RESEARCH OF DUAL WATERMARKING TECHNOLOGY FOR DIGITAL IMAGE

Fang Yinglan , Han Bing ,Zhang Yongmei and Tian Lin

Beijing Key Laboratory on Integration and Analysis of Large-scale Stream Data
School of Computer, North China University of Technology
Beijing, 100144, P.R. China
Emails: jlufangyl@163.com

Submitted: July 9, 2015 ***Accepted: Jan. 8, 2016*** ***Published: Dec. 1, 2016***

Abstract- Digital image watermark has been studied as object. It analyzed the typical digital watermark algorithms based on the space domain and transform domain and key researched watermarking algorithm based on discrete wavelet transform. It has designed and improved blind watermarking algorithm and color image watermarking algorithm. Finally, based on the two improved watermarking algorithm, it has designed a dual watermarking algorithm. Both are separated but related. It authenticates dual watermarking algorithm in addition to subjective visual evaluation, but also use numerical objective evaluation and quantitative analysis. Experimental results show that this dual watermarking algorithm combines with robustness and concealment.

Index terms*:* Dual watermarking, discrete wavelet transform, robustness, concealment .

I. INTRODUCTION

With the development of science and technology, people have entered the digital era. Now the transmission and exchange of information is a relatively simple and quick process. People can quickly and. easily transmit digital information to the world using electronic devices But the attendant side effects are very obvious. After many digital works are published in electronic format on the web, they are copied and distributed by the ulterior person or organization. This has greatly damaged the commercial interests of the product owner. Therefore, in the context of the Internet, how to protect the copyright of digital works and how to ensure the security of information content has become an urgent problem. As the new achievements of scientific development, digital works have their own new characteristic, but the existing copyright protection system was unable to protect its copyright. Digital watermarking technology as an important branch of information hiding technology research field, since it has been paid attention to by many domestic and foreign experts and scholars and business groups, and gradually become a research hotspot in the field of information security [1].

In order to change this situation of the digital works, people integrated communications theory, noise theory, coding theory, checking theory, information theory, cryptography, digital image processing, signal processing, algorithm design and many other subject. the digital watermarking technology was imported into the digital works reprocessing. As an effective complement to traditional encryption technology, digital watermarking has become a front research in information security. It is widespread attention by the governments, academics and business. Therefore, the study of digital watermarking is not only important to the learning but also has great commercial value. A digital image watermarking algorithm, and realizes the simulation, performance test work on the improved algorithm[2]. And the transform domain watermark algorithm embeds the watermark information into the transform spatial domain including the DCT domain and wavelet domain. On the other hand, according to the characteristics of watermarking algorithms, the watermark can be classified into: robust, semi-fragile and fragile watermark[3]. How to obtain the ideal target characteristics is the key that ensuring the reliability of the tracking system particularly in the complex environment. Because the environment of the target image recognition is complex, relevant processing methods such as preprocessing of image target, the processing of target separation and target edge detection should be researched to detect

the target[4] .In this regard some preprocessing operation such as noise reduction and the mean retention filters are applied on the input image[5].

II. TYPICAL DIGITAL WATERMARKING ALGORITHM

a. Space Domain Watermarking Algorithm

Space domain watermarking algorithm refers to directly modify the digital image pixel values using watermark information [6]. LSB algorithm and Patchwork algorithm are the representative algorithms.

- LSB Algorithm

Some of the earliest techniques used to embed m sequences into Least Significant Bit (LSB) of the data to provide effective transparent embedding technique [7].Another Spatial Domain technique consist of embedding a texture based watermark into a portion of the image with similar texture, it will be difficult to pensive the watermark. The watermark is detected using a correlation detector [8].The algorithm embeds watermark information through the least important pixel position (least significant bit) in the carrier image bit [6]. So it can ensure watermark's invisibility. However, the watermark can easily be destroyed by the digital signal processing technology due to the location of hidden watermark is unimportant. The robustness of the algorithm is poor.

- Patchwork Algorithm

The algorithm randomly selected N pairs pixels (ai, bi) in the carrier images. Then the brightness of ai in all the selected pixels was decreased one and the brightness of bi in all the selected pixels was added one, so the watermark is embedded. The average brightness of the carrier image has not changed, and it embedded watermark information, but the capacity of the watermarking algorithm is limited.

b. Transform Domain Watermarking Algorithm

The transform domain watermarking algorithm first transforms carrier image to obtain its frequency-domain coefficient [6]. Then it modifies the frequency domain coefficients based on the watermark information. Finally it does the corresponding inverse transform, and it can obtain the watermarked carrier.

