

Robust volume data watermarking based on perceptual hashing

Yujia Li, Jingbing Li*

College of Information Science and Technology, Hainan University, Haikou, China, 570228

Received 1 March 2014, www.cmmt.lv

Abstract

This paper proposed a perceptual hashing algorithm of robust blind watermarking method for volume data. Which address the problems of authentication and protection of personal information. The scheme obtains the feature vectors of volume data and quantizes them to generate the hash value of the volume data. By combining the concept of zero-watermarking, the algorithm for watermarking of volume data that is robust to geometric attacks. The experimental results demonstrate that the proposed algorithm has good invisibility and robustness

Keywords: watermarking, perceptual hashing, volume data, DFT

1 Introduction

With the progress of computer technology, the application of multimedia has a qualitative leap. But security concerns over copyright violation of multimedia data have also increased at the same time. On the one hand multimedia data can faster and more efficient transmitted in public network [1], on the other hand intercept and manipulation of the multimedia information has also become very easy [2]. Thus, the information security of multimedia data has attracted a lot of attention during the last few years.

Digital watermarking is an efficient tool for multimedia information protection [3]. However, the directions of research have been mostly in image [4], audio [5] and video watermarking [6]. Currently, there are a lot of volume data in real life. Such as most of the medical image (CT, MRI, etc.) is volume data, so study how to embed the digital watermarking in the volume data is significant. The volume data is not allowed to modify the content in principle [7]. As a result, to embed watermarking in volume data is difficult. Discrete cosine transform (DCT) [8], Discrete Fourier transform (DFT) [9] and discrete wavelet transform [10,11] are used in embedding watermarking of volume data. But the robustness of the algorithms is not very ideal. Wu [12] develop an algorithm based on the spread-spectrum communication technique to watermarking a volume data which is invisible and robust. However, the original volume data is needed in watermarking detection. It's not blind watermarking.

In allusion to invisible and robust Image Watermarking, there are a series of requirements. First, we hope the embedding of watermarking could not change the original image [13]. What is more, the watermarking must have good robustness and invisible. At last, we wish the capacity of watermarking is bigger. Whereas to the

traditional digital watermarking algorithm, difficult to achieve all requirements at a time.

In this paper, we propose a watermarking algorithm based on perceptual hashing which is a blind multi-watermarking algorithm and also can achieve a true embedded zero-watermarking [14]. The experiment results demonstrate that the algorithm has good robustness.

2 Theoretical background

2.1 THE 3D DISCRETE FOURIER TRANSFORM

The discrete Fourier transform is an important mathematical tool on the engineering application. Assuming the size of volume data is $X \times Y \times Z$. The corresponding 3D-DFT is done using:

$$F(u, v, w) = \sum_{x=0}^{X-1} \sum_{y=0}^{Y-1} \sum_{z=0}^{Z-1} f(x, y, z) \cdot e^{-j2\pi xu/X} e^{-j2\pi yv/Y} e^{-j2\pi zw/Z}, \quad (1)$$

$$u = 0, 1, \dots, X-1; v = 0, 1, \dots, Y-1; w = 0, 1, \dots, Z-1.$$

The corresponding volume data's inverse discrete Fourier transform (IDFT) is computed using:

$$f(x, y, z) = \frac{1}{XYZ} \sum_{u=0}^{X-1} \sum_{v=0}^{Y-1} \sum_{w=0}^{Z-1} F(u, v, w) \cdot e^{j2\pi xu/X} e^{j2\pi yv/Y} e^{j2\pi zw/Z}, \quad (2)$$

$$x = 0, 1, \dots, X-1; y = 0, 1, \dots, Y-1; z = 0, 1, \dots, Z-1.$$

Note that in our case $f(x,y,z)$ is the value at the point (x,y,z) of the volume data, $F(u,v,w)$ is the three-dimension DFT coefficient at the point (u,v,w) in frequency domain. Volume data is composed of many layers of slices, each slice is a two-dimensional image. The size of image is $M \times N$, the number of slice's layers is P .

*Corresponding author e-mail: Jingbingli2008@hotmail.com

2.2 PERCEPTUAL HASHING

In 2001, Kalker first proposed the concept of perceptual hashing. A majority of existing algorithms follow a three-step framework to generate a hash value [15], as illustrated in Figure 1.

