A blind robust watermarking scheme with non-cascade iterative encrypted kinoform

Ke Deng,[1] Guanglin Yang,[1,*] and Haiyan Xie[2]

[1]State Key Laboratory On Advanced Optical Communication System and Network, School of Electronic Engineering & Computer Science,Peking University, Beijing 100871, China
[2]China Science Patent Trademark Agents, Beijing 100083, China
**ygl@pku.edu.cn*

Abstract: A blind robust watermarking scheme is proposed. A watermark is firstly transformed into a non-cascade iterative encrypted kinoform with non-cascade phase retrieve algorithm and random fractional Fourier transform (RFrFT). An iterative algorithm and Human Visual System (HVS) are both presented to adaptively embed the kinoform watermark into corresponding 2-level DWT coefficients of the cover image. The kinoform accounts for much less data amount to be embedded than regular computer-generated hologram (CGH). And the kinoform can be extracted with the only right phase key and right fractional order, and reconstructed to represent original watermark without original cover image. The experiments have shown the scheme's high security, good imperceptibility, and robustness to resist attacks such as noise, compression, filtering, cropping.

OCIS codes: (070.2575) Fractional Fourier transforms; (090.1760) Computer holography; (100.2000) Digital image processing; (060.4785) Optical security and encryption.

References and links

1. M. He, Q. Tan, L. Cao, Q. He, and G. Jin, "Security enhanced optical encryption system by random phase key and permutation key," Opt. Express **17**(25), 22462–22473 (2009).
2. N. Takai, and Y. Mifune, "Digital watermarking by a holographic technique," Appl. Opt. **41**(5), 865–873 (2002).
3. Y. Aoki, "Watermarking technique using computer-generated holograms," Electron. Commun. Jpn. **84**(1), 21–31 (2001).
4. M. Liu, G. Yang, H. Xie, M. Xia, J. Hu, and H. Zha, "Computer-generated hologram watermarking resilient to rotation and scaling," Opt. Eng. **46**(6), 060501 (2007).
5. K. Deng, G. Yang, and C. Zhang, "Burch computer-generated hologram watermarking resilient to strong cropping attack," Biomedical Optics and 3-D Imaging (BIOMED) Topical Meeting, OSA Optics and Photonics Congress, April 2010, in Miami, FL, USA.
6. H. Zhai, F. Liu, X. Yang, G. Mu, and P. Chavel, "Improving binary images reconstructed from kinoforms by amplitude adjustment," Opt. Commun. **219**(1-6), 81–85 (2003).
7. P. Refregier, and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**(7), 767–769 (1995).
8. S. Kishk, and B. Javidi, "Information hiding technique with double phase encoding," Appl. Opt. **41**(26), 5462–5470 (2002).
9. Y. Sheng, Z. Xin, M. S. Alam, L. Xi, and L. Xiao-Feng, "Information hiding based on double random-phase encoding and public-key cryptography," Opt. Express **17**(5), 3270–3284 (2009).
10. R. Tao, Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the fractional Fourier domain," Opt. Express **15**(24), 16067–16079 (2007).
11. S. Deng, L. Liu, H. Lang, W. Pan, and D. Zhao, "Hiding an image in cascaded Fresnel digital holograms," Chin. Opt. Lett. **4**, 268–271 (2006).
12. S. Deng, L. Liu, H. Lang, D. Zhao, and X. Liu, "Watermarks encrypted in the cascaded Fresnel digital hologram," Optik (Stuttg.) **118**, 302–305 (2007).
13. C. Candan, M. A. Kutay, and H. M. Ozaktas, "The discrete fractional Fourier transform," IEEE Trans. Signal Process. **48**(5), 1329–1337 (2000).
14. S.-C. Pei, and W.-L. Hsue, "Random discrete fractional Fourier transform," IEEE Signal Process. Lett. **16**(12), 1015–1018 (2009).
15. S.-C. Pei, and W.-L. Hsue, "The multiple-parameter discrete fractional Fourier transform," IEEE Signal Process. Lett. **13**(6), 329–332 (2006).
16. Z. Liu, and S. Liu, "Random fractional Fourier transform," Opt. Lett. **32**(15), 2088–2090 (2007).
17. J. Li, X. Zhang, S. Liu, and X. Ren, "Adaptive watermarking scheme using a gray-level computer generated hologram," Appl. Opt. **48**(26), 4858–4865 (2009).