- Discrete Cosine Transform(DCT) Algorithm

The algorithm is first proposed by Koch and J Zhao. .DCT based transform domain watermarking started in later part of 90s. In 2004, Saraju P. Mohanty, N. Raga Nathan had also developed visible watermarking scheme on DCT [9]. After some period, wavelet based approach were starting due to their multi resolution property for wavelet [10]. First vector images are decomposed into many 8×8 sub-graphs, and the discrete cosine transform applied to the sub-block map key randomly chosen by, and then based on the binary sequence information of the watermark blocks of these points on a frequent domain coefficients to fine tune the watermark is embedded, and finally, the corresponding inverse transformation, to obtain the watermarked vector.

- Discrete Wavelet Transform(DWT) Algorithm

In 2005 later part, Sammy H. M.Hawk and Edumund Y. Lam proposed watermark implementation technique in digital photography with DWT approach [11]. In 2007, Cong JIN, Liang-Gang PAN and Ting SU proposed the scheme for Image watermark based of DWT with Visual based concept [12]. Compared with the previous DCT transform, wavelet transform has a better spatial and frequency localization capability and more accord with the human visual system (HVS) [13]. Combine human visual system masking character and brightness sensitivity directional characteristics, it implements watermark embedding in accordance with the wavelet coefficient which the watermark information not easy to detect modified carrier region (texture, edge, etc.). Because DWT has better accord with the HVS character and with JPGE2000 popular compression standard (based on wavelet transform). DWT has gradually paid more attention in the application in the field of information hiding and digital watermarking area and has a tendency to replace DCT.

c. Comparison of Various Watermarking Algorithm

In order to analyze the robustness of various algorithms, it performs the same attack (such as noise attack, median filtering attacks, compression attacks) to LSB watermarking algorithm , domain watermarking algorithm based on DCT transform and transform domain watermarking algorithm based on DWT. Meanwhile in order to make the results comparable, it adjusts the embedding parameter to different algorithms, so that the watermarked image and the original image obtained by different algorithms have the same PSNR. The comparative experimental results obtained with the original watermark extraction and original watermark to the three algorithms is as shown in table 1:

Table 1: Experiments of Three Algorithms

Algorithm	LSB Algorithm	DCT Algorithm	DWT Algorithm
Gaussian noise	0.7240	0.8970	0.9961
Salt & pepper noise	0.7707	0.9398	0.9987
JPGE compression	0.8492	0.9960	0.9962
Cut Attack	0.6669	0.7140	0.8417

III. DIGITAL IMAGE WATERMARK ALGORITHM DESIGN

Because blind watermarking algorithm needs not use original image in the extraction of the watermark. The extraction process of blind watermarking algorithm is relatively simple and storage costs are not as limited as the plaintext watermark [14].

The watermarking algorithm in the reference [15] has implemented blind watermarking. But the efficiency of this algorithm is low, because it needs many discrete wavelet transform and its robustness needs to be improved. Herein, the paper has improved the algorithm based on the reference [15]. It has done 2 level DWT to the carrier image obtained DA sub-graph, and block to it. It implements Arnold scrambling to the watermark image and the processed watermark image is as a control signal in accordance with certain rules it processes DWT coefficients of the DA sub-graph after block in order to achieve the embedded watermark information [16].

