Journal of Zhejiang University SCIENCE A
ISSN 1009-3095 (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Optical encryption with cascaded fractional wavelet transforms*

BAO Liang-hua[†1,2], CHEN Lin-fei[1], ZHAO Dao-mu[†‡1]
([1]*Department of Physics, Zhejiang University, Hangzhou 310027, China*)
([2]*Department of Physics, Zhejiang Education College, Hangzhou 310012, China*)
[†]E-mail: baolh001@163.com; zhaodaomu@yahoo.com
Received Jan. 6, 2006; revision accepted Mar. 22, 2006

Abstract: On the basis of fractional wavelet transform, we propose a new method called cascaded fractional wavelet transform to encrypt images. It has the virtues of fractional Fourier transform and wavelet transform. Fractional orders, standard focal lengths and scaling factors are its keys. Multistage fractional Fourier transforms can add the keys easily and strengthen information security. This method can also realize partial encryption just as wavelet transform and fractional wavelet transform. Optical realization of encryption and decryption is proposed. Computer simulations confirmed its possibility.

Key words: Wavelet transform (WT), Cascaded fractional wavelet transform (CFWT), Encryption, Decryption
doi:10.1631/jzus.2006.A1431 **Document code:** A **CLC number:** O43

INTRODUCTION

Recently, with the development of science and technology, more and more people become interested in researching image encryption techniques. Many methods have been proposed for optical image encryption. Random phase encoding methods and digital holography techniques are effectively used in encrypting (Javidi and Nomura, 2000; Unnikrishnan *et al.*, 2000a; Hennelly and Sheridan, 2003; Nishchal *et al.*, 2004). Meantime some important properties of light are used to realize encryption (Tajahuerce *et al.*, 2001; Unnikrishnan *et al.*, 2000b; Naulleau, 2001). Wavelet transform (WT) has been widely used to encrypt and compress images in wireless data communication, such as network, TV and multimedia, and has some relatively better compression ratio than MPEG and better image quality than JPEG. Extensive research has been focused on image encryption based on WT (Dang and Chau, 2000). Partial encryption is also realized by decomposing the frequency and hiding some significant parts (Cheng and Li, 2000). People can get some information but not all when they have parts of the keys. It is a useful method in signal processing, and deep research has been done in this area. A new method using fractional wavelet transform (FWT) to encrypt the image proposed by Chen and Zhao (2005) is better than the encryptions based on fractional Fourier transform (FRFT) or WT, because it has the virtues of both FRFT and WT. The fractional orders of FRFT and scaling factors of WT are the important keys.

In this paper we use the additive property of FRFT and propose a new method called cascaded fractional wavelet transform (CFWT) to encrypt the images so that it can add the keys easily by multistage transforms. The fractional orders, standard focal lengths and scaling factors are randomly chosen, so that the image would be well protected and not be cracked easily. So unauthorized people cannot obtain information without the correct keys. This method can be used both in optical encryption and wireless signal processing. The partial encryption technique is also realized by this method.

This paper is organized as follows. We introduce the basic theory of FWT, its inverse transformation and

‡ Corresponding author
* Project (No. 10276034) supported by the National Natural Science Foundation of China

its optical implementation in the second section. In the third section, the notion of CFWT is proposed and the optical realizations of encryption and decryption processes are also presented. Computer simulation results are shown in the fourth section. And finally we give some conclusions.

FRACTIONAL WAVELET TRANSFORM

Two-dimensional hybrid FWT of $f(x,y)$ (Mendlovic *et al*., 1997) can be defined as

$$W(\boldsymbol{a}_{mn},\bar{\boldsymbol{b}}) = \iiiint B_{p_1,p_1'}(x,y;x',y')f(x,y)h^*_{\boldsymbol{a}_{mn}\bar{\boldsymbol{b}}}(x',y')\mathrm{d}x\mathrm{d}y\mathrm{d}x'\mathrm{d}y', \quad (1)$$

