Signal Processing 92 (2012) 1480–1491

Contents lists available at SciVerse ScienceDirect

Signal Processing

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

A blind watermarking algorithm based on fractional Fourier transform and visual cryptography

Sanjay Rawat*, Balasubramanian Raman [1]

Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee 247667, India

ARTICLE INFO

Article history:
Received 21 February 2011
Received in revised form
20 October 2011
Accepted 5 December 2011
Available online 17 December 2011

Keywords:
Watermarking
Visual cryptography
Singular value decomposition
Fractional Fourier transform

ABSTRACT

This paper presents a robust copyright protection scheme based on fractional Fourier transform (FrFT) and visual cryptography (VC). Unlike the traditional schemes, in our scheme, the original image is not modified by embedding the watermark into the original image. We use the visual secret sharing scheme to construct two shares, namely, master share and ownership share. Features of the original image are extracted using SVD, and are used to generate the master share. Ownership share is generated with the help of secret image (watermark) and the master share, using VC technique. The two shares separately give no information about the secret image, but for ownership identification, the secret image can be revealed by stacking the master share and the ownership share. In order to achieve the robustness and security, the properties of VC, FrFT and SVD are used in our scheme. The experimental results show that the proposed scheme is strong enough to resist various signal processing operations.

1. Introduction

During the last decade, the availability of information in digital form has increased rapidly. The success of the internet, cost-effective recording and storage devices have made it possible to easily create, replicate, transmit, and distribute digital content. However, the information security, authentication of data and protection of intellectual property rights have also become an important issue. In such a scenario, a mechanism for copyright protection of multimedia data is essential. Digital watermarking is one of the popular mechanisms that have been widely used for the copyright protection of digital media. Digital watermarking is a technique for inserting information (the watermark) into the media, which can be detected and retrieved when necessary. On the basis of the information required during extraction process, watermarking schemes can be divided into three categories: non-blind watermarking, semi-blind watermarking, and blind watermarking. If the original host image is required to extract the embedded watermark, the scheme is non-blind. The practicality of the non-blind watermarking scheme is limited, since it needs extra storage to maintain the source image. Semi-blind watermarking scheme uses the watermark and/or some side information, instead of the host image to extract the embedded watermark. The blind watermark scheme does not require the host image or extra information to extract the watermark. Depending on the work domain in which the watermark is embedded, the watermarking schemes can be classified into two categories: spatial-domain watermarking schemes and transform-domain watermarking schemes. In spatial domain watermarking schemes, the watermark is embedded by directly modifying the pixel values of the image [1–3]. Transform domain watermarking schemes first apply transformation techniques, such as the discrete cosine transform (DCT) [4–6], discrete wavelet transform (DWT) [7–9], fractional

* Corresponding author. Tel./fax: +91 1332 285852.
E-mail addresses: sanjudma@gmail.com (S. Rawat), balaiitr@ieee.org (B. Raman).
[1] Tel.: +91 1332 285852.

0165-1684/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.sigpro.2011.12.006

Fourier transform (FrFT) [10–12] and singular value decomposition (SVD) [13–15] to an image. Watermark is then embedded by modifying the transform coefficients. These techniques show good robustness and security against various attacks as compared to spatial domain techniques.

In order to protect the security of a secret message, Naor and Shamir [16] proposed a lossless watermarking technique called visual cryptography (VC). The major advantage of this technique is that it does not modify the original image and decryption is done by human visual system. Many VC based watermarking schemes are proposed in the literature [17–21,23]. Wang et al. [17] proposed a VC based repeating watermarking scheme in spatial domain, that conceals a watermark by adding some parts of the watermark into the edge blocks of the host image. Their scheme is secure and robust against common attacks but the main drawback of the scheme is that host image is altered in order to embed the watermark. Hou et al. [18] used a modified VC scheme to split the watermark into two meaningless shares. The first share is embedded in some specific pixels of the host image by decreasing their gray level values. The watermark is revealed by superimposing the watermarked image and the second share. The method shows weak robustness against geometric attacks and also alters the host image during embedding process. Chang et al. [19] proposed a copyright protection scheme based on torus automorphism and VC. The scheme has the advantage that it does not modify the host image. However, the size of the watermark in their scheme is restricted by the size of the host image. Hsu et al. [20] proposed a copyright protection scheme based on sampling distribution of means and VC. Their scheme can register multiple secret images without altering the host image. In their scheme, the size of the watermark is not restricted by the size of the host image, i.e. binary image of any size can be used as a watermark. Lou et al. [21] proposed a copyright protection scheme based on discrete wavelet transform (DWT) and VC. They extracted the feature value of the host image by utilizing the secret key K and the relation between the low and middle sub-band wavelet coefficients. Then a secret image is generated with the help of watermark and the feature value. The scheme shows good robustness against various attacks. Later Chen et al. [22] analyzed the scheme proposed by Lou et al. [21], and claimed that the false alarm of their scheme is not negligible. They proved that the scheme is insecure since the verification watermark can be unreasonably extracted from other unprotected images using the identical secret key by the owner. Wang and Chen [23] proposed a hybrid DWT–SVD copyright protection scheme based on VC. In their scheme the host image is decomposed into subbands by two-level DWT and a list of pixel positions from the LL2 subband is randomly selected using pseudo-random number generator. Then, the SVD is performed on a small window centered at each selected pixel position, and some singular values of each window are used to create a feature vector. The feature vector is then classified into two clusters by k-means clustering. A master share is then generated based on the clustering result. Then an ownership share is constructed by using the master share and a secret image according to the VC technique. When a dispute over the ownership of the host image arises the hidden secret image can be revealed by stacking the generated master share and the ownership share. Their scheme is secure and robust against common signal processing attacks.

In this paper, a novel copyright protection scheme based on fractional Fourier transform (FrFT) and visual cryptography is proposed. The host image is divided into 4×4 non-overlapping blocks. A subimage is formed by selecting some blocks, using a pseudo-random number generator (PRNG) seeded with a private key. Features of the subimage are extracted by applying FrFT and SVD on the subimage. Next, a binary map is formed with the help of extracted image features. A master share is constructed by using the binary map. The ownership share is then constructed by using master share together with the secret image (watermark). Whenever there is a dispute over the rightful ownership of a suspected image, the secret image used for ownership identification can be revealed by stacking the master share and the ownership share.

