УДК 004.056.53

д.т.н., доц. **Єфіменко А.О.** (ОНПУ)
Трифонова К.О. (ОНПУ)
Зіновський В.Р. (ОНПУ)

АУДИТ СТЕГАНОГРАФІЧНОЇ ВРАЗЛИВОСТІ ВЕБ-ДОДАТКУ

У статті розглянуто виявлену індійським дослідником з інформаційної безпеки нову вразливість веб-додатку через цифрові зображення та атаку на веб-додаток, що реалізована засобами стеганографії. Запропоновано модифікований стеганоаналітичний алгоритм, заснований на аналізі пар близьких та унікальних кольорів, реалізація програмного продукту для аудиту вразливості веб-додатків засобами стеганоаналізу. В результаті виконання роботи розроблено веб-сервіс, для аудиту стеганографічної вразливості веб-додатку. Результати роботи можуть бути використані, як складова систем аудиту безпеки веб-додатку, що виконують аудит десяти категорій найбільш поширених вразливостей веб-додатків.

Ключові слова: веб-додаток, аудит, вразливість, стеганоаналіз, близька пара кольорів, унікальна пара кольорів.

Вступ. На сьогоднішній день інформатизація є одним з пріоритетних напрямків розвитку всіх економічних галузей. Практично кожна організація, комерційна чи державна, має свій інтернет-сайт, вводить всілякі онлайн-послуги. В електронному вигляді зберігаються персональні дані клієнтів і співробітників, фінансова інформація і дані про господарську діяльність.

У зв'язку з цим завдання аудиту та забезпечення безпеки веб-додатків стає важливішим рік від року, що робить тему даної роботи надзвичайно актуальною.

На жаль, розробники корпоративних інформаційних систем не завжди дотримуються вимог безпеки - через відсутність необхідного досвіду або просто зосереджуючись на інших цілях при розробці системи. Щорічні дослідження компанії Positive Technologies свідчать, що велика кількість веб-додатків містять вразливості високого ступеня ризику, які можуть стати причиною фінансового або репутаційного збитку [1].

Саме атака на веб-додатки часто стає першим етапом при зломі мереж великих

компаній, а публікація ганьбить власника інформації на офіційних веб-сайтах, служить зброєю в інформаційній війні. Чималу роль вразливі веб-додатки можуть зіграти в успіху вкрай поширених на сьогоднішній день розподілених атак, спрямованих на відмову в обслуговуванні (DDoS). Якщо на мережевому рівні спеціальні послуги від провайдерів і пристрої для захисту трафіку можуть впоратися з найбільш примітивними і масовими DDoS-атаками, то у випадку, коли зловмисник емулює дії легітимного користувача програми та використовує спеціальні ресурсомісткі запити до сайту, навіть невеликий обсяг трафіку може призвести до повної недоступності веб-додатку [1].

Кожного року відкритий проект захисту веб-додатків OWASP проводить дослідження та публікує класифікацію найбільш поширених вразливостей веб-додатків [2]. На даний час це: вставка інструкцій; некоректна аутентифікація та управління сеансами; міжсайтове виконання сценаріїв; небезпечні прямі посилання на об’єкти; небезпечна конфігурація оточення; витік критичних даних; відсутність контролю доступу до функціонального рівня; підробка міжсайтових запитів; використання компонентів з відомими вразливостями; небезпечні переадресування. Але не так давно індійський дослідник безпеки Саум Шах опублікував звіт про розроблений ним метод атаки, заснований на популярному серед користувачів обміні посилань на зображення. Спеціаліст зміг приховати виконуваний шкідливий код в пікселях довільної картинки, залишаючи таким чином свій експлоїт на самому видному місці [3]. Дослідник відзначає, що приховати шкідливий код безпосередньо в зображенні було найскладнішим, і для цього йому довелося використовувати засоби стеганографії. Частини шкідливого коду Шах розподілив всередині пікселів картинки, що дозволяє декодувати їх назад за допомогою елемента Canvas в HTML 5, який проводить динамічний рендеринг зображень.

Для успішної атаки не потрібно піклуватися про хостинг веб-сайту, не потрібні дані про домен. Дослідник завантажує зображення, опубліковує його у відкритому доступі і, якщо жертва завантажує його у своєму браузері, воно скомпрометує систему.

Окремо фахівець зазначає, що зміни, що виникають в кінцевому зображенні через наявність стороннього коду, помітні тільки при багаторазовому збільшенні картинки. Свою техніку нападу Шах назвав Stegosploit, а її подробиці він розкрив у ході конференції з інформаційної безпеки Hack In The Box, що недавно проходила в Амстердамі. Відео з подробицями атаки і коментарями експерта опубліковано на YouTube [3].

Однією з наук, що займається приховуванням даних, є стеганографія. Відмінною особливістю стеганографії є те, що при передачі секретної інформації в таємниці тут залишається сам факт передачі. Перевага стеганографії полягає в тому, що вона надає можливість таємно передати конфіденційне повідомлення – додаткову інформацію одночасно з відкритою інформацією – контейнером або основним повідомленням, яка не є конфіденційною. У якості основного повідомлення може бути обраний будь-який мультимедіа об'єкт – цифрове зображення, відео або аудіо.