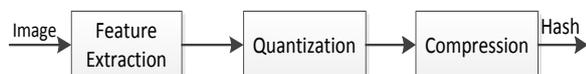


FIGURE 1 An example. Good quality with clear lettering

Perceptual hashing is a class of one way mappings from multimedia presentations to a perceptual hash value in terms of their perceptual content [16]. Perceptual hashing algorithm can transform volume data into binary sequences, and can be used to database search, content authentication, and watermarking [17-21]. The characteristics of the perceptual hashing function are robustness, collision resistance, compactness and one-wayness [16,22-25]. The specific method of perceptual hashing algorithm used in this paper was as follow:

Step 1: 3D-DFT to the volume data;

Step 2: 3D-IDFT to the precious 4×4×4 DFT coefficients;

Step 3: Calculate the average value of the real part of 4×4×4 IDFT coefficients.

Step 4 Compare the each IDFT real coefficient with the average. Greater than or equal to the average, recorded as 1. Less than the average, recorded as 0.

Step 5 Group the comparison result of the previous step together to constitute a 64 bits binary sequence, which is the hash value of the volume data. Group order is not important, as long as the order of all volume data using the same.

3 The watermarking algorithm

We choose a set of binary pseudo-random sequence B_g , $B_g = \{bg(i) | bg(i) = 0, 1; 1 \leq i \leq L\}$ represents information as multi-watermarking. Then, we select one MRI medical volume data as the original volume data which is describe as $F = \{f(i, j, k) | f(i, j, k) \in R; 1 \leq i \leq M, 1 \leq j \leq N, 1 \leq k \leq P\}$, where $w(j)$ and $f(i, j, k)$ represent the pixel gray-values of watermarking and the voxel values of the original volume data similar to the pixel gray-values of 2D image. To facilitate the operation, we assume $M1=M2=M, N1=N2=N$.

3.1 HASH VALUE EXTRACTION METHOD OF VOLUME DATA

Though the above method of perceptual hashing, we can extract the hash value of the volume data. That is to say: first, we use the 3D-DFT to the original medical volume data by the geometric transformation on each slice. We select the previous 4×4×4 coefficients. Then, the selected coefficient is computed using 3D-IDFT. We recognize the real part of IDFT coefficients as the feature vector of the volume data. Then, through the comparison of feature vector and the real part coefficients average realize binary quantization. At last, we can generate the hash value of volume data.

In order to prove that the robustness of the hash value, which we select above. We randomly choose 8 coefficients of the feature vector ($F(1,3,4), F(1,4,1), \dots, F(4,3,4), F(4,4,1)$), which show in Table 1 We can see that the value of the corresponding coefficients have changed after the volume data has undergone an attack (which is show in Figures 2 and 3) as illustrated in column “L2-L9”. But the hashing value unchanged, as shown in Table 1. It can be seen that the normalized cross-correlation (NC) between the hashing values is equal to 1.0, as shown in column “L12”. Therefore, the hash value can meet the perceptual robustness.

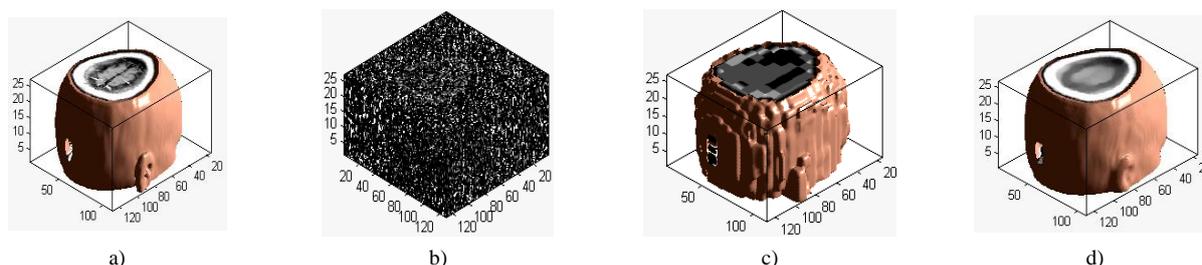


FIGURE 2 Different common attacks: a) Original volume data; b) Gaussian noise (10%); c) JPEG compression 2%); d) Median filter ([5×5])

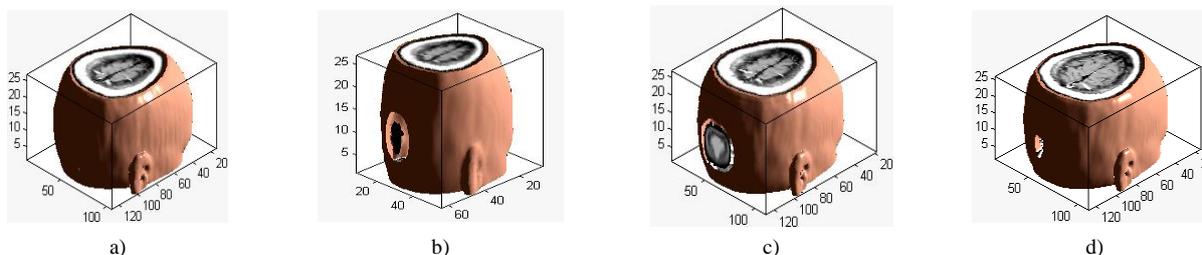


FIGURE 3 Different geometric attacks: a) Rotation (10°); b) Scaling (0.5 times); c) Translation (3%, down); d) Cropping (3%, from z direction)

