sciendo

Int. J. Appl. Math. Comput. Sci., 2019, Vol. 29, No. 4, 817–829
DOI: 10.2478/amcs-2019-0060

amcs

IMPROVED REFERENCE IMAGE ENCRYPTION METHODS BASED ON 2^K CORRECTION IN THE INTEGER WAVELET DOMAIN

TURKER TUNCER [a], SENGUL DOGAN [a], RYSZARD TADEUSIEWICZ [b], PAWEŁ PŁAWIAK [c,*]

[a]Department of Digital Forensics Engineering
Firat University, University Street, 23119 Elazig, Turkey
e-mail: {turkertuncer,sdogan}@firat.edu.tr

[b]Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering
AGH University of Science and Technology, al. Mickiewicza 30, 30-059 Cracow, Poland
e-mail: rtad@agh.edu.pl

[c]Department of Information and Communications Technology, Faculty of Computer Science and Telecommunications
Cracow University of Technology, ul. Warszawska 24, 31-155 Cracow, Poland
e-mail: plawiak@pk.edu.pl

Many visually meaningful image encryption (VMIE) methods have been proposed in the literature using reference encryption. However, the most important problems of these methods are low visual quality and blindness. Owing to the low visual quality, the pre-encrypted image can be analyzed simply from the reference image and, in order to decrypt nonblind methods, users should use original reference images. In this paper, two novel reference image encryption methods based on the integer DWT (discrete wavelet transform) using 2^k correction are proposed. These methods are blind and have high visual quality, as well as short execution times. The main aim of the proposed methods is to solve the problem of the three VMIE methods existing in the literature. The proposed methods mainly consist of the integer DWT, pre-encrypted image embedding by kLSBs (k least significant bits) and 2^k correction. In the decryption phase, the integer DWT and pre-encrypted image extraction with the mod operator are used. Peak signal-to-noise ratio (PSNR) measures the performances of the proposed methods. Experimental results clearly illustrate that the proposed methods improve the visual quality of the reference image encryption methods. Overall, 2^k correction and kLSBs provide high visual quality and blindness.

Keywords: visually meaningful image encryption, 2^k correction, discrete wavelet transform, least significant bits embedding.

1. Introduction

Nowadays, image processing has become one of the most important research areas in information security (Lee, 2014; Liu and Wu, 2011; Chang *et al.*, 2008). Data hiding, watermarking and cryptography methods have been generally used to provide information security of images (Chen *et al.*, 2014; Peng *et al.*, 2012; Prasanth Vaidya and Chandra Mouli, 2018). The main purpose of data hiding is to embed the secret message into a cover image that looks innocent and protects it from attackers. Watermarking techniques are used for copyright protection and authentication. Image encryption methods provide confidentiality by changing the content of the image and they are widely used for information security methods (Tuncer and Avci, 2016).

However, today there is no encryption standard for images and many image encryption methods do not provide information because the most important evaluation criteria are statistical models. Therefore, many cryptanalysis attacks did not apply these methods. They use only statistical evaluation criteria, e.g., the number of pixel change rates (NPCR) (Prasanth Vaidya and Chandra Mouli, 2017). It is also very easy to understand that an image is encrypted because image encryption methods often transform images into noise-like or texture-like forms (Chen *et al.*, 2004; Ghebleh *et al.*, 2014).

*Corresponding author

VMIE methods are proposed to increase confidentiality. These methods convert the image into a meaningful form. Noise-like, texture-like and visually meaningful encrypted images are shown in Fig. 1 (Dhall *et al*., 2018; Bao and Zhou, 2015; Kanso and Ghebleh, 2017; Yang *et al*., 2018).

VMIE methods consist of two encryption phases, these are pre-encryption and reference image encryption. Pre-encryption methods generally produce noise-like encrypted images. In reference image encryption, a pre-encrypted image is embedded into wavelet sub-bands of the reference image. The wavelet transform has been widely used to transform images and there are integer versions of the wavelets. Therefore, lossless encryption methods have been proposed using integer wavelet transformations, which also provides robustness (Bao and Zhou, 2015; Kanso and Ghebleh, 2017; Yang *et al*., 2018). Hence, the wavelet transformation is used for reference image encryption. Any robust and integer transformation can be used in reference image encryption. In this phase, wavelet sub-bands such as Low-High (LH), High-Low (HL) and High-High (HH) are used to achieve high visual quality (Liu and Wu, 2011; Avci *et al*., 2016).

Three important VMIE methods were proposed in the literature. These are the Bao and Zhou (BZ) (Bao and Zhou, 2015), Yang *et al.* (Yang *et al*., 2018) as well as Kanso and Ghebleh (KG) (Kanso and Ghebleh, 2017) methods. The main problems involved in these methods are as follows:

- The BZ method (Bao and Zhou, 2015) is the first VMIE method. The pre-encrypted image is embedded into HL and HH sub-bands but any of the data hiding methods is not used. Thus, the visual quality of this method is low.
- In order to improve visual quality of the BZ method, Yang *et al*. (2018) proposed a VMIE method. The pre-encrypted image is embedded into LH, HL and HH sub-bands. However, the original reference image is required to decrypt the encrypted reference image. Thus, this method has non-blind reference image decryption.
- The KG method (Kanso and Ghebleh, 2017) is a reference image encryption method using data hiding. However, an optimum visual quality value is not obtained in this method because the authors embedded 3, 3 and 2 bits into LH, HL and HH sub-bands respectively. 2^k correction was not used in their method.

Motivations of this paper are the following. The problems of VMIE are given as above. As we know from the literature, VMIE methods generally use either 2 or 3 wavelet sub-bands. To use optimal bands with optimum and simple methods, two novel reference image encryption methods are presented. The main characteristics and contributions of the proposed methods are listed below:

- 2^k correction methods are used for increasing the visual quality in the proposed methods.
- Optimal *DWT* sub-bands are selected to increase imperceptibility.
- Two novel reference image encryption methods are presented to solve the visual quality problem of the previously presented VMIE methods.
- The presented methods have short execution times. This situation demonstrate that these methods can be easily used in real world applications.
- To the best of our knowledge, this is the first article about reference image encryption using the 2^k correction method up to now.

The abbreviations used in this article are as follows:

2D DWT: two-dimensional discrete wavelet transform,

PE: pre-encryption function,

E: encryption function,

RE: reference image encryption,

I: image,

LL: low-low sub-band,

LH: low-high sub-band,

HL: high-low sub-band,

HH: high-high sub-band.

The structure of rest of this article is as follows. In Section 2, we characterize three state-of-the-art reference image encryption methods of VMIE. The 2^k correction method is explained in Section 3. The proposed reference image encryption methods are presented in Section 4. Results and discussions are given in Section 5 and, finally, conclusions are given in Section 6.

2. Related works

In this section, popular and previously presented VMIE methods in the literature are reviewed. VMIE methods generally consist of pre-encryption and reference image encryption. The general graphical outline of VMIE methods is shown in Fig. 2.

