ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/102071, October 2016* ISSN (Online) : 0974-5645

An Efficient QR-code Authentication Protocol using Visual Cryptography for Securing Ubiquitous Multimedia Communications

M. Gayathri[1*], A. John Blesswin[1] and G. Selva Mary[2]

[1]Department of Computer Science and Engineering, SRM University, Kattankulathur, Chennai - 603203, Tamil Nadu, India;gayathri.ma@ktr.srmuniv.ac.in, johnblesswin.a@ktr.srmuniv.ac.in
[2]Department of Information Technology, SRM University, Kattankulathur, Chennai - 603203, Tamil Nadu, India;selvamary.g@ktr.srmuniv.ac.in

Abstract

Background: Now a day, data communication plays a vital role in day-to-day life. There is a strong desire to develop and implement more secure authentication protocol to protect secret information against security threats. **Method:** The paper proposes a Quick Response (QR) code Authentication Protocol (QRAP) using Visual Cryptography. Visual Cryptography (VC) is a model of cryptography split the secret into share images, which prevents the secret image from being altered by using the concepts of the cipher and can reconstruct the secret image by stacking the legitimate share images. **Findings:** The passwords for authentication are encoded as QR-codes and later encrypted into colour share images. Thus, the colour share images by itself convey no information, but when the shares are combined, the secret password can be revealed. The necessary is that the user needs to handle a device containing a QR-code reader, most probably a Smartphone. The experimental result shows that the proposed QRAP scheme provides secure data communication with less computational complexity. **Applications/Improvement:** This research work can give a way for providing authentication to all services which are related to electronic devices.

Keywords: QR Codes, Security, Visual Cryptography, Visual Secret Sharing

1. Introduction

Recent Internet technology ranges from low-speed applications to high-speed multimedia applications. Naor and Shamir scheme[1] describes the principles of Visual Secret Sharing (VSS) to generate two shares by the perfect combination of black and white pixels according to the secret image. K out of N Visual Cryptography schemes but unable to get any secret information by stacking a less number of favorable shares[2]. Multi-secret scheme[3] is to share more than one secret image in two random shadows. Image Size Invariant Visual Cryptography scheme[4] minimized the size of share images, by invariant visual secret sharing scheme. Young-Chang scheme[5] describes that different cover images can be used for hiding secret images and has focused on the image quality of the share images. Visual protection scheme concentrated on the verification of encryption scheme of content protection and the techniques were proposed for handheld devices based on video coding but failed to work on authentication during transmission of videos. Optimal Contrast Grayscale Visual Cryptography Scheme satisfied user requirements and proposed a technique to use a minimum number of shares, it was given only for grayscale images and half-tone images and not for colour images[7]. A Lossless Tagged Visual Cryptography Scheme uses k-1 specific shares and embedding tag images to improve the contrast[8]. our proposed QRAP Will focus on improving better contrast for the colour images and thereby increase the quality of the colour image. The method called binocular VCS for secure data transmission, and it provided an optimization

* *Author for correspondence*

model for the improvement of quality[9]. The Novel Visual Cryptography without pixel expansion scheme focused only on the improvement of the quality of halftone images by the technique called extended VC, did not focus on the colour images[10]. The schemes[5–10]are applied to grayscale and colour images, which uses to carry out the work of generating shares with higher efficiency.

2. Materials and Methods

The proposed work focuses on making improvement in the authentication ability using VC. The QRAP proposes an introduced system of sharing the QR images for authentication using Visual Cryptography. The basic idea is to authenticate between two devices, and the proposed method describes three phases. First, share generation phase, each connecting device creates the QR secret image which is same as of the original, cover images and creates the share images. Second is the Service Request Phase. In this, one device sends the service request to the other device. Another device accepts the request and both devices exchange their share images to each other. Finally, confirmation phase, which reveals the secret QR image from the two share images that say, from the one share it already has and the one received from the other device by using XOR operation and checks with the secret image. Figure 1 shows a complete illustration of QRAP protocol.

