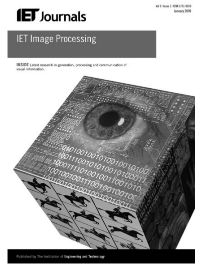
www.ietdl.org

Published in IET Image Processing
Received on 31st March 2014
Revised on 9th September 2014
Accepted on 9th October 2014
doi: 10.1049/iet-ipr.2014.0514



ISSN 1751-9659

Decomposition by binary codes-based speedy image encryption algorithm for multiple applications

Salim Mushin Wadi[1,2], *Nasharuddin Zainal*[1]

[1]Faculty of Engineering and Built Environment, Universiti Kebangsaan, Malaysia UKM, Bangi 43600, Malaysia
[2]Foundation of Technical Education, Najaf Technical College, Najaf 472, Iraq
E-mail: salim2007555@yahoo.com; salimmw@eng.ukm.my

Abstract: The rapid growth in the use of multimedia information has made the security of data storage and transmission important in avoiding unlawful, unofficial, unauthorised and illegal use. Encryption is an efficient operation to protect secret multimedia data secret. A new image encryption approach that uses binary coded decimal (BCD) code-based decomposition, reordering and scrambling bit planes, and an encryption process is suggested in this study. Image decomposition using BCD code for image encryption is introduced in this study. A simple scrambling process is used to shuffle binary bit planes after re-ordering them. A shift column operation is applied to the image that is constructed after scrambling the bit planes to increase the security level. A performance analysis and a comparison with other encryption algorithms are conducted to prove the proposed algorithm's image encryption capabilities. The experimental results show that the suggested method protects secret images against common attacks with shorter encryption/decryption times.

1 Introduction

With the fast development of communication networks and internet services, multifarious and modern technologies allow most people in the world to create, modify, send and receive multimedia files, such as images, audio and video. The protection of multimedia information such as image from different types of attackers has become important for people and governments [1, 2]. Ciphering techniques effectively protect visual information by converting it into an unknown form to the adversary [3].

Imagery is usually represented in the spatial domain or the frequency domain and can perform partial or full encryption [4]. Although, most image ciphering algorithms are in the spatial domain, a digital image could also be encrypted in the frequency domain [5]. Multimedia ciphering algorithms in the frequency domain are based on the fractional Fourier transform (FrFT) [6, 7], fast Fourier transform (FFT) [8], discrete cosine transform (DCT) [9] or Fresnel transform (FrT) [10, 11]. Most algorithms in the frequency domain cipher the coefficients of the previous transform.

In the spatial domain, ciphering algorithms change the information into an inapprehensible form based on changes in the pixel locations (confusion) or pixel values (diffusion) using various technologies [12, 13]. Chaos theory has been widely used in recent years for ciphering, which can generate sequences based on the initial condition and parameters using chaotic maps or systems [2, 5, 13–17]. However, chaos theory-based ciphering algorithms are not very secure [18], also additional computations must be performed to convert the resulting sequences into binary or integer numbers to make these sequences compatible with the ciphering requirements.

Many recently proposed ciphering algorithms are based on image decomposition technology [19–24]. However, previous techniques suffer from drawbacks such as atonality in the security level because the number of bit planes and contents of each bit planes are constant. In addition, there is little or, in some cases, almost no key space in these approaches, which leads to a decrease in the computational cost attacks.

The naive encryption algorithm is a public cryptography algorithm and is widely used in a large number of applications, such as smart cards, cell phones, automated teller machines and www servers [25]. Advanced Encryption Standard (AES) [26] and Data Encryption Standard [27] are examples of naive encryption algorithms. However, the high amount of computations required and artefacts appearance in ciphered image when the original has a large region of a single colour are the important troubles in those techniques [28–30]. A modification version of AES algorithm are proposed in [12] based on decrease the number of rounds to 1 instead of 10 in initial AES. Some ciphering algorithms incorporate both the AES algorithm and the decomposition technology. Podesser *et al.* [3] applied AES on one or more of the most significant bit planes of the original image and then recombined these planes to obtain the ciphered image. Later, Moon *et al.* [4] proposed carry out an Ex-OR operation between the least significant bit (LSB) plane and the whole image and then encrypted the LSB using the AES algorithm. Using AES with decomposition addressed

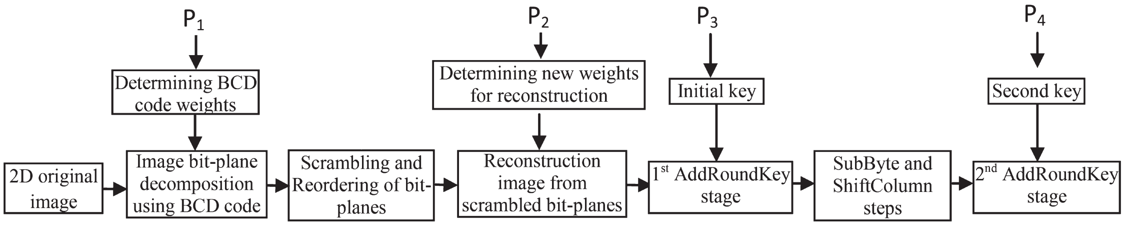


Fig. 1 *Basic block diagram of proposed encryption algorithm*

the problem of key space but increased the computational requirements.

In this paper, new speedy encryption approach is proposed based on decomposition and modified AES algorithm to cipher HD image. Binary codes are used to decompose a secret image as an improvement to binary system-based traditional decomposition operation. After improving its performance three transforms of the AES algorithm transforms are used in proposed method. A simple scrambling operation also used in suggested scheme to increase the security level.

The rest of this paper is organised as follows: Section 2 describes the proposed method. Section 3 presents several simulation examples to show the performance of the new algorithm for image encryption. Conclusions are drawn in Section 4.

2 Proposed method

In one paragraph, the binary codes will be briefly described as input to proposed method.

The traditional binary numbering system is usually used in most bit plane image decomposition-based techniques by applying (1). The number of bit planes and its weights are known. Therefore binary system is not compatible with security conditions

$$D = \sum_{i=0}^{n-1} a_i 2^i = a_0 2^0 + a_1 2^1 + \cdots + a_{n-1} 2^{n-1} \tag{1}$$

where binary code $(a_{n-1}, \ldots, a_0)$ is the binary representation of non-negative decimal number D.

Binary codes are a way to represent each digit in a decimal number with a binary code. An 8421 code is one example of binary code which named binary coded decimal (BCD). These numbers 8421 are represent weights used coding the decimal digit [31]. The location of these weights can be changed to get another code for each digit. For example, the equivalent of the number 137 in 8421 BCD code is (0001 0011 0111), whereas it becomes (0100 0101 1101) in 4182 code. In addition, the weights can be converted to any 4 or more numbers to obtain new codes. So, binary codes used to decompose an image instead of the traditional binary system, which makes it more compatible with ciphering through the increase in both the key space and computation cost for attackers.

