УДК 004.056

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
д.т.н., доц. **Шкуліпа П.А.** (ОДАТРЯ)
Прухніцький В.І. (ХмНУ)
к.т.н., доц. **Красильников С.Р.** (ХмНУ)

ШЛЯХИ ПІДВИЩЕННЯ ЗАХИСТУ АВТОРСЬКОГО ПРАВА ЗА ДОПОМОГОЮ ВИКОРИСТАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

У підсумку проведеного аналізу доводиться актуальність розробки технології використання цифрових знаків. Дана робота присвячена аналізу стеганографічних методів, які забезпечують конфіденційність та цілісність прихованих даних. Також, було розглянуто особливості використання цих методів для захисту авторських прав і прихованого зв'язку.

Було розглянуто особливості атак на стеганографічні системи, метою яких є руйнування або видалення цифрового водяного знака. Проаналізовано і наведено рекомендації із використання методів захисту від геометричних, криптографічних атак, а також атак на видалення цифрового водяного знака. Мета даного аналізу включає виявлення порушення безпеки або спроби порушення, які можуть нанести вразливість інформації, а також розглянемо класифікацію атак.

Розвиток засобів і методів захисту інформаційних документів є досить актуальний завданням. Одним з основних елементів багатьох документів є малюнок. Захист авторських прав, захист торгової марки, протидія копіюванню та підробкам фотографій – одні з основних завдань захисту зображень. Недоліком існуючих методів є їх низька ефективність. Тому метою даної роботи є виявлення основних критеріїв ефективності застосування цифрових зображень в стеганографії, а також визначення основних методів її підвищення.

Ключові слова: цифрова стеганографія, захист авторських прав, цифрові водяні знаки, атака, захист інформації.

Вступ. Сучасні інформаційні технології, які формують захищені документи, розвиваються швидкими темпами. Є потреба створювати нові види захисту друкованих документів, оскільки засоби та методи фальсифікації стають все поширенішими. Сьогодні фальсифіковані документи створюються новими більш технологічними методами, які

максимально близькі до методів виготовлення оригіналу. З кожним роком технічні характеристики копіювальних апаратів стають досконалішими, тому потрібно розробляти нові методи захисту друкованих документів. Одним з ефективних та надійних способів є цифровий захист документів.

Слово "стеганографія" в перекладі з грецької означає "таємнопис" Він може реалізуватися різними способами. В класичному випадку приховуване повідомлення вбудовується в деякий фізичний об'єкт, який не привертає уваги. Потім цей об'єкт відкрито передається адресату.

На сьогодні через використання комп'ютерів в усіх життєвих сферах розвинулася комп'ютерна стеганографія, яка в основному використовує цифрову обробку сигналів. Визначено такі напрями комп'ютерної стеганографії:

1. вбудовування інформації у фізичні об'єкти з метою її прихованої передачі для забезпечення конфіденційності;
2. вбудовування цифрових водяних знаків (ЦВЗ) з метою підтвердження достовірності;
3. вбудовування ідентифікаційних номерів та заголовків.

Фізичний об'єкт, в який вбудовується прихована інформація, називається контейнером. Контейнер може бути заповнений і незаповнений. Як правило, контейнером є цифровий носій інформації, що має аналогову природу, зазвичай це – аудіофайли, відеофайли та нерухомі зображення.

Стеганографія тісно пов'язана з криптографією, проте ці науки надають перевагу різним підходам до захисту інформації. Зокрема криптографія приховує інформацію за допомогою операції шифрування, тобто наперед відомо, що в криптограмі міститься зашифрована інформація. В свою чергу стеганографія приховує факт наявності секретної інформації, тому заповнений контейнер не повинен відрізнятися від порожнього. Для підвищення захищеності інформації методи криптографії і стеганографії можуть поєднуватися.

Стеганографія застосовує ЦВЗ, коли сторони обмінюються секретними повідомленнями, впровадженими в цифровий сигнал. Використовується як засіб захисту документів з фотографіями – паспортів, водійських посвідчень, кредитних карт з фотографіями. ЦВЗ можна також використовувати для виявлення потенційних піратів: під час продажу в зображення вбудовують інформацію про час продажу та інформацію про покупця. Ключовою відмінністю ЦВЗ від звичайного приховання інформації є наявність активного противника. Наприклад, використовуючи ЦВЗ для захисту авторського права, активний противник намагатиметься видалити чи змінити вбудовані ЦВЗ. Тому основною вимогою є стійкість вбудованих даних до атак. Таємність не є настільки важливою, як у прихованій комунікації.