TABLE 1 The change that the real part of IDFT coefficients with different attacks

L1	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12
Processing method	F(1,3,4)	F(1,4,1)	F(2,3,4)	F(2,4,1)	F(3,3,4)	F(3,4,1)	F(4,4,4)	F(4,4,1)	average	Hash value	NC
Original volume data	1.194	0.463	2.445	1.466	2.760	2.093	2.882	1.262	1.508	00101110	1.0
Gaussian noise (10%)	3.031	2.506	3.778	3.139	3.978	3.587	4.076	3.028	3.195	00101110	1.0
JPEG compression (2%)	1.239	0.525	2.520	1.548	2.784	2.132	3.008	1.314	1.575	00101110	1.0
Median filter [5×5]	1.177	0.463	2.478	1.474	2.756	2.139	2.911	1.212	1.508	00101110	1.0
Rotation (10°)	1.039	0.475	2.470	1.415	2.813	1.987	2.954	1.066	1.508	00101110	1.0
Scaling (×0.5)	0.290	0.113	0.613	0.368	0.695	0.514	0.726	0.304	0.378	00101110	1.0
Translation (down 3%)	1.400	0.469	2.356	1.340	2.687	2.100	2.828	1.373	1.507	00101110	1.0
Cropping (3% from x)	1.232	0.423	2.412	1.431	2.669	2.044	2.818	1.290	1.476	00101110	1.0
Cropping (3% from y)	1.462	0.481	2.393	1.399	2.648	2.053	2.758	1.348	1.504	00101110	1.0
Cropping (3% from z)	1.203	0.531	2.396	1.529	2.689	2.249	2.781	1.471	1.508	00101110	1.0

The unit of real part coefficients is 1.0e+005

Collision resistance is one of the important properties of perceptual hash value. Collision resistance means that there is large difference the hash value of two no similar images. In order to further illustrate the perception of the hash value, we select some different volume data as test objects which are shown in Figure 4. Calculate the NC between hash values of different test objects, as illustrated in Table 2.

In Table 2, we can see that the NC is largest between volume data itself, which is 1.00. The NC of a and b is larger, because a and b are brain volume data. The other

NC values are small, which are all less than 0.5. That is observed with our human eyes. Therefore, collision resistance of the hash value in our algorithm is good.

TABLE 2 The NC between test volume data

NC	a	b	c	d	e
a	1.00	0.61	-0.04	-0.47	0.20
b	0.61	1.00	0.21	-0.39	0.21
c	-0.04	0.21	1.00	-0.05	0.12
d	-0.47	-0.39	-0.05	1.00	0.18
e	0.20	0.21	0.12	0.18	1.00

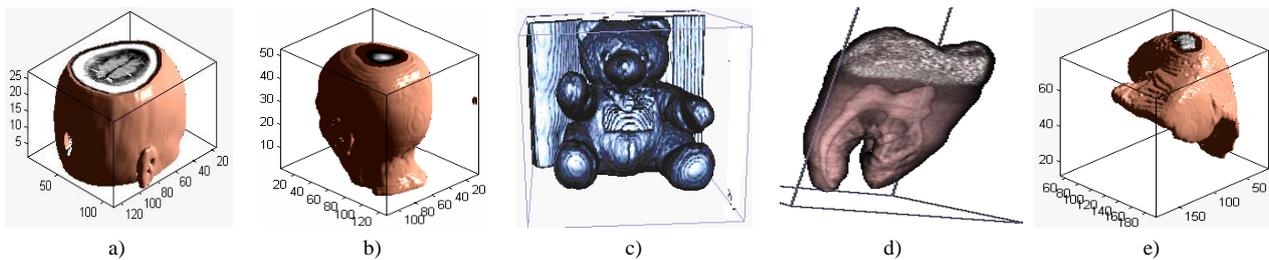


FIGURE 4 Different volume data which are test objects

3.2 EMBEDDING WATERMARKING

Step 1: Acquire the hash value of the original volume data. In his section, we use the proposed perceptual hashing algorithm to the original volume data. Through volume data's feature extraction and binary quantization process, and then, we can get the hash value of the original volume data:

