УДК 004.932.2

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 361-368

МЕТОД ЗАХИСТУ QR-КОДУ З ВИКОРИСТАННЯМ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ

О.В. Наріманова, Д.М. Семенченко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: semejka@ua.fm

В роботі розроблено новий метод нанесення та вилучення цифрового водяного знаку для захисту контенту QR-коду, що може бути використаний для перевірки цілісності та автентичності QR-коду після його зчитування за допомогою мобільного пристрою з паперового носія. На основі розробленого методу реалізовано програмний продукт для мобільного пристрою на операційній системі Windows Phone.

Ключові слова: цифровий водяний знак, QR-код, автентифікація, перевірка цілісності

Вступ

Постійне збільшення об’ємів інформації, що необхідно отримувати, аналізувати, обробляти та зберігати, призводить до появи нових інформаційних технологій. В роботі чи на відпочинку, вдома чи закордоном, людина звикла покладатися на мобільні пристрої, GPS-навігатори, отримувати бажану інформацію у будь-який час з Інтернету, інших пристроїв чи просто зчитувати її мобільним телефоном з QR-кодів [1]. На сьогоднішній день QR-коди набули такого широкого використання, що майже вся друкована інформація (рекламні та інформаційні плакати, етикетки різноманітних виробів, оголошення тощо) дублюється за допомогою QR-кодів чи супроводжується ними.

Проте, як відомо, новітні технології (особливо інформаційні) можуть бути використані і проти людини та її прав. У сьогоденні стало розповсюдженим таке явище соціальної інженерії як фішинг [2]. Суть махінацій полягає у заміні оригінального QR-коду іншим кодом, який після зчитування телефоном видає користувачеві неправдиву інформацію (приклад недобросовісної конкуренції) чи наводить останнього на web-сторінку зловмисника, що може призвести до крадіжки та/або втрати конфіденційної та персональної інформації.

Отже, використання технології QR-коду потребує залучення технологій забезпечення інформаційної безпеки. Однією з таких технологій є нанесення цифрового водяного знаку (ЦВЗ).

Мета та задачі дослідження

Метою даної роботи є розробка методу автентифікації та перевірки цілісності QR-коду за допомогою ЦВЗ.

Для досягнення мети роботи були поставленні наступні задачі:

1) Провести аналіз існуючих методів, що використовують ЦВЗ, та сформулювати основні вимоги до методу автентифікації та перевірки цілісності QR-коду;

2) Розробити метод для автентифікації та перевірки цілісності QR-коду, що використовує ЦВЗ, згідно з основними вимогами;

3) Реалізувати програмний продукт нанесення та перевірки ЦВЗ для QR-коду;

4) Провести обчислювальний експеримент для визначення точних значень параметрів розробленого методу для забезпечення виконання сформульованих вимог для організації захисту контенту QR-коду.

Основні вимоги до методу автентифікації та перевірки цілісності QR-коду за допомогою цифрового водяного знаку

QR-код (абревіатура розшифровується як *Quick Response* – «швидкий відгук») – це матрична двовимірна картинка, в якій знаходиться зашифрована інформація набагато більшого розміру, ніж вміщується в звичайний штрих-код. За допомогою QR-коду можна закодувати будь-яку інформацію, наприклад: текст, номер телефону, посилання на сайт або візитну картку. Навівши на код камеру телефону, користувач отримує закодовану інформацію на екрані. Зчитуються QR-коди за допомогою мобільного телефону, в який вбудована фотокамера і є спеціальне програмне забезпечення (спеціальний додаток для мобільних пристроїв – QR-reader).

У загальному вигляді QR-код поділяється на декілька зон, основні з яких виділені на рис. 1.

