Optics and Lasers in Engineering 103 (2018) 9–23

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion

M.H. Annaby [a,*], M.A. Rushdi [b], E.A. Nehary [b]

[a] Department of Mathematics, Faculty of Science, Cairo University, P.O. Box 12613, Giza, Egypt
[b] Department of Biomedical and Systems Engineering, Faculty of Engineering, Cairo University, P.O. Box 12613, Giza, Egypt

ARTICLE INFO

Keywords:
Discrete fractional Fourier transform
Random transforms
Color image encryption
Chaotic maps
Phase retrieval
Chaotic diffusion
Spectral decomposition

ABSTRACT

The recent tremendous proliferation of color imaging applications has been accompanied by growing research in data encryption to secure color images against adversary attacks. While recent color image encryption techniques perform reasonably well, they still exhibit vulnerabilities and deficiencies in terms of statistical security measures due to image data redundancy and inherent weaknesses. This paper proposes two encryption algorithms that largely treat these deficiencies and boost the security strength through novel integration of the random fractional Fourier transforms, phase retrieval algorithms, as well as chaotic scrambling and diffusion. We show through detailed experiments and statistical analysis that the proposed enhancements significantly improve security measures and immunity to attacks.

1. Introduction

Big amounts of color image data are generated and transmitted everyday in different applications in science, technology [1–3], medicine [4–6], and education [7–9]. Adversary attacks to recognize the content of color images impose serious threats that motivated research in color image encryption [10–15]. Color image encryption methods typically include one or more of basic encryption modules such as data scrambling, chaotic diffusion, orthogonal transforms, phase retrieval algorithms, and color space representations. First of all, data scrambling [16–19] could be viewed as the simplest and most intuitive encryption technique. In such a technique, one applies a permutation scheme to image pixel locations. The permutation is set as the encryption key and the inverse of this permutation is used for decryption. Moreover, discrete chaotic maps are extensively implemented in image and video processing [20–24]. These maps are based on the generation of chaotic sequences that can be used to create robust scrambling schemes. However, image encryption based on chaotic maps only showed weak immunity against both ciphertext-only and chosen plaintext attacks [25,26]. In addition, not only are chaos-based encryption schemes insecure, but also general permutation-based encryption schemes are insecure as is proved in [27]. Moreover, statistical encryption measures, in particular entropy, UACI, and NPCR, show the lack of security in permutation-based encryption approaches [28].

As a matter of fact, with modern computers and fast algorithms, permutation-only encryption methods are not expected to show sufficient security strength for multimedia security. For this reason, orthogonal transforms, in particular the discrete fractional Fourier transform, have been applied in image encryption to increase security strength [29,30]. While the orthogonal-transform approach, to the best of our knowledge, has a reasonable immunity against cipher text and chosen plain text attacks, it has weak results under statistical analysis as is shown in Section 6. Consequently, researchers have been adding more encryption keys to chaotic and permutation scrambling [31]. In most cases, orthogonal transforms such as discrete fractional Fourier transforms (DFrFT) [32–34], discrete fractional cosine and Hartley transforms [35,36], and discrete wavelet transforms [37,38] are merged with the implementation of chaotic scrambling or joint transform correlation [39,40] to reach satisfactory security strength. As we have mentioned, such a combined approach resolves security weaknesses against ciphertext and chosen plaintext attacks, but it still shows weaknesses [41] with respect to NPCR and UACI measures [28].

Several techniques have been proposed to tackle the aforementioned deficiencies and improve security and statistical indicators. For example, Sam et al. [42] have created enhanced chaotic orbits via three logistic maps together with XORing and a diffusion procedure. The technique gives good NPCR, UACI, and histogram indicators. Similarly, Li and Liu [43] implemented a family of XORing operations together with the use of 2D Hénon and Chebyshev maps. Moreover, discrete fractional transforms have been combined with chaotic scrambling to achieve better

* Corresponding author.
E-mail address: mhannaby@sci.cu.edu.eg (M.H. Annaby).

https://doi.org/10.1016/j.optlaseng.2017.11.005
Received 20 June 2017; Received in revised form 24 September 2017; Accepted 8 November 2017
0143-8166/

security strength [41,44]. However, as is indicated in the statistical analysis we carried out in Section 3, the technique of [44] fails against the UACI, NPCR, and entropy measures. In [41], the authors applied an additional phase retrieval algorithm that enhanced some of the statistical measures. Nevertheless, some measures are still not satisfactory.

In this paper, we introduce two encryption frameworks that apply the recently defined randomized transforms of [45] in image encryption together with chaotic permutation, chaotic diffusion and phase retrieval. Experimental results indicate strong encryption performance in comparison to existing models. The aim of the proposed framework in this context is not just to merge the four mentioned techniques (orthogonal transforms, phase retrieval, chaotic permutations and diffusion) to produce a strong encryption scheme, but also to enhance the implementation of the orthogonal transforms and the chaotic scrambling and diffusion stages. As for the orthogonal transforms, we apply the randomized multi-parameter transforms of [45], and for scrambling, we exploit coupled and non-coupled logistic maps, avoiding stability islands [46]. The chaotic diffusion, which is linear, is implemented on the phase only.

The rest of the paper is organized as follows. In Section 2, we briefly introduce the encryption tools implemented in the paper. Section 3 highlights a couple of state-of-the-art encryption techniques and their statistical encryption deficiencies. Section 4 details our proposed encryption schemes whose block diagrams are shown in Figs. 8 and 10. Sections5 and 6, respectively investigate sensitivity to encryption keys, statistical measures, and immunity analysis. Conclusions are summarized in Section 7.

