J Vis (2011) 14:85–93
DOI 10.1007/s12650-010-0067-5

REGULAR PAPER

Gaurav Bhatnagar · Jonathan Wu · Balasubramanian Raman

A robust security framework for 3D images

Received: 12 May 2010 / Accepted: 22 October 2010 / Published online: 9 December 2010

Abstract Three-dimensional (3D) visualization of spatial and non-spatial data is a well-established practice having numerous applications. The cheapest and the most efficient way to 3D visualization is 3D images/Anaglyphs. 3D images contain 3D information of the objects present in the image. These images are easily obtained by superimposing left and right eye images in different color in a single image. In this paper, a novel security framework, viz., watermarking scheme, is presented to ensure their security. The proposed security framework is employed in fractional Fourier transform domain of secret color channel followed by the embedding using singular value decomposition. The secret channels (SEC) are obtained by applying reversible integer transform on the RGB channels. The experimental results prove the robustness and imperceptibility of the proposed watermarking scheme.

Keywords 3D visualization · 3D images/Anaglyph · Digital watermarking · Reversible integer transform · Fractional Fourier transform · Singular value decomposition

1 Introduction

In the last decades, 3D reconstruction (Trucco and Verri 1998), which is the process of capturing the shape and appearance of real objects, is of main attraction among computer vision researchers. This process is achieved by either active or passive methods. Active methods are those methods which actively interfere with the reconstructed object, either mechanically or radiometrically. A simple example of a mechanical method is using a depth gauge to measure a distance to a rotating object put on a turntable. On the contrary, passive methods do not interfere with the reconstructed object, they only use a sensor to measure the radiance reflected or emitted by the object's surface to derive its 3D structure. Typically, the sensor is an image sensor in a camera sensitive to visible light and the input to the method is a set of digital images or video.

Recently, researchers have come up with a new terminology namely stereogram (Pinker 1997). A stereogram is an optical illusion of depth created from flat, two-dimensional image or images. The most renowned type of stereogram is Anaglyph/3D images (Rollmann 1853; Stoffer et al. 2003), which usually

G. Bhatnagar (✉) · J. Wu
University of Windsor, Windsor, ON N9B 3P4, Canada
E-mail: goravdma@gmail.com

J. Wu
e-mail: jwu@uwindsor.ca

B. Raman
Indian Institute of Technology Roorkee, Roorkee 247667, India
e-mail: balarfma@iitr.ernet.in

provides a stereoscopic 3D effect, when viewed with two color glasses (with lenses of chromatically opposite color, usually red and cyan). These two words, 3D images and Anaglyphs, are used as synonymous through out the paper. 3D images are a recent revitalization due to the presentation of images and videos on the Internet, Blu-ray HD discs, CDs and even in print. 3D images are made up of two color layers, superimposed, but offset with respect to each other to produce a depth effect. Generally, the main content is in the center, while the foreground and background are shifted laterally in opposite directions. The 3D image contains two differently filtered color images, one for each eye. When viewed through the "color coded" "anaglyph glasses", they reveal an integrated stereoscopic image. The visual cortex of the brain fuses this into perception of a three-dimensional scene or composition. 3D images are much easier to view than either parallel (diverging) or crossed-view pair stereograms. However, these side-by-side types offer bright and accurate color rendering which is not easily achieved.

In recent years, three-dimensional visualization has gained significant interest of research community in the area of visualization due to its application in the field of scientific arts, such as sculpture, rhythmical movement, fine arts, education and so on. The stressed motive of the present work is to give security to the 3D images. It is apparent that the amount of multimedia data such as photographs, paintings, speech, music, video, documents, etc., is distributed through international communication and mobile networks on a large scale which originates the concept of intelligent systems and technology to understand, index, manage, search and consume these data. Further, in such an environment, the multimedia data can be copied easily, tampered and transmitted back to the network. As a result, there is a strong need of developing some robust frameworks which ensure the security and authentication of multimedia data. Digital watermarking (Cox et al. 2001; Liu and Tan 2002; Alattar 2003; Ganic and Eskicioglu 2005; Sverldov et al. 2005; Bhatnagar and Raman 2009) is frequently used as the effective solution for persisting problem nowadays.