$$FF_4(i, j, k) = DFT3(F(i, j, k)), \tag{3}$$

$$FIF(i, j, k) = IDFT3(FF_4(i, j, k)), \tag{4}$$

$$RIF(i, j, k) = REAL(FIF(i, j, k)), \tag{5}$$

$$H(j) = BINARY(RIF(i, j, k)). \tag{6}$$

Step 2: Utilizing the HASH function of cryptograph, the logical sequence can got by us, $Key^s(j)$:

$$Key^s(j) = H(j) \oplus B^s(j), \tag{7}$$

where $H(j)$ is the hash value of volume data, B^s is the multi-watermark sequence. $Key^s(j)$ is a binary sequence. The $Key^s(j)$ is necessary to extract the watermarking, it would be saved. Moreover, we can take the $Key^s(j)$ for a secret key. In order to protect the copyright of the original volume data, we should registered the $Key^s(j)$ at the third part. In addition, during the watermarking embedding, the original volume data change a little. It's one of the zero-watermarking technologies.

3.3 EXTRACT WATERMARKING

Step 3: Acquire the hash value of the tested volume data. The perceptual hashing method is also performed on the test volume data $F'(x, y, z)$. As the same as Step 1, we can acquiring the hash value $H'(j)$.

$$FF'_4(i, j, k) = DFT3(F'(i, j, k)), \tag{8}$$

$$FIF'(i, j, k) = IDFT3(FF'_4(i, j, k)), \tag{9}$$

$$RIF'(i, j, k) = REAL(FIF'(i, j, k)), \tag{10}$$

$$H'(j) = \text{BINARY}(RIF'(i, j, k)), \tag{11}$$

Step 4: Utilizing the binary sequence $Key^s(j)$ and the hash value of tested volume data $H'(j)$, we can extract the watermarking $B^{s'}(j)$:

$$B^{s'}(j) = H'(j) \oplus Key^s(j), \tag{12}$$

$B^{s'}(j)$ describe the extracted multi-watermarking, can be also computed by the HASH function of cryptography. $Key^s(j)$ are obtained from Step 2.

3.4 WATERMARKING EVALUATING ALGORITHM

By calculating NC to determine whether it is embedded watermarking or not. We use NC to measuring the quantitative similarity between the extracted and embedded watermarking. The higher the value of NC is, the more approximation between the extracted watermarking $B^s(j)$ and the embedded watermarking $B^{s'}(j)$. Defined as:

$$NC = \frac{\sum_j B^s(j) B^{s'}(j)}{\sum_j B^s(j) B^s(j)}. \tag{13}$$

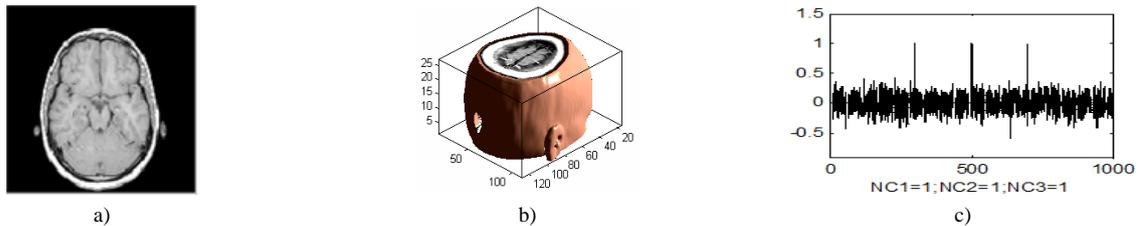


FIGURE 5 No attacking on watermarking: a) a slice of original volume data; b) the original volume data; c) watermarking detector

4.1 COMMON ATTACKS

In general, common attacks are common image processing. For example: Gaussian noise, digital to analogue and analogue to digital conversion, quantization and requantization, JPEG, median filtering and so on.

4 Experiment results on robustness of the watermarking algorithm

We have implemented the volume data watermarking algorithm in Matlab2010a platform to verify the effectiveness. In these experiments, we should do these with the help of a thousand groups of independent binary pseudo-random sequences as used. Every sequence consists of 64 bits. In the experiment, the 300th, the 500th and the 700th group are selected at random from the thousand groups as the embedded watermarking. The size of the volume data (MRI.mat) is $128 \times 128 \times 27$, which is offered in matlab.

