні є люди, в першу чергу людина зверне свою увагу на них. На фотографії людина звертає першочергову увагу на особу, очі, рот, руки.

8. Чутливість до зовнішніх подразників. Рух очей спостерігача залежить від конкретної обстановки, від отриманих їм перед переглядом або під час його інструкцій, додаткової інформації.

Для передачі прихованих повідомлень методами стеганографії використовуються спеціальні стеганографічні системи, так звані стегосистеми. Проте, для адекватної їх роботи висувається низка вимог [3]:

1. Безпека системи має повністю визначатися секретністю ключа. Це означає, що порушник може повністю знати всі алгоритми роботи стегосистеми та статистичні характеристики множин повідомлень та контейнерів, і це не дасть йому жодної додаткової інформації про наявність або відсутність повідомлення у цьому контейнері.

2. Знання порушником факту наявності повідомлення у будь-якому контейнері не повинно допомогти йому при виявленні повідомлень в інших контейнерах.

3. Заповнений контейнер повинен візуально не відрізнятися від незаповненого. Біти повідомлення, яке необхідно приховати, повинні вбудовуватися у візуально значущі області, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів, наприклад, модуляції з розширенням спектра.

4. Стегосистема повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не містить.

5. Повинна забезпечуватися потрібна пропускна спроможність (ця вимога є актуальною, в основному, для стегосистем прихованої передачі інформації).

6. Стегосистема повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система, тобто складний стегокодер і простий стегодекодер.

Приклад вбудовування секретної інформації в контейнер реалізовано на рисунку 2.

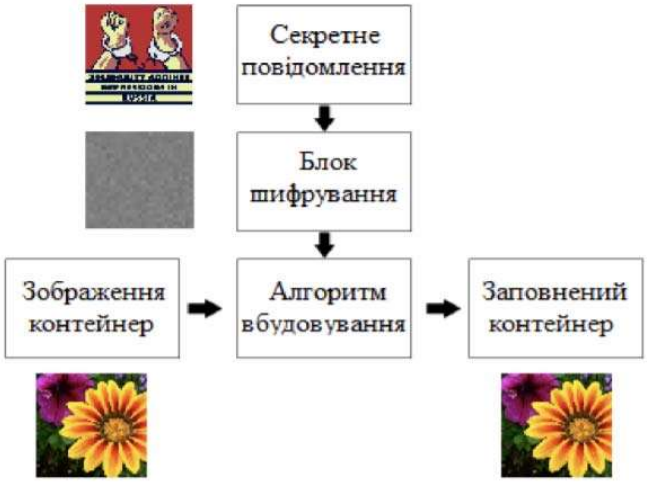

Рис. 2. Ілюстрація алгоритму вбудовування інформації в контейнер.

Для того щоб перейти до обговорення питань впровадження інформації в контейнери, необхідно визначити вимоги, які можуть бути пред'явлені до стеганосистем, які застосовуються для вбудовування інформації:

- інформація, що приховується, повинна бути стійкою до наявності різних пофарбованих шумів, стиснення з втратами, фільтрування, аналогово-цифрового та цифро-аналогового перетворень;
- інформація, що приховується, не повинна вносити в сигнал спотворення, що сприймаються системою слуху або органами зору людини;
- спроба видалення інформації, що приховується, повинна призводити до помітного пошкодження контейнера;
- інформація, що приховується, не повинна вносити помітних змін до статистики контейнера.

Керуючись даними вимогами, можна використовувати різні методи стеганографії для різних контейнерів. Це допоможе приховати інформацію і вирішити основні задачі.

На сьогоднішній день стеганографія використовується для захисту авторських прав, приховання зв'язку, автентифікації, для відстеження порушників (відбитків пальців), додавання додаткової інформації (наприклад, субтитрів до відео), додавання підписів до зображень, захист цілісності зображення (виявлення шахрайства), контроль копіювання при DVD-записі та в інтелектуальних браузерах, для автоматичного надання інформації в доступі та авторських правах, тощо (рисунок 3).

Рис. 2. Основні області застосування стеганографії.

Крім того, авторами було прийнято рішення більш детально описати основні задачі, а також технології та шляхи їх вирішення, які на сьогоднішній день використовують методи стагенографії. Така інформація наведена у таблиці 1.