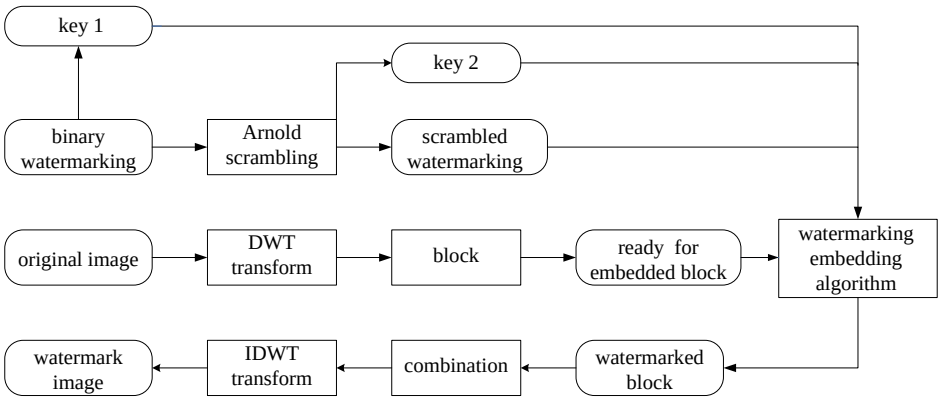


Figure 1. blind watermarking embedding process

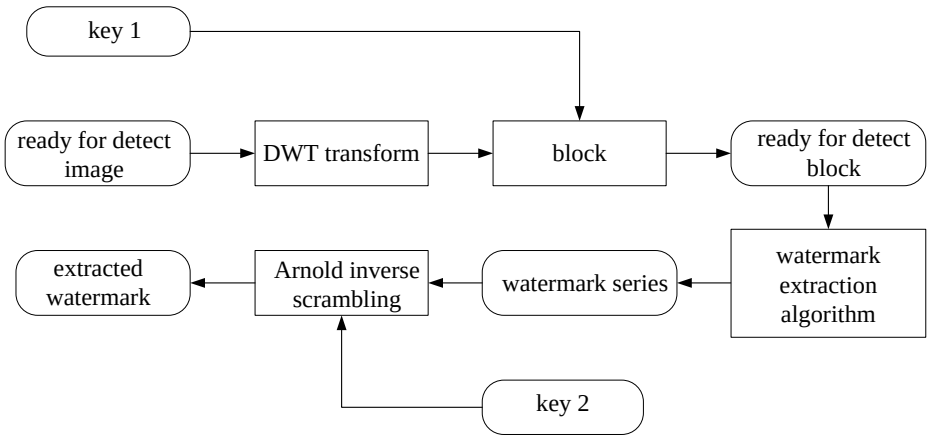


Figure 2. blind watermarking extracting process

The simulation experiment has been done in the MATLAB9.2 environment by using the above-mentioned algorithm. It selects 512×512 pixels gray image Lena as carrier image and selects 32×32 pixels binary meaningful image as watermark.

Experiments show that from the subjective perspective, whether the overall effect of the image or local contrast details, the original carrier image and the watermark image has almost no difference. Namely after embedding watermark, the image can still maintain a good visual effect. From the objective perspective, the PSNR value of the watermark image is 44.9927 dB, the NC value of correlation coefficient between the original watermarks and extracting watermark is 1. This shows that the algorithm has a good concealment.

From the experiment data contrast, it can seen that the NC value of extracted watermark image and the original watermark image is not only greater than 0.9 and higher than the algorithm in reference [15] after several kinds of common attack to containing watermark carrier obtained by the algorithm. This can show that the robustness of the paper algorithm is superior to and the efficiency is higher than the algorithm in reference [15].

IV. COLOR IMAGE WATERMARKING ALGORITHM DESIGN

With the rapid development of digital technology, people is widely used color brilliant images, it has more practical significance to research digital watermarking algorithm based on color vector image. In addition, the watermark information can adopt a color image; the watermark information will be greatly enhanced.

The watermarking algorithm in the reference has added color watermarking transformed by wavelet to the carrier image using additive watermark embedding rules. It has met the basic watermarking algorithm. The paper has improved the algorithm based on the reference [16]. First it embedded low frequency sub-graph watermark into carrier low frequency sub-graph in accordance with the additive watermark embedding rule. Then follow the iterative mixed method in the reference [17], it embedded high frequency sub-graph watermark into carrier middle frequency sub-graph [18]. Because it selects many iterations parameters in the iterative process, it has improved the security of the watermark and the mixing proportion of watermarked image in the iterative process; so it can improve the watermark anti-attack capability [19].

