Signal Processing 102 (2014) 122–131

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Fast communication

A symmetric image cipher using wave perturbations

Yue Wu [a,1], Yicong Zhou [b,*], Sos Agaian [c], Joseph P. Noonan [a]

[a] Department of Electrical and Computer Engineering, Tufts University, Medford, MA 02155, USA
[b] Department of Computer and Information Science, University of Macau, Macau 999078, China
[c] Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, USA

ARTICLE INFO

Article history:
Received 2 November 2013
Received in revised form
5 March 2014
Accepted 11 March 2014
Available online 20 March 2014

Keywords:
Symmetric image cipher
Image shuffling
Wave perturbation
Data protection

ABSTRACT

Inspired by the natural ripple-like phenomenon that distorts a reflection on a water surface, this paper introduces a new symmetric image cipher using wave perturbations to shuffle images in an n dimensional (n D) space. Its strong diffusion and confusion properties are ensured by pseudo-random wavefronts and additional salts and peppers bits. Extensive simulations and comparisons demonstrate that the proposed image cipher outperforms several existing bit-level scrambling methods with respect to the encryption quality and computation complexity.

1. Introduction

As a typical digital data format, images are used almost everywhere in the world. Due to the fact that many digital images are sensitive, private or even classified, the importance of protecting image contents is self-explanatory. According to application purposes, these protection techniques can be roughly classified into two groups: (1) digital watermarking techniques for copyright protection [1–6] in which watermarks are either visible, invisible, or both; (2) image ciphers (IC) for content protection including image scrambling (IS) or encryption (IE) techniques in which image contents are unrecognizable and unintelligible after processing [7–13]. IS and IE techniques are of a close relationship, where IS often focuses on scrambling image pixels to make an image content visually unrecognizable, while IE applies additional transforms to make image statistically indistinguishable from random noise.

Because IS aims to scramble image pixels visually random-like, it is often used in real-time scenarios asking for limited protection, *e.g.* protection for a short time frame. From the viewpoint of cryptography, IS is essentially a permutation cipher [14]. According to a working domain, an IS method can be of frequency-domain or spatial-domain. A frequency-domain IS commonly scrambles frequency components of a transformed image, and produces noticeably visual quality losses. A spatial-domain IS scrambles spatial components within an image and breaks the relationship between image pixels. Depending on the processing unit, the spatial-domain IS techniques can be divided into three subgroups: the block-level IS, byte-level IS, and bit-level IS [15–19]. Depending on the percentage of data to be scrambled, an IS method can also be partial or full IS. Many frequency-domain IS methods are partial IS, while most bit-level IS methods are full IS. Although the classic IS solution introduced by Durstendfeld [20] provides an efficient way of permuting a sequence in a (pseudo) random manner, its arbitrary permutation has to be done sequentially. To speed-up the IS process, many algorithms allowing parallel computing were proposed in recent years. By circularly shifting 8×8 bit blocks of an image in parallel, Chen et al. suggested a fast bit-level IS [21]. Treating a row/column of pixels as one unit, Ye proposed a faster IS solution [22].

* Corresponding author. Tel.: +853 83978458; fax: +853 28838314.
E-mail addresses: ywu03@ece.tufts.edu (Y. Wu), yicongzhou@umac.mo (Y. Zhou).
[1] Tel.: +1 6176276412; fax: +1 6176273220.

http://dx.doi.org/10.1016/j.sigpro.2014.03.015
0165-1684/

To further improve the randomness level of Ye's method, Fu et al. [18] applied the automorphism of the Cat map [23] to image permutation in a form of matrix multiplication. However, these methods [21,22,18] have either poor randomness degrees or a much high time complexity.

In contrast, IE aims to make an image statistically random-like and thus it contains more cryptographic primitives beyond permutation, *e.g.* substitution, whitening, etc. [14]. Depending on the source of pseudo-random numbers, IE methods can be classified into (1) chaotic IE and (2) non-chaotic IE. Chaotic IE [24–26] often uses a chaotic system to generate pseudo-random numbers where an encryption key often encodes the system parameters and initial conditions. Non-chaotic IE [27–30] uses conventional pseudo-random number generators (PRNG) where an encryption key commonly encodes a PRNG seed and parameters to translate a parametric transform. Though it might be inevitable to avoid computations for enhancing an IC security, it is possible to reduce the cost of generating a very large number of quality pseudo-random numbers by reusing a relative small number of pseudo-random numbers via appropriate transforms and translations.

In this paper, we design a new symmetric image cipher using wave perturbations in an n D space. In particular, we use parallel wavefronts to scramble image bits. Because these wavefronts are parallel, only zero-wavefronts are required to be generated whereas other wavefronts can be simply translated from zero-wavefronts. In this way, we only need to generate a small number of pseudo-random numbers, but are able to scramble an entire image efficiently. More importantly, the use of parallel wavefronts does not tradeoff the scrambling randomness. Additionally, confusion and diffusion properties of a good cipher can be achieved by introducing pseudo-noise and imposing chaining in neighboring bits.

The rest of paper is organized as follows: Section 2 proposes our new image cipher to shuffle images using wave perturbations; Section 3 discusses two primitives to improve the cipher confusion and diffusion properties [31]; Section 4 evaluates the image randomness and security issues of the proposed image cipher with comparisons to peer methods; and we conclude the paper in Section 5.

2. Symmetric image cipher using wave perturbations

2.1. Method overview

As shown in Fig. 1, ripples (because of wave perturbations) distort the original sky and clouds on the water surface and make it less recognizable. This natural process can be considered as that a plane wave passes through an image O with size of $M \times N$ along the y-axis direction (see Fig. 2(a)). All image pixels are pushed/pulled away from their original positions because of wave perturbations. A resulting new position of a pixel is then dependent on the wavefront passing through it.

2.2. Wave perturbations for image shuffling

Assume an image is a uniform media, all wavefronts are parallel in the space and thus can be fully characterized by one zero-wavefront. Say this wave propagates along the y-axis, and its zero-wavefront, namely the waveform at $y=0$ is denoted as $\mathbf{w}_x^{y=0} = \{w_{x=i}^{y=0}\}_{i \in \mathbb{R}}$. The row grid of the digital image 'samples' the continuous wavefront $w_x^{y=0}$ into N discrete points. Each point is a sample of the wavefront $w_x^{y=0}$ rounding to its nearest integer.

Fig. 1. The ripple effect: image scrambling in nature.

We denote the resulting discrete wavefront as $\mathbf{W}_x^{y=0} = \{W_{x=i}^{y=0}\}_{i \in \mathbb{Z}}$, which is a vector defined in Eq. (1). According to the parallel property among wavefronts, the jth wavefront $\mathbf{W}_x^{y=j}$ at the y-axis direction can be translated from the zero-wavefront as shown in Eq. (2), where 'mod' denotes the module operation to guarantee the onto property of data mapping. Fig. 2(b) shows the discrete wavefronts of $\mathbf{W}_x^{y=1}$ to $\mathbf{W}_x^{y=3}$ generated from $\mathbf{W}_x^{y=0}$:

$$\mathbf{W}_x^{y=0} = [W_{x=0}^{y=0}, W_{x=1}^{y=0}, \ldots, W_{x=N-1}^{y=0}]^T \tag{1}$$

$$\mathbf{W}_x^{y=j} = (j + \mathbf{W}_x^{y=0}) \bmod N \tag{2}$$

Integrating all wavefronts along the y-axis, we define a 2-dimensional (2D) wave perturbation IC (2D-WPIC) mapping the original image O into its scrambled version S defined in Eq. (3), and the corresponding inverse mapping in Eq. (4):

$$S(i,j) = \mathcal{F}_{2D}^{y,x}(O(i,j), W_{x=i}^{y=j}) = O(i, (j + W_{x=i}^{y=0}) \bmod N) \tag{3}$$

$$O(i,j) = \mathcal{F}_{2D}^{y,x\,-1}(S(i,j), W_{x=i}^{y=j}) = S(i, (j - W_{x=i}^{y=0}) \bmod N) \tag{4}$$

