ỨNG DỤNG MÃ QR VÀ CHỮ KÝ SỐ TRONG PHÒNG CHỐNG GIẢ MẠO VĂN BẰNG, CHỨNG CHỈ Ở DẠNG BẢN IN

APPLICATION OF QR CODE AND DIGITAL SIGNATURES TO THE PROCESS OF PREVENTING THE FORGERY OF PAPER-BASED DIPLOMAS AND CERTIFICATES

Nguyễn Thành Thủy
Trường Đại học Kinh tế - Đại học Đà Nẵng
Email: thuynt@due.edu.vn

TÓM TẮT

Tình trạng giả mạo các loại văn bản, tài liệu quan trọng trên giấy như bằng cấp, chứng chỉ và các loại văn bản pháp lý khác ngày càng nghiêm trọng và tinh vi hơn. Với các mục đích lừa đảo, chiếm đoạt tài sản, xin việc làm, bổ nhiệm chức vụ,… nhằm qua mặt các cơ quan công quyền, điều này đã dẫn đến những thiệt hại to lớn về vật chất cũng như sự suy giảm về niềm tin và gây nhiều bất ổn trong xã hội.Trong bài báo này, chúng tôi đề xuất một giải pháp có tính khả thi cao trong việc phát hiện và phòng chống giả mạo các loại văn bằng, chứng chỉ, giấy tờ pháp lý,… được xuất bản ở dạng bản in. Giải pháp được đề xuất, ứng dụng công nghệ mã vạch 2 chiều QR kết hợp với chữ ký số,sử dụng thuật toán mật mã hóa khóa công khai (RSA) giúp việc mã hóa, giải mã và xác minh thông tin trên văn bản in một cách chính xác,an toàn và nhanh chóng với các thiết bị điện thoại thông minh hay đầu đọc mã vạch.

Từ khóa: mã QR; thuật toán RSA; chữ ký số; khóa bí mật; khóa công khai; trung tâm chứng thực chữ ký số; hàm băm.

ABSTRACT

Forgery of important paper-based documents such as diplomas, certificates and other legal documents is more and more serious and sophisticated. For the purposes of fraud, appropriation of property, job application assignment and authority swindle, this has led to material loss, belief deterioration as well as social instability. This paper proposes a feasible solution to the forgery of paper-based diplomas, certificates and legal documents. With the application of QR bidirectional barcode and digital signatures and the usage of RSA algorithm, this proposed solution makes encryption, decryption and verification of information in a text on smart phones and barcode readers done correctly, safely and quickly.

Key words: QR Code; RSA algorithm; Digital signature; Private Key; Public Key; Root-CA; Hash function.

1. Đặt vấn đề

Trong những năm gần đây, tình trạng giả mạo tài liệu, giấy tờ (*ở dạng bản in*) nhằm mục đích lừa đảo ngày càng gia tăng. Lợi dụng sự phát triển của khoa học công nghệ; sự sơ hở trong công tác quản lý của các cơ quan, tổ chức; cộng với sự thiếu hiểu biết của mỗi cá nhân; các đối tượng phạm tội đã tạo ra nhiều giấy tờ, tài liệu giả mạo để thực hiện các hành vi lừa đảo gây ra những thiệt hại to lớn. Nhiều giấy tờ giả mạo giống đến mức nếu không có phương tiện kỹ thuật và nghiệp vụ chuyên môn thì khó lòng phát hiện được. Vì vậy, số nạn nhân các vụ lừa đảo bằng giấy tờ tài liệu giả vẫn không ngừng tăng lên.

Một số loại giấy tờ thường hay bị giả mạo như: các loại giấy tờ tùy thân (*giấy phép lái xe, CMND, giấy khám sức khỏe, visa…*), các loại giấy tờ chứng minh sở hữu tài sản (giấy tờ đất đai, nhà cửa,…), các loại bằng cấp (*bằng đại học, cao đẳng, chứng chỉ ngoại ngữ, tin học,…*), đến các loại văn bản, quyết định của các cấp có thẩm quyền.