The rest of the paper is organized as follows. In Section 2, a brief background about fractional Fourier transform, visual cryptography and singular value decomposition is provided. Details of the proposed scheme are given in Section 3. The experimental results are presented in Section 4. Finally, the conclusions are drawn in Section 5.

2. Background

In this section, the concepts of fractional Fourier transform, visual cryptography and singular value decomposition are briefly described.

2.1. Fractional Fourier transform

The fractional Fourier transform (FrFT) belongs to the class of time–frequency representations that have been extensively used by the signal processing community. The FrFT is a time–frequency distribution and is a generalized form of the classical Fourier transform. The conventional Fourier transform can be regarded as a $\pi/2$ rotation in the time–frequency plane, and the FrFT can be considered as a generalized form that corresponds to a rotation over some arbitrary angle α. The pth order FrFT of a signal is defined as [24]

$$F^p[f(x)] = \int_{-\infty}^{\infty} K_p(x,u) f(x)\, dx, \quad 0 \le |p| \le 2 \tag{1}$$

where $K_p(x,u)$ is the transform kernel of the FrFT and is given by

$$K_p(x,u) = \begin{cases} \sqrt{\dfrac{1-j\cot\alpha}{2\pi}} & \text{if } \alpha \text{ is not a multiple of } \pi \\ \quad \times \exp j\left(\dfrac{u^2+x^2}{2}\cot\alpha - xu\csc\alpha\right) & \\ \delta(u-x) & \text{if } \alpha \text{ is a multiple of } 2\pi \\ \delta(u+x) & \text{if } \alpha+\pi \text{ is a multiple of } 2\pi \end{cases} \tag{2}$$

where p is the order of FrFT, α is the rotation angle and the relation of p and α is $\alpha = p\pi/2$.

The inverse of an FrFT with an order p is the FrFT with order $-p$

$$f(x) = F^{-p}[F^{p}(f(x))] \tag{3}$$

Some of the important properties of FrFT, as summarized in [25] are defined as follows:

1. *Identity operator*: F^0 is the identity operator. The FrFT of order $p=0$ is the input signal itself. The FrFT of order $p=2\pi$ corresponds to the successive application of the ordinary Fourier transform four times and therefore also acts as the identity operator.

$$F^{0}[f(x)] = F^{2\pi}[f(x)] = f(x) \tag{4}$$

2. *Fourier transform operator*: $F^{\pi/2}$ is the Fourier transform operator. The FrFT of order $p=\pi/2$ gives the Fourier transform of the input signal.
3. *Successive applications of FrFT*: Successive applications of FrFT are equivalent to a single transform whose order is equal to the sum of the individual orders.

$$F^{\alpha}(F^{\beta}[f(x)]) = F^{\alpha+\beta}[f(x)] \tag{5}$$

4. *Inverse*: The FrFT of order $-p$ is the inverse of the FrFT of order p since

$$F^{-p}(F^{p}[f(x)]) = F^{-p+p}[f(x)] = F^{0}[f(x)] = f(x) \tag{6}$$

Several 2D unitary transforms have been used in signal processing, such as discrete cosine transform, discrete Walsh transform and so on. The (M,N)-point 2D unitary discrete transform is computed as

$$X(m,n) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} x(p,q)K(p,q,m,n) \tag{7}$$

where $K(p,q,m,n)$ is the 2D transform kernel. If $K = K_1 \otimes K_2$, then the transform kernel $K(p,q,m,n)$ is called separable, where $\otimes$ denotes the tensor product. For a 2D separable kernel, its 2D transform can be implemented by row-column computation. Since the 2D continuous FrFT transform kernel is separable, so the 2D discrete FrFT is also defined with a separable form. The forward and inverse 2D discrete fractional Fourier transform (2D-DFrFT) of the image signal are computed as [26]

$$F_{\alpha,\beta}(m,n) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} f(p,q)K_{\alpha,\beta}(p,q,m,n) \tag{8}$$

$$f_{\alpha,\beta}(p,q) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} F(m,n)K_{-\alpha,-\beta}(p,q,m,n) \tag{9}$$

where (α,β) is the order of 2D-DFrFT, and K_α, K_β are the 1D discrete fractional Fourier transform kernel.

2.2. Visual cryptography

In 1995, Naor and Shamir [16] proposed the concept of (k,n) visual secret sharing (VSS) scheme. This scheme splits an image into n different shares. The image can be retrieved with $k(k \le n)$ or more than k shares but any $k-1$ shares give absolutely no information about the image. Depending on the applications, there are many implementations of the (k,n) VSS scheme. The (n,n) VSS scheme is most secure and least convenient in key management. In this paper $(2,2)$ VSS scheme is used. A secret image with size $M \times N$ can be divided into two shares with size $2M \times 2N$ in which, every pixel of the image is represented by a block of 2×2 pixels. In the encryption process, every secret pixel is turned into two blocks, and each block belongs to the corresponding share image. At last, two share images are obtained. In the decryption process, two corresponding blocks of a pixel are stacked together to retrieve the secret pixel. Two share blocks of a white secret pixel are similar while share blocks of a black secret pixel are complementary. Table 1 shows the concept of $(2,2)$ VSS scheme. An example of the $(2,2)$ VSS scheme is shown in Fig. 1, where the share images are 2×2 times larger than the original secret image.

2.3. Singular value decomposition

The singular value decomposition (SVD) is one of the effective numerical analysis tools used to analyze matrices. A digital image can be viewed as a matrix of non-negative scalar entries. Let A be a digital image of order $m \times n$ where $m \le n$. SVD of A is the factorization of A into three matrices, U, S and V such that

$$A = U*S*V^{T} \tag{10}$$

Table 1
Concept of (2,2) VSS scheme.

Pixel color	White Pixel □	Black Pixel ■
Share 1		
Share 2		
Stacked Result		

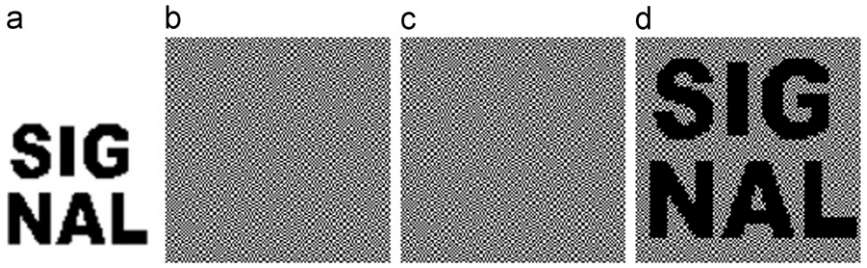

Fig. 1. An example of (2, 2) VSS scheme. (a) Original secret image. (b) First share image. (c) Second share image. (d) Stacked result of (b) and (c).

where U and V are orthogonal matrices and S is a diagonal matrix whose diagonal entries satisfy

$$\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \cdots \geq \lambda_r > \lambda_{r+1} = \cdots = \lambda_m = 0 \tag{11}$$

where r is the rank of A, which equals the number of non-zero singular values in S. The diagonal entries of S are non-negative square roots of the eigenvalues of AA^T or A^TA, and are called the *singular values* of A. Columns of U are eigenvectors of AA^T and are called the *left singular vectors* of A. Columns of V are eigenvectors of A^TA and are called the *right singular vectors* of A.