This paper presents a robust framework for the security and authenticity of 3D images via digital watermarking. First, the dependent RGB color channels of an original 3D image are secretly mapped to the independent color channels (SEC channel) by reversible integer transform (RIT) which is followed by the decomposition of any or all SEC channel using fractional Fourier transform (FrFT). Now, the largest singular value of each block is obtained from segmented transformed channel and stacked into an array to form key matrix. The watermark, which gives the security and authenticity to the 3D image, is embedded in the key matrix and embedding is done by modifying its singular values with the watermark singular values. The main benefit of the proposed scheme is the embedding of watermark robustly in the largest singular values of segmented blocks which contain most of the block energy and is less affected by the image processing manipulation. The experimental results demonstrate the robustness and superiority of the proposed algorithm.

The rest of paper is organized as follows: In Sect. 2, mathematical preliminaries are illustrated followed by the proposed security framework for 3D images in Sect. 3. In Sect. 4, experimental results using proposed framework are presented and finally Sect. 5 gives the concluding remarks regarding proposed security framework.

2 Mathematical preliminaries

This section reviews the basic mathematical concepts and results which are used in the proposed watermarking scheme for 3D images. These concepts are as follows.

2.1 Fractional Fourier transform (FrFT)

The concept of FrFT is introduced by Victor Namias in 1980 (Namias 1980). The FrFT is the generalization of Fourier transform. The essence of the generalization is to provide a parameter α that can be interpreted as a rotation by an angle α in the time–frequency plane or decomposition of the signal in terms of chirps. Generally, this parameter is called an angle or transform order associated with FrFT. Mathematically, the FrFT of a one-dimensional function $s(t)$ is defined as

$$F^{\alpha}[s(t)](x) = \int_{-\infty}^{\infty} s(t)K_{\alpha}(t,x)\,\mathrm{d}t, \tag{1}$$

where α is the transform order and $K_\alpha(t,x)$ is the transform kernel given by

$$K_\alpha(t,x) = \begin{cases} \sqrt{1-\mathrm{i}\cot\alpha}\,\mathrm{e}^{\mathrm{i}\frac{t^2+x^2}{2}\cot\alpha - \mathrm{i}xt\csc\alpha} & \alpha \neq n\pi \\ \delta(t-x), & \alpha = 2n\pi \\ \delta(t+x), & \alpha = 2n\pi \pm \pi \end{cases}, \tag{2}$$

where n is a given integer. The FrFT of a signal exists under the same conditions in which its Fourier transform exists. The inverse FrFT can be visualized as the FrFT with transform order $-\alpha$ (the detailed illustration on the computation of FrFT can be found in Almedia 1994; Ozaktas et al. 2000). The main property of FrFT is that the signal obtained is in purely time domain if transform order (α) is 0 and in purely frequency domain if transform order (α) is $\pi/2$. Some of the important properties of the FrFT are summarized as follows:

1. *Identity operator*: F^0 is the identity operator. The FrFT of order $\alpha = 0$ is the input signal itself. The FrFT of order $\alpha = 2\pi$ also acts as the identity operator because it can be viewed as the successive application of the ordinary Fourier transform four times. Mathematically,
$$F^0[s(t)] = F^{2\pi}[s(t)] = s(t). \tag{3}$$
2. *Fourier transform operator*: $F^{\pi/2}$ is the Fourier transform operator. The FrFT of order $\alpha = \pi/2$ 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. Mathematically,
$$F^\alpha(F^\beta[s(t)]) = F^{\alpha+\beta}[s(t)]. \tag{4}$$
4. *Inverse*: The inverse FrFT to reconstruct the original signal is the FrFT of order $-\alpha$, i.e.
$$F^{-\alpha}(F^\alpha[s(t)]) = F^{-\alpha+\alpha}[s(t)] = F^0[s(t)] = s(t). \tag{5}$$
5. *Higher dimensional FrFT*: Due to the separability of the transform, the higher dimensional FrFT can be obtained by successively taking one-dimensional FrFT along all the directions. For instance, 2D FrFT can be viewed as
$$F^{\alpha_x,\alpha_y}[s(t_x,t_y)](u,v) = \mathrm{FrFT}_{\alpha_y}^{t_y\to v}\{\mathrm{FrFT}_{\alpha_x}^{t_x\to u}\{s(t_x,t_y)\}\}. \tag{6}$$

The main benefit of using FrFT in proposed security framework via watermarking is its dependence on the transform orders. These transform orders are used as the keys to the watermark extraction because without using correct transform orders one cannot obtain correct transformed domain in which the watermark is embedded. Hence, one cannot extract the watermark efficiently with wrong transform orders.