After this introduction, we explain the steps of the new HD image encryption algorithm using BCD codes decomposition and a modified AES algorithm named decomposition by binary codes-based encryption algorithm (DBCEA), which can used to cipher grey scale and colour images for different applications and dimensions.

The proposed encryption method shown in Fig. 1 consists of following steps: (i) decomposing the image using binary codes, (ii) reordering the binary bit planes and scrambling its, (iii) reconstruction image from the scrambled bit planes with new weights in binary codes, (iv) add round key, (v) sub byte and (vi) shift column. First, the original image is decomposed to binary bit planes using binary code. The parameter P1 determines the code weights that are required for decomposition operation.

The 8-bit image grey levels are in the range (0–255). Therefore the decomposition operation results in 12 bit planes (4 bits for each digit). As explained in Section 2, each digit in a decimal number can be coded in BCD using more than 4 bits '4 weights', which raises the security level but also increase the computational cost. The bit planes resulting from decomposition are reordered using the following equation

$$\mathrm{BP_r}(i) = \mathrm{BP_{in}}(13 - i) \tag{2}$$

where $\mathrm{BP_r}$ and $\mathrm{BP_{in}}$ are the reordered and the initial bit planes, respectively. $i = 1, 2, 3, \ldots, 12$.

Each reordered bit plane is converted to row vector, which is the initial vector with length equal to dimensions of bit plane. Scrambled vectors are constructing from the initial vectors using the simple scrambling operation below.

Let SV and IV are the scrambled and initial vectors, respectively, $\boldsymbol{n}$ and $\boldsymbol{d}$ are the order of scrambling and initial vectors which equal to (1, 2, …, 12), respectively, r is the order of bit in SV and calculated from (3) below

$$r = 12(i - 1) + d \tag{3}$$

where $i = 1, 2, \ldots, m$, where m is calculated from (4) below

$$m = \frac{\text{no. of bits in one vector}}{\text{no. of vectors}} \tag{4}$$

while c is the order of bit in IV and calculated from (5) below

$$c = m(n - 1) + i \tag{5}$$

Now the value of bit in scrambled vector $\boldsymbol{n}$ with order r is calculated from (6) below

$$\mathrm{SV}n(r) = \mathrm{IV}d(c) \tag{6}$$

here the value of $\boldsymbol{n}$ is calculated from Table 1.

Number of possibilities to rewrite Table 1 is equal to '12!' cases where one case of these cases used between transmitter and authorised receiver, thus the key space will increased. The scrambling method suggested in this paper is shown in Fig. 2.

After scrambling the bit planes, an image is constructed with decimal values. The parameter P2 is used as the new

IET Image Process., pp. 1–11
doi: 10.1049/iet-ipr.2014.0514

Table 1 Determination the order of scrambling vectors according to *m* value

Range of *c*	Value of *n*
1–*m*	1
m–2*m*	2
2*m*–3*m*	3
3*m*–4*m*	4
4*m*–5*m*	5
5*m*–6*m*	6
6*m*–7*m*	7
7*m*–8*m*	8
8*m*–9*m*	9
9*m*–10*m*	10
10*m*–11*m*	11
11*m*–12*m*	12

weights for the reconstruction process, which increases the security level. Image shuffling divides an image into 16 pixels blocks that are arranged in a 4×4 matrix called state. AddRoundKey (ARK), SubByte (SB) and ShiftColumn (SC) transforms are applied to the state. The ARK operation is used in two stages to increase the security level. A distorted image is used as key in the first stage of the ARK operation. The method proposed in [12] is used to prepare the key image (P3) in same dimensions of encrypted image. The first stage of ARK is perform EX-OR operation between image key P3 and scrambled images [26]. The image results from previous EX-OR operation is divided into 4×4 blocks matrix named as 'state'.

The first transform applied on state is the SB transform. It is carry out by using new simple 16×16 hexadecimal matrix introduced in this paper as S-box. Equation (7) below used to produce the proposed S-box

$$x(i, j) = E1\ E2 \tag{7}$$

where $x(i, j)$ is element value in proposed S-box with location determined by (i, j), $E1 = i$, $E2 = F - j$, i and j are the hexadecimal number F is the largest number in hexadecimal system where $F = (15)_{10}$.

The S-box matrix suggested here has several properties such as, generated simplicity and one S-box used in encryption and decryption operation instead of two S-box used in the initial AES algorithm one for encryption and the other for decryption.

After that, the columns of the state are shifted in SC step as follow. Firstly, determining whether the first pixel of the state [0 0] is even or odd? If it is even, the second and third columns are shifted two bits to up and down, respectively. While if the first pixel of the state is odd, the first and fourth columns are shifted down by one and three bytes, respectively. As the final step, the second stage of ARK is executed by performing the EX-OR operation between the state and the 16 byte secret key P4 'initial key'. Finally, in ten iterations, the ARK, SB and SC transforms are applied under the cipher block chaining (CBC) mode. For more details about the ciphering mode, see [32, 33].

3 Experimental results

The DBCEA algorithm has been effectively used for approximately 250 HD remote sensing grey scale and true colour images, medical images and standard images. The proposed method is compared with several encryption algorithms to evaluate the encryption performance. Same security keys (P_1, P_2 and P_4) are used in all simulation results in the rest of the paper. Two secret images are used as initial key P_3 in the first stage of the ARK operation, one with the HD images tests and the other with the medical and standard images. The DBCEA method scrambled the bit planes bit by bit, as shown in Fig. 2. Of course, the user can replace bit by bit with 2 bit by 2 bit, or 3 bit by 3 bit and so on until row by row, where this number is secret.

The proposed method performance is evaluated by measuring the similarity between the original and reconstructed images, security analysis and encryption/decryption time.

3.1 Image similarity

3.1.1 Visual scene: The visual scene of image similarity is a measurement of differences between original and processed images.

3.1.2 Entropy: The concept of entropy comes from information theory and ergodic theory. Shannon entropy is defined as a metric associated with information content of the input signal. In image processing, the entropy is defined as the measure to randomness which can be interpreted as the average uncertainty of the information source [14, 15]. Entropy is calculated by (8) below [16]

$$H(x) = \sum_{i=1}^{K} P(x_i) \log_2 \frac{1}{P(x_i)} = - \sum_{i=1}^{K} P(x_i) \log_2 P(x_i) \tag{8}$$

where the $P(x_i)$ is the probability of symbol x_i. The entropy can used to measure the similarity through comparing between plain and deciphered images entropy. The similarity is large if the entropy difference is low.