Each singular value in S specifies the luminance (energy) of the image while the corresponding pair of singular vectors in U and V represent, respectively, the horizontal and vertical details (edges) of the image. Slight variations of singular values does not affect the visual perception of the image.

A theoretical analysis of the effects of ordinary geometric distortions on singular values of an image was given by Zhou et al. [27]. They showed that singular values of an image are invariant to following geometric distortions:

- *Transpose invariance*: Matrix A and its transpose A^T have the same non-zero singular values.
- *Flip invariance*: Matrix A the row flip A_{rf} and the column flip A_{cf} have the same non-zero singular values.
- *Rotation invariance*: Matrix A and A_r (A rotated by an arbitrary angle) have the same non-zero singular values.
- *Scale invariance*: If we scale up A by L_1 times in row and by L_2 times in column, simultaneously, for every non-zero singular value λ of A, $\sqrt{L_1L_2}\lambda$ is a non-zero singular value of the scaled-up image. And the two images have the same number of non-zero singular values.
- *Translation invariance*: If A is expanded by adding rows and columns of black pixels, the resulting matrix A_e has the same non-zero singular values as A.

3. Proposed scheme

In this section, we explain the proposed copyright protection scheme in detail. The scheme consists of two phases: the ownership registration phase and the ownership identification phase. In the ownership registration phase, master share M will be generated from the host image. Then, the master share M is used together with the secret image S to generate the ownership share O.

3.1. Ownership registration phase

Let us consider, H is the host image of size $M \times N$ and the secret image S is a binary image of size $m \times n$.

3.1.1. Master share construction

Master share construction involves following steps:

1. Divide the host image H into 4×4 non-overlapping blocks.
2. Select $m \times n$ blocks, using pseudo-random number generator seeded with a secret key K.
3. Perform DFrFT with order α,β on all $m \times n$ blocks.
4. Perform SVD on all transformed blocks and generate a matrix X by collecting first singular value of each block.
5. Calculate the binary map B of the matrix X as

$$B_{i,j} = \begin{cases} 0 & \text{if } X_{ij} < X_{av} \\ 1 & \text{if } X_{ij} \geq X_{av} \end{cases}$$

   where X_{av} is the average value of all pixels in X. Here 1 denotes the white pixel and 0 denotes the black pixel.
6. Assume that M is a master share of size $2m \times 2n$ pixels. Divide the master share into non-overlapping 2×2 blocks and the content of each block is determined according to the following master share generation rule:

   If B_i is a white pixel then

$$m_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

   If B_i is a black pixel then

$$m_i = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

3.1.2. Ownership share construction

After generating master share M, we generate ownership share O with the help of master share M and binary secret image S. Assume that O is the ownership share of size $2m \times 2n$. Divide O into non-overlapping 2×2 blocks. Now ownership share is constructed according to the following rule:

$$\text{If } S_i = 1 \text{ and } m_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{then } o_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

If $S_i=1$ and $m_i=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ then $o_i=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$

If $S_i=0$ and $m_i=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ then $o_i=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$

If $S_i=0$ and $m_i=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ then $o_i=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$

The ownership share O should be registered with a certified authority (CA) for further authentication.

3.2. Ownership identification phase

Whenever there is a dispute over the rightful ownership of the host image H', ownership is identified as follows:

1. Divide the suspected image H' into 4×4 non-overlapping blocks.
2. Select $m\times n$ blocks, using pseudo-random number generator seeded with a secret key K.
3. Perform DFrFT with order α,β on all $m\times n$ blocks.
4. Perform SVD on all transformed blocks and generate a matrix X' by collecting first singular value of each block.
5. Calculate the binary map B' of the matrix X' as

$$B'_{i,j}=\begin{cases}0 & \text{if } X'_{ij}<X'_{av},\\ 1 & \text{if } X'_{ij}\geq X'_{av}\end{cases}$$

where X'_{av} is the average value of all pixels in X'.

6. Generate the master share M' according to the master share generation rule.
7. Retrieve the secret image S' by stacking the master share M' and the ownership share O kept by the CA.
8. Divide the secret image S' into non-overlapping 2×2 blocks. Let us denote these blocks by s'.
9. Get the reduced secret image S'' as

$$S''_{i,j}=\begin{cases}0 & \text{if } \sum_i\sum_j s'_{i,j}<2,\\ 1 & \text{if } \sum_i\sum_j s'_{i,j}\geq 2\end{cases}$$

4. Experimental results and discussions

4.1. Experimental results

Various experiments are carried out in this section, to assess the performance of the proposed algorithm. Six gray scale images, "Lena", "Airplane", "Peppers", "Boats", "Payaso" and "Goldhill" of size 512×512 are used as host images. A binary logo of size 64×64 is used as secret image. The transform orders of FrFT are taken as $\alpha=3/2$ and $\beta=-1/2$. All the test images and secret image are shown in Fig. 2. Master share generated from the original image is shown in Fig. 3(a), the corresponding ownership share is shown in Fig. 3(b). Stacked result of Fig. 3(a) and

Fig. 2. Test images and secret image.

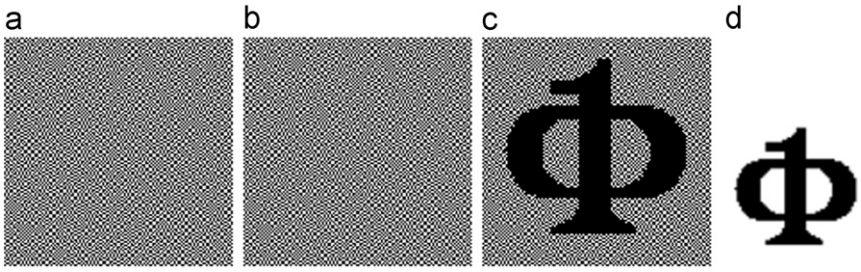

Fig. 3. (a) Master share. (b) Ownership share. (c) Stacked image. (d) Reduced secret image.