Постановка задачі. Головним завданням є дослідження сучасних методів захисту інформаційних ресурсів та виявлення їх недоліків. На основі проведеного аналізу, врахувати слабкі сторони існуючих способів захисту інформації для вдосконалення і формулювання покращеного методу. Основною особливістю якого буде вміння використання цифрових знаків та розроблення нових методів. Це дасть можливість підвищити якість систем захисту від несанкціонованих вторгнень.

Загальні вимоги до стеганосистем ЦВЗ. Система ЦВЗ може бути представлена як комунікаційна система, що складається з трьох основних елементів: вбудування, комунікаційний канал та детектор. Інформація ЦВЗ вбудовується безпосередньо у сигнал, а не зашифровується у заголовок як це відбувається в інших техніках захисту. Вбудовування відбувається до відправлення сигналу у комунікаційний канал, вбудована інформація може бути розпізнана детектором.

Методи нанесення ЦВЗ діляться на просторові та частотні. До першої групи можна віднести методи, які вбудовують біти ЦВЗ шляхом зміни абсолютних значень координат точок згідно з певним алгоритмом. До другої групи можна віднести методи вбудовування інформації в зображення шляхом його представлення у зміненій формі шляхом використання певного математичного перетворення.

До основних характеристик ЦВЗ можна віднести наступні:

1. об‘єм (величина повідомлення що вноситься);
2. оберненість (можливість видалити ЦВЗ з поміченого сигналу);
3. прозорість (міра спотворення об‘єкта після вбудовування ЦВЗ).

За надійністю ЦВЗ розрізняють:

1. крихкі – при найменших модифікаціях повідомлення уже не можливо виявити;
2. напів крихкі – ЦВЗ витримує незначні модифікації сигналу;
3. надійні – протистоїть усім відомим видам атак. Присутність таких ЦВЗ у зображенні найлегше виявити, оскільки вони є найбільш об‘ємними. Саме такі ЦВЗ використовують для захисту від копіювання та ідентифікації.

Одна з головних проблем у маркуванні 3D зображень це запобігання великій кількості різноманітних атак, що можуть бути застосовані до моделі. По причині більш складного представлення даних, атакам на 3D важче запобігти ніж атакам на картинки чи відео. Представлення поверхні моделі не є сукупністю значень як у випадку з аудіо, 2D зображеннями чи відео, а описується колекцією неорганізованих точок у трьох вимірному просторі з індивідуальними викривленнями та особливою топологією, визначеною з‘єднаннями між точками [1].

Для підвищення стійкості до спотворень часто застосовують кодування або використовують широкосмугові сигнали. Початкову обробку прихованого повідомлення робить прекодер. Важлива попередня обробка ЦВЗ - обчислення його узагальненого Фур'є - перетворення. Це підвищує завадостійкість. Первинну обробку часто виробляють з використанням ключа - для підвищення секретності. Потім водяний знак «вкладається» в контейнер. Тут використовуються особливості сприйняття зображень людиною. Очі людини подібні низькочастотному фільтру, який пропускає дрібні елементи зображення. Найменш помітні спотворення в високочастотної області зображень. Впровадження ЦВЗ також повинно враховувати властивості сприйняття людини.

У багатьох стегосистемах для запису і зчитування ЦВЗ використовується ключ. Він може призначатися для обмеженого кола користувачів або ж бути секретним. Наприклад, ключ потрібен в DVD-плеєрах для можливості читання ними того, що міститься на дисках ЦВЗ. Як відомо, не існує таких стегосистем, в яких би при зчитуванні водяного знака була потрібна інша інформація, ніж при його запису. У більшості моделей стегосистем сигнал-контейнер можна розглянути як адитивний шум. При цьому завдання виявлення та зчитування стегоповідомлення вже не представляє складності, але не враховує двох факторів: невипадковість сигналу контейнера і запитів щодо збереження його якості. Облік цих параметрів дозволить будувати більш якісні стегосистеми. Для виявлення факту існування водяного знака та його зчитування використовуються спеціальні пристрої – стегодетектори [2].

