WI-FI AUTHENTICATION USING VISUAL CRYPTOGRAPHY FOR SECURING WI-FI ENABLED DEVICES

Selvamary G.[1] and Gayathri M.[2]
[1]Department of Information Technology, SRM University, India
[2]Department of Computer Software Engineering, SRM University, India
E-Mail: g.selvamary@gmail.com

ABSTRACT

With the huge production of Wi-Fi-enabled devices, people expect to be able to use them everywhere. Wi-Fi routers generally resort to simply sharing the password. Security and liability issues set obstacles to Wi-Fi networks. However, existing authentication methodologies breach user's location privacy. To this end, we present a Wi-Fi Authentication using Visual Cryptography, called Wi-Fi AVC, and the related devices for network discovery and authentication. Our prototype implementation uses Wi-Fi enabled device requests to connect the legitimate neighboring devices. Adopting Wi-Fi AVC cannot only enhance the uses of secure authentication, ultimately providing research directions for constructing advanced ubiquitous society.

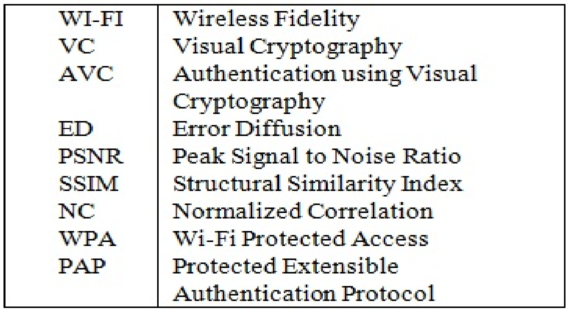
Keywords: authentication, secret sharing, security, Wi-Fi, visual cryptography.

1. INTRODUCTION

Wi-Fi-based wireless networks are essential mechanisms in next generation mobile varied networks, as Wi-Fi devices are widely used in laptops, PDAs (Personal Digital Assistant) and other mobile computing machines. As more and more wirelessly connected networks come online, security becomes a leading concern [5]. Unsecured Wi-Fi can result in harmful effects to both individuals and institutions. To protect Wi-Fi, authentication plays a significant role to avoid the initial level attacks [8].

Generally speaking, secure wireless communications should satisfy the requirements of authenticity is must[6]. The existing WPA (Wi-Fi Protected Access) and PAP (Protected Extensible Authentication Protocol) are used to authenticate by ASCII characters, and they give more chances for the intruders to hack it. Authenticity, confidentiality, integrity and availability are the important factors while securing the network or devices against threats[7]. Currently, the password using ASCII characters is used for Authentication. Protecting password from an intruder is a challenging work. In this proposed Wi-Fi AVC, the images are used to authenticate the system. Visual Cryptography techniques are efficient to share the images in a secure manner as well as by simple computational operations [2].

Nomenclature



WI-FI	Wireless Fidelity
VC	Visual Cryptography
AVC	Authentication using Visual Cryptography
ED	Error Diffusion
PSNR	Peak Signal to Noise Ratio
SSIM	Structural Similarity Index
NC	Normalized Correlation
WPA	Wi-Fi Protected Access
PAP	Protected Extensible Authentication Protocol

2. MATERIALS AND METHODS

The phases of the Wi-Fi AVC proposed system are explained in this section. The proposed system consists of three phases; Firstly, Share construction phase in which two shares Share1 and Share2 are generated from the given input secret image and two natural images (NI). Secondly, in Revealing phase, the two share images SH1 and SH2 are generated from the shares Share1 and Share2 respectively. A Reconstructed Image (RI) is revealed by stacking the two share images using Logical XOR operation. Figure-1 shows the overall phases in the proposed system.

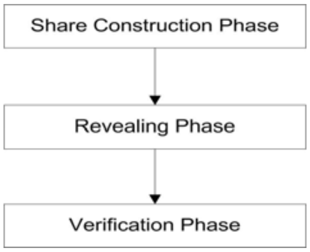


Figure-1. Phases in proposed method.

