

QR-

Швидкий розвиток і вдосконалення інформаційних технологій призвів до необхідності розробки систем захисту авторського права та систем захисту від копіювання мультимедійної інформації, зокрема, графічних зображень. Практично повсюдне використання мережі Інтернет обертається легкістю доступу до розміщеної в ній інформації. Тому для захисту графічних зображень та авторських прав актуальними є методи стеганографії. В статті розглянуто спосіб накладання цифрового водяного знаку. Запропоновано метод вставки в зображення QR коду в якості інструменту захисту авторських прав. Використання даного методу має на меті покращити захист зображень та запобігти несанкціонованому доступу до них.

Ключові слова: графічні зображення, стеганографія, цифровий водяний знак, QR-код, iWatermark.

S.V. KULYK, M.V. LYUTA

Kyiv National University of Technologies and Design

I.O. ROZLOMIY

Cherkasy Bohdan Khmelnytsky National University

STUDYING OF THE TECHNIQUES OF A QR-CODE USING TO PROTECT GRAPHIC IMAGES

The rapid development and improvement of information technology has led to the need to develop copyright protection systems and protection systems against the copying of multimedia information, in particular, graphic images. Virtually widespread use of the Internet is rotated by the ease of access to the information contained therein. Therefore, steganography methods are relevant to protect graphic images and copyrights. The article considers the method of digital watermarking. The method of inserting of QR-code into image as a copyright protection tool is proposed. The purpose of this method is to improve the protection of images and prevent unauthorized access to them.

Keywords: graphic images, steganography, digital watermark, QR-code, iWatermark.

. В наш час одним із способів захисту графічних зображень є стеганографія. Стеганографія – це спосіб передачі або зберігання інформації з урахуванням збереження в таємниці самого факту такої передачі (зберігання). На відміну від криптографії, яка приховує вміст таємного повідомлення, стеганографія приховує сам факт його існування. Як правило, повідомлення буде виглядати як що-небудь інше, наприклад, як зображення, стаття, список покупок або лист. Стеганографію зазвичай використовують спільно з методами криптографії, таким чином, доповнюючи її.

Перевага стеганографії над чистою криптографією полягає в тому, що повідомлення не привертають до себе уваги. Таким чином, криптографія захищає вміст повідомлення, а стеганографія захищає сам факт наявності будь-яких прихованих послань. Основним методом приховування інформації є цифровий водяний знак (ЦВЗ) [1].

Цифровий водяний знак – це спеціальна мітка, вбудована в цифровий контент (названий контейнером) з метою захисту авторських прав і підтвердження цілісності самого документа. ЦВЗ можна вбудовувати в електронні документи будь-якого типу [2, 3]. Поряд з різними зображеннями (фотографіями, малюнками, відсканованими паперовими документами і т.д.) зустрічаються і аудіозаписи, що несуть в собі ЦВЗ, і відео (наприклад, DVD-диски). ЦВЗ активно використовуються при розміщенні унікальних фотографій, відео, аудіотреков в електронному вигляді в глобальній мережі Інтернет. В якості ЦВЗ також може використовуватись QR код.

QR-код – товарний знак для типу матричних штрих-кодів (або двовимірних штрих-кодів), спочатку розроблених для автомобільної промисловості Японії. Штрих-код – це оптична мітка, що містить інформацію про об'єкт, до якого вона прив'язана [4].

Система QR-кодів стала популярною за межами автомобільної промисловості завдяки можливості швидкого зчитування і більшій місткості в порівнянні зі штрих-кодами стандарту UPC. Такі коди включають відстеження продукції, ідентифікацію предметів, відстеження часу, управління документами і загальний маркетинг.

QR-код складається з чорних квадратів, розташованих у квадратній сітці на білому тлі, які можуть зчитуватися за допомогою пристроїв обробки зображень, таких як камера, і оброблятися з використанням кодів Ріда – Соломона до тих пір, поки зображення не буде належним чином розпізнано. Потім необхідні дані витягуються з шаблонів, які присутні в горизонтальних і вертикальних компонентах зображення.

