

A novel meaningful secret image sharing method based on Arabic letters

Derya Avci

Dept. of Electrical and Electronic Engineering, Engineering Faculty, Firat University, Elazig, Turkey

Corresponding author: derya2344@hotmail.com

Abstract

In recent years, to provide information security for multimedia has become an important subject of study. Visual cryptography and secret sharing provide information security without using complex mathematical operators. Thus, visual cryptography and secret sharing are widely used. In this paper, letter based secret image sharing (LSIS) is used for protecting image contents. For this purpose, secret sharing and data hiding algorithms are used together in this LSIS method. The LSIS method consists of two parts. These are generating of meaningful secret sharing and data hiding. Secret sharing and visual cryptography methods commonly generate noise-like images. The noise-like images have attracted the attention of the attackers and several attacks have been developed to break these encrypted images. To prevent these attacks, meaningful secret shares are generated and these secret shares are embedded into cover image. In this paper, a novel secret image sharing method based on Arabic letters is suggested. The proposed method uses Arabic letters for generating meaningful secret shares and data hiding functions are used for camouflage. RGB images are used for cover images. In proposed method, secret shares are embedded into R, G and B channels respectively. Thus, cheatings occurring in visual cryptography are prevented. A secret image sharing method, which is independent morphological features of letters, is obtained by using the proposed method. In this proposed secret image sharing, Arabic letters are used because of Arabic is one of the richest languages in the world. In the data hiding method, 2LSBs data hiding function is used.

Keywords: Data hiding; image processing; information security; meaningful secret image sharing; visual cryptography.

1. Introduction

The purpose of information security is preventing unauthorized access to data. To provide the information security, three basic elements must be fulfilled. These are confidentiality, integrity and availability (Lin *et al.*, 2015; Nair *et al.*, 2015).

- Confidentiality: protecting against unauthorized access to information.
- Integrity: protecting against change to information from unauthorized parties.
- Availability: providing access to information by authorized parties.

Internet is mostly used communication network and this network is open access. For this reason; unauthorized third parties can have access to information. So, several methods have been developed against the third parties (Wu & Sun 2012; Nazari *et al.* 2015; Choi & Aizawa, 2002). The most widely used information security method

is cryptography and data hiding. Cryptography changes context of data, but data hiding does not change context of data. Data hiding uses a cover data for hiding secret data. The secret data is embedded into a cover object. Secure transmissions in data hiding are provided (Govind & Wilscy 2015). The most widely used data hiding function is least significant (LSB) bit insertion method. This method uses the least significant bits of cover object and inserts secret data instead of least significant bit/bits of cover object (Liu *et al.*, 2015). The mentioned method causes little changes on cover object and these changes are not perceived by human visual system. For this reason, this method is widely used in literature. However, this method is not robust. It is sensitive against the change (Lou & Hu 2012). To reduce this sensitivity, frequency domain techniques are used for data hiding. These technique use frequency transformations such as Discrete Wavelet Transform (Lee, 2014), Discrete Cosine Transform (Lin 2014), Discrete Fourier Transform (Liu & Zhao 2010) etc. The obtained coefficients are used for data hiding. In frequency domain, the basic aim of data hiding techniques

is robustness. The performance criteria of data hiding are capacity, robustness and visual quality. Mean square error (MSE) (Hussain, 2013; Veerappan & Pitchammal, 2012) and peak signal noise rate (PSNR) (Hussain, 2013; Tanchenko, 2014) metrics are used for measuring visual quality. The main aim of data hiding techniques is to develop high payload capacity, high visual quality and robustness (Mandal, 2012; Khamrui & Mandal, 2013). A lot of data hiding methods have been developed in literature. Yang & Lin (2015) proposed almost-aspect-ratio-invariant visual cryptography (AAIVCS) without adding extra subpixels. Their results demonstrated a better aspect ratio than the traditional visual cryptographic scheme (VCS). They showed that their construction method had the smallest aspect ratio difference. Lin *et al.* (2015) presented a method for establishing a visual cryptographic scheme (VCS) with the ability to prevent cheating. Theoretical proof and computer simulation of their method was provided in paper. Yan *et al.* (2015) presented generalized random grids (RG) based threshold visual cryptography (VC) with meaningful shares. A theoretical analysis and simulation result of their method was given in paper. Their result demonstrated the effectiveness and security of their proposed scheme. Chiu & Lee (2015) proposed a systematic visual cryptography method with complementary cover images. Their results surpassed the previous methods in terms of the visual quality of the recovered images and of the meaningful shares. Yan *et al.* (2015) proposed halftone visual cryptography with minimum auxiliary black pixels (ABPs) and uniform image quality. Their simulation results demonstrated outperformed visual quality and some advantages compared with related meaningful visual cryptographic scheme (VCS). Ou *et al.* (2015) presented XOR-based visual cryptography (VC). Their method solved the problems of poor visual quality and pixel alignment in OR-based visual cryptography scheme. The result of their method was ensured for illustrating the correctness of the proposed XOR-based visual cryptography. Yan *et al.* (2014) presented three general threshold construction methods from specific cases in visual cryptography. Their results demonstrated the security and efficiency of the proposed methods. D'Arco *et al.* (2014) presented characterizations of optimal visual cryptography schemes. The proposed method provided a connection between the deterministic and the random grid models. Ateniese *et al.* (1996) presented two techniques to construct visual cryptography schemes for general access structures. They also ensured lower bounds on the size of