Finally, in verification phase, one of the shares from each end (sender and receiver) is interchanged, and the Secret Image (SI) is reconstructed. If the reconstructed image is same of the original image, then they are authenticated. The individual shares do not reveal any information about the original secret image. Also, reduces the chances of assuming the presence of secret image will be considerably reduced. In the proposed Wi-Fi AVC system, Error Diffusion (ED) technique is used [1] to convert the Secret Image (SI) into Error Diffusion Image (EDI). The EDI is given to the share construction phase to generate shares. In the revealing phase, reconstructed Secret Image SI' is obtained by inverse error diffusion technique [3]. Block diagram of the proposed Wi-Fi AVC system is shown in Figure-2.

a) Share construction phase

Step 1. Consider a m × n Secret Image (SI) and two natural images as natural images (Equation.1); then

$$SI_{i,j} \in \{0,1,2,3\ldots,255\}$$
$$NI1_{i,j} \in \{0,1,2,3\ldots,255\} \qquad (1)$$
$$NI2_{i,j} \in \{0,1,2,3\ldots,255\}$$

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

Step 2. Generate an Error Diffusion Image (EDI) by applying the Error Diffusion (ED) technique on SI (Equation .2);

$$EDI_{i,j} \in \{0,255\} \quad \leftarrow \quad ED(SI_{i,j}) \qquad (2)$$

Step 3. Construct the shares $Share1_{i,j} \in \{0,1,2,3\ldots,255\}$ and $Share2_{i,j} \in \{0,1,2,3\ldots,255\}$ from EDI by using SHARE_GENERATION algorithm; now, shares Share1 and Share2 will have the pixel expansion of three and also assures that the secret information can be completely restored after stacking the shares together. Shares are delivered to the receiver.

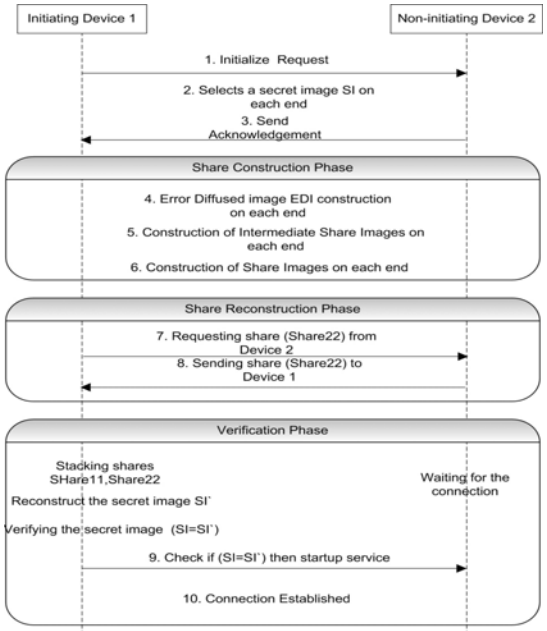

Initiating Device 1
Non-initiating Device 2
1. Initialize Request
2. Selects a secret image SI on each end
3. Send Acknowledgement
Share Construction Phase
4. Error Diffused image EDI construction on each end
5. Construction of Intermediate Share Images on each end
6. Construction of Share Images on each end
Share Reconstruction Phase
7. Requesting share (Share22) from Device 2
8. Sending share (Share22) to Device 1
Verification Phase
Stacking shares SHare11,Share22
Reconstruct the secret image SI'
Verifying the secret image (SI=SI')
Waiting for the connection
9. Check if (SI=SI') then startup service
10. Connection Established

Figure-2. Block diagram of proposed scheme

Figure-3 explains the Error Diffusion process.

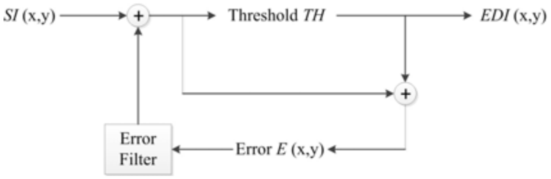


Figure-3. Flowchart for error diffusion.

Algorithm:

For given matrices NI^1, NI^2 and EDI of size (m × n).