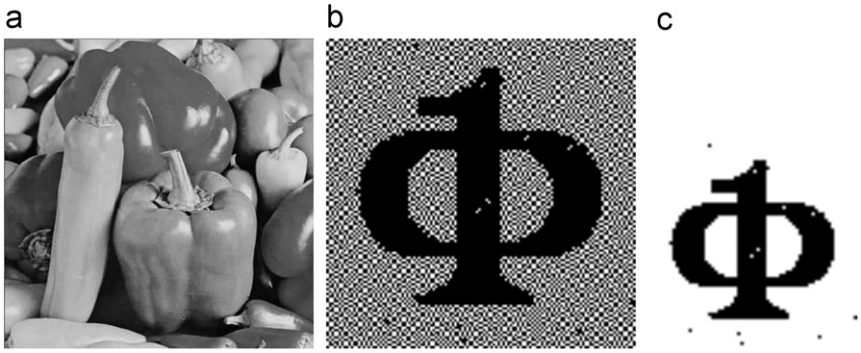

Fig. 4. (a) Image after JPEG compression (PSNR=33.5365). (b) Extracted secret image. (c) Reduced secret image (NC=0.9978).

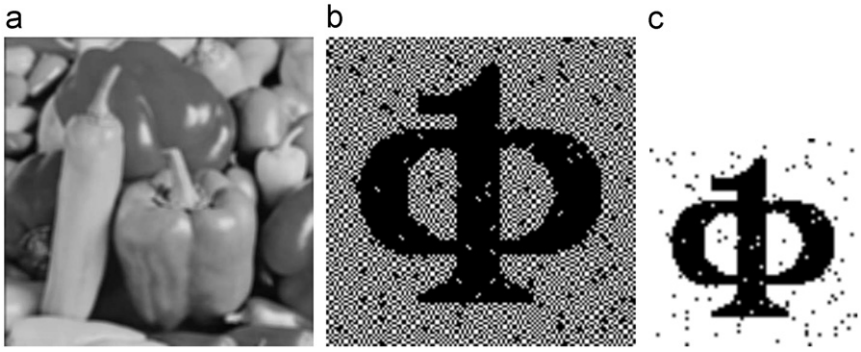

Fig. 5. (a) Average filtered image (PSNR=24.7970). (b) Extracted secret image. (c) Reduced secret image (NC=0.9798).

(b) is shown in Fig. 3(c) and the reduced secret image is shown in Fig. 3(d). Peak signal-to-noise ratio (PSNR) is used in this paper to analyze the visual quality of the watermarked image $\widehat{H}$ in comparison with the original image H. PSNR is defined as

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)\text{dB} \tag{12}$$

where MSE is the mean squared error between the original image H and the attacked image $\widehat{H}$, given by

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[H(i,j)-\widehat{H}(i,j)]^2 \tag{13}$$

The higher the PSNR value is, less distortion is there to the host image. Normalized correlation (NC) is used to measure the similarity between the extracted logo and the original logo. It is defined as

$$NC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\overline{S_{i,j}\oplus S''_{i,j}}}{m\times n} \tag{14}$$

where $S_{i,j}$ and $S''_{i,j}$ represents the original and extracted secret images respectively, $\oplus$ denotes the exclusive-or (XOR) operation and $m\times n$ is image size.

In the following experiments, the robustness of the proposed scheme is estimated by performing several image processing attacks, including JPEG compression, filtering, blurring, sharpening, noise addition, contrast adjustment, gamma correction, histogram equalization, resizing, rotation and distortion. All attack simulations were made using Matlab platform. Figs. 4–15 shows the

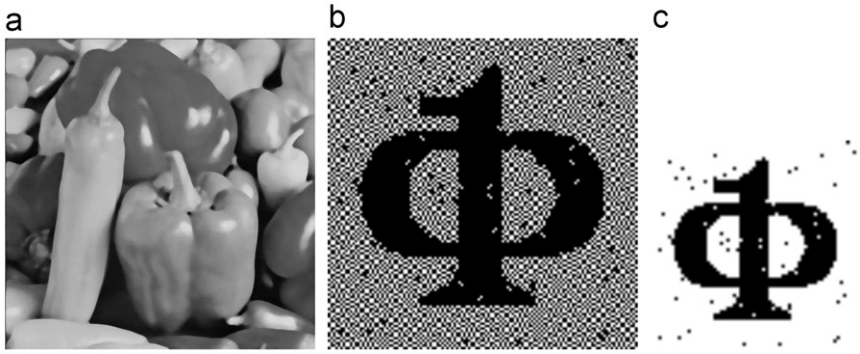

Fig. 6. (a) Median filtered image (PSNR=27.9817). (b) Extracted secret image. (c) Reduced secret image (NC=0.9890).

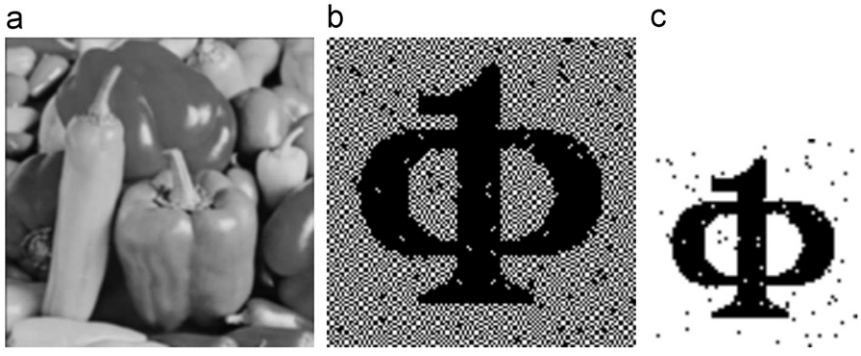

Fig. 7. (a) Blurred image (PSNR=26.1951). (b) Extracted secret image. (c) Reduced secret image (NC=0.9858).