the shares distributed to the participants in the method and their method provided a new technique to realize k out of n threshold VCS. Blundo *et al.* (2006) presented VCS with optimal pixel expansion. They provided a lower bound on the pixel expansion of the scheme and, for $(2, n)$ -threshold VCS. Their result was compared with the previous method and their result demonstrated the efficiency and security of their VCS. Bharanivendhan & Amitha (2014) proposed VCS for secret image sharing using general access structures (GAS) algorithm. Their proposed scheme consisted of two phases. In the first phase, the input secret image generates the four meaningless shares based on GAS algorithm, which is done at the sender side. In the second phase, the cover image was added in each share directly by using stamping algorithm and distributed the embedded images to the participants. Their results demonstrated high security, increase in the number of shares and reduced the pixel expansion problem and high resolution to visualize the secret object. Wang *et al.* (2007) proposed both deterministic (n, n) scheme for gray scale images and probabilistic $(2, n)$ scheme for binary images. Wang *et al.* (2007), Wang *et al.* (2006), simple Boolean operations are used, but it has no pixel expansion. In here, the $(2, n)$ scheme provides a better contrast and significantly smaller recognized areas than other methods. The (n, n) scheme gives an exact reconstruction.

In this paper, a novel Letter based secret image sharing (LSIS) with data hiding algorithm for binary images is proposed. This LSIS method used letters of Arabic alphabet. A secret image sharing method, which is independent morphological features of letters, is obtained by using the proposed method. In this proposed secret image sharing, Arabic letters are used, because Arabic is one of the richest languages in the world. In the data hiding method, 2LSBs data hiding function is used.

The proposed LSIS algorithm method is described in section 2. The experimental results of LSIS and data hiding mode results are mentioned in section 3 and conclusions and recommendations have been discussed in section 4.

2. The proposed method

In this article, 28 letters of the Arabic alphabet are used for visual cryptography and secret sharing. Using these letters, it is planned to create a secret sharing scheme consisting of significant parts. Arabic letters used for creating the scheme are shown in Figure 1.

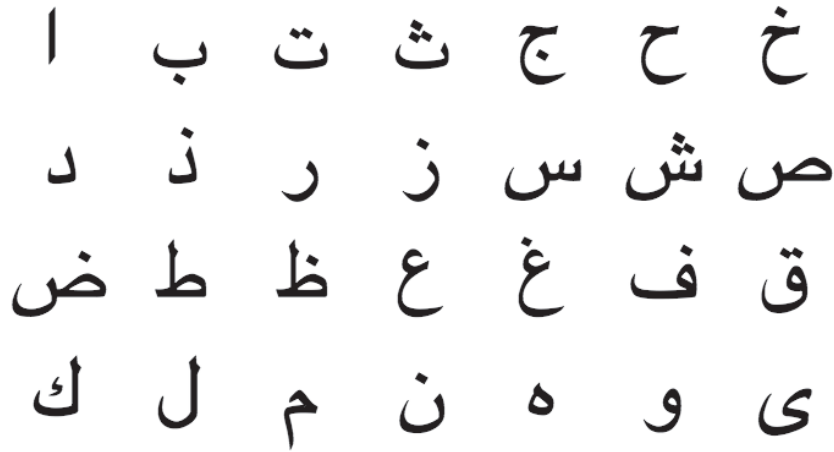


Fig. 1. Letters of Arabic alphabet.

A novel template based LSIS is created by using natural language letters. Letters of Arabic alphabet are expressed by 8 x 8 sized matrixes. The main purpose of using this matrix size is to encode letters as unique.

This matrix size is minimum adequate size for expressing letters. Each letter is defined using randperm (random permutation) function. Pseudo code of randperm function is given below.

Algorithm 1. Pseudocode of randperm function

Input: n is number of letters, perm= {1, 2, 3, ..., n} array of permutation, rand() is PRNG function.

1: **for** i=1 **to** n
 2: j = rand() (mod n-i)+i;
 3: t=perm(j);
 4: perm(j)=perm(i);
 5: perm(i)=t;
 6: **endfor**

Output: perm is randpermarray with size of n

The proposed method uses 28 Arabic letters for secret image sharing. The proposed method determines identifications of these letters by using randperm function.

Then, the watermark, which is divided into secret share is scanned by 2 x 2 sized matrix or window. If watermark is divided in n shares, n-1 of these shares are created randomly and obtained identities from meaningless secret share are used for finding letters, which are 8x8 sized matrixes. The last secret share is generated according to the obtained code from watermark. So, (n, n) secret image sharing scheme is created. The proposed secret image sharing scheme algorithm's steps are shown below.

Step 1: Use random permutation function for determining identifications of letters.