Similarly, we can characterize a plane wave propagating along the x-axis direction using a zero-wavefront $\mathbf{W}_y^{x=0}$. A 2D-WPIC mapping the image O into the scrambled image S is defined in Eq. (5), and the corresponding inverse mapping in Eq. (6):

$$S(i,j) = \mathcal{F}_{2D}^{x,y}(O(i,j), W_{y=j}^{x=i}) = O((i + W_{y=j}^{x=0}) \bmod M, j) \tag{5}$$

$$O(i,j) = \mathcal{F}_{2D}^{x,y\,-1}(S(i,j), W_{y=j}^{x=i}) = S((i - W_{y=j}^{x=0}) \bmod M, j) \tag{6}$$

Fig. 3 shows the 2D-WPIC results using wave perturbations. It is clear that the scrambled images have been distorted in a ripple-like way, and that image contents after scrambling are less recognizable. The proposed 2D-WPIC becomes the IS

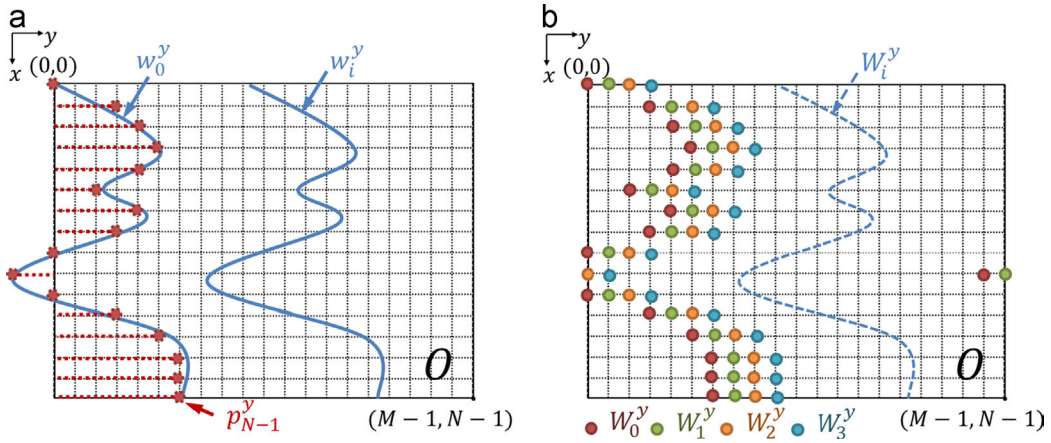

Fig. 2. Discretization of wave perturbations for digital images. (a) Continuous wavefronts (blue curves) and discrete zero-wavefront (stems), and (b) discrete wavefronts. (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this paper.)

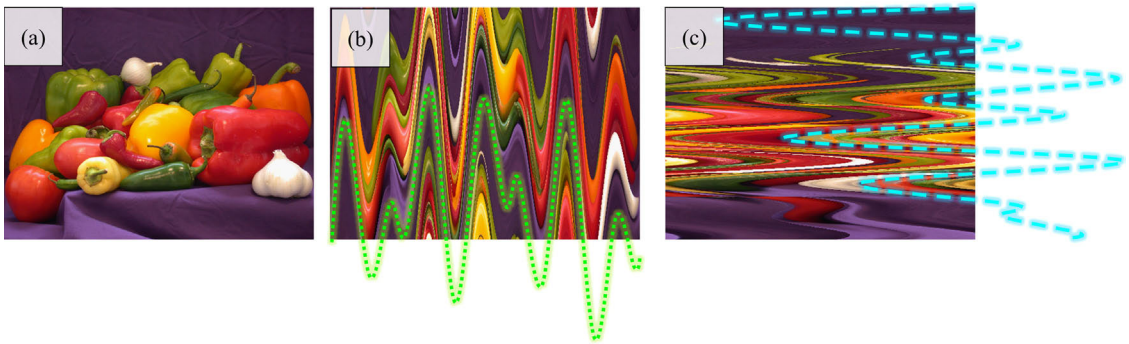

Fig. 3. Image scrambling using wave perturbations. (a) Original *peppers* image. The IS results using a wave propagating along the (b) *x*-axis and (c) *y*-axis directions.

method in [21] if it is applied to each 8×8 bit block within an image.

2.3. Wave perturbations in the n D space

Instead of being considered as a 2D signal, a digital image can also be viewed as a 3-dimensional (3D) signal, where the third dimension is the bit-depth of the image. Alternatively, a digital image can also be folded and packed as a high dimensional (HD) signal, *e.g.* the method in [23]. The idea of the proposed 2D-WPIC can be further extended to the n D wave perturbation IC (n D-WPIC) for scrambling these HD image representations.

Without loss of generality, consider an n D original image O defined on the integer lattice $[0, d_0-1] \times [0, d_1-1], \ldots, [0, d_{n-1}-1]$, where d_k is the length of the kth dimension. Each position then can be uniquely coded as a vector:

$$\mathbf{x} = [x_0, x_1, \ldots, x_{n-1}] \tag{7}$$

where x_k is the coordinate on the kth dimension.

Because any two dimensions out of n can be used to construct a 2D-WPIC, we realize n D-WPIC by using 2D-WPIC for different dimension pairs. One dimension in 2D-WPIC is considered as the direction which the 2D wave propagates towards. The other is viewed as the direction where the 2D wave has perturbations. In this manner, the proposed 2D-WPIC in Eqs. (3) and (5) can be successfully extended into the n D-WPIC in Eq. (8), once the two distinctive reference directions θ_k and θ_h are given ($h \neq k$):

$$S(\mathbf{x}) = \mathcal{F}_{nD}^{\theta_{kh}}(O(\mathbf{x}), W_{\theta_h = x_h}^{\theta_k = x_k}) = O(\ldots, x_h, \ldots, (x_k + W_{\theta_h = x_h}^{\theta_k = 0}) \bmod d_k, \ldots) \tag{8}$$

$$O(\mathbf{x}) = \mathcal{F}_{nD}^{\theta_{kh}^{-1}}(S(\mathbf{x}), W_{\theta_h = x_h}^{\theta_k = x_k}) = S(\ldots, x_h, \ldots, (x_k - W_{\theta_h = x_h}^{\theta_k = 0}) \bmod d_k, \ldots) \tag{9}$$

Correspondingly, one can find the inverse IS mapping as given in Eq. (9). This new n D-WPIC has the following diffusion property.

Property 1. *Let* $\mathbf{o}_1 = [\ldots, x_{h-1}, y_h, x_{h+1}, \ldots, x_k, \ldots]$ *and* $\mathbf{o}_2 = [\ldots, x_{h-1}, z_h, x_{h+1}, \ldots, x_k, \ldots]$ *be the nD position vectors of two pixels in the image O, which only differ at the hth coordinate, i.e.* $y_h \neq z_h$, *and* $\mathbf{s}_1$ *and* $\mathbf{s}_2$ *be the position vectors after the nD-WPIC using Eq. (8), the Euclidean distance of these two pixels increases after scrambling, namely* $\rho(\mathbf{s}_1, \mathbf{s}_2) \geq \rho(\mathbf{o}_1, \mathbf{o}_2)$.

