REVERSIBLE WATERMARKING AUTHENTICATION ALGORITHM FOR COLOR IMAGES BASED ON COMPRESSED SENSING

Dong Ruihong[1], Zuo Hangzhou[1, 2], Zhang Qiuyu[1] and Wu Dongfang[1]

[1] School of Computer and Communication, Lanzhou University of Technology， Lanzhou, 730050, China

[2]China Electronics Technology Group Corporation No.20 Research Institute， Xi'an, 710068, China

Emails: dongrh@lut.cn

Submitted: Dec. 18, 2015 ***Accepted: Mar. 30, 2016*** ***Published: June 1, 2016***

Abstract- Aiming at the shortcomings of existing reversible watermarking for image authentication, such as poor ability of tamper detection and localization, and low attention of reconstruction after tampering, a reversible watermarking authentication algorithm based on compressed sensing for color image was proposed. On the side of the sender, the original image has been divided into blocks and carried out compressed sensing to generate image hash which works as the watermark information, and was embedded by the reversible watermarking of difference histogram algorithm. On the side of the receiver, watermark was extracted for authentication. For the tampered block which was failed in authentication, original image will be restored by reconstruction of compressed sensing. Experimental results show that the algorithm combines of reversible watermarking and compressed sensing, so that the detection rate of image authentication has been improved, as well as the robustness to resist sparse noise and cutting and the ability to reconstruct the original image.

Index terms: image authentication, reversible watermarking, compressed sensing, difference histogram, image reconstruction.

I. INTRODUCTION

In the rapid development of computer network technology, multimedia information penetrated into all fields of today, the digital watermarking technology is widely used in digital document authenticity identification, network secret communication, implied title and annotations, using control, etc. Although the carrier of watermark embedding lead to distortion generally do not perceive, but medical images, military map, remote sensing image, the judicial authentication image in areas such as some special applications, often do not allow permanent distortion of watermark carrier. The integrity of the authenticity of the carrier, content to demand higher realm, the carrier of distortion cannot be applied. In the authenticity of the carrier, the integrity of the content to demand higher realm, the carrier of distortion cannot be applied. The reversible watermarking technology not only can extract the watermark at the decoding end without distortion, and after extracting the watermark can be undistorted to restore the original works. Especially the reversible watermarking that was proposed for color images which has higher integrity requirements has been the research hot spot. The proof of integrity and authenticity of reversible watermarking has been one large challenge[1-3]. In fact, generating a copy of digital signal is just reconstructing one same signal. So, when the digital domain of multimedia provide one simple approach of copy, at the same time, keeping integrity and authenticity of signal has became more difficult.

At present, there are three existing approaches which respectively named blind detection, image hashing and digital watermarking to deal with the problems of detection of images tamper[1-3].

Firstly, blind detection can find one kind of the certain particular attack, and the advantage is that it can detect tamper of images directly without any auxiliary information [4,5]. When the detected tamper original signal can’t be used again, it’s a good scheme. But, when the scheme need to simulate all kinds of tamper, it will have lower performance than normative algorithm.

Secondly, image hashing was described by a compact digital content which based on digital signal feature. The image hashing have to meet all these properties: sensing fidelity, single canal,

sensitive for inputs, the evaluation of image quality and using of database retrieval[6,7]. In addition, for a approach to deal with the problem of image authentication, image hashing can combine compressed sensing(CS)[8,9]. CS can reconstruct sample signal from parse sampling and have a lower sampling speed rate than Nyquist. The essence of this method is a kind of skill which can be used in reconstructing signal with the help of sparse or compressible signals. And, this kind of signal can be reconstruct by solving the convex optimization problem.

Thirdly, by being embedded in digital content, digital watermarking can be used in image authentication and integrity detection, at the same time, the loss of image integrity can be represented by fragile watermarking[10,11].

As the literature[10] says that the wavelet domain can be embed in watermark, and these operations can be located in frequency and space domain. The literature[11] says watermark signal was embed in least significant bit by the way of grading system. And, in this condition, it will effectively oppugn the vector quantitative attack. What's more, half fragile watermark combine compressed sensing is an approach to deal with the image authentication effectively[12-14].

In literature[12], sampling the image and creating projection, and random projection using unified quantize. Low-density Parity-check Codes can be used in forming hashing which embed as a robust watermark. Recovery watermarking lead to this condition that presumptive projection can be used in the distortion estimation of all the received images. If the image tamper is enough sparse, the tamper can be located. The literature[13] put forward a new algorithm based on image tamper detection and location and original image recovery(if the tamper is enough sparse).

The literature[14] put forward a new watermarking detection method based on compressed sensing in transform domain. This method depends on the fact that the coefficient of natural image is enough sparse in transform domain. Furthermore, by the way of using threshold, the coefficient will become a deep sparse. And the plus-xing watermark scheme can be embed middle frequency coefficients. Under the premise of sparse and the ratio between code word length and watermark length, watermark can have a recovery by compressed sensing. The

resistance poison noise robustness has been improved by the author. The literature[14] put forward a new watermarking detection method based on compressed sensing in transform domain. This method depends on the fact that the coefficient of natural image is enough sparse in transform domain. Furthermore, by the way of using threshold, the coefficient will become a deep sparse. And the plus-xing watermark scheme can be embed middle frequency coefficients. Under the premise of sparse and the certain ratio between code word length and watermark length, watermark can have a recovery by compressed sensing. The watermark resistance poisson noise robustness has been improved by the author.