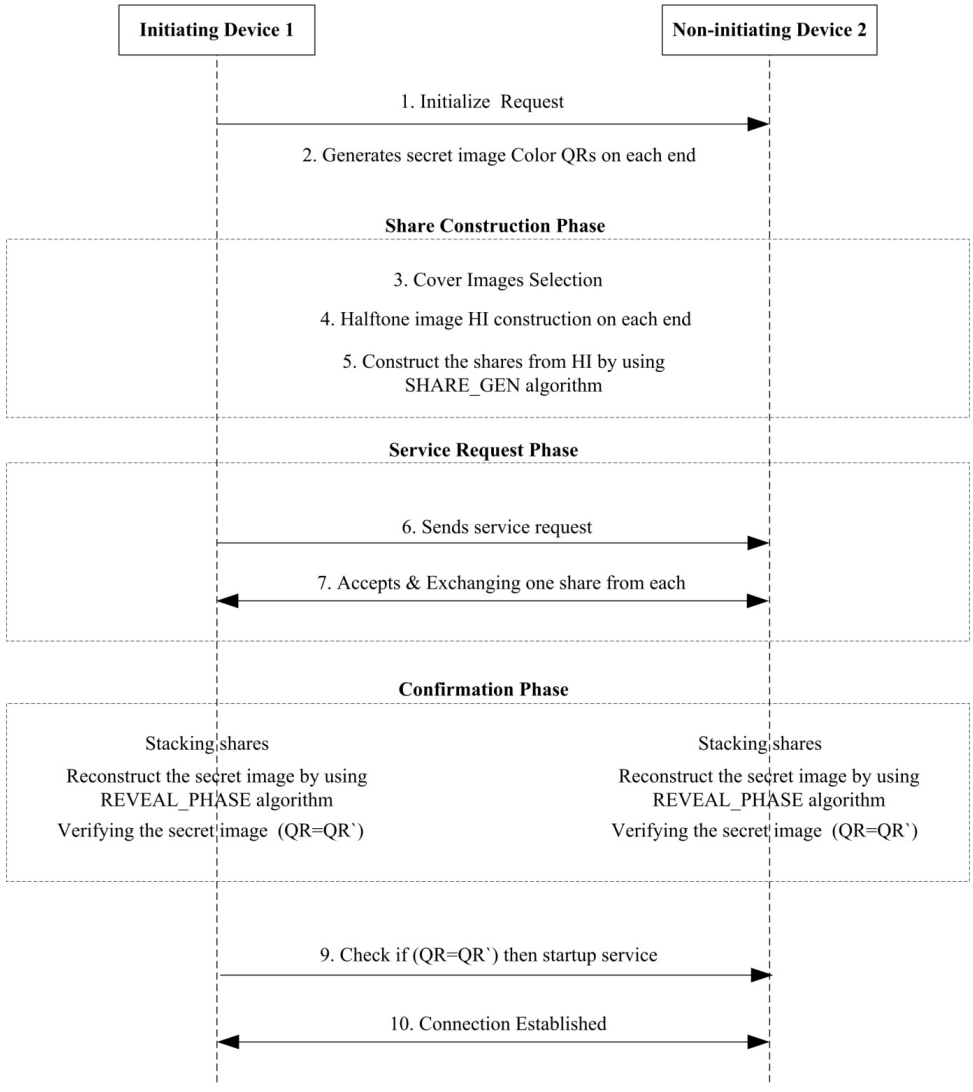


Figure 1. Block diagram of QRAP protocol.

2.1 Share Construction Phase

Input: The secret QR colourimage I and cover image CI_1, CI_2.

Output: Shares generated S_1, S_2.

Step 1: Consider secret QR colour image (I) and multi-channel (colour) image as the cover up images CI_1 and CI_2; then,

$$[I] \rightarrow RGB \rightarrow I^R, I^G, I^B$$

$$[CI_1] \rightarrow RGB \rightarrow CI_1^R, CI_1^G, CI_1^B$$

$$[CI_2] \rightarrow RGB \rightarrow CI_2^R, CI_2^G, CI_2^B$$

$$I, CI_1, CI_2 \in \{0,1,2,3\ldots,255\}$$

Step 2: Construct a half-tone image (HI) by applying the error diffusion technique on the secret QR colour image;

$$I^R, I^G, I^B \rightarrow ED \rightarrow HI^R, HI^G, HI^B$$

Step 3. Construct the shares S1and S2from HI by using SHARE_GEN algorithm; now, S1 and S2 shares will have the pixel expansion of three and assures that the secret information can be restored completely after stacking from the shares. Shares are delivered to the receiver[10].