where $B_{p_1,p_1'}(x,y;x',y')$ is the fractional kernel and is given by

$$B_{p_1,p_1'}(x,y;x',y') = B_{p_1}(x,x')B_{p_1'}(y,y') \quad (2)$$

and

$$B_{p_1}(x,x') = \frac{\exp\{-\mathrm{i}[\pi\,\mathrm{sgn}(\sin\phi_1)/4-\phi_1/2]\}}{\left|\lambda f_{s1}\sin\phi_1\right|^{1/2}} \times \exp\left[\mathrm{i}\pi\frac{x^2+(x')^2}{\lambda f_{s1}\tan\phi_1}-2\mathrm{i}\pi\frac{xx'}{\lambda f_{s1}\sin\phi_1}\right], \quad (3)$$

$$B_{p_1'}(y,y') = \frac{\exp\{-\mathrm{i}[\pi\,\mathrm{sgn}(\sin\phi_2)/4-\phi_2/2]\}}{\left|\lambda f_{s2}\sin\phi_2\right|^{1/2}} \times \exp\left[\mathrm{i}\pi\frac{y^2+(y')^2}{\lambda f_{s2}\tan\phi_2}-2\mathrm{i}\pi\frac{yy'}{\lambda f_{s2}\sin\phi_2}\right], \quad (4)$$

where p_1 and p_1' are the fractional orders of FRFT, $\varphi_1=\pi p_1/2$, $\varphi_2=\pi p_2/2$, λ is the wavelength of incident light, f_{s1} and f_{s2} are the standard focal lengths in x and y directions, respectively. And $h_{\boldsymbol{a}_{mn}\bar{\boldsymbol{b}}}(x',y')$ is the scaled and shifted wavelet function of mother wavelet function and is given by

$$h_{\boldsymbol{a}_{mn}\bar{\boldsymbol{b}}}(x',y') = (a_m a_n)^{-1/2}h\left(\frac{x'-b_{x'}}{a_m},\frac{y'-b_{y'}}{a_n}\right), \quad (5)$$

where $\boldsymbol{a}_{mn}=(a_m,a_n)$ is the discrete scaling vector, $\bar{\boldsymbol{b}}=(b_{x'},b_{y'})$ is the shift vector and * in Eq.(1) means the complex conjugate.

The inverse FWT is

$$f(x,y) = \frac{1}{C}\iint\left[\sum_m\sum_n\int\int\frac{1}{a_m a_n}W(\boldsymbol{a}_{mn},\bar{\boldsymbol{b}})h_{\boldsymbol{a}_{mn}\bar{\boldsymbol{b}}}(x',y')\mathrm{d}b_{x'}\mathrm{d}b_{y'}\right](x',y') \cdot B_{-p_1,-p_1'}(x,y;x',y')\mathrm{d}x'\mathrm{d}y', \quad (6)$$

FWT's optical configuration is proposed in Fig.1 showing that an FWT is implemented by joining an FRFT and a WT together. The multireference matched filter (MRMF) in the FWT configuration is described as

$$MRMF(u,v) = \sum_m\sum_n\{H^*[\boldsymbol{a}_{mn}(u-nu_0,v-mv_0)]\}, \quad (7)$$

where $H(u,v)$ is the Fourier transform of mother wavelet function $h(x,y)$. The spatial multiplexing distribution of MRMF is realized by a Dammann grating (Mendlovic and Konforti, 1993). And the optical implementation of inverse FWT can be obtained by a WT with the MRMF having the distribution of $H[\boldsymbol{a}_{mn}(u-nu_0,v-mv_0)]$ and a corresponding FRFT with $-p$ order.

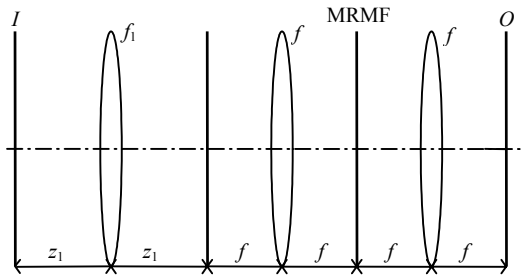

Fig.1 Optical implementation for a 2D FWT. *I*: Input plane; *O*: Output plane; *f* and f_1 are the focal lengths of the lenses; z_1 is the distance between the lens and input (or output) plane

CASCADED FRACTIONAL WAVELET TRANSFORM

As we know, FRFT has additive property (Lohmann, 1993; Mendlovic and Ozaktas, 1993; Lohmann *et al.*, 1998), so we can realize the CFWT. The optical implementation is proposed in Fig.2a.