Proof. Obviously, $\rho(\mathbf{o}_1, \mathbf{o}_2) = |y_h - z_h|$. After applying the n D-WPIC, we have

$$\mathbf{s}_1 = [\ldots, x_{h-1}, y_h, x_{h+1}, \ldots, (x_k + W_{\theta_h = y_h}^{\theta_k = 0}) \bmod d_k, \ldots]$$

$$\mathbf{s}_2 = [\ldots, x_{h-1}, z_h, x_{h+1}, \ldots, (x_k + W_{\theta_h = z_h}^{\theta_k = 0}) \bmod d_k, \ldots].$$

Let δ_k be the increased distance along θ_k as follows. Thus,

$$\delta_k = |(W^{\theta_k}_{\theta_h = y_h} - W^{\theta_k}_{\theta_h = z_h}) \bmod d_k| \tag{10}$$

Then
$\rho(\mathbf{s}_1, \mathbf{s}_2) = \sqrt{(y_h - z_h)^2 + \delta_k^2} \geq \sqrt{(y_h - z_h)^2} = \rho(\mathbf{o}_1, \mathbf{o}_2)$. □

This property shows that the n D-WPIC has a diffusion nature. Particularly, when $W^{\theta_k=0}_{\theta_h=y_h}, W^{\theta_k=0}_{\theta_h=z_h} \sim \mathbb{U}(0, d_k - 1)$ come from a discrete uniform distribution independently, it is demonstrable that the increased distance δ_k in Eq. (10) along θ_k has the following discrete triangular distribution:

$$\Pr(\delta_k = t) = \begin{cases} 2(d_k - t)/d_k^2 & \text{for } 0 < t \leq d_k - 1 \\ 1/d_k & \text{for } t = 0 \end{cases} \tag{11}$$

The mean and standard deviation of δ_k can be computed correspondingly as follows:

$$\mu_{\delta_k} = (d_k^2 - 1)/(3d_k) \tag{12}$$

$$\sigma^2_{\delta_k} = (d_k^2 - 1)(d_k^2 + 2)/(18d_k^2) \tag{13}$$

In summary, this diffusion property of n D-WPIC reveals that (1) d_k controls the probability of the increased distance δ_k, the greater the d_k is, the more likely the δ_k increases; and (2) d_h controls the number of samples pulled from the uniform distribution $\mathbb{U}(0, d_k - 1)$, the greater the d_h is, the more likely for δ_k to follow the triangular distribution in Eq. (11). These results imply to couple a given θ_k with the dimension θ_h with the largest d_h, *i.e.* $d_h = \max\{d_l | l \in [0, n-1] \& l \neq k\}$, because the triangular distribution in Eq. (11) will be better approximated than that using a dimension with a small d_h. Finally, one should apply the n D-WPIC with respect to different pairs of θ_k and θ_h so that image pixels can be diffused everywhere within an n D space.

3. Improvements

In previous sections, we discussed how to use wave perturbations to do image scrambling in an n D space. However, it is well known that the permutation-only cipher is insecure to chosen ciphertext attacks [32–34]. We therefore propose the following security enhancements adhering to Shannon's confusion and diffusion properties [31] to improve security.

3.1. Improving method's confusion properties

Shannon confusion properties require extremely complicated relationship between a key and its corresponding ciphertext. To achieve this goal while keeping the IS process simple, we improve the n D-WPIC by mixing the pseudo-random noises as shown in Eq. (14), where ¬ denotes the negation operation flips bit 0s to 1s and vice versa, and $\mathcal{P}(\cdot)$ is the parity function outputting 0s for even input, and 1s otherwise. In other words, according to the parity of $p^{\theta_k}_{x_h}$, we flip the parity of a bit correspondingly. As a result, it is clear that the new shuffling process should be modified as shown in Eq. (15):

$$S(\mathbf{x}) = \overline{\mathcal{F}}^{\theta_{k,h}}_{nD}(O(\mathbf{x}), W^{\theta_k = x_k}_{\theta_h = x_h}) = \begin{cases} \mathcal{F}^{\theta_{k,h}}_{nD}(O(\mathbf{x}), W^{\theta_k = x_k}_{\theta_h = x_h}) & \text{if } \mathcal{P}(W^{\theta_k = 0}_{\theta_h = x_h}) = 1 \\ \neg\mathcal{F}^{\theta_{k,h}}_{nD}(O(\mathbf{x}), W^{\theta_k = x_k}_{\theta_h = x_h}) & \text{if } \mathcal{P}(W^{\theta_k = 0}_{\theta_h = x_h}) = 0 \end{cases} \tag{14}$$

$$O(\mathbf{x}) = \overline{\mathcal{F}}^{\theta^{-1}_{k,h}}_{nD}(S(\mathbf{x}), W^{\theta_k = x_k}_{\theta_h = x_h}) = \begin{cases} \mathcal{F}^{\theta^{-1}_{k,h}}_{nD}(S(\mathbf{x}), W^{\theta_k = x_k}_{\theta_h = x_h}) & \text{if } \mathcal{P}(W^{\theta_k = 0}_{\theta_h = x_h}) = 1 \\ \neg\mathcal{F}^{\theta^{-1}_{k,h}}_{nD}(S(\mathbf{x}), W^{\theta_k = x_k}_{\theta_h = x_h}) & \text{if } \mathcal{P}(W^{\theta_k = 0}_{\theta_h = x_h}) = 0 \end{cases} \tag{15}$$

In this manner, n D-WPIC achieves the confusion properties, which indicates that the 0/1s in the resulting data is equally like and thus satisfies the confusion properties, namely the Property 2 listed below.

Property 2. *Let q^0_m and q^1_m be, respectively, the percentages of 0-bits and 1-bits in a scrambled image S after m times of nD-WPIC using Eq. (14). Then $q^0_m = q^1_m = 0.5$ as $m \to \infty$, when the zero-wavefront is uniformly distributed.*

Proof. Because the zero-wavefront is uniformly distributed, the probability $\Pr(\mathcal{P}(p^{\theta_k}_{x_h}) = 1)$ is around 0.5.[3] Then, the probability of negating a bit in the mth IS can be written as $g_m = 0.5 + \epsilon_m$, where ϵ_m is a small quantity in $[-0.5, 0.5]$ (ϵ_m actually follows a zero-mean binomial distribution). Therefore, the percentage q^0_m completely depends on g_m and the percentages of 0-bits and 1-bits after $(m-1)$ times of IS, namely

$$q^0_m = q^0_{m-1}(1 - g_m) + q^1_{m-1} g_m = 0.5 - \epsilon_m(q^1_{m-1} - q^0_{m-1}) \tag{16}$$

$$q^1_m = q^0_{m-1} g_m + q^1_{m-1}(1 - g_m) = 0.5 + \epsilon_m(q^1_{m-1} - q^0_{m-1}) \tag{17}$$

Let $\Delta_m = q^1_m - q^0_m$, then $\Delta_m = 2\epsilon_m \Delta_{m-1} = \Delta_0 \prod_{t=1}^{m} 2\epsilon_t$. It is clear that unless $|\epsilon_t| = 0.5 \forall t \in [1, m]$, we always have this limit to be zero, namely

$$\lim_{m\to\infty} \Delta_m = \Delta_0 \lim_{m\to\infty} (q^1_m - q^0_m) = \lim_{m\to\infty} \prod_{t=1}^{m} 2\epsilon_t = 0.$$

Because the negation is applied randomly, $\Pr(|\epsilon_t| < 0.5) = 1$ is almost surely. Thus, $q^1_m - q^0_m = 0$ as $m \to \infty$ is held, implying that $\lim_{m\to\infty} q^0_m = \lim_{m\to\infty} q^1_m = 0.5$ □

3.2. Improving method's diffusion properties

Besides equally likely distributed pixels, a secure image cipher shall also attain good diffusion properties that any slight change in the input data should lead to significant differences in the output data. Otherwise, an adversary is always able to crack a key successfully by continuously using this defect.