2. Encryption tools

2.1. Randomized transforms

Let $\lambda_k = e^{jk\frac{\pi}{2}}, k = 0, \dots, N-1$, where $N \in \mathbb{N}$ is fixed. The matrix of the discrete fractional Fourier transform (DFrFT) of order $\alpha \in \mathbb{R}$ is defined by [47]

$$F^{\alpha}[m,n] = \sum_{k=0}^{N-1} p_k(m) \left(\lambda_k\right)^{\alpha} p_k(n), \tag{1}$$

where $0 \le n, m \le N-1$, and $\{p_k(.)\}_{k=0}^{N-1}$ is an arbitrary orthonormal set of eigenvectors of the discrete Fourier transform (DFT). Since such an orthonormal basis (ONB) of eigenvectors is not unique, there has been established several techniques to compute such an ONB. In a novel classical piece of formal work [47], an ONB $\{u_k(.)\}_{k=0}^{N-1}$ is computed via the commutation of the DFT matrix $F := F^1$ and the matrix S defined by

$$S = \begin{pmatrix} -2 & 1 & \cdots & 1 \\ 1 & 2\cos(\omega) - 4 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 2\cos((N-1)\omega) - 4 \end{pmatrix}, \tag{2}$$

where $\omega = \frac{2\pi}{N}$. This leads to a DFrFT matrix

$$F^{\alpha}[m,n] = \sum_{k=0}^{N-1} u_k(m) \lambda_k^{\alpha} u_k(n), \tag{3}$$

where $\lambda_k^{\alpha} = e^{jk\alpha\frac{\pi}{2}}, k = 0, \dots, N-1$. As we have previously indicated, the DFrFT has been applied in image encryption [30], where NPCR, UACI, and entropy indicators show weak encryption strength against the ideal encryption standards of [28]. This stimulated research towards the derivation of randomized transforms [48–50].

In particular, Annaby et al. [45] introduced four variants of randomized discrete Fourier-type transforms by replacing the set of eigenvectors $\{u_k\}_{k=0}^{N-1}$ and the set of eigenvalues $\{\lambda_k^{\alpha}\}_{k=0}^{N-1}$ by randomized multi-parameter ones. In this paper, we use only one of these variants, namely, the multi-parameter discrete fractional random transform (MDFrRT). The implementation using other randomized transform variants can be carried out similarly, taking into account the computational and statistical aspects indicated in [45]. The MDFrRT transform is defined as follows. Let A be an $N \times N$ random matrix and $\vec{r} = (r_0, \dots, r_{N-1}) \in \mathbb{R}^N$ be a random vector. Let $\{v_k(.)\}_{k=0}^{N-1}$ be an ONB of eigenvectors of the Hermitian matrix $AA\dagger$, whose existence is guaranteed in [51]. The matrix of the MDFrRT transform is defined as

$$R^{\alpha}_{A,\vec{r}}[m,n] = \sum_{k=0}^{N-1} v_k(m) e^{\pi j \alpha \frac{r_k}{2}} v_k(n), \tag{4}$$

where the parameter $\alpha \in \mathbb{R}$ is chosen arbitrarily. This transform is privileged by having three strong keys: the fractional order α, the random matrix A, and the random vector $\vec{r}$.

2.2. The HSI color model

The HSI color model decomposes a color into three independent components of Hue, Saturation, and Intensity. This model is an ideal tool for creating image-processing techniques based on natural and intuitive color descriptions [52]. Images in the RGB color space can be converted into the HSI color space and vice versa. The model implemented here is that introduced in [52] as follows:

- An RGB image can be converted into an HSI image as follows. The hue H component is given by

$$H = \begin{cases} \theta, & \text{if } B \le G, \\ 360^\circ - \theta, & \text{if } B > G, \end{cases} \tag{5}$$

with

$$\theta = \cos^{-1}\left(\frac{0.5[\,(R-G) + (R-B)]}{[\,(R-G)^2 + (R-B)(G-B)]^{\frac{1}{2}}} \right).$$

The saturation S and intensity I components are given by

$$S = 1 - \frac{3}{(R+G+B)}[\min\{R,G,B\}],$$
$$I = \frac{1}{3}(R+G+B). \tag{6}$$

- Conversely, an HSI image representation can be converted into the RGB space depending on the range of the hue H values as follows:
  1. For the RG sector, where $0^\circ \le H < 120^\circ$,
  $$R = I\left(1 + \frac{S\cos(H)}{\cos(60^\circ - H)}\right),$$
  $$G = 3I - (R+B),$$
  $$B = I(1-S). \tag{7}$$
  2. For the GB sector where $120^\circ \le H < 240^\circ$, we offset the hue values to be $H \to H - 120^\circ$, then define the RGB components by:
  $$R = I(1-S),$$
  $$G = I\left(1 + \frac{S\cos(H)}{\cos(60^\circ - H)}\right),$$
  $$B = 3I - (R+G). \tag{8}$$
  3. For the BR sector where $240^\circ \le H \le 360^\circ$, we offset the hue values $H \to H - 240^\circ$, then define the RGB components as:
  $$R = 3I - (G+B),$$
  $$G = I(1-S),$$
  $$B = I\left(1 + \frac{S\cos(H)}{\cos(60^\circ - H)}\right). \tag{9}$$

2.3. Chaotic data scrambling

Data scrambling can be effectively carried out using chaotic mapping methods [46,53], particularly, the logistic map. A chaotic sequence can be generated by selecting a specific chaotic bifurcation parameter μ and initial point x_0 of the system

$$x_{n+1} = \mu x_n(1 - x_n),\ 0 < \mu < 4,\ x_0 \in [0,1]. \tag{10}$$