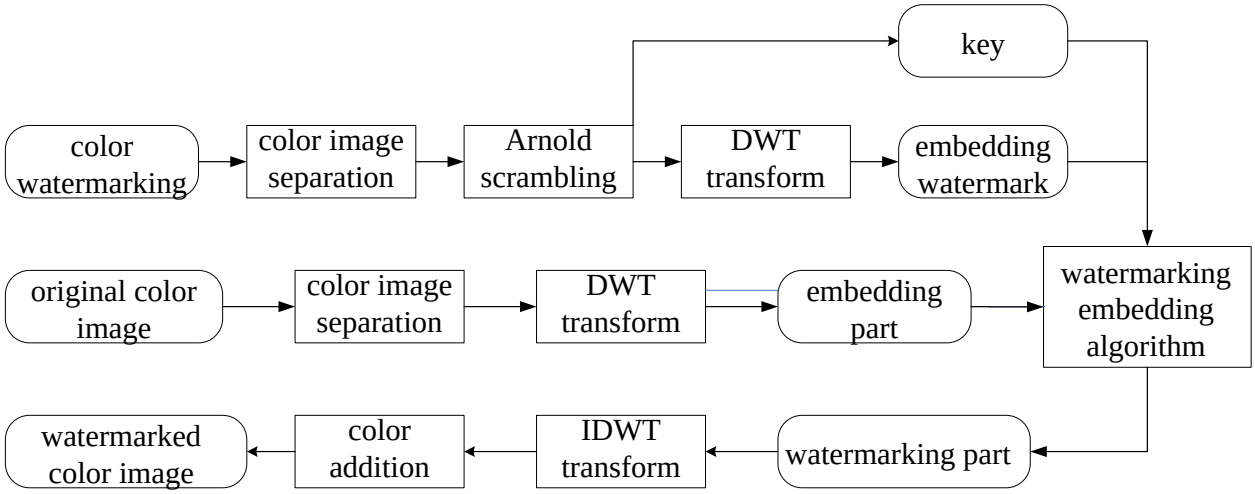


Figure 3. color watermarking embedding process

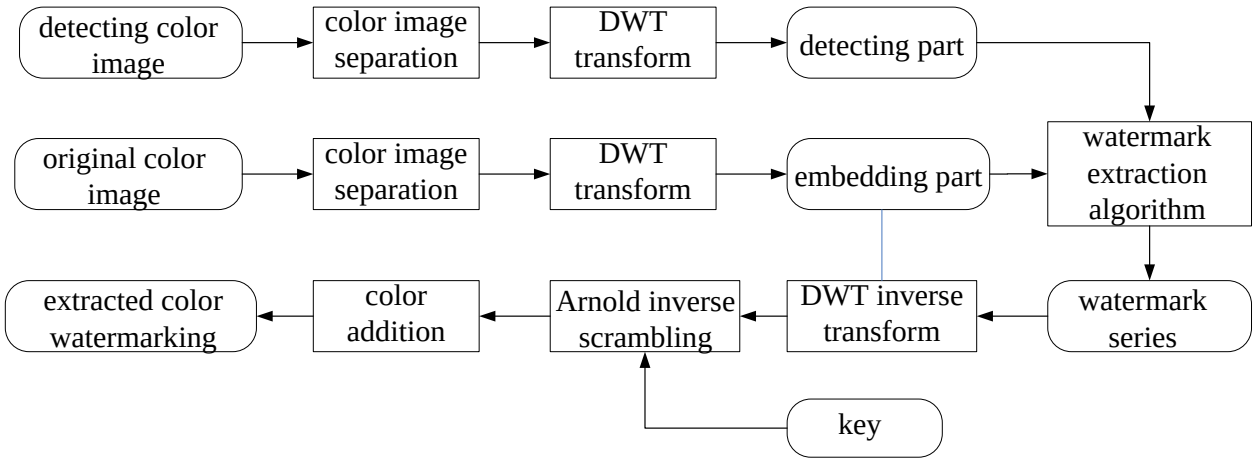


Figure 4. color watermarking extracting process

The simulation experiment has been done in the MATLAB9.2 environment with the above-mentioned algorithm simulation experiment. The experiment chooses 512×512 pixels color image Lena as carrier image and chooses 128×128 pixel color school badge image as watermark. Experiments show that from the subjective perspective, whether the overall effect of the image or local contrast details, the original carrier image and the watermark image are containing basic consistent. That is after embeds watermark, the images can still maintain a good visual effect. From the objective perspective, the PSNR value of original carrier and watermark image equal to 33.7604 dB. The NC value of correlation coefficient between the original watermark and the extracting watermark is 0.98522. The result indicates that the concealment of the proposed algorithm is better.

After several attacks on the extracted watermark in the image, the NC value between the extracting watermark and the original watermark basically all above 0.9. It shows that the color watermark algorithm has strong ability to resist attacks.

V. DESIGN AND IMPLEMENTATION OF DUAL DIGITAL WATERMARK ALGORITHM

It has designed a dual watermarking algorithm based on the above two improved algorithm. That is both binary watermark and color watermarks are also embedded into color vector image, which binary watermark played recognized role and color watermarks played affirm role[20]. The two are separated but related. Wherein the identifying watermark is used for testing copyright belongs preliminary and the confirming watermark is used for detecting more detailed copyright information. Through it correlating validates the extracted recognition watermark and the verification watermark to confirm the two watermarks are real and effective.

a. Dual Watermark Algorithm Basic Framework

The dual watermark algorithm basic framework is designed as figure 5, figure 6 and figure 7.

