Video Watermarking Algorithm based on Combined Transformation and Digital Holography

De Li[1], XueZhe Jin[1] and Jongweon Kim[2]
[1]*Department of Computer Science, Yanbian University, 133002, Yanji, China*
[2]*Department of Contents and Copyright, Sangmyung University, 03016, Seoul, Korea*

Keywords: Digital Hologram, 2D DWT, 3D DCT, DFRNT.

Abstract: Recent researches of robust digital watermarking are focused on the processing method in frequency field. Most of those algorithms are limited on one transform domain or combine different kinds of transform field together. In this paper, a new video watermarking algorithm is proposed, which is applied in 2D DWT and 3D DCT combined with Discrete Fraction Random Transform (DFRNT) encryption and digital holography respectively. The embedded information is applied in 2D bar-code which obtained from holograph. Extraction of the watermark uses the tech of holographic reconstruct. The results of experiment show that the proposed watermarking algorithm has a good performance of robustness and security.

1 INTRODUCTION

With the rapid development of Internet, more and more people share information and it is easier to store, copy and transmit the multi-media data than before. The evolution of network brings the great advancement of the information society but it also causes some challenges such as copyright protection. More and more researchers pay high attention to solve the digital copyright issues and it is not acceptable to distort, transmit and invade copyrighted material. The anti-attack watermarking algorithm for video is proposed in this paper. It shows good performance of concealing , anti-attack and security.

Newly developed digital watermarking algorithms are, wavelet transform with Singular Value Decomposition (SVD) (Bao, 2005), spread spectrum based on HVS (Zolghadrashli, 2007), Pseudo-3-D DCT and Quantization (Huang, 2010), 1D Discrete Fourier Transform (DFT) and Radon Transform (Liu, 2010), compression domain method (Ling, 2010. Gujjunoori, 2013) and adaptive method like Particle Swarm Optimization (PSO) (Margarita, 2009. Wang, 2010). Most recent watermarking algorithms applying binary or gray image for watermarking have limitation in the quantity of embedded information. Besides, various attacking methods have been developed constantly. Based on these researches, it was proposed that combine the optical technology such as visual optic with digital holography into the watermarking algorithm and got some positive achievement (Liang, 2006). But it was still not a perfect method which can resist all kinds of attack with strong performance of security. So, a video watermarking algorithm with robustness and security is hot issue. This paper proposes an algorithm that combine the tech of combined frequency domain processing, random exchange of discrete fraction and digital holography together.

2 CORRELATION THEORIES

2.1 Digital Holography

Digital holography is a tech that applying CCD to exchange board to record holography image and emulating diffraction to reconstruct the image. The whole reconstructing process contains record, store, process and reproduce. Recent researches focus on optical technology combining with information security. Especially, the field of digital watermarking has great potential. In 2002, Takai and his team (Takai, 2002) proposed an algorithm of digital holography getting the watermarking image, which is measured by holography tech and embed the watermark immediately in space domain and

Li, D., Jin, X. and Kim, J.
Video Watermarking Algorithm based on Combined Transformation and Digital Holography.
DOI: 10.5220/0005749803790383
In *Proceedings of the 11th Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2016) - Volume 3: VISAPP*, pages 381-385
ISBN: 978-989-758-175-5

recover the original watermarking image. But the robustness of their algorithm will deteriorate if the image is under a low-pass filtering attack. Except low-pass filtering attack, the digital holography has good characteristics of encryption, irrevocability and cropping.

Figure 1 is the process of computer-generated hologram.

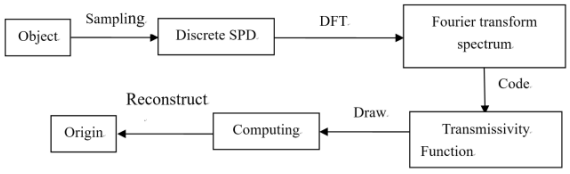
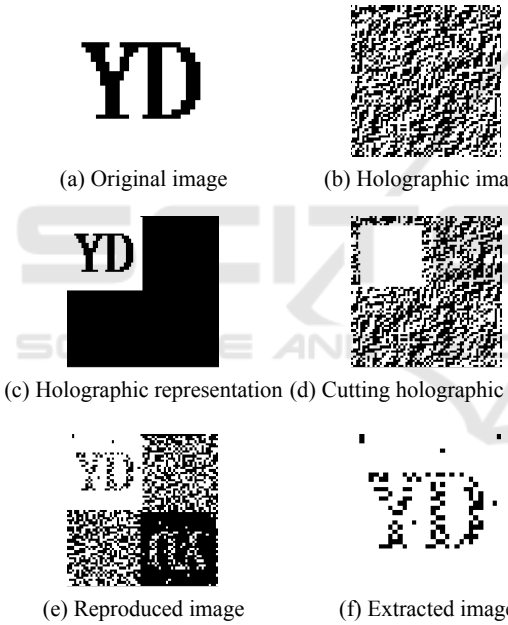


Figure 1: Process of computer-generated hologram.