Step 2: Divide 2x2 sized matrices to threshold watermark and calculate target value for each matrices according to Equation 1.

$$T = WI_{i,j}2^3 + WI_{i,j+1}2^2 + WI_{i+1,j}2^1 + WI_{i+1,j+1}2^0 \quad (1)$$

Step 3: Create values of n-1 secret shares using pseudo random number generators. Linear congruential generator and cubic map generator formulas are given in Equations 2 and 3 for using alphabet.

$$x_{i+1} = [(cx_i + d \text{ mod } p) \text{ mod } 28] \tag{2}$$

$$x_{i+1} = \text{round} \left(27rx_i(1 - x_i^2) \right), 3.5 \leq r \leq 4, x \neq 0.5, x \in [0,1] \tag{3}$$

Step 4: Create last secret share by using equation of universal hash function. The equations of generating last secret share are given in Equations 4 and 5.

$$\text{total} = \sum_{i=1}^{n-1} c \cdot id_i + d \text{ (mod } p) \tag{4}$$

$$id_n = \text{total} + T \text{ (mod } 28) \tag{5}$$

The last secret share can take multiple values according to Equation 6. Value of the last secret share is selected randomly. So that uniform distribution of secret shares is provided.

Step 5: Repeat steps 2 and 4 until reaching size of watermark image.

Step 6: Embed each secret share into each layer of color images using 2LSBs data hiding function.

This secret sharing algorithm is similar to Wang’s probabilistic secret sharing algorithm (Wang *et al.*, 2007). (2,n) and (n,n) probabilistic secret sharing scheme are applied in this method. In this proposed method, (2,3) and (3,3) secret image sharing scheme is used for embedding secret data into RGB images. Moreover, universal hash function is used instead of Boolean operators. In this method, 2LSBs data hiding function is used for creating meaningful secret shares.

Camerman image and 3 secret shares of cameraman are given in Figure 2 and this image is divided into 3 secret shares by applying the proposed algorithm.


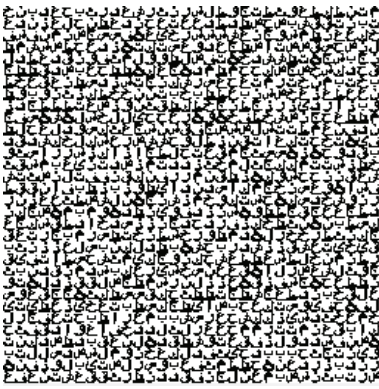
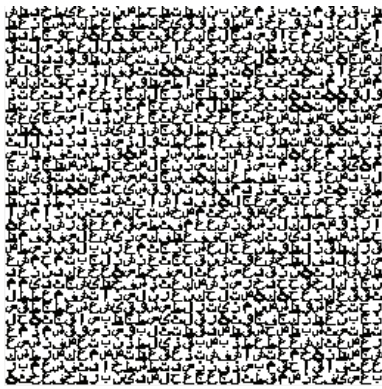
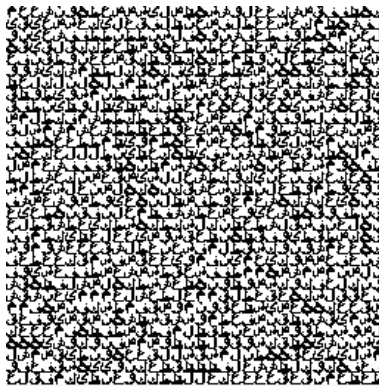
		
	(a) Original cameraman image	
		
(b) First secret share of cameraman	(c) Second secret share of cameraman	(d) Third secret share of cameraman

Fig. 2. Shares and original image of chessboard by using proposed algorithm

The pseudocode of the proposed secret sharing and data hiding method is given in Algorithm 2.

Algorithm 2. Pseudocode of the proposed method

Input: SI is secret binary image with size of $W \times H$, $\text{rand}()$ is PRNG, CI is cover image with size of $2W \times 2H \times 3$, AA is array of Arabic letters with size of $8 \times 8 \times 28$

```

1: row=0;
2: fori=1 to Wstep by 2do
3: col=0;
4: for j=1 to H step by 2 do
5: T is calculated by using Eq. 1.
6: val1=round(rand()*28)+1;
7: val2= round(rand()*28)+1;
8: total is calculated by using Eq. 4.
9: val3 is calculated by using Eq. 5.
10: SS1(row+1:row+8, col+1:col+8)=AA(:, :, val1);
11: SS2(row+1:row+8, col+1:col+8)=AA(:, :, val2);
12: SS3(row+1:row+8, col+1:col+8)=AA(:, :, val3);
13: col=col+8;
14: endfor
15: row=row+8;
16: endfor
17: Embed SS1, SS2 and SS3 into R, G and B layers of CI by using 2LSBs
Output: WI is watermarked image with size of  $2W \times 2H \times 3$ 

```

The original image acquisition steps from the resultant secret shares are given below.

Step 1: Use random permutation function for determining identifications of letters.

Step 2: Apply data extraction function to R, G and B channels of cover image.

Step 3: Obtain secret three shares.

Step 4: Pattern matching with window which size is 8×8 .