#136307 - $15.00 USD Received 11 Oct 2010; revised 4 Mar 2011; accepted 9 May 2011; published 10 May 2011

18. M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," IEEE Trans. Image Process. **10**(5), 783–791 (2001).
19. A. Reddy, and B. Chatterji, "A new wavelet based logo-watermarking scheme," Pattern Recognit. Lett. **26**(7), 1019–1027 (2005).
20. P. Bao, "Xiaohu Ma, "Image adaptive watermarking using wavelet domain singular value decomposition," IEEE Trans. Circ. Syst. Video Tech. **15**, 96–102 (2005).
21. W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, and Y. Pan, "An efficient watermarking method based on significant difference of wavelet coefficient quantization," IEEE Trans. Multimed. **10**(5), 746–757 (2008).
22. N. Bi, Q. Sun, D. Huang, Z. Yang, and J. Huang, "Robust image watermarking based on multiband wavelets and empirical mode decomposition," IEEE Trans. Image Process. **16**(8), 1956–1966 (2007).

1. Introduction

Rapid development in internet and wireless communication makes people much easier to get access to products such as images, videos and so on. However, it also provides convenient way for illegal acquisition and distribution of the copyright products. Recently, in order to effectively protect copyright, increasing research in both security and robustness of watermarking scheme [20–22] has been focused on.

To enhance the security of a watermarking scheme, some techniques in the field of security has been used in the watermarking. Double random phase encoding technique, proposed by Javidi, has been applied to optically or numerically encrypt the original watermark [7–9]. As a generation of traditional Discrete Fourier Transform (DFT), the fractional Fourier Transform (FrFT) [13] provides additional key for watermark embedding in the DFT domain of the cover image [10]. The cascaded Fresnel digital hologram is used for the encryption of digital image without lens architecture [11,12]. Also some other encryption algorithms such as pixel permutations and so on, are generally used to increase the difficulty to decrypt the watermark [1].

Meanwhile, to enhance the robustness of a watermarking scheme, Computer-generated hologram (CGH) has been investigated and used in watermarking [2–5]. With very good feature of the residue of empirical mode decomposition (EMD) to resist noise attack, literature [22] proposed robust image watermarking in multiband wavelet transform. However, an effective watermarking scheme demands comprehensive performance such as high security, good robustness and imperceptibility. The usage of CGH in watermarking accounts for large data amount and is reconstructed with conjugate images. Its security is much fragile. Besides, cascade phase retrieve watermarking algorithm converges slowly, which may lead to loss of source. Its robustness is poor as well. However, random fractional Fourier transform (RFrFT) [14–16] possesses good mathematical properties and can be directly used in optical encryption and decryption, which ensured good security. And non-cascade phase retrieve kinoform [6] converges quickly and account for less data amount, which not only ensured good imperceptibility, but also was reconstructed without conjugate image. The iterative embedding algorithm in Jianzhong Li's adaptive watermarking scheme [17] ensued both the imperceptibility and robustness of the watermarking. According to HVS, the Pixel-Mask model [18] also improved the imperceptibility of the watermarked image. Therefore, based on RFrFT, non-cascade phase retrieve kinoform and iterative embedding algorithm with HVS model, a new watermarking scheme is proposed in this paper to ensure quick convergence, high security, good imperceptibility, and robustness to resist attacks.

2. Non-cascade iterative encrypted kinoform

Compared to traditional CGH, kinoform is the one with less data amount and can be reconstructed with only one image. Also, because DFT is too simple to decrypt, the security of CGH is seriously affected. Therefore, a non-cascade iterative encrypted kinoform is proposed to ensure the security and less data amount to be stored.

2.1 Random fractional Fourier transform (RFrFT)

It is known that fractional Fourier transform (FrFT) [13] is generalization of common Fourier transform with high security of its fractional order. The α th order FrFT is defined as follows:

#136307 - $15.00 USD Received 11 Oct 2010; revised 4 Mar 2011; accepted 9 May 2011; published 10 May 2011

$$F^{\alpha}\left\{f(x)\right\}(u)=\int f(x)K_{\alpha}(x;u)dx, \tag{1}$$

where the F^{α} denotes the α th order FrFT function of the $f(x)$, the $f(x)$ denotes the original watermark, $K_{\alpha}(x;u)$ denotes the transform kernel function, and is defined as follows:

$$K_{\alpha}(x;u)=A_{\alpha}\exp\left[i\pi\left(\frac{u^2+x^2}{\tan\theta_{\alpha}}-\frac{2xu}{\sin\theta_{\alpha}}\right)\right], \tag{2}$$

where,

$$A_{\alpha}=\sqrt{1-i\cot\theta_{\alpha}}, \tag{3}$$

$$\theta_{\alpha}=\alpha\pi/2. \tag{4}$$

Based on FrFT definition, RFrFT [16] possesses good mathematical properties by randomizing the kernel function of FrFT to improve its high security. And it is defined as follows:

$$\Re^{\alpha}\left\{f(x)\right\}(u)=\int f(x)K'_{\alpha}(x;u)dx, \tag{5}$$

where $K'_{\alpha}(x;u)=P(x)K_{\alpha}(x;u)P^{*}(u)$, $P(x)$ and $P^{*}(u)$ represent two random mutually conjugated pure phase masks. Its simulation experiment has been done as shown in Fig. 1 and Fig. 2.