The general mathematical description of the VMIE is given by

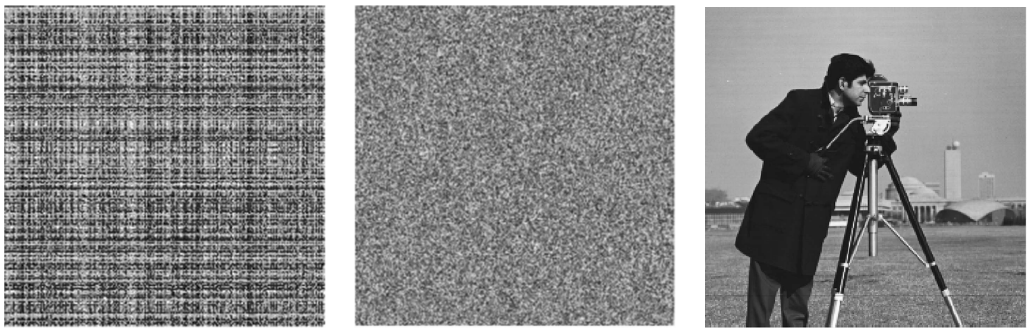
$$P = \text{PE}(I, K_1). \tag{1}$$

$$E = \text{RE}(R, P, K_2), \tag{2}$$

$$P = \text{RD}(E, K_2), \tag{3}$$

$$I = \text{PD}(P, K_1), \tag{4}$$

where I is original image, P is the pre-encrypted image, E is the final encrypted image, K_1 is the key of the pre-encryption method, K_2 is the key of reference image encryption and K_2 is used for integer wavelet filter selection, $\text{PE}(\cdot)$ is the pre-encryption function, $\text{RE}(\cdot)$ is the reference image encryption function, $\text{PD}(\cdot)$ is the



(a) (b) (c)

Fig. 1. Different cipher images: a texture-like encrypted image (a), a noise-like encrypted image (b), a visually meaningful encrypted image (c).

pre-decrypted function and RD$(\cdot)$ represents the reference the image decryption function.

These equations define pre-encryption, reference image encryption, reference image decryption and pre-image decryption, respectively. These methods use two keys. The first key is used for encryption and decryption of the pre-image and the second key is utilized for reference image encryption and decryption.

The mathematical description of the non-blind reference image decryption is

$$P = \text{RD}(E, R, K_2). \tag{5}$$

Reference image encryption methods are similar to data hiding methods. Therefore, visual quality is used for evaluating these methods because imperceptibility is very important for reference image encryption methods (Ghebleh *et al.*, 2014; Dhall *et al.*, 2018; Bao and Zhou, 2015; Kanso and Ghebleh, 2017; Avci *et al.*, 2016).

2.1. Bao and Zhou method. This method is the first known VMIE method (Bao and Zhou, 2015). It consists mainly of pre-encryption and reference image encryption sections. In this method, it is clearly shown that the pre-encryption method can use one of the secure image encryption methods in the literature. The originality of the method is reference image encryption. The reference image encryption method of the BZ technique is given as Algorithm 1.

Reference image decryption of the BZ method is mathematically described by

$$[\text{LL}, \text{LH}, \text{HL}, \text{HH}] = \text{DWT2}(R, K_2), \tag{6}$$

$$P = \text{HL} \times 10 + \text{HH}, \tag{7}$$

where DWT2$(\cdot)$ is the integer 2D DWT (Faragallah, 2013). Equations (6) and (7) show that the BZ method has a blind decryption scheme. K_2 represents the key of the wavelet filter. There are 37 integer wavelet filters. One of them is selected using this key, because the original reference image is not required by the original reference image decryption method.

Algorithm 1. Reference image encryption of the BZ method.

Input: Pre-encrypted image P with size $W \times H$, reference image R with size $2W \times 2H$ and reference image encryption key K_2.

Output: Final cipher image E with size $2W \times 2H$.

1: Apply the integer 2D DWT to the reference image (R) and obtain LL, LH, HL and HH sub-bands using K_2.
2: for $i = 1$ to W **do**
3: **for** $j = 1$ to H **do**
4: $\text{HL}_{i,j} = [P_{i,j}/10]$
5: $\text{HH}_{i,j} = P_{i,j} (\text{mod } 10)$
6: **endfor**
7: endfor
8: Apply the inverse integer 2D DWT and obtain the final cipher image E.

2.2. Kanso and Ghebleh method. A reference image encryption method based on kLSBs was proposed by Kanso and Ghebleh (2017). The KG method consists of integer 2D DWT, bit division of the pre-encrypted image, pre-encrypted image embedding into wavelet sub-bands of the reference images using 2LSBs and 3LSBs. The pseudo-code of reference image encryption of the KG method is listed in Algorithm 2.

There are two steps of the reference image decryption of the KG method:

Step 1: Apply (6) to final encrypted image and obtain LL, LH, HL and HH sub-bands of the final encrypted image.

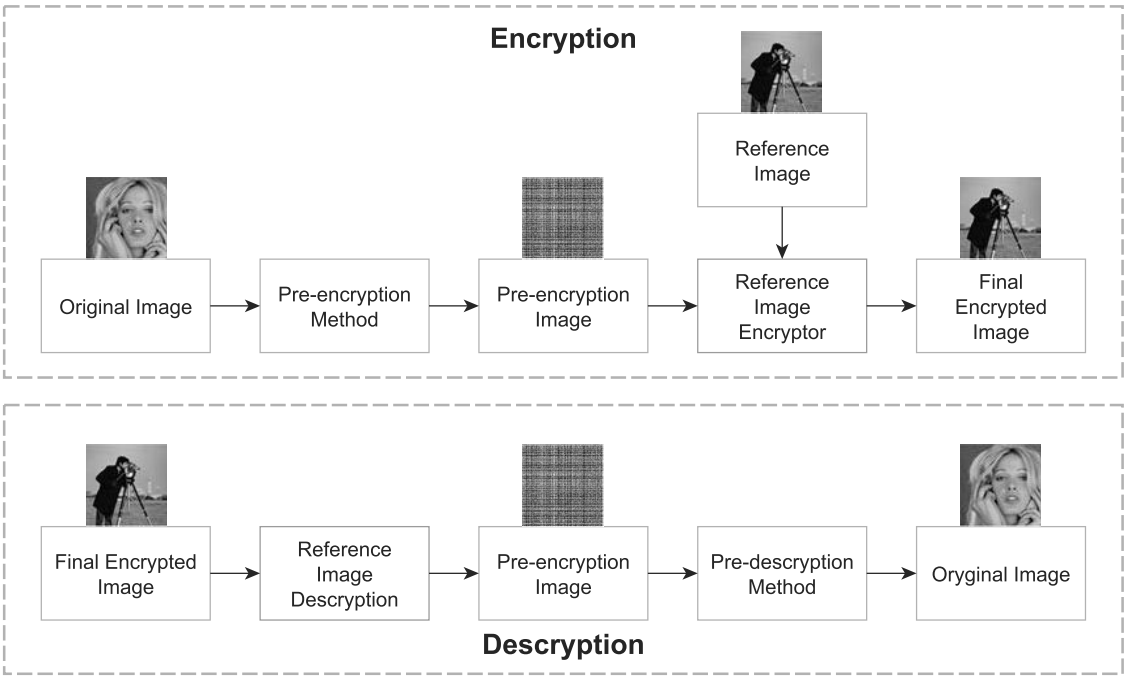


Fig. 2. General block diagram of VMIE.