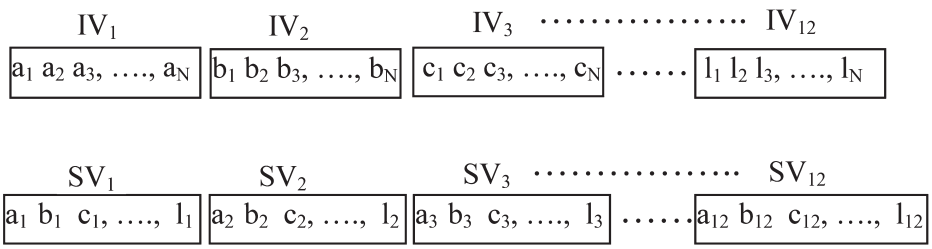


Fig. 2 *Scrambling method*

Let the image have dimensions of 12×1 pixels
IV is the initial bit planes
SV is the scrambled bit plane

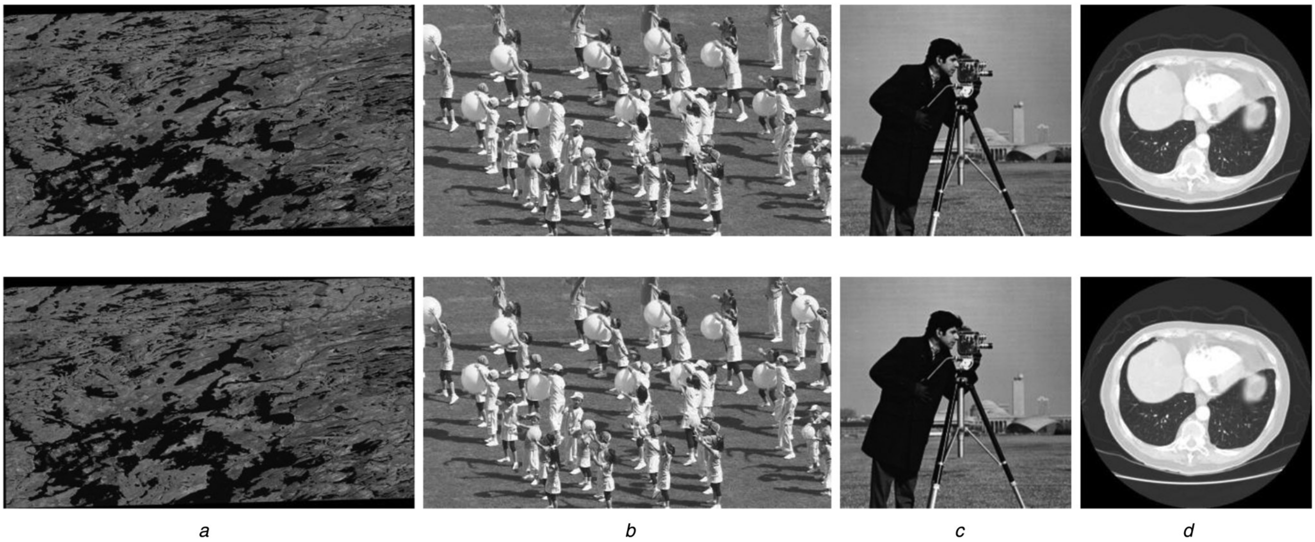


Fig. 3 *Visual scene of four tests of reconstructed images ciphered by EBCEA, where the original image is in the first row and the reconstructed image is in the second row*

a HD remote sensing image (1080 × 1920)
b HD image of kids (1080 × 1920)
c MRI image (512 × 512)
d Standard image cameraman (512 × 512)

3.1.3 Peak signal-to-noise ratio (PSNR): PSNR is a pixel-based evaluation of image quality after change pixels values of this image [16]. PSNR is calculated using (10) depend on mean-square error (MSE) as in the following equation

$$\mathrm{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij} - y_{ij})^2 \tag{9}$$

where M and N denote the images dimensions, $x_{i,j}$ and $y_{i,j}$ stand for the value of pixel $[i, j]$ in the original and the processed images, respectively

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right) \tag{10}$$

3.1.4 Structural similarity (SSIM): SSIM index is another index used to measure the similarity between two images [33]. SSIM is designed to improve on traditional methods (PSNR). SSIM considers image distortion as seeing changes in structural information. Structural information is the idea that the pixels have strong inter-dependencies especially when they are spatially close. These dependencies carry important information about the structure of the objects in the visual scene. The SSIM metric is calculated on various windows of an image as in (11) below

$$\mathrm{SSIM} = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{11}$$

where μ_x and μ_y are the average of x and y, respectively, σ_x^2 and σ_y^2 are the variance of x and y, respectively, $\sigma_{x,y}$ is the covariance of x and y which are calculated in (2.10–2.12) below, $C_1 = (k_1L)^2$, $C_2 = (k_2L)^2$ are two variables to stabilise the division with weak denominator, L is the dynamic range of the pixel-values (typically it is equal to $2^{\text{Number of bits per pixels}} - 1$), $k_1 = 0.01$ and $k_2 = 0.03$ by default

$$\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{12}$$

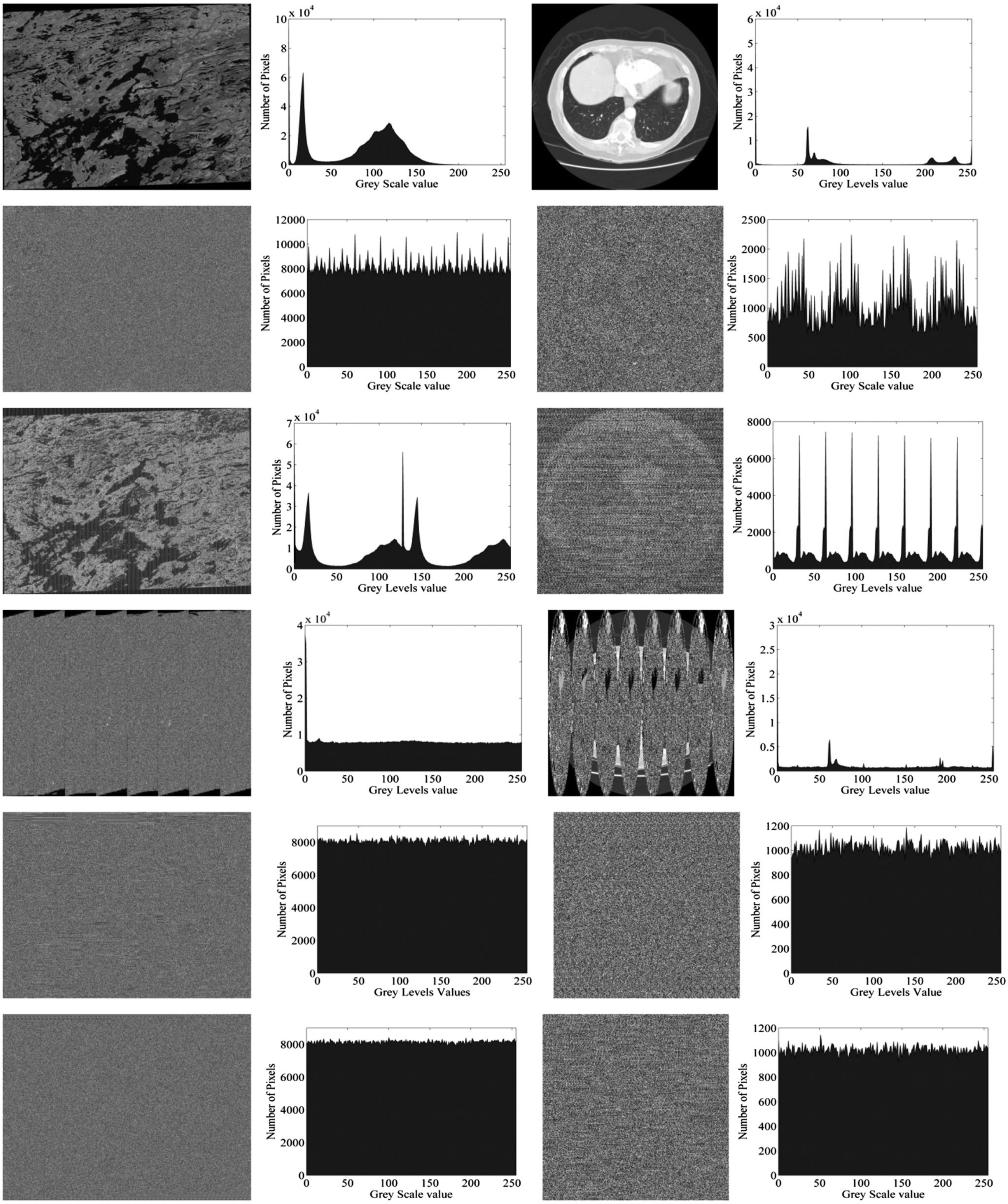
$$\sigma_x = \left(\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)^2\right)^{1/2} \tag{13}$$