To achieve this goal with a low computational cost again, we then adopt the chaining method to update

[3] The uniformly distributed wavefront is easy to achieve by using quantity pseudo-number generators, but we cannot assume that one of its realizations is exactly uniformly distributed due to its random nature.

a pixel as shown in the following equations:

$$S(\mathbf{x}) = \overline{\overline{\mathcal{F}}}_{nD}^{\theta_{k,h}}(O(\mathbf{x}), W_{\theta_h = x_h}^{\theta_k = x_k}) = \begin{cases} \mathcal{F}_{nD}^{\theta_{k,h}}(O(\mathbf{x}), W_{\theta_h = x_h}^{\theta_k = x_k}) & \text{if } \mathcal{P}(W_{\theta_h = x_h}^{\theta_k = 0}) = \mathcal{P}(c_k) \\ \neg\mathcal{F}_{nD}^{\theta_{k,h}}(O(\mathbf{x}), W_{\theta_h = x_h}^{\theta_k = x_k}) & \text{if } \mathcal{P}(W_{\theta_h = x_h}^{\theta_k = 0}) \neq \mathcal{P}(c_k) \end{cases} \tag{18}$$

$$O(\mathbf{x}) = \overline{\overline{\mathcal{F}}}_{nD}^{\theta_{k,h}^{-1}}(S(\mathbf{x}), W_{\theta_h = x_h}^{\theta_k = x_k}) = \begin{cases} \mathcal{F}_{nD}^{\theta_{k,h}^{-1}}(S(\mathbf{x}), W_{\theta_h = x_h}^{\theta_k = x_k}) & \text{if } \mathcal{P}(W_{\theta_h = x_h}^{\theta_k = 0}) = \mathcal{P}(c_k) \\ \neg\mathcal{F}_{nD}^{\theta_{k,h}^{-1}}(S(\mathbf{x}), W_{\theta_h = x_h}^{\theta_k = x_k}) & \text{if } \mathcal{P}(W_{\theta_h = x_h}^{\theta_k = 0}) \neq \mathcal{P}(c_k) \end{cases} \tag{19}$$

where we have the chaining quantity c_k defined as

$$c_k = \begin{cases} 0 & \text{if } x_k = 0 \\ S(x_0, \ldots, x_{k-1}, x_k - 1, x_{k+1}, \ldots, x_{n-1}) & \text{otherwise} \end{cases} \tag{20}$$

and in this way we now diffuse a previous bit at location $x_k - 1$ to its next location x_k. It is therefore noticeable that any change in the original input image first leads to different bits in all following bits along one dimension, then these different bits further lead to more different results when the n D-WPIC is applied to another direction, and eventually lead to a significantly different result after shuffling along many different directions. It is also worthy to note that the though condition that we change a bit's parity according to the parities of both a previous bit c_k and a pseudo-random wavefront perturbation $W_{\theta_h = x_h}^{\theta_k = 0}$, Property 2 still holds, because the probabilities that this condition is true or false are also close to 0.5. Finally, because the additional chaining diffusion is of a tempo process in an ascending order, one should decrypt in the exactly reverse order, *i.e.* a descending order.

3.3. Discussions

In the following discussions, we give three concrete examples and explain the effects of the proposed n D-WPIC and its improvements. Specifically, we illustrate the IS results of using pure wave perturbations ($\mathcal{F}_{nD}^{\theta_{k,h}}(\cdot)$), wave perturbations with the additional pseudo-noise ($\overline{\mathcal{F}}_{nD}^{\theta_{k,h}}(\cdot)$), and wave perturbations with both the additional noise and the diffusion chaining ($\overline{\overline{\mathcal{F}}}_{nD}^{\theta_{k,h}}(\cdot)$).

Fig. 4 illustrates the IS results of using the test image *Lenna*. As one can see, because of effective n D-WPIC in different dimensions, 0-bits and 1-bits are evenly spread. However, pure WPIC does not change the statistics of an image, namely the numbers of 0-bits and 1-bits are not changed, and this is reason why we see that this process changes the original pixel distribution, but fail to produce a uniform distribution. To solve this defect, we propose a remedy by using additional pseudo-noise. As one may see, pseudo-noise effectively scrambles image pixels to a uniform distribution as we expected. Finally, we see that the additional pixel chaining process does not harm a shuffling result. For the effect of this chaining process, we will discuss it later.

Fig. 5 illustrates the IS results of using the test image *ruler.512*. This is more challenging case in terms of highly tilted pixel distribution. Again, one may see that the pure WPIC successfully scrambles image pixels to random-like ones from the point view of human inspection, but fails to redistribute pixels evenly from the point view of pixel intensity distribution. Fortunately, the proposed improvements make up this defect successfully.

Fig. 6 illustrates the IS results of using the test image *zeros*, which is an all-zero image of size 512×512. This is an extreme case that the pure IS cannot defeat. To see this, one may compare the results before and after applying the

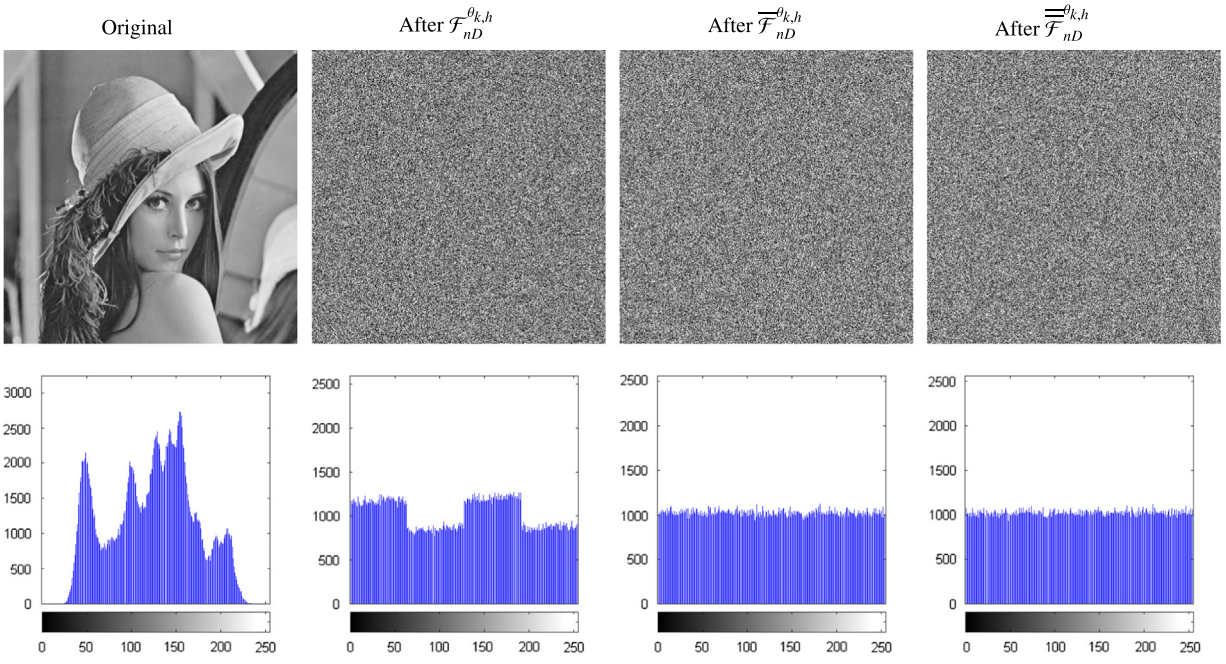

Fig. 4. n D-WPIC effects on image *Lenna*.