Thủ đoạn phổ biến, dễ thực hiện và có thể tạo ra với số lượng nhiều loại giấy tờ, tài liệu giả của các đối tượng là dùng phần mềm thiết kế, xử lý hình ảnh để làm giả tài liệu, hình dấu trên máy vi tính rồi in ra giấy in ảnh, giấy cứng. Đặc biệt, khó phát hiện hơn cả là việc các đối tượng sử dụng phôi, mẫu giấy tờ, tài liệu thật của cơ quan, tổ chức, rồi làm giả nội dung, chữ ký và con dấu; hoặc tẩy toàn bộ nội dung trên giấy tờ thật nhưng

vẫn giữ nguyên chữ ký và hình dấu, sau đó thiết kế bản in trên máy vi tính và in giả lại toàn bộ nội dung. Vì vậy nạn nhân không chỉ là cá nhân mà còn là các tổ chức, cơ quan và việc phát hiện tội phạm thường quá muộn.

Trong bài báo này, chúng tôi đề xuất một giải pháp có tính khả thi về công nghệ vàmang lại hiệu quả kinh tế cao, nhằm khắc phục triệt để tình trạng giả mạo các loại văn bằng, chứng chỉ, giấy tờ pháp lý trong xã hội.

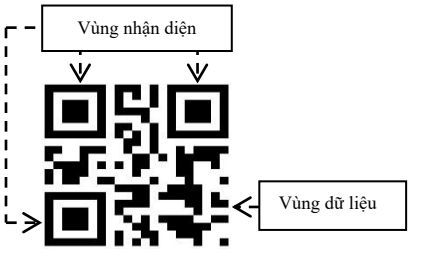
2. Cơ sở của việc nghiên cứu

Ngày nay, với sự phát triển nhanh chóng của khoa học công nghệ, điện thoại thông minh (ĐTTM) ngày càng trở nên phổ biến, cùng với sự phát triển của hạ tầng viễn thông, mạng Internet, 3G,… ĐTTM đã trở thành thiết bị giải trí hàng đầu trong thế giới công nghệ.

2.1. Công nghệ mã vạch 2 chiều QR Code

QR là từ viết tắt của Quick Response ("*Mã phản hồi nhanh*") hay còn gọi là mã vạch ma trận (*matrix-barcode*) là dạng mã vạch hai chiều (*2D*) được phát triển vào năm 1994 bởi công ty Denso Wave, Nhật Bản. Mã QR (*QR code*) có thể được đọc bởi máy đọc mã vạch hay ĐTTMcó chức năng chụp ảnh với phần mềm để quét mã vạch, trong đó sử dụng thuật toán sửa lỗi Reed-Solomon [1].

QR code gồm những module màu đen, được xắp xếp theo những quy luật nhất định trong một ô vuông có nền trắng. Sự tổ hợp những module này đã mã hóa cho rất nhiều loại dữ liệu, bao gồm: link dẫn đến trang web, hình ảnh, thông tin, chi tiết về sản phẩm, quảng cáo cho sản phẩm.



Hình 1. *Cấu trúc của QR Code*

Các QR code nhỏ nhất là 21x21 pixel, và lớn nhất là 177x177, mỗi mẫu có kích thước khác nhau đó được gọi là một phiên bản [2].

Khả năng sửa lỗi: ***Khả năng lưu trữ dữ liệu:*** **[2]**

Chuẩn	Sửa lỗi
L	7%
M	15%
Q	25%
H	30%

Loại dữ liệu	Lưu trữ
Numeric	7,089 ký tự
Alphanumeric	4,296 ký tự
Nhị phân	2,953 bytes
Kanji/Kana	1,817 ký tự

Các loại định dạng dữ liệu QR code có khả năng mã hóa:

- Địa chỉ URL
- Văn bản (Text)
- Hình ảnh (Images)
- Số điện thoại
- Tin nhắn (SMS)
- Thông tin liên hệ (Contact details)
- Vị trí địa lý (Geo-location)
- Mật khẩu truy cập Wifi
- Địa chỉ email
- Thông tin cá nhân trên mạng xã hội
- Thông tin sự kiện (Events)
- Địa chỉ download,…

2.2. Chữ ký số và thuật toán khóa công khai

Chữ ký số (*Digital Signature*) là một dạng chữ ký điện tử. Chữ ký số được tạo ra bởi người ký đóng vai trò như chữ ký đối với cá nhân hay con dấu đối với doanh nghiệp và được thừa nhận về mặt pháp lý. Chữ ký số dựa trên công nghệ mã khóa công khai (*RSA*).

Việc kiểm tra là so sánh tính đồng nhất của khóa bí mật trên chữ ký số của người gửi đến, với khóa công khai được lưu trữ trên hệ thống máy chủ của nhà cung cấp dịch vụ chứng thực chữ ký số (*Root Certification Authority – Root CA*) [3].

