IJCTA, 9(2) 2016, pp. 967-974
© International Science Press

A NovelQR-Code Authentication Protocol Using Visual Cryptography for Secure Communications

A. John Blesswin[1], A. Genitha[2] and G. Selvamary[3]

ABSTRACT

Visual cryptography (VC) is a distinct type of secret sharing scheme which hides secret images in share images such that, when the shares are superimposed, a hidden secret image is revealed. It does not require the complex computational method to decode the secret information. The paper proposes a novel Quick Response (QR) code authentication system using Visual Cryptography. The passwords for authentication are encoded as QR-codes and later encrypted into share images. Thus, the share images by itself convey no information, but when the layers are combined, the secret password is revealed. The only 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 QAP scheme provides secure data transmission with less computational complexity.

Keywords: Visual Cryptography, Visual Secret Sharing, Authentication, QR Code, Semantic

INTRODUCTION

Information sharing over the World Wide Web (WWW) increases vastly. It implies the pressure on securing the information. Visual Cryptography (VC) is the new method to encrypt the image data in a better way. The basic idea of VC is to divide the original secret image into many partitions which are also called share images. Naor and Shamir [1] scheme describes the principles of Visual Secret Sharing (VSS), as shown in Table 1, to generate two share images by the perfect combinations of black and white pixels according to the secret image. G. Ateniese *et al.* [2] designed a novel technique to bring k out of n Visual Cryptography schemes but unable to get any secret information by stacking a less number of favorable shares. Wu *et al.* [3] scheme is to share more than one secret image in two random shadows. Ito et al [4] minimized the size of share images, by invariant visual secret sharing scheme. The schemes [1-4] are applied to binary images, which uses to carry out the work of generating shares with higher efficiency.

Table 1
Model of Naor and Shamir [1] scheme

Images	*White Pixel*	*Black Pixel*
Share 1	□■ ■□	□■ ■□
Share 2	□■ ■□	■□ □■
Share 1 × Share 2	□■ ■□	■■ ■■

[1,3] Assistant Professor, [2]PG Student

[1] Department of Computer Science and Engineering, SRM University, India

[2] Department of Computer Science and Engineering, Karpagam University, India

[3] Department of Information Technology, SRM University, India

E-mail: wjohnbless@gmail.com

MATERIALS AND METHODS

The proposed work mainly focuses on making improvement in the authentication ability using VC. The QAP proposes an introduced system of sharing the QR images for authentication using Visual Cryptography. The basic idea to authenticate between two devices, the proposed method describes three phases. First, Share Construction Phase, each connecting device creates the same QR secret image, cover images and generates the share images. Second is the Service Request Phase, one device sends the service request to the other device which accepts the request and both devices exchange one of their share images to each other. Last is Confirmation phase, which reveals the QR secret image from the two share images that explain, from the one share it already possesses and the one it received from the other device by using XOR operation and verifies with the secret image. Figure 1 depicts a complete illustration of QAP protocol.

SHARES CONSTRUCTION

Step 1. Consider a m × n secret grayscale image (GI) and two natural grayscale images as cover images (1); then

$$GI_{i,j} \in \{0,1,2,3\ldots,255\} \tag{1}$$

$$CI1_{i,j} \in \{0,1,2,3\ldots,255\}$$

$$CI2_{i,j} \in \{0,1,2,3\ldots,255\}$$

where i and j are varying from 1 to m × n.

Step 2. Generate a halftone image (HI) by applying the Error Diffusion (ED) [5]on GI (2);

$$HI_{i,j} \in \{0,255\} \quad \leftarrow \quad ED(GI_{i,j}) \tag{2}$$

Step 3. Construct the shares $S1_{i,j} \in \{0,1,2,3\ldots,255\}$ and $S2_{i,j} \in \{0,1,2,3\ldots,255\}$ from HI by using SHARE_CONST algorithm; now, shares S1 and S2 will have the pixel expansion of 3 and also assures that the secret information can be completely restored after stacking from the shares. Shares are delivered to the receiver [10].