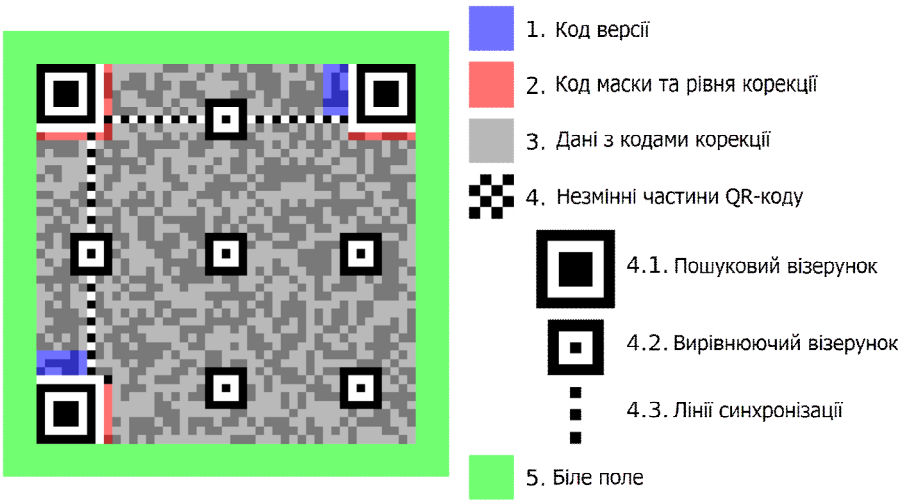

Рис. 1. Схема нанесення інформації на QR-код

З урахуванням правил формування QR-коду сформулюємо основні загальні вимоги до методу автентифікації та перевірки його цілісності за допомогою ЦВЗ. Повідомлення ЦВЗ має обиратися з урахуванням, що його довжина обмежена зверху значенням кількості байтів в QR-коді. При нанесенні цифрового водяного знаку має бути збережена (за можливості) візуальна стійкість, тобто цифровий водяний знак не повинен бути помітним для ока людини. Проте метод нанесення ЦВЗ має бути стійким до процесів друку та зчитування камерою телефону. Візуальною стійкістю можна поступитися на користь високого відсотку вірно декодованого повідомлення ЦВЗ за умови, що розпізнавання QR-коду не буде порушено. Отже, коротко основні вимоги до методу автентифікації та перевірки цілісності QR-коду можна сформулювати наступним чином:

1) Довжина повідомлення ЦВЗ не повинна перевищувати довжину повідомлення QR-коду;

2) Нанесений ЦВЗ не повинен перешкоджати зчитуванню QR-коду стандартними засобами;

3) Розроблений метод, що використовує ЦВЗ, має бути стійким до процесів друку та зчитування камерою телефону та (за можливості) задовольняти умові візуальної стійкості.

З урахуванням сформульованих основних вимог був проведений аналіз відомих технік та методів ЦВЗ.Найбільш поширеними та відомими робастними методами ЦВЗ є методи Куттера-Джордана-Боссена, Коха і Жао та їхні модифікації [3-6]. Проте вони не забезпечують ефективності вилучення повідомлення ЦВЗ після друку стеганоповідомлення на паперовому носії та зчитування камерою телефону. Тому постає задача розробки нового методу для захисту контенту QR-коду, враховуючи особливості його представлення і, насамперед, вимогу стійкості до процесів друку та зчитування камерою телефону. При розробці нового методу перевага надається роботі в просторовій області зображення, оскільки робота в частотній області вимагає додаткових обчислень та не гарантує стійкості до такого значного збурного впливу як процес друку та зчитування камерою.

Метод захисту контенту QR-коду, що використовує цифровий водяний знак

Було визначено, що найбільш доцільним для вирішення поставленої в роботі задачі є нанесення ЦВЗ на QR-код шляхом зміни значення яскравості пікселів матриці QR-коду. При цьому для підвищення стійкості повідомлення ЦВЗ до збурних дій пропонується корекція значення усіх трьох компонент зображення QR-коду: R – червоної, G – зеленої, B – блакитної. Далі необхідно визначити, які саме пікселі будуть підпадати корекції, та за яким правилом ця корекція буде виконуватися.

При формуванні QR-коду кожному біту інформації ставиться у відповідність всього один білий або чорний піксель у зображенні, проте при друці зображення QR-коду масштабується для того, щоб QR-код можна було прочитати камерою телефону. Для можливості нанесення ЦВЗ пропонується після формування QR-коду (до друку) кожному пікселю зображення поставити у відповідність 9 пікселів того ж кольору як показано на рисунку 2. Далі сукупність 3×3 пікселів будемо називати «квадрат» QR-коду.