Система виявлення вторгнень. Система виявлення вторгнень отримує інформацію про комп’ютерну систему для виконання діагностики стану безпеки останньої. Мета полягає в тому, щоб виявити порушення безпеки або спроби порушення, відкриті уразливості, які можуть привести до потенційних порушень.

Однією з основних частин системи є детектор, який обробляє інформацію, що надходить із комп’ютерної системи. Цей детектор може також запустити додаткові методи, так звані зонди для запуску процесу аудиту, наприклад, запиту номера версій для додатків, MAC-адрес пакета. Він використовує три види інформації: довгострокову інформацію, пов'язана з методом використовуваним для виявлення вторгнень (база даних атак), інформація про поточний стан системи та інформація про події, які відбуваються в системі. Роль детектора є усунення непотрібної інформації від аудиту. Після порівняння приймається рішення на основі оцінки ймовірності того, що ці дії або цей стан можна розглядатись, як симптоми вторгнення або уразливості.

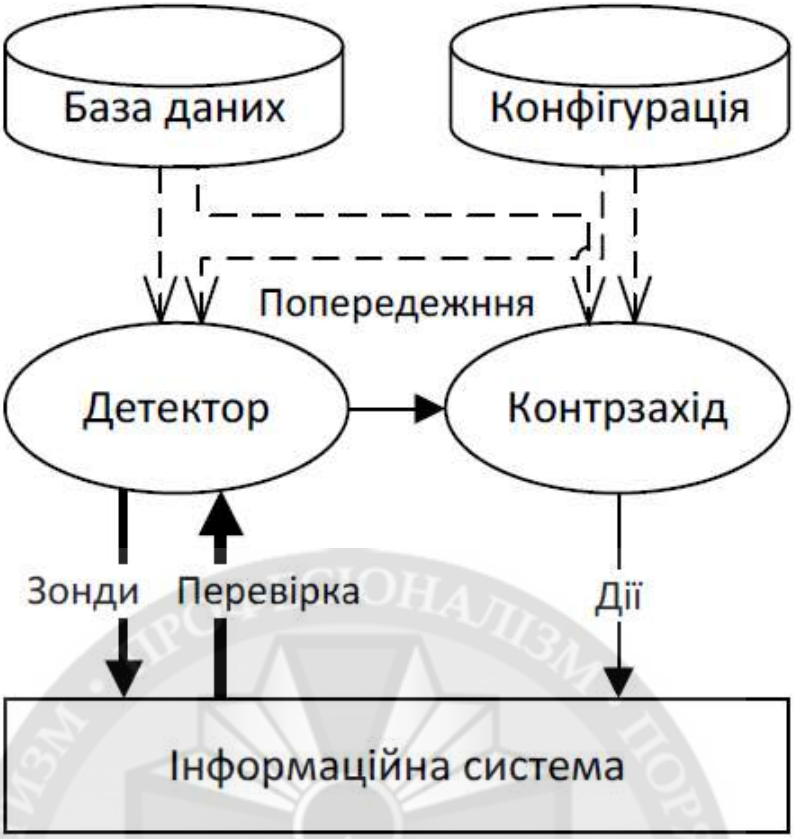

Рис. 1. Схема системи виявлення вторгнень

Для реалізації загроз порушники використовують атаки. Метою роботи є аналіз та класифікація атак, що можливі в стеганосистемах. Спочатку розглянемо загальні типи атак, що застосовуються до стеганосистем. Найпростішою з атак є суб'єктивна, яка полягає у визначенні за допомогою психовізуального спостереження та найпростішого аналізу заповненого контейнера наявності прихованого повідомлення у стегоконтейнері. Дана атака, як правило, здійснюється на першому етапі розкриття стеганосистеми та є ефективною лише в повністю незахищених стеганосистемах.

Аналіз заповненого контейнера передбачає проведення таких дій:

– виявлення прихованого повідомлення за зовнішніми ознаками;

– спроба використати відомий алгоритм вбудовування до заповненого контейнера;

– здійснення аналізу окремих ділянок контейнера або порівняння кількох заповнених контейнерів;

– виділення прихованого повідомлення за відомим алгоритмом вбудовування, проте невідомим ключем.

Активними атаками називаються будь-які модифікації контейнера з ЦВЗ. Вони можуть бути як природними (наприклад, пошкодження при передачі через канали зв’язку), так і спеціально задіяні зловмисниками, щоб вилучити водяні знаки [4].