В результаті занурення додаткової інформації в основне повідомлення не повинно відбуватися помітних змін контейнера. Даний процес називають стеганоперетворенням, а його результат – стеганоповідомленням. Використання стеганоперетворення часто дозволяє уникнути прямих атак на додаткову інформацію, оскільки невідомо, чи присутня вона в інформаційному потоці. Додаткова інформація, що вноситься в контейнер, може бути попередньо зашифрована, щоб ускладнити завдання стегоноаналітика. Основне завдання стеганоаналіза – встановлення факту присутності в контейнері прихованої інформації [4-8].

Робота стеганоаналізу полягає в пошуку та аналізі певних характеристик і ознак у досліджуваному цифровому об'єкті, визначення факту наявності або відсутності яких дозволяє отримати відповідь на питання, чи є об'єкт стеганоповідомленням або ж він не піддавався стеганоперетворенню.

На даний час на ринку програмних продуктів можна зустріти достатню кількість стеганопрограм, розроблених під деякі формати графічних, відео та аудіо файлів, що використовуються в Інтернеті. У більшості з них застосовуються різні модифікації LSB-

методу, основною ідеєю якого є використання одного або декількох молодших двійкових розрядів інтенсивності колірних компонент окремих пікселів для занурення додаткової інформації. Популярність даного методу обумовлена його простотою і тим, що він дозволяє приховувати в відносно невеликих файлах достатньо великі обсяги інформації. Візуально зображення при цьому не змінюється, особливо якщо в якості основного повідомлення вибрано багатобарвне зображення з великою кількістю деталей, тобто інформаційно навантажене. Якщо, наприклад, взяти цифрове зображення з колірною моделлю RGB, на кожну компоненту кольору R, G і B якого відводиться 8 біт, та змінити значення найменших значущих біт – то таке перетворення буде невловимо для людського сприйняття. Це значною мірою ускладнює роботу стеганоаналітика, якщо він не володіє спеціальними засобами стеганоаналізу. В якості таких засобів можуть виступати програми, що реалізують методи і алгоритми стеганоаналіза.

До таких засобів стеганоаналізу відносяться алгоритми, засновані на аналізі пар кольорів, які є ефективними і широко використовуються [10,11].

Тому, метою даної роботи є модифікація алгоритму [4,5,9], заснованому на аналізі пар кольорів, та реалізація програмного продукту для аудиту вразливості веб-додатків засобами стеганоаналізу.

Основна частина. В роботах [4,5] запропоновано стеганоаналітичний алгоритм, заснований на аналізі кількості близьких пар кольорів та унікальних пар кольорів, для контейнерів – цифрових зображень в довільному форматі.

Під кольором розуміють трійку компонент (R,G,B) або піксель, який також мається на увазі як триплет значень (R,G,B), де R – червона, G – зелена і B – синя компонента в колірній моделі RGB.

В якості статистичних характеристик для відділення стеганоповідомлення від цифрового зображення, що не містить додаткової інформації, використано коефіцієнти близьких пар кольорів та унікальних кольорів.

Для цифрових зображень, що зберігаються в форматі без втрат, під близькою парою [9] розуміють два кольори (R_1,G_1,B_1) і (R_2,G_2,B_2), якщо для них виконується наступне співвідношення:

$$\begin{cases} |R_1 - R_2| \le 1 \\ |G_1 - G_2| \le 1 \\ |B_1 - B_2| \le 1 \end{cases}. \quad (1)$$

Для цифрових зображень, що зберігаються в форматі з втратами, під близькою парою [5] розуміють два кольори (R_1,G_1,B_1) і (R_2,G_2,B_2), якщо для них виконується наступне співвідношення:

$$\begin{cases} |R_1 - R_2| \le 2 \\ |G_1 - G_2| \le 2 \\ |B_1 - B_2| \le 2 \end{cases}. \quad (2)$$

Для цифрових зображень, що зберігаються в форматі без втрат, під унікальною парою [9] розуміють два кольори (R_1,G_1,B_1) і (R_2,G_2,B_2), якщо для них виконується хоча б одна умова:

$$\begin{cases} |R_1 - R_2| \le 1 \\ |G_1 - G_2| \le 1 \\ |B_1 - B_2| \le 1 \end{cases}. \quad (3)$$

Для цифрових зображень, що зберігаються в форматі з втратами, під унікальною парою

[5] розуміють два кольори (R_1, G_1, B_1) і (R_2, G_2, B_2), якщо для них виконується хоча б одна умова:

$$\begin{aligned} |R_1 - R_2| &\le 2 \\ |G_1 - G_2| &\le 2 \\ |B_1 - B_2| &\le 2 \end{aligned}. \quad (4)$$

R – відношення кількості близьких пар кольорів до кількості унікальних пар кольорів:

$$R = \frac{P}{U}, \quad (5)$$

де P – кількість близьких пар кольорів в цифровому зображенні, що зберігається в форматі без втрат (з втратами);

U – кількість унікальних пар кольорів в цифровому зображенні, що зберігається в форматі без втрат (з втратами).