In Fig.1, according to the relationship $f=f_s/\sin\varphi$, $z=f_s\tan(\varphi/2)$ and $\varphi=\pi p/2$, it is easy to find that if the fractional orders of FRFT and scaling factors of WT

are chosen, the optical system is determined and the image would be encrypted after it passes through the process. The fractional orders and scaling factors are two series of keys. Fig.2a also shows that if the image passes through the CFWT, the keys would be added easily. All the fractional orders p_1, p_2, …, p_n and scaling factors are its keys. So the security of the information is strengthened and unauthorized people cannot obtain the correct information easily. Only when all the fractional orders and scaling factors are known, could the image be well decrypted. The cascading condition is that all the stages of optical FRFTs have the same standard focal lengths (Liu *et al.*, 1995). Therefore the standard focal lengths can be regarded as the other keys in encryption.

The decryption process is given in Fig.2b. The encrypted image at first passes through an inverse WT and then the inverse FRFTs with p_n, …, p_2, p_1 orders. According to the additive property of FRFT, the correct image would be decrypted at the output plane. If the scaling factors of the inverse WT or fractional orders of the inverse FRFTs are not correct, the image will not be correctly decrypted. Even if the fractional orders are correct, if the standard focal lengths are incorrect, according to the relationship $f=f_s/\sin\varphi$, $z=f_s\tan(\varphi/2)$ and $\varphi=\pi p/2$, correct optical FRFTs cannot be obtained. The simulation results will be given in the following based on the foundation of the optical configuration.

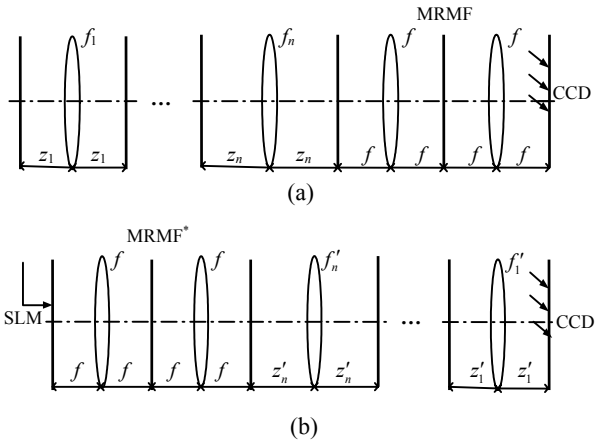

Fig.2 Optical realization of the encryption (a) and decryption (b) processes. SLM denotes spatial light modulator; CCD is the charge coupled device; MRMF is multireference matched filter; MRMF* is the conjugate of MRMF

COMPUTER SIMULATIONS

For simplicity, in the simulation we assume $p_1 = p_1' = 0.7048$, $p_2 = p_2' = -2.1144$, $f_s=f_{s1}=f_{s2}=300$ mm, $a_m=a_n$, $a_0=1$, $a_1=2$ and $a_2=4$, respectively. Haar wavelet function is the mother wavelet function. In fact, we can choose any fractional orders of FRFTs, scaling factors of WT and standard focal lengths.

In Fig.3a, the original image is a fingerprint with 296×296 pixels. Fig.3b is the encrypted result based on Eq.(1). We cannot find any characteristics of the original image in the encrypted picture, and the encryption effect is quite good. Based on Eq.(6) Figs.3c~3f show the decryption results. Fig.3c is the wrong decryption with incorrect fractional orders $p_1= p_1'=0.2000$, $p_2= p_2'=0.4000$ and incorrect scaling factors $a_0=2$, $a_1=4$ and $a_2=8$, so information on the image cannot be obtained. Fig.3d is the decryption result with wrong fractional orders but correct scaling