Figure 2 shows generation and reconstruction of the hologram.



(a) Original image (b) Holographic image

(c) Holographic representation (d) Cutting holographic image

(e) Reproduced image (f) Extracted image

Figure 2: Generation and reconstruction of the hologram.

2.2 Random Exchange of Discrete Fraction

The method of Random Exchange of Discrete Fraction Transform(REDFT) is based on DFT and it has better mathematical performance than DFT. It can be satisfied in linearity, unitarity, additivity, cyclicity and self-randomicity (Zhang, 2012).

The 1D and 2D signal of REDFT can be expressed as below.

$$X^{\alpha} = R^{\alpha}x \tag{1}$$

$$Y^{\alpha} = R^{\alpha}y[R^{\alpha}]^{T} \tag{2}$$

R^{α} is the kernel matrix of REDFT.

$$R^{\alpha} = \mathrm{V}D^{\alpha}(V)^{T} \tag{3}$$

α is factorial of discrete fraction, T is the cycle time of α, D^{α} is a diagonal matrix which represent a group of eigenvalues $\{\exp\left(-\frac{2\mathrm{i}\pi\mathrm{n}\alpha}{\mathrm{T}}\right) : \mathrm{n} = 0,1,2,\dots,\mathrm{N}-1\}$.

D^{α} can be expressed as formula(4).

$$diag\left[1, \exp\left(-\frac{2i\pi\alpha}{T}\right), \dots, \exp\left(-\frac{2(N-1)i\pi\alpha}{T}\right)\right] \tag{4}$$

The matrix V is formed from the eigenvector $\{V_1, V_2, \dots, V_N\}$ and the eigenvector can be get from Schmidt standard normalization.

Matrix V can be expressed as equation (5).

$$\mathrm{V} = [V_1, V_2, \dots, V_N] \tag{5}$$

V_N is eigenvector of diagonal random matrix Q and Matrix Q can be get from N × N random matrix P.

$$\mathrm{Q} = (\mathrm{P} + P^{T})/2 \tag{6}$$

Matrix V satisfied below relation.

$$VV^{T} = I \tag{7}$$

The result of the transform will differentiate by the matrix P and the eigenvector is random vector. The random matrix contains N(N+1)/2 isolated elements and the security can be expressed as 2N(N+1)/2. It means the method itself is an encryption procedure and the key is very difficult to decipher. Even though the adversary knows the transform procedure, there is little possibility of obtaining the embedded information.

3 WATERMARKING ALGORITHM AND RESULTS ANALYSIS

3.1 Watermarking Algorithm

If the watermark is embedded in high frequency field less sensitive for visual, it will be damaged during the attack of transmission. On the contrary it is embedded in low frequency field, the quality of the image will deteriorate. The proposed algorithm will choose an intermediate field to embed the watermark information. The algorithm uses 2D wavelet transform and 3D DCT first and performs DFRNT scramble to get the watermark information. The robustness and security of the algorithm has

improved by the technology of off-axis holography.

The process of the algorithm is shown in figure 3.

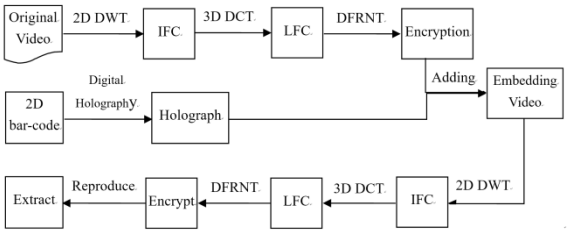


Figure 3: Process of the algorithm.

3.2 Experimental Results and Analysis

The original video for this experiment is 100 frames which are uncompressed and the image size for watermarking is 21×21 2D barcode image. Bit Error Rate (BER) performance evaluations are measured applying various attacks.

(1) Gaussian noise attacks

Table 1: Experimental results of Gaussian noise attacks.

Variance	Result	Extraction	BER
0.001			0.00
0.005			0.01
0.01			0.05

Table 1 shows that the video frame is not enough clear after Gaussian noise attack but we can extract the watermarking. It means that the algorithm can resist the Gaussian noise attack.

(2) Salt & pepper noise attacks

Table 2: Experimental results of salt & pepper noise attacks.

Density	Result	Extraction	BER
0.005			0.00
0.01			0.02
0.05			0.06

Table 2 shows that the extraction of watermarking still works enough after the salt & pepper attack. It means the algorithm has a good performance to resist salt & pepper attack.

(3) Low-pass filtering attack

Low-pass filtering attack impairs the edge of the video frame so that the image is blurred.

Table 3: Experimental results of low-pass filtering attacks.