В роботі [5] запропоновано стеганоаналітичний алгоритм, заснований на аналізі кількості близьких пар кольорів та унікальних пар кольорів. Встановлено, що для контейнерів, що зберігаються в форматі з втратами, якщо дана умова виконується $R - min(R') < T_1$, то контейнер не є стеганоповідомленням, в противному випадку – вважають стеганоповідомленням; для контейнерів, що зберігаються в форматі без втрат, якщо дана умова виконується $R - max(R') > T_2$, то контейнер не є стеганоповідомленням, в противному випадку – вважають стеганоповідомленням. В результаті виконаного аналізу в роботі [4] запропоновано використовувати наступні порогові значення $T_1 = 1{,}23$ та $T_2 = 0{,}28$.

В поданій роботі була виконана реалізація запропонованого в [5] стеганоаналітичного алгоритму. На рис. 1, як на прикладі аналізу двох різних цифрових зображень, збережених в форматі без втрат, показано, як змінюється відношення кількості близьких пар кольорів до кількості унікальних пар кольорів в результаті виконання стеганоперетворення над контейнером (рис. 1а)), що не містив додаткової інформації, та над стеганоповідомленням (рис. 1 б)). Вісь ординат – значення R і R', вісь абсцис – це кількість найменш значущих біт, що змінюється. Кожен з графіків складається з n відрізків. Ордината точки, з якої виходять відрізки – відповідає коефіцієнту R, кінцеві точки відрізків – це n коефіцієнтів R'. Для наочності представлення графіки побудовані для цифрового зображення, що не містило додаткової інформації, та для стеганоповідомлення розміщені на одній координатній площині (рис. 1в)).

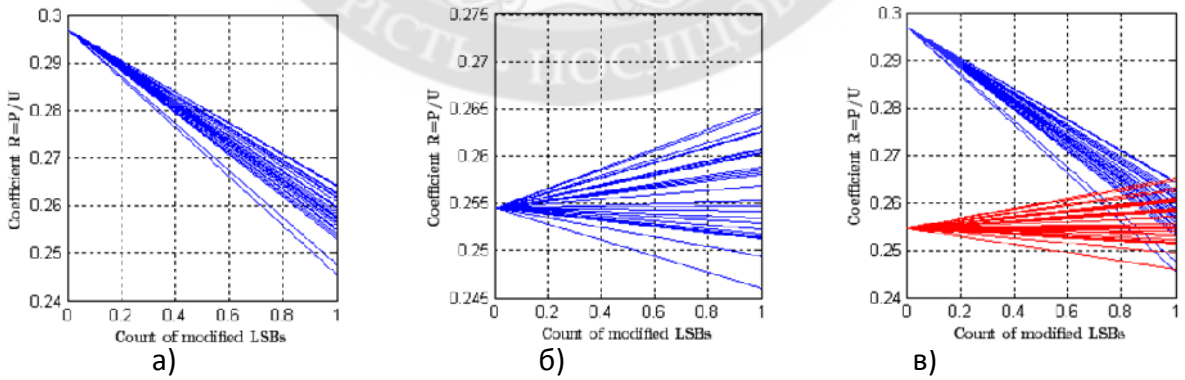


Рис. 1. Графіки зміни значення коефіцієнта R та R' при стеганоперетворенні в форматі без втрат а) – для цифрового зображення, що не містить додаткової інформації; б) – для цифрового зображення з додатковою інформацією; в) – для цифрового зображення без

На рис. 2, як на прикладі аналізу двох різних цифрових зображень, збережених в форматі з втратами, показано, як змінюється відношення кількості близьких пар кольорів до

кількості унікальних пар кольорів в результаті виконання стеганоперетворення над контейнером (рис. 2 а)), що не містив додаткової інформації, та над стеганоповідомленням (рис. 2 б)).

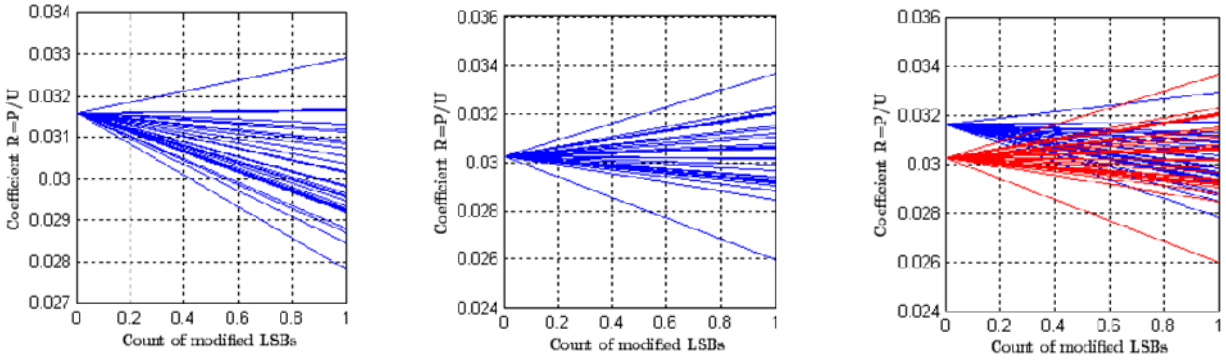


Рис. 2. Графіки зміни значення коефіцієнта R та R' при стеганоперетворенні в форматі з втратами а) – для цифрового зображення, що не містить додаткової інформації; б) – для цифрового зображення з додатковою інформацією; в) – для цифрового зображення без (синій) та з (червоний) додатковою інформацію

В результаті експерименту були виявлені цифрові зображення в форматі JPEG, що не містили додаткової інформації або були стеганоповідомленням, але не відповідали встановленій умові відділення стеганоповідомлень від цифрових зображень, що не містили додаткової інформації. На рис. 2 представлено приклад таких цифрових зображень. Тому була запропонована модифікація дослідженого стеганоаналітичного алгоритму.