. Звичайні водяні знаки не зможуть забезпечити високий рівень захисту закодованої інформації. QR-код в цьому плані виділяється більшою надійністю та захищеністю. Наносити зображення QR-коду можна з різною прозорістю, кольором, розміром для мінімізації спотворень зображення. QR-код дозволить вирішити проблему забезпечення достовірності зображення та гарантії авторства.

. Досить багато публікацій присвячено розгляду проблеми забезпечення достовірності, гарантії авторства графічних зображень. Завданням пошуку ефективних механізмів захисту графічних зображень займалися такі вчені: Д.А. Нікулін, Ю.А. Белобокова, О.О. Євсютін, О.В. Негацова та інші. В працях Д.А. Нікуліна досліджено особливості нанесення цифрового водяного знаку на графічні зображення з метою захисту авторських прав [5]. Також варто відмітити роботи Ю.А. Белобокової, в яких запропоновано методи вбудовування ЦВЗ в цифрові фотографії [6]. Проте, ще залишаються питання, які потребують подальшого доопрацювання та вивчення. Зокрема, до тепер мало уваги приділялося застосуванню технології нанесення QR-коду для захисту графічних зображень.

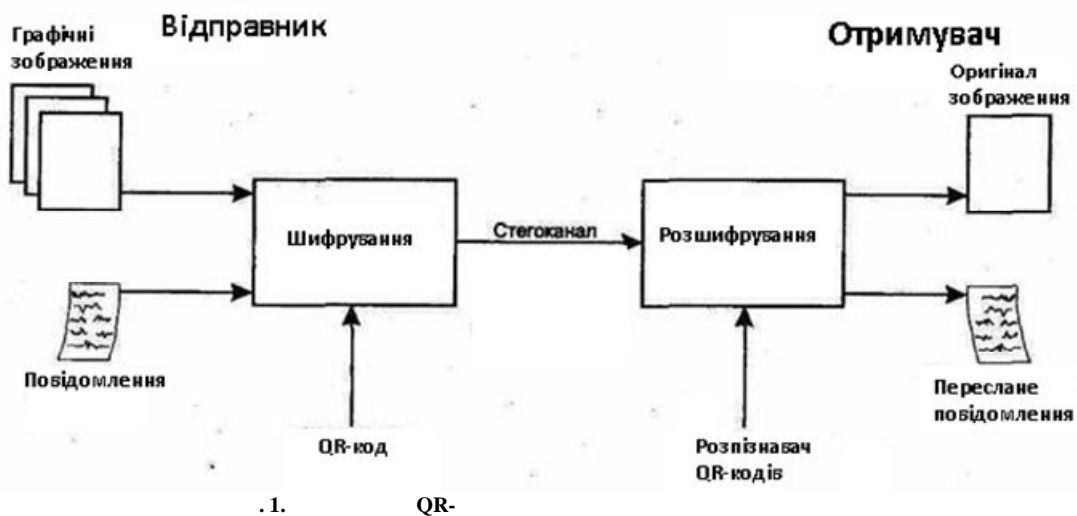
. Метою роботи дослідження принципів нанесення QR-коду для захисту графічних зображень від несанкціонованого доступу та захисту авторських прав.

. Програмне забезпечення, призначене для захисту авторських прав на графічні роботи, складає інтерес для фахівців, що займаються дизайном, фотографією, графікою і т.п., яким необхідно, з одного боку, представляти свої роботи потенційному замовнику, а з іншого боку, бути застрахованими від можливого порушення авторських прав, пов'язаного з незаконним використанням їх робіт.

Інтернет і авторські права не сумісні між собою в принципі. Сучасне авторське право до сих пір побудовано на праві автора заборонити використання твору, що в інтернеті неможливо в силу природи мережі. Інтернет – це свобода, авторське право – це обмеження. Всі проблеми виходять з цього фундаментального протиріччя. З використанням мережі відбуваються найрізноманітніші правопорушення:

- плагіат;
- незаконна торгівля об'єктами прав інтелектуальної власності;
- торгівля контрафактною продукцією через інтернет-магазини.

В даний час автори змушені представляти портфоліо, яке часто містить зменшені цифрові зображення, якість яких спеціально занижено, що не дозволяє в повній мірі оцінити їхні переваги. У зв'язку з цим, додаток, що дозволяє надати зображення в оригінальному форматі, але без можливості їх копіювання, представляє значний практичний інтерес для широких кіл фахівців, що працюють в області дизайну, фотографії, digital art і т.д.