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y) \tag{14}$$

Table 2 Statistical measures for deciphered image by DBCDEA method

Test name	Size	Image type	Entropy	PSNR, dB	SSIM
remote sensing (HD)	1080 × 1920	original image	4.8321	inf.	1
		reconstructed image	4.8321		
kids (HD)	1080 × 1920	original image	7.3132	inf.	1
		reconstructed image	7.3132		
medical image	512 × 512	original image	5.9179	inf.	1
		reconstructed image	5.9179		
standard image	512 × 512	original image	6.4320	inf.	1
		reconstructed image	6.4320		

doi: 10.1049/iet-ipr.2014.0514



a *b* *c* *d*

Fig. 4 *Two tests original and ciphered images for proposed and related works with histogram distribution*

First row original images, second, third, fourth, fifth and sixth rows represent ciphered image by BPEXOR [1], SBEAES [3], SBELBP [4], MAES [12] and proposed method, respectively
a Original and ciphered image of first test HD remote sensing image (1080 × 1920)
b Histogram distribution of first test image
c Original and ciphered image of second test medical image (512 × 512)
d Histogram distribution of second test image

The value of SSIM index is in range '−1 to 1', if SSIM = 1 that mean the two images are identical.

Fig. 3 clearly shows that the deciphered images are completely reconstructed for all tests. In addition, the values

doi: 10.1049/iet-ipr.2014.0514

of the statistical measures, including PSNR, entropy and SSIM are clearly shown the similarity between reconstructed and original images as shown in Table 2.

3.2 Security analysis

The first issue for each security algorithm is its security levels which is determined by the protection level of the encrypted objects. In this subsection, several security parameters are used to evaluate the performance of the proposed method, such as the visual scene, histogram, correlation coefficients, key space, key sensitivity and attacks. Two samples from each type are used in our discussion and compared in the following subsections. The evaluation results of proposed method are compared with four other ciphering algorithms [1, 3, 4, 12] to verify the effectiveness of the proposed method.

3.2.1 Visual scene: The encrypted image scene should be similar to the jamming scene on TV. Therefore if the encryption algorithm did not satisfy the visual scene requirements then other security analysis parameters do not need to be checked. Fig. 4 shows the scene of the original and encrypted image for two tests: HD remote sensing with dimensions (1080×1920) and medical image with dimensions (512×512). The original images with histogram distribution shown in the first row of the figure, while, encrypted images by the BPEXOR [1], SBEAES [3], SBELBP [4], MAES [12] and the proposed method shown in second, third, fourth, fifth and sixth rows, respectively. All tested encryption algorithms are produced ciphered images with artefacts except the proposed method, which satisfy the visual scene requirements.

3.2.2 Histogram analysis: An image histogram represents the distribution of intensity levels for the image pixels. The encrypted image histogram should be uniformly distributed to prevent statistical attacks [13, 34].

Figs. 4*b* and *d* show the histograms of the original and encrypted images of two test images. As obviously shown in Figs. 4*b* and *d*, the histogram of the ciphered images by the encryption algorithms BPEXOR, SBEAES and SBELBP (second, third and fourth rows of Figs. 4*b* and *d* contain information of the original image, which confirms the results of the visual scene. However, the histogram distribution of the encrypted image by the MAES and proposed method is very uniformly distributed for all image types as shown in fifth and sixth rows of Figs. 4*b* and *d* which means that these two methods is stronger against statistical attacks compared with the other methods.

3.2.3 Correlation coefficients: In all types of images, each pixel is usually highly correlated with its adjusted pixels. The perfect cipher system is a system that produces ciphered image with very low correlation between the adjacent pixels [34]. One of the basic factors for measuring the dissimilarity between the plain and ciphered image is a correlation coefficients factor. The correlation coefficients are calculated using (15)–(18) below [13]

$$E(X) = \frac{1}{N}\sum_{i-1}^{N} x_i \tag{15}$$

$$D(x) = \frac{1}{N}\sum_{i-1}^{N} (x_i - E(x))^2 \tag{16}$$

$$\mathrm{cov}(x, y) = E[(x - E(x))(y - E(y))] \tag{17}$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{18}$$

where x and y are the values of grey levels in the image and N is the total number of samples.

First, 5000 pair of adjacent pixels are randomly selected from the original and encrypted by proposed method images of HD remote sensing image, in the horizontal, vertical and diagonal directions. Fig. 5 shows the plot of the correlation coefficients of the adjacent pixels for the remote sensing images (original and encrypted images), Figs. 5*a–c* show horizontal, vertical and diagonal correlation coefficients of the original image in the first row and ciphered image in the second row, respectively. The figure clearly shows a strong correlation between adjacent pixels in the original images for pixels situated in a certain region (such as a diagonal line). The adjacent pixels of the ciphered images are uniformly distributed, which means that the correlation between the pixels is very low.

To confirm results of Fig. 5, the correlation coefficients were quantitatively calculated, as shown in Table 3.