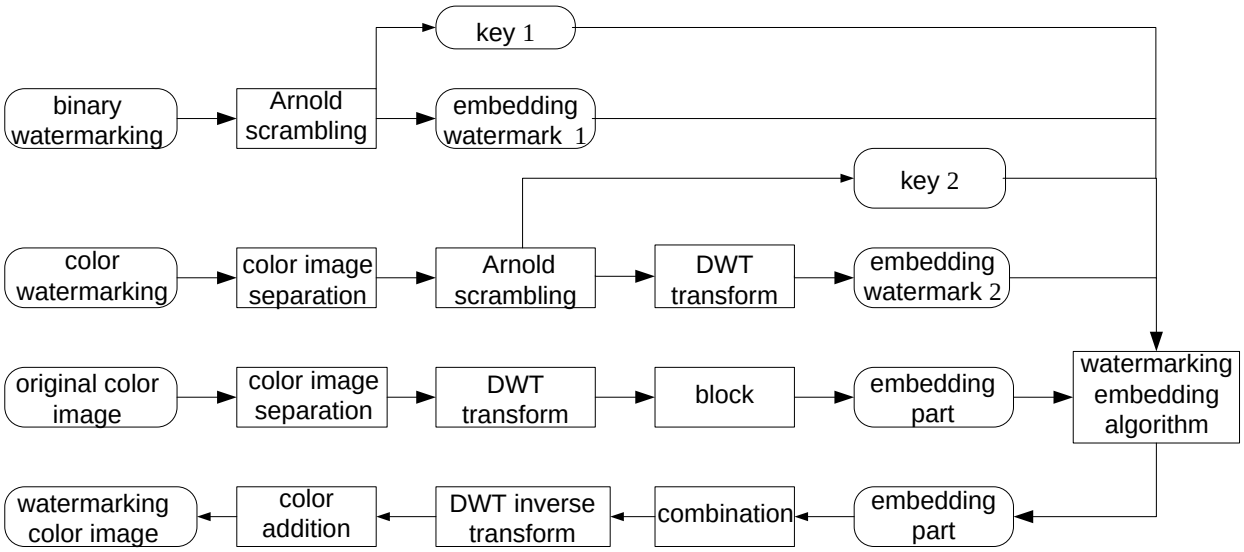


Figure 5. Dual Watermarking Embedding Process

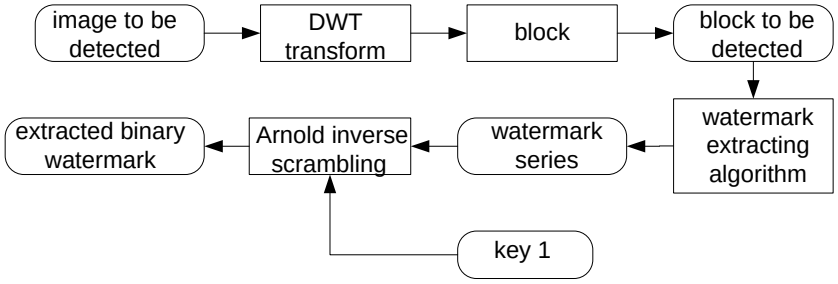


Figure 6. Recognition Watermarking Extracting Process

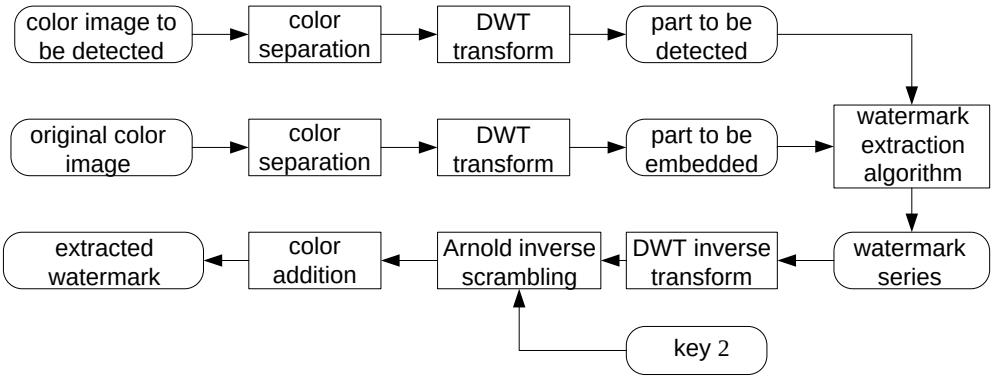


Figure 7. Verification Watermarking Extracting Process

b. Associated with the Generation Of the Watermark

The recognition watermark of the algorithm is binary watermarking and recognition watermark is color watermarking. These two watermarks are not only independent but also relevant. Independence represent that the two separate watermark information can be extracted separately and identifying watermark belong to blind watermark and authentication watermarking belong to plaintext watermark[21]. Copyright information of confirmation watermark is determined by the randomly generated sequence number of identification watermark. The specific correlative rules are as follows in figure 8 and figure 9.