It can be seen visually from Figure 5 that the quality of the volume data embedded has hardly any change. The quality of extracted watermarking is of high-quality with no difference with the original in normal case, all the NC are 1.0, which is shown in Figure 5a. (no attacking on watermarking)

The following are several types of common and geometric attacks to test the robustness of the algorithm. By attacks on each slice to achieve the purpose that an attack on the volume data in this experiment.

4.1.1 Gaussian noise

Figures 6a and 6b show the slice and volume data with the Gaussian noise (10%), respectively. As the Figure 6c shows, the PSNR is 3.30dB, and the multi-watermarking sequence can be detected, all of the NC are 1.00. Different parameters of noise impact on the volume data. The corresponding different PSNR and NC are given in Table 3. The result shows the value of NC is when the noise parameter top to 25%. Therefore, our algorithm has strong robustness against noise attacks.

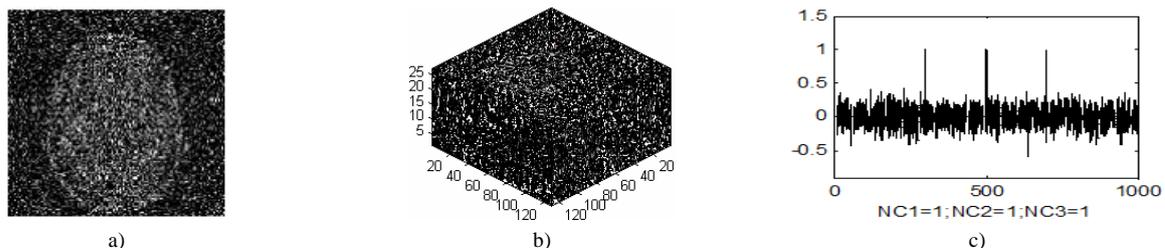


FIGURE 6 With noise attack: a) a slice with noise attack; b) the corresponding volume data; c) watermarking detector

TABLE 3 The PSNR and corresponding NC with Gaussian noise

Noise parameters (%)	1	3	5	10	15	20	25
PSNR	12.52	8.02	6.03	3.32	1.80	0.82	0.10
NC1	1.00	1.00	1.00	1.00	1.00	1.00	1.00
NC2	1.00	1.00	1.00	1.00	1.00	1.00	1.00
NC3	1.00	1.00	1.00	1.00	1.00	1.00	1.00

4.1.2 JPEG attacks

Figure 7a indicates the slice with JPEG attack (5%). Figure 7b indicates the corresponding volume data. As the Figure 7c displays the multi-watermarking sequence can be detected, NC1=1.00, NC2=1.00, NC3=1.00. Table 4

gives the PSNR and corresponding NC when different parameters of JPEG attacks are inflicted on the volume data. If the compression quality is down to 2%, the multi-watermarking still can be detected nevertheless. When the JPEG attacks, the results demonstrate that algorithm is robust.

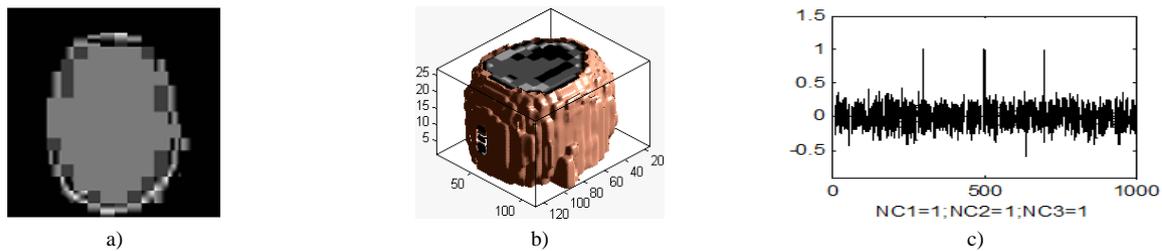


FIGURE 7 With JPEG attack (10%): a) a slice with JPEG attack; b) the corresponding volume data; c) watermarking detector

TABLE 4 The PSNR and corresponding NC with JPEG attacks

Compression quality (%)	2	4	8	10	20	40	60
PSNR	16.57	17.82	20.21	21.20	23.10	25.06	26.61
NC1	1.00	1.00	1.00	1.00	1.00	1.00	1.00
NC2	1.00	1.00	1.00	1.00	1.00	1.00	1.00
NC3	1.00	1.00	1.00	1.00	1.00	1.00	1.00

4.2 GEOMETRIC ATTACKS

Geometric attacks are refer to the watermarking image under rotation, scaling, cropping, translation and so on. It is almost the watermarking attack method which is hardest to solve. The implementation of the geometric attacks is very convenient. Just simple geometric attacks are often can cause the loss of watermarking. It affects the effectiveness of the watermarking algorithm greatly. Resistance to geometric attacks is a focus in the study of watermarking algorithm.