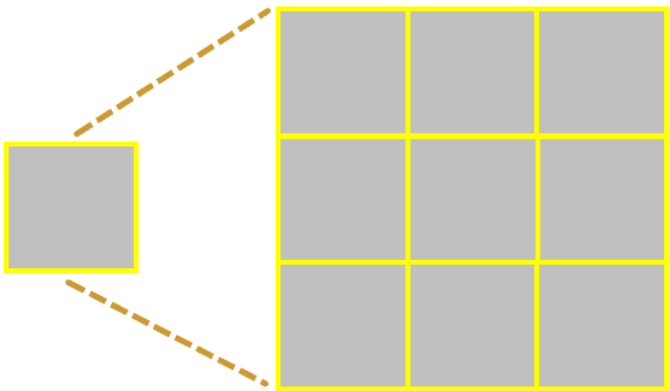

Рис. 2. Формування квадрату QR-коду для одного пікселя

Після такого масштабування QR-коду будемо проводити нанесення ЦВЗ шляхом модифікації середнього пікселя кожного квадрату 3×3.

Зауваження 1. Заміна саме середнього пікселя при зчитуванні ЦВЗ має певні переваги. По-перше, незначна корекція яскравості тільки одного з дев'яти пікселів не завадить зчитуванню безпосередньо повідомлення QR-коду стандартними засобами. По-друге, наявність корекції яскравості середнього пікселя навіть після збурного впливу можна встановити, проаналізувавши оригінальні значення сусідніх пікселів, бо первісно вони мають той самий колір.

Зауваження 2. Таке правило визначення пікселів, що підлягають корекції своїх значень, на перший погляд, дає пропускну здатність алгоритму 1/9 біт на піксель. Проте по відношенню до первісного (ще до масштабування) зашифрованого у QR-код повідомлення маємо пропускну здатність 1 біт на піксель.

Отже, було отримане правило, за яким визначаються пікселі, що підлягають корекції своїх значень. Далі необхідно визначити правило, за яким буде виконуватися корекція значень пікселів QR-коду. Пропонується наступне.

Нехай необхідно нанести повідомлення ЦВЗ, яке має послідовність біт $\{1,1,0,0\}$. Нанесення виконується на фрагмент QR-коду, який до масштабування за кожною з компонент $\{R,G,B\}$ приймає значення $\begin{Bmatrix}255,0\\255,0\end{Bmatrix}$. На рис. 3 представлена схема такого нанесення ЦВЗ.

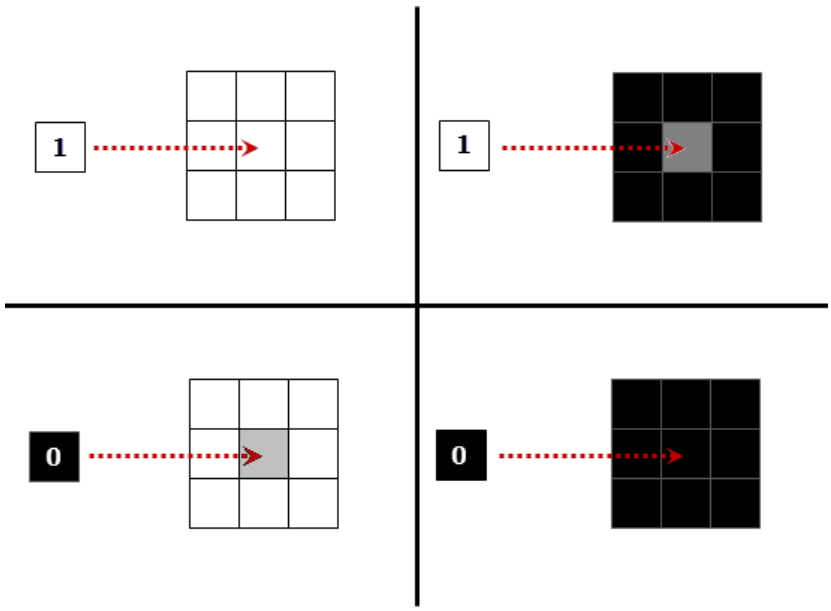

Рис. 3. Корекція значень квадрату QR-коду в залежності від біту повідомлення ЦВЗ, що вбудовується

Таким чином, корекція значення середнього пікселя квадрату QR-коду на деяке значення $\pm\Delta$ необхідна тільки у двох випадках з чотирьох: при вбудовуванні одиниці в квадрат чорних пікселів $(+\Delta)$ та нуля в квадрат білих пікселів $(-\Delta)$. Корекція значення середнього пікселя квадрату QR-коду для кожної з компонент $\{R,G,B\}$ в цих випадках виконується за наступною формулою:

$$\overline{p}_{i,j}=\begin{cases}p_{i,j}-\Delta, & p_{i,j}=255;\\ p_{i,j}+\Delta, & p_{i,j}=0.\end{cases} \qquad (1)$$

де

$p_{i,j}$ та $\overline{p}_{i,j}$ — значення яскравості середнього пікселя квадрату QR-коду до та після корекції відповідно;

Δ — значення корекції, деяке невід'ємне значення з інтервалу $(0,127)$.