Algorithm 1: Shares Construction

For given matrices CI^1, CI^2 and HIof size (m × n).

Let shares S^1 and S^2 be empty as size of m × 3n.

procedureSHARE_CONST (HI, CI^1, CI^2)

```
for i = 1 to m do
    for j = 1 to n do
        $PA_{i,j} \leftarrow AVG\ (CI1_{i,j} + CI2_{i,j})$

        if$HI_{i,j}$ = = 255 then
            $Wa \leftarrow [PA_{i,j}, PA_{i,j}-1, PA_{i,j}, PA_{i,j}-1]$
            $Wb \leftarrow [\ PA_{i,j}-1, PA_{i,j}, PA_{i,j}-1, PA_{i,j}]$
            $Pi \leftarrow RANDOM(Wa,Wb)$
        end if
        if$HI_{i,j}$ = = 0 then
```

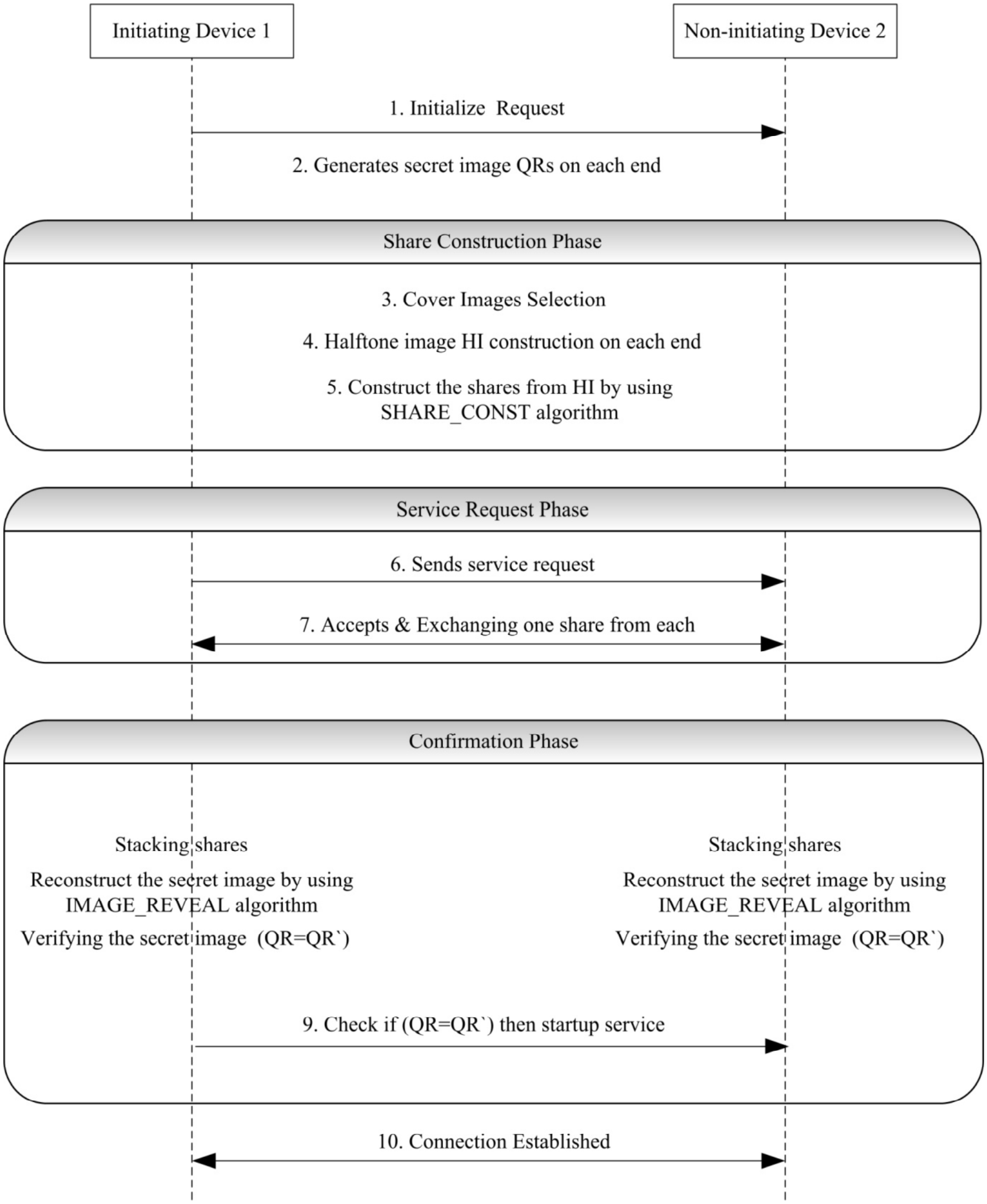

Initiating Device 1
Non-initiating Device 2
1. Initialize Request
2. Generates secret image QRs on each end
Share Construction Phase
3. Cover Images Selection
4. Halftone image HI construction on each end
5. Construct the shares from HI by using SHARE_CONST algorithm
Service Request Phase
6. Sends service request
7. Accepts & Exchanging one share from each
Confirmation Phase
Stacking shares
Reconstruct the secret image by using IMAGE_REVEAL algorithm
Verifying the secret image (QR=QR`)
Stacking shares
Reconstruct the secret image by using IMAGE_REVEAL algorithm
Verifying the secret image (QR=QR`)
9. Check if (QR=QR`) then startup service
10. Connection Established

Figure 1: Block diagram of QAP protocol