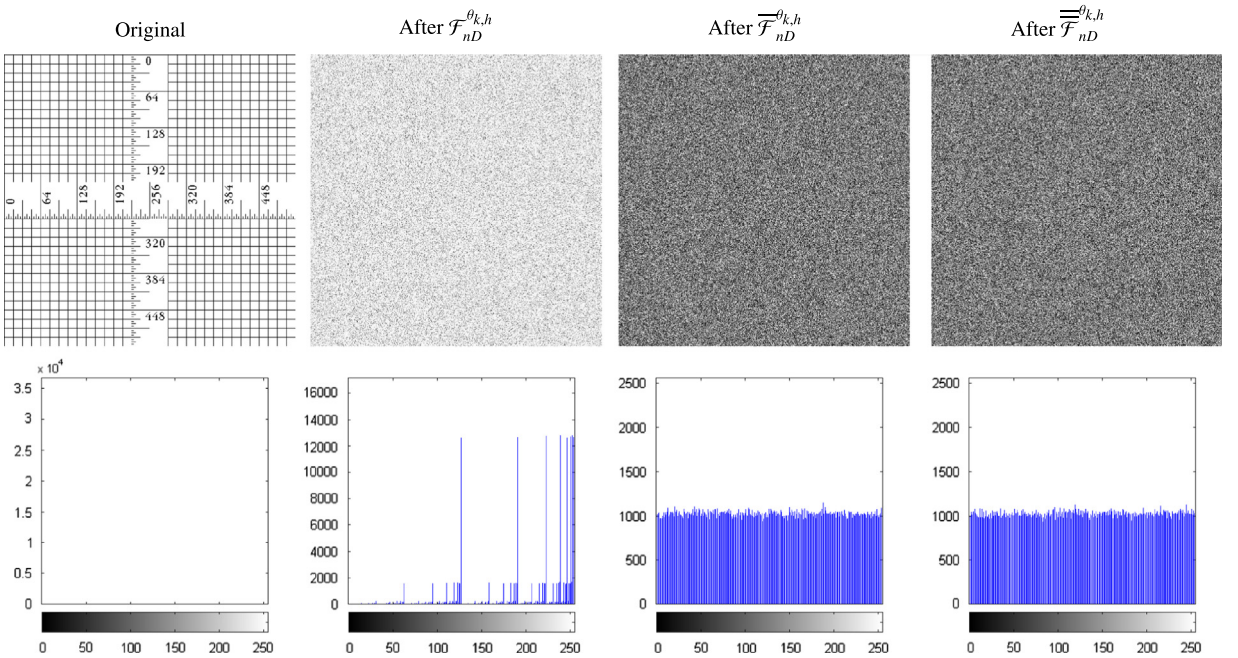

Fig. 5. *n* D-WPIC effects on image *ruler.512*.

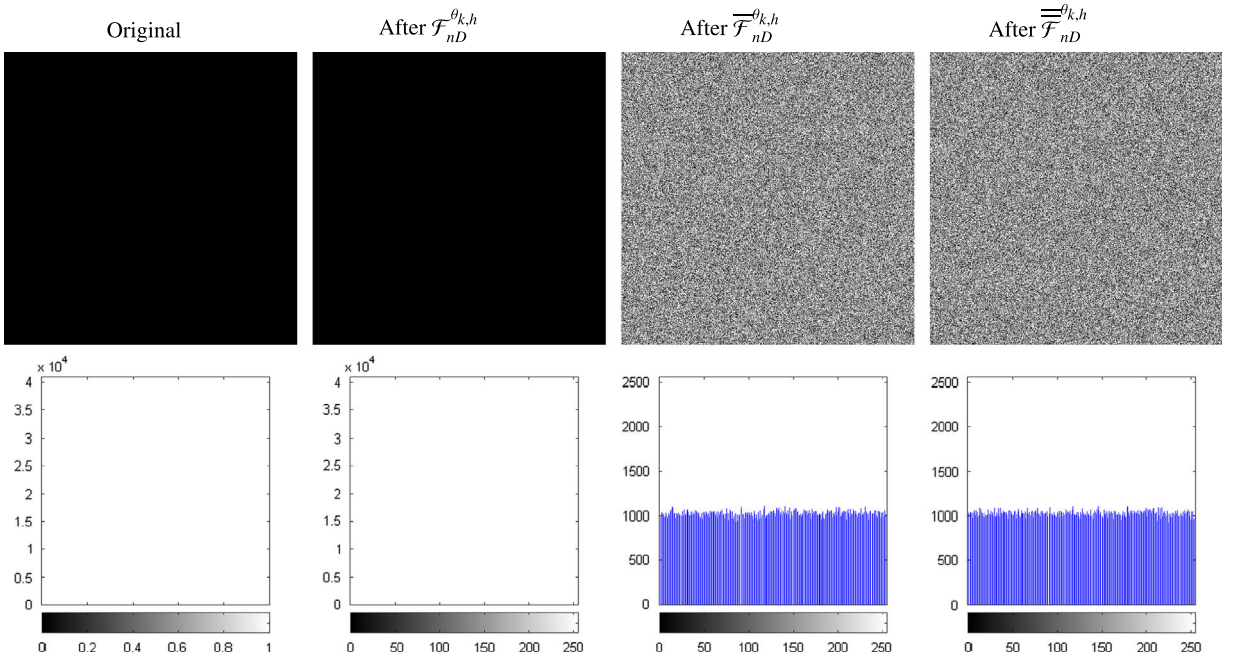

Fig. 6. *n* D-WPIC effects on image *zeros*.

pure WPIC. It is noticeable that these two images are identical, because the pure WPIC has the nature of permutation-only. If bits in different locations are different, the pure WPIC is able to produce a different result by rearranging these bits such as the ones in Figs. 4 and 5. However, in this case in Fig. 6, all bits in any locations are identically zeros, indicating that any rearrangement on these bits will be canceled. Hence, pure WPIC fails to achieve the random-like output from the view point of human inspection. In contrast, because the pseudo-random noise is not independent on an input image, Property 2 is then attained for an arbitrary input image, and we again see that this effective improvement indeed enhances randomness of a resulting image.