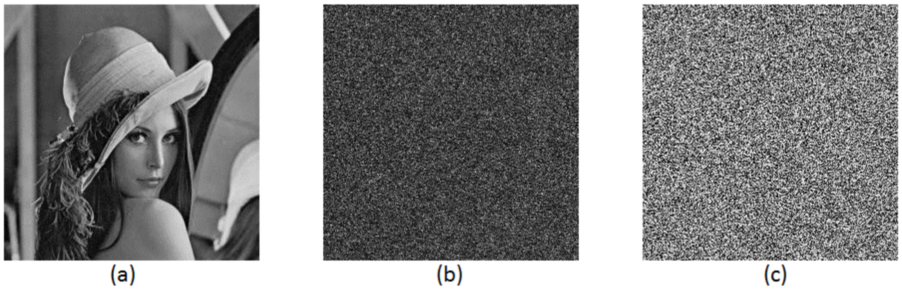

Fig. 1. (a) Cover image, (b) RFrFT amplitude image of the cover image (a), (c) RFrFT phase image of the cover image (a).

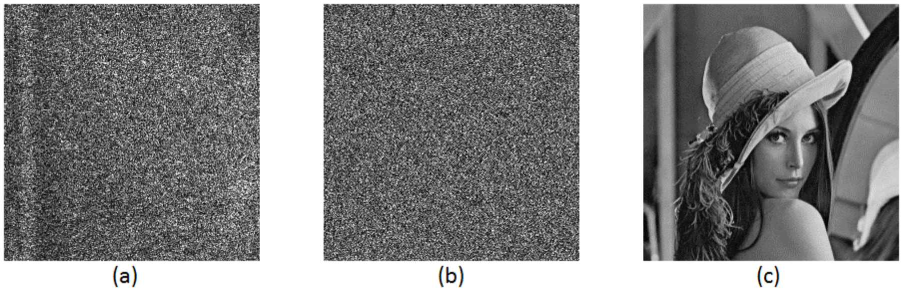

Fig. 2. Reconstructed image (a) with wrong order, (b) with wrong phase key, (c) with right order and right phase key.

#136307 - $15.00 USD Received 11 Oct 2010; revised 4 Mar 2011; accepted 9 May 2011; published 10 May 2011

2.2 Kinoform watermark generation

In order to conquer the disadvantage of large data amount of regular CGH, a non-cascade iterative encrypted kinoform, which possesses much less data amount and without conjugated image in reconstruction, is proposed based on the RFrFT and non-cascade phase retrieve algorithm. Its flowchart has been shown in Fig. 3.

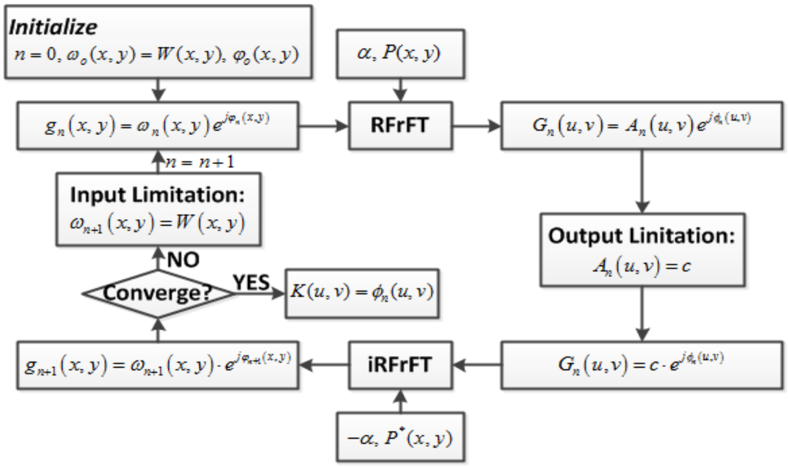
Initialize
$n=0, \omega_o(x,y)=W(x,y), \varphi_o(x,y)$
$\alpha, P(x,y)$
$g_n(x,y)=\omega_n(x,y)e^{j\varphi_n(x,y)}$
RFrFT
$G_n(u,v)=A_n(u,v)e^{j\phi_n(u,v)}$
$n=n+1$
Input Limitation:
$\omega_{n+1}(x,y)=W(x,y)$
Output Linitation:
$A_n(u,v)=c$
NO
Converge?
YES
$K(u,v)=\phi_n(u,v)$
$g_{n+1}(x,y)=\omega_{n+1}(x,y)\cdot e^{j\varphi_{n+1}(x,y)}$
iRFrFT
$G_n(u,v)=c\cdot e^{j\phi_n(u,v)}$
$-\alpha, P^*(x,y)$

Fig. 3. Kinoform watermark generation flowchart.

