Research Journal of Applied Sciences 9 (8): 503-510, 2014
ISSN: 1815-932X

A Novel Visual Image Confirmation (VIC) Protocol Using Visual Cryptography for Securing Ubiquitous Bluetooth Mobile Communications

A. John Blesswin and P. Visalakshi
Department of Electronics and Communication Engineering,
PSG College of Technology, 641004 Coimbatore, India

Abstract: In the last few years with the increasing popularity of the Bluetooth Technology (BT) also the interest in robbing the personal information has arisen. Bluetooth is a connection oriented service. To communicate with one another, one of them needs to initiate the connection. In July 2007, Bluetooth Special Interest Group (SIG) introduces a new method called Simple Secure Pairing (SSP). It uses Visual Number Confirmation (VNC) to meet the highest security requirements. If a malicious intruder error occurs while performing Visual Number Confirmation (VNC) verification then security could be violated. This study introduces a novel Visual Image Confirmation (VIC) protocol uses Visual Cryptography (VC) to address this problem. The proposed VIC protocol not only secures the data transmission but also increases operational efficiency.

Key words: Popularity, Bluetooth Technology (BT), requirments, Visual Cryptography (VC), efficiency

INTRODUCTION

Bluetooth has become one of the most important core technologies in ubiquitous Information and Communication Technology (ICT) applications for mobile devices, electronic devices, internet applications, etc. Bluetooth is a minimal range wireless communication in an ad-hoc manner (Gehrmann *et al*., 2004). It enables electronic devices (mobile phones, laptops, etc.) to connect with one another and communicate. In 1998, Bluetooth SIG (Special Interest Group) developed Bluetooth technology to minimize the complexity in communications (SIG, 2002). Since, 1997 IEEE has adopted the standard of IEEE 802.11 for Wireless Personal Area Networks (WPAN) (Bluetooth, 2006; Salonidis *et al*., 2001). Bluetooth technology is used in many applications like banking applications, mobile manufacturers, medical applications, car/bike manufacturers, personal computer manufacturers, handheld devices, etc.

Bluetooth wireless technology is used in many confidential data communications and payment transactions (Chen and Adams, 2004). However, transferring confidential data in such a manner, there is the need of security than earlier Basic Protection Method. In existing, the PIN entry process is done security is the open issue for Ubiquitous Bluetooth mobile communications (Gehrmann *et al*., 2004). Bluetooth hosts are not able to communicate unless they have previously discovered each other in a secure way (Salonidis *et al*., 2005). There is a chance for malicious intruders to spoof the data being transferred. To deal with the high security requirements, the proposed system used visual secret image sharing techniques, instead of Numeric Number Comparisons (NNC) (Bluetooth, 2006; Miklos *et al*., 2000). A Visual Cryptography (VC) technique is an easy, convenient way for implementing Visual Secret Sharing (VSS) which applies the best Authentication Method for connecting the legal devices. VC is the best encryption technique for transferring images, introduced by Naor and Shamir (1994) in their scheme share images are generated by random manner. The idea is to encode the secret image into a number of transparencies called shares (Naor and Shamir, 1994). When stacking the legal shares, the secret image will be revealed. The study introduces Visual Image Confirmation (VIC) for between legal devices with support mostly for PC and Ubiquitous Bluetooth mobile communications. During the authentication process, shares can be exchanged to find the legal Bluetooth device.

This study shows a better protection method and accordingly proposes a suitable method by which devices can achieve secure data transmission using Visual Image Confirmation (VIC). It leads to increases the consumer privacy and computational efficiency of local communication between small groups of legal Ubiquitous Bluetooth mobile devices.

Corresponding Author: A. John Blesswin, Department of Electronics and Communication Engineering,
PSG College of Technology, 641004 Coimbatore, India

Error diffusion technique: Halftone technique transforms a grayscale image into a binary image. Error Diffusion Method is mostly used to perform the halftone process on multi-level images in visual cryptography (Floyd, 1976). The basic idea of Floyd and Steinberg error diffusion strategy is to distribute the error into its neighboring pixels. It leads to improve the quality and maintains the contrast and luminance (Wang *et al*., 2009). W×H is the width and height of the grayscale image GI where $GI(x, y) \geq 0$ and $GI(x, y) \leq 255$. Threshold TH is set at 127.5. The size of the HI is W×H. The following steps are employed to create a Halftone Image HI.