Оскільки невідомо початковий формат зберігання цифрового зображення, то запропоновано використовувати наступні способи визначення близьких та унікальних пар кольорів. Під близькою парою будемо розуміти два кольори (R_1, G_1, B_1) і (R_2, G_2, B_2), якщо для них виконується наступне співвідношення:

$$\begin{cases} |R_1 - R_2| \le 2 \\ |G_1 - G_2| \le 2 \\ |B_1 - B_2| \le 2 \end{cases}. \quad (6)$$

Під унікальною парою розуміють два кольори (R_1, G_1, B_1) і (R_2, G_2, B_2), якщо для них виконується наступне співвідношення:

$$\begin{cases} |R_1 - R_2| > 2 \\ |G_1 - G_2| > 2 \\ |B_1 - B_2| > 2 \end{cases}. \quad (7)$$

$\overline{R}$ – відношення кількості близьких пар кольорів до кількості унікальних пар кольорів:

$$\overline{R} = \frac{P}{\overline{U}}, \quad (8)$$

де P – кількість близьких пар кольорів в цифровому зображенні, визначений у відповідності до (6);

$\overline{U}$ – кількість унікальних пар кольорів в зображенні, визначений у відповідності до (7).

Для контейнерів, що зберігаються в довільному форматі, якщо дана умова виконується,

$$\overline{R} > \max_{i=1}^{30}\left(\overline{R_i}'\right), \quad (9)$$

то контейнер не містить додаткової інформації, в противному випадку – вважають стеганоповідомленням.

Отже, стеганоаналітичний алгоритм, заснований на аналізі кількості близьких пар кольорів та унікальних пар кольорів, на основі нового визначення унікальних пар кольорів цифрового зображення, складається з наступних кроків:

а) для цифрового зображення розрахувати кількість близьких пар кольорів P; кількість унікальних пар кольорів $\overline{U}$; коефіцієнт $\overline{R}$;

б) сформувати випадкову бінарну матрицю та за допомогою методу LSB виконати її занурення в цифрове зображення; виконати розрахунок P', $\overline{U'}$, $\overline{R'}$ для отриманого стеганоповідомлення; повторити цей крок $n = 30$ раз;

в) визначити максимальне значення в наборі з n значень $\overline{R'}$;

г) для контейнерів, що зберігався в довільному форматі, якщо дана умова виконується $\overline{R} > \max_{i=1}^{30}\left(\overline{R_i'}\right)$, то контейнер не містить додаткової інформації, в противному випадку – вважають стеганоповідомленням.

На рис. 3, для тих самих зображень, для яких було виконано дослідження на рис. 1, збережених в форматі без втрат, показано, як змінюється модифіковане відношення $\overline{R}$.

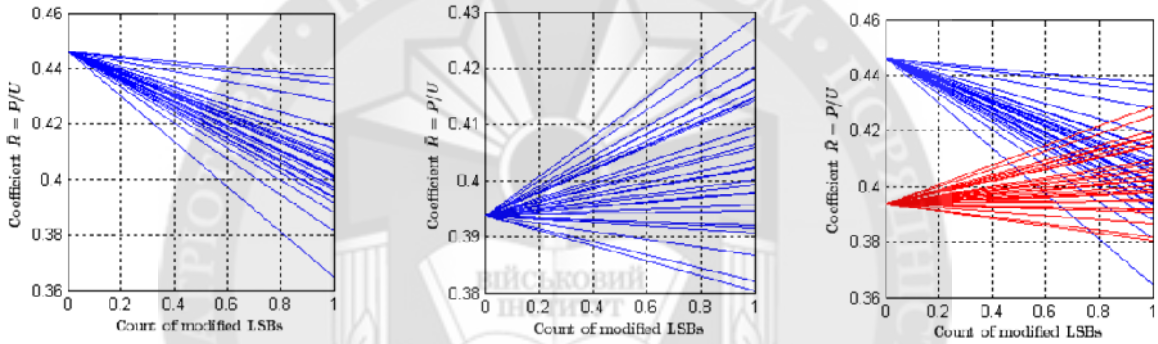
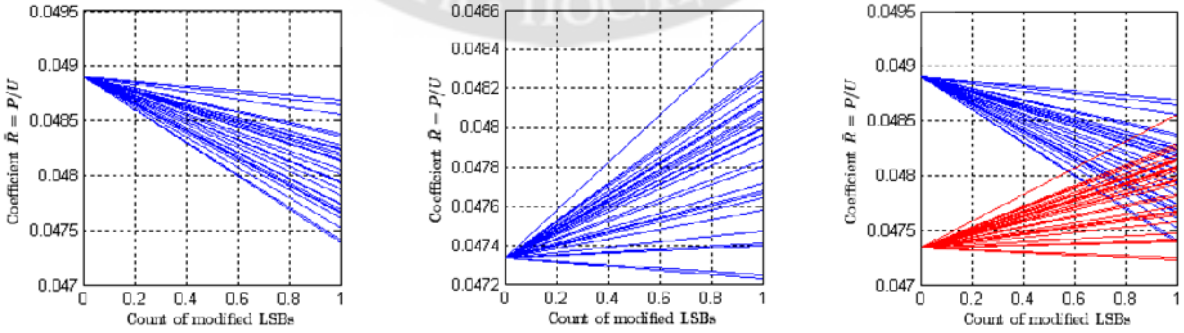


