Mathematical description of the two-dimensional Gabor transform. Application to image encryption

Mathematical description of the two-dimensional Gabor transform. Application to image encryption

Ronal Perez[1], **Juan M. Vilardy**[1], **Cesar O. Torres**[2]

[1] Grupo GIFES. Faculty of engineering. Universidad de La Guajira, Riohacha (La Guajira), Colombia

[2] Grupo de óptica e informática. Department of electronic engineering. Universidad Popular del Cesar, Valledupar (Cesar), Colombia

E-mail: rperez@uniguajira.edu.co, jmvilardy@uniguajira.edu.co

Abstract. Information security with optical processing, such as the double random phase encoding and the Gabor transform (GT) has been investigated by various researchers. We present a two-dimensional (2-D) generalization of the one-dimensional GT. This 2-D GT is applied to encrypt digital images in this paper. The scaling factors of the GT can be used as new keys, providing a new encryption system with a high security characteristics. This method can encrypt and protect the information of the digital images with a high security for information processing systems.

1. Introduction

The Gabor transform (GT) has been used in texture segmentation [1-4] and defect detection [2]. The GT can be tuned to a specific frequency and orientation and achieve both localization in the time domain and frequency domain; two-dimensional (2-D) Gabor filters are multichannel filters with a multi-resolution decomposition process, which is similar to wavelet analysis. Time-frequency analysis, such as the GT, plays an important role in many signal processing applications [5-7].

In recent years, with the interests of people all around the world growing, optical image encryption techniques have shown great potential in the field of optical information processing, and various optical image encryption techniques have been proposed for optical image encryption by virtue of the arbitrary parameter selection, high computation speed, and extensive application. Some are done by Fourier transform (FT) [8-10], Fresnel transform (FrT) [11-13], or fractional Fourier transform (FrFT) [14-19], which is the generalization of the FT, and compared with it, the fractional orders are the additional key when the original image is encrypted. Since Réfrégier and Javidi proposed the double random phase encryption method in 1995 [8], the method has been effectively and extensively used. Nowadays, most of these above mentioned encryption systems often encrypt information with double random phase in the way of transforming the information into noise-like pictures, and only when the phase random keys and others system parameters are correctly used in decryption, will be recovered the original image. For instance, Situ and Zhang presented a novel encryption technique based on double random phase encoding in Fresnel domain by removing the lenses that are used in Fourier

domain [8]. Unnikrishnan et al. proposed double random phase encoding technique in the FrFT domain [14].

In this paper, we suggest a 2-D generalization of the 1-D GT. Like many well-known transforms, the GT also has a number of potential applications. The GT is better in comparison to the conventional FT with respect to the information processing [4]. It is possible that GT will become a useful information-processing tool in the future. Then, we propose a new encryption method based on the GT. Besides, the 2-D GT is a reversible transform analogous to FT. The use of the GT allows to increase the security of the encryption system due to the addition of new keys, these keys are represented by the scaling factors of the GT.

The outline of the paper is as follows: the mathematical description of the 2-D GT is introduced in section 2. The application of the 2-D GT for the digital images encryption and decryption processes are described in section 3. In section 4 are presented the computer simulations of the encryption and decryption methods based on the GT. Finally, the main ideas of the paper are summarized in section 5.

2. Definition of the Gabor transform (GT)

The one-dimensional (1-D) description of the GT is presented, most of the results of the 1D GT can be conveniently generalized to the case 2-D. The normalized 1-D Gabor filter is [4]

$$G_f(x_0,u)=\mathrm{GT}\{g(x)\}=\int_{-\infty}^{+\infty}\exp\left\{-\frac{(x-x_0)^2}{2}\right\}\exp\left\{-i2\pi u\left(x-\frac{x_0}{2}\right)\right\}g(x)\mathrm{d}x, \tag{1}$$

where u is the frequency coordinate and x_0 is a shift parameter in the spatial domain. The 1-D Fourier transform (FT) is

$$G(u)=\mathrm{F}\{g(x)\}=\int_{-\infty}^{+\infty}e^{-i2\pi ux}g(x)\mathrm{d}x. \tag{2}$$