Step 1: Consider the pixel in grayscale image GI(x, y) Eq. 1 to be set as (1, 1):

$$GI_{x,y} \in \{0,1,2,3, ...,255\} \quad (1)$$

Step 2: Compute the error value E(xy), according to Eq. 1 and 2 for the pixel located at coordinates (x, y) in grayscale image GI:

$$HI_{x,y} = \begin{cases} 1, & \text{if}(GI_{x,y} \geq TH \\ 0, & \text{if}(GI_{x,y} \leq TH \end{cases} \quad (2)$$

$$E_{x,y} = GI_{x,y} - HI_{x,y} \quad (3)$$

Step 3: The different weight factors of Floyd (1976) are 7/16, 5/16, 3/16 and 1/16 to generate a correction factor of past error values. It will be added into its neighboring pixels.

Step 4: If x = H and y = W then stop and output the halftone image HI (Eq. 4); otherwise, go to step 2 and process the next pixel in the grayscale image GI (Fig. 1).

$$HI_{x,y} \in \{0,1\} \quad (4)$$

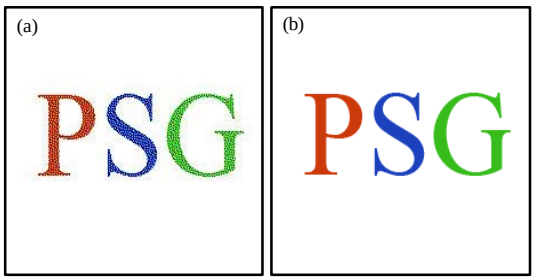

Fig. 1: Halftone image constructions; a) color secret image and b) halftone secret image

MATERIALS AND METHODS

This study proposes an introduced system of sharing the images for authentication. The basic idea of proposed system described in three phases. First, share construction phase each connecting device selects the same secret image and generates the shares in two Bluetooth devices, the second is service request phase, device 1 sends the service request to another device 2 which wants to communicate then device 2 accepts the request and send any one share to device 1 and last is visual image confirmation phase which reveals the secret image from the shares and verifies the secret image. A complete illustration of VIC protocol is depicted in Fig. 2.

Share construction phase: This study defines the procedure of generating the shares from the secret color image SI. The user selects a secret image SI for each of the two Bluetooth mobile devices. Complete details of share construction phase are justified in three techniques. First, halftone image construction that helps to transform color image into a bi-level image (Blundo *et al*., 2000), the second is the construction of matrices which creates the

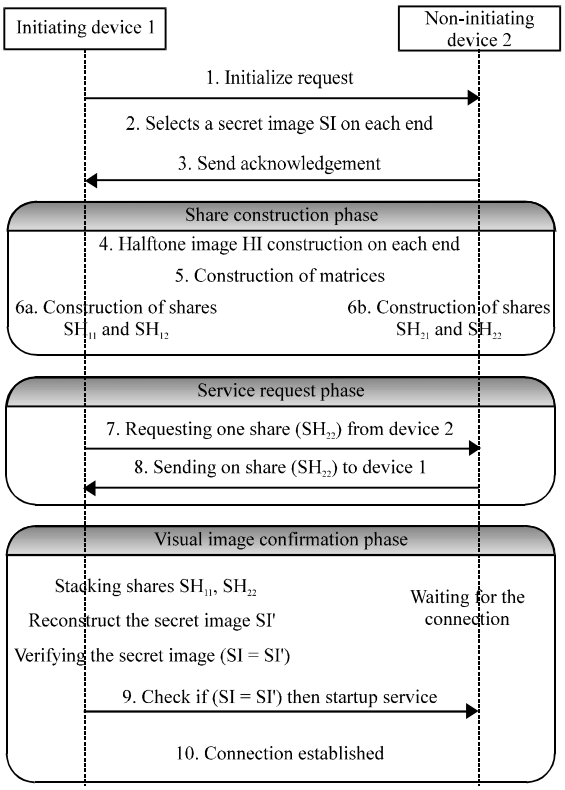

Fig. 2: The proposed protocol

two shares from the secret image and the last is importing cover images into shares which produces the meaningful shares.