(a) Confirmation Watermark (b) Identification Watermark

Figure 8. Uncorrelated Confirmation Watermark and Identification Watermark

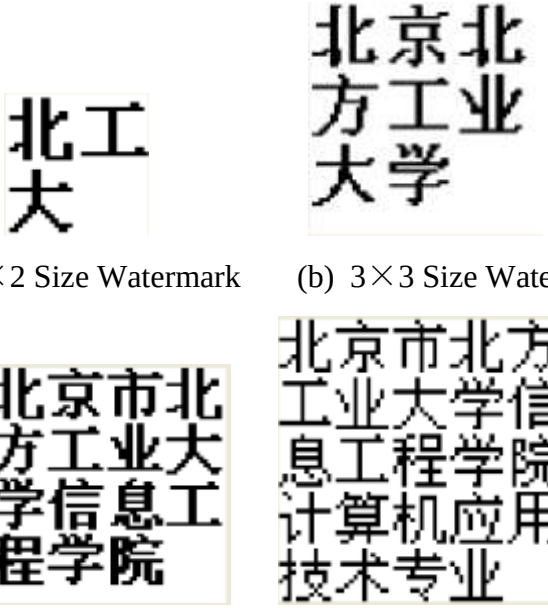
(a) Sequence number 1 (b) Sequence Number 2

(c) Sequence Number 3 (d) Sequence Number 4

Figure 9. Correlated Confirmation Watermark And Identification Watermark

Identification watermark's content is decided by embedding watermark, but it has no more than 24 characters. When the number of characters is less than 4, the watermark size is 2×2 and the remainder is filled with spaces. When the number of characters is more than 3 and less than 9, the watermark size is 3×3 and the remainder is filled with spaces. When the number of characters is more than 9 and less than 16, the watermark size is 4×4 and the remainder is filled with spaces.

When the number of characters is more than 16 and less than 25, the watermark size is 5×5 and the remainder is filled with spaces. Different size user-defined watermark is shown as figure 10.



(a) 2×2 Size Watermark (b) 3×3 Size Watermark

(c) 4×4 Size Watermark (d) 5×5 Size Watermark

Figure 10. User-Defined Identification Watermark

c. Dual Watermark Embed

Suppose carrier image is I and its size is M×M. The generated color watermark is W1 and its size is N1×N1 . The generated binary watermark is W2 and its size is N2×N2. First color watermark W1 is embedded into carrier image I in accordance with color watermark embedding method, then the binary watermark W2 is embedded into 2 level component sub-graph of the carrier image I in accordance with blind watermark embedding method.

d. Dual Watermark Extraction

Dual watermark can be separately extracted. If it only need the initial ownership detection, it extracts copyright identification watermark. If it needs further confirmation to get more detailed copyright information, it must extract confirmation watermark. The process of identification watermark extraction is as the follows.

(1) It reads the watermarked image $I^{\tilde{}}$ and separates its implementation color and then select its green component $I_G^{\tilde{}}$;

(2) It extracts according to the blind watermark extraction method and gets the binary identify watermark $W_2^{\sim}$.

The process of confirmation watermark extraction is that it reads watermarked image $I^{\sim}$ and the original carrier image I. It extracts according to the color watermark extraction method and gets the color confirmation watermark $W_1^{\sim}$.

e. Experimental results and analysis

In the MATLAB 9.2a environment, it has done the simulation experiment according to the above algorithm. It selects Lena color image with 512×512 pixels as carrier, and select badge plus additional information color image with 128×128 pixels as confirmation watermark and select binary watermark image with 32×32 pixels as identification watermark to do experiment.

e.i Experimental Results with No Attack

The experiment has done with no attack. The experimental result is shown in figure 11.

(a) Original Carrier Image (b) Watermarked Image

(c)Original Confirm Watermark (d) Extracted Confirm Watermark

(e) Original Identify Watermark (f) Extracted Identify Watermark

Figure 11. Experimental Results with No Attack

Experiments show that from the subjective point of view, the original image and watermarked image are basically same whether the whole effect of the image or the contrast local details. The image still maintains good visual effect after it is embedded watermark. From the objective point of view, the PSNR value between the original carrier and the watermarked carrier equal to 33.2654dB. The NC value between the original confirmation watermark and the extracted confirmation watermark equals to 0.9790. The NC value between the original identification watermark and the extracted identification watermark equals to 1. This result indicates that the concealment of the double watermarking algorithm is well.

e.ii Experimental Results with various attacks

It detects anti-attack capability of the algorithm through simulation experiments. The specific approach is make a series of attacks on the watermarked image. We chose the attacks that do not make serious distortion to the watermarked image, such as noise attacks, filter attacks, geometric attacks (scale, rotation, cut), and JPEG compression attack. Then it detect watermark situation of carrier image after the attack. The experimental result is shown from figure 12, figure 13, figure 14, figure 15 and figure 16.

