International Journal of Electronic Networks, Devices and Fields.
ISSN 0974-2182 Volume 8, Number 1 (2016), pp. 7-11

http://www.irphouse.com

Noise attacks using Discrete Cosine Transform Domain

Neelam Turk
Electronics Engineering Department,
YMCA University of Science and Technology
Faridabad-121006 (Haryana)

Abstract

The increasing popularity of the internet means that digital multimedia is transmitted more rapidly and easily. And people are very aware for media ownership. However, digital watermarking is an efficient and promising means to protect intellectual properties. Based on the intellectual property attention in the information era, how to protect the personal ownership is extremely important and a necessary scheme. In this paper, we propose an effective video watermarking method based on a discrete cosine transform (DCT) against several attacks. Experimental results demonstrate that the watermark isrobust to various attacks.

1. Introduction

Models describe relationships between measured signals. It is convenient to distinguish between input signals and output signals, such that the outputs are partly determined by the inputs. For example, consider an airplane where the inputs are control surfaces, such as ailerons and elevators, and the outputs are the orientation, velocity, and position of the airplane. In most cases, the outputs are also affected by signals other than the measured inputs. Such unmeasured inputs are called disturbance signals or noise. For the airplane, these additional signals would be wind gusts and turbulence effects.

Noise amplification is a common problem of maximum likelihood methods that attempt to fit data as closely as possible. After much iteration, the restored image can have a speckled appearance, especially for a smooth object observed at low signal-to-noise ratios. These speckles do not represent any real structure in the image, but are artifacts of fitting the noise in the image too closely. To control noise amplification we are using a key and then subtracting the noisy image from the watermarked image. For pixels that deviate in the vicinity of their original values, iterations are suppressed. First of all, we have to distinguish two “reasons” or “Purposes” for an attack against a watermark image:

- Hostile or malicious attacks, which are an attempt to Weaken, remove or alter the watermark, and
- Coincidental attacks, which can occur during common image processing and are not aimed at tampering with the watermark.

2. Proposed Noise or Attacks

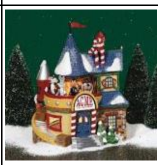
The proposed attacks are as follows: Speckle Noise, Poisson Noise, Gaussian Noise, Salt & Pepper Noise, JPEG image compression.

3. Noise And Quality Measures

3.1 Noise Attacks on watermarked image:To detect the watermarked attacked we test the robustness of the proposed watermarking scheme, seven watermark removal attacks are applied to the watermarked image. The severity of these attacks can be adjusted by modifying their corresponding parameter values. Different watermark attacks have different coefficient to detect.

3.2 Quality measure: The peak signal-to noise rat io (PSNR) was used as a measure of the quality of a watermarked image. To evaluate -the robustness of the proposed approach, the watermarked image was tested against five kinds of attacks: MSE, PSNR, NCC of the images to check the robustness of the watermarked images, are calculated .

Table I: DCT watermarked images with various attacks

Type of attacks	House (256x256)	Baby (256x256)	YMCA (256x256)	Bangles (256x256)
No attack	 (Size--15.6 kb)	 (10.8 kb)	 (12.4 kb)	 (9.82 kb)
Speckle Noise (Mean=0, Var.=0.02)	 (15.7 kb)	 (12.7 kb)	 (14.4 kb)	 (12.2 kb)
Poisson Noise (Mean=0, Var.=0.02)	 (17.1 kb)	 (15.5 kb)	 (16.1 kb)	 (14.2 kb)
Salt &Pepper Noise (Noise Density=.02	 (16.3 kb)	 (11.9 kb)	 (13.8 kb)	 (11.4 kb)

Gaussian Noise (Mean=0, Var.=0.02)	 (17.8 kb)	 (13.9 kb)	 (14.8 kb)	 (12.9 kb)
JPEG compression Quality-100	 (50.8 kb)	 (42.9 kb)	 (51.6 kb)	 (46.7 kb)
JPEG compression Quality-50	 (11.4 kb)	 (7.22 kb)	 (9.12 kb)	 (7.02 kb)

Table II: DCT MSE between the noised watermarked image and the cover image

S. No.		House (MSE)	Baby (MSE)	YMCA (MSE)	Bangles (MSE)
1.	Speckle(0,0.002)	23.69	73.78	65.30	58.01
2.	Poisson(0,0.02)	80.914	176.03	138.18	125.38
3.	Salt & Pepper(0.002)	49.1023	46.16	54.18	62.50
4.	Gaussian(0,0.002)	102.85	119.35	89.67	87.36
5.	JPEG compressionQ-100	1.83	1.52	1.91	2.24
	JPEG compressionQ-50	5.52	3.5	4.46	4.28