Halftone image construction: The secret image SI will decompose into three sub-channel images: red (S_R), green (S_G) and blue (S_B). Each sub-image has the value range between 0 and 255. From these channels, halftone images will generated by applying Floyd (1976) and Steinberg error diffusion which is discussed in study. The following two steps are employed to create a Halftone Image (HI):

Step 1: The secret image SI will decompose into red (S_R), green (S_G) and blue (S_B) channels (Eq. 5).

$$\begin{aligned} S_R &\in \{0,1,2,3,\ldots,255\} \\ S_G &\in \{0,1,2,3,\ldots,255\} \\ S_B &\in \{0,1,2,3,\ldots,255\} \end{aligned} \tag{5}$$

Step 2: Apply the error diffusion process on each sub channel to get $S_{R(HT)}$, $S_{G(HT)}$ and $S_{B(HT)}$.

Construction of matrices: First, researchers construct the basis matrices as shown in Table 1. The encryption technique focuses on quality shares across color channels. Matrices M_0 and M_1 are used to encode bit 0 and 1 of each color in original secret color image SI. Different structures of M_0 and M_1 are shown in Table 1. The 'OR'-ed row vectors in M_0 gives (1111) and M_1 gives (1110). Each encoded sub-pixel has the same positions across three channels. The following steps are employed to construct the intermediate shares IS1 and IS2 by randomly using a set of basis matrices of types T1, T2, T3, $T4 \in \{0, 1\}$.

Step 1: Consider a $S_{R(HT)}$, $S_{G(HT)}$ and $S_{B(HT)}$ Halftone Images (HI) then:

Table 1: Construction of matrices

Type	White pixel	Black pixel
T_1	$M_0 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$	$M_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$
T_2	$M_0 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$	$M_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$
T_3	$M_0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$	$M_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$
T_4	$M_0 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$	$M_1 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

$$\begin{aligned} S_{R(HT)} &\in \{0,1\} \\ S_{G(HT)} &\in \{0,1\} \\ S_{B(HT)} &\in \{0,1\} \end{aligned} \tag{6}$$

Step 2: T_i is selected by random manner, one of the rows of matrices in T_1, T_2, T_3, T_4.

Step 3: Construct the intermediate shares $IS1_R$, $IS1_G$, $IS1_B$ and $IS2_R$, $IS2_G$, $IS2_B$ from halftone images by Eq. 7:

$$ISi_{x,y} = \begin{cases} T_i(M_0) & \text{if}(ISi_{x,y}=1) \\ T_i(M_1) & \text{otherwise} \end{cases} \tag{7}$$

Importing cover images: Cover image C1 and C2 can be imported into the $IS1_R$, $IS1_G$, $IS1_B$ and $IS2_R$, $IS2_G$, $IS2_B$ which makes the encoded shares are meaningful (Li *et al*., 2008). Thus, the shares look like meaningful images. The C1 and C2 denote the cover image pixels. An example with given (2, 2) visual cryptography is followed.

Example: Consider a given T_4 matrix M_0 and M_1 with pixel expansion m = 4:

$$T_4 \rightarrow M_0 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, M_1 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

In T_4, the 'OR'-ed row vectors in M_0 gives (1111) and M_1 gives (1110). Here, inserting C1 in the first row of first position as ($c_1$110). For the second rows, third position for replacing v_2 as (10$c_2$1) or (10$c_2$0). After replacing, the matrices as:

$$T_4 \rightarrow M_0 = \begin{bmatrix} c1 & 1 & 1 & 0 \\ 1 & 0 & c2 & 1 \end{bmatrix}, M_1 = \begin{bmatrix} c1 & 1 & 1 & 0 \\ 1 & 0 & c2 & 0 \end{bmatrix}$$

Moreover, M_0 produces ($c_1$1$c_2$1) and M_1 produces ($c_1$1$c_2$0) because 'OR'-ed vectors M_0 has c_1 and c_2. Table 2 specifies the better positions of T_i for replacing