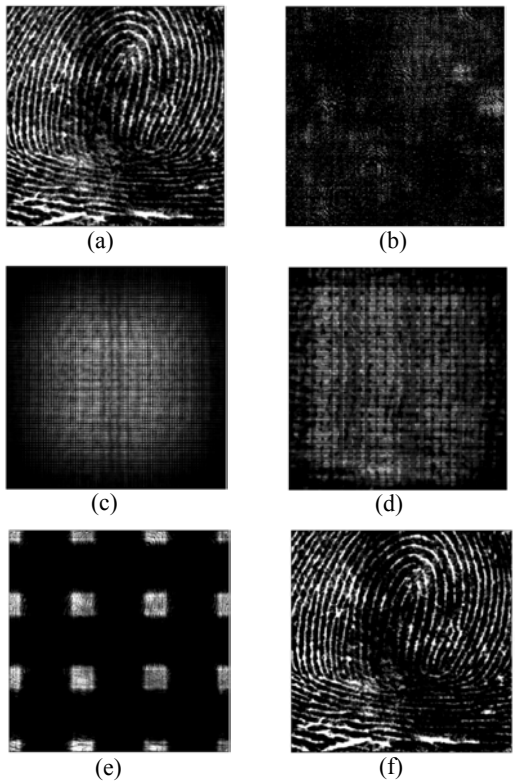

Fig.3 Computer simulations of encryption and decryption results. (a) Original input image (296×296); (b) Encryption results; (c) Incorrect decryption image; (d) Decryption image with incorrect fractional orders; (e) Decryption image with incorrect standard focal lengths; (f) Correct decryption result

factors, $p_1 = p_1' = 0.1000$, $p_2 = p_2' = 0.0410$. And Fig.3e is decryption image with incorrect standard focal lengths $f_s = f_{s1} = f_{s2} = 386$ mm, and shows that the correct standard focal lengths are also required in decryption even if the total fractional orders are correct. Fig.3f is the correct decryption result.

Fig.4 is total square error (TSE) of the decrypted image and original image versus the total fractional orders. It is defined as (Chen and Zhao, 2005)

$$TSE = \iint [f(x,y) - f_0(x,y)]^2 \mathrm{d}x\mathrm{d}y. \quad (8)$$

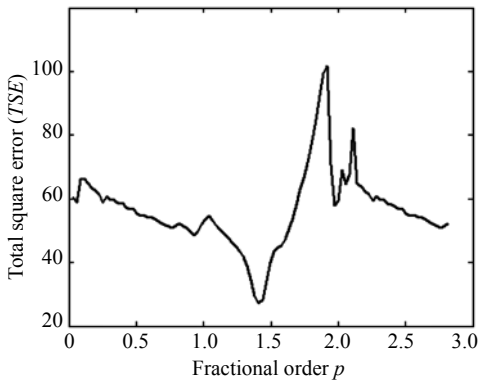

Fig.4 Total square error (TSE) of the decrypted image and original image versus total fractional order

In Fig.4, the x-axis denotes different total fractional order and y-axis denotes the value of *TSE* versus p. When $p = -(p_1 + p_2) = 1.4096$, it is noticed that *TSE* is minimal and the image is well decrypted. When the fractional order approaches the correct key, *TSE* is relatively small, and the reconstructed image will show some significant information on the original image. So when all the fractional orders in FRFTs are known, correct decryption would be realized. For an unauthorized person, even if he guesses the total fractional order by chance with combination of incorrect fractional orders p_1, p_2, …, p_n, without the correct standard focal lengths and scaling factors, he could not obtain the correct information. In fact, the fractional orders, standard focal lengths and scaling factors are randomly chosen, so it is impossible for unauthorized people to obtain correct information only by guess.

Generally, people often use WT to encrypt the image partially. Therefore when the fractional orders are correct, FWT can be used to encrypt the image partially (Chen and Zhao, 2005). In this paper it is noticed that CFWT can also be used to realize partial encryption. Fig.5 shows the partial encryption and decryption results. Fig.5a is the original image with 256×256 pixels. Fig.5b is the decryption result of losing some low frequency while Fig.5c is the result of losing some high frequency. And finally the decryption result with correct keys is given in Fig.5d.