Hiện nay ở Việt Nam và nhiều quốc gia trên thế giới, đã thừa nhận tính pháp lý của chữ ký số và được ứng dụng nhiều trong các hoạt động giao dịch điện tử.

2.3. Hàm băm

Hàm băm (*Hash function*) là giải thuật nhằm sinh ra các giá trị băm tương ứng với mỗi khối dữ liệu, giá trị băm đóng vai trò gần như một khóa để phân biệt các khối dữ liệu. Hiện nay, hàm băm được sử dụng các thuật toán mã hóa dữ liệu có độ an toàn cao như MD5, SHA-2. Hàm băm được sử dụng cho nhiều ứng dụng bảo mật thông tin như chứng thực hay kiểm tra tính nguyên vẹn của thông điệp [3].

2.4. Các kỹ thuật truyền thống trong phòng chống giả mạo

2.4.1. Nhận dạng bằng phương pháp trực quan

Dựa vào kiến thức và kinh nghiệm của người kiểm soát về đặc điểm, hình dáng, kích thước, màu sắc, dấu vết của một số loại giấy tờ từ đó phát hiện ra các tài liệu thật giả.

2.4.2. Sử dụng tem chống giả mạo

Tem chống giả Hologram: được sản xuất bằng công nghệ laser hiện đại không dùng mực in. Màu sắc của tem là màu tán sắc ánh sáng biến đổi theo từng góc quan sát. Tem bám chắc đều trên bề mặt các sản phẩm và sẽ tự phá huỷ nếu bóc ra để tái sử dụng [4].

Tem chống giả Decal vỡ: sử dụng công nghệ phát quang và công nghệ nhiệt. Khi cho bề mặt tem tiếp xúc với nhiệt độ thì màu sắc và hình ảnh của tem sẽ thay đổi. Khi bóc tem sẽ vỡ thành từng mảnh nhỏ [5].

Hình 2*. Tem kỹ thuật số*

Hình 3*. Tem Decal vỡ*

Tem chống giả kỹ thuật số: tem sử dụng công nghệ chống giả bằng mã PIN, in lên tem một dẫy các mã số bí mật dưới lớp phủ. Người dùng xác minh sản phẩm bằng cách kiểm tra mã PIN thông qua tổng đài thoại, qua tin nhắn hoặc tra cứu trực tuyến trên website [6].

2.5. Một số kết quả nghiên cứu và ứng dụng QR code trong bảo mật dữ liệu

Nhờ có ưu điểm là dễ dàng được tạo ra và được đọc bởi các ĐTTM ở mọi lúc, mọi nơi nên QR code có thể được sử dụng để xác thực định danh người dùng [7], hay kết hợp với chữ ký điện tử để xác minh nguồn gốc của văn bản [8].

Với cấu trúc đặc biệt, QR code đã mang lại một khả năng mã hóa thông tin với dung lượng lớn, đồng thời cho phép người sử dụng có thể định nghĩa lại các module cấu trúc QR code, theo các quy tắc riêng với mục đích mã hóa và che dấu các dữ liệu thực [9].

3. Đề xuất giải pháp xác thực tài liệu sử dụng QR code

Giải pháp được đề xuất nhằm xác thực các loại giấy tờ là văn bằng và chứng chỉ (*sau này được gọi tắt là văn bản*) ở dạng in. Trong đó, sử dụng hệ thống mã vạch hai chiều QR, kết hợp chữ ký số dựa trên thuật toán mã hóa bất đối xứng RSA.

Trong đó, phạm vi của giải pháp được giới hạn cho các loại văn bản có tính duy nhất, Cụ thể bao gồm các loại giấy tờ là văn bằng hay chứng chỉ, chẳng hạn như: bằng tốt nghiệp, giấy phép lái xe (*GPLX*), chứng minh nhân dân, hộ chiếu,… thông tin trên các loại văn bản thường đơn giản, cô đọng và xác định rõ danh tính của cá nhân và tổ chức sở hữu hay phát hành văn bản.

3.1. Mô tả giải pháp

Trọng tâm của giải pháp tập trung vào việc tạo và xác thực tính hợp pháp của QR code được in trên văn bản. Giải pháp được tóm lược như sau:

Bước 1: Rút trích thông tin đặc trưng của văn bản;

Bước 2: Tạo QR code từ: các thông tin đặc trưng, kết hợp với chữ ký số của đơn vị phát hành văn bản;

Bước 3: In QR code lên văn bản;

Bước 4: Người dùng sử dụng thiết bị đọc mã vạch hoặc ĐTTM có phần mềm được thiết kế riêng trong việc xác thực QR code này.