In the flowchart above, the original watermark image is defined as $W(x,y)$; the amplitude and random phase mask of input object function $g_n(x,y)$ are $\omega_n(x,y)$ and $e^{j\varphi_n(x,y)}$, respectively; the orders of RFrFT and inverse random fractional Fourier transform (iRFrFT) are α and $-\alpha$, respectively; the phase keys for RFrFT and iRFrFT are $P(x,y)$ and $P^{'}(x,y)$, respectively; the amplitude and phase mask of output image function is $A(u,v)$ and $e^{j\phi(u,v)}$, respectively. The limitation of the input plane and output plane are $\omega(x,y)=W(x,y)$ and $A(u,v)=c$ (i.e., c is a constant, normally c = 1), respectively.

The output image function and input object function is presented as follows:

$$\begin{cases} A(u,v)e^{j\phi(u,v)} = \Re_{\alpha}^{P}\left\{\omega(x,y)e^{j\varphi(x,y)}\right\} \\ \omega(x,y)e^{j\varphi(x,y)} = \Re_{-\alpha}^{P^*}\left\{A(u,v)e^{j\phi(u,v)}\right\} \end{cases}. \tag{6}$$

The non-cascade iterative encrypted kinoform is generated according to the following steps:

Step 1: The phase function $\varphi_0(x,y)$ of input object function $g_n(x,y)$, which uniquely distributes in $(0,2\pi)$, is generated; and the amplitude function $\omega_0(x,y)$ of input object function is the original watermark image $W(x,y)$. Therefore, the input complex function $g_0(x,y)=\omega_0(x,y)e^{j\varphi_0(x,y)}$ is obtained. According to the need of the scheme, the fractional order α and key $P(x,y)$ are generated;

Step 2: $g_0(x,y)$ is transformed by RFrFT to generate output image function $G_n(u,v)=A_n(u,v)e^{j\phi_n(u,v)}$; According to the output limitation $G_n(u,v)=c\cdot e^{j\phi_n(u,v)}$;

#136307 - $15.00 USD Received 11 Oct 2010; revised 4 Mar 2011; accepted 9 May 2011; published 10 May 2011

Step 3: The new image function is transformed by iRFrFT and phase key $P^{'}(x,y)$, andtheinputobjectcomplexfunction $g_{n+1}(x,y) = iRFrFT(G_n(u,v)) = \omega_{n+1}(x,y)e^{j\varphi_{n+1}(x,y)}$;

a: if the NMSE between $\omega_{n+1}(x,y)$ and $W(x,y)$ converges, go to step 4;

b: if not, according to the input limitation, $g_{n+1}(x,y) = W(x,y)e^{j\varphi_{n+1}(x,y)}$, and go to Step 2;

Step 4: The output image complex function is generated as $G(u,v) = \Re_{\alpha}^{P}\left\{W(x,y)e^{j\varphi(x,y)}\right\} = c \cdot e^{j\phi(u,v)}$, which actually is a pure phase function. After quantification, $\phi_n(u,v)$ is saved as a kinoform $K(u,v)$.

After generation of the non-cascade iterative encrypted kinoform, it can be embedded into the cover image according to the proposed embedding algorithm, which will be described in the following section.

3. Watermarking embedding

In order to extract original watermark without original cover image, a method is proposed to embed the kinoform into corresponding 2-level DWT coefficients of the cover image. First, the cover image is transformed by 2-level DWT, and HL2, LH2, HL1, and LH1 are selected and divided into several 3✖3 blocks, as shown in Fig. 4. Then, certain coefficients of the central position in each block are revised according to the kinoform and revision intensity of HVS mode [18,19]. In order to embed more information, overlapping blocks are preferred.

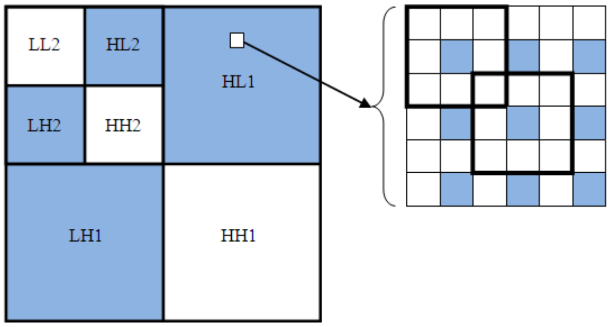

Fig. 4. Blocks and 2-level DWT coefficients selection.