Algorithm 1: Shares Generation

For specified matrix CI^1, CI^2 and HIof size (m × n).

Then shares S_1 and S_2 be empty (unfilled) as size of m × 3n.

function_SHARE_GEN (HI, CI^1, CI^2)
I^R, I^G, $I^B \leftarrow$ I
$CI_1^R, CI_1^G, CI_1^B \leftarrow CI_1$
$CI_2^R, CI_2^G, CI_2^B \leftarrow CI_2$
S_1^R, $S_2^R \leftarrow$ ISHARE (I^R, CI_1^R, CI_2^R)
S_1^G, $S_2^G \leftarrow$ ISHARE (I^G, CI_1^G, CI_2^G)
S_1^G, $S_2^G \leftarrow$ ISHARE (I^B, CI_1^B, CI_2^B)

function [S^1, S^2] = **ISHARE**(HI, CI^1, CI^2)
for i = 1 to m do
for j = 1 to n do
$PA_{i,j} \leftarrow$ AVGERAGE ($CI1_{i,j}$ + $CI2_{i,j}$)
if$HI_{i,j}$ = = 255 then
Wa← [$PA_{i,j}$, $PA_{i,j}$-1, $PA_{i,j}$, $PA_{i,j}$-1]
Wb← [$PA_{i,j}$-1, $PA_{i,j}$, $PA_{i,j}$-1, $PA_{i,j}$]
Pi ← RANDOM_FUNCTION(Wa,Wb)
end if
if$HI_{i,j}$ = = 0 then
Ba← [$PA_{i,j}$, $PA_{i,j}$-1, $PA_{i,j}$-1, $PA_{i,j}$]
Bb← [$PA_{i,j}$-1, $PA_{i,j}$, $PA_{i,j}$, $PA_{i,j}$-1]

Pi ← RANDOM_FUNCTION(Ba, Bb)
end if
$SS^1_{(i,3*j-2)} \leftarrow CI1_{i,j}$
$SS^1_{(i,3*j-1)} \leftarrow$ Pi(1)
$SS^1_{(i,3*j)} \leftarrow$ Pi(2)

$SS^2_{(i,3*j-2)} \leftarrow CI2_{i,j}$
$SS^2_{(i,3*j-1)} \leftarrow$ Pi(3)
$SS^2_{(i,3*j)} \leftarrow$ Pi(4)
end for
end for
return S^1, S^2
end function
$S_1 \leftarrow SSI_1^R, SSI_1^G, SSI_1^B$
$S_2 \leftarrow SSI_2^R, SSI_2^G, SSI_2^B$
end function

2.2 Revealing Phase

Step 1. Let the share images S1, S2.

Step 2. The share images SH1 and SH2 can be derived from S_1, S_2 using REVEAL_PHASE algorithm. Now, shares have the pixel expansion of 3 as of I.

Step 3. To generate the reconstructed halftone Image HI', digitally stacking the share images S_1 and S_2 by XOR operation[9].

Step 4. The inverse halftoning technique applied to HI' to generate the reconstructed secret Image RI[11].HI extracted during the revealing phase could be either original image or noise-like image based on whether the received images are original or fake one. Let d be the difference between I and RI, i.e. d=I-RI. If d is equal to zero, it shows RI is completely restored from HI' by inverse half-toning technique[11].

Algorithm 2: Revealing Secret Image

For given matrices S_1, S_2 of size (m × n).

Let shares SH_1 and SH_2 be empty as size of m × n/3.

procedureREVEAL_PHASE (S^1, S^2) $SI_1^R, SI_1^G, SI_1^B \leftarrow S_1$
$SI_2^R, SI_2^G, SI_2^B \leftarrow S_2$

$RI^R \leftarrow$ REVEAL_IMAGE(SI_1^R, SI_2^R)
$RI^G \leftarrow$ REVEAL_IMAGE(SI_1^G, SI_2^G)
$RI^B \leftarrow$ REVEAL_IMAGE(SI_1^B, SI_2^B)
function [SH_1, SH_2] = **RIMAGE**(S_1 , S_2)
for i = 1 to m do
for j = 1 to n do
R1=$S_{1(i,3*j-1)}$ - $S_{1(i,3*j)}$
R2=$S_{2(i,3*j-1)}$ - $S_{2(i,3*j)}$
If (R1==1and R2==1)