Step 5: If the pattern does not match the character patterns in the dictionary, match the characters of the index indicated on the map and automatically assign a value of 1 or 0 to pixels.

Step 6: The original pixel values to be obtained is calculated using the following equations.

$$T = \sum_{i=1}^n id_i(\text{mod } 28) \quad (6)$$

$$\text{value}(\text{mod } 16) = \text{dec2bin}(T, 4) \quad (7)$$

$$WI_{i,j} = \text{value}_1, WI_{i,j+1} = \text{value}_2, WI_{i+1,j} = \text{value}_3, WI_{i+1,j+1} = \text{value}_4, \quad (8)$$

$$i = \{1, 3, 5, \dots, m-1\}, j = \{1, 3, 5, \dots, n-1\}$$

Step 7: Repeat Steps 2 and 6 until size of the secret shares.

In this paper, (2,n) Wang's secret sharing scheme (Wang *et al.*, 2006) is used to obtain (k,n) secret sharing scheme.

3. Experimental results

In this section, the proposed LSIS secret image sharing algorithm is presented as watermarking model and testing performance of this method is evaluated. RGB images are used for obtaining experimental results as test images. The

watermark is divided to 3 secret shares and each of secret shares is embedded into R, G and B channels of test image respectively. In the experiments, eight test images of SIPI database (<http://sipi.usc.edu/database>) are used. These images are used as cover images which are 512x512x3 sized. These are "Lena", "Peppers", "Baboon", "F16", "Barbara", "Tiffany", "Goldhill" and "Sailboat". Two watermarks are embedded into cover images. The size of these watermarks is 128x256. After implementation of proposed LSIS, each of secret share size will be 512x1024. The used binary images as watermarks for experiments are shown in Figure 3.

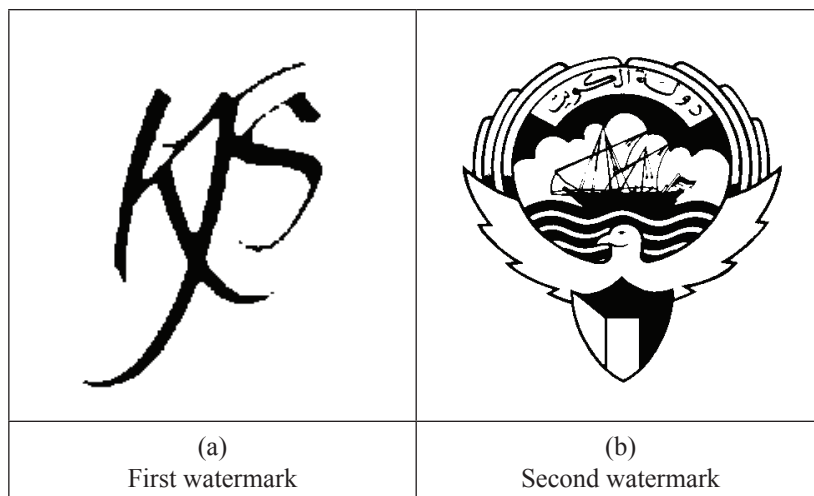


Fig. 3. The used binary images as watermarks for experiments.

LSIS (3,3) of proposed algorithm is shown in Figure 4 and LSIS (2,3) is shown in Figure 5.

In LSIS (3,3), used watermark is obtained by combining the 3 secret shares. In LSIS (2,3), used watermark is obtained by combining the 2 secret shares.