```
        $Ba \leftarrow [\ PA_{i,j}, PA_{i,j}-1, PA_{i,j}-1, PA_{i,j}]$
        $Bb \leftarrow [\ PA_{i,j}-1, PA_{i,j}, PA_{i,j}, PA_{i,j}-1]$
        $Pi \leftarrow RANDOM(Ba, Bb)$
    end if
    $S^1_{(i,3*j-2)} \leftarrow CI1_{i,j}$
    $S^1_{(i,3*j-1)} \leftarrow Pi(1)$
    $S^1_{(i,3*j)} \leftarrow Pi(2)$
```

```
                $S^2_{(i,3*j-2)} \leftarrow CI2_{i,j}$
                $S^2_{(i,3*j-1)} \leftarrow Pi(3)$
                $S^2_{(i,3*j)} \leftarrow Pi(4)$
            end for
        end for
end procedure
```

Revealing Secret Image

Step 1. Let the share images $S1_{i,j} \in \{0,1,2,3\ldots,255\}$ and $S2_{i,j} \in \{0,1,2,3\ldots,255\}$

Step 2. The share images $SH1_{i,j} \in \{0,1,2,3\ldots,255\}$ and $SH2_{i,j} \in \{0,1,2,3\ldots,255\}$ can be derived from $S1_{i,j}, S2_{i,j}$ using SHARE_REVEAL algorithm. Now, SH1 and SH2 have the pixel expansion of 2 as of GI.

Step 3. To generate the reconstructed Halftone Image HI', digitally stacking the share images SH1, SH2 by XOR operation [9].

Step 4. The inverse half-toning technique is applied to HI' to generate the reconstructed Gray scale Image GI' [11].

However, HI extracted during the revealingphase could be either an original image or a noise-like image depending on whether the received shared images are original or fake.