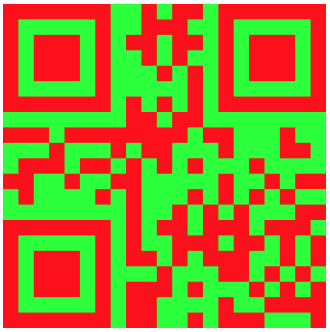
$SH_{1i,(2*j-1)}$=**255**
$SH_{1i,(2*j)}$=**0**
$SH_{2i,(2*j-1)}$=**255**
$SH_{2i,(2*j)}$=**0**
else if(R1==-1and R2==-1)
$SH_{1i,(2*j-1)}$=**0**
$SH_{1i,(2*j)}$=**255**
$SH_{2i,(2*j-1)}$=**0**
$SH_{2i,(2*j)}$=**255**
else if(R1==1and R2==-1)
$SH_{1i,(2*j-1)}$=**255**
$SH_{1i,(2*j)}$=**0**
$SH_{2i,(2*j-1)}$=**0**
$SH_{2i,(2*j)}$=**255**
else if(R1==-1and R2==1)
$SH_{1i,(2*j-1)}$=**0**
$SH_{1i,(2*j)}$=**255**
$SH_{2i,(2*j-1)}$=**255**
$SH_{2i,(2*j)}$=**0**
end for
end for
RI ← BITXOR(SH_1, SH_2)
return RI
end function
RI ← RI^R, RI^G, RI^B
end procedure

3. Experimental Results

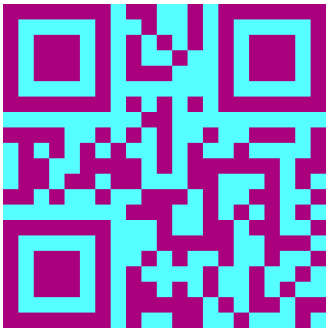
Experimental results demonstrate on three objectives. First, the robustness of the algorithm; secondly, construct the original secret image with high quality and lastly, less computational time. The proposed QRAP allows no limitation on the size of the secret images. The set of QR test images and data are shown in Figure 2 illustrates that QAP can perform well on colour images.

Password
(a)

JOHN%2016
(b)



$*****$
(c)



9025405
(d)

http://www.google.com
(e)

bless@gmail.com

(f)

Figure 2. Eight 512×512 images (a) QR1 (b) QR2 (c) QR3 (d) QR4 (e) QR5 (f) QR6.

The performance of the proposed method listed in this paper is tested by coding and running the algorithm in MATLAB 7.10 Tool. The image quality measures[6] such as Normalized Correlation (NC) and Peak Signal to Noise Ratio (PSNR) are evaluated between reconstructed images as well as original secret images using following equations;

Peak Signal to Noise Ratio (PSNR): It is defined as the maximum possible power of a signal to the power of corrupting noise that affects the fidelity of its representation[11]. PSNR is expressed regarding the logarithmic decibel is given by,

$$PSNR = \log \frac{(2^n - 1)^2}{MSE}$$

Normalized Correlation (NC): It measures the similarity between the original image and reconstructed image (4).

$$NC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (I[i,j] I'[i,j])}{\sum_{i=1}^{M} \sum_{j=1}^{N} (I[i,j])^2}$$

where, I(i, j) is original image and I`(i, j) is decrypted image, M is height and N is width of the image[7].

Figure. 3(a), (b), (c), (d), (e) and (f) shows QR1 secret image, Lena, and Baboon which are cover images, Share1, Share2 and reconstructed QR1 secret image. Table 1 depicts the performance analysis between original images and reconstructed images. The graph of the various reconstructed quality measures for the QR image is shown in Figure 4. The PSNR values range from 30.23 to 32.52 dB. From the result of PSNR and NC values[6], the quality of the reconstructed QR image is maintained as the original secret image. Table 2 shows the time was taken to run the algorithm for different images. The result indicates that the method is less computational time, and it is efficient.RIATest automated tool has been used to test the competence of the proposed method. The device has recorded different actions, debugged the scripts for the errors, code completion and has generated statistical reports[12].

