УДК 004.4

М. В. Гиндей
В. А. Лужецький

УДОСКОНАЛЕННЯ МЕТОДУ ЗАХИСТУ ЗОБРАЖЕНЬ НА ОСНОВІ РОЗПОДІЛУ СЕКРЕТУ

Вінницький національний технічний університет

Анотація

Розроблено метод та програмний засіб для захисту зображень на основі розподілення секрету. Запропоновано власний метод розподілення секрету, що використовує в якості ключа два молодші біти кожного байту. Розроблено web-додаток, що реалізує розподілення та відновлення секрету.

Ключові слова*: кібербезпека, розподіл зображення, захист зображень, розподілення секрету, вебзастосунок.*

Abstract

Method and software for image protection based on secret distribution has been developed. A proprietary secret allocation method is proposed that uses two lower bits of each byte as a key. A web application has been developed that implements the distribution and recovery of the secret.

Keywords*: cybersecurity, image sharing, image protection, secret sharing, web applications.*

Вступ

Інформація завжди відігравала в житті людей велике значення. І з кожним роком обсяги інформації тільки зростають, і з цим зростанням з'являються нові методи перехоплення та видозмінення інформації. І саме з цієї причини необхідно розробляти нові та вдосконалювати вже існуючі методи захисту інформації від зловмисників.

Метод розподілу секрету між декількома учасниками дозволяє розділити секрет так, що кожен отримує тільки певну частині всієї інформації, таким чином, що одна частина не несе в собі жодної інформації, і для відновлення секрету необхідно об'єднати всі існуючі частини.

Як спосіб розподілу інформації може використовуватись графічний спосіб її представлення, на основі візуальної криптографії.

Візуальна криптографія – це спеціальний метод шифрування, суть якого полягає у прихованні інформації в зображеннях таким чином, що воно може бути розшифровано тільки якщо використовуються правильні ключ-зображення. Перевагою даного методу є те, що він є простим як у реалізації, так як не вимагає спеціального обладнання, а інформація може бути розшифрована людським оком. Процес парольної автентифікації не вимагає зовсім ніяких витрат: він реалізований у більшості програмних продуктів.

Існуючі схеми мають дві складові: розподіл і відновлення секрету. До поділу відноситься формування частин секрету і розподіл їх між членами групи, що дозволяє розділити відповідальність за секрет між її учасниками. Зворотна схема повинна забезпечити його відновлення за умови доступності його зберігачів у деякій необхідній кількості.

Метою роботи є підвищення захисту секрету, що міститься в зображенні, шляхом розробки методу та засобу розподілу секрету.

Результати дослідження

Під час дослідження було розроблено програмний засіб для захисту зображення на основі розподілення секрету. Інтерфейс програмного засобу реалізовано у вигляді веб-застосунку. Було проаналізовано та визначено переваги та недоліки схожих методів захисту зображення, а також оцінено ефективність кожного з методів.

Проаналізовано основні методи розподілу секрету.

Метод чорно-білих зображень передбачає відновлення інформації без втрат, але може застосовуватись тільки для чорно-білих зображень [3].

Перевагою методу кольорових зображень є то, що він застосовується для будь-яких зображень, але відновлення відбувається з втратами.

Метод розподілу зображень за допомогою перетворень Фур'є має відновлення без втрат, застосовується для будь-яких типів зображень, але потребує значних математичних розрахунків при розподілі.

Метод захисту зображення на основі розподілення секрету опирається на молодші біти кожного байту графічного файлу, та розподіляє їх між користувачами.

Дані про розташування пікселів та їх колір зберігаються в масиві пікселів у вигляді масиву.

$$M = [P_0 \quad P_1 \quad P_2 \quad \cdots \quad P_{n-1} \quad P_n]$$

Кожен піксель в матриці має чотири складові:

$$P_i = [PR_{i0} \quad PG_{i1} \quad PB_{i2} \quad PA_{i3}]$$

де: PR_{i0}- значення червоного кольору, PB_{i1}- значення синього кольору,

PG_{i2}- значення зеленого кольору,

PA_{i3}- альфа значення пікселя, i - порядковий номер пікселя в масиві.

