

# A Novel Semi-Fragile Image Watermarking, Authentication and Self-restoration Technique Using the Slant Transform

X. Zhao, A.T.S. Ho, H. Treharne, V. Pankajakshan, C. Culnane and W. Jiang

University of Surrey  
Department of Computing  
School of Electronics and Physical Sciences  
Guildford-GU2 7XH, UK  
a.ho@surrey.ac.uk

## Abstract

*A novel semi-fragile digital watermarking method based on the Slant transform (SLT) for image authentication and self-restoration is introduced in this paper. The watermark bits are embedded into the middle frequency region of each block after applying SLT of the original image. The original image is further compressed and then embedded into the least significant bits (LSBs) of the watermarked image for subsequent self-restoration. The tampered regions of the watermarked image can be detected and localised by extracting the embedded watermark to compare with the original watermark for authentication. Localised tampered regions are self-recovered by extracting the LSBs of the watermarked image. Results achieved show that the SLT algorithm is more robust, faster and accurate than other transform methods based on the DCT and Pinned Sine Transform. It could survive cut-and-paste attacks with robustness to JPEG attacks up to  $QF=75$  compression prior to image authentication. The tampered regions can be detected with an average 91% detection rate after surviving the compression attack.*

## I. Introduction

Nowadays, the increasing affordable and affordability of image editing software has led to the possibility of illegal activities such as tampering and faking of digital images. The integrity of the original image content must be securely protected, and this is particularly important for law enforcement applications such as crime scene analysis and traffic enforcement.

Semi-fragile watermarking techniques for image content authentication have recently attracted much attention. These included the use of Discrete Cosine Transform (DCT) [2] and Pinned Sine Transform (PST) [3] methods to localise tampered regions in image attacks such as cutting and pasting, and JPEG compression. The Slant Transform (SLT)

has been applied to image coding in the past [4] and was recently adopted for robust image watermarking [5]. In this paper, the Slant Transform is proposed for semi-fragile watermarking and authentication of images. Furthermore, SLT is also used for compressing the original image, providing a means to self-recovering the tampered regions by embedding the compressed cover image into the least significant bits (LSBs) of the watermarked image.

In section II, a brief introduction of SLT is presented followed by our proposed approach in section III. The experimental results are analyzed and illustrated in section IV and finally, a conclusion and future work are presented in section V.

## II. Slant Transform

Slant Transform has a fast computational algorithm which provides a significant bandwidth reduction. This results in a lower mean-square error (MSE) for moderate size image blocks [4]. Moreover, for textured images, the quality of the Slant Transformed images was higher than images coded by using other transforms such as DCT and Hadamard [5]. The Slant Transform is considered to be sub-optimum for energy compaction; however it is important for digital watermarking, as it can improve the watermark robustness by capitalizing on the spread of the middle to higher frequency bands [5]. Also, the Slant Transform is simpler and faster as its basic functions are somewhat similar to the Hadamard Transform [4]. The forward and inverse of SLT [4] [5] can be expressed as follows:

$$[V] = [S_n][U][S_n]^T, \quad [U] = [S_n]^T[V][S_n] \quad (1)$$

Where  $[U]$  represents the original image of size  $N \times N$ ,  $[S_n]$  is the  $N \times N$  unitary Slant matrix and  $[V]$  represents the transformed components. The inverse transformation to recover  $[U]$  is  $[S_n]^T$  equals  $S_n^{-1}$ , which is the permutation of  $[S_n]$

### III Semi-fragile Slant Transform Method

#### A. Watermark Embedding

A novel semi-fragile Slant Transform digital watermarking method is adopted based on previous work relating to PST [3] and DCT [2]. The embedding process using the Slant Transform is illustrated in Figure 1. The first 7 bits of the cover image are extracted and divided into 8\*8 blocks by applying SLT. The watermark embedding algorithm is then utilised, which is illustrated in the pseudo code below. After watermark embedding, frequency coefficients of each block of the watermarked image are extracted by using the inverse Slant Transform. For restoration, the original image sub-blocks also undergo the same Slant Transform and compression is then achieved by discarding the high frequency coefficients. The compressed image bits are assigned by replacing the selected LSBs of the watermarked image. Once authentication is initiated, the localised tampered regions will be restored using the appropriate compressed image blocks.