Таблиця 1.

Основні задачі та області застосування стеганографії

Задача	Технології та шляхи вирішення	Приклад реалізації	Область застосування
1	2	3	4
Захист конфіденційної інформації від несанкціоновано го доступу	Вбудовування прихованої інформації у загальнодоступну мультимедійну інформацію	1 секунда оцифрованого звуку (44100 Гц, 8 біт, стерео) дозволяє приховати 5 сторінок текстової інформації, зміна значень відліків становить 1%	Військові та інші додатки, а також застосування у випадках, коли не можна використовувати криптографію
Подолання систем моніторингу та управління мережевими ресурсами	Стегометоди, спрямовані на протидію промисловому шпигунству, дозволяють протистояти контролю над інформацією в комп'ютерних мережах	Група Hacktivismo випустила утиліту Camera/Shy, яка працює не залишаючи в браузері історії діяльності, використовуючи стеганографічну техніку LSB та алгоритм шифрування AES з 256-розрядним ключем, функціонує дуже швидко та дозволяє приховувати повідомлення у gif-файлах. Крім того, ця програма здатна автоматично сканувати HTML-сторінки на наявність графічних зображень з прихованою інформацією	За заявою авторів, ця програма була створена для обходу національних міжмережевих екранів, що дає можливість безпечно обмінюватися будь-яким цифровим контентом через Інтернет.

1	2	3	4
Камуфлювання програмного забезпечення (ПЗ)	У випадках, коли використання ПЗ обмежено, воно може бути закамуфльовано під стандартні програми або приховано у файлах мультимедіа	Використовуються офіційні редактори, звуковий супровід, реклама тощо.	Забезпечується багаторівневий санкціонований доступ до ПЗ
Захист авторського права на інтелектуальну власність від копіювання та автентифікація	Використовуються технології цифрових водяних знаків (ЦВЗ) та ідентифікаційних номерів (ІН)	ЦВЗ вбудовуються в об'єкт, що захищається і можуть бути як видимими, так і невидимими. Вони містять автентичний код, інформацію про власника та керуючу інформацію. Відмінністю ІН від ЦВЗ є те, що будь-яка копія має свій ІН (технологія відбитків пальців)	Використовується для збереження авторського права
Прихована анотація документів та оптимізація банків даних (інформації)	Використовуються технології ЦВЗ та ІН	Інформація в електронних медичних документах, доступна тільки лікарю	Використовується для прихованої анотації документів у медицині, картографії, мультимедійних банках даних, а також для пошуку потрібної інформації

У таблиці 1 також наведено поширені приклади застосування методів стеганографії в залежності від задачі, яку необхідно вирішити.

У роботі наведено основні вимоги, які необхідно виконувати при приховуванні інформації. Автори також структурували використання стеганографічних методів за областю їх застосування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. R. Din. Review on Steganography Methods in Multi-Media Domain / R. Din, M. Mahmuddin, A. J. Qasim // International Journal of Engineering & Technology, 2019 – № 8 (1.7). – p. 288-292.
2. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика [Монографія] / Г.Ф. Конахович, А.Ю. Пузиренко. – К.: "МК-Пресс", 2006. – 288 с.
3. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 232 с.
4. Мартинюк Г.В. Доцільність використання стеганографічного LSB-методу для аудіосигналу / Г.В. Мартинюк, Т.В. Мелешко, А.Д. Сорокун // Актуальні питання забезпечення кібербезпеки та захисту інформації: Матеріали VII міжнарод. наук.-практ. конф., 24–27 лютого 2021 р.: тези доп. – К., 2021. – С. 53-56.
5. Основи комп'ютерної стеганографії: навч. посібн. для студентів і аспірантів / В. О. Хорошко, О. Д. Азаров, М. В. Шелест та ін. – Вінниця : ВДТУ, 2003. – 143 с.
6. A secure, robust watermark for multimedia / I. J. Cox, J. Kilian, T. Leighton, T. G. Shamoon // Information hiding: first international workshop. Lecture Notes in Comp. Science. – 1996. – Vol. 1174. – P. 183–206.