Після перетворення зображення в масив пікселів формується новий масив *M**, в який послідовно записуються значення пікселів.

$$M^* = [PR_{00} \quad PG_{01} \quad PB_{02} \quad PA_{03} \quad \ldots \quad PR_{n0} \quad PG_{n1} \quad PB_{n2} \quad PA_{n3}]$$

На рисунку 1 показано схематичне зображення масиву *M** з 20 байтів.

Байт	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
Молодші біти	10	10	11	10	01	00	10	11	11	01

Байт	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}
Молодші біти	00	11	00	11	01	11	10	10	10	00

Рисунок 1 – Схематичне зображення масиву *M** з 20 байтів

Після того як було сформовано масив *M** можна починати формувати масиви *M1*, *M2*, *M3* та *M4*.

Формування масивів користувачів відбувається покроково. На першому кроці (рисунок 2) байт a_0 передається першому користувачу.

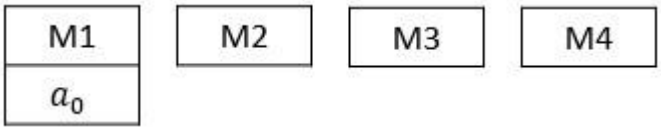

Рисунок 2 – Положення першого байту на першому кроці розподілу зображення

Після того як байт був переданий користувачу, аналізуються молодші біти, і в залежності від їх значення визначається, котрий з користувачів наступним отримає байт.

Після того як всі кроки були виконані формуються фінальні масиви, як показано на рисунку 3.

M1	M2	M3	M4
a_0	a_5	a_1	a_3
a_6	a_{10}	a_2	a_8
a_{11}	a_{15}	a_4	a_9
a_{13}	a_{17}	a_7	a_{12}
	a_{18}		a_{14}
	a_{19}		a_{16}

Рисунок 3 – Значення масивів *M1, M2, M3* та *M4* після останнього кроку розподілу зображення

Для того, щоб відновити зображення необхідно зібрати всі масиви разом. Якщо хоча б один з масивів буде відсутнім, зображення буде неможливо відновити.

Відновлення початкового зображення виконується за оберненим алгоритмом, тобто байти з масивів *M1, M2, M3* та *M4* покроково виймаються та зберігаються в масив *M*, так як показано на рисунку 4.

Байт	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
Молодші біти	10									

M1	M2	M3	M4
a_0	a_5	a_1	a_3
a_6	a_{10}	a_2	a_8
a_{11}	a_{15}	a_4	a_9
a_{13}	a_{17}	a_7	a_{12}
	a_{18}		a_{14}
	a_{19}		a_{16}

Рисунок 4 – Значення масивів *M, M1, M2, M3* та *M4* на першому кроці відновлення зображення

Після виконання останнього кроку з відновлення зображення, можна побачити, що масив *M* був повністю відновлений, а в масивах M1, M2, M3 та M4 більше не залишилось байтів (рисунок 5).

Байт	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
Молодші біти	10	10	11	10	01	00	10	11	11	01

Байт	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}
Молодші біти	00	11	00	11	01	11	10	10	10	00

M1	M2	M3	M4

Рисунок 5 – Значення масивів *M, M1, M2, M3* та *M4* після останнього кроку відновлення зображення

Висновки

У процесі дослідження було розроблено та реалізовано методи і засіб для розподілення та відновлення секрету, було розглянуто та проаналізовано відомі схеми і методи для розподілення та відновлення секрету, а також розглянуто їх переваги та недоліки при формуванні секрету. Під час тестування програмний засіб показав відмінні результати роботи, при обробці різних за розміром та кольоровою гамою зображень, а також відмінні показники під час відновлення зображення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.
2. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.
3. Naor, Moni, and Adi Shamir. "Visual cryptography." Workshop on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg, 1994.
4. Визуальная криптография [Електронний ресурс]. – Режим доступа : URL http://cryptowiki.net/index.php?title=Визуальная_криптография - Назва з екрану.

Гиндей Михайло Васильович *— студент групи 1БС-19м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: hundey@ukr.net*

Лужецький Володимир Андрійович *— професор інформатики, Вінницький національний технічний університет, м. Вінниця*

Hindey Mikhail *- student of group 1BS-19m, Faculty of Information Technology and Computer Engineering,*
Vinnitsa National Technical University, Vinnitsa, e-mail: hundey@ukr.net

Volodymyr Luzhetsky *- Professor of Informatics, Vinnitsa National Technical University, Vinnitsa*