According to the HVS model proposed in Ref [18], coefficient revision intensity β_i is calculated; According to the embedding algorithm proposed in Ref [17], we proposed the following embedding algorithm in Fig. 5. Δ is the quantization step; C_i is the value of central position in each block; A_i is the average value of C_i's 8 nearest neighbor positions; K_i ($0 \le K_i \le 1$)is normalized gray kinoform value; γ_i controls embedding intensity; and the embedding algorithm is executed as follows:

Step1: Let $C_i^{'} = |A_i| + \gamma_i \cdot K_i$, $m_i = 0$;

Step2: If $\left|C_i^{'} - |C_i|\right| > \beta_i |C_i|$, revise appropriate value of m_i according to the following rules:

a: If $C_i^{'} - |C_i| > \beta_i |C_i|$, let $C_i^{'} = C_i^{'} - \Delta$ and $m_i = m_i + 1$. Repeat until $C_i^{'} - |C_i| \le \beta_i |C_i|$. Otherwise go to b.

b: If $C_i^{'} - |C_i| < -\beta_i |C_i|$, let $C_i^{'} = C_i^{'} + \Delta$ and $m_i = m_i - 1$. Repeat until $C_i^{'} - |C_i| \ge -\beta_i |C_i|$.

Step 3: If $C_i < 0$, let $C_i^{'} = -C_i^{'}$;

Step 4: Replace C_i with $C_i^{'}$.

#136307 - $15.00 USD Received 11 Oct 2010; revised 4 Mar 2011; accepted 9 May 2011; published 10 May 2011

After kinoform watermark embedding, the coefficients satisfy the following equations. And a watermarked image is obtained after inverse 2-level DWT.

$$\begin{cases} \left|C_i^{'}\right| = \left|A_i\right| + \gamma_i \cdot K_i - m_i \cdot \Delta \\ \left|C_i^{'} - C_i\right| \le \beta_i \cdot \left|C_i\right| \\ C_i^{'} \cdot C_i > 0 \end{cases} . \tag{7}$$

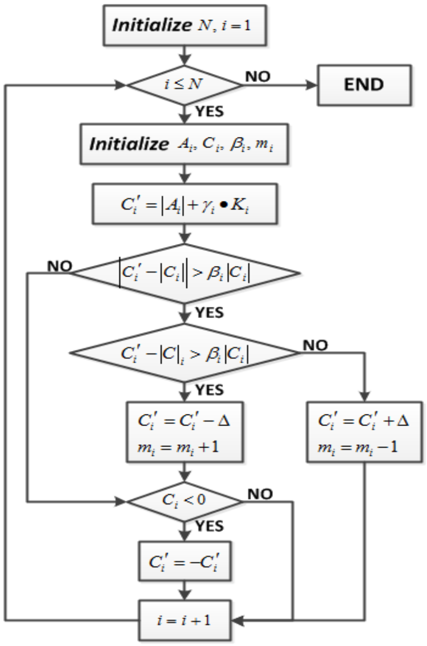

Fig. 5. Kinoform watermark embedding flowchart.

4. Watermarking extraction and reconstruction

Similar to the watermarking embedding procedure, the watermarked image is decomposed to be LL2, HL2, LH2, HH2, HL1, LH1, LL2 by 2-level DWT; and the corresponding embedding position is selected from HL2, LH2, HL1 and LH1. According to the following equation, the each pixel of the kinoform could be extracted:

$$K_i^{'} = \frac{\left|C_i\right| - \left|A_i\right| + m_i \cdot \Delta}{\gamma_i} . \tag{8}$$

After rearrangement of extracted pixel values, $K^{'}\left(u,v\right)$ could be obtained. Then, according to the kinoform generation flowchart and Eq. (9), the original watermark can be reconstructed with the right order $-\alpha$ and phase key $P^{'}$.

$$W^{'}\left(x,y\right) = \left|\Re_{-\alpha}^{P^*}\left\{e^{jK^{'}(u,v)}\right\}\right| . \tag{9}$$

5. Numerical simulations and analysis

5.1 Judgment principle

In order to evaluate the performance of the proposed scheme, three parameters are defined and used to make a quantitative measure.

#136307 - $15.00 USD Received 11 Oct 2010; revised 4 Mar 2011; accepted 9 May 2011; published 10 May 2011

A. to measure the perceptual distortion of the watermarked image, the Peak Signal to Noise Ratio (PSNR) was defined as follows:

$$PSNR = 10\log_{10}\frac{L^2}{\frac{1}{N_x N_y}\sum_{x=1}^{N_x}\sum_{y=1}^{N_y}\left[I_o(x,y) - I_w(x,y)\right]^2}\ dB, \tag{10}$$

where L is the peak value of the signal, and the size of the image is $N_x \times N_y$, $I_o(x,y)$ and $I_w(x,y)$ represent the original cover image and watermarked image, respectively.

B. To evaluate the similarity degree between the original watermark and extracted watermark, Normalized Cross Correlation (NCC) is defined as follows:

$$NCC = \frac{\sum_i\sum_j W_{ij}W_{ij}^{'}}{\sum_i\sum_j (W_{ij})^2}, \tag{11}$$

where the W_{ij} and $W_{ij}^{'}$ present the pixel values at the position (i, j) of the original and extracted watermark by that $0 \le i \le N_x, 0 \le j \le N_y$, respectively.