4.2.1 Rotation attacks

The slice with 20° rotated clockwise is indicated in Figure 8a. The corresponding volume data is indicated in Figure 8b. As the Figure 8c) displays the multi-watermarking sequence can be detected, NC1=0.91, NC2=0.90, NC3=0.90. Table 5 gives the PSNR and corresponding NC when different rotated angles are inflicted on the volume data. As the angle of rotation top to 35°clockwise, the multi-watermarking can be detected, too. When the rotation attacks, the results demonstrate that algorithm is robust.

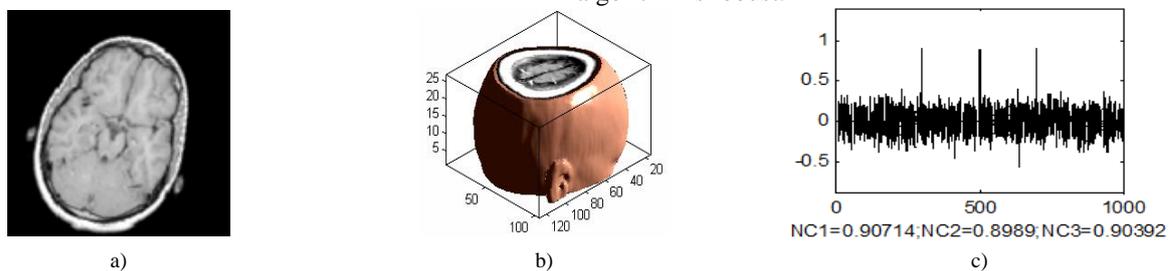


FIGURE 8 With rotation attack (20°): a) a slice with rotation attack; b) the corresponding volume data; c) watermarking detector

TABLE 5 The PSNR and corresponding NC with rotation attacks

Rotated (clockwise)	5	10	15	20	25	30	35
PSNR	16.54	13.97	12.98	12.44	12.04	11.68	11.33
NC1	0.97	0.94	0.91	0.91	0.88	0.84	0.84
NC2	0.96	0.93	0.90	0.90	0.87	0.83	0.83
NC3	0.97	0.94	0.90	0.90	0.87	0.85	0.85

4.2.2 Cropping attacks

The slice under cropping 10% from Z displays on Figure 9a. Then, the corresponding volume data is shown in Figure 9b. Figure 9c shows that the watermarking can

be detected, NC1=1.00, NC2=1.00, NC3=1.00. Different cropping rates inflict on the volume data, the corresponding NC are given in Table 6. Hence, we can conclude the algorithm is robust to cropping attacks.

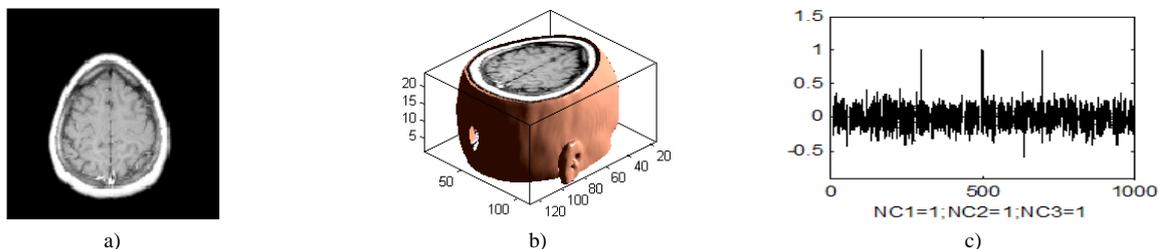


FIGURE 9 With noise attack: a) a slice with noise attack; b) the corresponding volume data; c) watermarking detector

TABLE 6 The PSNR and corresponding NC with cropping attacks

Cropping rate (from Z %)	2	4	6	8	10	20	40
NC1	1.00	1.00	1.00	1.00	1.00	0.97	0.88
NC2	1.00	1.00	1.00	1.00	1.00	0.97	0.87
NC3	1.00	1.00	1.00	1.00	1.00	0.97	0.88

