International Journal of Engineering and Techniques - Volume 2 Issue 4, July – Aug 2016

RESEARCH ARTICLE OPEN ACCESS

Hybrid Watermarking Technique Based on DWT-SVD-FRFT

Damanbir Singh[1], Guneet Kaur[2]
Department of Electronics and Communication, ACET, Punjab, India.

Abstract:
Digital watermarking has been proposed as a solution to the problem of copyright protection of multimedia documents in networked environments. There are two important issues that watermarking algorithms need to address. First, watermarking schemes are required to provide trustworthy evidence for protecting rightful ownership. Second, good watermarking schemes should satisfy the requirement of robustness and resist distortions due to common image manipulations (such as filtering, compression, etc.). In this paper, a watermarking algorithm is proposed based on the Discrete Wavelet Transform (DWT), Fractional Fourier Transform (FrFT) and Singular value decomposition (SVD). Analysis and experimental results show that the proposed watermarking method performs well in both security and robustness.

Introduction

The advent of the Internet and the wide availability of computers, scanners, and printers make digital data acquisition, exchange, and transmission quite simple tasks. However, making digital data accessible to others through networks also creates opportunities for malicious parties to make salable copies of copyrighted content without permission of the content owner. Digital watermarking techniques have been proposed in recent years as methods to protect the copyright of multimedia data [1]-[2].

In general, an effective watermarking scheme should satisfy the requirement that the perceptual difference between the watermarked and the original documents should be unnoticeable to the human observer, namely, watermarks should not interfere with the media being protected. A satisfactory watermarking scheme should also guarantee that it is impossible to generate counterfeit watermarks and should provide trustworthy evidence to protect the rightful ownership[3]. An unauthorized party should not be able to destroy the watermark without also making the document useless that is, watermarks should be robust to common signal processing and intentional attacks [4].

In order to advance the health and imperceptibility, a novel set in and removing process with DWT-SVD is proposed. The approximation matrix of the third level of image in DWT domain is modified with SVD to embed the singular value of watermark to the singular value of DWT coefficient [5]. In the scheme proposed by [6], the inscribed circle of the original image matrix is selected as the ZM calculation area, and the square of the inscribed circle is chosen to embed watermark. Firstly, the watermarking embedding area is conducted with 1-level DWT and the low frequency DWT coefficient is divided into non-overlapping blocks; SVD is applied to every block. Secondly, a bit of the watermark is embedded through slight modifications of the singular value (SV) matrix in each block. A novel feature is defined in [7] to assess the robustness of the visual watermarking method, which is a single method that can enhance watermarked data to objective image documents occupied with digital cameras without any unambiguous additional hardware construction. A delicate watermarking procedure is proposed for hologram verification in [8]. In this algorithm, the watermark is embedded in the transform domain. The noticeable hologram is kept in the spatial domain with the finite resolution level. The algorithm is based on Hadamard transform for both watermark embedding and extraction.

In this paper, a proposed watermarking technique is based on the combination of DWT, FrFT and SVD. The proposed method makes the image watermarking system more secure and robust. The advantages of our proposed methodology are the watermark is completely invisible in cover image as well as the encryption process is quite simple but robust in nature .The recovered watermark is about nearest the main watermark. Experimental results show that the proposed algorithm enhances the anti- attack capability and the hidden nature of the image, increases the security of the watermarking detection, and has maximum robustness to cutting, random noise attack and JPEG compression.

Scientific background

A. Discrete Wavelet Transform

The DWT has received considerable attention in various signal processing applications, including image watermarking. The main idea behind DWT results from multi resolution analysis [9], which involves decomposition of an image in frequency channels of constant bandwidth on a logarithmic scale. It has advantages such as similarity of data structure with respect to the resolution and available decomposition at any level. The DWT can be implemented as a multistage transformation. An image is decomposed into four subbands denoted LL, LH, HL, and HH at level 1 in the DWT domain, where LH, HL, and HH represent the finest scale wavelet coefficients and LL stands for the coarse-level coefficients. The LL subband can further be decomposed to obtain another level of decomposition. The decomposition process continues on the LL subband until the desired number of levels determined by the application is reached. Since human eyes are much more sensitive to the low-frequency part (the LL subband), the watermark can be embedded in the other three subbands to maintain better image quality.