2.2 Singular value decomposition (SVD)

Let A be a general real(complex) matrix of order $m \times n$. The SVD (Strang 1993) of A is the factorization

$$A = U * S * V^{\mathrm{T}} \tag{7}$$

where U and V are *orthogonal*(*unitary*) and $S = \mathrm{diag}(\sigma_1, \sigma_2, \ldots, \sigma_r)$, where σ_i, $i = 1(1)r$ are the singular values of the matrix A with $r = \min(m, n)$ and satisfying $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r$. The first r columns of V are the *right singular vectors* and the first r columns of U are the *left singular vectors*.

The use of SVD in digital image processing has some advantages. First, the size of the matrices from SVD transformation is not fixed. It can be a square or rectangular. Secondly, singular values contain intrinsic algebraic image properties. Finally, singular values in a digital image are less affected if general image processing is performed. These properties of SVD make it a perfect tool for watermarking.

3 Proposed security framework

In this section, some of the motivating factors in design of security framework are discussed. We have used FrFT and SVD for developing the watermarking scheme. Let us consider F is the host 3D image and

W is the watermark. In order to form 3D image, the linear projection method is used which is proposed in Dubois (2001). The watermark W is embedded in the host 3D image, which can be further extracted for variety of purposes including identification and authentication. The host 3D image is a color image of size $M \times N$ whereas the watermark image is a gray scale meaningful image/logo instead of Gaussian noise type sequence and of size $m \times n$. The proposed security framework comprises of two processes, viz. (1) embedding process and (2) extraction process. The first process essentially embeds the watermark in the host 3D image to get watermarked 3D image, whereas extraction process extracts an estimate of the watermark from the possibly attacked watermarked 3D image whenever needed. These processes are as follows.

3.1 Secret color channel conversion

In image processing, the integer color transform is a reversible operation that can transform one color coordinate into another one and both the inputs and the outputs are of integer forms. There are many integer color transforms in literature which are frequently used and are reversible. Since in the present work, the main concern is the security of 3D image via watermarking and it is evident that the R, G and B channels are highly dependent on each other but for a good watermarking scheme this relation must be broken before embedding so that the watermark will survive a variety of attacks. Therefore, to give randomness and enhance security, RGB color channels are first transformed into secret color channels, say SEC. For this purpose, the corresponding pixels are collected from each R, G and B channel and transformed by triplet-based reversible integer transform (T-RIT) to get the corresponding pixels of S, E and C channels. Hence, RGB channels are first transformed into three secret independent channels, i.e. SEC channel using T-RIT and then the embedding is done either in all or any of S, E and C channel.

The RIT is a reversible transform which maps integers to integers. The main advantage of RIT is that it can be implemented by fixed-point processors and no floating-point processor is required. Since the computation time for the fixed-point processors is much less, the RIT is usually very efficient. Let us consider a vector triplet $\mathbf{u} = (u_1, u_2, u_3)$, where u_is are integers. The T-RIT (Alattar 2003) of $\mathbf{u}$ is given by

$$v_1 = \left\lfloor \frac{a_1u_1 + a_2u_2 + a_3u_3}{a_1 + a_2 + a_3} \right\rfloor, \quad v_2 = u_2 - u_1, \quad v_3 = u_3 - u_1, \tag{8}$$

where $\lfloor\, r \,\rfloor$ is the largest integer not greater than r and $\mathbf{a} = (a_1, a_2, a_3)$ is a constant vector which is secret and plays a vital role of key in the transformation. Obviously, for different $\mathbf{a}$, different values of $\mathbf{v}$ are obtained. Now, in order to get original integers back from transformed integers ($\mathbf{v}$), the inverse T-RIT is defined as

$$\begin{aligned} u_1 &= \left\lceil v_1 - \frac{a_2v_2}{a_1 + a_2 + a_3} - \frac{a_3v_3}{a_1 + a_2 + a_3} \right\rceil, \\ u_2 &= \left\lceil v_1 + \frac{(a_1 + a_3)v_2}{a_1 + a_2 + a_3} - \frac{a_3v_3}{a_1 + a_2 + a_3} \right\rceil, \\ u_3 &= \left\lceil v_1 - \frac{a_2v_2}{a_1 + a_2 + a_3} + \frac{(a_1 + a_2)v_3}{a_1 + a_2 + a_3} \right\rceil, \end{aligned} \tag{9}$$

where $\lceil r \rceil$ is the smallest integer not less than r. For example, if we want to convert RGB channel values [200 175 145] in the corresponding values in SEC channel with $\mathbf{a} = [17\ 12\ 10]$, the whole process of conversion can be done by Eq. 8 as

