Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, **2015**, *9*, 1-6

Open Access

A Novel Watermark Embedding Scheme using Compressive Sensing in Wavelet Domain

Bin Liao* and Jintao Lv

School of Electrical and Electronic Engineering, North China Electric Power University, Beijing 102206, China

Abstract: Most existing research achievements of digital watermarking techniques are in transform domain. In comparison with spatial domain, its advantages are larger data volume, higher security and stronger robustness. But its limitations are also obvious: complex computing requirement, weak in resisting attack and anti-extraction. In this paper, a novel blind digital watermarking algorithm is proposed, which performs digital watermark embedding process in Compressive Sensing (CS) domain based on the characteristics of CS and Human Visual System (HVS). The sub-blocks with larger capacity are selected to embed the scrambled digital watermark, considering the non-uniformity of blocks. Besides that, suitable quantization steps are chose adaptively by using quantization method. Experimental results show that the algorithm obtains robust and invisible embedded watermark with larger capacity of data. At the same time, the ability of defending against attack or extraction of embedded watermark is greatly improved. Most important feature in our algorithm is that the watermark can be extracted without any reference to the original image. As a result, the cost of storing carrier data can be saved remarkably.

Keywords: Blind extraction, compressive sensing (CS), digital watermark.

1. INTRODUCTION

Digital watermarking technology has many applications in different fields. Especially, there are broad application prospects in copy protection and content authentication. With the rapid development of advanced digital multimedia compression, network communication and information processing technology, the multimedia information on the Internet expands rapidly. More and more images are being readily available both to professional and amateur users due to astonishing advancements in imaging technologies. Meanwhile, the research in information security attracts more and more attention. Previous researches were mainly focused on spatial domain, for example, Least Significant Bit [1] (LSB) or transform domain like Discrete Wavelet Transform (DWT). Spatial domain watermarking algorithm needs simple operation but has weak robustness. And in transform domain the opposite is true. In this paper, the theory of Compressive Sensing [2] (CS) is employed for digital watermarking technology. Blind digital watermark embedding process is performed in CS domain based on the characteristics of CS and HVS. This can greatly enhance the robustness and invisibility with less costs of storage space. And the ability of defending against attack and extraction of embedded watermark is also greatly enhanced.

CS is a hot topic in the area of information science and it is becoming "A Big Idea" in signal processing. The theory breaks the limitations of traditional sampling theory due to the synchronization of sampling and compression. CS is a new sampling theory with extensive application prospects, which have an absolute advantage in digital watermark over DWT and DCT.

In the past years, lots of researchers proposed different digital watermark algorithms with strong robustness and security. Huang [3] *et al.,* applied CS method in embedding watermark for the first time, affirming the feasibility of CS in information hiding. Lin proposed an improved reconstruction algorithm [4] according to the advantages of CS for embedding watermark. She picked out some special sub-blocks for sensing and got a set of coefficients for embedding additive watermark in CS domain. But there is a major drawback that extracting watermark needs original image thus may cause the waste of storage. Wei [5] and others got wavelet coefficients after the DWT of carrier image. Then they used CS for high and low frequency coefficients respectively and embedded the watermark in the former. The method ensured the invisibility and robustness of watermark, but it ignored that if the same intensity of watermark is embedded in all high frequency, the robustness cannot be ensured as much as possible actually, considering that visual capacity of each block is different. What's more, they did much extra work for using CS in low frequency part, too.

In this paper, the existing achievements based on previous contributions of watermark and CS [6-8] is improved. Firstly, the whole image is divided into many blocks, and the sub-blocks with larger visual capacity are selected to embed the watermark in CS domain considering the non-uniformity of the block based on HVS. Thus, the invisibility and the robustness of the watermark can be ensured. Then the coefficient matrix is obtained by multiplying a sensing matrix to each sub-block. At last, the quantization steps are adjusted

*Address correspondence to this author at the School of Electrical and Electronic Engineering, North China Electric Power University, Beijing 102206, China; E-mail: nathan@ncepu.edu.cn

1874-110X/15

adaptably according to the non-uniformity property to modify the coefficients bit by bit. Finally an image embedded with the watermark is generated. In this way, only a small amount of information is needed to reconstruct the original image perfectly. This greatly reduces the sampling time and data storage space. Moreover, CS has strong anti-interference ability that the remaining measurements still can reconstruct the original image, even if some measurements are lost. In addition, we embed the watermark in CS domain and make the measurement matrix as a key, it is hard to extract or damage the watermark without the key due to the diversity of measurement matrix. Experimental results show that our proposed method improves the security and attack-resistance of the watermark greatly.