B. Fractional Fourier Transform

There are several definitions for the Fractional Fourier Transform (FRFT) [10]. The first proposed one is the integral definition shown in the following formula (1).

$$X_p(u) = \int_{-\infty}^{+\infty} \tilde{K}_p(u,t)\,x(t)\,dt \qquad (1)$$

Here, the definition of the kernel function $\tilde{K}_p(u,t)$ can be shown as formula (2).

$$\tilde{K}_p(u,t) = A_a exp[j\pi(u^2 cota - 2utcsct\alpha + t^2 cot\alpha)] \qquad (2)$$

And the coefficient A_a is described as in the following formula (3).

$$A_a = \sqrt{1 - jcot\alpha}, \alpha = \frac{p\pi}{2}, p \neq 2n, n \in Z \qquad (3)$$

$$\begin{cases} \tilde{K}_p(u,t) = \delta(u-t), p = 4n(\alpha = 2n\pi) \\ \tilde{K}_p(u,t) = \delta(u+t), p = 4n \pm 2(\alpha = (2n \pm 1)\pi) \end{cases}$$

It is clear from the definition; the results of FRFT belong to a time-frequency mixing status which means there are both time information and frequency information in the transform domain.

B. SVD-Based Watermarking

From the perspective of image processing, an image can be viewed as a matrix with nonnegative scalar entries. The SVD of an image $A$with size $m \times m$is given by $A = USV^T$, where $U$and $V$are orthogonal matrices, and $S = diag(\lambda_i)$ is a diagonal matrix of singular values $\lambda_i, i = 1, \ldots, m,$

which are arranged in decreasing order. The columns of U are the left singular vectors, whereas the columns of V are the right singular vectors of image A. The basic idea behind the SVD-based watermarking techniques is to find the SVD of the cover image or each block of the cover image, and then modify the singular values to embed the watermark. There are two main properties to employ the SVD method in the digital-watermarking scheme. First is when a small perturbation is added to an image, large variation of its singular values does not occur. Secondly, singular values represent intrinsic algebraic image properties [11].

Methodology

A. Watermarking Embedding

The binary image is used as watermarks in our paper. 0 and 1 in the watermarks are represented as the two different random sequences respectively. The first random sequence will be embedded if the current position of the watermarking information is 0 and the other random sequence will be embedded if it is 1. In this way, 0/1 sequence is transformed into random sequences. During the embedding process, binary watermarking is firstly preprocessed by DWT and the obtained 0/1 sequence respectively corresponds to two different random sequences. Carrier image is divided into blocks. And each of them is transformed by using FrFT and then SVD is employed on this transform by considering the watermark image. After that IDWT is applied which results in the watermarked image.

B. Watermarking extracting

Extracting process is just the reverse of the embedding. Firstly, DWT is applied on the watermarked image and then coefficients are transformed by using FrFT technique. The approximation coefficient obtained holds the maximum information. Then SVD technique is applied which results in the extracted watermark image and host image.

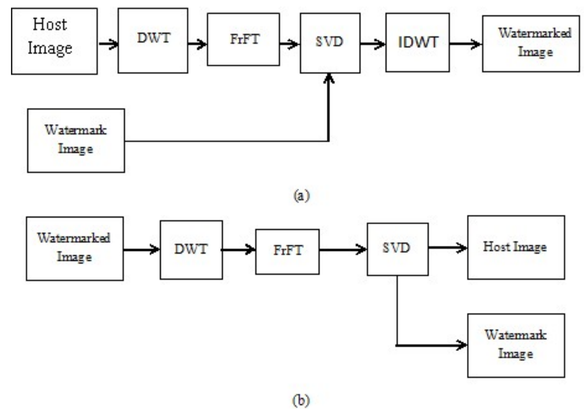


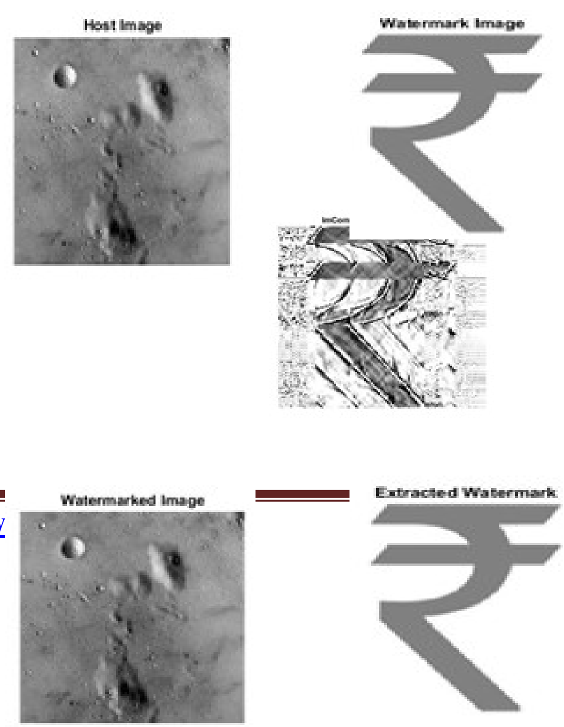
Fig. 1. (a) Watermark embedding process,