3.2. Giải pháp xác thực tài liệu

Bảng 1. *Danh mục các từ viết tắt*

Từ	Ý nghĩa
SI	Specific Information: thông tin đặc trưng
PK	Private Key: Khóa bí mật
QK	Public Key: Khóa công khai
DS	Digital Signature: chữ ký số
$\mathbf{E_{PK}}$	Hàm mã hóa dữ liệu với thuật toán RSA
$\mathbf{D_{QK}}$	Hàm giải mã dữ liệu với thuật toán RSA
H()	Hàm băm

3.2.1. Giải thuật sinh QR code

Bước 1: Trích thông tin đặc trưng SI của văn bản (*được thực hiện thủ công*);

Bước 2: Tạo chữ ký số DS, bằng cách kết hợp giữa PK của đơn vị phát hành với SI của văn bản, sử dụng hàm băm H() và hàm mã hóa E_{PK} của thuật toán RSA. Ta có DS: E_{PK}(H(SI), PK);

Bước 3: Tạo QR code từ cặp thông tin (DS,SI);

Bước 4: In QR code lên văn bản.

Giải thuật sinh QR code được mô tả trong Hình 4.

3.2.2. Giải thuật xác thực QR code

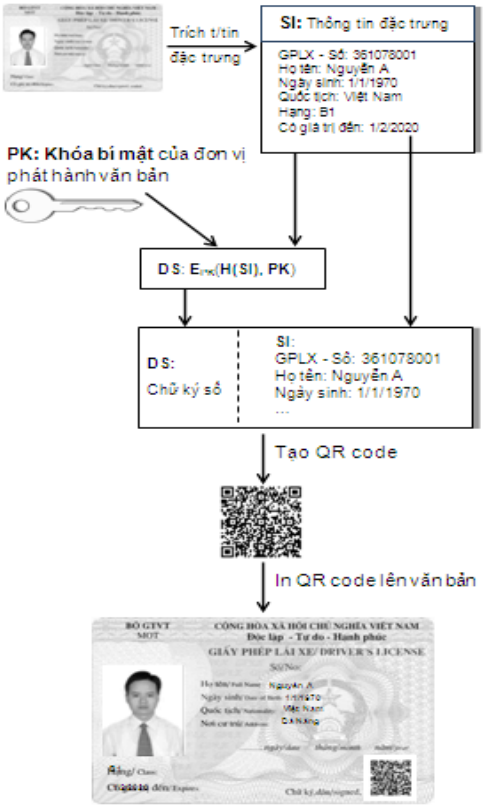
Bước 1: Sử dụng đầu đọc mã vạch hay ĐTTM để quét QR code trên tài liệu cần xác minh. Trích ra DS và SI của văn bản;

Bước 2: Giải mã DS bằng cách sử dụng hàm giải mã D_{PK} của thuật toán RSA, kết hợp với khóa công khai (QK) của đơn vị phát hành văn bản (*được lưu trữ tại Root-CA*). Ta có DecValue: D_{QK}(DS,QK);

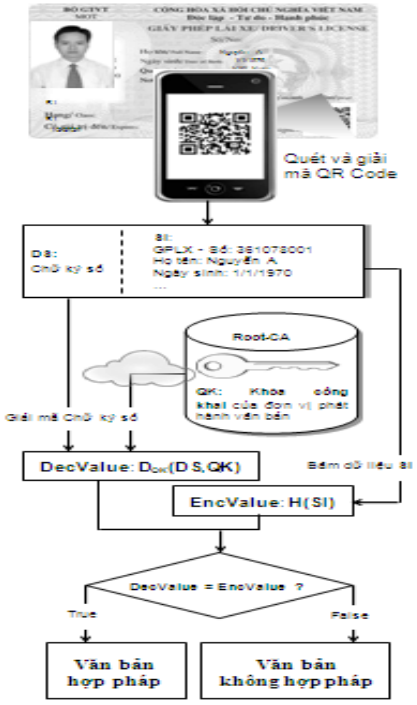
Bước 3: Dùng hàm H() để băm thông tin SI, ta có EncValue: H(SI);

Bước 4: Đối chiếu cặp giá trị DecValue và EncValue; nếu khớp nhau thì QR code này là hợp pháp (*nghĩa là văn bản này có giá trị pháp lý và được cấp bởi một cơ quan có thẩm quyền*).