Table 2: Replacing type T_i with meaningful image pixels

Types	White pixel	Black pixel
T1	$M_0 = \begin{bmatrix} 1 & 1 & c1 & 0 \\ c2 & 0 & 1 & 1 \end{bmatrix}$	$M_1 = \begin{bmatrix} 1 & 1 & c1 & 0 \\ c2 & 0 & 1 & 0 \end{bmatrix}$
T_2	$M_0 = \begin{bmatrix} 1 & 1 & c1 & 0 \\ 0 & c2 & 1 & 1 \end{bmatrix}$	$M_1 = \begin{bmatrix} 1 & 1 & c1 & 0 \\ 0 & c2 & 1 & 0 \end{bmatrix}$
T_3	$M_0 = \begin{bmatrix} 1 & c1 & 1 & 0 \\ c2 & 1 & 0 & 1 \end{bmatrix}$	$M_1 = \begin{bmatrix} 1 & c1 & 1 & 0 \\ c2 & 1 & 0 & 0 \end{bmatrix}$
T_4	$M_0 = \begin{bmatrix} c1 & 1 & 1 & 0 \\ 1 & 0 & c2 & 1 \end{bmatrix}$	$M_1 = \begin{bmatrix} c1 & 1 & 1 & 0 \\ 1 & 0 & c2 & 0 \end{bmatrix}$

the pixels. Since, the shares are look like better quality. The replaced pixels are made in $IS1_R$, $IS1_G$, $IS1_B$ and $IS2_R$, $IS2_G$, $IS2_B$. The shares SH_1 and SH_2 will generate by adding three channel images together (Eq. 8):

$$\begin{aligned} SH1_{x,y} &\in \{0,1\} \\ SH2_{x,y} &\in \{0,1\} \end{aligned} \quad (8)$$

The Boolean OR operation performed on the vectors and contrast α is 1/4. Cover Image CI pixels are imported across channels, regard to pixel colors and thus results in good contrast in the encrypted meaningful shares SH_1 and SH_2. Then, share has been distributed to the Bluetooth device which want to communicate. Individual share does not reveal the secret information. Likewise, device 1 and 2 generates the shares (Eq. 9):

$$\begin{aligned} SH_{11} &\in \{0,1\} \\ SH_{12} &\in \{0,1\} \\ SH_{21} &\in \{0,1\} \\ SH_{22} &\in \{0,1\} \end{aligned} \quad (9)$$

Service request phase: In this study, researchers provide the procedures in such a way to request the service to other Bluetooth device. For example, Bluetooth device 1 wants to send a file to device 2. For initiating this service, Bluetooth device 1 requests the share from device 2. Before that, device 1 generates shares SH_{11} and SH_{12} from the secret image itself. By seeing in the Fig. 2, device 1 wants to start the service and sends the service request to device 2. Then, device 2 accepts the request and sends the share SH_{22} image to device 1.

Visual image confirmation phase (authentication phase): This phase has the two functions. The first is to reveal the reconstructed secret image from the set of shares SH_{11} and SH_{22}. The second is to verify the reconstructed secret image. If the original secret image is revealed then acknowledgement can be sent to another device for startup the services. Otherwise, it identifies the other one is a faulty user. By stacking the shares SH_{11} and SH_{22} secret image SI can be revealed. If the reconstructed secret image SI is correct, device 1 send the startup service to device 2. That is, device 1 identified the legitimate user.

RESULTS AND DISCUSSION

In this study, researchers provide some experimental results illustrate the effectiveness of the proposed VIC. The set of test images shown in Fig. 3 illustrates that the

Fig. 3: Three 225×225 color images; a) PSG image; b) numbered image and c) Lena

VIC can perform well on color images. The proposed VIC allows no limitation on the size of the secret images. The set contains three 225×225 color images: PSG image, numbered image and Lena. The efficiency of the proposed method outlined in this study is tested by coding and running the algorithm in MATLAB 7.10 Tool.

The image quality measures such as Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR) and Mean Absolute Error (MAE) are evaluated between reconstructed and original secret images using following equations.

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. PSNR is expressed in terms of the logarithmic decibel is given by Chang *et al.* (2009):

$$PSNR = \log \frac{(2^n - 1)^2}{MSE} \quad (10)$$

Signal to Noise Ratio (SNR): It is defined as the ratio of signal power to the noise power, often expressed in decibels. The SNR is given by Ciptasari *et al.* (2014):

$$SNR = 10.\log 10\left[\frac{\sum_0^{n_x-1}\sum^{n_y-1}[r(x,y)]^2}{\sum_0^{n_x-1}\sum^{n_y-1}[r(x,y)-t(x,y)]^2}\right] \quad (11)$$

Here, $r = \{x_i|, i = 1, 2, ..., n\}$ and $t = \{y_i|, i = 1, 2, ..., n\}$ be the original and reconstructed image signals, respectively. Table 2 represents the computed values for image quality evaluation for the reconstructed images.