Step 2: Use

$$P = (\text{LH}(\text{mod } 8)) \times 2^5 + (\text{HL}(\text{mod } 8)) \times 2^2 + \text{HH}(\text{mod } 4). \quad (8)$$

to extract pre-encrypted image to final encrypted image.

The KG method has a blind reference image decryption function.

2.3. Yang *et al.* method. Another VMIE method was proposed by Yang *et al*. (2018). Its main purpose is to eliminate the texture feature in visually meaningful cipher images. Reference image encryption of this method consists of the integer 2D DWT, digit separation of pixel values of the pre-encrypted image and digits embedding into LH, HL and HH sub-bands of the reference image. However, the data hiding method used in this technique is not blind because reference image decryption of the Yang *et al.* method uses the original reference image. The reference image encryption algorithm of the Yang *et al.* method is listed below.

The reference image decryption of the Yang *et al.* method is given by

$$[\text{LL}^R, \text{LH}^R, \text{HL}^R, \text{HH}^R] = \text{DWT2}(R, K_2), \quad (9)$$

$$[\text{LL}^E, \text{LH}^E, \text{HL}^E, \text{HH}^E] = \text{DWT2}(E, K_2), \quad (10)$$

Algorithm 2. Reference image encryption of the KG method.

Input: Pre-encrypted image P with size $W \times H$, reference image R with size $2W \times 2H$ and reference image encryption key K_2.

Output: Final cipher image E with size $2W \times 2H$.

1: Apply the integer 2D DWT to R and obtain LL, LH, HL and HH sub-bands of R using K_2.

2: for $i = 1$ to W **do**

3: **for** $j = 1$ to H **do**

4: $\text{LH}_{i,j} = \left\lfloor \frac{P_{i,j}}{32} \right\rfloor + \left\lfloor \frac{\text{LH}_{i,j}}{8} \right\rfloor \times 8$

5: $\text{HL}_{i,j} = \left\lfloor \frac{P_{i,j} - 32 \times (P_{i,j}(\text{mod } 8))}{4} \right\rfloor + \left\lfloor \frac{\text{HL}_{i,j}}{8} \right\rfloor \times 8$

6: $\text{HH}_{i,j} = P_{i,j}(\text{mod } 4) + \left\lfloor \frac{\text{HH}_{i,j}}{4} \right\rfloor \times 4$

7: **endfor**

8: endfor

9: Apply the inverse integer 2D DWT and obtain the final cipher image E.

$$P = (\text{LH}^E - \text{LH}^R) \times 10^2 + (\text{HL}^E - \text{HL}^R) \times 10^1 + (\text{HH}^E - \text{HH}^R) \times 10^0, \quad (11)$$

where LL^R, LH^R, HL^R, HH^R are integer wavelet sub-bands of the reference image and LL^E, LH^E, HL^E,

Algorithm 3. Reference image encryption of the KG method.

Input: Pre-encrypted image P with size $W \times H$, reference image R with size of $2W \times 2H$ and reference image encryption key K_2.

Output: The final cipher image E with size $2W \times 2H$.

1: Apply the integer 2D DWT to R and obtain LL, LH, HL and HH sub-bands of R using K_2.
2: for $i = 1$ to W **do**
3: **for** $j = 1$ to H **do**
4: $\mathrm{LH}_{i,j} = \left\lfloor \frac{P_{i,j}}{100} \right\rfloor + \mathrm{LH}_{i,j}$
5: $\mathrm{HL}_{i,j} = \left\lfloor \frac{P_{i,j} (\mathrm{mod}\ 100))}{10} \right\rfloor + \mathrm{HL}_{i,j}$
6: $\mathrm{HH}_{i,j} = P_{i,j} (\mathrm{mod}\ 10) + \mathrm{HH}_{i,j}$
7: **endfor**
8: endfor
9: Apply the inverse integer 2D DWT and obtain the final cipher image E.

HH^E are integer wavelet sub-bands of the final encrypted image. This method is superior to the BZ method in terms of the visual quality but decryption of this method is not blind.

3. 2^k Correction

The 2^k correction method is one of the methods used to increase the visual quality in data hiding. This method increases the visual quality of kLSBs (k least significant bits) data hiding methods. The mathematical description of the 2^k correction is the following (Sun, 2016):

$$\mathrm{SP} = \left\lfloor \frac{\mathrm{OP}}{2^k} \right\rfloor \times 2^k + \mathrm{SD}, \tag{12}$$

$$\mathrm{NSP} = \begin{cases} \mathrm{SP} - 2^k & \text{if } \mathrm{SP} - \mathrm{OP} > 2^{k-1} \text{ and} \\ & \mathrm{SP} - 2^k \geq \mathrm{LB}, \\ \mathrm{SP} + 2^k & \text{if } \mathrm{SP} - \mathrm{OP} < 2^{k-1} \text{ and} \\ & \mathrm{SP} + 2^k \leq \mathrm{UB}, \\ \mathrm{SP} & \text{otherwise}, \end{cases} \tag{13}$$

where SP is the stego pixel value, OP is the original pixel value, NSP is the new stego pixel and SD means secret data, LB is a lower bound and UB is an upper bound. Equation (12) defines and Eqn. (13) defines the kLSBs 2^k correction. The advantage of 2^k correction is given in the following example.

Example 1. Assume that a pixel value is 201 and secret data is 5. If these secret data are embedded into this pixel value using 3LSBs, the stego pixel is calculated as $\lfloor 201/2^3 \rfloor \times 2^3 + 6 = 206$. If the 2^k correction method is applied to the stego pixel, the new stego pixel is calculated as $206 - 8 = 198$. The difference between the original pixel and the stego pixel is $|201 - 206| = 5$ and the difference between the original pixel and new stego pixel is $|201 - 198| = 3$. This example shows that the difference between the new stego pixel and the original pixel is smaller than the difference between the stego pixel and the original pixel and that higher imperceptibility can be achieved using the 2^k correction method. ♦

4. Proposed blind reference encryption methods

The reference image encryption methods are divided into two sub-groups according to the wavelet sub-bands used. In the first group, HL and HH sub-bands are used for pre-encrypted image embedding and LH, HL and HH sub-bands are used in the second group. Thus, two novel reference image encryption methods are proposed for VMIE in this paper. The main objective of these methods is to achieve blind reference image encryption with high visual quality. The proposed methods are called as Scheme 1 and Scheme 2. Scheme 1 consists of bit separation of the pre-encrypted image, the integer 2D DWT, embedding pre-encrypted image bits into HL and HH sub-bands by 4LSBs and 2^4 corrections. Scheme 1 is similar to the BZ method. Scheme 1 achieved optimum visual quality using 4LSBs and 2^4 corrections together for HL and HH sub-bands. Scheme 2 is similar to Scheme 1 but it divides the pre-encrypted image pixels into 2, 3 and 3 bits and these bits are embedded into LH, HL, HH sub-bands, respectively. Finally, 2^2, 2^3 and 2^3 corrections are applied to stego LH, HL and HH sub-bands. The main purpose of Scheme 2 is to achieve better visual quality than for the Yang *et al.* and KG methods because these methods used LH, HL and HH sub-bands, too. Schemes 1 and 2 are described in Sections 4.1 and 4.2, respectively.