3.2.4 Entropy: The entropy is used as an indicator to security level. Generally, the grey levels number of grey-scale images are 2^8 or 256 and if the probability of grey levels is equal, then by applies (8) the entropy must equal to 8 which it is an ideal value. Therefore the best ciphered algorithm is that produce encrypted image with entropy near 8. That means the pixels are uniformly distributed on grey levels and this decrease the effect of statistical attacks. The entropy for the four tests is shown in Table 4. The results in Table 4 prove that the entropy values for the proposed method are nearer to 8 than are the results of the other encryption algorithms for all tests. Considering the other proof, these results support that the proposed method is strong against statistical attacks.

3.2.5 Chosen plaintext attacks: The goal of plaintext attack is to recover the plaintext from ciphertext in a systematic way, or sometimes to deduce the decryption key. There are two types of plaintext attack, known and chosen plaintext attack. The known plaintext attackers try to get the secret key through studying the known parts of plaintext and their corresponding ciphertext. While chosen plaintext attackers more complicated because they did not know the plaintext, so, they choose any useful information as the plaintext in order to deduce the security keys of encryption algorithms, or reconstruct the original plaintexts from the unknown ciphertexts [23]. The proposed method is strong against this attack because the length of key and data block is long.

3.2.6 Noise attacks: Data transmitted through communication channels usually suffer from various types of noise. One of the most important challenges facing encryption algorithms is the noise attack. To evaluate the performance of the proposed method against noise attacks, it is compared with other ciphering algorithms. One original image (Test 4, cameraman image) is tested in this case. This image is encrypted by ciphering algorithms (BPE-XOR, SBE-AES, SBE-LBP, MAES and the proposed method), and salt and pepper noise is added to the ciphered image with a density of 0.05. Subsequently, these noised ciphered images are deciphered to obtain the original image. The similarities between the original and decrypted

IET Image Process., pp. 1–11
doi: 10.1049/iet-ipr.2014.0514

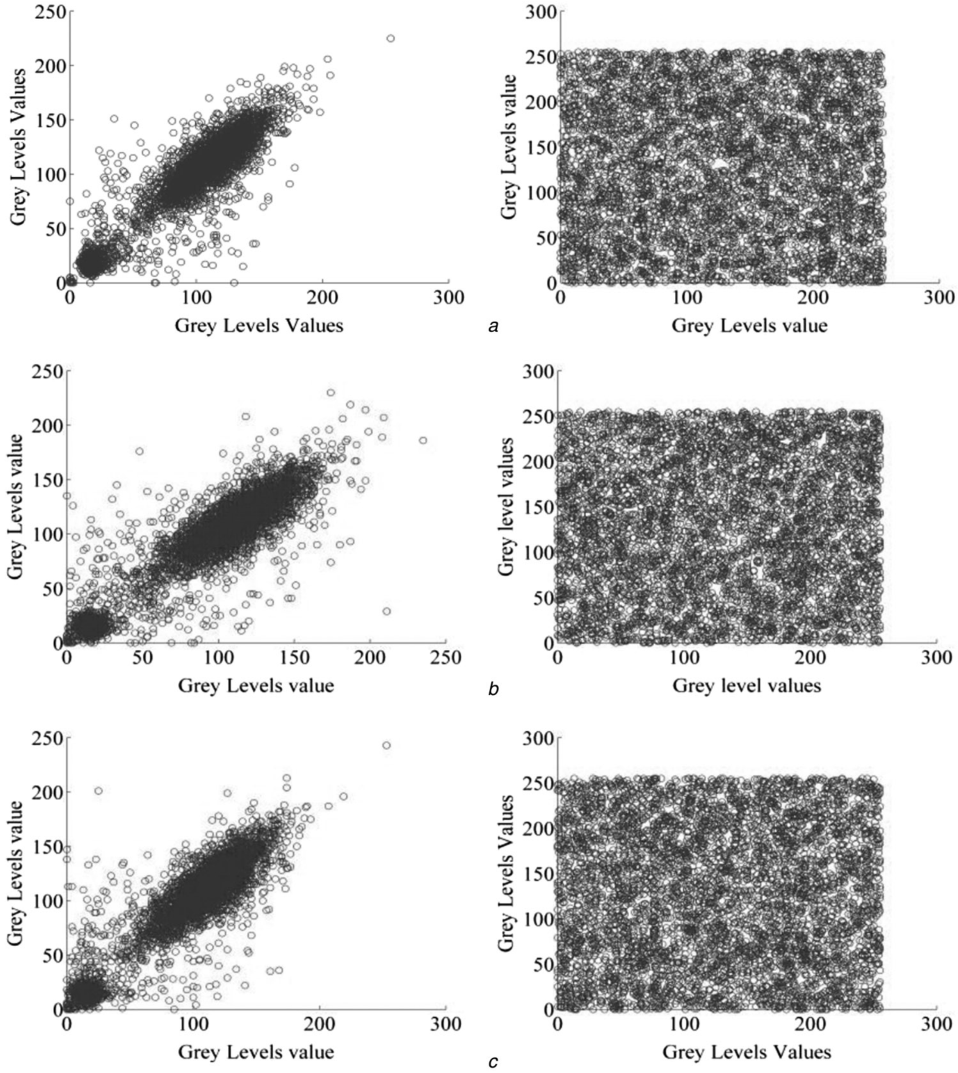


Fig. 5 *Correlation coefficients of remote sensing HD images (original and ciphered image by proposed method)*

Original image in 1st row and ciphered images in the second row
a Horizontal CC
b Vertical CC
c Diagonal CC

Table 3 Correlation coefficients of the original image and the images encrypted using the proposed method

Image	Original image			Ciphered image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
remote sensing (HD) image	0.9814	0.9821	0.9830	−0.0015	−0.0024	−0.0031
kids (HD) image	0.9646	0.9649	0.9665	0.0081	0.0072	0.0078
medical image	0.9952	0.9956	0.9958	0.0053	0.0021	0.0031
cameraman image	0.9732	0.9451	0.9631	0.0099	0.0083	0.0081

Table 4 Entropy values of original images and their encrypted images by different encryption algorithms