(1) Noise Attack

Figure 12. Experimental Results with Noise Attack

Figure 12 is the result of image which suffered noise attack. The noise attack is to add salt and pepper noise with the noise density value equals to 0.001 and the extracted watermark image with the confirmation watermark NC value is 0.9487 and the identification watermark NC value equals to 0.9884

(2) Filter Attack

Figure 13. Experimental Results with Filter Attack

Figure 13 is the result of image which suffered filter attack. The filter attack is to add wiener filter and the extracted watermark image with the confirmation watermark NC value equals to 0.9167 and the identification watermark NC value equals to 0.9897.

(3). Geometric Attack

Figure 14. Experimental Results with Geometric Attack I

Figure 15. Experimental Results with Geometric Attack II

Figure 14 and1figure 15 are the results of image which suffered geometric attack.In figure 14, the geometric attack is to expand twice and the extracted watermark image with the confirmation watermark NC value equals to 0.9476 and the identification watermark NC value equals to 0.9987.

In figure 15, the geometric attack is to reduce twice and extracted watermark image with confirmation watermark NC value equals to 0.9286 and the identification watermark NC value equals to 0.9794.

(4). JPER Compression Attack

Figure 16 Experimental Results with JPER Compression Attack

Figure 16 is the result of image which suffered JPER compression attack. The JPER compression attack is to add gauss noise with the version value equals to 0.001 and the extracted watermark image with the confirmation watermark NC value equals to 0.8813 and the identification watermark NC value is 0.9796. The quality of PSNR and NC of Anti-GPEG compression resistance is shown in table 2.

Table 2. PSNR and NC of Anti-GPEG Compression Resistance

Quality	**PSNR/dB**	**Confirmation Watermark NC**	**Identification Watermark NC**
100%	33.2654	0.9790	1
90%	32.7756	0.9289	0.9949
80%	32.0943	0.9115	0.9545
70%	31.7488	0.8967	0.9820
60%	31.4888	0.8812	0.7745

It is experimented by Lena color images with 512×512 pixels as carrier, pixel logo plus, color image attached school badge with 128×128 pixels as confirmation watermark, binary images with 64×64 pixels as recognition watermark. Results are shown in table 3.

Table 3. Experimental results

Attack Name	**PSNR/dB**	**Confirmation Watermark NC**	**Identification Watermark NC**
No Attack	32.4562	0.98671	0.99969
Gauss Noise	29.9615	0.90221	0.97946
Salt and Pepper Noise	31.5777	0.98118	0.98942
Median Filter	30.9200	0.92765	0.95551
Wiener Filter	31.5012	0.94144	0.98569
Zoom 200%	32.3306	0.98197	0.99690
Zoom 50%	30.3221	0.95783	0.97449
JPGE compress 90%	32.0869	0.95556	0.99502
JPGE Compress 80%	31.5009	0.93530	0.95800
JPGE Compress 70%	31.2434	0.91796	0.90044
JPGE Compress 60%	31.0336	0.90386	0.79060

It has extracted watermark after several attacked image. The NC value between confirmation watermark and the original watermark which extracted the NC value between recognition watermark and the original watermark are all above 0.9. It shows the anti-attack ability of the double watermarking algorithm is strong, namely it has good robustness.

VI. CONCLUSIONS

In the field of copyright protection, the key and the original image used in dual watermarking algorithm will be secretly saved by the copyright owner. Organization or individual who want to illegally obtain copyright cannot extract confirmed watermark with the correlation information. At the same timed if they are adding false watermark in the pirated image, it will not able to

through the verification. Namely in terms of robustness, double watermark is better than single watermark. For tracking piracy, it can add the relevant information of the buyer to the confirmed watermark. When there is large number of illegal copies, it can find the illegal communicators from the extracted watermarking. In the field of information hiding, the information of secret transmission can be regularly and respectively added to the identification watermark and confirmation watermark. Only it has correctly extracted two watermarks, it can see the corresponding secret information and effectively improve the security of information hiding.

In this paper, it has validated the dual watermarking algorithm. In addition to the subjective visual evaluation, it also quantitatively analyses the algorithms using the objective PSNR and NC evaluation standard. All the analysis results are passed by MATLAB simulation software. The numerical value results show that the dual watermarking algorithm with good concealment and robustness.

CONFLICT OF INTEREST

The author confirms that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This paper is supported by the National Natural Science Foundation of China (61371143), Beijing Natural Science Foundation Project (4132026), North China University of Technology special project (XN054) North China University of Technology Advantageous Subject(XN078).