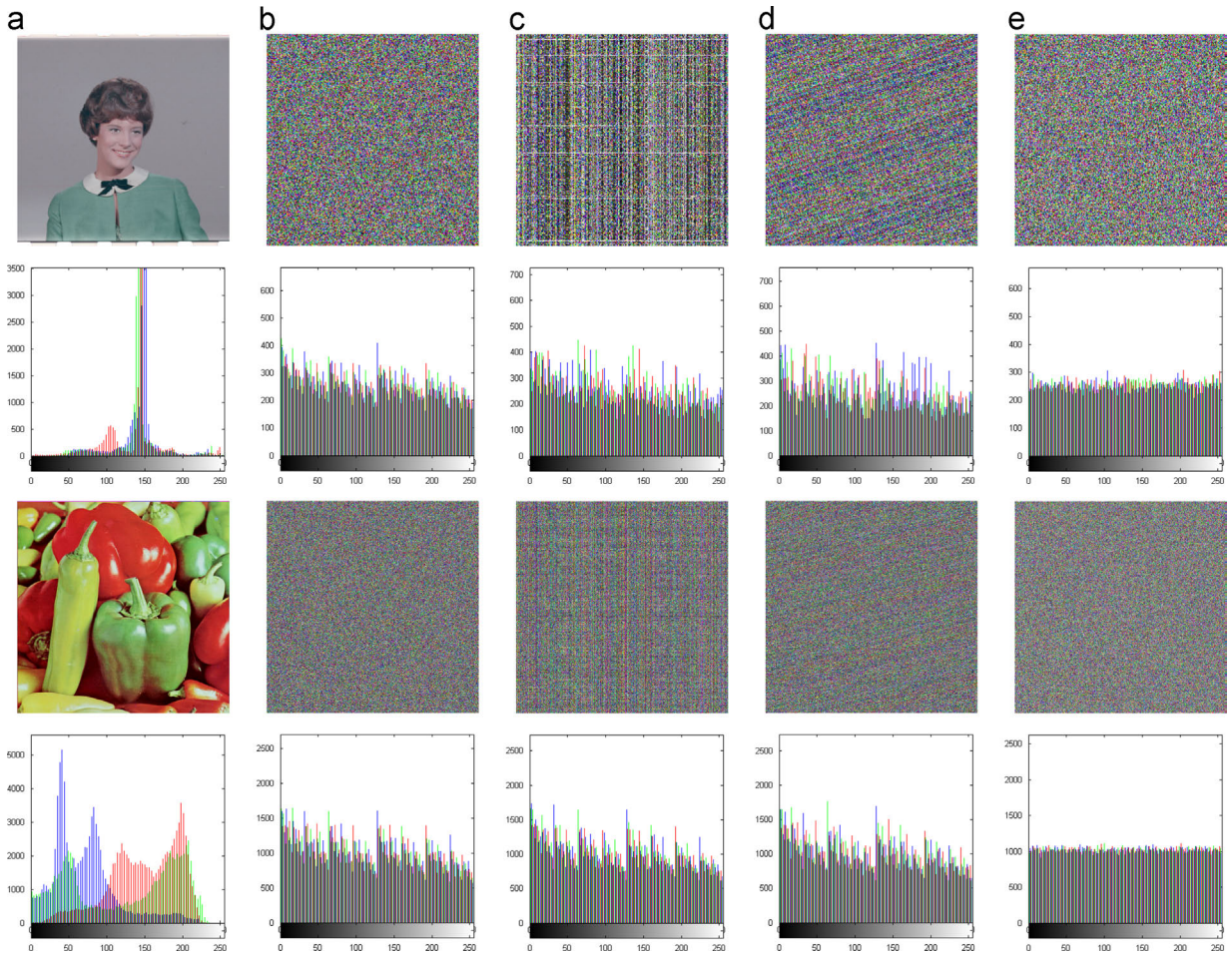

Fig. 7. Image scrambling using various methods (images in the 1st and 3rd rows are sizes of $256 \times 256 \times 3$ and $512 \times 512 \times 3$, respectively). (a) original images and their histograms. Scrambled images and their histograms using the (b) classic method, (c) Ye's method, (d) Fu's method, and (e) proposed n D-WPIC.

4. Comparison and analysis

Simulations in this section have been done under the MATLAB 2012a in a computer using the Windows 7 operating system with 4 GB RAM and Intel Xeon 2.4 GHz CPU. The tested IS algorithms include the *Classic* FisherC̈Yates shuffle method [20], *Ye's* method in [22], *Fu's* method in [18] and proposed n D-WPIC (with a key of length 256 bits and the build-in MATLAB PRNG). In particular, we only decompose an input image as a 3D signal, where the 3rd dimension is image bit depth to avoid possible unfair comparisons (because many peer algorithms do not support image encryption as an n D signal). However, the proposed method can be naturally extended to higher dimensional signals.

The 16 test images are color images in the *Miscellaneous* set in the USC-SIPI image database,[4] where eight images are of size $256 \times 256 \times 3$ and other eight ones are of size $512 \times 512 \times 3$. Figs. 7(b)–(e) show the results of test images in Fig. 7(a) using these four algorithms. It is noticeable that *Ye's* method is of mesh patterns and *Fu's* method is of slant patterns. The proposed n D-WPIC is of a flat histogram and visually indistinguishable from the results obtained by the *Classic* method in Fig. 7(b).

We first quantitatively evaluate results of each method with respect to image randomness using x-Correlation, y-Correlation, Global Entropy and the standard deviation of Block Entropy [35]. The x-Correlation and y-Correlation denote the absolute values of the Pearson correlation coefficients between two neighbor image pixel sequences at the horizontal and vertical directions, respectively. The Pearson correlation is defined in Eq. (21), where X, Y are two equal length sequences, $\mathrm{E}[\cdot], \mu_X, \mu_Y$ denote their mean values, and σ_X, σ_Y indicate their standard deviations. Global entropy is the Shannon entropy of a scrambled image by considering each image as an observation from a byte (8-bit) symbol source. It is defined in Eq. (22), where I denotes an image and $\Pr(I = i)$ is the probability of seeing a pixel of symbol i. Finally, the standard deviation of the block entropy [35] is the deviation of the Shannon entropy of all non-overlapping 16×16 image blocks in I as defined

[4] Available at http://sipi.usc.edu/database.

Table 1
Image randomness analysis.

Test image sizes	Method	x-Correlation	y-Correlation	Global Entropy	Block Entropy Std.
$256 \times 256 \times 3$	*Classic* [20]	0.00106 ± 0.000825	0.00261 ± 0.001760	7.88131 ± 0.227046	0.05753 ± 0.009571
	Ye's [22]	0.14273 ± 0.050056	0.01841 ± 0.015433	7.87216 ± 0.225127	0.08834 ± 0.032170
	Fu's [18]	0.00451 ± 0.004195	0.00586 ± 0.003555	7.87654 ± 0.226308	0.06511 ± 0.019094
	AES-CBC [37]	0.00135 ± 0.001053	0.00123 ± 0.000904	7.99905 ± 0.000075	0.05365 ± 0.001087
	n D-WPIC	0.00247 ± 0.001592	0.00234 ± 0.001580	7.99818 ± 0.004321	0.05209 ± 0.001231
$512 \times 512 \times 3$	*Classic* [20]	0.00038 ± 0.000284	0.00136 ± 0.000630	7.91756 ± 0.186379	0.05567 ± 0.008401
	Ye's [22]	0.10861 ± 0.074170	0.00781 ± 0.005567	7.91640 ± 0.186797	0.09009 ± 0.047542
	Fu's [18]	0.00244 ± 0.001899	0.00297 ± 0.002022	7.91639 ± 0.187257	0.05849 ± 0.012425
	AES-CBC [37]	0.00082 ± 0.000391	0.00107 ± 0.000782	7.99976 ± 0.000024	0.05233 ± 0.000518
	n D-WPIC	0.00122 ± 0.001075	0.00102 ± 0.000654	7.99830 ± 0.001619	0.05296 ± 0.001549

Table 2
Differential randomness analysis.