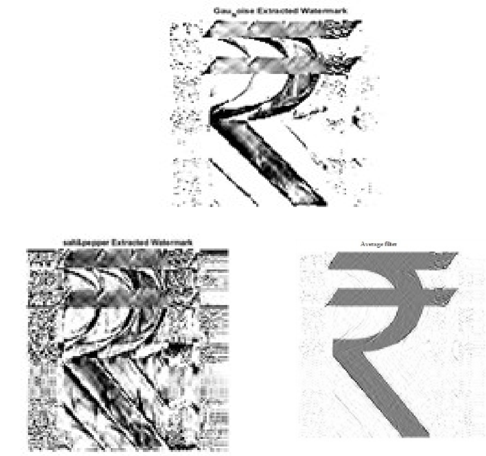
(b) Watermark extraction process

Experiment Results

The 256×256 pixels gray image is use as original image. The binary image with size 64×64 is used as the watermark image. To evaluate the distortion degree, PSNR value is use here. Let I to be the original image and I' is the watermarked image, the PSNR can be calculate as follows:

$$PSNR = 10log10\frac{MN\ \max[\max(I^2)]}{\sum_{i=1}^{i=M}\sum_{j=1}^{j=M}[I(i,j) - I'(i,j)]^2} \qquad (4)$$





(i)

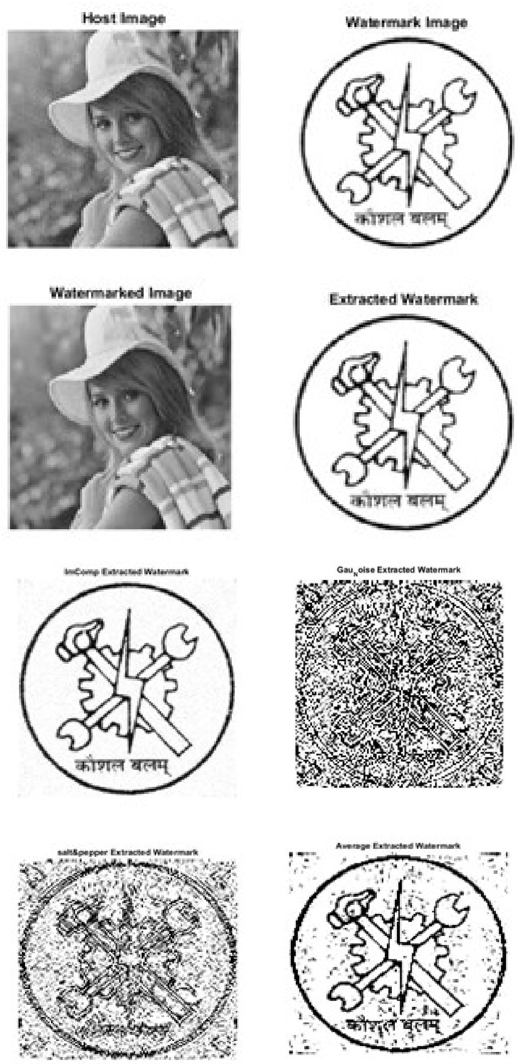


Fig. 2. DWT-FrFT-SVD in terms of visual quality of extracted watermarks from different watermarked images (i) and (ii) under different attacks like DCT compression, Gaussian noise, Salt & pepper noise.

The original input correlation coefficient is taken to be 1. Thus, in the overall process, the correlation of the pixels is hampered. The coefficients that are close to one can be considered the best one. The detailed study of the correlation coefficients can be carried out considering the results provided ahead.

Table 1. Extraction results under average filter attacks

Filter Size	Correlation Coefficient value for Planet Image	Correlation Coefficient value for Model Image
3x3	0.803209	0.832718
5x5	0.672058	0.680018
7x7	0.637155	0.621827

The algorithm is tested for three cases of filter size as shown in table 1. It can be observed that the technique performs well for the case when filter size is 3x3. Also, the technique performs well for average filtering as all the obtained correlation coefficients results are close to 1.