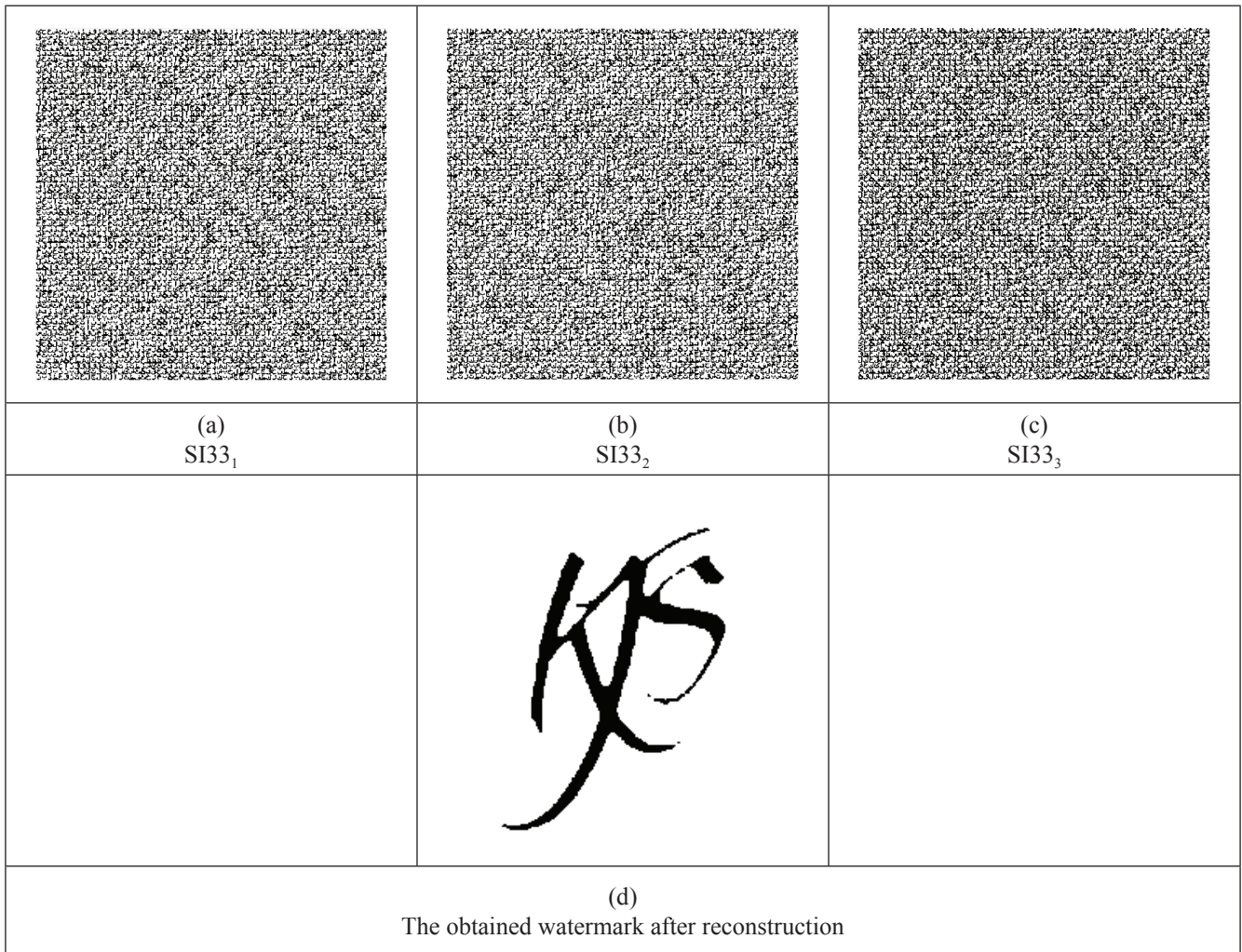


Fig. 4. The composed secret shares using LVCS (3,3).