Рис. 3. Графіки зміни значення коефіцієнта $\overline{R}$ та $\overline{R'}$ при стеганоперетворенні в форматі без втрат а) – для цифрового зображення, що не містить додаткової інформації; б) – для цифрового зображення з додатковою інформацією; в) – для цифрового зображення без (синій) та з (червоний) додатковою інформацію

На рис. 4, для тих самих зображень, для яких було виконано дослідження на рис. 2, збережених в форматі з втратами, показано, як змінюється модифіковане відношення $\overline{R}$.



а) б) в)

Рис. 4. Графіки зміни значення коефіцієнта $\overline{R}$ та $\overline{R'}$ при стеганоперетворенні в форматі з втратами а) – для цифрового зображення, що не містить додаткової інформації; б) – для цифрового зображення з додатковою інформацією; в) – для цифрового зображення без (синій) та з (червоний) додатковою інформацію

Одною з важливих характеристик стеганографічного методу вважається пропускна спроможність. Відповідно до [8] під пропускною спроможністю каналу передачі повідомлень, що приховуються, або просто під прихованою пропускною спроможністю, розуміють максимальну кількість інформації, яка може бути вкладена в один елемент контейнера.

Оскільки канал прихованого зв'язку утворюється усередині каналу відкритого зв'язку, то пропускна спроможність буде менше пропускної спроможності каналу відкритого зв'язку, в якому за одне використання каналу передається один елемент стеганоповідомлення, що містить додаткову інформацію [8].

Алгоритм, який на сьогоднішній день є найбільш кращим з точки зору забезпечення значної прихованої пропускної спроможності, є стеганографічний алгоритм модифікації найменш значущого біта. Даний алгоритм може задіяти при стеганоперетворенні всі пікселі цифрового зображення, тобто прихована пропускна спроможність складає 1 біт/пікс, для цифрового зображення в кольоровій моделі Grayscale, хоча вона потенційно може бути збільшена, наприклад, в два або три рази за рахунок модифікації не одного, а двох трьох найменш значущих бітів.

Для встановлення факту наявності в контейнері прихованої інформації, що була занурена саме за допомогою алгоритмів модифікації найменш значущого біту, як найкраще зарекомендував себе стеганоаналітичний алгоритм, заснований на аналізі кількості близьких пар кольорів та унікальних пар кольорів [9-11].

Для перевірки ефективності модифікованого стеганоаналітичного алгоритму, на основі нового визначення унікальних пар кольорів цифрового зображення, тобто виявлення наявності додаткової інформації, окрім дослідження контейнерів отриманих в результаті стеганоперетворення алгоритмом найменш значущого біту, виконано дослідження контейнерів отриманих за допомогою алгоритму Кутера-Джордана-Босеена.

Куттер, Джордан і Боссен запропонували алгоритм вбудовування секретної інформації в канал синього кольору зображення, оскільки до синього кольору зорова система людини є найменш чутливою, в випадковим чином обрані пікселі [6]. Тобто в результаті роботи алгоритму не всі пікселі зазнають змін, що є важливим для стеганоаналітичного алгоритму, заснованому на аналізі пар кольорів.

Алгоритм занурення одного біта секретної інформації в запропоновану методі, виконується в результаті модифікації випадковим чином обраного синьої складової пікселя, розташованого в (x, y), наступним чином:

$$B'_{x,y} = \begin{cases} B_{x,y} - v \cdot \lambda_{x,y}, & m_i = 0 \\ B_{x,y} + v \cdot \lambda_{x,y}, & m_i = 1 \end{cases} \qquad (10)$$

де $B_{x,y}$ – синя складова пікселя, розташованого в (x, y);

$\lambda_{x,y} = 0{,}29890 \cdot R_{x,y} + 0{,}58662 \cdot G_{x,y} + 0{,}11448 \cdot B_{x,y}$ – коефіцієнт, що відповідає яскравості пікселя, розташованого (x, y);