2.1. 2-D GT

The 2-D is given by

$$\begin{aligned}G_f(x_0,y_0,u,v)=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}&\exp\left\{-\frac{(x-x_0)^2}{2}\right\}\exp\left\{-\frac{(y-y_0)^2}{2}\right\}\\&\times\exp\left\{-i2\pi u\left(x-\frac{x_0}{2}\right)\right\}\exp\left\{-i2\pi v\left(y-\frac{y_0}{2}\right)\right\}g(x,y)\mathrm{d}x\mathrm{d}y.\end{aligned} \tag{3}$$

The 1-D GT of equation (1) can be described by

$$G_f(x_0,u)=\mathrm{GT}\{g(x)\}=\int_{-\infty}^{+\infty}e^{-i2\pi ux}g_r(x)\mathrm{d}x, \tag{4}$$

where

$$g_r(x)=\exp\left\{-\frac{(x-x_0)^2}{2}\right\}\exp\{i\pi ux_0\}\,g(x). \tag{5}$$

Taking into account that

$$Gauss\left(\frac{x-x_0}{b}\right)=\exp\left\{-\pi\left(\frac{x-x_0}{b}\right)^2\right\}. \tag{6}$$

Scaling equation (5) with $x \to \sqrt{\pi}x$ and $x_0 \to \sqrt{\pi}x_0$, we get

$$g_r\left(\sqrt{\pi}x\right) = Gauss\left(\frac{x-x_0}{2}\right)\exp\left\{i\pi\sqrt{\pi}ux_0\right\}g\left(\sqrt{\pi}x\right). \tag{7}$$

Scaling equation (4) with $x \to \sqrt{\pi}x$, $x_0 \to \sqrt{\pi}x_0$ and $u \to \frac{u}{\sqrt{\pi}}$, we obtain

$$\begin{aligned} G_f\left(\sqrt{\pi}x_0, \frac{u}{\sqrt{\pi}}\right) &= \sqrt{\pi}\int_{-\infty}^{+\infty} e^{-i2\pi ux} g_r\left(\sqrt{\pi}x\right)\mathrm{d}x \\ &= \sqrt{\pi}\int_{-\infty}^{+\infty} e^{-i2\pi ux} Gauss\left(\frac{x-x_0}{2}\right)\exp\left\{i\pi ux_0\right\}g\left(\sqrt{\pi}x\right)\mathrm{d}x \\ &= \sqrt{\pi}\mathsf{F}\left\{Gauss\left(\frac{x-x_0}{2}\right)\exp\left\{i\pi ux_0\right\}g\left(\sqrt{\pi}x\right)\right\}. \end{aligned} \tag{8}$$

The Gabor transform can be considered as an inner product of the signal $g\left(\sqrt{\pi}x\right)$ and a shifted and modulated version of the analysis window.

Using the result of equation (8), the 2-D GT can be expressed as

$$\begin{aligned} G_f\left(\sqrt{\pi}x_0, \sqrt{\pi}y_0, \frac{u}{\sqrt{\pi}}, \frac{v}{\sqrt{\pi}}\right) = \pi\mathsf{F}\ \Big\{&Gauss\left(\frac{x-x_0}{2}\right)Gauss\left(\frac{y-y_0}{2}\right) \\ &\times\exp\left\{i\pi(ux_0+vy_0)\right\}g(\sqrt{\pi}x, \sqrt{\pi}y)\Big\}. \end{aligned} \tag{9}$$

This is a Fourier transform of a product of two functions. Furthermore, if we use the following scaling factors $x \to \frac{x}{a}$, $x_0 \to \frac{x_0}{a}$, $y \to \frac{y}{b}$, $y_0 \to \frac{y_0}{b}$ and coordinate inversions $u \to au$ and $v \to bv$ in previous equation, we obtain

$$\begin{aligned} G_f\left(\sqrt{\pi}\frac{x_0}{a}, \sqrt{\pi}\frac{y_0}{b}, \frac{au}{\sqrt{\pi}}, \frac{bv}{\sqrt{\pi}}\right) &= \pi\mathsf{F}\ \left\{Gauss\left(\frac{x-x_0}{2a}\right)Gauss\left(\frac{y-y_0}{2b}\right)\right. \\ &\quad\left.\times\exp\left\{i\pi(ux_0+vy_0)\right\}g\left(\sqrt{\pi}\frac{x}{a}, \sqrt{\pi}\frac{y}{b}\right)\right\} \\ &= \mathrm{GT}\left\{g\left(\sqrt{\pi}\frac{x}{a}, \sqrt{\pi}\frac{y}{b}\right)\right\}. \end{aligned} \tag{10}$$

The previous definition and implementation of the 2-D GT will be applied for the digital images encryption and decryption processes in the next section.

