УДК 004.056.55

Гринько Д.В.
Куперштейн Л.М.

ДОСЛІДЖЕННЯ ВІЗУАЛЬНОЇ КРИПТОГРАФІЇ ТА ЇЇ РОЛЬ ДЛЯ БЕЗПЕЧНОГО ЗВ'ЯЗКУ

Вінницький національний технічний університет

Анотація

Досліджено підхід розподілу секрету і, зокрема, здатність візуальної криптографії вирішувати питання безпеки в роботі з зображеннями. Візуальна криптографія являє собою потужний метод, який поєднує в собі поняття шифрування і таємного обміну в криптографії. Однією із ключових особливостей візуальної криптографії є необов'язковість комп'ютера у процесі дешифрування.

Ключові слова: *візуальна криптографія, поділ секрету, шифрування зображення.*

Abstract

Secret sharing approach and in particular visual cryptography try to address the security issues in dealing with images. In fact, visual cryptography is a powerful technique that combines the notions of perfect ciphers and secret sharing in cryptography. No computer participation is required, thus showing one of the distinguishing features of visual cryptography.

Key words: *Visual cryptography, secret sharing, image encryption.*

ВСТУП

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 і може бути розшифрована людським оком. Процес парольної автентифікації не вимагає зовсім ніяких витрат: він реалізований у більшості програмних продуктів. Метою даних досліджень є покращення методу шифрування, шляхом встановлення додаткових засобів безпеки.

ВІЗУАЛЬНА КРИПТОГРАФІЯ

Візуальна криптографія визначається як процес абсолютне шифрування цифрових даних, які можуть бути розкодовані тільки з використанням зорової системи людини [3]. Ця ідея дозволить виводити дані, в нашому випадку зображення, які передаються або зберігаються в цифровій формі, не хвилюючись про те, що дані можуть бути перехоплені і випадково виявлені неуповноваженими особами. Первинне повідомлення кодується в два або більше шарів. Коли дивився на окремі шари, то вони не розкривають ніякої інформації про повідомленні, що міститься в них і нагадують випадковий шум.

Наор і Шамір продемонстрували (k, n) -візуальну схему секретного обміну, де зображення було розбито на n частин, таким чином, що будь-хто, що володів будь-якими k частинами міг розшифрувати його, в той час як будь-які k-1 частин не давали ніякої інформації про зміст вихідного зображення. Коли всі k частини будуть накладені один на одного, ми побачимо вихідне зображення [4].

Алгоритм візуального шифрування має ряд наступних властивостей:

1) незалежність шифрування кожного пікселя;

2) простота вибору матриць;

3) однакові дії для кожного вихідного пікселя;

Легко побачити, що для схеми візуальної криптографії (k, n), алгоритм шифрування зображення має такі властивості:

Якщо візуальна криптографія використовується для безпечного спілкування, то відправник передасть одну або більше копії випадкового шару 1 завчасно одержувачу.

Якщо у відправника є повідомлення, він створює шар 2 для конкретного відправленого шару 1 і передає його одержувачу. Одержувач з'єднує два шари і отримує секретну інформацію. При цьому всьому, йому не потрібно використовувати пристрої розшифрування, робити складні математичні розрахунки, і навіть не обов'язково застосовувати комп'ютер (якщо зображення знаходяться в друкованому вигляді). Система є стійкою до тих пір, поки обидві частини зображення не потраплять в чужі руки. Якщо ж перехоплений тільки один шар, то розшифрування вихідного зображення неможливе.

Як додатковий засіб криптостійкості можливе використання візуальної криптографії на основі стеганографічних методів. Одним із таких методів є приховання шарів у зображенні. Зашифроване зображення виходить накладенням випадкового шуму на картинку з текстом із застосуванням операції XOR або аналогічних, але при цьому використовується робота з матрицями пікселів. Стійкість методу до злому - безумовна, але при цьому потрібні і одноразові ключі. Крім того, відправка шумових графічних повідомлень малоцікава в сучасному світі: навіть якщо у одержувача немає комп'ютера і криптопрограм, сам факт отримання підозрілого шумового графічного повідомлення він приховати не може.

Таким чином, використовуючи спеціально підготовлені на комп'ютері зображення з впровадженим текстом, одержувач, також має ключове зображення у вигляді роздрукованої картинки, може отримати повідомлення від відправника та прочитати його поєднанням аркушів паперу на просвіт, без використання криптографічного або стеганографічного програмного забезпечення.

Даний метод може використовуватися для приховування фактів використання стеганографії, для таємного зберігання або передавання ключів шифрування при загрозі обшуків або оглядів, надсилання коротких повідомлень в умовах листування для осіб, які не мають доступу до комп'ютерів [5].

ВИСНОВОК

Візуальний криптографія є одним з надійних способів передавання і зберігання цифрових даних. Основна перевага візуальної криптографії є те, що не потрібно проводити обчислень для розшифрування кінцевого результату. Це дає можливість тому, хто має мало знань про шифрування, пройти через етап дешифрування легко. Найбільш важливою частиною будь-якої схеми візуальної криптографії є контраст виділеного секрету з певного набору шарів, так як він не буде таким же, як і вихідне зображення. Таким чином є ще можливості для розробки більш ефективних шляхів вирішення цієї проблеми.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Naor, Moni, and Adi Shamir. "Visual cryptography." Workshop on the Theory and Application of of Cryptographic Techniques. Springer Berlin Heidelberg, 1994.
2. Horng, G, Chen, T. and Tasi, D.S. Cheating in Visual Cryptography, Designs, Codes and Cryptography, 2006, pp. 219—236.
3. D. Jin, W.Q. Yan, and M.S. Kankanhalli Charm: Progressive color visual cryptography. In Journal Of Electronic Imaging, 2005.— Vol. 14, Issue 3
4. Feng Liu and ChuanKun Wu. Embedded extended visual cryptography schemes. — China, 2006.
5. От визуальной криптографии к визуальной стеганографии и разделению секрета [Электронний ресурс]. – Режим доступа :https://www.pgpru.com/novosti/2010/otvizualjnojjkriptografiikvizualjnojjsteganografiiirazdelenijusekreta?show_comments=1&p=1#Comment41480

Гринько Дмитро Володимирович— студент групи 1БС-13б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, Україна

Науковий керівник: Куперштейн Леонід Михайлович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет

Hrynko Dmytro — Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University

Supervisor: Kupershtein Leonid — PhD, Associate Professor of Information Protection Chair, Vinnytsia National Technical University