$$\begin{aligned} S &= \left\lfloor \frac{17 \times 200 + 12 \times 175 + 10 \times 145}{17 + 12 + 10} \right\rfloor = \lfloor 178.2051 \rfloor = 178, \\ E &= 175 - 200 = -25, \\ C &= 145 - 200 = -55 \end{aligned}$$

and reverse process is done by Eq. 9 as

$$R = \left\lceil 178 - \frac{12 \times (-25)}{17+12+10} - \frac{10 \times (-55)}{17+12+10} \right\rceil = \lceil 199.7949 \rceil = 200,$$
$$G = \left\lceil 178 + \frac{(17+10) \times (-25)}{17+12+10} - \frac{10 \times (-55)}{17+12+10} \right\rceil = \lceil 174.7949 \rceil = 175,$$
$$B = \left\lceil 178 - \frac{12 \times (-25)}{17+12+10} + \frac{(17+12) \times (-55)}{17+12+10} \right\rceil = \lceil 144.7949 \rceil = 145.$$

3.2 Embedding process

The embedding process is given as follows.

- Map RGB color channels of host 3D image (F) into secret SEC color channels.
- Perform (α_x, α_y)-FrFT on selected channel (say $\widetilde{S}$,) which is denoted by f, where α_x and α_y are the transform orders along x- and y-axis.
- Segment f into non-overlapping blocks of size $p_1 \times p_2$, which are denoted by f^q, where $p_1 = \lfloor \frac{M}{m} \rfloor$, $p_2 = \lfloor \frac{N}{n} \rfloor$ and $q = mn$ are the total number of blocks.
- Perform SVD transform on all non-overlapping blocks f^q, i.e.

$$f^q = U_{f^q} S_{f^q} V_{f^q}^{\mathrm{T}}. \tag{10}$$

- Collect the highest singular value of all non-overlapping blocks f^q and stack into an array of size $m \times n$ to form a key matrix (K) as

$$K = \begin{bmatrix} \sigma_1 & \sigma_2 & \sigma_3 & \dots & \sigma_n \\ \sigma_{n+1} & \sigma_{n+2} & \sigma_{n+3} & \dots & \sigma_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_{m(n+1)} & \sigma_{m(n+2)} & \sigma_{m(n+3)} & \dots & \sigma_{mn} \end{bmatrix}. \tag{11}$$

- Perform SVD transform on K and watermark image W

$$K = U_K S_K V_K^{\mathrm{T}}, \quad W = U_W S_W V_W^{\mathrm{T}}. \tag{12}$$

- Modify the singular values of K with the singular values of the watermark as

$$S_K^* = S_K + \beta S_W, \tag{13}$$

where β gives the watermark strength.

- Perform inverse SVD to construct modified K as $K_{\mathrm{new}} = U_K S_K^* V_K^{\mathrm{T}}$.
- Map modified highest singular value on their original position followed by inverse SVD to get modified non-overlapping blocks f_{new}^q.
- Map modified blocks to their original position followed by inverse (α_x, α_y)-FrFT to get watermarked channel $\widetilde{S}$.
- Map modified secret color channel $\widetilde{\mathrm{S}}$EC to modified RGB channel to get watermarked 3D image $\widetilde{F}$.

3.3 Extraction process

- Map RGB color channel of watermarked 3D image ($\widetilde{F}$) into secret SEC color channels.
- Perform (α_x, α_y)-FrFT on the watermarked channel ($\widetilde{S}$), which is denoted by $\widetilde{f}$, where α_x and α_y are the transform orders along x- and y-axis.
- Segment $\widetilde{f}$ into non-overlapping blocks of size $p_1 \times p_2$, which are denoted by $\widetilde{f}^q$, where $p_1 = \lfloor \frac{M}{m} \rfloor$, $p_2 = \lfloor \frac{N}{n} \rfloor$ and $q = m\ n$ are the total number of blocks.
- Perform SVD transform on all non-overlapping blocks $\widetilde{f}^q$, i.e.

$$\widetilde{f}^q = U_{\widetilde{f}^q} S_{\widetilde{f}^q} V_{\widetilde{f}^q}^{\mathrm{T}}. \tag{14}$$

- Collect the highest singular value of all non-overlapping blocks $\widetilde{f}^q$ and stack into an array of size $m \times n$ to form a watermarked key matrix ($\widetilde{K}$) as

$$\widetilde{K} = \begin{bmatrix} \widetilde{\sigma}_1 & \widetilde{\sigma}_2 & \widetilde{\sigma}_3 & \dots & \widetilde{\sigma}_n \\ \widetilde{\sigma}_{n+1} & \widetilde{\sigma}_{n+2} & \widetilde{\sigma}_{n+3} & \dots & \widetilde{\sigma}_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \widetilde{\sigma}_{m(n+1)} & \widetilde{\sigma}_{m(n+2)} & \widetilde{\sigma}_{m(n+3)} & \dots & \widetilde{\sigma}_{mn} \end{bmatrix}. \tag{15}$$