4.1. Scheme 1. The main objective of this method is to achieve a more successful reference image encryption method by modifying the BZ reference image encryption method. Scheme 1 consists of MSB and LSB separation, integer the 2D DWT, pre-encrypted image embedding by 4LSBs and 2^4 corrections. Block diagram of Scheme 1 is shown in Fig. 3.

The pseudo code of Scheme 1 is shown as Algorithm 4.

Steps of the decryption of Scheme 1 are as follows:

Step 1: Apply the integer $2DDWT$ to the final encrypted image using K^2 and obtain LL, LH, HL and HH.

Step 2: Use

$$P = 16 \times (\mathrm{HL}(\mathrm{mod}\ 16)) + \mathrm{HH}(\mathrm{mod}\ 16) \tag{14}$$

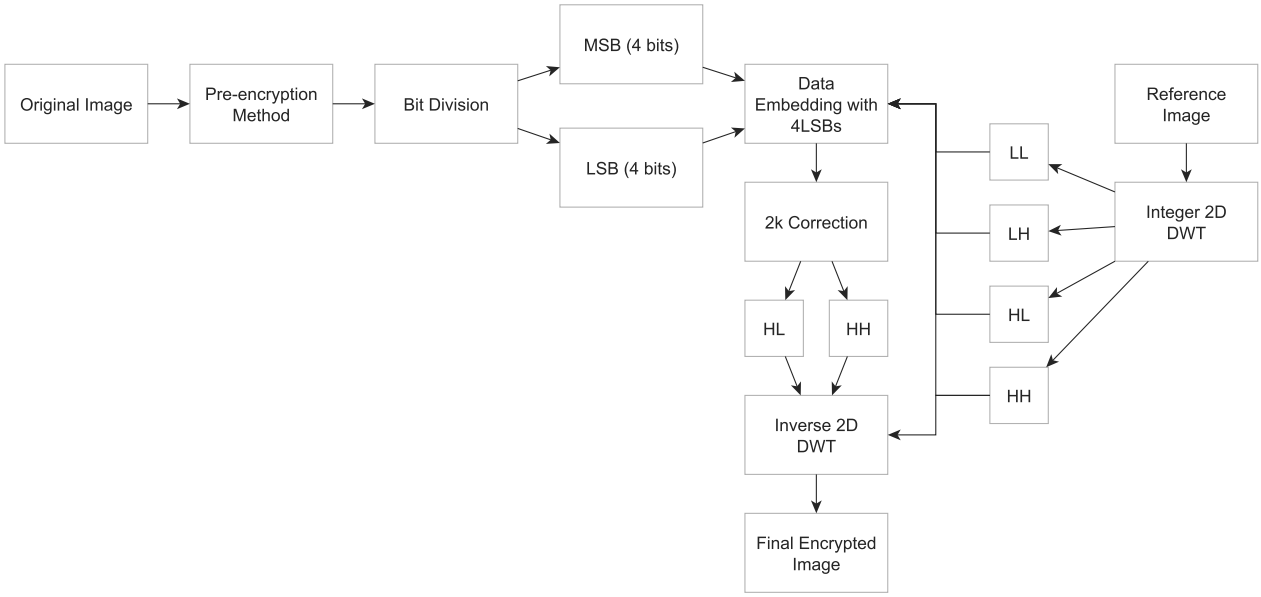


Fig. 3. Block diagram of reference image encryption of Scheme 1.

and obtain the pre-encrypted image.

4.2. Scheme 2. The main objective of this method is to propose a more successful and blind method by modifying reference image encryption of the Yang *et al.* and KG methods and it is also aimed to achieve superior visual quality to the previously presented method using the 2^k correction method. Scheme 2 consists of the integer 2D DWT, pre-encrypted image embedding into reference image using 2LSBs, 3LSBs and 2^2, 2^3 corrections. The graphical representation of Scheme 2 is shown in Fig. 4.

The pseudo code of Scheme 2 is shown as Algorithm 5.

Steps of the decryption of Scheme 1 are as follows:

Step 1: Apply the integer 2D DWT to the final encrypted image using K_2 and obtain LL, LH, HL and HH using (6).

Step 2: Decrypt the final encrypted image using

$$P = 64 \times (\text{LH}(\text{mod } 4)) + 8 \times (\text{LH}(\text{mod } 8)) + \text{HH}(\text{mod } 8). \quad (15)$$

5. Experimental results and a discussion

Visual quality and execution time are used to test the performance of the methods. To obtain the results, randomly generated data are used as the pre-encrypted image and these are embedded into the test reference images because most pre-encryption methods transform the original image into a noise-like form. The reference image data set used is given in Fig. 5.

Algorithm 4. Reference image encryption of Scheme 1.

Input: Pre-encrypted image P with size of $W \times H$, reference image R with size of $2W \times 2H$ and reference image encryption key K_2.

Output: The final cipher image E with size of $2W \times 2H$.

1: Apply the integer 2D DWT to R and obtain LL, LH, HL and HH sub-bands using K_2.
2: for $i = 1$ to W **do**
3: **for** $j = 1$ to H **do**
4: $\text{HL}_{i,j} = 16 \times \left[\frac{\text{HL}_{i,j}}{16}\right] + \left[\frac{P_{i,j}}{16}\right]$
5: $\text{HH}_{i,j} = 16 \times \left[\frac{\text{HH}_{i,j}}{16}\right] + P_{i,j}(\text{mod } 16)$
6: Apply 2^4 correction to $\text{HL}_{i,j}$ and $\text{HH}_{i,j}$
7: **endfor**
8: endfor
9: Apply the inverse integer 2D DWT and obtain the final cipher image E.

In this paper, we proposed two reference image encryption methods. Therefore, we are not interested in the pre-encryption method. 256×256 random generated images are utilized as pre-encrypted images and these are embedded into the reference images, which are shown in Fig. 5. These tests were implemented 100 times.