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

```
procedure SHARE_GENERATION (EDI, NI^1, NI^2)
for i = 1 to m do
  for j = 1 to n do
    $AP_{i,j} \leftarrow AVG\ ( NI1_{i,j} + NI2_{i,j} )$
    if $EDI_{i,j}$ = = 255 then
      Wa ← [ $AP_{i,j}$, $AP_{i,j}$-1, $AP_{i,j}$, $AP_{i,j}$-1 ]
      Wb ← [ $AP_{i,j}$-1, $AP_{i,j}$, $AP_{i,j}$-1, $AP_{i,j}$ ]
      Pi ← RANDOM(Wa,Wb)
    end if
    if $EDI_{i,j}$ = = 0 then
      Ba ← [ $AP_{i,j}$, $AP_{i,j}$-1, $AP_{i,j}$-1, $AP_{i,j}$]
      Bb ← [ $AP_{i,j}$-1, $AP_{i,j}$, $AP_{i,j}$, $AP_{i,j}$-1]
      Pi ← RANDOM(Ba, Bb)
    end if
    $Share^1_{(i,3*j-2)}$ ← $NI1_{i,j}$
    $Share^1_{(i,3*j-1)}$ ← Pi(1)
    $Share^1_{(i,3*j)}$ ← Pi(2)
    $Share^2_{(i,3*j-2)}$ ← $NI2_{i,j}$
    $Share^2_{(i,3*j-1)}$ ← Pi(3)
    $Share^2_{(i,3*j)}$ ← Pi(4)
  end for
end for
end procedure
```

b) Revealing phase

Step 1. Let the share images $Share1_{i,j} \in \{0,1,2,3\ldots,255\}$ and $Share2_{i,j} \in \{0,1,2,3\ldots,255\}$

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 $Share1_{i,j}, Share2_{i,j}$ using SHARE_RECONSTRUCTION algorithm. Now, SH1 and SH2 have the pixel expansion of 2 as of SI [4].

Step 3. To generate the reconstructed Error Diffusion Image EDI', digitally stack the share images SH1, SH2 by XOR operation.

Step 4. The inverse Error Diffusion technique is applied to EDI' to generate the reconstructed Secret Image SI'.

c) Verification phase

In this phase, the reconstructed image is compared with the original secret image to authenticate the secure connection. EDI reconstructed during the share reconstruction phase could result to be either a noise-like image or an original image depending on whether the received shared images are original or altered [3]. Let *diff* be the difference between the SI and SI', *diff=SI-SI'*. If the value of *diff* is equal to zero, it implies that SI is completely restored from EDI' by inverse Error Diffusion technique.

Algorithm:

For given matrices $Share^1$, $Share^2$ of size (m × n).

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

```
procedure SHARE_ RECONSTRUCTION ($S^1, S^2$)
for i = 1 to m do
  for j = 1 to n do
    Reconst1= $Share^1_{(i,3*j-1)}$ - $Share^1_{(i,3*j)}$
    Reconst2= $Share^2_{(i,3*j-1)}$ - $Share^2_{(i,3*j)}$
    If (Reconst1==1and Reconst2==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(Reconst1==-1and Reconst2==-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(Reconst1==1and Reconst2==-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(Reconst1==-1and Reconst2==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
```

3. EXPERIMENTAL RESULTS

Experimental results demonstrate on two objectives. First, the reconstructed secret image should maintain the quality of the original image. Secondly, the proposed Wi-Fi AVC should minimize the computational complexity. The set of sample images shown in Figure-4 illustrates that proposed Wi-Fi AVC can function well on grayscale images. The set includes eight 512×512 grayscale images.

Figure-4. Eight 512×512 images (a) Airplane (b) Fruits (c) Woman1 (d) Camera-man (e) Fingerprint (f) Zelda (g) Girl face and (h) Barbara.

Coding tests the effectiveness of the Wi-Fi AVC method described in this paper and working the algorithm in MATLAB 7.10 Tool.

The image quality measures [4] such as Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM) and Normalized Correlation (NC) are calculated between reconstructed images and original secret images using following equations;

Peak signal to noise ratio (PSNR): It is the ratio between the maximum possible power and the power of corrupting noise of a signal that affects the accuracy of its representation. PSNR is expressed regarding the logarithmic decibel is given by (Equation. 3),

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

Structural similarity index (SSIM): It measures the correlation of two images, based on an original uncompressed or distortion-free image (Equation. 4).