Image	Original	BPEEXOR	SBEAES	SBELBP	MAES	Proposed method
remote sensing (HD) image	4.8321	7.9051	5.5286	6.7901	7.9865	7.9999
kids (HD) image	7.3132	7.9987	7.7631	7.9993	7.9999	7.9999
medical image	5.9179	7.9424	6.4706	7.6014	7.9321	7.9999
cameraman image	6.4320	7.9893	7.2472	7.9987	7.9941	7.9999

images are evaluated using the SSIM index value. As clearly demonstrated in Fig. 6 (first and second columns), we note that the SBE-AES and SBE-LBP algorithms fail to reconstruct the original image. The proposed, MAES and

doi: 10.1049/iet-ipr.2014.0514

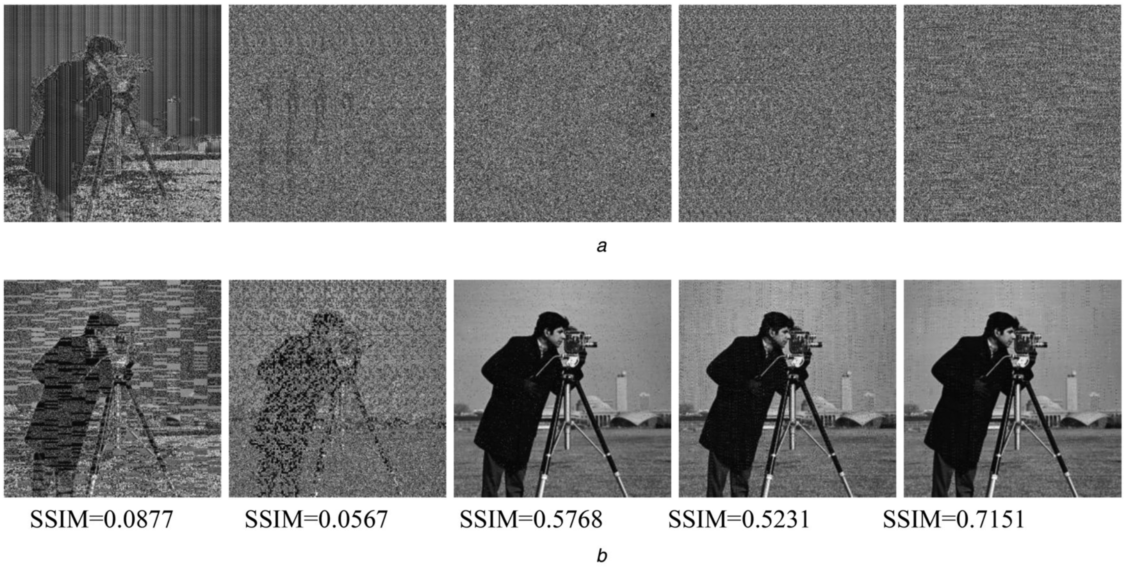


Fig. 6 *Noise attacks test results for cameraman image, where first, second, third, fourth and fifth column represent the SBEAES, SBELBP, BPEXOR, MAES and the proposed method, respectively*

a Noised encrypted
b Decrypted images, respectively

BPE-XOR algorithms reconstruct the original image but with several artefacts as shown in Fig. 6 (third, fourth and fifth columns). The SSIM value proves that the performance of the proposed method is better against noise attacks compared to the BPE-XOR and MAES algorithms.

3.2.7 Key space: The security key of the proposed method consists of four stages (P_1, P_2, P_3, P_4 and possibilities of Table 1), as shown in Fig. 1. P_3 is a block key that consists of 128 bits. Therefore, the number of all likelihoods is 2^{128}. P_4 is the key image, which has a size equal to the original image size. Generally, the security key indicates the number of possible probabilities for the whole key in the algorithm. Therefore the security key space of the proposed method is shown in the following equation

$$KS = 2^{128} * 2^{M*N} + 12! = 2^{128+(M*N)} + 12! \qquad (19)$$

where M and N are original image dimensions. Equation (19) shows that the security key space of suggested algorithm is large enough to face a brute force attack, which tries to estimate the security key by searching for all possible of keys in the ciphering algorithm [34].

3.2.8 Key sensitivity: The key sensitivity test is conducted to measure the encryption algorithm's sensitivity to key changes. The reconstructed image should be completely different from the original image with small changes in the security key. The Test 4 image (cameraman) is used to test the security of the suggested key. The SSIM index is used to measure the similarity between the reconstructed and original images. As illustrated in Section 4.2.7, the suggested algorithm has four keys: P_1, P_2, P_3 and P_4. P_4 is an image used as a key and therefore cannot be tested because it is very long. P_1 and P_2 have the same effect on the encryption algorithm; therefore we only test P_1. Fig. 7 shows the results of the security key tests when P_1 and P_3 are changed. Two bits were changed only from P_1 and P_3, and the encrypted image was then reconstructed. The scene of the reconstructed image as shown in Figs. 7*c* and *d* is unlike of original image scene, which indicates that the proposed method is very sensitive with to changes in the security key.

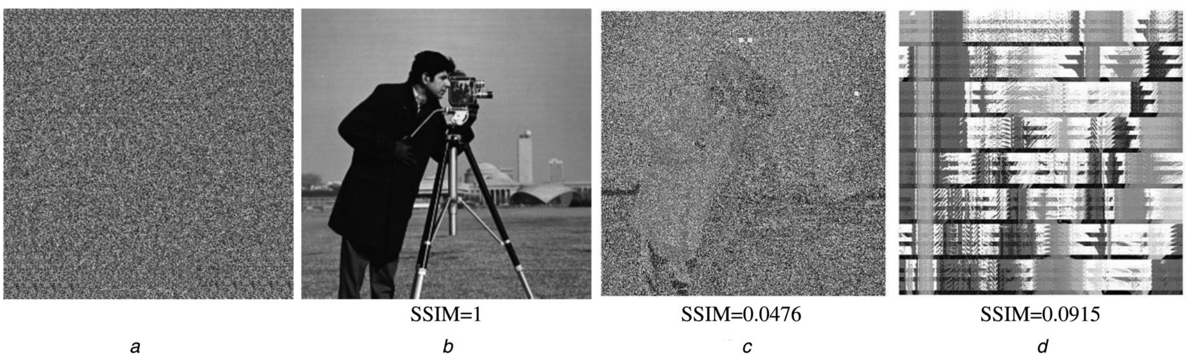


Fig. 7 *Results of key sensitivity for proposed method*

a Encrypted image
b Reconstructed image with the correct key
c Reconstructed image when 2 bits of P_1 are changed
d Reconstructed image when 2 bits of P_3 are changed

doi: 10.1049/iet-ipr.2014.0514

Table 5 Encryption/decryption time of the proposed and the other three methods (time measured in second)

Method	Test 1, 1080 × 1920 pixel, 2025 kB		Test 2, 512 × 512 pixel, 256 kB	
	Enc. time, s	Dec. time, s	Enc. time, s	Dec. time, s
proposed method	82.49	85.72	7.24	8.73
BPE-XOR	81.54	83.86	7.32	6.67
SBE-AES	153.01	274.00	22.87	38.80
SBE-LBP	159.12	282.97	23.31	38.92
MAES	137.10	150.43	17.52	20.65

3.3 Encryption and decryption times

In addition to the security level of an encryption algorithm, the encryption/decryption time is an important factor and is very influential on the performance of a ciphering algorithm, especially with HD image encryption. The simulation was executed using an *HP* laptop with the following specifications: system model: HP Pavilion *g*4 Notebook PC; processor: Intel (R) Core™ i5-2430 M CPU@ 2.40 GHz (4CPUs) – 2.4 GHz; memory: 8192 MB RAM; BIOS: InsydeH2O version 03.61.01F.62. A comparison among SBE-AES, SBE-LBP, BPE-XOR and the proposed methods is introduced in terms of encryption and decryption time. Two images with different sizes are used in this experiment [256 kB (512 × 512 pixels) and 2025 kB (1080 × 1920) pixel)]. Table 5 clearly shows that the times of LBP-XOR and the proposed method are very short when compared with the other methods. Therefore, the proposed method is more compatible with image encryption, especially for HD images.