The remainder of this paper is organized as follows. Compressive sensing theory is reviewed in Section 2. In Section 3, the proposed watermark embedding and extraction is introduced. Simulate results and analyses are described in Section 4. Section 5 concludes the work.

2. COMPRESSIVE SENSING THEORY

2.1. Compressive Sensing

Traditional sample and encoding theory suffers from two inherent inefficiencies: The Shannon/Nyquist sampling theorem specifies that signal sampling rate should be at least two times of the signal bandwidth in order to avoid losing information. In many applications, including digital image and video, the Nyquist rate is so high that too many samples result, which make compression necessary prior to storage and transmission. Nevertheless, in the process of compression, a large number of transform coefficients are discarded when the signal is compressible, thus causes greatly waste of the data computation and memory store resources.

Different from conventional encoding and decoding theory, compressive sensing is new approach to represent compressive signals at a rate significantly below the Nyquist rate. CS employs non-adaptive linear projections that preserve the structure of the signal and the signal can be reconstructed from these projections using an optimization process. It does the process of signal sampling and compression coding simultaneously.

There are three processes in CS [6]--sparse representation of the signal, construction of measurement matrix and reconstruction of the signal. The core of CS is using a small amount of information to restore the original high-dimensional signals.

Consider a real valued, finite length, one dimension, discrete signal **x**, which can be viewed as an Nx1 column vector in the R^N. Any signal in R^N can be represented as the linear combination of the column vectors in the basis matrix Ψ:

$$x = \Psi\alpha \quad (1)$$

where α is the N x 1 column vector of weighting coefficients. The signal **x** is K-sparse if only K of coefficients α are none-zero. The signal **x** is compressible if the representation (1) has just a few large coefficients and many small coefficients.

Compressive sensing acquires a compressed representation directly without experiencing the procedure of N sampling. Considering that general measurement process can be described as computing inner products between the signal **x** and a group of vectors which are arranged as the row vectors of the $M \times N$ ($M<N$) measurement matrix Φ.

$$y = \Phi x \quad (2)$$

The measurement result is denoted as the M×1 column vector **y**. Then by substitution (1) in (2), **y** can be written as:

$$y = \Phi \Psi\alpha = \Theta\alpha \quad (3)$$

where Θ is the sensing matrix. Now, the problem is that how to design a stable measurement matrix Φ such that the salient information in the signal **x** is not damaged during the dimensionality reduction from N to M. And another problem is a reconstruction algorithm to recover the signal **x** from the measurement **y**. This is a complex optimization problem because the process of getting x from y is an underdetermined problem:

$$\min \|x\|_{l1} \quad s.t \quad y = \Theta x \quad (4)$$

Actually, this is a reconstructing question which is computing a minimum 1 norm of x with a constraint condition $y = \Theta x$.

2.2. The Signal Reconstruction

At present, the common reconstruction algorithms include greedy pursuit algorithm and convex optimization algorithm [8, 9] *et al.* In this paper, the Orthogonal Matching Pursuit [8] (OMP) is adopted, which is a special greedy pursuit algorithm with lower computation, better reconstruction ability, and easier realization. The process of OMP is described as follows:

Input: Sensing matrix Θ, sampling vector α, sparse degree K;

Output: The K-sparse approximation matrix $\hat{\alpha}$ of α, the reconstruction error r;

Initialization: the residual $r_0 = y$, index set $J_0 = \Phi$, iterations t=1;

Step 1: Find the maximum value of the inner product of residual r_t and the column of sensing matrix Θ: $g_t = \Theta^t r_{t-1}$.

Step 2: renew the index set $J_t = J_{t-1} \cup \{ \rho_i \}$, the sensing matrix $\Phi_{Jt} = \Phi_{Jt-1} \cup \{ \varphi_{\rho i} \}$.