- Perform SVD transform on $\widetilde{K}$, i.e. $\widetilde{K} = U_{\widetilde{K}} S_{\widetilde{K}} V_{\widetilde{K}}^{\mathrm{T}}$.
- Extract the singular values of watermark from watermarked image as

$$S_W^{\mathrm{ext}} = \frac{S_{\widetilde{K}} - S_K}{\beta}. \tag{16}$$

- Obtain the extracted watermark as

$$W_{\mathrm{ext}} = U_W S_W^{\mathrm{ext}} V_W^{\mathrm{T}}. \tag{17}$$

4 Experimental results

In order to explore the performance of proposed security framework, MATLAB platform is used and a number of experiments are performed on Cone, Tsukuba and Dolls 3D images which are of size 400 × 256 and are depicted in Fig. 1a, e and i, respectively. All the 3D images are obtained from linear projection algorithm considering red–cyan colors, i.e. to visualize these 3D images red and cyan colors are used as the two color glasses. For watermark, eight-bit gray scale University of Windsor (UofW), Circle and IIT logos are used which are of size 80 × 80 and are shown in Fig. 1b, f and j, respectively. The values of p_1 and p_2 are selected equally and taken to be 4, whereas the vector **a**, for mapping RGB channels to SEC channels, is taken as (13, 11, 21). The transform order for FrFT is $\alpha_x = 0.1270$ and $\alpha_y = 0.9134$. Figure 1a–c shows the original left, right and 3D Tsukuba images. Figure 1c, g and k shows the watermarked 3D Cone, Tsukuba and Dolls image, whereas Fig. 1d, h and l shows the extracted watermark images. The quality of watermarked 3D image is measured using Peak Signal to Noise Ratio (PSNR). The PSNR for watermarked Cone, Tsukuba and Dolls 3D images is 41.3992, 40.4135 and 41.7545 dB, respectively. Now, the watermarked image undergoes to different kinds of intentional and un-intentional attacks followed by the watermark extraction. In order to verify the quality of extracted watermark, different measures can be used to show the similarity between the original and the extracted watermarks. In the proposed algorithm, correlation coefficient is given by

$$\rho(w, \bar{w}) = \frac{\sum_{i,j}[w(i) - w_{\mathrm{mean}}][\overline{w}(i) - \overline{w}_{\mathrm{mean}}]}{\sqrt{\sum_{i,j}[w(i) - w_{\mathrm{mean}}]^2 \sum_{i,j}[\overline{w}(i) - \overline{w}_{\mathrm{mean}}]^2}}, \tag{18}$$

where w and $\bar{w}$ are the original and the extracted watermark images. The value of ρ lies between $[-1, 1]$. If the value of ρ is equal to 1, then the singular values of extracted watermark are just equal to the original one. If the value of ρ is -1, then the difference is negative for the largest singular values. In this case, the lighter parts of the image become darker and darker parts become lighter, i.e. constructed watermark looks like negative thin film. According to statistics, the principle range for correlation coefficient is [0, 1]. Hence, the negative image transform (NIT) is performed on the extracted watermark whenever ρ takes negative value, in order to get ρ in the principle range. The NIT with intensity levels in the range $[0, L-1]$ is given by the expression $s = L - 1 - r$, where r is the original intensity and s is the transformed intensity.

To investigate the robustness of the proposed framework, the watermarked Tsukuba 3D image is attacked by average and median filtering, Gaussian noise addition, JPEG compression, cropping, resizing, rotation, histogram equalization, contrast adjustment and sharpening attacks. After these attacks on the watermarked image, the extracted watermarks are compared with the original one using Eq. 18. In Fig. 1, original host, original watermark, watermarked host and extracted watermark images are shown. If original and watermarked images are observed, then no perceptual degradation is found according to the human visual system. For further analysis, Tsukuba 3D image is used because it has minimum PSNR among all the experimental images. The detailed results in order to verify robustness of the proposed algorithm are discussed below.