4.3 ALGORITHM COMPARISON

In order to further demonstrate the robustness properties, we consider the performance of others volume data watermarking schemes, such as DCT, DFT, DWT-DCT, DWT-DFT [8], [10-11], [26]. We show the comparison results with different attacks in terms of NC in Figure 10. The results account for that the proposed volume data watermarking algorithm has good robustness. The performance for Gaussian noise and rotation attacks, are shown in Figure 10. In the case of Gaussian noise, the NC

of the proposed perceptual hashing algorithm all are 1.00. We can also observe that the NC of other volume data watermarking schemes are less than 1.00. We show the performance for rotation attacks is shown in Figure 10. In the case of rotation attacks, the NC of the perceptual hashing algorithms is very high. The NC of DCT scheme and DWT-DCT scheme are the same. In all, we observe that the proposed volume data watermarking scheme perform very well for both common attacks and geometric attacks. The algorithm has good robustness against common attacks and geometric attacks

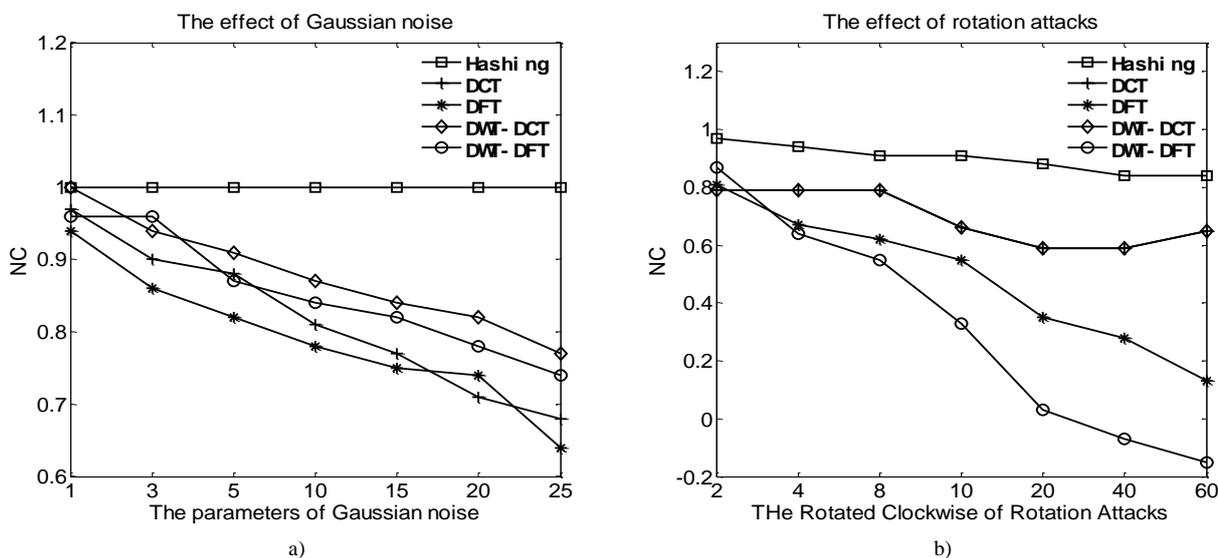


FIGURE 10 The performance of watermarking schemes under common attacks. a) Gaussian noise; b) JPEG attacks. To generate a point on the curve, X-axis is the volume data under different attacks; the corresponding watermarking of resulting volume data was detected. And the corresponding NC with the original watermarking is shown in the Y-axis.

5 Conclusion

A novel blind watermarking scheme appropriate for 3D volume data by using perceptual hashing was proposed in this paper. The method combines DFT transform, feature vector and database technology. The watermarking is a blind watermarking. In addition, the embedding of watermarking would not change the volume data. And the multi-watermarking could be embedded in volume data. It proved that the algorithm has a great capacity of

watermarking embedding. The experiments results show that the algorithm has good robustness against common and geometric attacks, In a word, it is a efficiency algorithm.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No:61263033) and the NSF of Hainan Province of China(60894).