The SLT watermark embedding algorithm in pseudo code form is shown as follows:

```

if w = 1 then
    if x * h >= t then y = x; else y = s end if
else if w = 0 then
    if x * h < -t then y = x; else y = -s end if
end if
    
```

where  $w$  (1 or 0) represents the watermark, which is a pseudo-random sequence stored in a key file,  $x$  and  $y$  are the coefficients before and after watermarking.  $h$  represents the value that increases  $x$ , as  $x$  tends to have smaller values.  $t$  is utilized to examine the value size of  $x*h$ .  $s$  represents the watermark strength that influences the quality and robustness of the watermarked image.

To determine the optimum embedding regions for SLT, we evaluated different frequency locations based on 28 horizontal, 28 vertical and 55 zigzag watermarked locations for 6 images. As a result, we generated 666 images in total. Figure 2 shows the three best regions for watermark embedding (dashed rounded rectangles) and the final embedded watermark was determined to be concentrated in the middle frequency band (filled ellipse) for the Slant Transform.

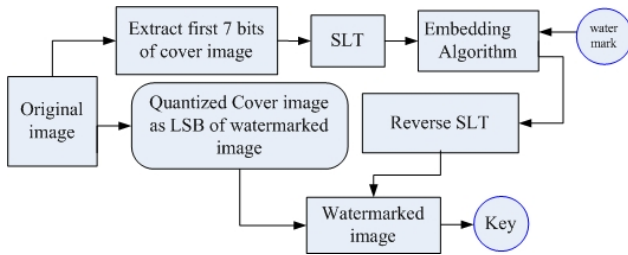


Figure 1 embedding process using the Slant Transform

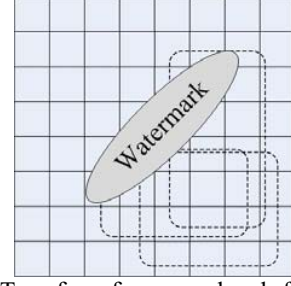


Figure 2 Slant Transform frequency bands for watermarking embedding

#### B. Watermark Retrieval-Authentication and Restoration

The proposed semi-fragile Slant Transform for image authentication and restoration method is shown in Figure 3. The retrieved watermark needs to be compared with the watermark that exists in the key file.

if  $y > 0$  then  $w = 1$  else  $w = 0$

After the watermark bits from the entire block have been retrieved, the comparison between the watermark bits can be accomplished by using the correlation coefficient as follows:

$$\rho = \frac{\sum_m \sum_n (W_{mn} - \bar{W})(W1_{mn} - \bar{W1})}{\sqrt{\sum_m \sum_n (W_{mn} - \bar{W})^2 \sum_m \sum_n (W1_{mn} - \bar{W1})^2}} \quad (2)$$

Where  $m, n$  represents the block size as column and row,  $W$  represents the retrieved watermark bits of entire block and  $W1$  indicates the watermark bits of entire block of the original image. For error correction, the correlation coefficient  $\rho$  can be compared with a pre-determined threshold value  $f$ . If  $\rho < f$ , which indicates that the block has been tampered as authentication which is followed by restoration of the tampered regions based on the decompression and extraction of the LSBs for the watermarked image.

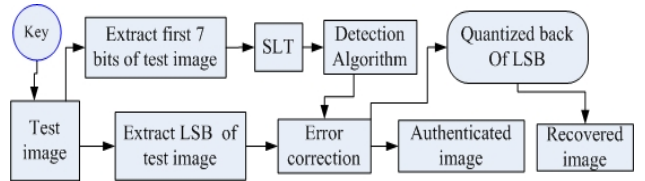


Figure 3 Authentication and Restoration using the Slant Transform

### IV Result and Analysis

Five greyscale test images of the size 256\*256 were utilized for comparative analysis. Table 1 shows that the average times taken for the Slant Transform embedding and detection was faster than DCT and PST.

On Intel Core 2 Duo 2.16GHz 1GB memory		
	Embed	Authenticate & Recovery
SLT	4.85 sec	1.25 sec
DCT	5.18	1.49
PST	5.24 sec	1.72 sec

Table 1 Average Speed (on 256\*256 greyscale image)

In addition, the Peak Signal-to-noise Ratio (PSNR) values of the Slant Transform were slightly lower than the DCT and PST as illustrated in Table 2. The reason for the relative lower quality of the watermarked images using the Slant Transform was the embedding locations concentrated mainly in the middle frequency band, which is considered to be more robust, whereas DCT and PST mainly concentrated more on high frequencies. However, the outcomes of subjective evaluation of SLT are similar to DCT and PST. The PSNR values for all authenticated and recovered images were greater than 30dB, which is subjectively considered as acceptable.