$$SSIM\,(x,y) = \frac{2\times \mathrm{m_1(P)}\times \mathrm{m_2(P)}+\mathrm{C_1}}{\mathrm{m_1(P)^2}+\mathrm{m_2(P)^2}+\mathrm{C_1}} \times \frac{2\times \mathrm{c(P)}+\mathrm{C_2}}{\mathrm{s_1(P)^2}+\mathrm{s_2(P)^2}+\mathrm{C_2}} \tag{4}$$

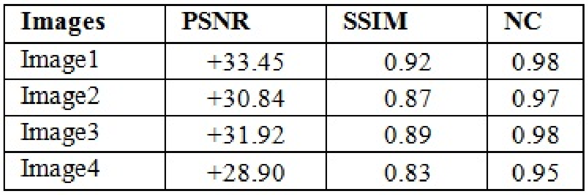
Where m1(P) and m2(P) are average conditions. s1(P) and s2(P) are standard deviations of seq1 and seq2. c(P) is the covariance with seq1 and seq2 measured over the corresponding window. C1 = (K1*L)^2: regularization constants, C2 = (K2*L)^2, K1, K2: regularization parameters, L=255, and the default window is a Gaussian window with standard deviation 1.5 along both the X and the Y axis.

Normalized correlation (NC): It covers the relationship representation between the original image and decrypted image (Equation. 5).

$$NC = \frac{\Sigma_{i=1}^{M}\Sigma_{j=1}^{N}(I[i,j]I'[i,j])}{\Sigma_{i=1}^{M}\Sigma_{j=1}^{N}(I[i,j])^2} \quad (5)$$

Where I(i, j) is secret image and I`(i, j) is decrypted image, M is the height of the image and N is the width of the image. The statistical analysis of various reconstructed images is shown in Table-1.

Table-1. Statistical analysis.



Images	PSNR	SSIM	NC
Image1	+33.45	0.92	0.98
Image2	+30.84	0.87	0.97
Image3	+31.92	0.89	0.98
Image4	+28.90	0.83	0.95

Camera-man, cover images Lena and Baboon, Share1, Share2 and reconstructed secret image Camera-man. Share images are looking completely different from the secret image; therefore, this method can show the robustness.

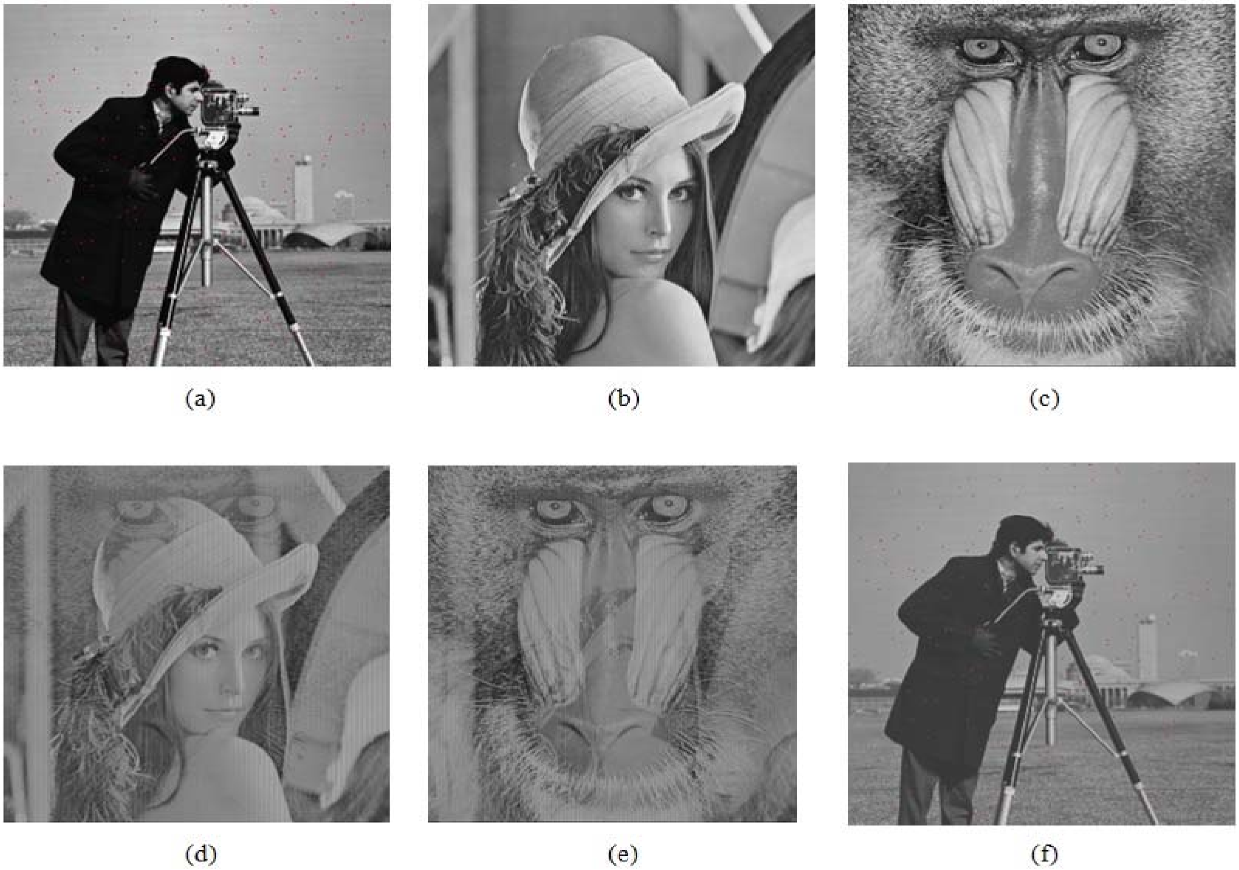
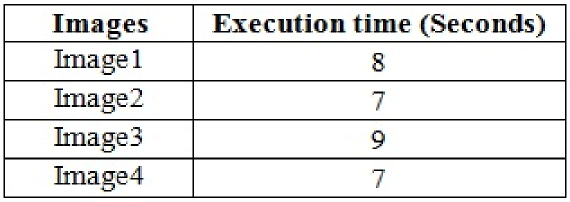