Table 2. Extraction results under Gaussian noise attacks

Gaussian Variance	Correlation Coefficient value for Planet Image	Correlation Coefficient value for Model Image
0.01	0.292355	0.284393
0.02	0.158995	0.176711
0.03	0.101369	0.146225
0.04	0.089288	0.077759
0.05	0.059626	0.082811
0.06	0.063164	0.069815
0.07	0.033546	0.081041
0.08	0.047091	0.063758
0.09	0.056399	0.090005

The proposed scheme performs well when the variance of Gaussian noise is very less. As the variance of the noise increases the extracted output correlation coefficient goes on decreasing. Also, the technique doesn't withstand itself against the Gaussian noise attack, as the correlation coefficient of the extracted watermark is very less when compared to the original input correlation coefficient.

Table 3. Extraction results under salt & pepper noise attacks

Noise density	Correlation Coefficient value for Planet Image	Correlation Coefficient value for Model Image
0.01	0.717994	0.734304
0.02	0.476781	0.524750
0.03	0.389986	0.426309
0.04	0.305726	0.373534
0.05	0.245445	0.318291
0.06	0.215994	0.257205
0.07	0.185694	0.273652
0.08	0.174088	0.251818
0.09	0.170451	0.218177

Similar to the Gaussian noise attack, the technique performs well when the noise density of the salt and pepper noise is very low as illustrated in table 3.

Table 4. Extraction results under image compression attacks

Compression Ratio	Correlation Coefficient value for Planet Image	Correlation Coefficient value for Model Image
25%	0.999941	0.999986
50%	0.997201	0.999055
75%	0.845826	0.891553

The proposed scheme performs exceptionally well for image compression, as the extracted output correlation coefficient is very close to one, as depicted in table 4. The watermark is pretty much preserved even when the image is compressed.

Table 5. PSNR of watermarked image

	Planet Image	Model Image
PSNR (dB)	40.773122	40.386799

If the watermarked images are tested on their quality factor, PSNR, it can be noted that the PSNR obtained is close to 40 dB, which is very much evident that the watermarked image is good in quality. Thus, in simple words, the watermark introduced in the image doesn't damage the original content of the image.

Table 6. Performance of different techniques in terms of PSNR on three different images

Technique \ Images	PSNR		
	Barbara	**Car**	**Lena**
DWT+FrFT+SVD	46.48	38.17	41.70
FrWT+SVD	38.28	36.87	37.46
FrFT+SVD	32.40	31.05	31.57
FrDCT+SVD	31.18	29.11	30.06

Table 7. Performance comparison of DWT+FrFT+SVD, FrWT and FrFT based algorithms in terms of correlation coefficient (ρ) between original and extracted watermark under various attacks (column 1) on Barbara watermarked image

Correlation coefficient (ρ) between original watermark and extracted watermark									
Techniques	DWT+FrFT+SVD			FrWT+SVD			FrFT+SVD		
Attacks	IEEE*	PU*	PP*	IEEE	PU	PP	IEEE	PU	PP
No attack	1	1	1	0.997	0.996	0.996	0.996	0.996	0.96
Average	0.382	0.414	0.590	0.330	0.276	0.265	0.414	0.359	0.318
Gaussian Noise	0.977	0.349	0.230	0.254	0.229	0.249	0.247	0.231	0.283
Salt & Pepper	0.829	0.716	0.619	0.620	0.572	0.572	0.493	0.464	0.482
DCT	0.912	0.994	0.999	0.759	0.721	0.716	0.557	0.509	0.474

Fig. 3 shows the visual comparison between embedded and extracted watermark from different images using proposed model. For watermark, gray scale logo of size $M/3 \times N/3$ namely, IEEE Logo, PU Logo and PP logo have been used. Table 6 shows the PSNR values obtained after watermarking different gray scale low intensity images using DWT-FrFT-SVD, FrWT+SVD, FrFT+SVD and FrDCT+SVD based watermarking method. The less value of PSNR implies that it introduces more error while embedding the watermark. It has also been observed that the PSNR of proposed method is above or equal 40 dB for all the selected low intensity images.