References

- [1] Kaur S, Farooq O, Singhal R, Ahuja B S 2010 Digital watermarking of ECG data for secure wireless communication *Proceedings Information, Telecommunication and Computing (ITC) Conference Kochi Kerala* 140-4
- [2] Hartung F, Kutter M 1999 *Proceedings of the IEEE* **87(7)** 1079-107
- [3] Cox I, Miller M, Bloom J, Fridrich J, Kalker T 2007 Digital watermarking and steganography *Morgan Kaufmann USA*
- [4] Lai C C, Tsai C C 2010 *IEEE Transactions on Instrumentation and Management* **59(11)** 3060-3
- [5] Vivekanda B K, Sengupta I, Das A 2011 An audio watermarking scheme using singular value decomposition and dither-modulation quantization *Multimedia Tools and Applications* **52(2)** 369-83
- [6] Preda R O, Vizireanu N D 2011 Quantization-based video watermarking in the wavelet domain with spatial and temporal redundancy *International Journal of Electronics* **98(3)** 393-405
- [7] Rajendra A U, Niranjana U C, Iyengar S S, Kannathal N, Min K C 2004 Simultaneous storage of patient information with medical images in the frequency domain *Computer Methods and Programs in Biomedicine* **76(1)** 13-9
- [8] Li J, Du W, Bai Y, Chen Y 2012 3D-DCT based zero-watermarking for medical volume data robust to geometrical attack *Wireless Communications and Applications Springer Berlin Heidelberg* 434-44
- [9] Solachidis V, Pitas I 2007 *IEEE Transactions on Multimedia* **9(7)** 1373-83
- [10] Li J, Du W, Bai Y, Chen Y 2011 Robust multiple watermarks for volume data based on 3D-DWT and 3D-DFT *2011 International Conference on Electronics, Communications and Control (ICECC) Ningbo* 446-50
- [11] Li J, Du W, Bai Y, Chen Y 2011 3D DWT-DCT based multiple watermarks for medical volume data robust to geometrical attacks *2011 International Conference on Electronics, Communications and Control (ICECC)* 605-9
- [12] Wu Y, Guan X, Kankanhalli M S, Huang Z 2001 Robust invisible watermarking of volume data using the 3D DCT *Proceedings of the Computer Graphics International Conf Hong Kong* 359-62
- [13] Coatrieux G, Maitre H, Sankur B 2001 Strict integrity control of biomedical images *Proceedings of SPIE – The international Society for Optical Engineering* 229-40
- [14] Li X, He G 2012 Efficient Audio Zero-Watermarking Algorithm for Copyright Protection Based on BIC and DWCM Matrix *International Journal of Advancements in Computing Technology* **4(6)** 109-17
- [15] Swaminathan A, Mao Y, Wu M 2006 *IEEE Transactions on Information Forensics and Security* **1(2)** 215-30
- [16] Niu X, Jiao Y 2008 An overview of perceptual hashing *Acta Electronica Sinica* **36(7)** 1405-11 (in Chinese)
- [17] Lin S, Ozsu M T, Oria V, Ng R 2001 An extendible hash for multi-precision similarity querying of image databases *Proceedings of the 27th Very Large Data Bases (VLDB) Conference Roma, Italy*
- [18] Wang L, Jiang X, Lian S, Hu D, Ye D 2011 Image authentication based on perceptual hash using Gabor filters *Soft Computing* **15(3)** 493-504
- [19] Kailasanathan C, Safavi Naini R 2001 *IEEE-EURASIP Workshop on Nonlinear Signal and Image Processing* Baltimore
- [20] Li C, Song H A 2009 geometrically robust watermarking scheme based on perceptual hashes and genetic Algorithm *Proceedings of the 4th International Conference on Computer Science & Education (ICCSE'09) Nanning* 673-8
- [21] Holliman M, Memon N, Yeung M M 1999 On the need for image dependent keys for watermarking *Proceedings of the Content Security and Data Hiding in Digital Media Newark*
- [22] Kozat S S, Venkatesan R, Mihcak M K 2001 *Proceedings of the IEEE Conference on Image Processing* **5** 3443-6
- [23] Monga V, Banerjee A, Evans B L 2004 Clustering algorithms for perceptual image hashing *Proceedings of the 3rd IEEE Signal Processing Education Workshop* 283-7
- [24] Monga V, Banerjee A, Evans B L 2006 *IEEE Transactions on Information Forensics and Security* **1(1)** 68-79
- [25] Monga V, Mihcak M K 2007 *IEEE Transactions on Information Forensics and Security* **2(3)** 376-90 2007
- [26] Li J, Du W, Bai Y, Chen Y 2011 3D-DFT Based Robust Multiple Watermarks of Medical Volume Data *Proceedings of the 3th Multimedia Information Networking and Security (MINES) Shanghai* 484-8

Authors



Yujia Li, born in December, 1990, Wannian, Jiangxi Province, China

Current position, grades: Master degree student in Information and Communication Engineering at University of Hainan, College of information science and technology.

University studies: BS degree in Information and Computing Science at Hainan University, Hainan, China, in 2012.

Scientific interests: multimedia information security, digital watermarking, image processing.

Publications: 4 papers.



Jingbing Li, born in June, 1966, Handan, Hebei Province, China

Current position, grades: doctor of Control Theory and control Engineering. Professor and doctoral supervisor in Hainan University

University studies: PhD degree at the Department of automation, Chongqing University, Chongqing, China in 2007.

Scientific interests: multimedia information security, digital watermarking, computer control.

Publications: 4 patents, 52 papers, 4 books.