При розробці алгоритмів мають враховуватись можливі модифікації контейнера. Оскільки в цій роботі розглядається тільки приховання ЦВЗ у зображення, то, відповідно, буде робитись акцент на пошкодженні зображень. Можна виділити наступні пошкодження:

1. Зображення можуть піддаватись компресії (наприклад JPEG, TIFF, GIF, PNG).
2. Геометричні перетворення:
    a. зсув зображення (translation);
    b. масштабування (scaling);

c. поворот (rotation);
d. обрізка (cropping);

3. Накладення шумів (як в частотну область зображення, так і в просторову).
4. Зміна кольорової гами.

Атаки, які видаляють цифрові водяні знаки. Цей тип атак використовує характеристику цифрового водяного знака у вигляді статистично описаного шуму. Очищення від шуму полягає у фільтрації сигналу з використанням різних статистичних критеріїв. Стиснення з втратами і очищення сигналів від шумів зменшують пропускну здатність каналу, особливо при наявності однорідних областей зображення, коефіцієнти перетворення яких можуть бути обнулені без помітного зниження якості відновленого зображення.

Існує ефективна для високочастотного ЦВЗ атака перемодуляції, яка робить спробу обману декодера при виявленні водяних знаків. Останній передбачається шляхом порівняння фільтрованої версії зображення і заповненого контейнера, тому реальні ЦВЗ будуються так, щоб їх спектр відповідав спектру початкового зображення. Після віднімання високочастотної частини ЦВЗ низькочастотна залишається незмінною, що свідчить про наявність ЦВЗ в зображенні. В свою чергу, високочастотна складова скомпенсує низькочастотну і ЦВЗ не буде знайдений. Протидією цій атаці є виконання низькочастотної фільтрації.

Ефективними також є атаки видалення ЦВЗ, які передбачають наявність великої кількості заповнених контейнерів з різними ЦВЗ або з різними ключами. Зокрема, при атаці усереднення атакуючий може одержати узагальнений цифровий водяний знак і відняти його від зображення. Атака змови передбачає розбиття різних заповнених контейнерів на частини, з яких створюється множина, на яку здійснюється атака. Із збільшенням кількості заповнених контейнерів у порушника збільшується можливість виявити ЦВЗ. Захистом від атаки змови є спеціальна побудова заповненого контейнера. Ще одна ефективна атака на ЦВЗ називається мозаїчною. При ній зображення розбивається на декілька частин таким чином, що цифровий водяний знак неможливо знайти [3].

Аналіз існуючих стеганографічних методів. Методи заміни в просторовій області. Класичним прикладом є метод заміни молодших біт (LSB- метод), який базується на тому, що молодші розряди графічних, аудіо і відео форматів несуть мало інформації і їх зміна практично не позначається на якості переданого зображення або звуку. Це дає можливість використання їх для кодування конфіденційної інформації.

Основною перевагою даного методу є простота реалізації та можливість таємної передачі великого обсягу інформації. Однак шляхом введення додаткової інформації спотворюються статистичні характеристики файлу-контейнера і приховане повідомлення легко виявити за допомогою статистичних атак, таких як оцінка ентропії та коефіцієнтів кореляції. Для зниження компрометуючих ознак потрібна корекція статистичних характеристик. Недоліком методу є також його чутливість до операцій цифрової обробки: стиснення, застосування фільтрації, конвертації кольорів, геометричних перетворень, додаткового зашумлення та зміни формату контейнера [4].

У методах, що діють в частотній області дані приховуються у коефіцієнтах частотного представлення контейнера. Для цього найчастіше використовуються перетворення, які застосовуються у сучасних алгоритмах стиснення із втратами (дискретне косинусне перетворення в стандарті JPEG). Приховання інформації може проводитися як в початкове зображення, так і одночасно із здійсненням стиснення зображення-контейнера. Важливо, що стегосистеми, у яких враховані особливості алгоритму стиснення, є нечутливими до подальшої компресії контейнера. Також вони забезпечують більшу стійкість до геометричних перетворень і виявлення каналу передачі (порівняно з методом LSB), оскільки є можливість в широкому діапазоні варіювати якість стисненого зображення, що робить неможливим визначення походження спотворення.