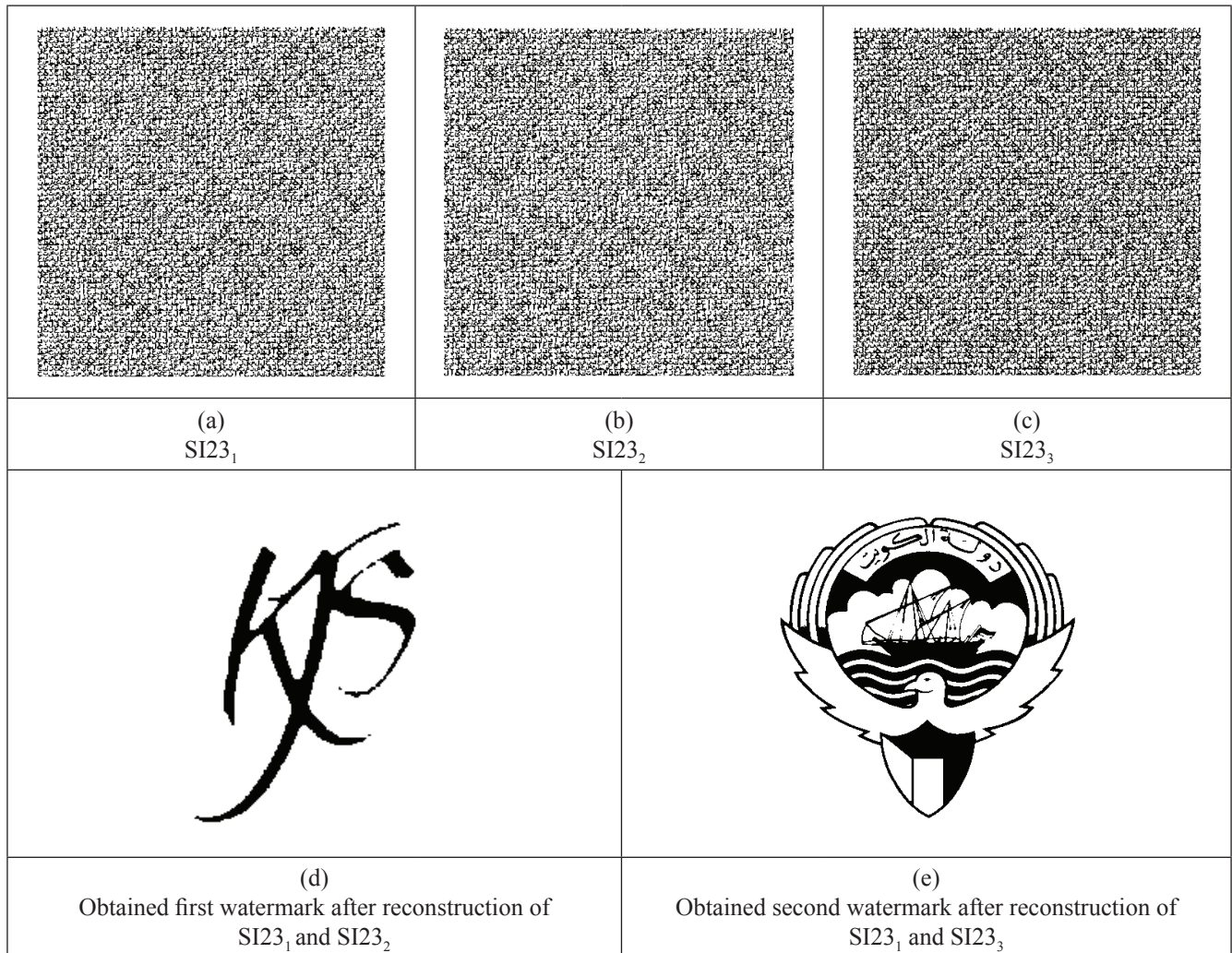


Fig. 5. The composed secret shares using LSIS (2,3).

$$MSE = \frac{1}{mn} \sum_{i=1}^m \sum_{j=1}^n (CI_{i,j} - SI_{i,j})^2 \quad (9)$$

$$PSNR = 10 \log \frac{\max(CI_{i,j}^2)}{MSE} \quad (10)$$

The watermark is divided into 3 secret shares. These secret shares are named as shadows. The shadows

are embedded into R, G, B channels of cover image respectively. Mean square error (MSE) and Peak signal noise rate (PSNR) are used for evaluating the test performance of proposed LSIS method and their equations are given in Equations 9 and 10 (Tanchenko, 2014, Choi, 2013). The obtained PSNR values of test images are shown in Table 1.

Table 1. Experimental results of the proposed LSIS method for different test images.

Image	PSNR Color Image	Shadow 1 R layer	Shadow 2 G layer	Shadow 3 B layer
Lena	43.5657	43.5946	43.5704	43.5324
Peppers	43.4229	43.5714	43.3871	43.3142
Baboon	43.5633	43.6111	43.5692	43.5101
F16	43.5254	43.5780	43.5367	43.4622
Barbara	43.5888	43.6041	43.6155	43.5472
Tiffany	43.5910	43.6753	43.5620	43.5371
Goldhill	43.5719	43.6039	43.5791	43.5329
Sailboat	43.5198	43.5619	43.5434	43.4548

The proposed LSIS method provides noiseless reconstruction. The test performance of LSIS method is compared to Shamir's method (Naor & Shamir, 1994) and Lin *et al.*'s method (Lin *et al.* 2013) in this experiments. Comparison results are shown in Figure 6.

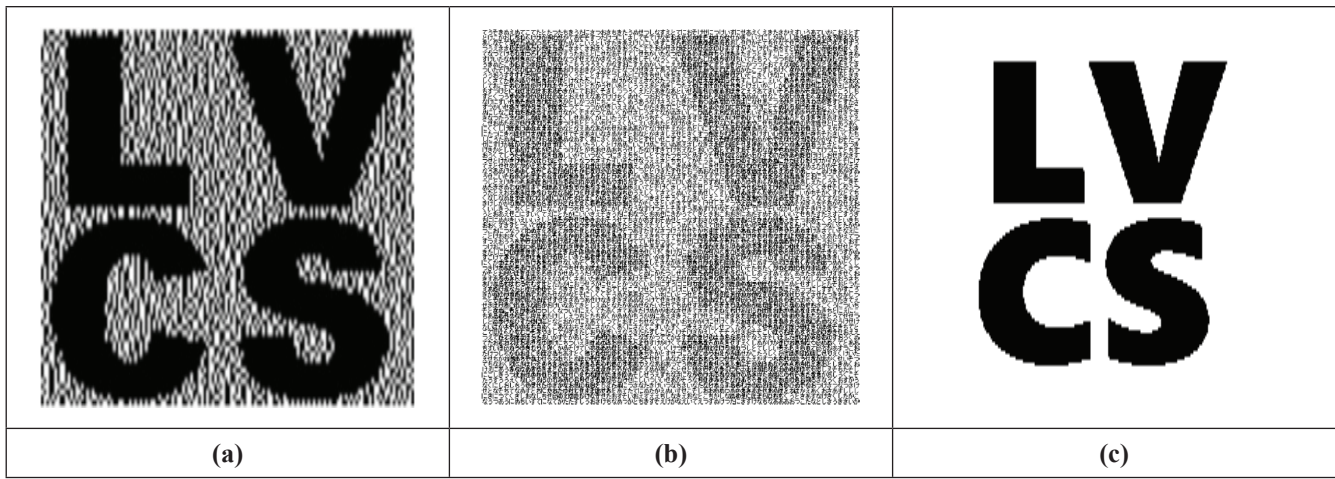


Fig. 6. (a) Reconstructed image with using Shamir and Naor Method, (b) Reconstructed image with using Lin *et al.* Method, (c) Reconstructed image with using proposed LSIS method.