Để phát hiện việc sửa đổi thông tin trên văn bản, người xác minh cần đối chiếu nội dung trên văn bản với thông tin SI (*được tiến hành thủ công*).



Hình 4*. Giải thuật sinh QR code*



***Hình 5**. Giải thuật xác thực QR code*

4. Phân tích và đánh giá tính khả thi của giải pháp

Trong phần này, chúng tôi phân tích tính hiệu quả và chất lượng bảo mật của giải pháp được đề xuất so sánh với các phương pháp xác thực và phòng chống giả mạo văn bản truyền thống.

4.1. Phân tích các yếu tố bảo an của giải pháp

Ví dụ đối với một GPLX, thông tin trên đó được xác định chính xác và là duy nhất cho một công dân, bao gồm: họ tên, ngày sinh, quê quán, hình ảnh nhân dạng, số giấy phép, hạng, thời hạn giá trị, đơn vị phát hành giấy phép,…

Toàn bộ thông tin đặc trưng (SI) được trích rút từ văn bản (*thông tin thể hiện tính duy nhất đối với những văn bản đồng loại*), sau đó được mã hóa và đính kèm chữ ký số (DS) được tạo bởi PK của đơn vị phát hành văn bản. Nội dung của PK do đơn vị phát hành văn bản quản lý, nên chữ ký số được tạo ra có độ tin cậy cao bởi thuật toán RSA.

Mã vạch QR được tạo ra từ cặp thông tin (DS+SI) và được in lên văn bản. Để chứng minh một văn bản là hợp pháp và đã được phát hành bởi một đơn vị có thẩm quyền, người xác minh chỉ cần sử dụng đầu đọc mã vạch hay ĐTTM có phần mềm được thiết kế đặc biệt.

Tất nhiên, QR code này (*cũng giống những QR code thông thường khác*) có thể được đọc và giải mã bởi bất kỳ phần mềm đọc QR code thông dụng. Điểm đặc biệt của phần mềm chúng tôi đề xuất ở đây là có khả năng xác minh được chữ ký số kèm theo trong QR code là hợp pháp.

Chữ ký số được xác minh bằng cách kết hợp với QK của đơn vị phát hành. PK và QK là một cặp khóa duy nhất được tạo bởi thuật toán tạo khóa RSA, do một Root-CA có uy tín và thẩm quyền cấp phát và lưu giữ (*chẳng hạn như Trung tâm chứng thực chữ ký số quốc gia Bộ Truyền thông và Thông tin*). Và cho đến nay, độ an toàn cao của chữ ký số đã được nhiều công trình khoa học chứng minh.

Chúng ta thử phân tích một số tình huống có thể làm giả mạo văn bản:

- Trường hợp người giả mạo sử dụng một khóa PK khác (*không phải của đơn vị phát hành văn bản*) để tạo chữ ký số, trong trường hợp này chữ ký số sẽ không được chứng thực bởi khóa QK còn lại thuộc sở hữu của đơn vị phát hành văn bản.

- Trường hợp người giả mạo sử dụng hình ảnh của một QR code hợp pháp để in lên một văn bản không hợp pháp: lúc này, QR code sẽ được xác minh là hợp lệ, tuy nhiên người xác minh có thể đối chiếu thông tin SI (*được đọc từ mã QR*) với nội dung được in trên văn bản để phát hiện giả mạo.

- Trường hợp người giả mạo thay đổi nội dung trên một văn bản hợp pháp: lúc này, chữ ký số sẽ được chứng thực nhưng người xác minh có thể phát hiện nội dung bị thay đổi bằng cách đối chiếu với thông SI.

4.2. So sánh yếu tố bảo an với các giải pháp khác

Qua phân tích, chúng tôi nhận thấy giải pháp được đề xuất có yếu tố bảo an cao hơn so với những giải pháp được trình bày ở mục 2.4. (*trong giới hạn phát hiện và chống giả mạo các loại văn bản được nêu ở mục 3.*)

Phương pháp xác thực bằng trực quan: dựa chủ yếu vào kinh nghiệm của người xác minh, có

tính rủi ro cao, mang nặng cảm tính,… chỉ có khả năng phát hiện nhưng không thể ngăn ngừa giả mạo ở mức độ cao.