Table 7 illustrates the correlation coefficient between original and extracted watermark recovered after different attacks (like average filtering, median filtering, Gaussian noise of zero mean, salt and pepper noise and DCT compression) on watermarked image obtained using proposed watermarking scheme. From the results presented in Tables 6, 7, it is clear that the proposed watermarking scheme shows a performance better than FrFT and FrDCT based watermarking schemes in terms of PSNR and correlation coefficient. The Fig. 4 demonstrates the embedding and extracting results of DWT-FrFT-SVD on Barbara image under various attacks in comparison to FrWT and FrFT. For the comparison purpose IEEE, Punjab Police and Punjabi University logo are also used. The closer look on Fig. 4 reveals that DWT-FrFT-SVD retains the better visual quality of watermark even after attacks in comparison to FrWT and FrFT at transform order a_x=-0.5 along x direction and a_y=-0.28 along y direction. These values of transform order (both along x and y direction) have been obtained by using hit and trial method.

IEEE: IEEE Logo *PU: Punjabi University Logo *PP: Punjab Police Logo

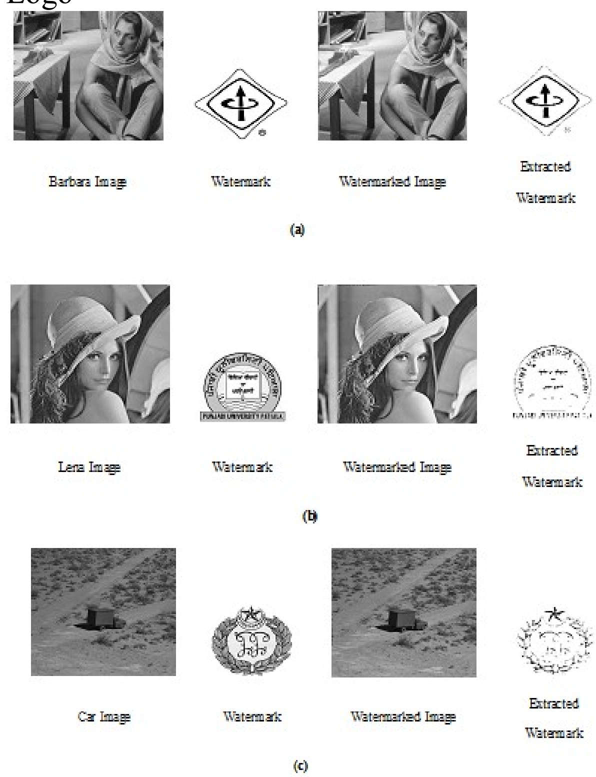
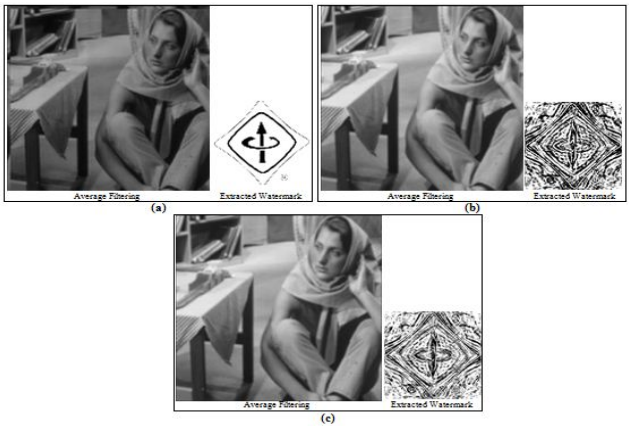
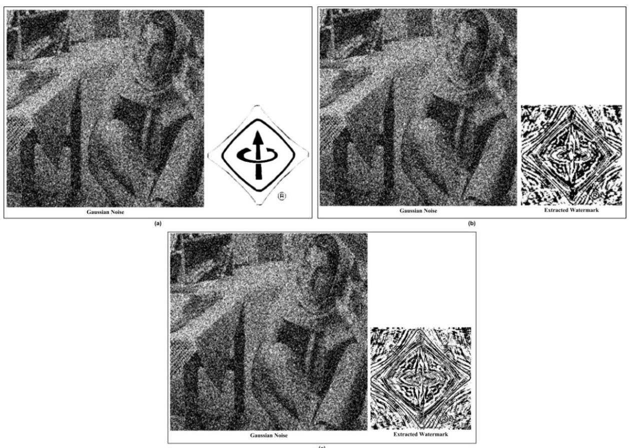