4. Conclusion

In this proposed secret image sharing, Arabic letters are used because of Arabic is one of the richest languages in the world (Gutub 2010, Parvez & Gutub 2011). In this paper, Arabic letters are used for visual cryptography. This alphabet has 28 letters. The proposed LSIS algorithm provides noiseless reconstruction. In this study, the prime cyclic groups are used for identification of letters and this study shows that noiseless secret image sharing algorithm can be developed using natural languages. Pseudo random number generator (PRNG) is used for providing the uniform distribution of letters at these experiments. Thus, data hiding mode for authenticate images is developed. Then, measuring visual quality of this proposed LSIS method is done by using PSNR values. The obtained results are very impressive.

In here, letter based secret image sharing (LSIS) is used for protecting image contents. For this purpose, secret sharing and data hiding algorithms are used together in this LSIS method. The LSIS method consists of two parts. These are generating of meaningful secret sharing and data hiding. Secret sharing and visual cryptography methods commonly generate noise-like images. The noise-like images have attracted the attention of the attackers and several attacks have been developed to break these encrypted images. To prevent these attacks, meaningful secret shares are generated and these secret shares are embedded into cover image. A novel secret image sharing method based on Arabic letters is proposed.

The proposed method uses Arabic letters for generating meaningful secret shares and data hiding functions for data hiding. RGB images are used for cover images. In proposed method, secret shares are embedded into R, G and B channels respectively. Thus, cheatings occurring in visual cryptography are prevented.

References

- Ateniese, G., Blundo, C., De Santis, A. & Stinson, D.R. (1996). Visual cryptography for general access structures. *Information and Computation*, **129**:86–106.
- Bharanivendhan, N. & Amitha, T. (2014). Visual cryptography schemes for secret image sharing using GAS Algorithm. *International Journal of Computer Applications*, **92**(8):11-16
- Blundo, C., Cimato, S. & De Santis, A. (2006). Visual cryptography schemes with optimal pixel expansion. *Theoretical Computer Science*, **369**:169–182.
- Chiu, P.L. & Lee, K.H. (2015). User-friendly threshold visual cryptography with complementary cover images. *Signal Processing*, **108**:476-488.
- Choi, Y. & Aizawa, K. (2002). Digital watermarking technique using block correlation of DCT coefficients. *Electronics and Communications in Japan (Part II: Electronics)*, **85**(9):23–31.
- Choi, K.S. (2013). Bit plane modification for improving MSE-near optimal DPCM-based block truncation coding. *Digital Signal Processing*, **23**(4):1171-1180.
- D'Arco, P., De Prisco, R. & De Santis, A. (2014). Measure-independent characterization of contrast optimal visual cryptography schemes. *Journal of Systems and Software*, **95**:89-99.
- Gutub, A., Ghouti, L., Elarian, Y., Awaideh, S. & Alvi, A. (2010). Utilizing diacritic marks for arabic text steganography. *Kuwait Journal of Science & Engineering*, **37**(1):89-109.
- Govind, P.V.S. & Wilsy, M. (2015). A new reversible data hiding

scheme with improved capacity based on directional interpolation and difference expansion. *Procedia Computer Science*, **46**:491-498.

Hussain, I. (2013). A novel approach of audio watermarking based on image-box transformation. *Mathematical and Computer Modelling*, **57**(3-4):963-969.

Khamrui, A. & Mandal, J.K. (2013). A genetic algorithm based steganography using discrete cosine transformation (GASDCT). *Procedia Technology*, **10**:105-111.

Lee, S.H. (2014). DWT based coding DNA watermarking for DNA copyright protection. *Information Sciences*, **273**:263-286.

Lin, C.C., Liu, X.L. & Yuan, S.M. (2015). Reversible data hiding for VQ-compressed images based on search-order coding and state-codebook mapping. *Information Sciences*, **293**:314-326.

Lin, Y.K. (2014). A data hiding scheme based upon DCT coefficient modification. *Computer Standards & Interfaces*, **36**(5):855-862.

Lin, H.C., Yang, C.N., Lai, C.S. & Lin, H.T. (2013). Natural language letter based visual cryptography scheme. *Journal of Visual Communication and Image Representation*, **24**(3):318-331.

Lin, P.Y., Wang, R.Z., Chang, Y.J. & Fang, W.P. (2015). Prevention of cheating in visual cryptography by using coherent patterns. *Information Sciences*, **301**:61-74.

Liu, Y. & Zhao, J. (2010). A new video watermarking algorithm based on 1D DFT and Radon transform. *Signal Processing*, **90**(2):626-639.

Liu, J.F., Tian, Y.G., Han, T., Yang, C.F. & Liu, W.B. (2015). LSB steganographic payload location for JPEG-decompressed images. *Digital Signal Processing*, **38**:66-76.

Lou, D.C. & Hu, C.H. (2012). LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis. *Information Sciences*, **188**:346-358.

Mandal, J.K. (2012). Watermarking in transform domains (WTD). *Procedia Technology*, **4**:19-26.

Nair, N.S., Mathew, T.A., Neethu, S., Viswanath, V.P., Nair, M. S. et al. (2015). A proactive approach to reversible data hiding in encrypted images. *Procedia Computer Science*, **46**:1510-1517.