C. To evaluate the convergence of the generated kinoform, Normalized Mean Square Error (NMSE) is used and defined as follows:

$$NMSE = \frac{1}{N_x N_y}\sum_{x=1}^{N_x}\sum_{y=1}^{N_y}\left[I_o(x,y) - \alpha I_r(x,y)\right]^2, \tag{12}$$

where $\alpha = \frac{\sum_{x=1}^{N_x}\sum_{y=1}^{N_y} I_o(x,y) I_r(x,y)}{\sum_{x=1}^{N_x}\sum_{y=1}^{N_y}[I_r(x,y)]^2}$, the size of the image is $N_x \times N_y$, I_o and I_r represent original image and reconstructed image, respectively.

5.2 Numerical simulations

In the numerical simulation experiments, a gray image “Lena” (256 × 256 pixels) and a binary image “PKU” (64 × 64 pixels) are chosen as the cover image and the original watermark, respectively, as shown in Fig. 6 (a) and (b). And several numerical tests are implemented to verify the performance of the proposes watermarking scheme under the hardware environment of Dell Precision T 5400 Intel Xeon CPU 2.5 GHz workstation with 4 GB RAM memory and MATLAB version 7.

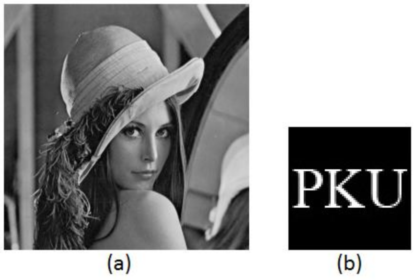

Fig. 6. (a) Original cover image (256✖256 pixels), (b) original watermark (64✖64 pixels).

5.2.1 Non-cascade encrypted kinoform generation

A non-cascade encrypted kinoform (64 × 64 pixels) is generated and shown in Fig. 7(a) according to the kinoform watermark generation algorithm. After watermark embedding procedure, a watermarked image(PSNR = 42.34, 256 × 256 pixels)is generated, as shown in Fig. 7(b). Without any attacks, a whole kinoform (64 × 64 pixels) can be extracted, as shown in Fig. 7(c), and the original watermark can be reconstructed with high NCC value of 0.9592, as shown in Fig. 7(d).

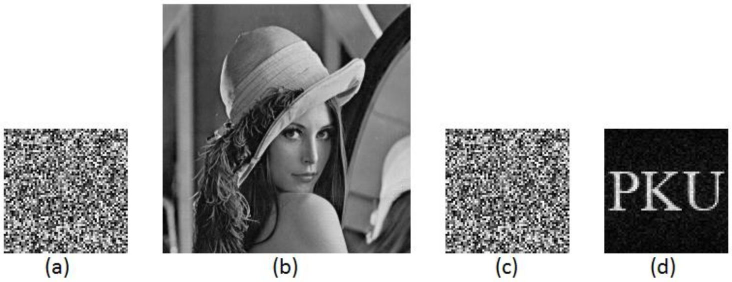

Fig. 7. (a) Non-cascade encrypted kinoform, (b) watermarked image (PSNR = 42.34), (c) extracted kinoform, (d) reconstructed watermark (NCC = 0.9592).

5.2.2 Convergence tests

During the non-cascade iterative encrypted kinoform generation periods, the kinoform is obtained after iterative calculation. After each loop, the amplitude of the new object function is calculated by NMSE, as shown in Fig. 8. In Fig. 8, we can find that the NMSE is converging fast before 20 loops, and slow down after 20 loops. Compared to HE's method [1] "Cascade FrFT" in Fig. 8, the convergence in the proposed scheme goes much quickly than that of HE's method. And the NMSE in the proposed scheme can reach less than 0.08, while the HE's method can only reach about 0.1. Therefore, the proposed watermarking scheme converges much faster and reaches a much lower NMSE value.

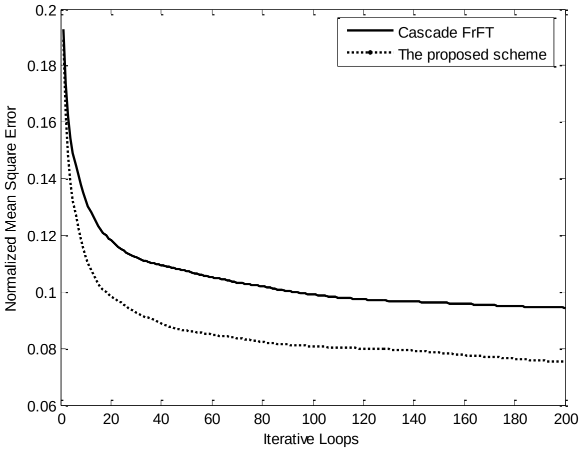

Fig. 8. NMSE value and iterative loops for non-cascade encrypted kinoform generation.