REFERENCES

[1] Ashdown M., Flagg M., Sukthankar R., and Rehg J.M., A Flexible Projector-Camera System for Multi-Planar Displays, Computer Vision and Pattern Recognition (CVPR), 2014, pp. II-165 - II-172

[2] Zhu Yuefeng, Lin Li ," DIGITAL IMAGE WATERMARKING ALGORITHMS BASED ON DUAL TRANSFORM DOMAIN AND SELF-RECOVERY ",International Journal on Smart Sensing and Intelligent Systems (S2IS), VOL. 8, NO. 1, MARCH 2015, pp 199-219.

[3] YUAN Fei, YE Zheng-Shan, LIN Cong-Ren,CHENG En ," Image Quality Assessment Method for Underwater Acoustic Communication Based on Digital Watermarking" , International Journal on Smart Sensing and Intelligent Systems (S2IS), VOL. 6, NO. 2, APRIL 2013,pp 752-771.

[4] Liping Lu, Jinfang Wang, "IMAGE PROCESSING AND RECOGNITION ALGORITHM FOR TARGET TRACKING", International Journal on Smart Sensing and Intelligent Systems (S2IS), VOL. 9, NO. 1, MARCH 2016,pp 353 – 376.

[5] Elyas Abbasi Jennat Abadi , Sohey Akhlaghi Amiri , Masoud Goharimanesh and Aliakbar Akbari, " VEHICLE MODEL RECOGNITION BASED ON USING IMAGE PROCESSING AND WAVELET ANALYSIS", International Journal on Smart Sensing and Intelligent Systems (S2IS), VOL. 8, NO. 4, DECEMBER 2015,pp 2212 – 2230.

[6] Jin Cong, "Digital watermarking theory and technology", Beijing: Tsinghua University Press, 2008, pp. 22-25.

[7] R.G. Van Shindig, A.Z.Tirkel and C. F. Osborne, "A Two-Dimensional Digital Watermark," in proc. DICTA, 1993, pp. 378-393

[8] S. Arivazhagan and L. Ganesan, "Texture Segmentation Using Wavelet Transform," Pattern recognition Letters, Vol. 24,December-2003,pp 3197-3203

[9] Saraju P. Mohanty, N. Raganathan, Ravi K. Namballa, "VLSI Implementation of Visible Watermarking for a Secure Digital Camera Design," Proceeding of 17th International Conference on VLSI design,2004.

[10] A. Gavlasova,A. Prochazka, and M. Mudrova, "Wavelet Use for Image Classification," 15th International Conference on Process Control,2005.

[11]Sammy H. M. Kwok and Edmund Y. Lam, "Watermark implementation in digital photography," Processing Of 2005 International Symposium on Intelligent Signal Processing and Communication Systems, Dec- 2005.

[12] Cong Jin, Liang-Gang Pan, Ting Su, "A Blind Watermarking Scheme Based on Visual Model for Copyright Security," MCAM, 2007, pp 454- 463.

[13] Stephane M, "A Theory for Multiresolution Signal Decomposition: The Wavelet Representation", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 11, Jul.1989,pp 674-693.

[14] Yu yan min, "Gray image blind watermarking algorithm based on wavelet domain", Journal of Taiyuan University of Science and Technology, vol. 30, Sep. 2009, pp. 212-215.

[15] Ren peng kuan, "Image blind watermarking algorithm research based on DCT and DWT domain", M.S. thesis, xi'an university of science and technology, xi'an, China, 2008.

[16] Fang Yinglan, Tian Lin,"An Improved Blind Watermarking Algorithm for Image Based on DWT Domain", Journal of Theoretical and Applied Information technology, vol. 45, Nov. 2012, pp. 168-173.

[17] Zhu Xiankun, "Double color image digital watermarking algorithm based on wavelet domain", Northwest normal university, M.S. thesis, xi'an, China, 2009.

[18] Zhang Guicang, Wang Rangding, Zhang Yujin, "Digital image hiding technology based on iterative blending ", Chinese Journal of Computers,vol. 26, May. 2003 , pp. 567-574.

[19] Fang Yinglan, Tian Lin, Han Bin, "An Improved Watermarking Algorithm for Color Image Based on Wavelet Domain", Journal of Engineering Science and Technology Review, vol. 6, Dec. 2013, pp 139-144.

[20] Sachin Mehta, Vijayaraghavan Varadharajan, Rajarathnam Nallusamy, "Tampering Resistant Dual Watermarking Method for Copyright Protection of Still Images", Advanced Computing Networking and Security, vol. 7135, Dec. 2012, pp. 575-582.

[21] Nisar Ahmed Memon, Zulfiqar Ali Keerio, Fatima Abbasi, "Dual Watermarking of CT Scan Medical Images for Content Authentication and Copyright Protection", Communications in Computer and Information Science, vol. 414, Sep. 2014, pp.173-183.