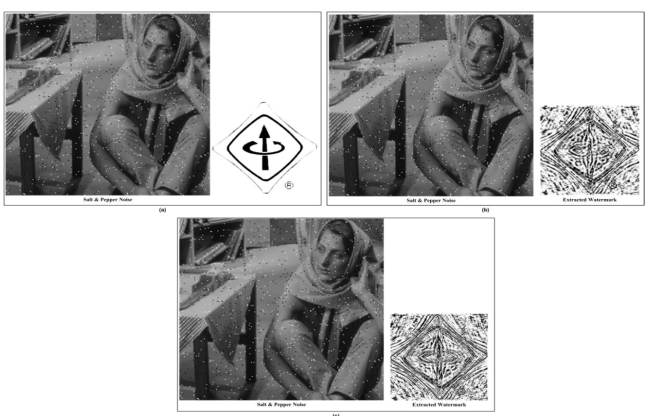
Fig. 3. Result of watermarking using DWT-FrFT-SVD scheme on (a) Barbara image, (b) Lena image, and (c) Car image with three different watermarks.



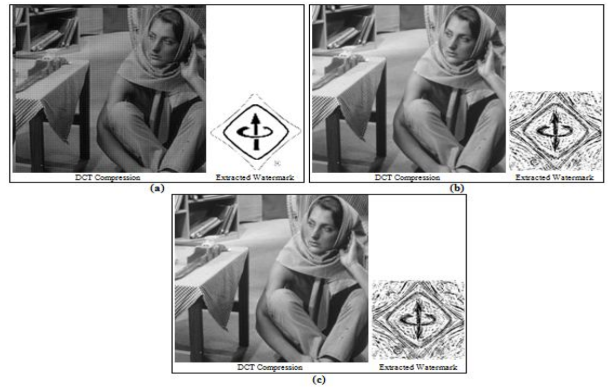
(i)



(ii)



(iii)



(iv)

Fig. 4. Comparison of (a) DWT-FrFT-SVD, (b) FrWT and (c) FrFT in terms of visual quality of extracted watermarks from Barbara watermarked image under different attacks like (i) Average filtering (ii) Gaussian noise (iii) Salt & pepper noise (vi) DCT compression.

Conclusion

The proposed watermarking scheme has satisfactory performance against various attacks such as average filter attacks, noise attacks and the compression attacks. The proposed watermarking scheme provides PSNR of above 40 dB which is better than the existing state of art approaches. Also, the proposed watermarking scheme shows a better performance as compare to FrFT and FrDCT based watermarking schemes in terms of correlation coefficient.

References

1. B. R. Macq and I. Pitas, "Special issue on water making," *Signal Process.*, vol. 66, no. 3, pp. 281–282, 1998.
2. M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data embedding and watermarking technologies," *Proc. IEEE*, vol. 86, pp. 1064–1087, June 1998.

3. J. Zhao, E. Koch, and C. Luo, “Digital watermarking in business today and tomorrow,” *Commun. ACM*, vol. 41, no. 7, pp. 67–72, 1998.
4. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” *IEEE Trans. Image Processing*, vol. 6, pp. 1673–1687, Dec. 1997.
5. Seema, Sheetal Sharma, “DWT-SVD Based Efficient Image Watermarking Algorithm to Achieve High Robustness and Perceptual Quality,” vol. 2, no. 4, (2012**),** April.
6. X. Ye, M. Deng, Y. Wang and J. Zhang, “A Robust DWT-SVD Blind Watermarking Algorithm based on Zernike Moments”, in Proc. Communications Security Conference, pp. 1-6, 2014.
7. Y. Ishikawa and K. Uehira,”Tolerance Evaluation for Defocused Images to Optical Watermarking Technique”, Journal of Display Technology, vol. 10, no. 2, (2014**)** February.
8. H.-T. Chan, W.-J. Hwang, and C.-J. Cheng, “Digital Hologram Authentication Using a Hadamard-Based Reversible Fragile Watermarking Algorithm,” Journal of Display Technology, vol. 11, no. 2, (2015**)** February.
9. S. Mallat, “The theory for multiresolution signal decomposition: The wavelet representation,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 11, no. 7, pp. 654–693, Jul. 1989.
10. L.B. Almeida, “The fractional Fourier transform and time-frequency representations,” IEEE Transaction on Signal Processing, 42, 1994, pp: 3084-3091.
11. R. Liu and T. Tan, “An SVD-based watermarking scheme for protecting rightful ownership,” *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002.