5.1. Visual quality. In order to evaluate imperceptibility, peak signal-to-noise ratio (PSNR)

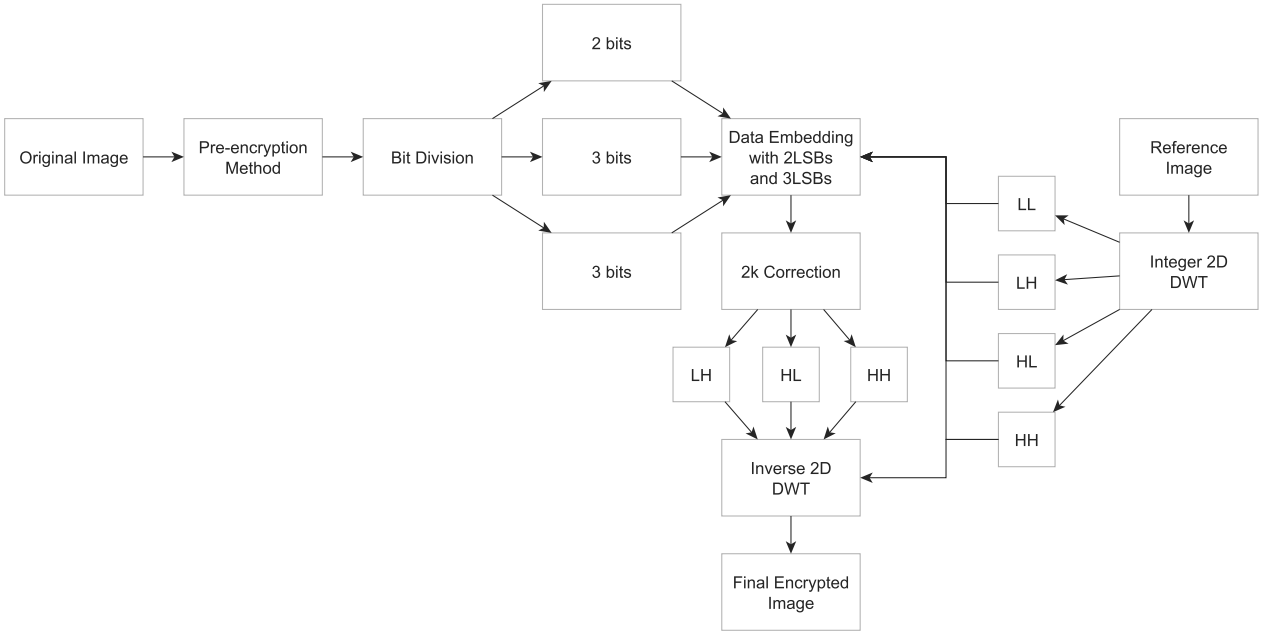


Fig. 4. Block diagram of reference image encryption of Scheme 2.

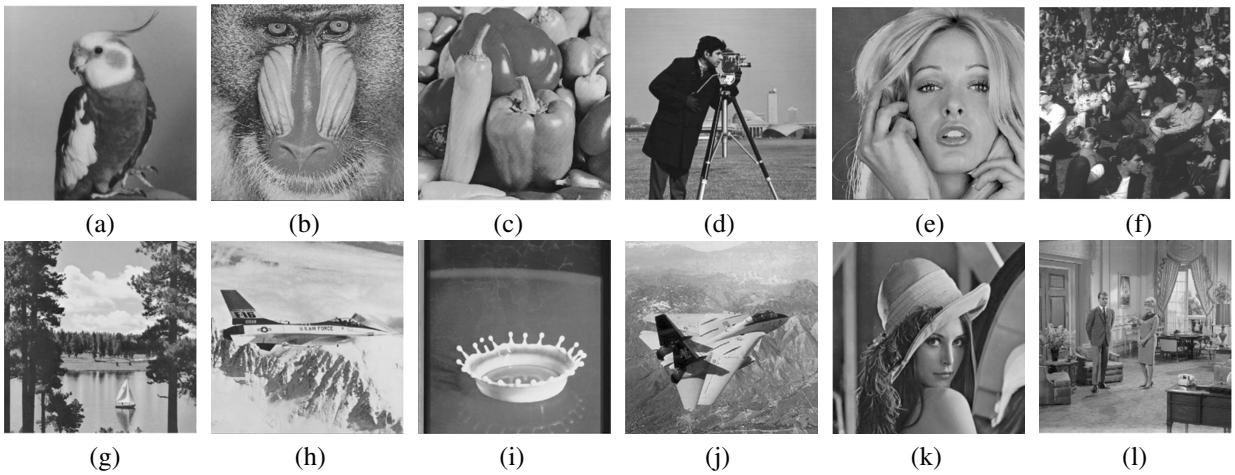


Fig. 5. Gray-level reference images with size 512 × 512: Parrot (a), Baboon (b), Peppers (c), Cameraman (d), Tiffany (e), Crowd (f), Sailboat (g), Airplane (h), Splash (i), F16 (j), Lena (k), Couple (l).

is generally used in the literature (Tanchenko, 2014),

$$\text{PSNR} = 10\log_{10}\frac{255^2 \times 2W \times 2H}{\sum_{i=1}^{2W}\sum_{j=1}^{2H}(R_{i,j} - E_{i,j})^2}. \quad (16)$$

Scheme 1 and the BZ method used HL and HH sub-bands to embed the pre-encrypted image. Therefore, these methods are compared with each other and the PSNR values of these methods are listed in Table 1.

Table 1 shows results of Scheme 1 and the BZ method. As can be seen from these results, the proposed method achieved an approximately 7 dB higher PSNR value. These results clearly proved the success of the 2^k correction.

Table 2 lists the PSNR values of the Yang *et al.*, KG and Scheme 2 methods. Because these methods use LH, HL and HH sub-bands to embed pre-encrypted images into reference images.

As shown in Table 2, the proposed Scheme 2 is compared to 2 state-of-the-art methods. Our approaches achieved approximately a 6 and 4 dB higher PSNR value than the KG (Chen *et al.*, 2004) and the Yang *et al.* method, respectively. These results prove the success of optimal sub-band selection and 2^k correction on reference image encryption.

Table 1. PSNR (dB) results of the BZ method and Scheme 1.

Image	PSNR (dB)	
	BZ method (Ghebleh *et al*., 2014)	Scheme 1
Parrot	30.3145	38.5508
Baboon	28.5814	37.8322
Peppers	29.8935	37.8592
Cameraman	29.2734	35.4617
Tiffany	29.9257	36.9822
Crowd	29.3165	35.4969
Sailboat	29.2943	35.2667
Airplane	29.7337	36.0793
Splash	30.0449	37.6353
F16	29.2516	38.0756
Lena	29.3941	36.0062
Couple	29.6134	36.7030

Table 2. PSNR (dB) results of the Yang *et al.* and KG methods as well as Scheme 2.

Image	PSNR (dB)		
	Yang *et al.* method (Bao and Zhou, 2015)	KG VMIE method (Dhall *et al*., 2018)	Scheme 2
Parrot	38.4841	38.8135	44.0116
Baboon	38.4736	39.9647	43.6071
Peppers	38.4869	39.5991	43.8880
Cameraman	38.4939	39.9455	43.9193
Tiffany	38.4861	39.9822	43.8648
Crowd	38.4593	39.5813	43.7464
Sailboat	38.4586	39.5035	43.7541
Airplane	38.4864	39.2711	43.8721
Splash	38.4968	39.1327	43.9544
F16	38.4707	39.7670	43.7538
Lena	38.4731	39.4227	43.8027
Couple	38.4620	39.6615	43.7549

The PSNR values produced by all the methods are shown in Fig. 6.