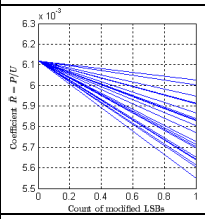
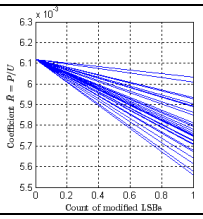
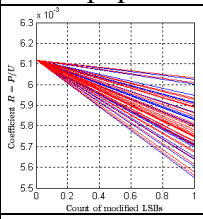
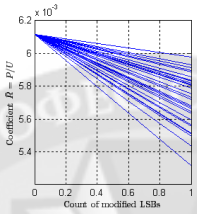
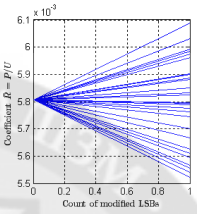
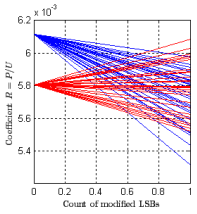
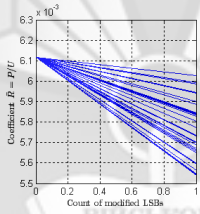
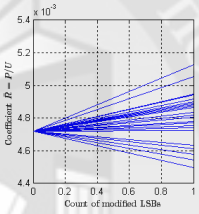
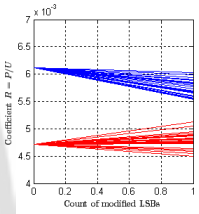
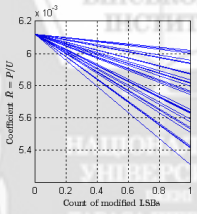
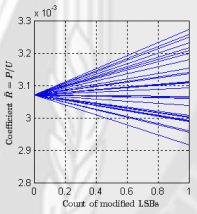
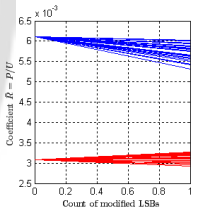
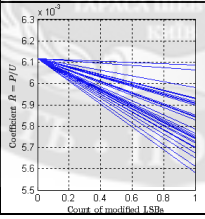
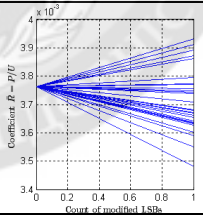
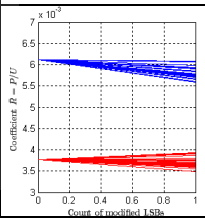
v – константа, що визначає енергію вбудованого сигналу, величина залежить від призначення стеганосистеми, чим більше v, тим вище стійкість вбудованої інформації до спотворень, проте і тим сильніше її помітність, у відповідності до [6], дорівнює 0,15;

m_i – біт, що вбудовується в канал синього кольору.

Для демонстрації результатів дослідження зміни відношення кількості близьких пар кольорів до кількості унікальних пар кольорів в результаті виконання стеганоперетворення різними алгоритмами, короткий опис яких наведено вище, над цифровим зображенням контейнером, що не містив додаткової інформації, та над стеганоповідомленням, як на прикладі аналізу двох різних цифрових зображень з втратами та без представлені графіки зміни значення коефіцієнта $\overline{R}$ та $\overline{R'}$ відповідно в таблиці 1 та таблиці 2.

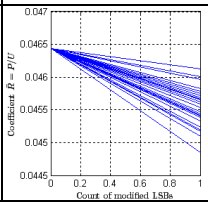
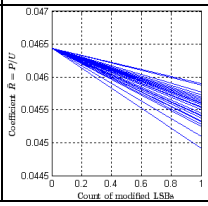
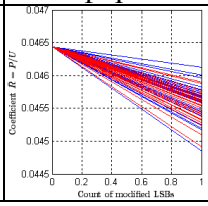
Таблиця 1

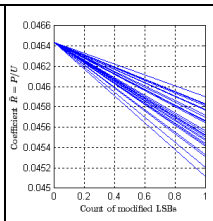
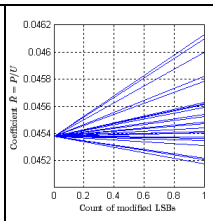
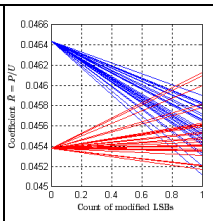
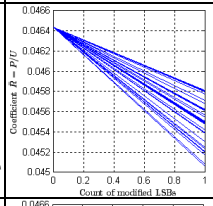
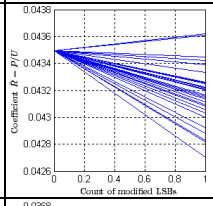
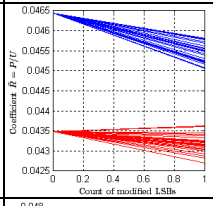
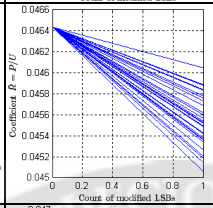
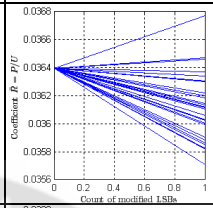
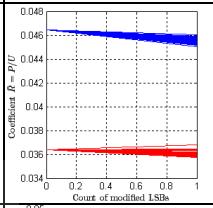
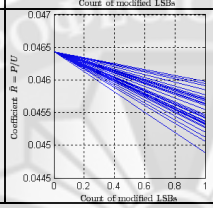
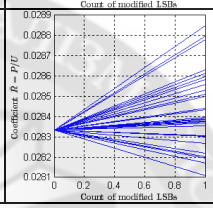
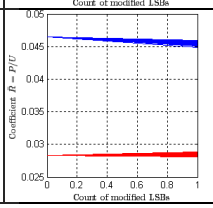
Аналіз зміни значення коефіцієнта $\overline{R}$ та $\overline{R'}$ при стеганоперетворенні цифрового зображення в форматі без втрат