Програма для захисту графічних файлів має швидко працювати з великими обсягами інформації (якісні графічні файли мають великий обсяг) і забезпечувати контроль доступу до цієї інформації. При цьому зображення не повинно бути доступно в незахищеному вигляді ні на одному з етапів його передачі.

Схему накладання QR-коду у вигляді цифрового водяного знаку показано на рис. 1.

QR-код з'явився в 1994 році в Японії. Створений дослідниками Denso-Wave (дочірня компанія «Toyota»), цей двовимірний, або матричний, штрих-код застосовувався спочатку для ідентифікації автозапчастин на заводах корпорації, але швидко знайшов популярність за межами виробничих ліній. Абревіатура QR означає Quick Response, тобто «Швидкий відгук». Особливість даного типу кодів в тому, що вони легко розшифровуються не тільки за допомогою спеціального сканера, але і за допомогою будь-якого смартфона, оснащеного фотокамерою і досить простим програмним забезпеченням, що відкриває завидні перспективи його застосування в повсякденному житті. Хоча термін QR код як і раніше є зареєстрованим товарним знаком DENSO Corporation, використання кодів не обкладається жодними ліцензійними відрахуваннями, а самі вони описані і опубліковані в якості стандартів ISO.

У QR-коді кодується різноманітна інформація, яка складається із символів (включаючи кирилицю, цифри і спеціальні символи), наприклад: електронна візитка, координати місця розташування, інтернет-адреса, контактні дані, адреса електронної пошти, SMS, текст, телефонні номери. Один QR-код може містити цифри – 7089, цифри і букви (Латиниця) – 4296, двійковий код – 2953 байт (отже, близько 2953

літер кирилиці в кодуванні windows – 1251 або близько 1450 літер кирилиці в utf-8), ієрогліфи – 1817.

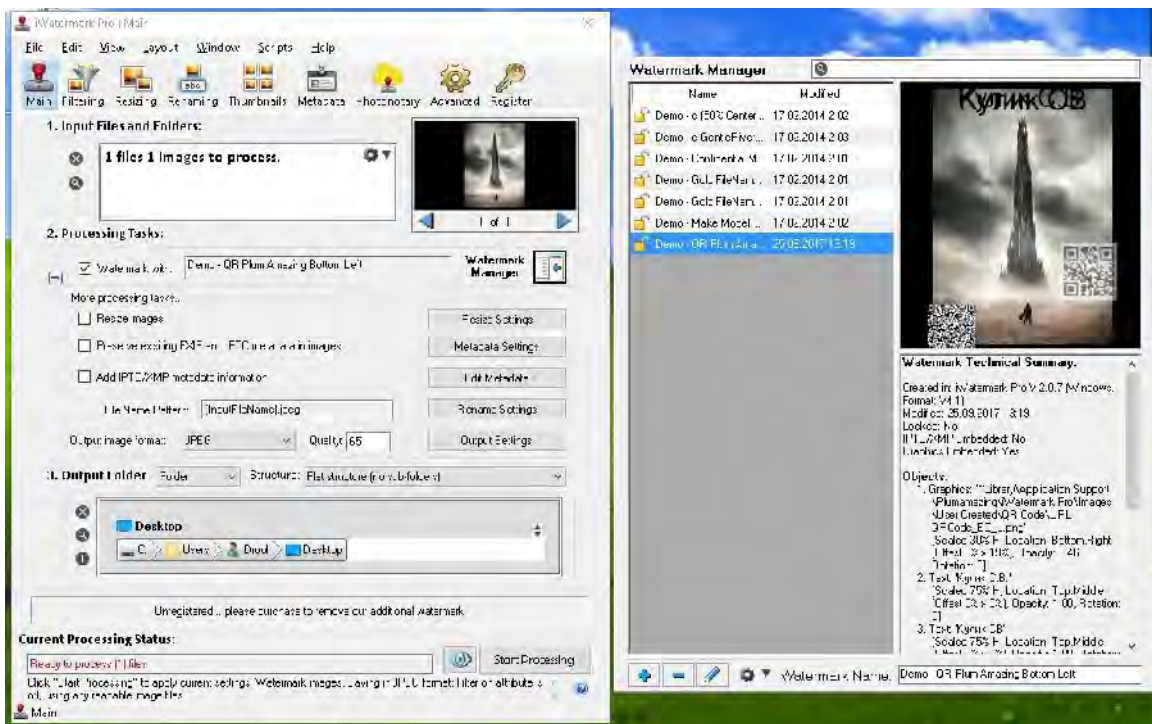
Вигляд так структура QR-коду зображено на рис. 2.