The structural similarity (SSIM) is one of the widely used performance evaluation metrics. It is defined as

$$\mathrm{SSIM}(R,E)=\frac{(2\bar{R}\bar{E}+c_1)(2\sigma_{RE}+c_2)}{(\bar{R}^2+\bar{E}^2+c_1)(\sigma_R^2+\sigma_E^2+c_2)} \quad (17)$$

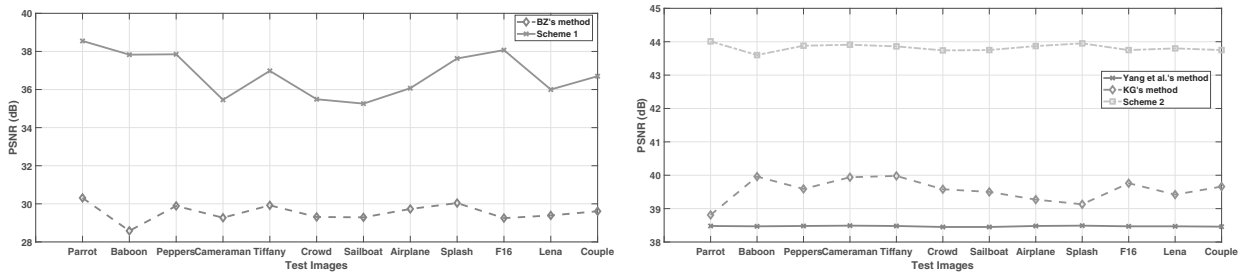
where $\bar{R}$, $\bar{E}$, σ_R, σ_E are the mean value of the reference image, the mean value of the encrypted image, the standard deviation of the reference image and the standard deviation of the original image respectively; c_1 and c_2 are constants. $\mathrm{SSIM}(\cdot,\cdot)$ is the structural similarity function. The SSIM values of Schemes 1 and 2 are listed in Table 3.

As shown in Table 3, the average SSIM value of Schemes 1 and 2 are approximately 0.85 and 0.70, respectively. To calculate these values, the proposed methods were executed 100 times.

Visual quality experiments clearly showed that the best method using two wavelet bands is Scheme 1 and the best method using three wavelet bands is Scheme 2. Scheme 2 is similar to the KG method but Scheme 2 has better visual quality than the KG method. There are two main reasons to achieve better visual quality than the

Table 3. SSIM values of Schemes 1 and 2.

Image	SSIM	
	Scheme 2	Scheme 1
Parrot	0.8755	0.7319
Baboon	0.8621	0.7091
Peppers	0.8519	0.7092
Cameraman	0.8596	0.6789
Tiffany	0.8525	0.6877
Crowd	0.8496	0.6788
Sailboat	0.8563	0.6785
Airplane	0.8567	0.6881
Splash	0.8701	0.7116
F16	0.8554	0.7303
Lena	0.8601	0.6889
Couple	0.8517	0.6902



(a) (b)

Fig. 6. PSNR (dB) chart of the reference image encryption methods: PSNR (dB) results of the BZ method and Scheme 1 (a), PSNR (dB) results of the Yang *et al.* and KG methods as well as Scheme 2 (b).

Algorithm 5. Reference image encryption of Scheme 2.

Input: Pre-encrypted image P with size of $W \times H$, reference image R with size of $2W \times 2H$ and reference image encryption key K_2.

Output: The final cipher image E with size of $2W \times 2H$.

1: Apply the integer 2D DWT and obtain LL, LH, HL and HH sub-bands of R using K_2.

2: for $i = 1$ to W **do**

3: **for** $j = 1$ to H **do**

4: $\mathrm{LH}_{i,j} = \left\lfloor \frac{P_{i,j}}{64} \right\rfloor + \left\lfloor \frac{\mathrm{LH}_{i,j}}{4} \right\rfloor \times 4$

5: $\mathrm{HL}_{i,j} = \left\lfloor \frac{P_{i,j} - 64 \times (P_{i,j} (\mathrm{mod}\ 8))}{8} \right\rfloor + \left\lfloor \frac{\mathrm{HL}_{i,j}}{8} \right\rfloor \times 8$

6: $\mathrm{HH}_{i,j} = P_{i,j} (\mathrm{mod}\ 8) + \left\lfloor \frac{\mathrm{HH}_{i,j}}{8} \right\rfloor \times 8$

7: Apply 2^2 correction on the $\mathrm{LH}_{i,j}$ and 2^3 correction on the $\mathrm{HL}_{i,j}$, $\mathrm{HH}_{i,j}$

8: **endfor**

9: endfor

10: Apply the inverse integer 2D DWT and obtain the final cipher image E.

KG method. These are using the 2^k correction method and selection of optimum sub-bands to pre-encrypted image embedding. Scheme 2 embeds 2, 3 and 3 bits of pre-encrypted data into the LH, HL and HH sub-bands, respectively, whereas the KG method embeds 3, 3 and 2 bits data into the LH, HL and HH sub-bands respectively. Also, Chai *et al*. (2017) proposed a discrete cosine transform based VMIE method and their best PSNR value was calculated as approximately 36 dB. These results clearly demonstrated that the presented 2^k correction based methods are the best reference image encryption methods among these methods in view of the imperceptibility.

5.2. Execution time. One of the important parameters used to evaluate the image encryption methods is execution time. The performance characteristics of the laptop used in simulations are listed in Table 4.

Execution times of reference image encryption with 512×512 size of images are shown in Table 5. Each method was run 30 times for each test images to calculate execution times and the average execution times are shown in Table 5.

The results in Table 5 show that Schemes 1 and 2 have shorter execution times. Also, the computational complexity of the proposed 2^k correction based methods are calculated as $O(n^2)$. The space complexities of these methods have been calculated in Algorithms 6 and 7.

The results clearly demonstrate that the proposed methods have low computational complexities. Therefore, the proposed reference encryption methods are fast and they can be used in the real-world applications to create VMIE.

Table 4. Performance of the laptop.

Systems	Features
Operating system	Windows 10.1
Programming tool	MATLAB 2016a
CPU	Intel Core i5-4300U
CPU frequency	1.90 GHz and 2.50 GHz with Turbo boost
The core/threads	2 core 4 threads
RAM	4 GB
Buffer	3M
HDD	128 GB SSD

Table 5. Execution time comparison of the proposed methods (time unit: millisecond).

Method	Encryption time	Decryption time
Scheme 1	250.613	64.130
Scheme 2	239.185	63.907
Difference	11.428	0.223

Algorithm 6. Space complexity of Scheme 1.