Широкосмугові методи. Суть даних методів полягає в розширенні смуги частот сигналу, до ширини спектру, значно більшої ніж це необхідно для передачі реальної інформації. Для розширення діапазону існують два способи: метод прямого розширення спектру, за

допомогою псевдо – випадкової послідовності, і метод стрибкоподібного налаштування частоти. При цьому корисна інформація розподіляється по всьому діапазону, тому при втраті сигналу в деяких смугах частот в інших смугах залишається достатньо інформації для її відновлення. Принцип дії широкосмугових методів схожий із завданнями, які вирішують стегосистеми, спробувати заховати секретне повідомлення в контейнері й ускладнити його виявлення.

Оскільки сигнал, розподілений по всій смузі спектра, його важко виділити. Це є суттєвою превагою даних методів, як і стійкість до випадкових та умисних спотворень. Тому вони застосовуються в техніці зв'язку для забезпечення високої завадостійкості і складності процесу перехоплення та виявлення. Проте недоліком є можливість стегоаналізу за рахунок цифрової обробки з використанням шумопоглинаючих фільтрів.

Статистичні методи приховують інформацію шляхом зміни деяких статистичних властивостей зображення. Наприклад, ідея алгоритму Patchwork базується на припущенні, що значення пікселів незалежні і однаково розподілені. При цьому генерується секретний ключ для ініціалізації генератора псевдовипадкових чисел, які вказують на місце в зображенні, куди вносяться біти водяного знака. Для цього у відповідності зі стегоключем вибирається n пар пікселів (b_i,c_i) у яких значення яскравості змінюється в такий спосіб:

$$\bar{b} = bi + 1, \bar{c} = ci + 1 \ , \tag{1}$$

$$Sn = \sum_{i=1} n(\bar{b}\, i - \bar{c}\, i) \ . \tag{2}$$

Якщо Sn значно відрізняється від нуля, то приймається рішення про наявність ЦВЗ. Такий метод забезпечує високу стійкість до операцій цифрової обробки. А наявність секретного ключа у широкосмугових та статистичних методах, що використовують псевдовипадкове кодування, підвищує їх надійність.

Висновки. У даній статті розглянуто основні відомості про цифрові водяні знаки, схеми їх використання, основні характеристики. А також загальні вимоги до стеганосистем цифрових водяних знаків, що використовуються для стеганографічного захисту інформації, виділено їх основні характеристики, переваги й недоліки. В процесі досліджень було виявлено клас задач захисту, що можуть мати ефективне вирішення за допомогою методів цифрової стеганографії.

Також здійснено аналіз системи виявлення вторгнень, мета якої виявити порушення безпеки або спроби порушення, відкриті вразливості, які можуть привести до потенційних порушень. Для захисту від криптографічних атак основну увагу потрібно приділити ключовій псевдовипадковій послідовності, згідно з якою вбудовується прихована інформація. Правильний вибір параметрів псевдовипадкової послідовності може значно підвищити стійкість стеганосистем до атак додавання шуму, стиснення та інших. Розглянуто різні існуючі стеганографічні методи, які на сьогоднішній день допомагають зробити інформацію більш захищеною.

ЛІТЕРАТУРА:

1. Козлюк П. В. Розробка ефективного дискретного перетворення для потокової обробки / П. В. Козлюк// Прогресивні інформаційні технології в науці та освіті. Збірник наукових праць. – Вінниця: – 2007.

2. Напівпроводникові лазери з електронним накачуванням. Том 2. Активні середовища. Розробка приладів. Монографія / О.С. Гаркавенко, С.В. Лєнков, В.А. Мокрицький, В.В. Видолоб. – Одеса, Поліграф, 2006. -456 с.

3. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2002.

4. Горпенюк А.Я., Стороженко А.О. Дослідження та порівняльний аналіз стеганографічних методів для впровадження даних у цифрові файли. Національний університет „Львівська політехніка” – 2015.

5. Кошкина Н. В. Обзор и классификация методов стеганоанализа / Н. В. Кошкина // УСиМ. – 2015. № 3. – С. 3 – 12.

6. Аграновский А. В. Стеганография, цифровые водяные знаки и стегоанализ / А. В. Аграновский, А. В. Балакин, В. Г. Грибунин. – М. : Вузовская книга, 2009. – 220 с.