3. Mathematical formulation of the image encryption and decryption

The real image to encrypt is represented by $g\left(\sqrt{\pi}\frac{x}{a}, \sqrt{\pi}\frac{y}{b}\right)$. The image encryption uses the 2-D GT and two random phase masks (RPMs) [6], given by $P(x,y)$ and $Q(u,v)$. The implemented 2-D GT of the previous section introduces the scaling factor as new keys of the encryption system, this feature increases the security of the encryption system. The encrypted image is described by

$$e(s,t) = \mathrm{GT}\left\{Q(u,v)\mathrm{GT}\left\{P(x,y)g\left(\sqrt{\pi}\frac{x}{a},\sqrt{\pi}\frac{y}{b}\right)\right\}\right\}. \tag{11}$$

The decrypted image is given by

$$g\left(\sqrt{\pi}\frac{x}{a},\sqrt{\pi}\frac{y}{b}\right) = \left|\mathrm{GT}^{-1}\left\{Q^*(u,v)\mathrm{GT}^{-1}\left\{e(s,t)\right\}\right\}\right|, \tag{12}$$

where GT^{-1} represent the inverse GT and $Q^*(u,v)$ is the complex conjugate of $Q(u,v)$. The RPM $P(x,y)$ is used to spread the information content of the original image $g\left(\sqrt{\pi}\frac{x}{a},\sqrt{\pi}\frac{y}{b}\right)$ onto the encrypted distribution $e(s,t)$. The security keys of the encryption system are the RPM $Q(u,v)$ and the scaling factor a and b.

4. Computer simulation of the encryption and decryption techniques

The digital simulation for the encryption and decryption techniques was implemented on the platform of Matlab v.7.7, due to their facilities in handling matrices (images).

All image used in the computer simulations have 512 × 512 pixels. The encrypted images are grayscale images with 8 bits of quantization; the values of the pixels are integers between 0 and 255 (different shades of gray), the test image (original image) is depicted in figure 1.

After digitally implement the equations (10) and (11), using a digital algorithm for computing the discrete GT [20, 21], it was possible to encrypt the original image, obtaining an image with a completely random distribution, as shown in figures 1(a) and 1(b), the distribution of encrypted image (both its magnitude and phase) varies by changing the keys (the RPM $Q(u,v)$ and the scaling factor a and b).

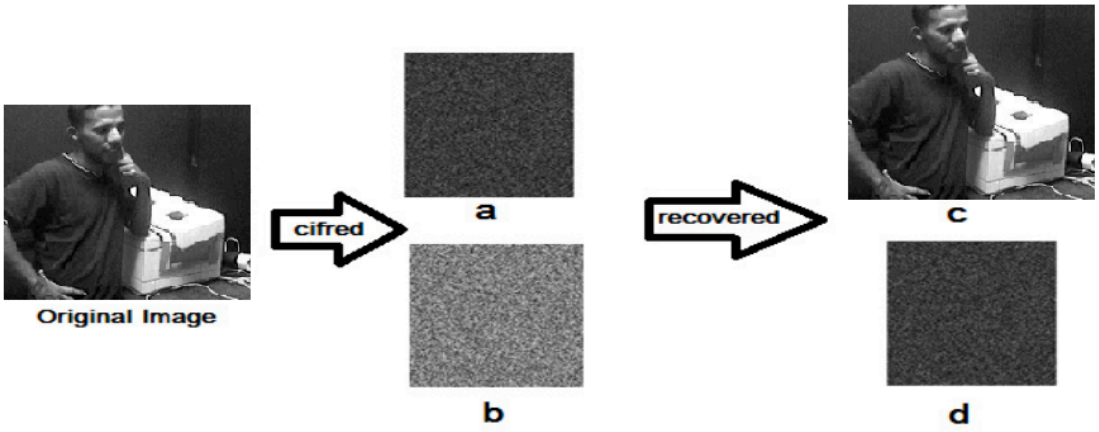

Figure 1. Digital simulation of the image encryption and decryption systems.