Computational complexity of the encryption method.	
1: Apply the integer 2D DWT to R and obtain LL, LH, HL and HH sub-bands using K_2.	1: $O(WH)$
2: for $i = 1$ to W **do**	2:
3: **for** $j = 1$ to H **do**	3:
4: $\mathrm{HL}_{i,j} = 16 \times \left[\frac{\mathrm{HL}_{i,j}}{16}\right] + \left[\frac{P_{i,j}}{16}\right]$	4: $O(WH)$
5: $\mathrm{HL}_{i,j} = 16 \times \left[\frac{\mathrm{HH}_{i,j}}{16}\right] + P_{i,j} (\mathrm{mod}\ 16)$	5: $O(WH)$
6: Apply 2^4 correction to $\mathrm{HL}_{i,j}$ and $\mathrm{HH}_{i,j}$	6: $O(2WH)$
7: **endfor**	7:
8: endfor	8:
9: Apply the inverse integer 2D DWT and obtain the final cipher image E.	9: $O(WH)$
$T(W,H) = O(6WH)$	
Computational complexity of the decryption method.	
1: Apply the integer 2D DWT to cipher image and obtain LL, LH, HL and HH sub-bands using K_2.	1: $O(WH)$
2: for$i = 1$ to$W$ **do**	2:
3: **for** $j = 1$ to H **do**	3:
4: Use Eqn. (14)	4: $O(WH)$
5: **endfor**	5:
6: endfor	6:
$T(W,H) = O(2WH)$	

5.3. Robustness. Robustness is one of the widely used performance evaluation parameters for data hiding and reference image encryption. To test robustness, data loss, Gaussian and salt and peppers attacks, a cameraman image is used for tests and the results are given in Fig. 7.

The attacks are applied to output images. We tested robustness using the bit error rate

$$\mathrm{BER} = \sum_{i=1}^{W} \sum_{j=1}^{H} \frac{P_{i,j} \bigoplus P'_{i,j}}{W \times H}, \tag{18}$$

where P is the original pre-encrypted image, P' is attacked pre-encrypted image, W is the watermark width of H is the height of the pre-encrypted image. The average BERs of Scheme 1 for salt and pepper, Gaussian and data loss attacks were calculated as 0.25, 0.44 and 0.03, respectively. BER rates of Scheme 2 were calculated as 0.23, 0.39 and 0.01 for salt and pepper, Gaussian and data loss attack, respectively. Scheme 2 uses a more robust wavelet sub-band which is LH. Hence, it is more robust than Scheme 1. These methods have satisfactory robustness because they used kLSBs with 2^k correction. As we know, these methods are fragile. However, our methods provided robustness by using wavelets.

The advantages of the proposed methods are given below:

- In this article, two novel methods are presented. These are called Schemes 1 and 2. These methods have high visual quality. Hence, more powerful encryption methods than other state-of-the-art VMIE approaches are presented.
- One of the problems of the reference image encryption method is blindness. Here, two blind reference image encryption methods are presented and the blindness problem is solved using kLSBs and 2^k correction.
- These methods are cognitive because the sub-bands are not selected randomly. We used HH and HL in Scheme 1. HH, HL and LH are used in Scheme 2. These sub-bands have been used to gain robustness and high visual quality. Hence, successful results were obtained.
- The effects of the 2^k correction are shown in VMIE.
- The proposed methods have low computational complexity.
- Reference image encryption and its performance evaluation criteria are clearly defined.

The disadvantage of the proposed methods is a bit higher computational complexity. These methods use 2^k correction because it increases computational complexities of the methods. However, the 2^k correction solve the problems of low visual quality and blindness of

Algorithm 7. Space complexity of Scheme 2.

Computational complexity of the encryption method.	
1: Apply the integer 2D DWT to R and obtain LL, LH, HL and HH sub-bands of R using K_2.	1: $O(WH)$
2: for $i = 1$ to W **do**	2:
3: **for** $j = 1$ to H **do**	3:
4: $\mathrm{LH}_{i,j} = \left\lfloor \frac{P_{i,j}}{64} \right\rfloor + \left\lfloor \frac{\mathrm{LH}_{i,j}}{4} \right\rfloor \times 4$	4: $O(WH)$
5: $\mathrm{HL}_{i,j} = \left\lfloor \frac{P_{i,j} - 64 \times (P_{i,j} (\mathrm{mod}\ 8))}{8} \right\rfloor + \left\lfloor \frac{\mathrm{HL}_{i,j}}{8} \right\rfloor \times 8$	5: $O(WH)$
6: $\mathrm{HH}_{i,j} = P_{i,j} (\mathrm{mod}\ 8) + \left\lfloor \frac{\mathrm{HH}_{i,j}}{8} \right\rfloor \times 8$	6: $O(WH)$
7: Apply 2^2 correction on the $\mathrm{LH}_{i,j}$ and 2^3 correction on the $\mathrm{HL}_{i,j}$, $\mathrm{HH}_{i,j}$	7: $O(3WH)$
8: **endfor**	8:
9: endfor	9:
10: Apply the inverse integer 2D DWT and obtain the final cipher image E.	10:$O(WH)$
$T(W,H) = O(8WH)$	
Computational complexity of the decryption method.	
1: Apply the integer 2D DWT to cipher and obtain LL, LH, HL and HH sub-bands of R using K_2.	1: $O(WH)$
2: for $i = 1$ to W **do**	2:
3: **for** $j = 1$ to H **do**	3:
4: Use Eqn. (15)	4: $O(WH)$
5: **endfor**	5:
6: endfor	6:
$T(W,H) = O(2WH)$	

the reference image encryption method.

6. Conclusions

The most important feature that distinguishes VMIE methods from other image encryption techniques is that reference image encryption methods are used for data hiding to create VMIE. However, the reference image encryption approaches previously proposed in the literature have two basic problems. These are low visual quality and non-blind reference image encryption problems. Also, the methods in the literature used either HL, HH, LH or HL, HH bands for reference image encryption. In order to solve these problems, two novel 2^k correction based reference image encryption methods are presented in this paper. These methods use the integer 2D DWT and kLSBs data embedding methods to provide blindness and the 2^k correction method to provide high imperceptibility. In order to evaluate performance of the methods, visual quality and execution times are used. Experimental results and comparisons clearly demonstrated that the presented methods have short execution times with superior visual quality to others. Briefly, the 2^k correction effect for reference image encryption is demonstrated using the proposed methods.

Reference image encryption is a new and multidisciplinary research area because it uses image encryption and data hiding together. In this article, two reference image encryption methods are presented to solve problems usually treated by the state-of-the-art methods. The proposed methods can be used by other image encryption (pre-encryption) methods. A novel secure message transmission application can be developed using the proposed methods. These methods can also be used with quantum encryption methods to propose quantum VMIE approaches in future works. The proposed methods can also be utilized as data hiding methods.

References

Avci, E., Tuncer, T. and Avci, D. (2016). A novel reversible data hiding algorithm based on probabilistic XOR secret sharing in wavelet transform domain, *Arabian Journal for Science and Engineering* **41**(8): 3153–3161, DOI: 10.1007/s13369-016-2124-4.

Bao, L. and Zhou, Y. (2015). Image encryption: Generating visually meaningful encrypted images, *Information Sciences* **324**: 197–207.