Figure-5.(a) Secret image, camera-man (b) Cover image, Lena (c) Cover image, Baboon (d) Share1 (e) Share2 (f) Reconstructed secret image, camera-man.

Table-2. Computational analysis.



Images	Execution time (Seconds)
Image1	8
Image2	7
Image3	9
Image4	7

The PSNR values of the reconstructed secret images and the original images range from 28.40 to 33.45 dB. From the obtained PSNR, SSIM and NC values [1], the quality of the reconstructed secret image is maintained as the original secret image. Table-2 shows the time taken to execute the algorithm on different images and the result indicates that the proposed method is less computational and efficient.

CONCLUSIONS

In this paper, a novel Wi-Fi Authentication using Visual Cryptography is proposed for securing Wi-Fi enabled device. Wi-Fi AVC scheme protects the secret image by dividing them to shares. Both devices (initiating and non-initiating) devices generate the shares respectively. Verification is done by exchanging the shares among them. If the secret image is reconstructed, then the connection is established among the devices or it is denied.

ACKNOWLEDGEMENTS

The work is supported by 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, Engineering and Technology under Research Projects.

REFERENCES

[1] A. John Blesswin, P. Visalakshi, “A Novel Visual Image Confirmation (VIC) Protocol Using Visual Cryptography for Securing Ubiquitous Bluetooth Mobile Communications”, Research Journal of Applied Sciences 9(8): 503-510,2014.

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

[3] 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.

[4] Shyong Jian Shyu, Ming Chiang Chen, Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures, Circuits and Systems for Video Technology, IEEE Transactions on Volume: 25, Issue: 9, 2015.

[5] J. Xiong and K. Jamieson, “Secure Array: Improving Wi-Fi security with fine-grained physical-layer information,” in Proceedings of the 19th ACM International Conference on Mobile Computing and Networking (ACM MobiCom’13), Miami, USA, September 2013.

[6] IEEE Std 802.15.1-2002 IEEE Std 802.15.1 IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), 2002

[7] Vainio, T. Juha, “Bluetooth security”, Internetworking seminar, Department of Computer Science and Engineering, Helsinki University of Technology, 2000 .

[8] K. Wong, Y. Zheng, J. Cao, and S. Wang, “A dynamic user authentication scheme for wireless sensor networks,” Proceedings of the 2006 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, vol. 14, no. 4, Taichung, Taiwan, June 2006.