№	Файл	Стегано графічний алгоритм	Без додаткової інформації	З додатковою інформацією	Без (синій) та з (червоний) д. інформацію
1	«onion.png»	Занурення не виконується			
2	«onion.png»	Алгоритм модифікації одного найменш значущого біта			
3	«onion.png»	Алгоритм модифікації двох найменш значущих біт			
4	«onion.png»	Алгоритм модифікації трьох найменш значущих біт			
5	«onion.png»	Алгоритм Куттера, Джордана і Боссена			

Таблиця 2

Аналіз зміни значення коефіцієнта $\overline{R}$ та $\overline{R'}$ при стеганоперетворенні цифрового зображення в форматі з втратами

№	Файл	Стегано графічний алгоритм	Без додаткової інформації	З додатковою інформацією	Без (синій) та з (червоний) д. інформацію
1	«greens.jpg»	Занурення не виконується			

2	«greens.jpg»	Алгоритм модифікації одного найменш значущого біта			
3	«greens.jpg»	Алгоритм модифікації двох найменш значущих біт			
4	«greens.jpg»	Алгоритм модифікації трьох найменш значущих біт			
5	«greens.jpg»	Алгоритм Куттера, Джордана і Боссена			

З метою перевірки ефективності модифікованого стеганоаналітичного алгоритму, заснованому на новому визначенні унікальних пар кольорів цифрового зображення, в результаті розрахункового експерименту протестовано 500 цифрових зображень, що початково зберігались з втратами та без.

Помилкою першого роду являється випадок, коли цифрове зображення без додаткової інформації, вважається цифровим зображенням, отриманим в результаті стеганоперетворення.

Помилкою другого роду являється випадок, коли цифрове зображення, отримано в результаті стеганоперетворення, вважається цифровим зображенням без додаткової інформації.

Для розрахункового експерименту побудована координатна площина, вісь абсцис – $\overline{R}$, вісь ординат – $\underset{i=1}{\overset{30}{max}}\left(\overline{R_i}'\right)$. Кожне зображення на площині представлено точкою з координатами $\left(\overline{R}, \underset{i=1}{\overset{30}{max}}\left(\overline{R_i}'\right)\right)$. Точки червоного кольору відповідають цифровим зображенням, отриманим в результаті стеганоперетворення, точки блакитного кольору – цифрові зображення без додаткової інформації (рис. 5). Отже, в результаті розрахункового експерименту встановлено, що помилки першого та другого роду склали 0.2%.

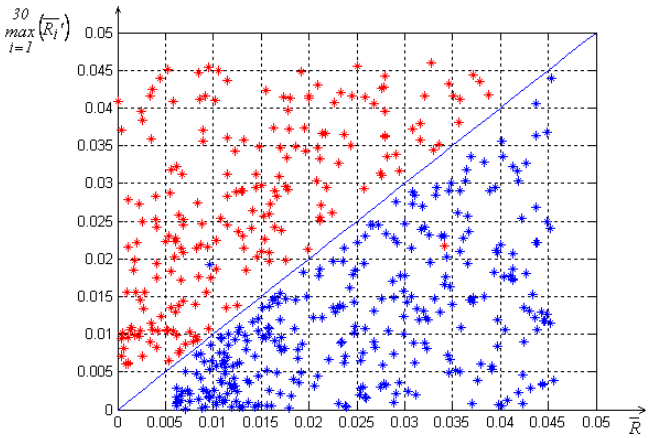


Рис. 5. Відображення цифрових зображень, з додатковою інформацією та без на координатній площині залежності $\overline{R}$ від $\max_{i=1}^{30}(\overline{R_i}')$

Висновки. В результаті даної роботи розглянуто виявлену індійським дослідником з інформаційної безпеки нову вразливість веб-додатку через цифрові зображення та атаку на веб-додаток, що реалізована засобами стеганографії.

Для розв'язку задачі аудиту стеганографічної вразливості веб-додатку. реалізовано та досліджено стеганоаналітичний алгоритм, заснований на аналізі кількості близьких пар кольорів та унікальних пар кольорів.

Запропоновано модифікований стеганоаналітичний алгоритм, заснований на аналізі кількості близьких пар кольорів та унікальних пар кольорів, на основі нового визначення унікальних пар кольорів цифрового зображення.

Результатом роботи є веб-сервіс, для аудиту стеганографічної вразливості веб-додатку, що може бути використаний для доповнення систем аудиту безпеки веб-додатку, що виконують аудит визначених десяти категорій найбільш поширених вразливостей веб-додатків.

ЛІТЕРАТУРА:

1. Statystyka uyazvymostey veb-prylozhenyy: [Elektronnyy resurs] // Positive Technologies. Rezhym dostupu: http://www.ptsecurity.ru/download/PT_Web_application_vulnerability2014_rus.pdf (Data zvernennya: 15.04.2015).