Nazari, S., Moghadam, A.M.E. & Moin, M.S. (2015). A novel image steganography scheme based on morphological associative memory and permutation schema. *Security and Communication Networks*, **8**(2):110-121.

Naor, M. & Shamir, A. (1994). Visual cryptography, in: A. DeSantis (Ed.), *Advances in Cryptology – EUROCRYPT'94*. Lecture Notes in

Computer Science, Perugia, Italy, **950**:1-12.

Ou, D., Sun, W. & Wu, X. (2015). Non-expansible XOR-based visual cryptography scheme with meaningful shares. *Signal Processing*, **108**:604-621.

Parvez, M.T. & Gutub, A.A. (2011). Vibrant color image steganography using channel differences and secret data distribution. *Kuwait Journal of Science and Engineering*, **38**(1B):127-142.

SIPI Image Dataset, University of Southern California, signal and image processing institute. Available online: <http://sipi.usc.edu/database> (05.01.2016).

Tanchenko, A. (2014). Visual-PSNR measure of image quality. *Journal of Visual Communication and Image Representation*, **25**(5):874-878.

Veerappan, J. & Pitchammal, G. (2012). Interpolation based image watermarking using segmentation resisting to geometrical attacks. *Procedia Engineering*, **38**:3528-3540.

Yang, C.N. & Lin, C.Y. (2015). Almost-aspect-ratio-invariant visual cryptography without adding extra subpixels. *Information Sciences*, **312**:131-151.

Yan, X., Wang, S., Niu, X. & Yang, C.N. (2015). Generalized random grids-based threshold visual cryptography with meaningful shares. *Signal Processing*, **109**:317-333.

Yan, X., Wang, S., Niu, X. & Yang, C.N. (2015). Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. *Digital Signal Processing*, **38**:53-65.

Yan, X., Wang, S. & Niu, X. (2014). Threshold construction from specific cases in visual cryptography without the pixel expansion. *Signal Processing*, **105**:389-398.

Wang, D., Li, X. & Yi, F. (2007). Probabilistic (n, n) visual secret sharing scheme for grayscale images. In *Information Security and Cryptology*. Lecture Notes in Computer Science, **4990**:192-200.

Wang, D., Zhang, L., Ma, N. & Li, X. (2006). Two secret sharing schemes based on Boolean operations. *Pattern Recognition*, **40**(10):2776-2785.

Wu, X. & Sun, W. (2012). Random grid-based visual secret sharing for general access structures with cheat-preventing ability. *Journal of Systems and Software*, **85**(5):1119-1134.

Submitted : 21/12/2015

Revised : 08/03/2016

Accepted : 15/03/2016

طريقة جديدة لمشاركة صورة سرية ذات مغزى على أساس حروف عربية

دریا أفسی

قسم الهندسة الكهربائية والإلكترونية، كلية الهندسة، جامعة فرات، إيلازيق، تركيا

المؤلف: derya2344@hotmail.com

خلاصة

في السنوات الأخيرة، أصبح توفير أمن المعلومات للوسائط المتعددة موضوعاً هاماً للدراسة. التشفير البصري والتشارك في السر يوفر طريقة لأمن المعلومات دون استخدام شفرة رياضية معقدة. وبالتالي يتم استخدام التشفير البصري وتقاسم السر على نطاق واسع. في هذه الورقة، نستخدم تقاسم صورة سرية على أساس أحرف (LSIS) لحماية محتويات الصورة. لهذا الغرض، يتم استخدام خوارزميات لسرية تبادل وإخفاء البيانات معا في هذه الطريقة. وتتكون طريقة LSIS من جزأين: توليد مفتاح سري ذا مغزى مشترك وإخفاء البيانات.

التقاسم السري وأساليب التشفير البصرية عادة تولد صوراً تشبه الضوضاء. وتلك الصور تجذب انتباه المهاجمين والعديد من الهجمات وضعت لكسر هذه الصور المشفرة. لمنع هذه الهجمات، يتم إنشاء صور مشتركة سرية ذات معنى، وجزءاً من هذه الصور السرية يوضع في صورة غلاف.

في هذه الورقة، نقترح طريقة جديدة لمشاركة الصور السرية على أساس الحروف العربية. الطريقة المقترحة تستخدم الحروف العربية لتوليد صوراً سرية ذات معنى وتستخدم دوال إخفاء البيانات للتمويه. صور RGB تستخدم لتغطية الصور. في الطريقة المقترحة، تكون الصور المشتركة جزءاً من قنوات ال B ، G ، R على التوالي. وهكذا يتم منع التزوير الذي يحدث في التشفير البصري. طريقة مشاركة الصور السرية المقترحة لا تعتمد على الميزات المورفولوجية للأحرف. وتستخدم الحروف العربية لأن اللغة العربية هي واحدة من أغنى اللغات في العالم. في هذه الطريقة يتم استخدام الدالة 2LSBs لإخفاء البيانات.

الكلمات المفتاحية: إخفاء البيانات؛ معالجة الصورة؛ أمن المعلومات؛ تقاسم صورة سرية ذات معنى؛ التشفير البصري.