Frequency	Result	Extraction	BER
55			0.04
75			**0.02**
95			0.00

Table 3 shows that the filtering attack has little effect on the quality of the video frame.

(4) Rotation attack

During the transmission, the video file can be attacked by rotation. In this paper, the angle of rotation attack is from 1 to 90 degrees.

Table 4: Experimental results of rotation attacks.

Rotation angle	Result	Extraction	BER
10°			0.05
45°			0.13
60°			0.10

Table 4 shows that the extraction of the watermark can be performed successfully in three cases of rotation angle: 10, 45 or 60 degrees.

(5) Frame attack

Frame attack is exchange the order of frame, add or delete frame so that the user can not be able to get the correct video file. Test results of robustness to frame attack is shown in table 5.

Table 5: Experimental results of frame attacks.

Frame exchange	Extraction	BER
$1^{st} \leftrightarrow 9^{th}$		0.00
$5^{th} \leftrightarrow 21^{st}$		0.01
$29^{th} \leftrightarrow 53^{rd}$		0.02

Table 5: Experimental results of frame attacks (cont.).

Lost frames	Extraction	BER
3		0.00
5		0.01
15		0.02

(6) Compression attack

Most video files on Internet are compressed by MPEG. The compressed video file in MPEG has a good performance but the loss of information cannot be avoid 100%. MPEG-4 compressed video files are tested and the performance is evaluated. Table 6 shows the result of compression attack by different bit rate. Even if the bit rate goes up to 500Kbps, the extraction still can be clear to clarify.

Table 6: Experimental results of compression attacks.

Standard	MPEG-4	
Bit rate	256Kbps	512Kbps
Extraction		
BER	0.19	0.07

The experimental results show that the algorithm combining DFRNT with digital holography has a good performance to endure all kinds of attack and the encryption feature of DFRNT provide a good security than other algorithm.

4 CONCLUSIONS

The proposed algorithm shows good performance of robustness and security. The algorithm combines 2D wavelet transform and 3D DCT and then apply DFRNT for scramble. During the construction of watermarking the 2D bar-code information will be added to the video file as the mode of holography image. The extraction of watermarking takes holograph-reproduce which can improve security of the algorithm. The result of experiment shows good performance to various attacks and reasonable improvement of robustness and security.

ACKNOWLEDGEMENTS

This research is supported by Ministry of Culture, Sports and Tourism(MCST) and Korea Creative Content Agency(KOCCA) in the Culture Technology(CT) Research & Development Program 2015.

REFERENCES

P, Bao. and X, Ma. 2005. Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition. *IEEE Transactions on Circuits and Systems for Video Technology*, 15:96~102.

A, Zolghadrashli. and S. Rezazadesh, 2007. Evaluation of Spread Spectrum Watermarking Schemes in the Wavelet Domain Using HVS Characteristics. *International Journal of Information Science and Technology*, 5(2):1~4.

Huang Hui-Yu, Yang Cheng-Han, H. Wen-Hsing, 2010. A Video watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation. *Transaction on Information in Forensics and Security*, 5(4):625-637.

Y. Liu, J. Y. Zhao, 2010. A New Video Watermarking Algorithm Based on 1D DFT and Radon Transform. *Signal Processing*, 90(2): 626~639.

H. Ling, L. Wang, F. Zou, 2011. Robust Video Watermarking Based on Affine Invariant Regions in the Compressed Domain. *Signal Process*, 91(8): 1863~1875.

S. Gujjunoori, B. B. Amberker, 2013. DCT Based Reversible Data Embedding for MPEG-4 Video Using HVS Characteristics. *Journal of Information Security and Applications*, 18(4): 157~166.

S. Margarita, O. Gabrieda, N. Shawn, 2009. A PSO/ACO Approach to Knowledge discovery in a pharmacyo vigilance context. *Proceedings of the 11th Annual Conference Companion on Genetic and Evolutionary Computation Conference.* Montreal, Canada, 2679~2684.

Y. G. Wang, L. Fan, Y. Q. Lei, 2010. PSO-Based Robust Watermarking of AVS-Encoded Video. *Proceedings of the 2010 IEEE International Conference on Multimedia and Expo (ICME 2010)*. Singapore, 1647~1650.

Yuchi Liang, Gu Jihua, Liu Wei, Tao Zhi, 2006. An Image Digital Watermark Technique Based on Digital Holography and Discrete Cosine Transform. *Journal of Optics*, 26(3): 355~361.

N. Takai, Y. Mifune, 2002. Digital Watermarking by a Holographic Technique. *Applied Optics*, 41(5): 865~873.

Zhang Wen-quan, Zhou Nan-run, 2012. Double-color Image Encryption Based on Discrete Fractional Random Transform. *Journal of Electronics&Information Technology*, 34(7): 1727~1734.