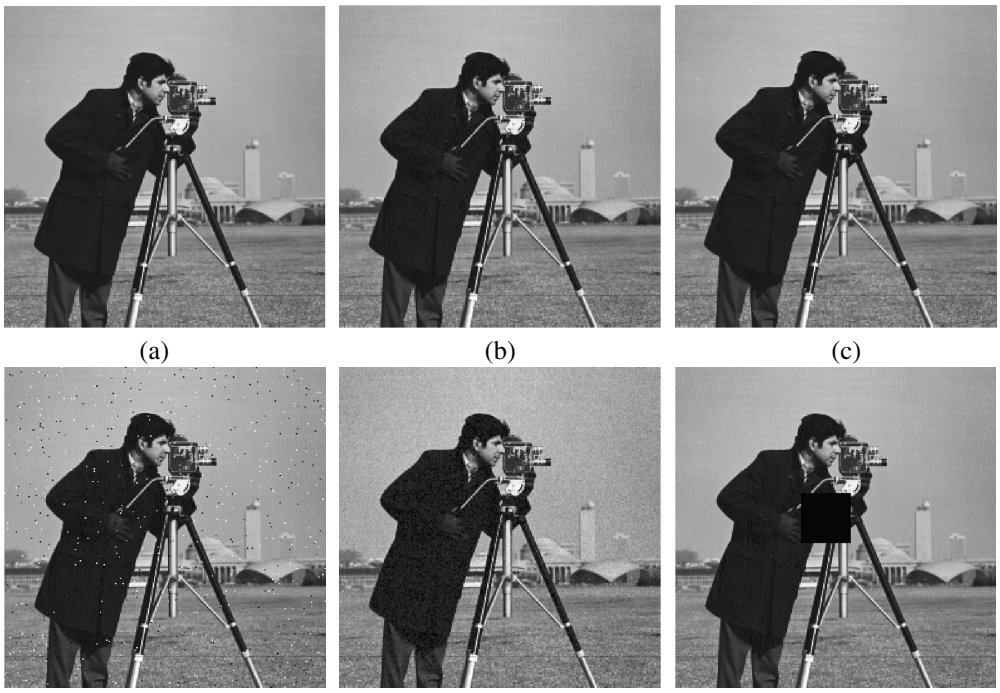


Fig. 7. Output images: the original image (a), the output image of the proposed Scheme 1 (b), the output image of the proposed Scheme 2 (c), salt and pepper noise with 0.01 density (d), Gaussian noise with 0.001 density (e), 80 × 80 sized data loss (f).

Chai, X., Gan, Z., Chen, Y. and Zhang, Y. (2017). A visually secure image encryption scheme based on compressive sensing, *Signal Processing* **134**: 35–51.

Chang, C.-C., Lin, C.-C. and Chen, Y.-H. (2008). Reversible data-embedding scheme using differences between original and predicted pixel values, *IET Information Security* **2**(2): 35–46.

Chen, B., Coatrieux, G., Chen, G., Sun, X., Coatrieux, J.L. and Shu, H. (2014). Full 4-d quaternion discrete Fourier transform based watermarking for color images, *Digital Signal Processing* **28**: 106–119.

Chen, G., Mao, Y. and Chui, C.K. (2004). A symmetric image encryption scheme based on 3d chaotic cat maps, *Chaos, Solitons & Fractals* **21**(3): 749–761.

Dhall, S., Pal, S. K. and Sharma, K. (2018). Cryptanalysis of image encryption scheme based on a new 1d chaotic system, *Signal Processing* **146**: 22–32.

Faragallah, O.S. (2013). Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain, *International Journal of Electronics and Communications* **67**(3): 189–196.

Ghebleh, M., Kanso, A. and Noura, H. (2014). An image encryption scheme based on irregularly decimated chaotic maps, *Signal Processing: Image Communication* **29**(5): 618–627.

Kanso, A. and Ghebleh, M. (2017). An algorithm for encryption of secret images into meaningful images, *Optics and Lasers in Engineering* **90**: 196–208.

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

Liu, F. and Wu, C. (2011). Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners, *IET Information Security* **5**(2): 121–128.

Peng, F., Li, X. and Yang, B. (2012). Adaptive reversible data hiding scheme based on integer transform, *Signal Processing* **92**(1): 54 – 62.

Prasanth Vaidya, S. and Chandra Mouli, P.V.S.S.R. (2017). A robust semi-blind watermarking for color images based on multiple decompositions, *Multimedia Tools and Applications* **76**(24): 25623–25656, DOI: 10.1007/s11042-017-4355-0.

Prasanth Vaidya, S. and Chandra Mouli, P.V.S.S.R. (2018). Adaptive, robust and blind digital watermarking using Bhattacharyya distance and bit manipulation, *Multimedia Tools and Applications* **77**(5): 5609–5635, DOI: 10.1007/s11042-017-4476-5.

Sun, S. (2016). A novel edge based image steganography with 2k correction and Huffman encoding, *Information Processing Letters* **116**(2): 93–99.

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

Tuncer, T. and Avci, E. (2016). A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images, *Displays* **41**: 1–8.

Yang, Y.-G., Zhang, Y.-C., Chen, X.-B., Zhou, Y.-H. and Shi, W.-M. (2018). Eliminating the texture features in visually meaningful cipher images, *Information Sciences* **429**: 102–119.

Turker Tuncer was born in 1986. He received the BS, MS and PhD degrees in 2009, 2011 and 2016, respectively, all from Firat University. He works as a research assistant in digital forensic engineering at Firat University. His research interests include feature engineering, image processing, signal processing, data hiding, image authentication, cryptanalysis, cryptography. He has published more than 60 papers in national and international journals and conferences.

Sengul Dogan was born in 1980. She received the PhD degree at Firat University in 2011. She works as an associate professor of digital forensic engineering at Firat University. Her research interests include feature engineering, image processing, signal processing, data hiding, and cryptography.

Ryszard Tadeusiewicz is a professor at the AGH University of Science and Technology in Krakow. Since 1971 he has performed research in the areas of bio-cybernetics, automatic control engineering, and computer science. In 1975 he was awarded the PhD degree, and in 1981 the DSc degree. In 1986 he became an associate professor and in 1991 a full professor at the AGH University of Science and Technology. He has published over 1200 scientific papers in prestigious Polish and foreign scientific journals, as well as numerous conference presentations. Prof. Tadeusiewicz has also authored over 100 scientific monographs and books, among them several highly popular textbooks, which have been adopted by dozens of Polish universities and have had many editions.

Paweł Pławiak was born in 1984. He obtained his BEng and MSc degrees in electronics and telecommunications, and his PhD degree (with honors) in biocybernetics and biomedical engineering at the AGH University of Science and Technology in 2012 and 2016, respectively. He is the head of the Department of Information and Communications Technology and an assistant professor at the Cracow University of Technology. He has published 21 papers in refereed international journals. He is a reviewer of many prestigious and reputed journals. His research interests include machine learning and computational intelligence, ensemble learning, deep learning, evolutionary computation, classification, pattern recognition, signal processing and analysis, data analysis and data mining, sensor techniques, medicine, biocybernetics, and biomedical engineering.

Received: 19 March 2019
Revised: 25 May 2019
Accepted: 10 July 2019