Вилучення кожного біту ЦВЗ виконується у відповідності з формулами:

$$\overline{\Delta} = \frac{p_{i-1,j-1} + p_{i-1,j} + p_{i-1,j+1} + p_{i,j-1} + p_{i,j+1} + p_{i+1,j-1} + p_{i+1,j} + p_{i+1,j+1}}{8} - p_{i,j};$$

$$m_k = \begin{cases} 1, & \overline{\Delta} \le -\Delta, \overline{\Delta} + p_{i,j} \le 127; \\ 0, & \overline{\Delta} > -\Delta, \overline{\Delta} + p_{i,j} \le 127; \\ 0, & \overline{\Delta} \ge \Delta, \overline{\Delta} + p_{i,j} > 127; \\ 1, & \overline{\Delta} < \Delta, \overline{\Delta} + p_{i,j} > 127, \end{cases} \quad (2)$$

де

$p_{i,j}$ — значення яскравості середнього пікселя квадрату QR-коду після зчитування;

Δ — значення корекції з формули (1);

m_k — вилучений k-й біт ЦВЗ.

Отже, можемо визначити основні кроки алгоритмів нанесення та вилучення цифрового водяного знаку для QR-коду.

Основні кроки алгоритму нанесення ЦВЗ:

1) визначити послідовність та довжину повідомлення ЦВЗ;

2) визначити послідовність пікселів, в які буде виконуватись вбудування ЦВЗ;

3) послідовно виконати корекцію значень пікселів QR-коду, якщо це необхідно, за формулою (1).

Основні кроки алгоритму вилучення ЦВЗ:

1) визначити послідовність пікселів зображення для вилучення ЦВЗ;

2) обчислити значення біту вбудованої інформації за формулами (2).

В даному розділі представлена розробка методу ЦВЗ для захисту контенту QR-коду та наведені основні кроки алгоритмів нанесення та вилучення повідомлення цифрового водяного знаку. Для можливості практичної реалізації розробленого методу необхідно визначити таке значення корекції Δ, яке задовольняло би сформульованим у першому розділі вимогам: нанесений ЦВЗ не повинен перешкоджати зчитуванню QR-коду стандартними засобами; метод ЦВЗ має бути стійким до процесів друку та зчитування камерою телефону та (за можливості) задовольняти умові візуальної стійкості. У наступному розділі описана програмна реалізація алгоритмів нанесення та вилучення ЦВЗ для QR-коду, описаний обчислювальний експеримент та представлені його результати для визначення значення корекції Δ та перевірки стійкості розробленого методу до зазначених збурних дій.

Програмний продукт для захисту контенту QR-коду

Для програмної реалізації розроблених алгоритмів нанесення та вилучення ЦВЗ для QR-коду було обрано мобільну операційну систему Windows Phone, враховуючи розповсюдженість та перспективи розвитку мобільних пристроїв саме з цією операційною системою. Реалізація програмного продукту була проведена з використанням набору інструментів Microsoft Visual Studio 2010 Express for Windows Phone. Формування та зчитування QR-коду проводилося за допомогою стандартної для цієї задачі бібліотеки ZXing [7].

Нижче наведений приклад роботи та інтерфейс створеного програмного продукту (див. рис. 4, 5).

Рис. 4. Нанесення ЦВЗ на сформований QR код з подальшим його збереженням

Рис. 5. Відкриття QR-коду та вилучення повідомлення ЦВЗ

При проведенні обчислювального експерименту використовувалися різні значення корекції Δ з проміжку від 1 до 127. При цьому фіксувалися можливість зчитування QR-коду стандартними засобами і відсоток вірно вилученої інформації

повідомлення ЦВЗ, а також оцінювалася візуальна стійкість. При проведенні обчислювального експерименту було визначено, що для коректної та ефективної роботи програмного продукту на мобільному пристрої необхідна камера з роздільною здатністю не менше 8.0 мегапікселів. Основні результати обчислювального експерименту представлені в табл. 1.

Таблиця 1.