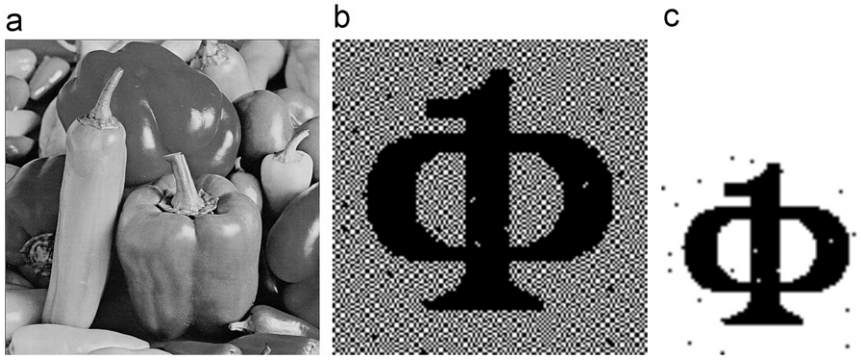

Fig. 8. (a) Sharpened image (PSNR=31.6187). (b) Extracted secret image. (c) Reduced secret image (NC=0.9963).

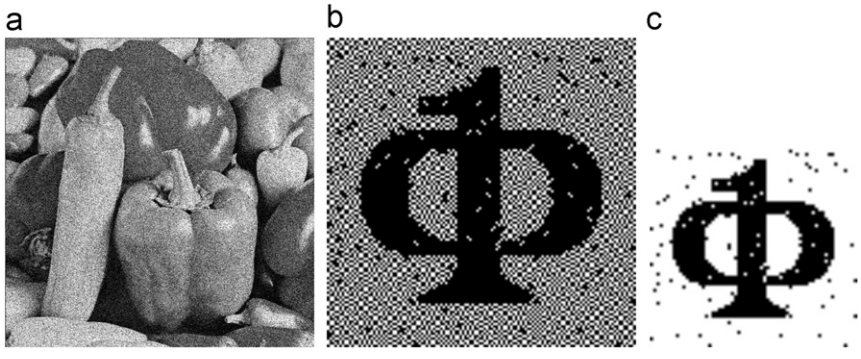

Fig. 9. (a) Image after noise addition (PSNR=16.6995). (b) Extracted secret image. (c) Reduced secret image (NC=0.9830).

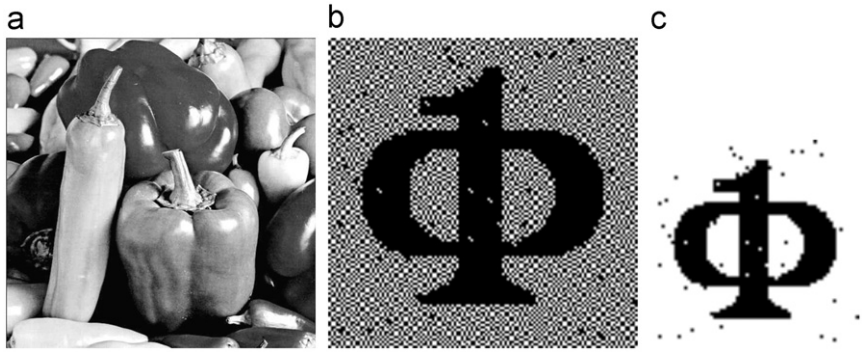

Fig. 10. (a) Image after contrast enhancement (PSNR=19.2179). (b) Extracted secret image. (c) Reduced secret image (NC=0.9929).

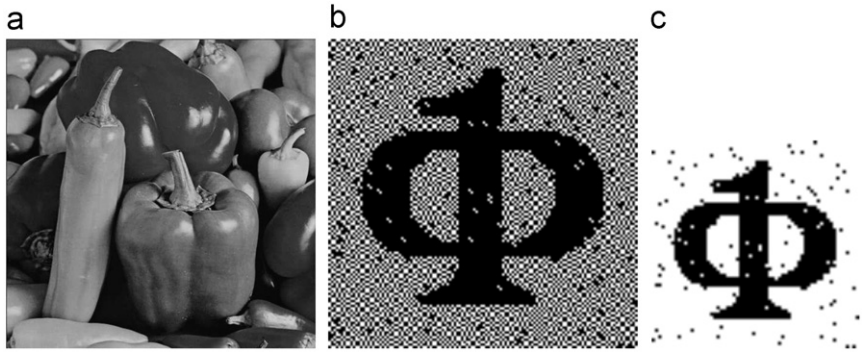

Fig. 11. (a) Image after Gamma correction (PSNR=15.0547). (b) Extracted secret image. (c) Reduced secret image (NC=0.9816).

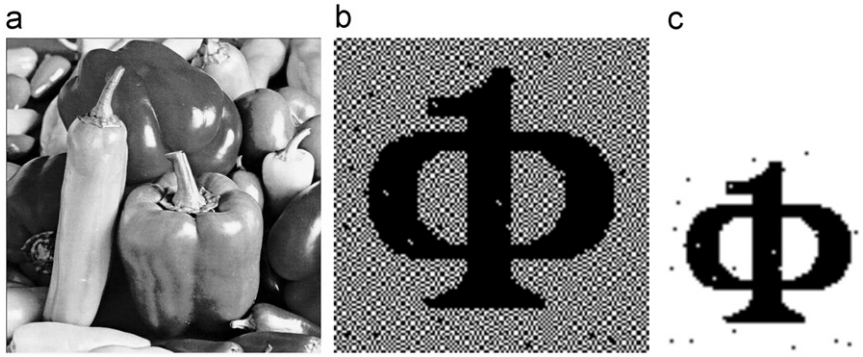

Fig. 12. (a) Image after histogram equalization (PSNR=20.9588). (b) Extracted secret image. (c) Reduced secret image (NC=0.9961).

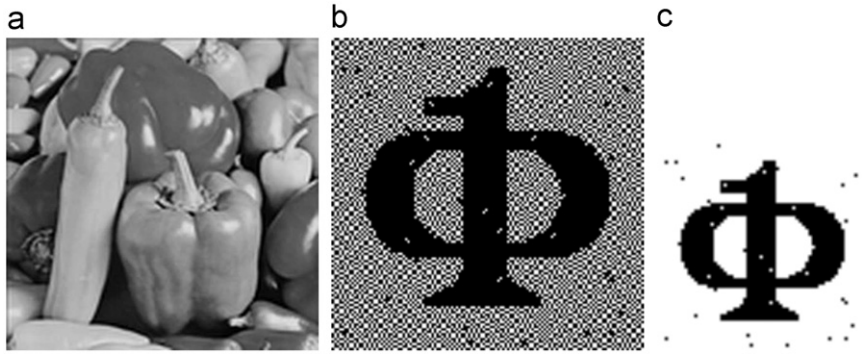

Fig. 13. (a) Image after resizing (PSNR=27.6880). (b) Extracted secret image. (c) Reduced secret image (NC=0.9944).