When performing the decryption process with the correct keys, we were able to recover the original image without any loss of information, as it is shown in fig. 1(c). If the keys used in the decryption process are not equal to the keys used in the encryption process, we obtain the random pattern image of the figure 1(d) at the output of the decryption system.

The RPM key $Q(u, v)$ have a size of 512×512 pixels and each pixel has 256 possible values. The number of attempts required to retrieve the RPM key $Q(u, v)$ image is of the order of $256^{(512)(512)}$. The possible values of the scaling factors a and b are considered between 0.5 and 1.5. The sensitivity to changes in values of the scaling factors is of the order of 1×10^{-6}. The total key space of the proposed

encryption process is $(1\times10^{12})\cdot256^{262144}$, this value for the key space is larger than the results obtained in refs. [10-19].

From numerical simulation, the time computing for obtaining the encrypted image with a size of 512×512 pixels is about 3.14 seconds and the time computing of the decrypted image is 2.92 seconds. These results of the time computing for the encryption and decryption processes are similar to the results presented in the encryption-decryption systems of the refs. [8-10, 11, 14-17].

5. Conclusions

We have described another mathematical expression for the 2-D GT. We have presented the relationship between the GT and the Fourier Transform; which makes possible a computational implementation of an images encryption-decryption system without loss of information in the retrieval of the original image. The 2-D GT was applied to the digital images encryption and decryption processes. A double random phase encoding based technique for image encryption using the GT and RPMs has been proposed. Digital simulations were presented to demonstrate the good performance of the presented encryption-decryption system. The scaling factors of the 2-D GT increased the security of the security system because these factors represent new keys. The three key of the encryption system (one RPM and two scaling factors) allow to obtain a very larger key space for the proposed security system.

Acknowledgments

This research has been funded by the Universidad de La Guajira and the Universidad Popular del Cesar.

References

[1] Okombi-Diba B, Miyamichi J and Shoji K 2000 *IAPR Workshop on machine vision applications* (*Tokyo*) pp 267–70
[2] Dunn D and Higgins W 1995 *IEEE Trans. Image Process.* **4** 947–64
[3] Lee T 1996 *IEEE Trans. On Pattern Analysis and Machine Intelligence* **18** 959–71
[4] Gabor D 1946 *J. IEE* **93** 429–59
[5] Movellan *J Tutorial on Gabor filters* (Open Source Document)
[6] Redondo R, Šroubek F, Fischer S and Cristóbal G 2009 *Information Fusion* **10** 163–71
[7] Soo-Hwan C, Gilsoo J and Sae-Hyuk K 2010 *IEEE Transactions on Power Delivery* **25** 494–9
[8] Réfrégier P and Javidi B 1995 *Opt. Lett.* **20** 767–9
[9] Nomura T and Javidi B 2000 *Opt. Eng.* **39** 2031–5
[10] Vilardy J, Millán M S and Pérez-Cabré E 2013 *J. Opt.* **15** 025401
[11] Situ G and Zhang J 2004 *Opt. Lett.* **29** 1584–6
[12] Vilardy J, Millán M S and Pérez-Cabré E 2014 *Appl. Opt.* **53**, 1674–82
[13] Vilardy J, Millán M S and Pérez-Cabré E 2013 *Proc. of SPIE* **8785**, 87853J
[14] Unnikrishnan G, Joseph J and Singh K 2000 *Opt. Lett.* **25** 887–9
[15] Vilardy J, Torres C and Mattos L 2008 *AIP Conf. Proc.* **992** 1067–72
[16] Vilardy J, Torres C and Mattos L 2008 *Revista Colombiana de Física* **40** 143–6
[17] Vilardy J, Torres C and Mattos L 2011 *Revista Colombiana de Física* **43** 523–7
[18] Vilardy J, Torres Y, Millán M S and Pérez-Cabré E 2014 *J. Opt.* **16** 125405
[19] Vilardy J, Millán M S and Pérez-Cabré E 2014 *Opt. Pura y Apl.* **47** 35–41
[20] Qian S and Chen D 1993 *IEEE Transactions on Signal Processing* **41** 2429–38
[21] Sondergaard P 2007 *Finite discrete Gabor analysis* (Academic dissertation: Ph.D thesis, Technical University of Denmark)