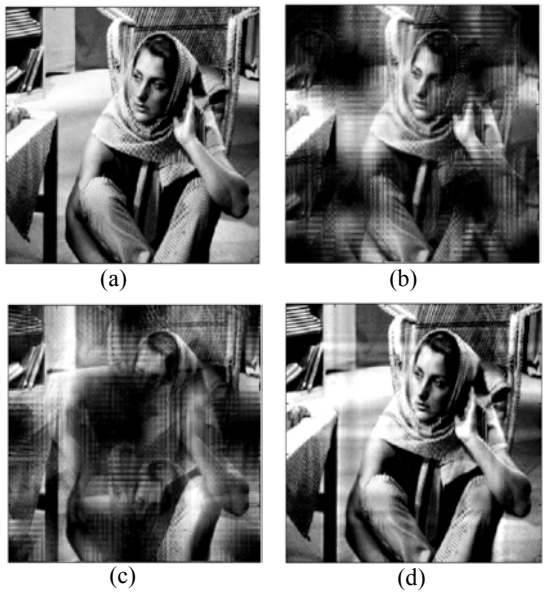

Fig.5 Computer simulations of partial encryption and decryption results. (a) Original input image (256×256); (b) Losing some low frequencies; (c) Losing some high frequencies; (d) Correct decryption image

CONCLUSION

In conclusion, we have proposed a new method named cascaded fractional wavelet transform (CFWT) to encrypt an image. Optical realization of encryption and decryption are proposed and some numerical simulations prove its reliability. This method has the virtues of both FRFT and WT. Fractional orders of FRFTs, scaling factors of WT and standard focal lengths are its keys and multistage transforms can add the keys easily. So the information is well secured. It can also realize partial encryption just as WT.

References

Chen, L.F., Zhao, D.M., 2005. Optical image encryption based on fractional wavelet transform. *Opt. Commun.*, **254**(4-6): 361-367. [doi:10.1016/j.optcom.2005.05.052]

Cheng, H., Li, X.B., 2000. Partial encryption of compressed images and videos. *IEEE Trans. Signal Process.*, **48**(8): 2439-2451. [doi:10.1109/78.852023]

Dang, P.P., Chau, P.M., 2000. Image encryption for secure Internet multimedia applications. *IEEE Trans. Consum. Electr.*, **46**(3):395-403. [doi:10.1109/30.883383]

Hennelly, B., Sheridan, J.T., 2003. Optical image encryption by random shifting in fractional Fourier domains. *Opt. Lett.*, **28**(4):269-271.

Javidi, B., Nomura, T., 2000. Securing information by use of digital holography. *Opt. Lett.*, **25**(1):28-30.

Liu, S.T., Wu, J., Li, C.F., 1995. Cascading the multiple stages of optical fractional Fourier transforms under different variable scales. *Opt. Lett.*, **20**(12):1415-1417.

Lohmann, A.W., 1993. Image rotation, Wigner rotation, and the fractional Fourier transform. *J. Opt. Soc. Am. A*, **10**(10):2181-2186.

Lohmann, A.W., Mendlovic, D., Zalevsky, Z., 1998. Fractional transformations in optics. *Prog. Opt.*, **38**:263-342.

Mendlovic, D., Konforti, N., 1993. Optical realization of the wavelet transform for two-dimensional objects. *Appl. Opt.*, **32**(32):6542-6546.

Mendlovic, D., Ozaktas, H.M., 1993. Fractional Fourier transforms and their optical implementation: I. *J. Opt. Soc. Am. A*, **10**(9):1875-1881.

Mendlovic, D., Zalevsky, Z., Mas, D., Garcia, J., Ferreira, C., 1997. Fractional wavelet transform. *Appl. Opt.*, **36**(20): 4801-4806.

Naulleau, P., 2001. A coherence encoding method for optical switching, encryption, and arithmetic. *Opt. Commun.*, **189**(1-3):55-61. [doi:10.1016/S0030-4018(01)00991-9]

Nishchal, N.K., Joseph, J., Singh, K., 2004. Securing information using fractional Fourier transform in digital holography. *Opt. Commun.*, **235**(4-6):253-259. [doi:10.1016/j.optcom.2004.02.052]

Tajahuerce, E., Lancis, J., Javidi, B., Andrés, P., 2001. Optical security and encryption with totally incoherent light. *Opt. Lett.*, **26**(10):678-680.

Unnikrishnan, G., Joseph, J., Singh, K., 2000a. Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt. Lett.*, **25**(12):887-889.

Unnikrishnan, G., Pohit, M., Singh, K., 2000b. A polarization encoded optical encryption system using ferroelectric spatial light modulator. *Opt. Commun.*, **185**(1-3):25-31. [doi:10.1016/S0030-4018(00)00977-9]