	SLT	DCT	PST
Couple	31.74	34.9	32.3
Man	31.65	34.55	32.15
Pyramids	30.99	33.71	31.87
Tank	31.74	34.48	32.24
Singapore	30.2	32.32	31.1

Table 2 PSNR Comparison

Figure 4 (a - d) illustrates the differences between the “pyramid” cover image, attacked image, authenticated image and recovered image. The subjective qualities of the authenticated and restored images of “pyramid” were considered to be acceptable with no noticeable degradation.

We evaluated six greyscale images (512\*512) for JPEG compression attack with QF=75 for the purpose of comparing the three transforms. The PSNR values of the watermark embedded images for the transforms were approximately 33dB for all tested images. The average authentication rate for SLT was approximately 91% which was much better than PST and DCT. The average authentication rate is evaluated by the following equation:

$$P_{avF} = 1 - \left( \frac{P_{mF} + P_{iF}}{2} \right) \quad (3)$$

Where  $P_{mF}$  is the percentage of undetected pixel of modified area and  $P_{iF}$  is the percentage of error detected pixel of the rest of image.

Figure 5 and Table 3 illustrate that SLT has a significantly

higher authentication rate than DCT and PST for compression attacks lower than QF=75. As a result, the SLT is considered to be more robust than DCT and PST.

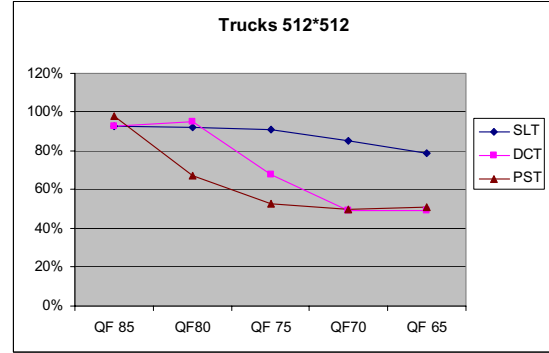


Figure 5 diagram of Authentication for Trucks image by using SLT, DCT and PST (PSNR 33)

Trucks PSNR 33.33					
	QF 85	QF 80	QF 75	QF 70	QF 65
SLT	93%	92%	91%	85%	79%
DCT	93%	95%	68%	49%	49%
PST	98%	67%	53%	50%	51%

Table 3 Authentication rate for Trucks image by using SLT, DCT and PST (PSNR 33)

Nevertheless, all the attacked images could not be recovered after applying JPEG compression attack with QF=75%. In terms of authentication, the tampered region of all images can be located with some false detection error after the JPEG compression attack. Overall, we found that higher texture watermarked images have better detection and authentication rate than the other two transforms.

## V Conclusion and Future Work

A novel semi-fragile Slant Transform digital watermarking method for authentication and restoration was proposed in this paper. The watermark embedding and retrieval were performed in a selected SLT frequency band optimised through iteration using the PSNR as the main criterion. Experimental results demonstrated the effectiveness of the new method, resulting in approximately 91% in terms of authentication accuracy after copy-and-paste attack with 75% JPEG compression. For future work, irregular sampling could be used to improve restoration after compression attack [3].