Let d is the difference between the GI and GI', d=GI-GI'. If the value of d is equal to zero, it implies that the GI 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.

```
procedureIMAGE_REVEAL ($S^1$, $S^2$)
    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)
                $SH^1_{i,(2*j-1)}$=255
                $SH^1_{i,(2*j)}$=0
                $SH^2_{i,(2*j-1)}$=255
                $SH^2_{i,(2*j)}$=0
            else if(R1==-1and R2==-1)
                $SH^1_{i,(2*j-1)}$=0
                $SH^1_{i,(2*j)}$=255
                $SH^2_{i,(2*j-1)}$=0
                $SH^2_{i,(2*j)}$=255
            else if(R1==1and R2==-1)
```

```
                $SH^{1}_{i,(2*j-1)}$=255
                $SH^{1}_{i,(2*j)}$=0
                $SH^{2}_{i,(2*j-1)}$=0
                $SH^{2}_{i,(2*j)}$=255
            else if(R1==-1and R2==1)
                $SH^{1}_{i,(2*j-1)}$=0
                $SH^{1}_{i,(2*j)}$=255
                $SH^{2}_{i,(2*j-1)}$=255
                $SH^{2}_{i,(2*j)}$=0
        end for
    end for
    RI=BITXOR($SH^{1}$, $SH^{2}$)
end procedure
```

EXPERIMENTAL RESULTS

Experimental results demonstrate on three objectives. First, robustness of the algorithm; secondly, construct the original secret image with high quality and lastly, less computational time. The proposed QAP allows no limitation on the size of the secret images. The set of QR test images and data are shown in Fig. 2 illustrates that QAPcan perform well on grayscale images. The efficiency of the proposed method outlined in this paper is tested by coding and running the algorithm in MATLAB 7.10 Tool. The image quality measures [6] such as Peak Signal to Noise Ratio (PSNR)and Normalized Correlation (NC) are evaluated between reconstructed images and original secret images using following equations;

Table 2
Statistical analysis

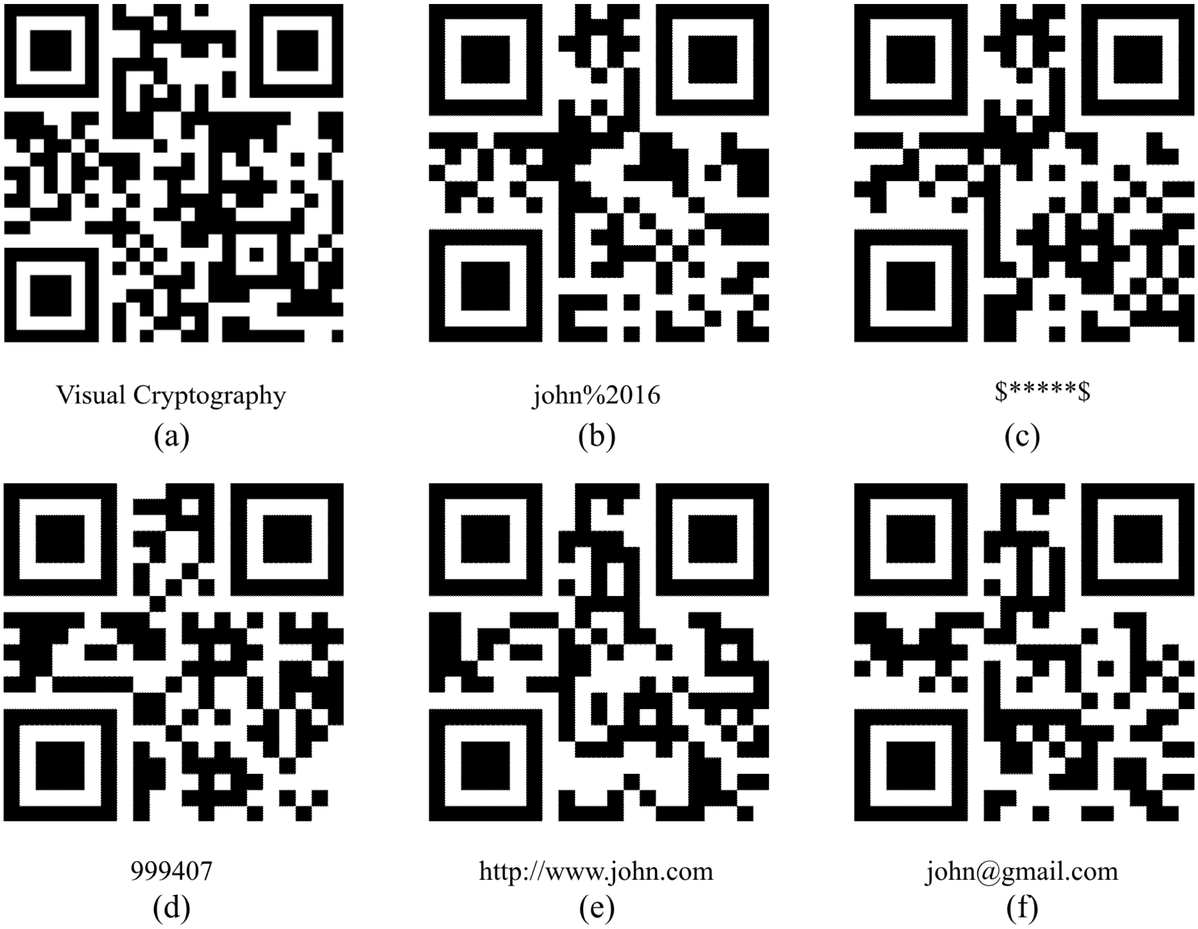
Image	*PSNR*	*NC*
QR1	+32.50	0.98
QR2	+30.23	0.97
QR3	+31.23	0.91
QR4	+31.01	0.92
QR5	+32.52	0.92
QR6	+31.63	0.94