Step 3: solve $\alpha_t = (\Theta_{Jt}^T \Theta_{Jt})^{-1} \Theta_{Jt}^T y$ by least-square method;

Step 4: renew the residual $r_t = y - \Theta\alpha_t$, $t = t + 1$;

Step 5: if $t > K$, stop the iteration, $\hat{\alpha} = \alpha_t$, $r = r_t$, else do step 1.

3. PROPOSED METHOD

3.1. Watermark Embedding

The whole digital watermark algorithm includes embedding process and watermark extraction process, and the watermark embedding process includes the preprocessing of original watermark, the selection of embedding position, embedding formula and the reconstruction of the watermark.

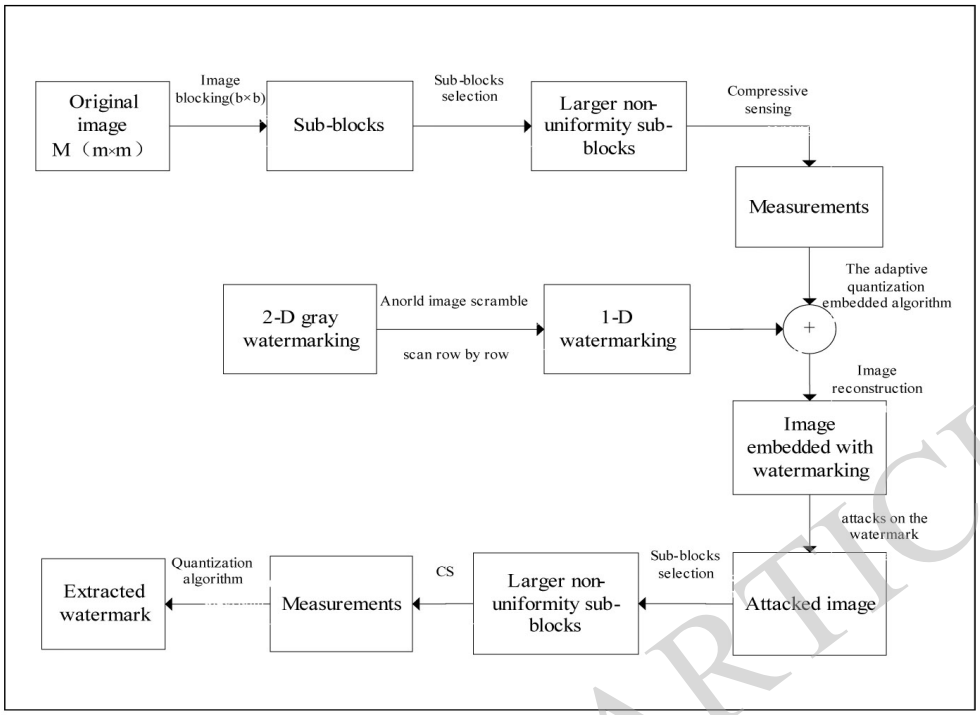

Fig. (1). Proposed digital watermark algorithm.

The watermark extraction process can be viewed as the inverse process of watermark embedding. The basic model of this algorithm is given in Fig. (**1**).

3.1.1. Watermark Image Scrambling

For the sake of security and robustness of the watermark, Arnold algorithm is employed to scramble the 2-D watermark w(x, y) (16×16), the scrambling formula is given as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{16} \tag{5}$$

where (x, y) and (x′, y′) represent the pixel coordinates of original watermark w(x, y) and scrambled watermark w(x′, y′). w(x′, y′) is obtained by scrambled k times on w(x, y). After scrambled, the watermark image is reshaped into one-dimension vector by scanning row by row:

$w_n(i)(i = \{0,1\}, 1 \le i \le 16 \times 16)$.

3.1.2. Embedding Position

Different image patch can be embedded in the watermark with different strength, and the strength of watermark will influence its robustness and invisibility.