The most common manipulation in digital images is filtering. The watermarked image is filtered by average and median filtering considering 7 × 7 window and watermark is then extracted from the attacked images. The visual results are depicted in Figs. 2I and II, respectively. Another most common method to

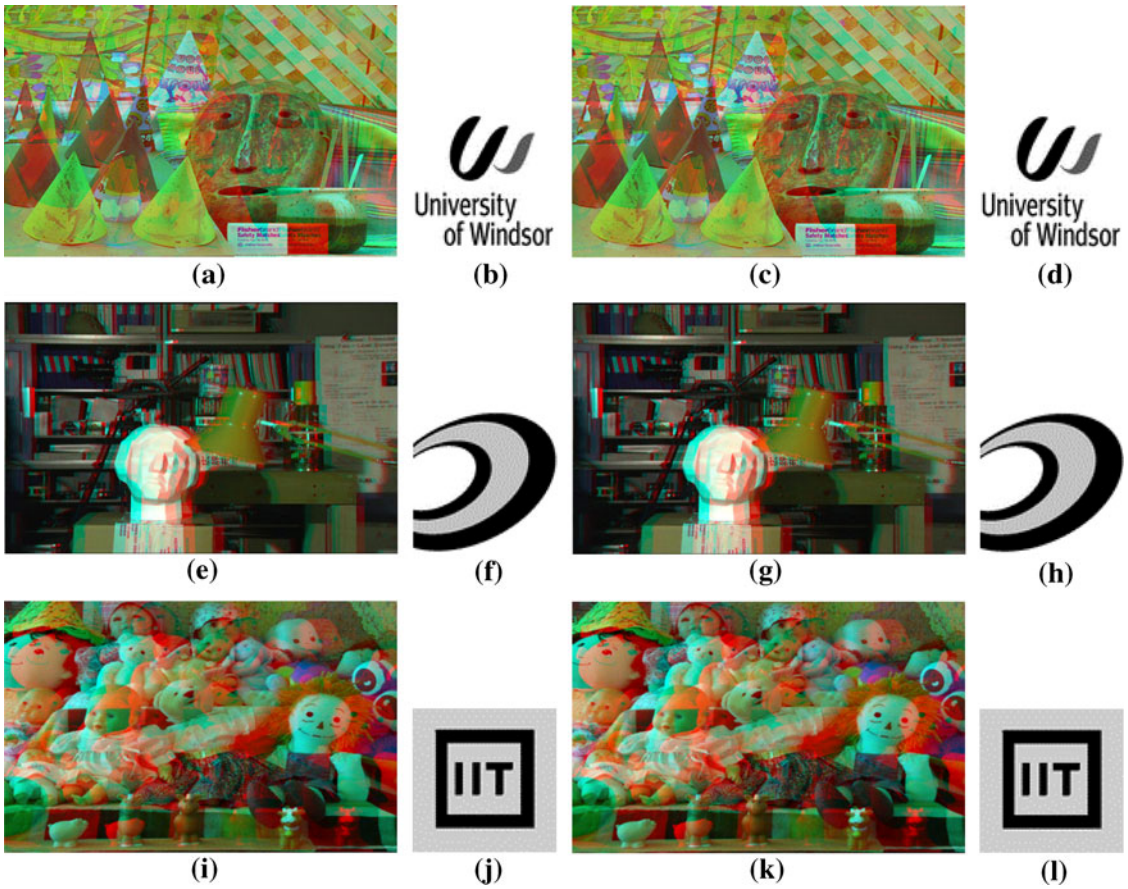

Fig. 1 **a** 3D Cone image, **b** UofW logo, **c** watermarked 3D Cone image, **d** extracted UofW logo, **e** 3D Tsukuba image, **f** Circle logo, **g** watermarked 3D Tsukuba image, **h** extracted Circle logo, **i** 3D Dolls image, **j** IIT logo, **k** watermarked 3D Dolls image, and **l** extracted IIT logo