REFERENCES:

1. Kozlyuk P. V. Rozrobka efektivnogo diskretnogo peretvorennya dlya potokovoyi obrobki / P. V. Kozlyuk// Progresivni informatsiyni tehnologiyi v nautsi ta osviti. Zbirnik naukovih prats. – Vinnitsya: – 2007.

2. Napivprovodnykovi lazery z elektronnym nakachuvannjam. Tom 2. Aktyvni seredovyshha. Rozrobka pryladiv. Monografija / O.S. Garkavenko, S.V. Ljenkov, V.A. Mokryc'kyj, V.V. Vydolob. – Odesa, Poligraf, 2006. -456 s.

3. Gribunin V. G. Tsifrovaya steganografiya / V. G. Gribunin, I. N. Okov, I. V. Turintsev. – M. : SOLON-Press, 2002.

4.Gorpenyuk A.Ya. Storozhenko A.O. Doslidzhennya ta porivnyalniy analiz steganografichnih metodiv dlya vprovadzhennya danih u tsifrovi fayli. Natsionalniy universitet „Lvivska politehnika” – 2015.

5. Koshkina N. V. Obzor i klassifikatsiya metodov steganoanaliza / N. V. Koshkina // USiM. – 2015. № 3. – S. 3 – 12.

6. Agranovskiy A. V. Steganografiya, tsifrovye vodyanye znaki i stegoanaliz / A. V. Agranovskiy, A. V. Balakin, V. G. Gribunin. – M. : Vuzovskaya kniga, 2009. – 220 s

Без рецензії.

д.т.н., проф. Лєнков С.В., д.т.н., доц. Шкулипа П.А.
Прухницкий В.И., к.т.н., доц. Красильников С.Р.

ПУТИ ПОВЫШЕНИЯ ЗАЩИТЫ АВТОРСКОГО ПРАВА СРЕДСТВОМ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

По результатам проведенного анализа доказывается актуальность разработки технологии использования цифровых знаков. Данная работа посвящена анализу стеганографических методов, которые обеспечивают конфиденциальность и целостность скрытых данных. Также, были рассмотрены особенности использования этих методов для защиты авторских прав и скрытой связи.

Были рассмотрены особенности атак на стеганографические системы, целью которых является разрушение или удаление цифрового водяного знака. Проанализированы и приведены рекомендации по использованию методов защиты от геометрических, криптографических атак, а также атак на удаление цифрового водяного знака. Цель данного анализа включает выявления нарушения безопасности или попытки нарушения, которые могут нанести уязвимость информации, а также рассмотрим классификацию атак.

Развитие средств и методов защиты информационных документов является достаточно актуальной задачей. Одним из основных элементов многих документов является фотография. Защита авторских прав, защита торговой марки, противодействие копированию и подделкам фотографий - одни из основных задач защиты изображений. Недостатком существующих методов является их низкая эффективность. Поэтому целью данной работы является выявление основных критериев эффективности применения цифровых изображений в стеганографии, а также определение основных методов ее повышения.

Ключевые слова: цифровая стеганография, защита авторских прав, цифровые водяные знаки, атака, защита информации.

prof. Lenkov S.V., Ph.D. Shkulipa P.A., Prukhnitskyi V.I., Ph.D. Krasilnikov S.R.

WAYS OF ENHANCEMENT OF COPYRIGHT PROTECTION THROUGH THE USE OF DIGITAL WATERMARKS

As a result of the analysis was proved the relevance of technology development of use of the digital signage. As a result of the analysis proved the relevance of technology development of use of digital signage.

This work is devoted to the steganographic methods which provide the confidentiality and integrity of confidential data. Also was considered features of the use of these methods for copyright protection and covert communications.

Was examined the features of the attacks on the steganographic systems, which goal is a the destruction or removal of a digital watermark. Was analyzed and provides recommendations on the using of methods of protection from geometric, cryptographic attacks and attacks by removing of a digital watermark. The purpose of this analysis includes the detection of security breaches or attempts to breach which may inflict vulnerability of information and we will consider the classification of the attacks.

The development of tools and methods of protection of informational documents is very important task. One of the key elements of many documents is the image. Copyright protection, trademark protection, combating falsification and copying photos - one of the main tasks of image protection. The disadvantage of existing methods is their low efficiency. Therefore, the aim of this work is to identify the main criteria of effectiveness of using of the digital image steganography and to identify the main methods to improve it.

Keywords: digital steganography, copyright protection, digital watermarks, protection of information.