Peak Signal to Noise Ratio (PSNR): It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation [8]. PSNR is expressed in terms of the logarithmic decibel is given by (3),

$$PSNR = \log \frac{(2^{n}-1)^{2}}{MSE} \tag{3}$$

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

$$NC = \frac{\Sigma_{i=1}^{M} \Sigma_{j=1}^{N} (I[i,j] I'[i,j])}{\Sigma_{i=1}^{M} \Sigma_{j=1}^{N} (I[i,j])^{2}} \tag{4}$$



Visual Cryptography
(a)

john%2016
(b)

$*****$
(c)

999407
(d)

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

john@gmail.com
(f)

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

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

Fig. 3(a), 3(b), 3(c), 3(d), 3(e) and 3(f) shows secret image QR1, cover images Lena and Baboon, Share1, Share2 and reconstructed secret image QR1. Table 2 shows the Statistical analysis between original secret images and reconstructed secret images.

The graph representation of the various reconstructed QR image quality measures are shown in Fig. 4. The PSNR values of the reconstructed secret QR images and the original QR images range from 30.23 to 32.52dB.From the obtained PSNR and NC values [6], the quality of the reconstructed QR image is maintained as original secret image.

TABLE 3
Computational analysis

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

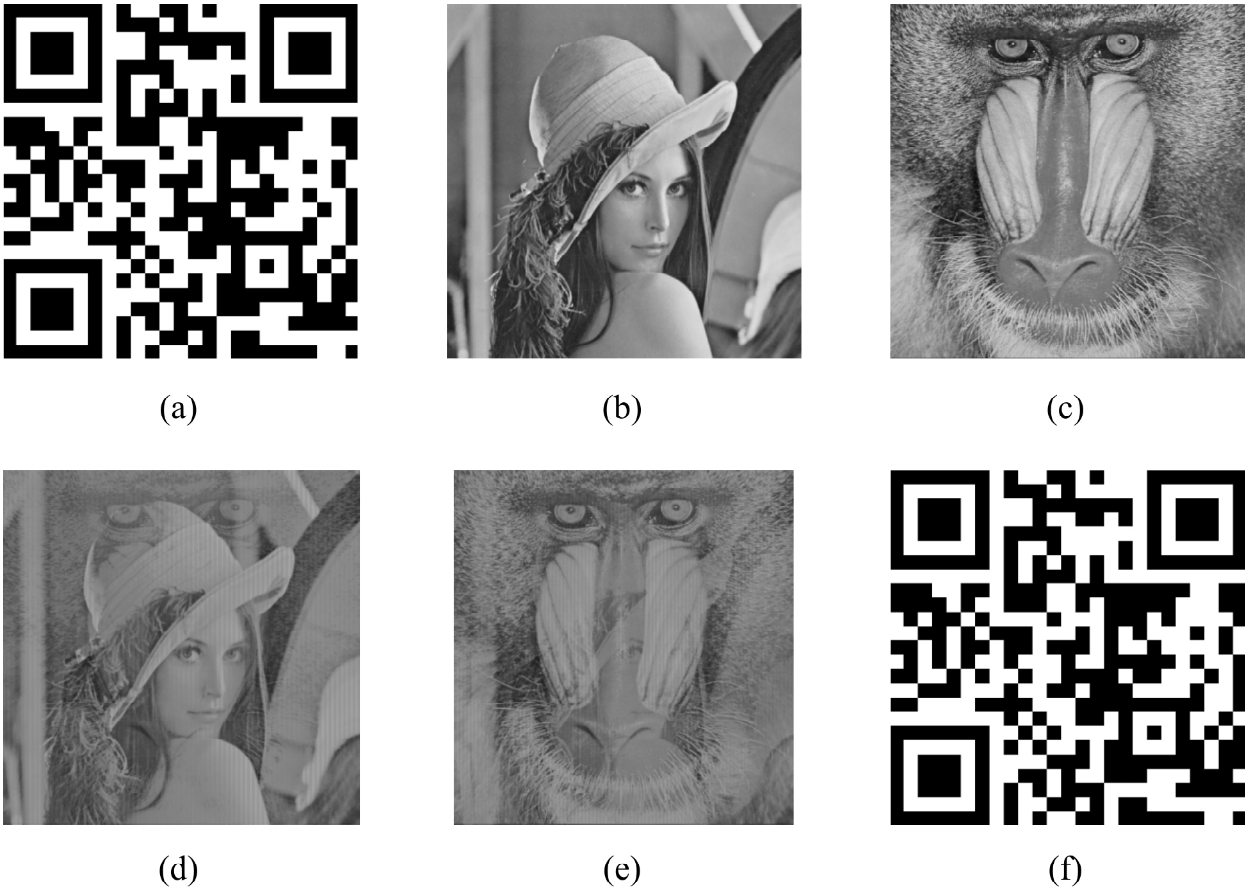


Figure 3: (a) Secret image, Q1 (b) Cover image, Lena (c) Cover image, Baboon (d) Share1 (e) Share2 (f) Reconstructed secret image, Q1