estimate the robustness of watermark is the addition of noise. In many cases, the degradation and distortion of the image are due to noise addition. Robustness against additive noise is estimated by degrading watermark image by adding 50% Gaussian noise randomly. It is clear from the Fig. 2III that lot of information is lost after this attack but the extracted watermark is still recognizable. To check the robustness against image compression, the watermarked image is attacked by JPEG compression attack. The extracted watermark logo from compressed watermarked host image using JPEG compression with compression ratio 50 is given in Fig. 2IV. Image cropping is another most common manipulation in digital images. To check the robustness against image cropping, 50% area of the watermarked image is cropped and then watermark is extracted. The corresponding visual results are given in Fig. 2V. Enlargement or reduction is commonly performed to fit the image into the desired size resulting in information loss of the image including embedded watermarks. Hence, the proposed technique is also tested for resizing attack. For doing this task, the size of watermarked host image is first reduced to 200 $\times$ 128 and then carried back to its original size, i.e. 400 $\times$ 256 followed by the watermark extraction and corresponding results are shown in Fig. 2VI. The proposed technique is also tested for rotation attack. For this purpose, the watermarked image is rotated by 50° (see Fig. 2VII). In Fig. 2VIII, IX and X, the results for histogram equalization, contrast adjustment and sharpening attacks are shown, respectively. For contrast adjustment, the contrast of the watermarked image is decreased by 50%, whereas the sharpness of the watermarked image is increased by 50% for sharpening attack. The correlation coefficients of all extracted watermarks are depicted in Table 1. Further, the SVD-based watermarking scheme given by Liu and Tan (2002) is implemented and compared with proposed algorithm (see Table 1). Comparison has been done by using same host 3D and watermark images which are used in the proposed algorithm. Table 1 clearly ensures that the proposed algorithm perform better than the existing one (this fact can easily be observed by the obtained maximum values of ρ).

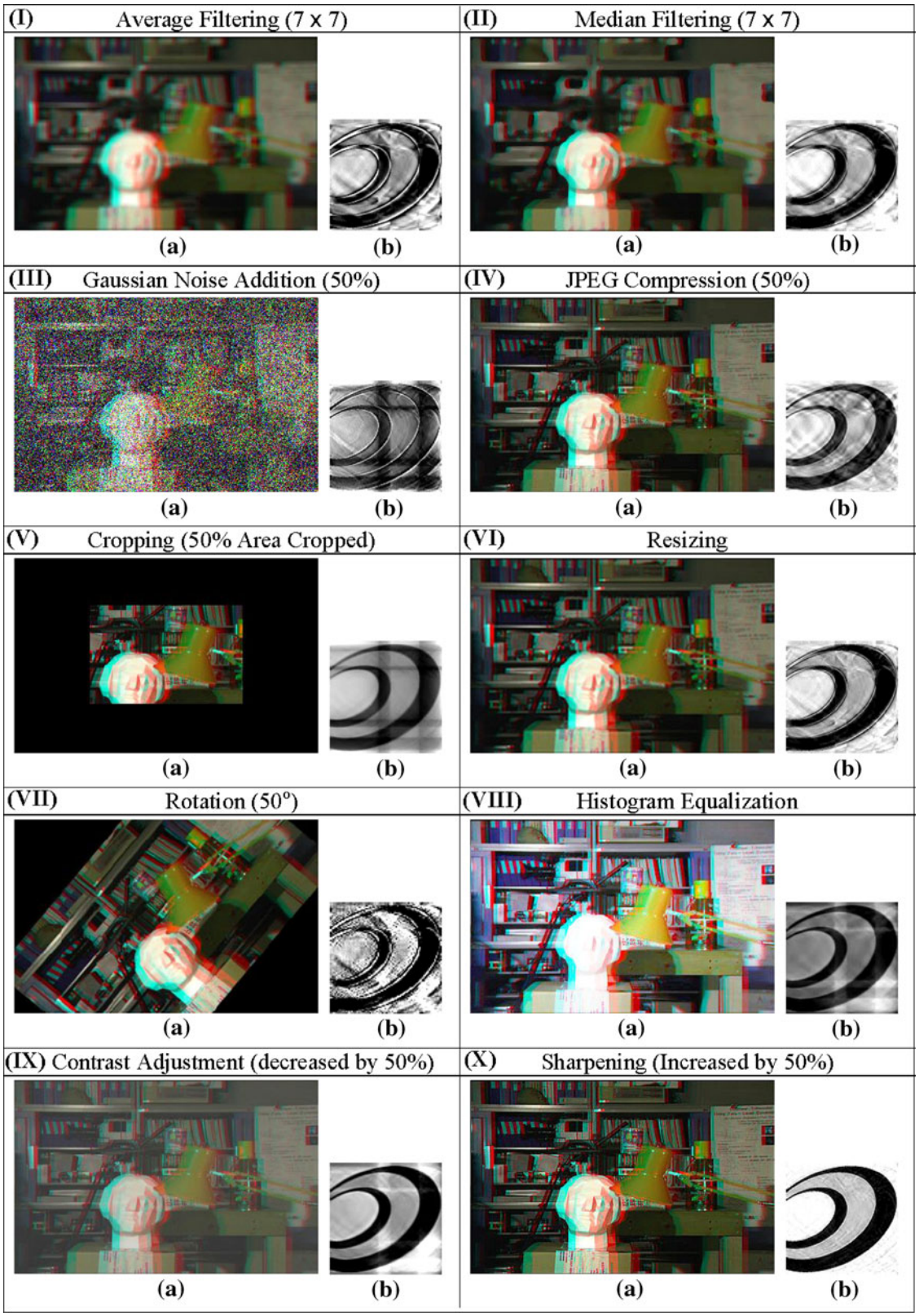

Fig. 2 Attack analysis for Tsukuba 3D image: **a** attack 3D image and **b** extracted watermark image