5.2.3 Security tests

The watermarking scheme possessed good security characteristics with α order and phase key $P(x,y)$ in RFrFT. From Fig. 9, it is found that on the condition of right phase key $P(x,y)$, only with the right order ($\alpha = 0.8718$), the watermark image can be extracted with high NCC value of 0.9614. When α goes much closer to the right order value, the watermark can be extracted with a much higher NCC value, which can be shown in Fig. 9 and the curve “Right phase key” in Fig. 11. And vice versa.

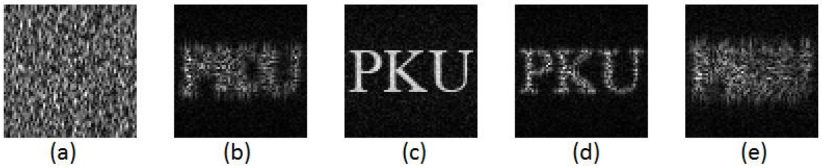

Fig. 9. Extracted watermark with right phase key and (a) with α = 0.15, NMSE = 0.9111, NCC = 0.2981, (b) with α = 0.8, NMSE = 0.6647, NCC = 0.5791, (c) with α = 0.8718, NMSE = 0.0757, NCC = 0.9614, (d) with α = 0.9, NMSE = 0.3738, NCC = 0.7913, (e) with α = 0.99, NMSE = 0.7327, NCC = 0.5170.

However, with the wrong phase key $P(x,y)$, the watermark cannot be extracted with high NCC value whatever α order is, which can be shown as Fig. 10 and the curve “Wrong phase key” in Fig. 11.

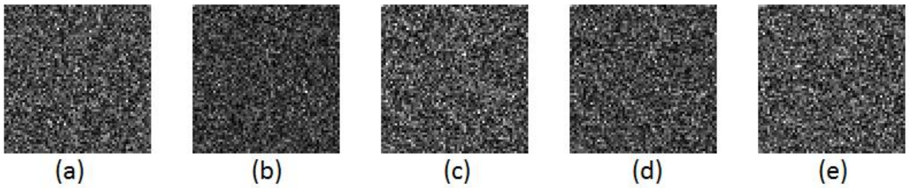

Fig. 10. Extracted watermark with wrong phase key and (a) with α = 0.15, NMSE = 0.9201, NCC = 0.2826, (b) with α = 0.8, NMSE = 0.9270, NCC = 0.2702, (c) with α = 0.8718, NMSE = 0.9257, NCC = 0.2726, (d) with α = 0.9, NMSE = 0.9230, NCC = 0.2775, (e) with α = 0.99, NMSE = 0.9178, NCC = 0.2867.

And, the following curve in Fig. 11 also account for the high security.

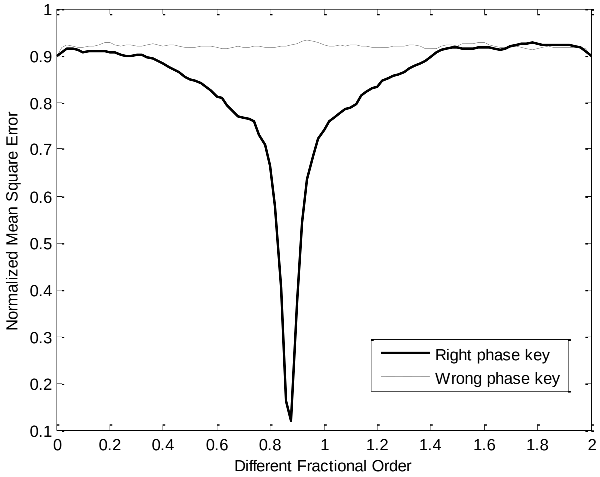

Fig. 11. The NMSE value in kinoform reconstruction with different fractional order by the right phase key and wrong phase key.

5.2.4 Attack tests

In order to test the robustness of the proposed scheme, related simulation attack experiments are executed as shown in Fig. 12. The robustness of resisting JPEG loss compression is good. Related experiments are shown as follows:

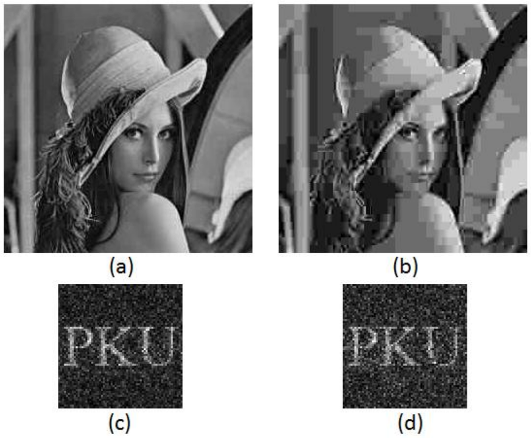

Fig. 12. (a) Watermarked image suffering from 30% JPEG compression, $PSNR = 27.38dB$, (b) watermarked image suffering from 5% JPEG Compression, $PSNR = 23.70dB$, (c) extracted watermark from (a), $NCC = 0.6885$, (d) extracted watermark from (b), $NCC = 0.6132$.