In the watermark system, these two features are always contradictory and only one feature could be guaranteed as large as possible on the basis of another feature inevitably in order to get a balance of both. For example, most of energy is concentrated in the low frequency. Any distortion in low frequency part is sensitive to human visual system (HVS). Therefore, it is not easy to keep its invisibility for us to embed the watermark in low frequency part. But the low frequency part has strong sensory capacity, which can be seen as strong background and accommodate more strenghful watermark information. In this way, the robustness of the watermark can be ensured. On the contrary, the HVS system is not sensitive to the distortion in high frequency part, which can ensure the concealment of the watermark. But the embedding capacity of the high frequency part is low. So it's difficult to guarantee the robustness of the watermark. Therefore, whatever the watermark is embedded in the low frequency part or high frequency part, it is to enhance the robustness with the loss of concealment or vice versa.

In this paper, a novel embedding strategy is proposed. Not taking the image as low frequency or high frequency globally, the whole image is divided into blocks and to search those blocks appropriate for embedding the watermark based on some rules. As we know, the information distribution in the image is ununiformed. Some blocks contain abundant texture information, while other blocks are homogeneous. In comparison, the blocks with worse uniformity have high visual capacity and are suitable for embedding strength watermark. The measure of the non-uniformity in the block is given as follows:

Assuming the original image (M×M) is dividing into the b×b blocks. The non-uniformity d(B) of every block is computed by the formula (6):

$$d(B_k) = \frac{1}{b^2} \sum_{i,j \in B_k} \frac{\left| f(i,j) - m_k \right|}{m_k^{1+\tau}} \tag{6}$$

And $k = 1,2 \ldots \frac{M \times M}{b \times b}$, where B_k is the k^{-th} sub-block, the mean of B_k is denoted as m_k, τ is the weighting parameter. The larger value of $d(B_k)$ means the more rich information, and the larger visual capacity. Then we choose the first L sub-blocks, which have larger capability to embed the watermark, so that the robustness of watermark can be ensured.

Next, discrete wavelet transform (DWT) will be performed on each block to get a sparse representation. Then set the sampling rate as σ, and choose a Gaussian random matrix Φ_L ((b*b*σ) ×(b*b)) as a sensing matrix to perform compressive sensing on the sparse wavelet coefficients, thus, we can get the measurements y_i (i=1, 2,…,b*b*σ). Finally, the (b*b*σ)×L measurement matrix is obtained and take the sensing matrix Φ_L as a key to be used for extracting the watermark.

The detailed implementation of above procedure is described in Algorithm **1**.

Algorithm 1. (Compressive Sensing).

Input: I(M×M);

Output: y_i;

Initialization: iterations k=1, j=1,σ = 0.3, N=(m*m)/(b*b)

I (M×M)→ {B_k} (k=1,2…N)

For k=1 to N do

calculate d(B_k);

rank d(B_k) from larger to smaller ;

choose former L(L<N) d(B_k) → B_k;

End

For j=1 to L do

do DWT to $B_k \rightarrow x_t$ (t = 1,2 …,b ∗ b),

Ψ ((b ∗ b) × (b ∗ b)) is the transform matrix;

randn (b ∗ b ∗ σ) × (b ∗ b)→ sensing matrix Φ_j, save Φ_j;

yi = Φ × Ψ × x_t;

j=j+1!

End

3.1.3. Embedding Algorithm

After the measurement matrix is obtained, the watermark information is embedded into the measurement matrix through quantization method. Due to the size of the watermark is b*b, it is necessary to repeat embedding the same watermark K times ($K = L * \frac{b*b*s}{b*b} = L*s$). According to the quantization principle, the measurements yi is modified bit by bit. The embedding formula is as follows:

$$\lambda_i = \text{round}(yi/\delta) \quad (7)$$

$$\delta = a * d(B_k) \quad (8)$$

$$\tilde{y}i = \begin{cases} (\lambda_i - 1/2) * \delta, \text{mod}(\lambda_i + w_n, 2) = 1 \\ (\lambda_i + 1/2) * \delta, \text{mod}(\lambda_i + w_n, 2) = 0 \end{cases} \quad (9)$$

where yi is the measurement before embedded, and $\tilde{y}i$ is the measurement after embedded. The "round" function is used to get the nearest integer, and the "mod" function represents module operation. In addition, δ is the quantization step, which depends on the value of $d(B_k)$, and a is constant. The larger of $d(B_k)$, the larger of date volume and quantization step, then we can embed watermark with more capacity, and therefore the quantization step is adaptable here. Through previous theory proof [9], the equation (9) has optimality. In this way, a watermark with high security, robustness and invisibility can be achieved.