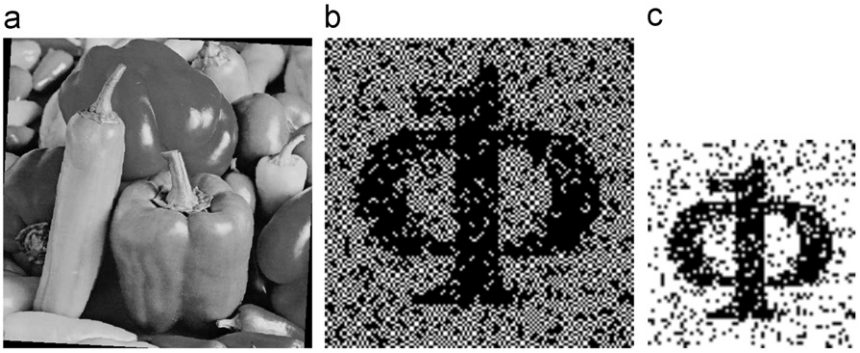

Fig. 14. (a) Rotated image (PSNR = 14.2895). (b) Extracted secret image. (c) Reduced secret image (NC = 0.8906).

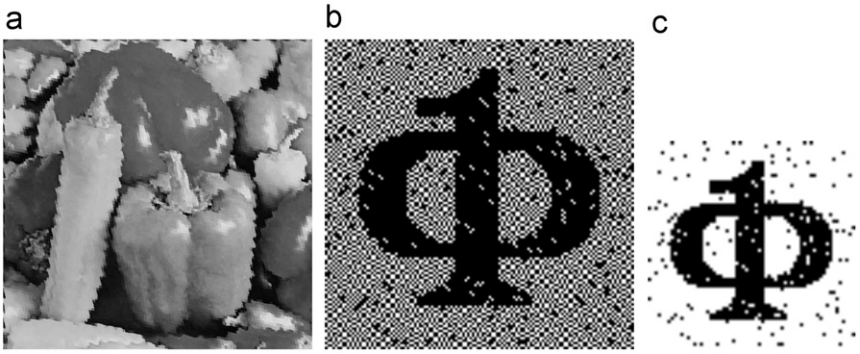

Fig. 15. (a) Distorted image (PSNR = 19.2116). (b) Extracted secret image. (c) Reduced secret image (NC = 0.9886).

results obtained by performing the proposed scheme on the "Peppers" image. The attacks are described as follows:

JPEG compression: We compressed the image by JPEG with quality factor 50%. The PSNR of the compressed image is 33.5365 dB. The NC of the extracted logo from the compressed image is 0.9978.

Filtering: We tested our image by applying average filter and median filter with 9×9 window. The PSNR of the average filtered image is 24.7970 dB and NC of the extracted logo is 0.9798. The PSNR of the median filtered image is 27.9817 dB and NC of the extracted logo is 0.9890.

Blurring: The blurred image is obtained by applying Gaussian blur with 9×9 window. The image quality of the blurred image is 26.1951 dB and NC of the extracted logo is 0.9858.

Image sharpening: We increased the sharpness of the image by 50%. The PSNR of the sharpened image is 31.6187 dB and the NC of the extracted logo is 0.9963.

Noise addition: A noisy image is obtained by adding 30% Gaussian noise to the original image. The PSNR of the noisy image is 16.6995 dB and the NC of the extracted logo is 0.9830.

Contrast enhancement: The contrast of the original image is increased by 50%. The PSNR of the image is reduced to 19.2179 dB and the NC of the extracted logo is 0.9929.

Gamma correction: The gamma value of the original image is reduced to 0.6. The PSNR of the image is reduced to 15.0547 dB and the NC of the extracted logo is 0.9816.

Histogram equalization: The PSNR of the image after histogram equalization is 20.9588 dB and the NC of the logo extracted from the image is 0.9961.

Resizing: We first downscaled the image from 512×512 to 128×128 pixels and then upscaled the image again to the original size. The quality of the image is reduced to 27.6880 dB and the NC of the extracted logo is 0.9944.

Rotation: The image is rotated by 3°. The PSNR of the rotated image is 14.2895 dB and the NC of the extracted logo is 0.8906.

Distortion: The image is distorted using ripple effect. The PSNR of the distorted image is 19.2116 dB and the NC of the extracted logo is 0.9886.

Detailed evaluation results for all images are summarized in Tables 2 and 3. We can see from the tables that NC values of all the extracted secret images are close to 1, which shows that the proposed scheme is extremely robust against various image processing attacks. To demonstrate the effectiveness of the proposed scheme, a comparison of the proposed scheme with two other visual cryptography based watermarking schemes, is summarized in Table 4. From the table we can see that our scheme has higher NC values for all the attacks, when compared with Hsu et al. scheme. When compared with Wang et al. scheme we see that for JPEG compression, median filtering and noise addition attack, NC value in our scheme is less than Wang et al. scheme. For rest of the attacks we are having higher NC values. Hence we can conclude that our scheme is

Table 2
Results of the proposed scheme under different attacks.

Image attacks	Lena		Airplane		Peppers	
	PSNR	NC	PSNR	NC	PSNR	NC
JPEG compression	34.9623	0.9934	36.8212	0.9968	33.5365	0.9978
Average filtering	25.8328	0.9779	23.9523	0.9724	24.7970	0.9798
Median filtering	27.5152	0.9837	25.1933	0.9813	27.9817	0.9890
Blurring	27.1754	0.9830	25.6286	0.9785	26.1951	0.9858
Sharpening	32.7046	0.9948	33.6064	0.9949	31.6187	0.9963
Gaussian noise addition	16.5798	0.9586	15.9835	0.9649	16.6995	0.9830
Contrast adjustment	19.0081	0.9956	16.4888	0.9943	19.2179	0.9929
Gamma correction	15.4385	0.9617	16.6915	0.9878	15.0547	0.9816
Histogram equalization	19.4699	0.9726	12.0623	0.8650	20.9588	0.9961
Resizing	29.1509	0.9919	28.8822	0.9919	27.6880	0.9944
Rotation	15.7998	0.8868	13.6072	0.8905	14.2895	0.8906
Distortion	20.6368	0.9786	19.9525	0.9789	19.2116	0.9886

Table 3
Results of the proposed scheme under different attacks.