(a)

(b)

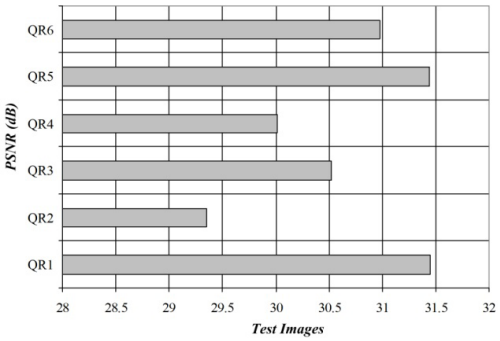
(c)

(d)

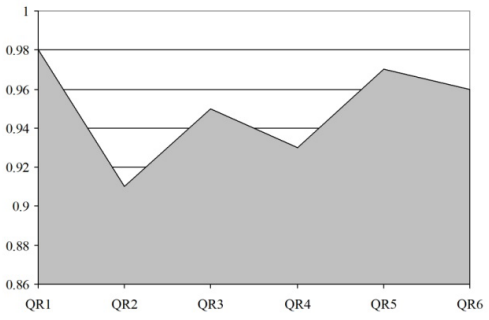
(e)

(f)

Figure 3. (a) Secret image, Q1 (b) Cover image, Lena (c) Cover image, Baboon (d) Share1 (e) Share2(f) Reconstructed secret image, Q1.



(a)



(b)

Figure 4. Graph representation of reconstructed image quality measures (a) PSNR (b) NC.

Table 1. Statistical analysis

Image	PSNR	NC
QR1	+31.45	0.98
QR2	+29.35	0.91
QR3	+30.52	0.95
QR4	+30.01	0.93
QR5	+31.44	0.97
QR6	+30.98	0.96

Table 2. Computational analysis

Images	Execution time(Seconds)
QR1	8
QR2	9
QR3	7
QR4	10
QR5	11
QR6	9

4. Conclusion

Proposed QRAP protocol gives a new way for authentication by using QR code colour images. The proposed protocol adds a layer of security in authentication. Visual cryptography methodology increases the level of security. Many advanced applications, where there are demands for high-level security in an efficient manner can use the proposed QRAP protocol.

5. References

1. NaorM, Shamir A. Visual cryptography. Proceedings of Advances in Cryptology (Eurprocrypt'94);1994. p. 1–12.
2. Ateniese G, Blundo C, DeSantis A, Stinson DR.Visual cryptography for general access structures.Proceedings of ICALP 96, Springer, Berlin; 1996. p.416–28.
3. Wu CC, Chen LH. A study on visual cryptography. Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, R.O.C; 1998.
4. Ito R, Kuwakado H, Tanaka H.Image size invariant visual cryptography, IEICE Transactions on Fundamentals. 1999; E82-A(10):2172–7.
5. Hou Y-C, Wei S-C, Lin C-Y.Random-grid-based visual cryptography schemes.IEEE Transactions on Circuits and Systems for Video Technology. 2014 May; 24(5).
6. Shahid Z, Puech W. Visual protection of HEVC video by selective encryption of CABAC bin strings.IEEE Transactions on Multimedia. 2014Jan; 16(1).
7. Wang D-S, Song T, Dong L, Yang CN.Optimal contrast

grayscale visual cryptography schemes with reversing. IEEE Transactions on Information Forensics and Security. 2013Dec; 8(12).
8. Wang X, Pei Q, Li H.A lossless tagged visual cryptography scheme.IEEE Signal Processing Letters. 2014 Jul; 21(7).
9. Lee K-H, Chiu P-L.Sharing visual secrets in single image random dot stereograms.IEEE Transactions on Image Processing. 2014Oct; 23(10).
10. Askari N, Heys HM, Moloney CR.Novel visual cryptography schemes without pixel expansion for halftone images. Canadian Journal of Electrical and Computer Engineering. 2014; 37(3).
11. Blesswin AJ, Visalakshi P.A new Semantic Visual Cryptographic Protocol (SVCP) for securing multimedia communications.International Journal of Soft Computing, Medwell Journals. 2015; 10(2):175–82.