Finally, after embedding watermark into the carrier image, each block is reconstructed by the OMP algorithm mentioned in section 2. Then Inverse Discrete Wavelet Transform (IDWT) will be performed for whole image. Thus, the image embedded with watermark $\tilde{I}$ is obtained.

3.2. Watermark Extraction

The process of watermark extraction isn't ready to discuss in details, considering that the extraction is the inverse process of the watermark embedding. So simple summarization is given as follows: segment the image into the 16x16 blocks, then compute the non-uniformity of each block based on formula (6) and choose the first L blocks of larger non-uniformity to perform compressive sensing according to the key Φ_L. Then the watermark is extracted as follows:

$$\tilde{W}_n = \begin{cases} 1 \; ! \; \text{mod}(\tilde{\lambda}_i, 2) = 1 \\ 0 \; ! \; \text{mod}(\tilde{\lambda}_i, 2) = 0 \end{cases} \quad (10)$$

where $\tilde{\lambda}_i = \text{floor}(\tilde{y}_i / \delta)$, floor is the downward integral function.

4. SIMULATION RESULTS AND ANALYSIS

Although CS has been applied successfully in watermark recently, but most of them are not blind watermark. In this paper, a novel blind watermark embedding algorithm based on CS (BWCS) is proposed. In order to verify the performance of proposed method, the following experimental results will show that a clear embedding image can be obtained even under a low sampling rate, and the proposed method can resist some common attacks in most cases.

Given a 16x16 watermark image, its numerical bits are embedded into the gray carrier image Lena (256x256) or Baboon (256x256), using the watermark embedding algorithm introduced in Section 3. The sampling rate σ is set as 0.3 and the block size b is set as 16. The experiment results are shown in Fig. (**2**). We can hardly distinguish the difference between the original and embedding image visually. This indicates the high invisibility of the watermark.

4.1. Robustness Analysis

To simulate the communication conditions and deliberate or unintentional processing, some attacks need to be used in the watermarked image to test the robustness of a watermark system. Experiments are performed under the filter attack, noise attack or compression attack. The results are compared with traditional watermarking methods based on DWT transform domain (DWT) [10] and non-adaptive quantization watermarking method (NAQW) [11].

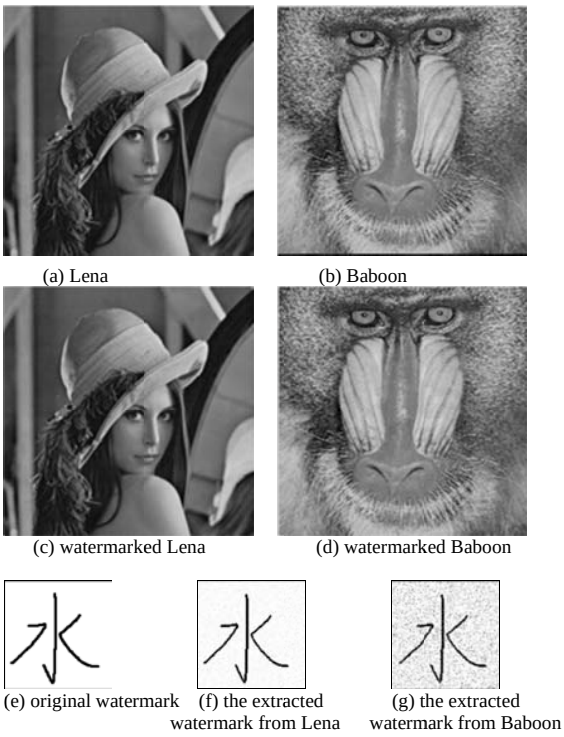

Fig. (2). Watermark embedding results.

(1) Filtering Attack. The watermarked image is filtered by Gaussian Low-Pass Filter (GLPF), shown in Fig. (**3a**). The extracted watermarks by three methods are given in Figs. (**3b-d**). Although the extracted watermarks are not so clear, the key information in Fig. (**3d**) is still clear. The result is better than other two methods.