Table 1 Correlation coefficients of extracted watermarks after attacks

Attacks:	ρ					
Methods:	Proposed			Liu and Tan (2002)		
Images:	Cones	Tsukuba	Dolls	Cones	Tsukuba	Dolls
No attack	1	1	0.9999	1	0.9998	1
Average filtering (7 × 7)	0.8503	0.8543	0.8422	0.7560	0.7502	0.7547
Median filtering (7 × 7)	0.9406	0.9357	0.9372	0.8091	0.8171	0.8003
Gaussian noise addition (50%)	0.8491	0.8514	0.8435	0.8169	0.8118	0.8157
JPEG compression (CR = 50)	0.9719	0.9763	0.9757	0.9440	0.9497	0.9475
Cropping (50% area cropped)	0.9649	0.9586	0.9558	0.6472	0.6420	0.6441
Resizing	0.9475	0.9455	0.9424	0.7511	0.7678	0.7517
Rotation (50°)	0.8909	0.8970	0.8891	0.6838	0.6887	0.6853
Histogram equalization	0.9597	0.9587	0.9548	0.9593	0.9672	0.9508
Contrast adjustment (50% decreased)	0.9768	0.9777	0.9744	0.9517	0.9599	0.9537
Sharpening (50% increased)	0.9956	0.9963	0.9964	0.9906	0.9876	0.9931

5 Conclusions

In this paper, a simple yet efficient security solution for 3D images, viz., watermarking scheme, is proposed which is based on reversible integer transform, FrFT and singular value decomposition. The proposed scheme uses a meaningful gray scale image as watermark instead of Gaussian noise type sequence. The main benefit of the proposed scheme is the use of RIT and FrFT because the secret channel (obtained from RIT) and transform orders (for FrFT) play a vital role of keys. Since, without knowing correct secret channel and transform orders, one cannot obtain the correct domain in which watermark is embedded and therefore cannot extract the watermark correctly. The experimental results clearly demonstrate the improved performance in terms of imperceptibility and robustness against different kinds of attacks.

References

Alattar AM (2003) Reversible watermark using difference expansion of triplets. In: Proceedings of IEEE international conference on image processing, vol 1, Barcelona, Spain, pp 501–504

Almeida LB (1994) The fractional Fourier transform and time–frequency representations. IEEE Trans Signal Process 42:3084–3091

Bhatnagar G, Raman B (2009) A new robust reference watermarking scheme based on DWT-SVD. Comput Stand Interface 31(5):1002–1013

Cox IJ, Miller ML, Bloom JA (2001) Digital watermarking. Morgan Kaufmann, San Francisco, CA

Dubois E (2001) A projection method to generate Anaglyph stereo images. In: Proceedings of IEEE international conference on acoustics speech signal processing, vol 3, Salt Lake City, UT, pp 1661–1664

Ganic E, Eskicioglu AM (2005) Robust embedding of visual watermarks using DWT-SVD. J Electron Imag 14(4):043004

Liu R, Tan T (2002) An SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans Multimed 4(1):121–128

Namias V (1980) The fractional order Fourier transform and its application to quantum mechanics. J Inst Math Appl 25:241–265

Ozaktas HM, Kutay MA, Zalevsky Z (2000) The fractional Fourier transform with applications in optics and signal processing. Wiley, New York

Pinker S (1997) The Mind's eye. In: Pinker S (ed) How the mind works. WW Norton & Company, New York, pp 211–233

Rollmann W (1853) Notiz zur Stereoskopie. Ann Phys 165(6):350–351

Stoffer PW, Phillips E, Messina P (2003) Anaglyph image technology as a visualization tool for teaching geology of national parks. EOS Trans AGU 84(46), Fall meet. suppl., Abstract ED32B-1198

Strang G (1993) Introduction to linear algebra. Wellesley-Cambridge Press, Wellesley

Sverldov A, Dexter S, Eskicioglu AM (2005) Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies. In: Proceedings of European signal processing conference, Antalya, Turkey, pp 1–4

Trucco E, Verri A (1998) Introductory techniques for 3D computer vision. Prentice Hall PTR, New Jersey