Image attacks	Boats		Payaso		Goldhill	
	PSNR	NC	PSNR	NC	PSNR	NC
JPEG compression	35.1390	0.9963	35.6383	0.9959	32.2942	0.9914
Average filtering	23.8834	0.9709	23.6545	0.9760	24.9795	0.9592
Median filtering	24.7791	0.9710	24.7623	0.9793	25.6226	0.9606
Blurring	25.4609	0.9769	25.2699	0.9805	26.1348	0.9692
Sharpening	32.6478	0.9932	32.4999	0.9934	20.8770	0.9642
Gaussian noise addition	16.5026	0.9682	17.5410	0.9866	16.9385	0.9449
Contrast adjustment	21.2778	0.9844	17.9551	0.9866	19.1346	0.9966
Gamma correction	14.3176	0.9696	16.9850	0.9636	15.1027	0.9511
Histogram equalization	17.0615	0.8892	18.0117	0.9566	17.7883	0.9631
Resizing	27.8478	0.9868	27.0648	0.9898	27.2292	0.9861
Rotation	14.7746	0.8890	15.6059	0.9084	15.9263	0.8603
Distortion	20.9390	0.9609	19.8614	0.9629	22.2134	0.9569

Table 4
Comparison results of the proposed scheme with existing schemes.

Attacks	Hsu et al. scheme [20]	Wang et al. scheme [23]	Proposed scheme
JPEG compression	0.956	0.997	0.991
Median filtering	0.938	0.987	0.984
Blurring	0.918	0.989	0.992
Sharpening	0.819	0.985	0.995
Noise addition	0.761	0.989	0.959
Resizing	0.887	0.984	0.988
Distortion	0.838	0.985	0.989

robust against all the attacks and performs better than the existing schemes for most of the attacks.

4.2. Discussions

Robustness and security are two most important properties that a watermarking scheme should hold. Our scheme is robust, as after all the attacks the extracted watermarks are visually recognizable and all the extracted watermarks are very close to the original watermark. The minimum NC value of the extracted watermark in our experiment is 0.8603, which is still a high retrieved ratio, as many watermarking schemes in the existing literature are vulnerable to geometric attacks such as rotation and resizing attacks. The security of our scheme is ensured by using FrFT. The transform orders, α and β of FrFT, are used as keys in our scheme. The FrFT is sensitive to its transform orders as without knowing the correct transform orders nobody can extract the correct watermark. The key sensitivity of FrFT can be defined in two aspects. One is change in the transformed coefficients of the image due to change in the keys, i.e. if we apply FrFT on an image with different transform orders, the coefficients of all the transformed images will be different from each other. Fig. 16(b)–(f) shows the transformed images with different transform orders. If we check the intensity values of the transformed images, we see that almost 100% values are different when different keys are used. Second aspect is that if we apply inverse FrFT on the transformed image with wrong transform orders then the inverse transformed image is not recognizable. Fig. 17(c) shows the result when Fig. 17(b) is inverse transformed using correct keys. Fig. 17(d)–(f) shows the results when Fig. 17(b) is inverse transformed using incorrect keys. Hence

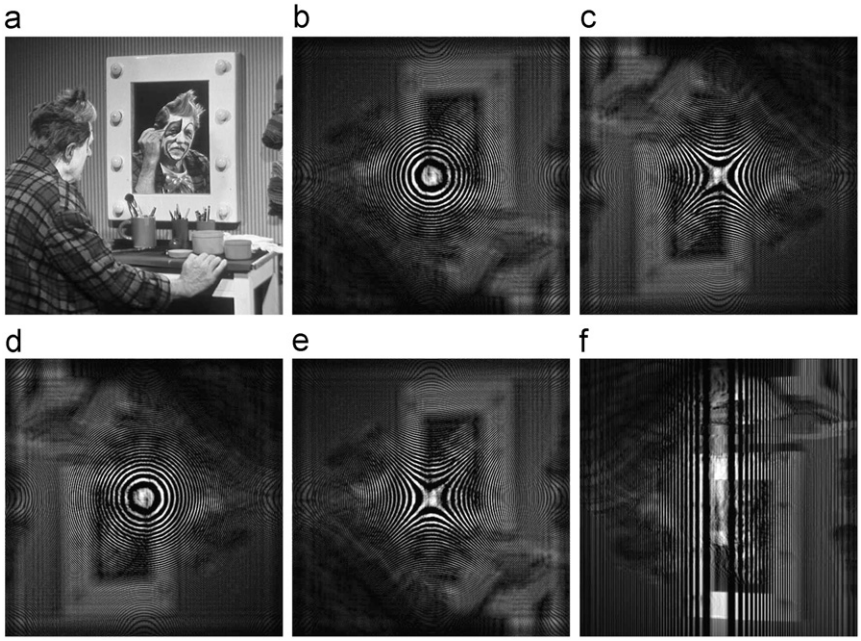

Fig. 16. (a) Original payaso image. (b) FrFT with order (1/2,1/2). (c) FrFT with order (3/2,5/2). (d) FrFT with order ($-3/2$,5/2). (e) FrFT with order ($-1/2$,1/2). (f) FrFT with order ($-1/2$,4/2).

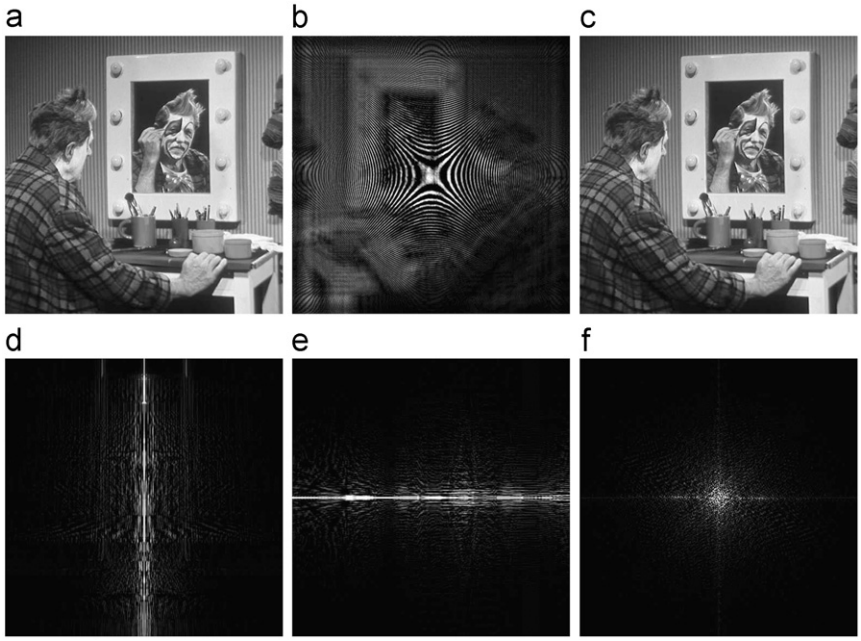

Fig. 17. (a) Original payaso image. (b) FrFT with order (3/2,1/2). (c) Inverse FrFT with order (3/2,1/2). (d) Inverse FrFT with order ($-3/2$,1/2). (e) Inverse FrFT with order ($3/2,-1/2$). (f) Inverse FrFT with order ($-3/2,-1/2$).