(2) Noise Attack. The salt and pepper noise with density of 0.02 is added into the watermarked image, the extracted watermarks are showed in Figs. (**4c-d**). Due to the noise interference, some information maybe lost when extracting the watermark through sparse decomposition of the watermarked image. But a clear watermark is still obtained, which is better than that of other two methods. Therefore, the watermark embedding algorithm proposed in this paper has better anti-noise ability.

(3) Compression Attack. The watermarked image is compressed by JPEG algorithm and the recovered watermarked image is shown in Fig. (**5a**). It is obvious in Fig. (**5d**) that the extracting watermark by our proposed method is relative clear even though some information is lost during quantization coding, the quality of which is superior to DWT and NAQW methods. It is enough to demonstrate that the image embedding with watermark by the algorithm in this paper can resist against the JPEG compressing in a great degree.

4.2. Invisibility Analysis

The invisibility of watermark is evaluated by the structure similarity index (SSIM) criterion [12]. SSIM reflects the similarity of original image and the embedding image. The

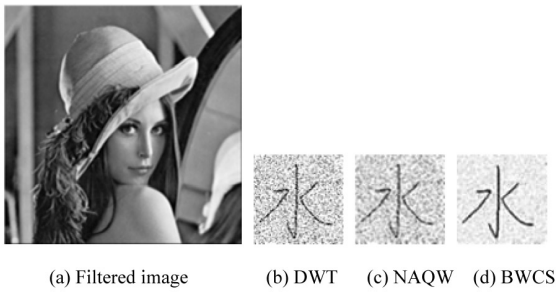

Fig. (3). Filtering Attack.

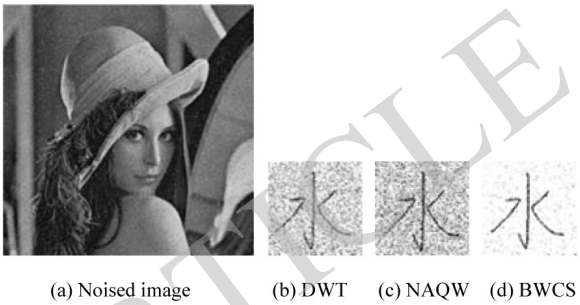

Fig. (4). Noise Attack.

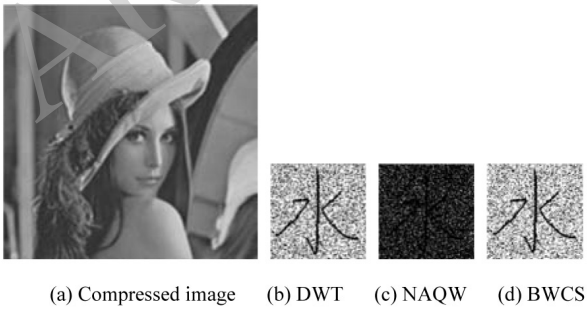

Fig. (5). Compression attack.

larger of the SSIM value, the higher of the watermark quality and the better of the watermark invisibility. The formula is showed as follows:

$$\mathrm{SIMM}(I, \hat{I}) = L(I, \hat{I}) \cdot C(I, \hat{I}) \cdot S(I, \hat{I}) \tag{11}$$

where the brightness similarity function,

$$L(I, \hat{I}) = \frac{2\mu(I) * \mu(\hat{I}) + c_1}{\mu^2(I) + \mu^2(\hat{I}) + c_1} \tag{12}$$

$\mu(\cdot)$ is the average of an image. And the contrast similarity function,

$$C(I, \hat{I}) = \frac{2\sigma(I) * \sigma(\hat{I}) + c_2}{\sigma^2(I) + \sigma^2(\hat{I}) + c_2} \tag{13}$$

$\sigma(\cdot)$ is the variance of an image. And the structure similarity function,

$$S(I, \hat{I}) = \frac{\mathrm{cov}(I, \hat{I}) + c_3}{\mathrm{cov}(I) * \mathrm{cov}(\hat{I}) + c_3} \tag{14}$$

$\mathrm{cov}(I, \hat{I})$ is the covariance between the original image I and the watermarked image $\hat{I}$. The Table **1** shows the invisi-

bility of watermark by the proposed method BWCS in comparison with DWT and NAQW.