3.4 RGB image encryption

In this subsection, a true colour image (RGB image) is used to confirm the high performance of the proposed algorithm with all image types. HD RGB remote sensing image (1080 × 1920) is tested in this section. The ciphered and

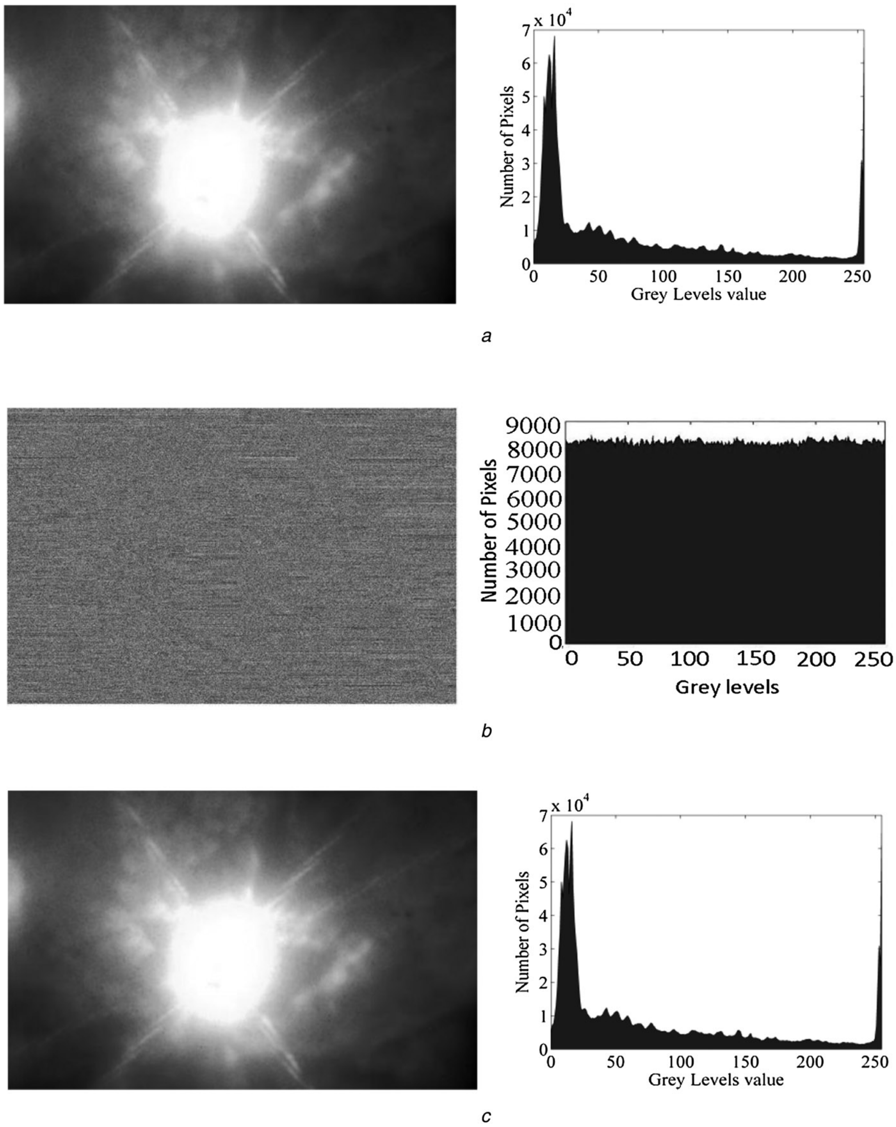


Fig. 8 *Remote sensing (HD) RGB test image (1080 × 1920)*

a Original image with histogram
b Ciphered image with histogram
c Reconstructed image with histogram

reconstructed images are shown for performance evaluation. The visual scene, entropy and histogram analysis are important evaluation factors for the encrypted image. The results of the entropy and the histogram are the average results for the three components of image (red, green and blue). The results of the HD remote sensing test are shown in Fig. 8. First, the scene of the ciphered image is similar to the jumping on TV, which is the best appearance for the encrypted image as in Fig. 8*b*. The ciphered image entropy is very near the ideal entropy for the ciphered image, which equals 8. As is obvious from the results shown in Fig. 8, the proposed algorithm satisfies high performance with RGB image encryption.

4 Conclusions

The aim of this paper is to introduce a fast and high security image ciphering algorithm for different applications images in multiple dimensions. Firstly, secret image was decomposed to bit planes based on binary codes using weights (P_1) then reordering and scrambling resulted bit planes. After that, the scrambled bit planes will be reconstructed using new weights (P_2), then SubByte, ShiftColumn and AddRoundKey transforms carry out on the reconstructed image. The AddRoundkey transformation is executed Ex-OR operation between scrambled image and keys P_3 and P_4 in two stages.

The most important challenges facing encryption algorithms are security levels and encryption/decryption time. The security levels is improved in proposed method through increasing the key space in four stages 'P_1, P_2, P_3 and P_4', change the value of pixels using scrambling, AddRoundKey and SB operations, and change pixels locations by applying reordering and SC operations. The binary codes used in image encryption for first time in proposed paper to decompose the secret image and reconstruct it using different keys 'P_1 and P_2' after scrambling operation. A new scrambling operation was introduced in suggested algorithm and applied on bit planes to change the value of pixels and increasing the key space by 12!. SC transform executed adaptively based on the order of first pixel of state matrix. The proposed algorithm is executed in record time compared with the other encryption algorithm.

Finally, the performance of the proposed algorithm is evaluated by comparing the original and reconstructed images, security analysis and encryption/decryption times. Security analysis proved that the suggested approach is strong against various types of attacks, including statistic, plaintext, data loss and noise attacks. The results of the evaluations, especially the encryption time, show that the DBCEA algorithm is very compatible with images encryption especially HD images in different applications such as medical and remote sensing images.