Зараз існує багато різних програм для вбудовування водяних знаків різного типу. Для вбудовування qr-коду в графічне зображення можна використати програму iWatermark, яка дозволить вбудовувати в графічні зображення водяні знаки. Однією з функцій цієї програми є також і генерування в QR-коду та вбудовування його в зображення. iWatermark Pro для Mac та Windows може працювати з Lightroom, Photoshop, Picasa, ACDSee, Cumulus, Portfolio, PhotoStation, Xee, iView, PhotoMechanic та іншими організаторами фотографій.

Спочатку користувач вільний обирати який тип водяного знаку він хоче використовувати для захисту зображення. Типи водяних знаків та програма зображені на рис. 3. В даному випадку обираємо водяний знак у вигляді QR-коду.



. 2.

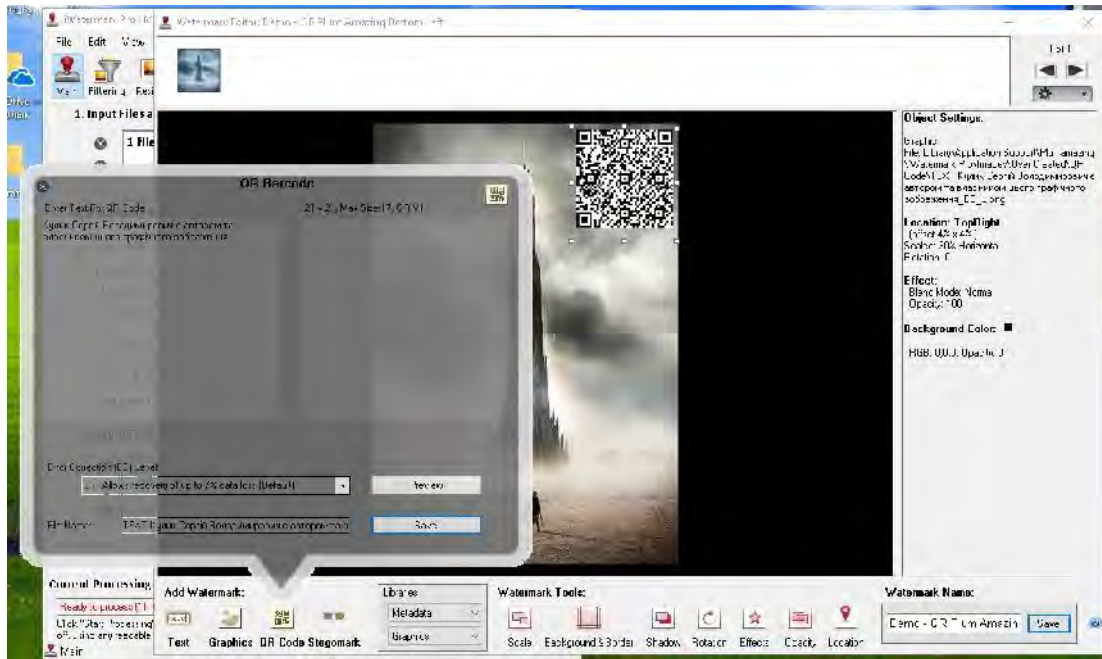


. 3.