Mean Absolute Error (MAE): It is a capacity used to measure how nearby predictions are to the eventual consequences. The mean absolute error is given by:

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|f_i - y_i| = \frac{1}{n}\sum_{i=1}^{n}|e_i| \quad (12)$$

Here, mean absolute error is an average of the absolute errors $e_i|f_i-y_i|$ where f_i is the prediction and y_i the true value.

Figure 4 shows the experimental results of encoding and decoding of image files, applicable when both devices are capable of displaying images. The device 1 requesting the share from device 2 then device 2 sends the share SH_{22} to device 1. The shares are stacked in device 1. If the secret image is revealed, the communication is initiated and device 1 startup the services. Otherwise, communication is disconnected.

In Fig. 4a, the secret image of size 225×225 pixels show the letters 'P', 'S' and 'G', respectively. Cover images 'Baboon' and 'Pepper' of size 225×225 in colors are provided for share generation shown in Fig. 5b and c. The secret image can be revealed with the PSNR value of 22.32. The reconstructed image by stacking two shares and letters are in preferred color and researchers can easily recognize them. In Fig. 4, the natural 'Lena' secret image of size 225×225 pixels is used. The reconstructed secret image can be revealed with the PSNR value of 17.96. Table 3 explains the results as to the reconstructed secret image quality and reliability.

To demonstrate the verification ability of this scheme, the one of the share SH_{22} is assumed to be altered by some device. Figure 5 explains the results of the reconstructed secret image. The original secret image shows the letters 'P', 'S' and 'G', respectively. The second share can be replaced by a fake share. Therefore, original secret image is not revealed. By seeing the reconstructed secret image, researchers easily identify which share is the fake one. Researchers can able to see the original share in the reconstructed image. The acts of defrauding are described in the following scenarios.

- The original secret image SI shows the letters 'P', 'S' and 'G'. The second share SH_{22} is replaced by fake share
- The original secret image shows the letters 'P', 'S' and 'G'. The first share SH_{21} is replaced by fake share

Table 3: Experiment Results of various secret images

Images	PSNR (dB)	SNR	MAE	Reliability
PSG image	+22.32	-11.76	9.14	Sure
Number image	+23.26	-10.72	7.90	Sure
Lena	+17.10	-17.20	29.30	Sure

Fig. 4: Reconstructed secret image results when no cheating; a) secret PSG image; b) reconstructed PSG image; c) secret numbered image; d) reconstructed numbered image; e) secret image, Lena and f) reconstructed secret image, Lena

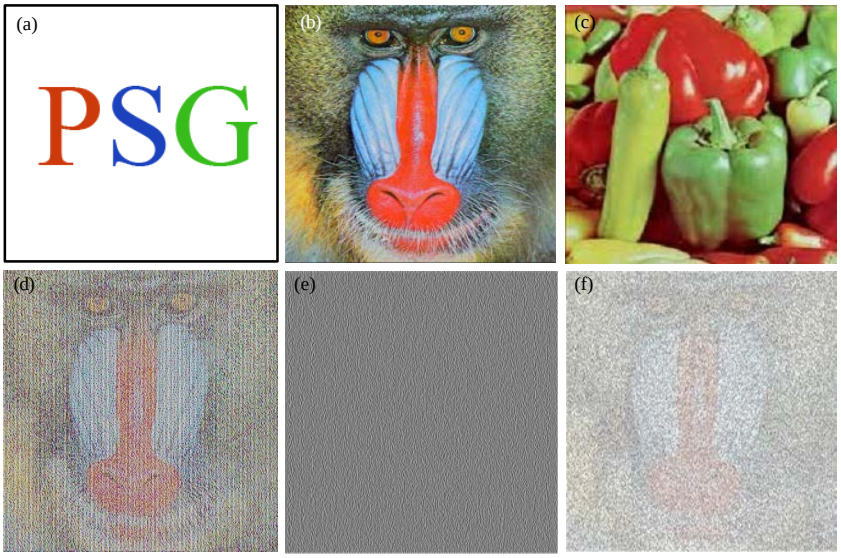

Fig. 5: Reconstructed secret image results when some cheating occurs; a) secret PSG image; b) cover image1, Baboon; c) cover image2, Pepper; d) correct Share SH_{11}; e) fake Share SH_{22} and f) reconstructed image