2. Desyat' naybil'sh krytychnykh ryzykiv dlya bezpeky veb-dodatkiv: [Elektronnyy resurs] // OWASP Top 10. Rezhym dostupu: https://www.owasp.org/index.php/Top_10_2013-Top_10 (Data zvernennya: 15.04.2015).

3. Yndyyskyy yssledovatel' spryatal эkployt v pykselyakh kartynky: [Elektronnyy resurs] // SecurityLab.ru by Positive Technologies. Rezhym dostupu: http://www.securitylab.ru/news/473126.php (Data zvernennya: 01.06.2015).

4. Uzun, Y.A. Stehanoanalyz tsyfrovыkh yzobrazhenyy, khranyashchykhsya v proyzvol'nыkh formatakh / Y.A. Uzun // Ynformatyka y matematycheskye metodы v modelyrovanyy. – Odessa. – Tom3,#2. – 2013. – S. 179–189.

5. Rudnytskyy, V.N. Stehanoanalytycheskyy alhorytm dlya yzobrazhenyy, podverhavshykhsya operatsyy szhatyya s poteryamy / V.N. Rudnytskyy, Y.A. Uzun // Zakhyst informatsiyi. – 2013. – Tom 15, # 2. – S. 122–127.

6. Konakhovych, H.F. Komp'yuternaya stehanohrafyya. Teoryya y praktyka / H.F. Konakhovych, A.Yu. Puzыrenko. – K.: «MK-Press», 2006. – 288 s.

7. Ahranovskyy, A.V. Stehanohrafyya, tsyfrovыe vodyanыe znaky y stehoanalyz / A.V. Ahranovskyy, A.V. Balakyn, V.H. Hrybunyn. – M.: Vuzovskaya knyha, 2009. – 220 s.

8. Hrybunyn, V.H. Tsyfrovaya stehanohrafyya / V.H. Hrybunyn, Y.N. Okov, Y.V. Turyntsev. – M.: Solon-Press, 2009. – 272 s.

9. Mitra, S. Steganalysis of LSB Encoding in Uncompressed Images by Close Color Pair Analysis / S. Mitra, T. Roy, D. Mazumdar, A.B. Saha // IIT Kanpur Hackers' Workshop 2004 (IITKHACK04), 23–24 Feb 2004. – 2004. – PP. 23–24.

10.Fridrich, J. Steganalysis of LSB encoding in Color images / J. Fridrich, R. Du, M. Long // IEEE International Conference on Multimedia and Expo. – Vol.3. – 2000. – PP. 1279–1282.

11.Geetha, S. Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images / S. Geetha, S. Sivatha, N. Kamaraj // Transactions on Data Privacy. – Vol.1. – 2009. – PP. 140–161.

12.Tryfonova, K.O. Audyt bezpeky veb-zastosunkiv / K.O. Tryfonova, V.R. Zinovs'kyy // V mizhnarodna naukovo-tekhnichna konferentsiya «ITSEC». – Kyyiv. – 19–22-travnya 2015r. – S. 18–19.

13.Tryfonova, K.O. Audyt vrazlyvosti veb-dodatku zasobamy stehanoanalizu / K.O. Tryfonova, V.R. Zinovs'kyy // Mizhnarodna naukovo-praktychna konferentsiya «Komp"yuterni tekhnolohiyi ta informatsiyna bezpeka». – Kirovohrad. – 2–3-lypnya 2015r. – S. 27.

Рецензент: д.т.н., проф. Кобозєва А.А., зав. кафедри «Інформатики та управління захистом інформаційних систем», Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій, Одеський національний політехнічний університет

д.т.н., доц. Єфименко А.А., Трифонова Е.А., Зиновский В.Р.

АУДИТ СТЕГАНОГРАФИЧЕСКОЙ УЯЗВИМОСТИ ВЕБ-ПРИЛОЖЕНИЯ

В статье рассмотрено выявленную индийским исследователем по информационной безопасности новую уязвимость веб-приложения через цифровые изображения и атаку на веб-приложение, реализованную средствами стеганографии. Предложено модифицированный стеганоаналитический алгоритм, основанный на анализе пар близких и уникальных цветов, реализация программного продукта для аудита уязвимости веб-приложений средствами стеганоанализа. В результате выполнения работы разработан веб-сервис для аудита стеганографической уязвимости веб-приложения. Результаты работы могут быть использованы, как составляющая систем аудита безопасности веб-приложения, выполняющие аудит десяти категорий наиболее распространенных уязвимостей веб-приложений.

Ключевые слова: веб-приложение, аудит, уязвимость, стеганоанализ, близкая пара цветов, уникальная пара цветов.

Prof. Iefimenko A.A, Tryfonova K.O., Zinovskyi V.R.

AUDIT STEGANOGRAPHY WEB APPLICATION VULNERABILITIES

The article considers the revealed by the Indian researcher in information security a new web application vulnerabilities through digital images and an attack on a web application, implemented by means of steganography. Proposes a modified steganoanalysis algorithm based on the analysis of pairs of close and unique colors, the implementation of software for auditing a web application vulnerability by means of steganoalysis. This thesis study presents a web service to audit the steganography web application vulnerabilities. The results can be used as part of security audit web application that perform audit identified ten categories of the most common web application vulnerabilities.

Keywords: web application, audit, vulnerability, steganalysis, close color pair, unique color pair.