Далі користувач може надрукувати будь-який текст, який буде закодований у QR-коді. Також він може вибрати розмір коду, прозорість та його розташування на зображенні. Це зображено на рис. 4. Також на рис. 5 зображено різні види QR-коду, які пропонує програма на вибір користувачеві.

iWatermark – це один з найпростіших і в той же час досить багатофункціональних інструментів для додавання друкованих водяних знаків в малюнки, цифрові фотографії та інші зображення. Програма підтримує всі поширені формати зображень і дозволяє додати до знімків і підпис, і логотип, в тому числі одночасно. Для тексту допустимо зміна шрифту, його розміру і накреслення, а для логотипу, якщо він задіяний разом з текстом, можна вибрати положення відносно тексту: над текстом, під текстом, ліворуч або праворуч від нього. Крім того, для водяного знаку можна визначити ступінь прозорості (в тому числі зробити його невидимим), положення на знімку, повернути його під будь-яким кутом, змінити розмір і

накласти один з ефектів: тінь, обведення, карбування та ін. При бажанні можна, наприклад, пустити логотип через все зображення, багато разів повторюючи його в певному порядку. При цьому iWatermark не буде переписувати оригінальні файли, а просто створить послідовну копію зображення в попередньо зазначеній папці. Програма підтримує пакетну обробку файлів, однак в демонстраційній версії дана можливість не працює.



. 4. , QR-



. 5. QR-

Після обробки маємо зображення з готовим нанесеним QR-кодом на зображенні. Готове зображення показано на рис. 6.



. 6.

QR-

. В даній роботі було розкрито особливості захисту графічних зображень за допомогою стеганографії, зокрема цифрового водяного знаку. Було розглянуто використання QR-коду в якості ЦВЗ. Було визначено що QR-код є більш ефективним методом захисту авторських прав на графічні зображення. В якості програми, що вставляє в зображення розглянутий код, використовувався додаток iWatermark. З її допомогою можна ефективно вставляти в зображення не тільки QR-коди, а й інші цифрові водяні знаки. Дана програма є простим і водночас ефективним методом захисту графічних зображень.

1. Коханович Г.Ф. Компьютерная стеганография. Теория и практика / Коханович Г.Ф., Пузыренко А.Ю. – Киев : МК-Пресс, 2006. – 288 с.
2. Стеганография, цифровые водяные знаки и стегоанализ / Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. – М. : Вузовская книга, 2009. – 220 с.
3. Cox, I.J. Digital watermarking and steganography / I.J. Cox, M. Miller, J. Bloom, J. Fridrich. – San Francisco : Morgan Kaufmann Publishing, 2008. – 624 p.
4. Wang S. Does a QR-code must be black and white? // 2015 International Conference on Orange Technologies (ICOT). – IEEE, 2015. – pp. 161–164.
5. Никулин Д.А. Особенности применения машиночитаемых ЦВЗ для защиты авторских прав на изображение / Д.А. Никулин // Таврический научный обозреватель. Технические науки. – 2016. – № 7(12). – С. 137–140.
6. Грачева Ю.А. (Белобоква). Применение цифровых водяных знаков для защиты цифровых фотографий / Ю.А. Грачева // Новые информационные технологии в автоматизированных системах : материалы 14 научно-практ. семинара. – М. : МИЭМ, 2011. – С. 52–57.

References

1. Kokhanovich, G.F. and Pusyrenko, A.Y. (2006) Computer steganography. Theory and practice. Kiev: MK-Press, 288 p.
2. Agranovsky, A.V., Balakin, A.V., Gribunin, V.G. and Sapozhnikov, S.A. (2009) Steganography, digital watermarks and steganalysis. Moscow: University book, 220 p.
3. Cox, I., Miller, M., Bloom, J. and Fridrich, J. (2008) Digital watermarking and steganography. San Francisco: Morgan Kaufmann Publishing, 624 p.
4. Wang S. (2015) Does a QR-code must be black and white? International Conference on Orange Technologies (ICOT). IEEE, pp. 161–164.
5. Nikulin D.A. (2016) The peculiarities of the use of machine-readable digital photo frames for the protection of copyright of images. Taurian Scientific Observer. Technical sciences, 7 (12), pp. 137–140.
6. Gracheva Yu.A. (Belobokova) (2011) Using of digital watermarks to protect digital photos. New information technologies in automated systems. Materials of 14 scientific and practical workshops. Moscow: MIEM, pp. 52–57.

Рецензія/Peer review : 06.09.2017 p.

Надрукована/Printed :26.10.2017 p.