Test image sizes	Method	**NPCR** (Δkey)	**UACI** (Δkey)	**NPCR** (ΔO)	**UACI** (ΔO)
$256 \times 256 \times 3$	*Classic* [20]	99.5124 ± 0.19321	33.0035 ± 0.91197	0.0019 ± 0.00053	0.0002 ± 0.00014
	Ye's [22]	99.5377 ± 0.14993	29.5945 ± 1.36838	0.0019 ± 0.00053	0.0003 ± 0.00021
	Fu's [18]	99.5211 ± 0.19118	33.3202 ± 0.94574	0.0019 ± 0.00053	0.0002 ± 0.00010
	AES-CBC [37]	99.6140 ± 0.01584	33.4195 ± 0.04430	99.6170 ± 0.00983	33.4343 ± 0.05125
	n D-WPIC	99.6058 ± 0.01122	33.4867 ± 0.04409	99.6090 ± 0.01409	33.4640 ± 0.06804
$512 \times 512 \times 3$	*Classic* [20]	99.5492 ± 0.14286	33.1161 ± 0.73653	0.0006 ± 0.00023	0.0001 ± 0.00007
	Ye's [22]	99.5181 ± 0.23525	30.8273 ± 1.70269	0.0006 ± 0.00023	0.0001 ± 0.00007
	Fu's [18]	99.5496 ± 0.14957	33.2411 ± 0.66827	0.0005 ± 0.00023	0.0001 ± 0.00005
	AES-CBC [37]	99.6085 ± 0.00720	33.4438 ± 0.03566	99.6068 ± 0.00670	33.4470 ± 0.02864
	n D-WPIC	99.6090 ± 0.00603	33.4781 ± 0.03311	99.6102 ± 0.00679	33.4586 ± 0.03576

in Eq. (23), where B denote the image block variable:

$$\phi_{X,Y} = \mathrm{E}[(X-\mu_X)(Y-\mu_Y)]/(\sigma_X\sigma_Y) \tag{21}$$

$$H(I) = -\sum_{i=0}^{255} \Pr(I=i)\log \Pr(I=i) \tag{22}$$

$$\sigma_{16\times 16}(I) = \sqrt{\mathrm{E}[(H(B)-\mu_{H(B)})^2]} \tag{23}$$

The means and standard deviations of these measures for each method are listed in Table 1. As one can see, the *Classic* method can be still considered as the fast and robust one. *Ye's* method is not only the fastest one, but also the worst one due to high correlations and low global entropy with a larger standard deviation in block entropy. *Fu's* method is close to the *Classic* method, but also the slowest one. The proposed n D-WPIC is the best among these IS methods in terms of random-like statistics: (1) it attains much higher global entropy and a much smaller standard deviation in block entropy, indicating that the data distribution in the scrambled images is more uniform-like; and (2) it has the comparable performance, if not better than, to the listed methods in pixel correlations.

We now focus on quantitatively evaluating the IS results of each method with respect to the differential randomness of two related images. In particular, we use the metrics of the Number of Pixel Changing Rate (NPCR) and of the Unified Average Changed Intensity (UACI) [36] defined, respectively, in the following equations:

$$\mathrm{NPCR}(X,Y) = \frac{\sum_i \mathbf{1}_0(X_i - Y_i)}{T} \times 100\% \tag{24}$$

$$\mathrm{UACI}(X,Y) = \frac{\sum_i |X_i - Y_i|}{255\,T} \times 100\% \tag{25}$$

Both metrics here evaluate the pixel-wise change of two related images X and Y. $\mathbf{1}_0(x)$ is the indicator function giving value 1 when $x=0$ and value 0 otherwise, $|x|$ is the absolute value function, and T is the total number of pixels.

According to the relationship between the test images X and Y, one may apply NPCR and UACI for evaluating different security aspects of a method. We use these two metrics to evaluate (1) key sensitivity, and (2) plaintext sensitivity. Specifically, to test the key sensitivity of a method, we set the pairwise X and Y to be the resulting encrypted images of one identical original image with two keys only differing from each other for one bit. In contrast, to test plaintext sensitivity, we set X and Y to be the resulting encrypted images of two images differing from each other for one pixel with one identical key. The corresponding NPCR and UACI scores are listed in Table 2.

It is worthwhile to note that only methods with good diffusion and confusion properties [31] could achieve good NPCR and UACI scores. Specifically, the NCPR and UACI scores of two truly random $256 \times 256 \times 3$ images follow the Gaussian distributions $\mathbb{N}(99.6094\%, 0.01407\%^2)$ and $\mathbb{N}(33.4635\%, 0.05337\%^2)$, respectively [36]. And the NCPR and UACI scores of two truly random $512 \times 512 \times 3$ images follow the Gaussian distributions $\mathbb{N}(99.6094\%, 0.00703\%^2)$ and $\mathbb{N}(33.4635\%, 0.02668\%^2)$, respectively [36]. Comparing these theoretical NPCR and UACI statistics to those we observed in Table 2, we therefore say that the proposed method makes resulting images undistinguishable from

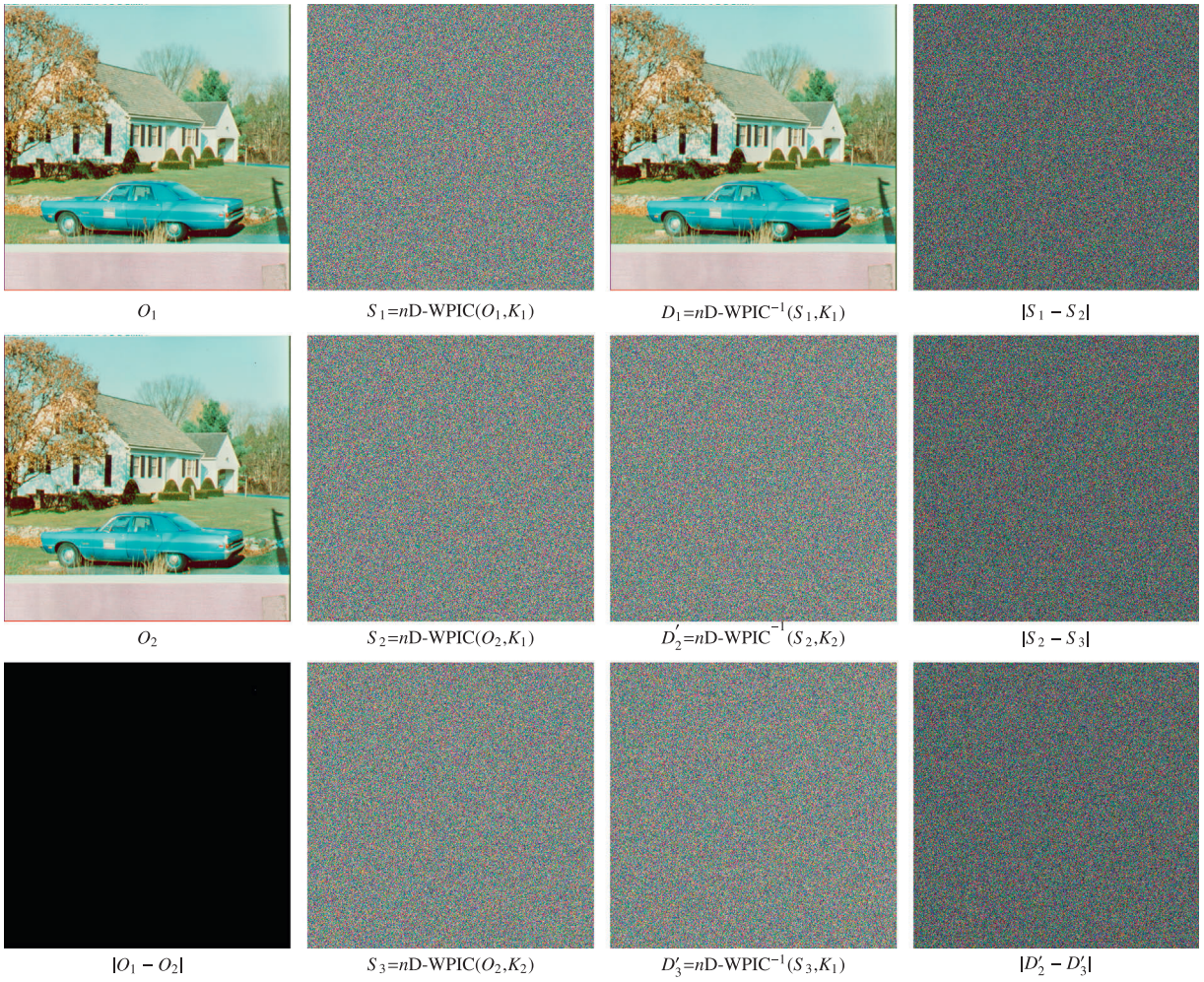

Fig. 8. Differential image randomness of using n D-WPIC. O_1 and O_2 are two images only different from each other at the pixel located at (50,450). K_1 and K_2 are two keys only different from each other for 1 bit.

those truly random ones. A visual example of the differential randomness of the proposed method is given in Fig. 8. As one can see, any slight change in an original image or a key bit will lead to significant changes after n D-WPIC.