Table II: DCT PSNR between the noised watermarked image and the cover image

S. No.	Noise	House PSNR (db)	Baby PSNR (db)	YMCA PSNR (db)	Bangles PSNR (db)
1.	Speckle(0,0.002)	34.38	29.45	29.98	30.49
2.	Poisson(0,0.02)	29.05	25.67	26.72	27.15
3.	Salt & Pepper(0.002)	31.22	31.48	30.79	30.18
4.	Gaussian(0,0.002)	27.31	27.36	28.60	28.72
5.	JPEG compression Q-100	43.34	44.92	43.12	41.50
	JPEG compression Q-50	33.29	37.48	35.22	35.58

Table IV: DCT Recovered watermarks and their correlation coefficient NCC with the original watermark

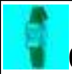
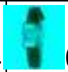
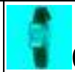
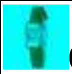
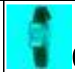
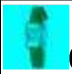
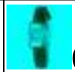
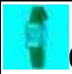
S. No.	Noise	House(db)	Baby (db)	YMCA(db)	Bangles(db)
1.	Speckle (0,0.002)	 0.8984	 0.866	 0.6392	 0.7161
2.	Poisson (0,0.02)	 0.8935	 0.7702	 0.5474	 0.5489
3.	Salt & Pepper (0.002)	 0.8663	 0.856	 0.6772	 0.8340
4.	Gaussian (0,0.002)	 0.8329	 0.861	 0.6224	 0.7645
5.	JPEG compressionQ-100	0.69867	0.8313	0.5462	0.7190
	JPEG compression Q-50	0.3451	0.3668	0.4330	0.3245

Table V: DCT—correlation co-efficient NCC between the recovered watermark from compressed watermarked image and filtered watermark

S.No.	Compression type	House	Baby	YMCA	Bangles
1.	JPEG compressionQ-100	0.69867	0.8313	0.5462	0.7190
	JPEG compressionQ-50	0.3451	0.3668	0.4330	0.3245

4. Results

The tool used for the execution of this algorithm is 'Matlab'. Finally, the images are separated from the concatenated recovered watermarked image. Thus, the original base and watermark images are recovered. They are saved as 'Recovered Base Image.jpg' and 'Recovered Watermark Image.jpg'.

The peak signal-to noise ratio (PSNR) was used as a measure of the quality of a watermarked image. To evaluate the robustness of the proposed approach, the watermarked image was tested against five kinds of attacks:

The DCT based watermarking schemes were tested using five attacks. The chosen attacks were Speckle noise, Salt & pepper noise, Poisson noise, Gaussian noise, JPEG image compression of quality 100,50.

5. Conclusion

This paper implemented watermarking algorithms using MATLAB based on Discrete Cosine Transform(DCT).The capability of watermarking algorithm is robust to salt and pepper, Poisson and speckle, but somewhat weaker to Gaussian Noise. The identification of useful features from compressed data for the watermark to be embedded is typically difficult because each compressed technique poses additional constrains, e.g. nonlinear processing, rigid data structure syntax, and so forth. The compressed-domain approach provides significant advantages but also brings new challenges.. The results of experiments show that this approach is very promising, because it is robust to common image processing distortions.

References

[1] K. K. Wong, C. H. Tse, K. S. Ng, T. H. Lee and L. **M.** Cheng, "Adaptive watermarking", IEEE transactions on consumer electronics, Vol. 43, No. 4,November 1997.

[2] Young Jin Nam and ChanikPark ,"An Adaptive High-Low Water Mark Destage Algorithm for Cached RAID5",Pacific Rim International Symposium, IEEE, 2002.

[3] Sheng Huang and Jian Kang Wu, "Optical Watermarking for Printed Document Authentication", IEEE , Vol. 2,No. 2,June 2007

[4] P.Vidyasagar , S. Han and E. Chang. "A survey of digital image watermarking techniques”, 3rd IEEE International Conference on Industrial Informatics (INDIN 2005), edited by T. Dillon, X. Yu. and E. Chang, pp. 495-502, Perth, Western Australia, 2005.

[5] A. Khan and A.M. Mirza, “Genetic perceptual shaping: utilizing cover image and conceivable attack information during watermark embedding”. Inf. Fusion, Vol. 8, pp. 354-365, Oct. 2007.

s