Because of the property of CGH to resist cropping attack, the proposed watermarking scheme with the kinoform is tested with different kinds of cropping attacks. The experiment results are shown in Fig. 13.

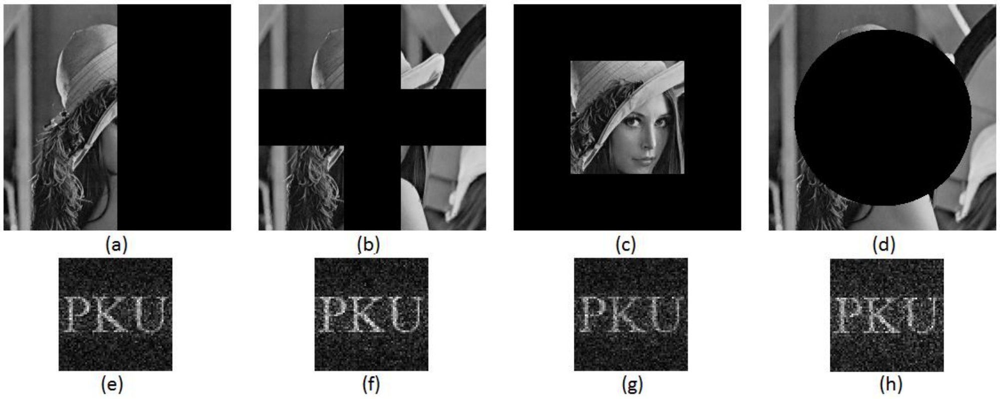

Fig. 13. Robustness to resist cropping attack (a) column attack 50%, $PSNR = 8.46dB$, (b) cross attack 44%, $PSNR = 10.03dB$, (c) anonymous attack $PSNR = 7.83dB$, (d) circle attack $PSNR = 9.72dB$, (e) extracted watermark from (a) $NCC = 0.7465$, (f) extracted watermark from (b) $NCC = 0.7634$, (g) extracted watermark from (c) $NCC = 0.7142$, (h) extracted watermark from (d) .

The measurement of robustness to resist other attacks and extracted watermark images have been shown in Table 1 and Fig. 14, respectively. Table 1 shows the measure of the robustness of the proposed scheme to resist different attacks.

Received 11 Oct 2010; revised 4 Mar 2011; accepted 9 May 2011; published 10 May 2011

Table 1. Robust to Different Attacks

Attack Type	PSNR	NCC
Gaussian noise (sigma = 0.001)	28.68dB	0.8081
Salt and pepper noise(0.01)	24.04dB	0.6634
Gaussian filtering (4✖4, sigma = 1)	24.60 dB	0.6706
Average filtering (4✖4)	23.67dB	0.6558
Median filtering (4✖4)	23.96dB	0.6528
Motion Blurring	19.41dB	0.6515
Histogram Equalization	18.59dB	0.6887

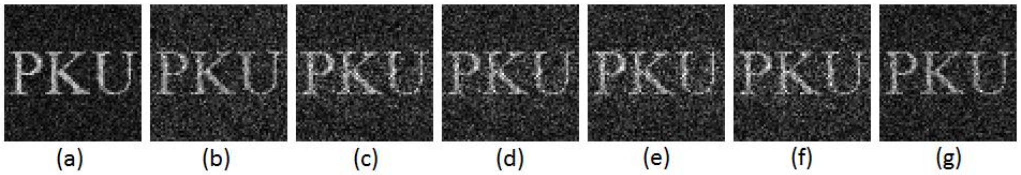

Fig. 14. Reconstruction of extracted kinoform under different attacks (a) Gaussian noise (sigma = 0.001), (b) Salt and pepper noise (0.01), (c) Gaussian filtering (4✖4, sigma = 1), (d) Average filtering (4✖4), (e) Median filtering (4✖4), (f) Motion Blurring, (g) Histogram Equalization.

6. Conclusion

By means of non-cascade iterative encrypted kinoform and corresponding embedding algorithm, a new watermarking scheme has been proposed to embed the kinoform to the 2-level DWT coefficients of the cover image. The proposed scheme secured watermarked image's imperceptibility and possesses good security as well as robustness. And the watermark is extracted without original cover image. Compared to the optical holography, the kinoform is much easier to generate by computers. Besides, the data amount of the kinoform account only 1/4 of the CGH, which can be embedded into the cover image so as to ensure the watermarked image's good imperceptibility. And the kinoform generation algorithm converges more quickly than the cascaded method in literature [1]. Besides, with the good security feature of RFrFT, the proposed scheme possesses high security, and can also resist other malicious attacks, such as JPEG compression, cropping attack, noise attack, filtering. Therefore, the scheme generally possesses comprehensive performance (imperceptibility, quick convergence, less data amount, security, and robustness).