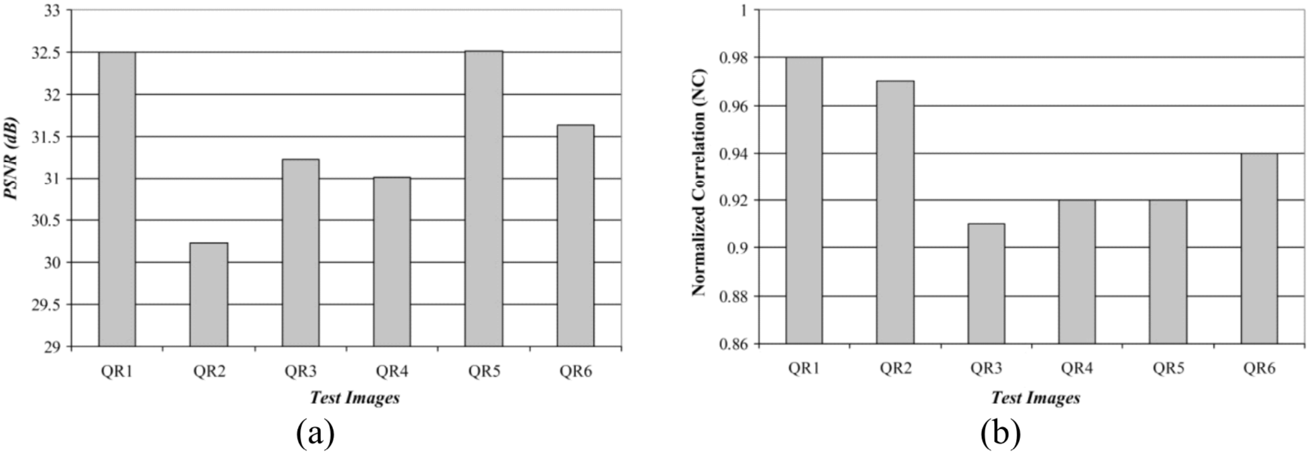


Figure 4: Graph representation of reconstructed image quality measures (a) PSNR (b) NC

Table 3 shows the time taken to execute the algorithm on different images and the result shows that the method is less computational and efficient.

CONCLUSION

Data transmission among digital devices always needs additional security concerns. Most of the existing protocols rely on Numeric comparison for authentication that gives a gateway for man-in-the-middle attacks. The proposed QAP protocol is using QR codes to achieve image based comparison in a secured manner.

This protocol uses convenient method for generating same QR codes on both connecting devices for the given user password.Visual cryptography technique increases the level of security in an efficient manner. Many advanced applications where there are demands for high-level security can use the proposed QAP protocol.

ACKNOWLEDGEMENT

The work is supported with the project of "An insight study on Visual Secret Sharing scheme: Design and development of optimal strategies to reconstruct the secret image using Visual Cryptography in Healthcare applications" by SRM University under Research Projects Engineering and Technology. We would also like to show our gratitude to Dr.Sundaram, Dean from SRM Hospital Medical college and Research centre who provided facilities to test the proposed work in real time using images that greatly assisted the research.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography", Proc. Advances in Cryptology (Eurprocrypt'94), pp.1 -12, 1994.

[2] G. Ateniese, C. Blundo, A. DeSantis, D. R. Stinson, Visual cryptography for general access structures, Proc. ICALP 96, Springer, Berlin, pp. 416-428, 1996.

[3] C.C. Wu, L.H. Chen, A Study On Visual Cryptography, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, R.O.C, 1998.

[4] R. Ito, H. Kuwakado, H. Tanaka, Image Size Invariant Visual Cryptography, IEICE Transactions on Fundamentals, Vol. E82-A, No. 10, pp. 2172-2177, 1999.

[5] Zhongmin Wang, Gonzalo R Arce and Giovanni Di Crescenzo, Halftone Visual Cryptography Via Direct Binary Search, 14th European Signal Processing Conference, Florence, Italy, 2006.

[6] Chin-Chen Chang, Chia-Chen Lin, Le, T.H.N, Hoai BAC Le, Self-Verifying Visual Secret Sharing Using Error Diffusion and Interpolation Techniques,IEEE Information Forensics and Security, Issue Date: Dec. 2009, Volume: 4 Issue: 4 on page(s): 790 - 801, 2009.

[7] A. John Blesswin, Dr. P. Visalakshi, "A New Semantic Visual Cryptographic Protocol (SVCP) for Securing Multimedia Communications", International Journal of Soft Computing, Medwell Journals 10(2), 175-182, 2015

[8] Blude, A. D. Santis, and M. Naor, Visual cryptography for grey level images, Information Processing Letter, vol. 27, pp. 255–259, 2000.

[9] Zhongmin Wang, Gonzalo R. Arce and Giovanni Di Crescenzo, Halftone Visual Cryptography Via Error Diffusion, Information Forensics and Security IEEE, Issue Date: Sept, Volume: 4 Issue:3, On page(s): 383 – 396, 2009.

[10] Li, Ling Chen and Shuenn-Shyang Wang, Visual Cryptography for meaningful shares, Thesis for master science, Institute of communication engineering, Tatung University, 2007.

[11] J. B. Feng, I. C. Lin, and Y. P. Chu, Halftone image resampling by interpolation and error-diffusion, Conference on Ubiquitous Information Management Communication, pp. 409–413, 2008.