5. Conclusion

In this paper, we introduced a new image cipher using n D wave perturbations to encrypt images. We showed that image contents can be scrambled by using wave perturbations, and wavefront at different locations can be viewed as a translation of a zero-wavefront. In this way, we only need to use PSNR to generate a zero-wavefront, but we are able to scramble an entire image. To improve the image cipher's confusion and diffusion properties, we introduced the additional pseudo-noise and diffusion chaining. These improvements require a low computational cost but guarantee a uniform distribution for 0-bits and 1-bits. Simulation results have shown that the proposed cipher is a fast solution to protect image contents, outperforms several existing methods, and has higher randomness and more evenly distributed pixels.

Acknowledgments

This work was supported in part by the Macau Science and Technology Development Fund under Grant 017/2012/A1 and by the Research Committee at University of Macau under Grants MYRG113(Y1-L3)-FST12-ZYC and MRG001/ZYC /2013/FST.

References

[1] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F.G.B. De Natale, A. Neri, A commutative digital image watermarking and encryption method in the tree structured haar transform domain, Signal Process.: Image Commun. 26 (1) (2011) 1–12.
[2] J. Li, X. Li, B. Yang, Reversible data hiding scheme for color image based on prediction-error expansion and cross-channel correlation, Signal Process. 93 (9) (2013) 2748–2758.
[3] X. Wang, X. Li, B. Yang, Z. Guo, Efficient generalized integer transform for reversible watermarking, IEEE Signal Process. Lett. 17 (6) (2010) 567–570.

[4] C.-Y. Lin, P. Prangjarote, L.-W. Kang, W.-L. Huang, T.-H. Chen, Joint fingerprinting and decryption with noise-resistant for vector quantization images, Signal Process. 92 (9) (2012) 2159–2171.
[5] X. Feng, H. Zhang, H.-C. Wu, Y. Wu, A new approach for optimal multiple watermarks injection, IEEE Signal Process. Lett. 18 (10) (2011) 575–578.
[6] S. Rawat, B. Raman, A blind watermarking algorithm based on fractional Fourier transform and visual cryptography, Signal Process. 92 (6) (2012) 1480–1491.
[7] Y. Zhou, L. Bao, C.L.P. Chen, Image encryption using a new parametric switching chaotic system, Signal Process. 93 (11) (2013) 3039–3052.
[8] W. Zeng, S. Lei, Efficient frequency domain selective scrambling of digital video, IEEE Trans. Multimedia 5 (1) (2003) 118–129.
[9] T.H. Chen, K.H. Tsao, Y.S. Lee, Yet another multiple-image encryption by rotating random grids, Signal Process. 92 (9) (2012) 2229–2237.
[10] L. Li, A.A. Abd El-Latif, X.M. Niu, Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images, Signal Process. 92 (4) (2012) 1069–1078.
[11] S.M. Seyedzadeh, S. Mirzakuchaki, A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, Signal Process. 92 (2012) 1202–1215.
[12] X. Wang, L. Teng, X. Qin, A novel colour image encryption algorithm based on chaos, Signal Process. 92 (2012) 1101–1108.
[13] Y. Zhou, L. Bao, C.L.P. Chen, A new 1D chaotic system for image encryption, Signal Process. 97 (2014) 172–182.
[14] D. Stinson, Cryptography: Theory and Practice, Discrete Mathematics and Its Applications, 3rd ed. Taylor & Francis, 2005, http://www.crcpress.com/product/isbn/9781584885085.
[15] L. Teng, X.Y. Wang, A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive, Opt. Commun. 285 (20) (2012) 4048–4054.
[16] T. Gao, Z. Chen, Image encryption based on a new total shuffling algorithm, Chaos Solitons Fract. 38 (1) (2008) 213–220.
[17] X. Wang, G. He, Cryptanalysis on a novel image encryption method based on total shuffling scheme, Opt. Commun. 284 (24) (2011) 5804–5807.
[18] C. Fu, B. Lin, Y. Miao, X. Liu, J. Chen, A novel chaos-based bit-level permutation scheme for digital image encryption, Opt. Commun. 284 (23) (2011) 5415–5423.
[19] Z.-L. Zhu, W. Zhang, K.-W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, Inf. Sci. 181 (6) (2011) 1171–1186.
[20] R. Durstenfeld, Algorithm 235: random permutation, Commun. ACM 7 (7) (1964) 420–421.
[21] H. Chen, J. Guo, L. Huang, J. Yen, Design and realization of a new signal security system for multimedia data transmission, EURASIP J. Appl. Signal Process. 2003 (2003) 1291–1305.
[22] G. Ye, Image scrambling encryption algorithm of pixel bit based on chaos map, Pattern Recognit. Lett. 31 (5) (2010) 347–354.
[23] G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Solitons Fract. 21 (3) (2004) 749–761.
[24] S. Behnia, A. Akhavan, A. Akhshani, A. Samsudin, Image encryption based on the jacobian elliptic maps, J. Syst. Softw. 86 (9) (2013) 2429–2438.
[25] Y. Wu, J.P. Noonan, S. Agaian, A wheel-switch chaotic system for image encryption, in: 2011 International Conference on System Science and Engineering (ICSSE), IEEE, 2011, pp. 23–27.
[26] Y. Wu, G. Yang, H. Jin, J.P. Noonan, Image encryption using the two-dimensional logistic chaotic map, J. Electron. Imaging 21 (1) (2012). 013014-1.
[27] K. Loukhaoukha, J.-Y. Chouinard, A. Berdai, A secure image encryption algorithm based on Rubik's cube principle, J. Electr. Comput. Eng. 2012 (2012) 7.
[28] A.B. Abugharsa, A.S.B. Hasan Basari, H. Almangush, A novel image encryption using an integration technique of blocks rotation based on the magic cube and the AES algorithm, Int. J. Comput. Sci. Issues 9 (4).
[29] Y. Wu, Y. Zhou, J.P. Noonan, S. Agaian, Design of image cipher using latin squares, Inf. Sci. 264 (2014) 317–339.
[30] Y. Wu, Y. Zhou, J.P. Noonan, K. Panetta, S. Agaian, Image encryption using the sudoku matrix, in: SPIE Defense, Security, and Sensing, International Society for Optics and Photonics, 2010, pp. 77080P–77080P-12.
[31] C.E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. 28 (4) (1949) 656–715.
[32] S. Li, C. Li, G. Chen, N.G. Bourbakis, K.-T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Process.: Image Commun. 23 (3) (2008) 212–223.
[33] C. Li, K.-T. Lo, Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Process. 91 (4) (2011) 949–954.
[34] H. Hermassi, R. Rhouma, S. Belghith, Security analysis of image cryptosystems only or partially based on a chaotic permutation, J. Syst. Softw. 85 (9) (2012) 2133–2144.
[35] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. Noonan, P. Natarajan, Local Shannon entropy measure with statistical tests for image randomness, Inf. Sci. 222 (2013) 323–342.
[36] Y. Wu, J.P. Noonan, S. Agaian, NPCR and UACI randomness tests for image encryption, Cyber J.: Multidiscip. J. Sci Technol. J. Sel. Areas Telecommun. (2011) 31–38.
[37] Advanced Encryption Standard, Federal Information Processing Standards Publication 197.