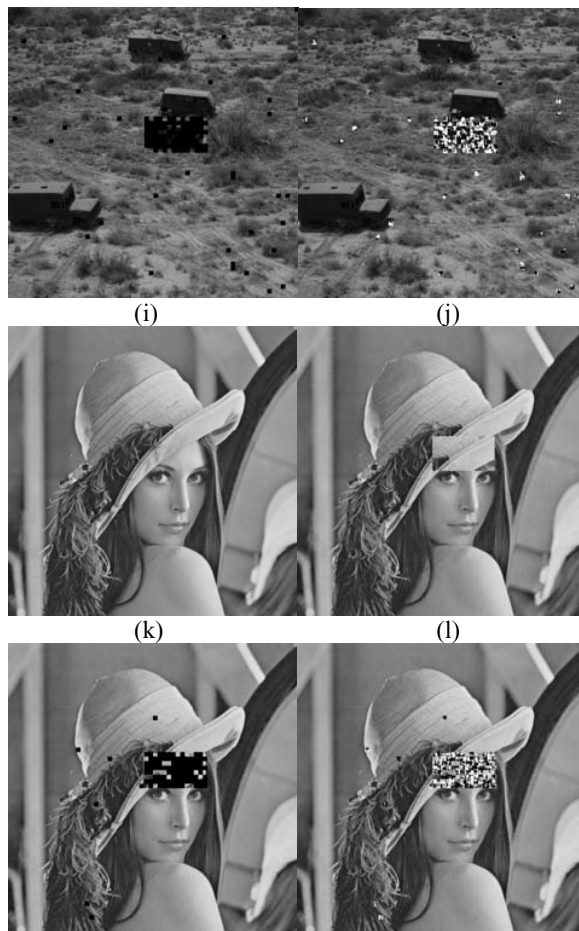
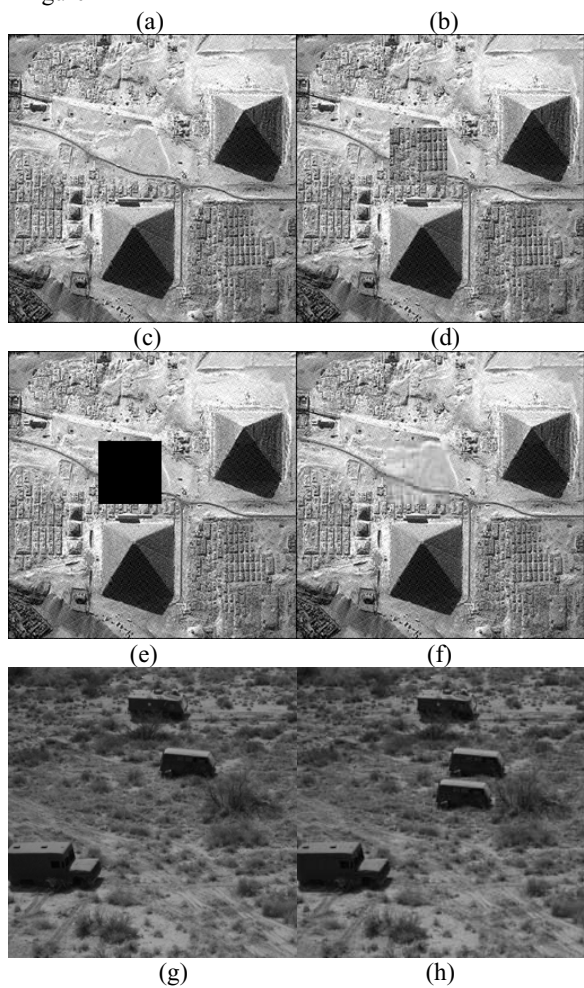
## References

- [1] Zhu, X., Ho, A.T.S. and Woon, W. M. (2006), “A semi-fragile pinned sine transform watermarking system for content authentication of satellite images”, *Geoscience and Remote Sensing Symposium, 2005. IGARSS '05.*

*Proceedings. 2005 IEEE International*, Vol. 2, pp. 25-29, Digital Object Identifier

- [2] Fridrich, J. and Goljan, M. (1999), "Images with self-correcting capabilities" in *IEEE International Conf. on Image Processing*, Kobe, Japan
- [3] Zhu, X., Ho, A.T.S. and Marziliano, P. (2007), "Semi-fragile Watermarking Authentication and Restoration of Images Using Irregular Sampling," *Accepted for publication in EURASIP Signal Processing: Image Communication*
- [4] Pratt, W.; Wen-Hsiung Chen; Welch, L. (1974), "Slant Transform Image Coding", *Communications, IEEE Transactions on [legacy, pre - 1988]*, Vol, 22, Issue 8, pp.1075 – 1093
- [5] Zhu, X.; Ho, A.T.S. (2003), "A slant transform watermarking for copyright protection of satellite images", *Information, Communications and Signal Processing, 2003 and the Fourth Pacific Rim Conference on Multimedia. Proceedings of the 2003 Joint Conference of the Fourth International Conference on Vol. 2*, 15-18, pp.1178 - 1181 vol.2

Figure 4



- (a) Watermarked Image
- (b) Attacked Image
- (c) Authenticated Image
- (d) Recovered Image
- (e,i) Watermarked Image
- (f,j) Attacked Image with 75% QF
- (g, k) Authenticated Image 75% QF
- (h,l) Recovered Image 75% QF