Các phương pháp xác thực bằng tem chống giả: tem được sản xuất bằng các công nghệ hiện đại, dễ nhận diện bằng mắt thường để phát hiện thật giả, nhưng người giả mạo vẫn có thể tạo ra những mẫu tem tương tự. Đặc biệt, đối với phương pháp này, chúng ta không thể phát hiện được những nội dung bị chỉnh sửa tinh vi trên các văn bản thật.

Giải pháp được tác giả đề xuất, có tính an toàn cao về bảo mật (*dựa vào độ tin cậy của chữ ký số*), khả năng làm giả QR code gần như là không thể. Đặc biệt khả năng phát hiện những thông tin bị chỉnh sửa trên văn bản bằng cách đối chiếu nội dung trên văn bản với thông tin đặc trưng SI.

Với khả năng tự sửa lỗi đến 30% (*với chuẩn H*) [2], dữ liệu lưu trữ trên QR code dễ dàng được phục hồi ở mức cho phép khi bị phai mờ trong quá trình sử dụng của văn bản.

4.3. Phân tích tính hiệu quả

Giải pháp được đề xuất đã mang lại hiệu quả cao về mặt kinh tế. Việc tạo một QR code có chữ ký số và in QR code lên văn bản với một chi phí thấp nhất và dễ thực hiện, không đòi hỏi các thiết bị và công nghệ phức tạp so với sử dụng tem chống giả.

Ngoài ra, đơn vị sử dụng giải pháp cần đăng ký với một cơ quan hữu quan để sở hữu một chữ ký số, có giá trị pháp lý cho việc chứng thực QR code.

Chỉ cần một thiết bị ĐTTM được kết nối với mạng Internet, bất kỳ ai cũng có thể dễ dàng xác minh được tính hợp pháp của một văn bản ở bất kỳ nơi đâu, vào bất kỳ lúc nào.

5. Kết luận

Bài báo thực hiện việc nghiên cứu và đề xuất một giải pháp mới, ứng dụng công nghệ mã vạch 2 chiều QR kết hợp với chữ ký số giúp việc mã hóa, giải mã và xác minh thông tin trên văn bản in một cách chính xác, an toàn và nhanh chóng với các thiết bị ĐTTM hay đầu đọc mã vạch. Đối tượng nghiên cứu được giới hạn trong phạm vi xác minh và phát hiện giả mạo đối với các loại văn bằng, chứng chỉ, giấy tờ pháp lý,… ở dạng bản in.

Kết quả nghiên cứu của bài báo mở ra một hướng mới trong việc ứng dụng chữ ký số trên văn bản in kết hợp với QR code.

TÀI LIỆU THAM KHẢO

[1] Prepared by the Association of Nova Scotia Museums (2013), "*QR Code How-To Guide*", Canadian Heritage Information Network (CHIN).

[2] Peter Kieseberg, Manuel Leithner (2010), "*QR Code Security*", SBA Research Favoritenstrasse 16 AT-1040 Vienna, Austria.

[3] Phạm Nguyên Khang (2013), "*Giáo trình An toàn và bảo mật thông tin*", ĐH Cần Thơ.

[4] Huy Vũ Label, "*Tem chống giả Hologram*", *http://tembaohanh.com/inan/frame/products_category/id/214/tem-chong-gia-hologram.html* (truy cập ngày 10/1/2015).

[5] Trung tâm KTTLNV- Bộ Công An, "*Tem chống hàng giả decal vỡ sử dụng công nghệ phát quang*", *http://temchonghanggiasg.com/tem-chong-hang-gia/tem-chong-hang-gia-decal-vo-su-dung-cong-nghe-phat-quang.html* (truy cập ngày 10/1/2015).

[6] Công ty TNHH Công nghệ chống giả DAC, "*Tem chống giả kỹ thuật số", http://www.temchonggia.com.vn/Desktop.aspx/Giai-phap-cong-nghe/Tem-chong-gia-ky-thuat-so/Tem_chong_gia_ky_thuat_so/*(truy cập ngày 10/1/2015).

[7] Young-Gon Kim, Moon-Seog Jun (2011), "*A Design of User Authentication System Using QR code*

Identifying Method", 2011 6th International Conference on, IEEE Conference Publications.

[8] Maykin Warasart, Pramote Kuacharoen (2012), "*Paper-based Document Authentication using Digital Signature and QR Code*", 2012 4TH International Conference on Computer Engineering and Technology.

[9] Somdip Dey, Asoke Nath (2013), "*Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System*", 2013 International Conference on, IEEE Conference Publications.