Результати обчислювального експерименту з використання камери з роздільною здатністю 8.7 мегапікселів

Діапазон значень корекції Δ	Можливість зчитування QR-коду стандартними засобами	Відсоток вірно вилученої інформації повідомлення ЦВЗ, %	Дотримання вимоги візуальної стійкості
$1 \div 9$	+	ЦВЗ не отримано	+
$10 \div 90$	+	100	–
$91 \div 127$	–	100	–

За представленими результатами значення корекції $\Delta = 10$ було обране для використання в алгоритмах нанесення та вилучення ЦВЗ як таке, що менше за всі порушує візуальну стійкість і при цьому задовольняє вимогам зчитування QR-коду стандартними засобами і дає 100% вірно вилученої інформації повідомлення ЦВЗ.

Висновки

В роботі розроблено новий метод нанесення та вилучення цифрового водяного знаку для захисту контенту QR-коду, що дозволяє перевіряти цілісність та автентичність QR-коду після його зчитування за допомогою мобільного пристрою з паперового носія.

В процесі розробки методу та програмного продукту на його основі були враховані особливості формування та змісту QR-кодів, а також наступні вимоги:

1) Можливість зчитування QR-коду стандартними засобами без наявного спеціалізованого програмного додатку, розробленого в даній роботі;

2) Ефективність вилучення ЦВЗ після зчитування роздрукованого на паперовому носії QR-коду камерою мобільного пристрою;

3) Незначні порушення візуальної стійкості після нанесення ЦВЗ, що є прийнятним для робастного методу ЦВЗ.

Розроблений в роботі програмний продукт для генерації QR-коду та нанесення на нього ЦВЗ може бути рекомендований для використання власними та часними підприємствами, державними установами та банками, які використовують QR-коди в будь-яких цілях. При цьому доцільним може бути використання асиметричних криптографічних алгоритмів для шифрування повідомлення ЦВЗ до його нанесення на QR-коду. Програмний продукт для зчитування і перевірки автентичності та цілісності QR-коду може бути розповсюджений у вільному доступі тим підприємством, що зацікавлений у захищеності своєї інформації або продукції і, як наслідок, своїх клієнтів.

Список літератури

1. What is a QR-code? : *[Електронний ресурс]* // QRCode.com. DENSO WAVE Incorporated. Режим доступу: http://www.qrcode.com/en/about/ (Дата звернення: 11.11.2013 р.)
2. Понимание киберпреступности: Руководство для развивающихся стран : *[Електронний ресурс]* // Международный союз электросвязи. Отдел приложений ИКТ и кибербезопасности. Департамент политики и стратеги. Сектор развития электросвязи МСЭ. Режим доступу: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf (Дата звернення: 11.11.2013 р.)
3. Хорошко, В.О.Основи комп'ютерної стеганографії: Навч. посіб. для студ. і асп. / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук; Нац. авіац. ун-т. — Вінниця, 2003. — 143 с.
4. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
5. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
6. Защелкин, К.В. Усовершенствование метода стеганографического скрытия данных Куттера-Джордана-Боссена / К.В. Защелкин, А.И. Иващенко, Е.Н. Иванова // Радіоелектронні і комп'ютерні системи. — 2013. — № 5(64). — С. 151–155.
7. ZXing barcode for Windows Phone : *[Електронний ресурс]* // CodePlex. Project Hosting for Open Source Software. Режим доступу: http://zxingwindowsphone.codeplex.com/ (Дата звернення: 11.11.2013 р.)

МЕТОД ЗАЩИТЫ QR-КОДА С ИСПОЛЬЗОВАНИЕМ ЦИФРОВОГО ВОДЯНОГО ЗНАКА

Е.В. Нариманова, Д.М. Семенченко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: semejka@ua.fm

В работе представлен новый метод нанесения и извлечения цифрового водяного знака для защиты контента QR-кода, который может быть использован для проверки целостности и аутентичности QR-кода после его считывания при помощи мобильного устройства с бумажного носителя. На основе разработанного метода реализован программный продукт для мобильного устройства на операционной системе Windows Phone.

Ключевые слова: цифровой водяной знак, QR-код, аутентификация, проверка целостности

DIGITAL WATERMARKING APPROACH FOR QR-CODE PROTECTION

Olena V. Narimanova, Daria M. Semenchenko

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: semejka@ua.fm

In this paper a new approach of digital watermarking for QR-code protection is developed. This approach can be used for authentication and integrity checking of QR-code after its reading with mobile device from paper. On the basis of proposed approach a software application for mobile device on Windows Phone is implemented.

Key words: digital watermarking, QR-code, authentication, integrity checking