5 References

1 Han, W., Kim, H., Park, S., *et al.*: 'Optical image encryption based on XOR operations', *Opt. Eng.*, 1999, **38**, (1), pp. 47–54

2 Akhshani, A., Behnia, S., Akhava, A., *et al.*: 'A novel scheme for image encryption based on 2D piecewise chaotic maps', *Opt. Commun.*, 2010, **283**, (17), pp. 3259–3266

3 Podesser, M., Schmidt, H., Uhl, A.: 'Selective bitplane encryption for secure transmission of image data in mobile environments'. The Fifth Nordic Signal Processing Symp., Hurtiguten, Norway, 2002, pp. 1037–1042

4 Moon, D., Chung, Y., Pan, S., *et al.*: 'An efficient selective encryption of fingerprint images for embedded processors', *ETRI J.*, 2006, **28**, (4), pp. 444–452

5 Borujeni, E., Eshghi, M.: 'Chaotic image encryption system using phase-magnitude transformation and pixel substitution', *Telecommun. Syst.*, 2013, **52**, (2), pp. 525–537

6 Zhou, N., Wang, Y., Gong, L.: 'Novel optical image encryption scheme based on fractional Mellin transform', *Opt. Commun.*, 2011, **284**, (13), pp. 3234–3242

7 Ge, F., Chen, L., Zhao, D.: 'A half-blind color image hiding and encryption method in fractional Fourier domains', *Opt. Commun.*, 2008, **281**, (17), pp. 4254–4260

8 Borujeni, E.: 'Speech encryption based on fast Fourier transform permutation'. The Seventh IEEE Int. Conf. on Electronics Circuits and Systems, Jounieh, Lebanon, April 2000, pp. 290–293

9 Liu, Z., Xu, L., Liu, T., *et al.*: 'Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains', *Opt. Commun.*, 2011, **284**, (1), pp. 123–128 **Q2**

10 Chang, H., Hwang, H., Lee, C.: 'Position multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain', *Opt. Commun.*, 2011, **284**, (18), pp. 4146–4151

11 Hwang, H.: 'An optical image cryptosystem based on Hartley transform in the Fresnel transform domain', *Opt. Commun.*, 2011, **284**, (13), pp. 3243–3247

12 Wadi, S., Zainal, N.: 'Rapid encryption method based on AES Algorithm for gray scale HD image encryption', *Proc. Technol.*, 2013, **8C**, (6), pp. 52–57

13 Fu, C., Lin, B., Miao, Y., *et al.*: 'A novel chaos-based bit-level permutation scheme for digital image encryption', *Opt. Commun.*, 2011, **284**, (23), pp. 5415–5423

14 Liu, H., Wang, X.: 'Color image encryption using spatial bit-level permutation and high-dimension chaotic system', *Opt. Commun.*, 2011, **284**, (16–17), pp. 3895–3903

15 Akhavan, A., Samsudin, A., Akhshani, A.: 'A symmetric image encryption scheme based on combination of nonlinear chaotic maps', *J. Franklin Inst.*, 2011, **348**, (8), pp. 1797–1813

16 Ye, R.: 'A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism', *Opt. Commun.*, 2011, **284**, (22), pp. 5290–5298

17 Zhu, Z., Zhang, W., Wong, K., *et al.*: 'A chaos-based symmetric image encryption scheme using a bit-level permutation', *Inf. Sci.*, 2011, **181**, (6), pp. 1171–1186

18 Alexander, P., Massimiliano, Z.: 'Chaotic map cryptography and security. Encryption: methods, software and security, horizons in computer science research' (Nova Science Publishers, 2012), pp. 301–332

19 Jiancheng, Z., Ward, R., Dongxu, Q.: 'A new digital image scrambling method based on Fibonacci numbers'. Int. Symp. on Circuits and Systems, Vancouver, Canada, May 2004, pp. 965–972

20 Jiancheng, Z., Ward, R., Dongxu, Q.: 'The generalized Fibonacci transformations and application to image scrambling'. IEEE Int. Conf. on Acoustics, Speech, and Signal Processing, Montreal, Canada, May 2004, pp. 385–392

21 Chen, L., Zhao, D., Ge, F.: 'Image encryption based on singular value decomposition and Arnold transform in fractional domain', *Opt. Commun.*, 2013, **291**, pp. 98–103

22 Qiudong, S., Yan, W., Huang, J., Ma, W.: 'Image encryption based on bit-plane decomposition and random scrambling'. Second Int. Conf. on Consumer Electronics Communications and Networks, Hubei, China, April 2012, pp. 2630–2633

23 Yicong, Z., Panetta, K., Agaian, S.: 'Image encryption algorithms based on Generalized P-Gray Code bit plane decomposition'. Conf. Record of the 43rd Asilomar Conf. on Signals Systems and Computers, California, USA, November 2009, pp. 400–404

24 Zheng, W., Cheng, Z., Yue, C.: 'Image data encryption and hiding based on wavelet packet transform and bit planes decomposition'. Fourth Int. Conf. on Wireless Communications Networking and Mobile Computing, Dalian, China, September 2008, pp. 1–4

25 Nandi, S., Kar, B., Chaudhuri, P.: 'Theory and applications of cellular automata in cryptography', *IEEE Trans. Comput.*, 1994, **43**, (12), pp. 1346–1357

26 Daemen, J., Rijmen, V.: 'The block cipher Rijndael, Smart card research and applications' (Springer, Berlin Heidelberg, 2000), pp. 277–284

27 FIPS PUB 46–3: 'Data encryption standard (DES)', 1999

28 Kamali, S., Shakerian, R., Hedayati, M., *et al.*: 'A new modified version of advanced encryption standard based algorithm for image encryption'. Int. Conf. on Electronics and Information Engineering, Kyoto, Japan, August 2010, pp. 1–5

doi: 10.1049/iet-ipr.2014.0514

29 Grangetto, M., Magli, E., Olmo, G.: 'Multimedia selective encryption by means of randomized arithmetic coding', *IEEE Trans. Multimed.*, 2006, **8**, (5), pp. 905–917
30 Wadi, S., Zainal, N.: 'A low cost implementation of modified advanced encryption standard algorithm using 8085A microprocessor', *J. Eng. Sci. Tech.*, 2013, **8**, (4), pp. 406–415
31 Floyd, T.: 'Digital fundamentals' (Prentice-Hall, 2003, 1st edn.)
32 Huang, C., Yen, C., Chen, C.: 'The AES application in image using different operation modes'. The Fifth IEEE Conf. on in Industrial Electronics and Applications, Taichung, Taiwan, June 2010, pp. 393–398
33 Zhou, W., Bovik, A., Sheikh, R.: 'Image quality assessment: from error visibility to structural similarity', *IEEE Trans. Image Process.*, 2004, **13**, (4), pp. 600–612
34 Schneier, B.: 'Applied cryptography' (John Wiley & Sons, 1994, 1996, 2nd edn.)
35 Huang, C., Nien, H.: 'Multi chaotic systems based pixel shuffle for image encryption', *Opt. Commun.*, 2009, **282**, (11), pp. 2123–2127 **Q3**
36 Hermassi, H., Rhouma, R., Belghith, S.: 'Improvement of an image encryption algorithm based on hyper-chaos', *Telecommun. Syst.*, 2013, **52**, (2), pp. 539–549

IPR20140514

Author Queries

Salim Mushin Wadi, Nasharuddin Zainal

Q1 Please check the e-mail id of the corresponding author.
Q2 Please check author names for Ref. [9].
Q3 Please cite Refs. [35, 36] in appropriate place in the text.