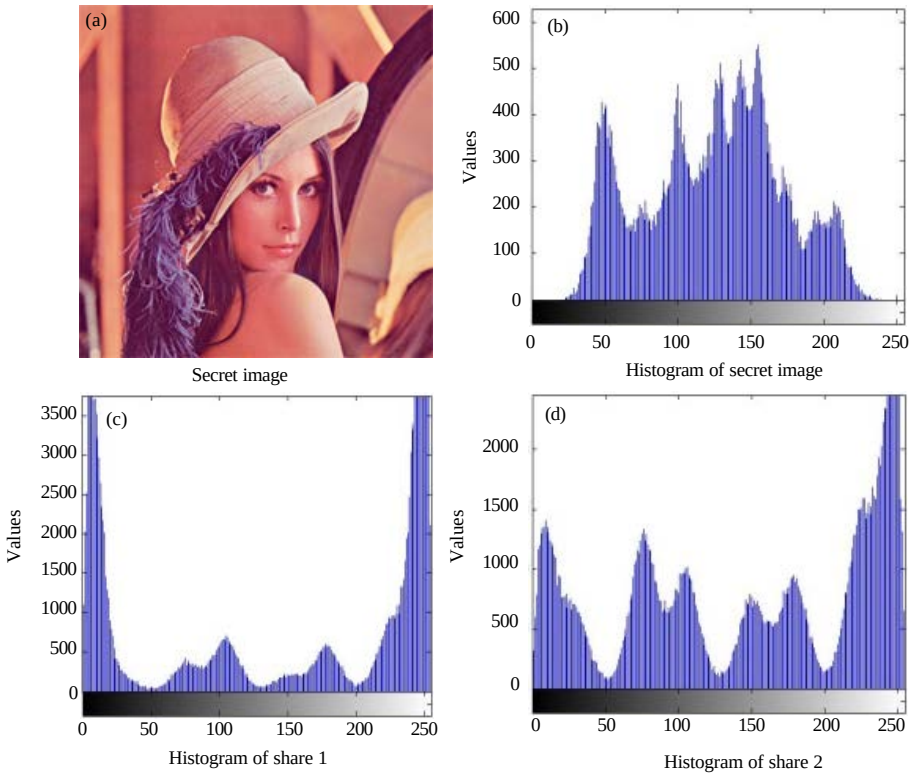

Fig. 6: a-d) Histogram of images

Security analysis: This study addresses the security of the proposed Visual Image Confirmation (VIC) Method. To prove that the security of this scheme is guaranteed that each individual share reveals no information about the original secret image. Analyzing the histogram in the secret image and in the share images is the statistical analysis to prove the robustness of the proposed VIC against any statistical attack. Figure 6 shows the histogram of secret images and its share images.

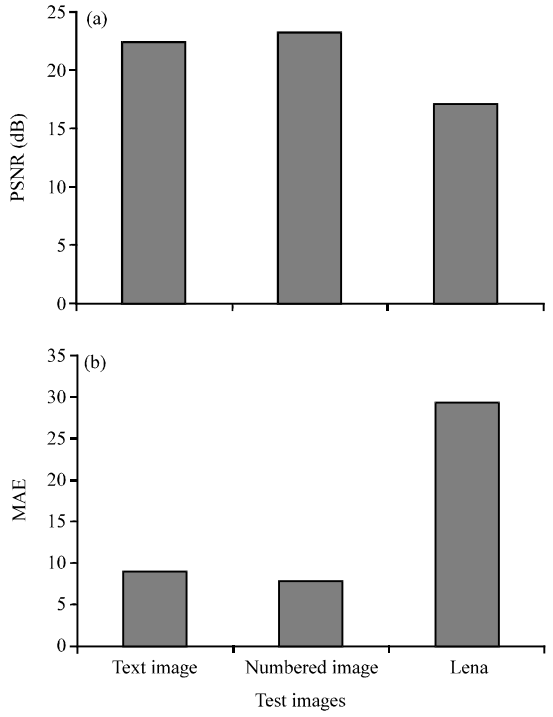

Fig. 7: Graph representation of reconstructed image quality measures; a) PSNR; b) MAE

Man in the middle attack: Only legal device with the correct shares can retrieve the original secret image. If devices fail to get the secret image then the connection will be disconnected. Moreover, different shares protect the communication among the two connecting devices. The man in the middle attacks can thus be avoided. Figure 7 shows the graph representation of the various image quality measures. The PSNR values of the reconstructed secret images range from 17.10-22.32 dB. By seeing the obtained PSNR and MAE values, reconstructed images can be presumed to be absolutely believable.