it is clear that FrFT is sensitive to its transform orders and it provides good security to our scheme.

5. Conclusion

In this paper, a watermarking scheme based on fractional Fourier transform (FrFT) and visual cryptography (VC) is proposed. The robustness of the scheme is tested by performing various image processing attacks. The extracted secret image is visually recognizable after all attacks which proves the robustness of the scheme. An important feature of the proposed scheme is that it is based on VC, which can recover the secret image with human eyes without the aid of computers. The transform orders of the FrFT are used as

keys in the algorithm, which gives more security to the algorithm, as without knowing the correct keys no attacker can extract the correct data. The experimental results show that the proposed scheme outperforms the two existing VC based watermarking schemes in most of the cases.

References

[1] R. Ni, Q. Ruan, Y. Zhao, Pinpoint authentication watermarking based on a chaotic system, Forensic Science International 179 (2008) 54–62.
[2] C. Deng, X. Gao, X. Li, D. Tao, Local histogram based geometric invariant image watermarking, Signal Processing 90 (2010) 3256–3264.
[3] O. Findik, I. Babaoglu, E. Ulker, A color image watermarking scheme based on hybrid classification method: particle swarm optimization and k-nearest neighbor algorithm, Optics Communications 283 (2010) 4916–4922.
[4] F. Huang, Z.H. Guan, A hybrid SVD-DCT watermarking method based on LPSNR, Pattern Recognition Letters 25 (2004) 1769–1775.
[5] J.C. Patra, J.E. Phua, C. Bornand, A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression, Digital Signal Processing 20 (2010) 1597–1611.
[6] S.D. Lin, S.C. Shie, J.Y. Guo, Improving the robustness of DCT-based image watermarking against JPEG compression, Computer Standards & Interfaces 32 (2010) 54–60.
[7] D. Kundur, D. Hatzinakos, Towards robust logo watermarking using multiresolution image fusion, IEEE Transactions on Multimedia 6 (2004) 185–197.
[8] W.H. Lin, Y.R. Wang, S.J. Horng, A wavelet-tree-based watermarking method using distance vector of binary cluster, Expert Systems with Applications 36 (2009) 9869–9878.
[9] H.M. Al-Otum, N.A. Samara, A robust blind color image watermarking based on wavelet-tree bit host difference selection, Signal Processing 90 (2010) 2498–2512.
[10] N.K. Nishchal, Optical image watermarking using fractional Fourier transform, Journal of Optics 38 (1) (2009) 22–28.
[11] D. Cui, Dual digital watermarking algorithm for image based on fractional Fourier transform, in: Proceedings of Second Pacific–Asia Conference on Web Mining and Web Based Applications, Wuhan, 2009, pp. 51–54.
[12] M.A. Savelonas, S. Chountasis, Noise-resistant watermarking in the fractional Fourier domain utilizing moment-based image representation, Signal Processing 90 (2010) 2521–2528.
[13] E. Ganic, A.M. Eskicioglu, Robust embedding of visual watermarks using DWT-SVD, Journal of Electronic Imaging 14 (4) (2005) 043004.
[14] A.A. Mohammad, A. Alhaj, S. Shaltaf, An improved SVD-based watermarking scheme for protecting rightful ownership, Signal Processing 88 (2008) 2158–2180.
[15] C.C. Lai, An improved SVD-based watermarking scheme using human visual characteristics, Optics Communications 284 (2011) 938–944.
[16] M. Naor, A. Shamir, Visual cryptography, in: Proceedings of the Advances in Cryptology—EUROCRYPT'94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1995, pp. 1–12.
[17] C.C. Wang, S.C. Tai, C.S. Yu, Repeating image watermarking technique by the visual cryptography, IEICE Transactions on Fundamentals E 83-A (2000) 1589–1598.
[18] Y.C. Hou, P.M. Chen, An asymmetric watermarking scheme based on visual cryptography, in: Proceedings of the 5th Signal Processing Conference, vol. 2, 2000, pp. 992–995.
[19] C.C. Chang, J.C. Chung, An image intellectual property protection scheme for gray level images using visual secret sharing strategy, Pattern Recognition Letters 23 (2002) 931–941.
[20] C.S. Hsu, Y.C. Hou, Copyright protection scheme for digital images using visual cryptography and sampling methods, Optical Engineering 44 (2005) 077003.
[21] D.C. Lou, H.K. Tso, J.L. Lin, A copyright protection scheme for digital images using visual cryptography technique, Computer Standards & Interfaces 29 (2007) 125–131.
[22] T.H. Chen, C.C. Chang, C.S. Wu, D.C. Lou, On the security of a copyright protection scheme based on visual cryptography, Computer Standards & Interfaces 31 (2009) 1–5.
[23] M.S. Wang, W.C. Chen, A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography, Computer Standards & Interfaces 31 (2009) 757–762.
[24] H.M. Ozaktas, O. Arikan, Digital computation of the fractional Fourier transform, IEEE Transactions on Signal Processing 9 (1996) 2141–2149.
[25] V.A. Narayanan, K.M.M. Prabhu, The fractional Fourier transform: theory, implementation and error analysis, Microprocessors and Microsystems 27 (2003) 511–521.
[26] S.C. Pei, M.H. Yeh, Two dimensional discrete fractional Fourier transform, Signal Processing 67 (1998) 99–108.
[27] B. Zhou, J. Chen, A geometric distortion resilient image watermarking algorithm based on SVD, Chinese Journal of Image and Graphics 9 (2004) 506–512.