It can be easily seen that the SSIM of the BWCS is higher than that of DWT or NAQW, which means that there is higher invisibility of the watermark in this paper than other two methods.

Table 1. Comparison of SSIM.

Original Image	BWCS	DWT	NAQW
Lena	0.94	0.88	0.91
Baboon	0.93	0.86	0.91

4.3. Computation Complexity Analysis

The time cost of an algorithm is an important measure of the computation complexity. The Table **2** gives the comparison of running time embedding the same watermark into the "Lena" and "Baboon" image, using three different methods respectively.

Table 2. Running time comparison.

Original Image	BWCS	DWT	NAQW
Lena	11.31s	18.74s	11.25s
Baboon	11.02s	18.81s	10.97s

We can find the running time of the algorithm in this paper is obviously less than the DWT, but comparable with the NAQW.

CONCLUSION

In this paper, an improved digital watermarking algorithm, which performs digital watermark embedding process in CS domain, is proposed. Experimental results show that the algorithm obtains robust and invisible embedded watermark with larger capacity of data. At the same time, the ability of defending against attack and extraction of embedded watermark is greatly improved. The watermark is detected without any reference to the original image. This remarkably decreases the costs of storing carrier data and the computation complexity. We can achieve a watermark with high security, strong ability of defending against attack and extraction due to the irreversibility of CS.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

The authors would like to appreciate the anonymous reviewers for their valuable comments and suggestions. This work is supported by the Fundamental Research Funds for the Central Universities (No. NCEPU2014MS02).

REFERENCES

[1] V.R. Schydel, A. Triklel, and C. Osbome, "A digital watermark," In: *Proceedings of International Conference on Image Processing.* Texas: IEEE, 1994, vol. 2, pp. 86-88.

[2] E.J. Candes, and M.B. Wakin, "An introduction to compressive sampling," *IEEE Signal Proc. Mag.*, vol. 25, no.2, pp. 21-30, 2008.

[3] H.C. Huang, F.C. Chang, and C.H. Wu, "Watermarking for compressive sampling applications," In: *Proceedings of the 8th International Conference on Intelligent Information on Hiding and Multimedia Signal Processing*, Washington: IEEE, 2012, pp. 223-226.

[4] W.J. Lin, *Reconstruction algorithm for compressive sensing and their applications to digital watermarking*, Jiaotong University: Beijing, 2011.

[5] F. Wei, D. Liang, C. Zhang, and W.X. Bao, "Watermarking algorithm for digital image based on compressive sensing measurements," *J. Anhui Univ.*, vol. 1000-2162, no. 3, pp. 61-68, 2013.

[6] R. Baraniuk, "Compressive sensing," *IEEE Signal. Proc. Mag.*, vol. 24, no.4, pp. 118-121, 2007.

[7] G.M. Shi, D.H. Liu, D.H. Gao, Z. Liu, J. Lin, and L.J. Wang, "Advances in theory of compressed sensing," *Acta Electron. Sin.*, vol. 37, no.5, pp. 1070-1081, 2009.

[8] J. Shihao, X. Ya, and L. Carin. "Bayesian compressive sensing," *IEEE Signal Proc. Mag.*, vol. 56, no.6, pp. 2346-2356, 2008.

[9] Li X D, "Optimization analysis of formulas quantization-based image watermarking," *Opto-Electron. Eng.*, vol. 37, no. 2, pp. 96-102, 2010.

[10] Y.J. Cai, Y. Niu, and S.U. Qing, "Blind watermarking algorithm for images based on DWT-SVD and Fibonacci transformation," *Application Res. Comput.*, vol. 29, no.8, pp. 3025-3028, 2012.

[11] H. Xu, and C.Z. Xiong, "Analysis of quantization-based watermarking," *J. Communi.*, vol. 27, no. 3, pp. 15-27, 2006.

[12] Z. Wang, A.C. Bovik, H.R. Sheikh and E.P. Simoncelli, "Image quality assessment: from error visibility to structure similarity," *IEEE Trans. Image Process*, vol. 13, no.4, pp. 600-612, 2004.

Received: September 12, 2014 Revised: October 19, 2014 Accepted: October 24, 2014