CONCLUSION

This study proposes an easy and reliable VIC protocol which applies the well-known authentication method entering the PIN number on both Bluetooth connecting devices (Li *et al*., 2008) as an alternative to confirming displayed multimedia images. In internet, proper safeguards are required to prevent the unauthorized leakage of information. The proposed VIC protocol is addressing the security issues. VIC protocol can offer fast and secure access to Ubiquitous Bluetooth mobile communications. The proposed Visual Image Confirmation (VIC) protocol not only secures the consumer privacy but also increases the efficiency of operation.

ACKNOWLEDGEMENT

Researchers would like to acknowledge the support provided by UGC, New Delhi, India under Major Research Projects in Engineering and Technology on January 2013.

REFERENCES

Bluetooth, SIG., 2006. Simple pairing whitepaper. Technical Report, Bluetooth, Special Interest Group, 3 August, 2006, pp: 3-23. http://mclean-linsky.net/joel/cv/Simple%20Pairing_WP_V10r00.pdf.

Blundo, C., A. de Santis and M. Naor, 2000. Visual cryptography for grey level images. Inform. Process. Lett., 75: 255-259.

Chang, C.C., C.C. Lin, T.H.N. Le and H.B. Le, 2009. Self-verifying visual secret sharing using error diffusion and interpolation techniques. IEEE Trans. Inform. Forensics Secur., 4: 790-801.

Chen, J.J. and C. Adams, 2004. Short-range wireless technologies with mobile payments systems. Proceedings of the 6th International Conference on Electronic Commerce, October 25-27, 2004, The Netherlands, pp: 649-656.

Ciptasari, R.W., K.H. Rhee and K. Sakurai, 2014. An enhanced audio ownership protection scheme based on visual cryptography. EURASIP J. Inform. Secur., 10.1186/1687-417X-2014-2.

Floyd, R.W., 1976. An adaptive algorithm for spatial gray-scale. Proc. Soc. Inf. Dis., 17: 75-77.

Gehrmann, C., J. Persson and B. Smeets, 2004. Bluetooth Security. Artech House, Norwood, MA., ISBN-10: 1580535046.

Li, C.T., M.S. Hwang and Y.P. Chu, 2008. A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. Comput. Commun., 31: 2803-2814.

Miklos, G., A. Racz, Z. Turanyi, A. Valko and P. Johansson, 2000. Performance aspects of Bluetooth scatternet formation. Proceedings of the 1st ACM International Symposium on Mobile Ad Hoc Networking and Computing, August 11-11, 2000, Boston, MA., USA., pp: 147-148.

Naor, M. and A. Shamir, 1994. Visual cryptography. Adv. Cryptol., 950: 1-12.

SIG, 2002. Bluetooth™ security white paper. Special Interest Group (SIG), 19 April, 2002, pp: 1-46. http://up.backtrack.cz/data/ebooks/BlueTooth/bluetooth-security-sig.pdf.

Salonidis, T., P. Bhagwat, L. Tassiulas and R. LaMaire, 2001. Distributed topology construction of Bluetooth personal area networks. Proceedings IEEE INFOCOM 2001, 20th Annual Joint Conference of the IEEE Computer and Communications Societies, Volume 3, April 22-26, 2001, Anchorage, AK., pp: 1577-1586.

Salonidis, T., P. Bhagwat, L. Tassiulas and R. LaMaire, 2005. Distributed topology construction of Bluetooth wireless personal area networks. IEEE J. Selected Areas Commun., 23: 633-643.

Wang, Z., G.R. Arce and G. Di Crescenzo, 2009. Halftone visual cryptography via error diffusion. IEEE Trans. Inform. Forensics Secur., 4: 383-396.