All the above, these literature have some disadvantages as follow:

(1) Not a reversible watermark, so cannot be used in sensitive image;

(2) The authentication result just obtain tamper detection or tamper location;

(3) Didn’t reconstruct or evaluate the tamper signal;

(4) Most researched images are gray images without practicality;

This paper promote a kind of color image reversible watermark authentication algorithm based on compressed sensing(CS-CRAW). On the sender, with the help of this algorithm, the image is reconstructed by discrete wavelet transform. Meanwhile, the subband image hashing was counted. By compressed sensing and binding the key, the reversible watermark can be generated. And, make use of reversible watermark algorithm adjusted by difference histogram to embed image hashing in the vector color image as a watermark. On the receiver, extract the watermark. And, with the key reconstruction of hashing watermark, the compared authentication can be realized by comparing extracted hashing with reconstructed hashing. The algorithm combined with compressed sensing and image reversible watermarking, and make full use of some properties, for instances: compressed sensing high compressed image and accurate reconstruction image and so on, to realize the detection and location of tamper. What’s more, by this way, enhance the security of transmission of secret information, improve the resistance coefficient noise and tailoring of robustness, decrease the complexity of watermarking and increase the detection rate of authentication.

II. THE RECONSTRUCTION OF COMPRESSED SENSING SIGNAL

Compressed sensing theory is a kind of theoretical framework and to achieve compression. The literature[7,8] show the reconstruction of compressed sensing sparse signal. The signal $X(X \in R^N)$can be expressed as:

$$X = \Psi S \tag{1}$$

There are four variables, let:1) Ψ be n*n orthogonal based matrix; 2) S be K-sparse matrix; 3) X be sparse signal; 4) S be the sparse coefficient of X on Ψ;

The observed value Y of M*1 matrix generate by follow equation:

$$Y = \Phi X \tag{2}$$

where Φ be M*N observed matrix(M<N), reference equation (1), the above equation can therefore be written as

$$Y = \Phi X = \Phi \Psi S \tag{3}$$

where compressed sensing matrix $\Theta = \Phi \Psi$ meet limited isometric characteristics, S can be written as follows:

$$\hat{S} = min \| S' \|_0 , \mathbf{\Theta} S' = Y , \tag{4}$$

where l_0 norm express the number of non-zero coefficient in S', and this is a NP problem without a good approach to deal with.

$$\hat{S} = min \| S' \|_1 , \mathbf{\Theta} S' = Y , \tag{5}$$

where

$$M \geq O\ (K\ \log\ N). \tag{6}$$

By solving one more simple l_1 optimization problem, the K-spare signal can be reconstructed (require that Φ and Ψ are uncorrelated). The little difference make problem become convex optimization one. So, the problem can simplify as linear programming problem. The BP algorithm become the typical algorithm represents. Even if BP algorithm is feasible, there are still two problems need to handle. 1) When process the norm size of basic image, the computational complexity is cannot be tolerant. 2) When the number of sampling point meet M ≥

cK, $c \approx \log 2(N/K+1)$, the order of reconstruction calculation complexity is $O(N^3)$.

III. PROCESS OF CS-CRAM ALGORITHM

The process of CS-CRAW algorithm authentication be shown in Figure 1. The generator embed watermark in original image, then send it to the receiver. After receiving the watermark image, the authentication system give two messages including distortion complexity and authentication result of original image and tamper image.

a. The structure of image hash

By the way of image blocking and having a discrete wavelet transform, the wavelet transform coefficient x of subbend image can be generated. Then, x random projection to obtain observed y:

$$y = \Phi x. \tag{7}$$

where key S generated by key generator, Φ be orthogonal Gaussian matrix generated from key S. The random key S only belongs to the generator and decoder. So, the decoder need the same key S which is necessary for the receiver to generate Φ.The observed y use the unified quantization and coding to produce image hashing $H \in \{0,1\}$.

b. Watermark embedding process

CS-CRAW algorithm uses the discrepant absolute value of difference histogram to adjust embedding watermark. Firstly, count the difference histogram of color components of color image. Secondly, obtain the absolute value of difference from difference histogram. Finally, adjust absolute value of difference to embed watermark.

Figure 2 show the histogram of color image (512*512) named Lena where R, G, B respectively red, green, blue three color channel. d_1 be the difference of row vector pixel of component R; d_2 be difference of row vector pixel of component G; d be the difference of d_1 and d_2.

From the figure 2, we can see obviously that the difference histogram (d_1) of component R is more aggregated than the histogram of component R and mainly distributed nearby zero. At

the same time, the absolute value d can be obtained by the difference between d_1 and d_2 and the histogram of absolute value of d which is basic within 20 is more aggregated. So, the CS-CRAW algorithm can realize that obtaining large embedding capacity and ensuring high image quality.

c. Watermark detection authentication

Firstly, the integrity authentication use DWT transformation to process the received image. The receiver extract the watermark information from watermark image and recover the vector image. And the watermark information decryption can generated $\hat{y}$ At the same time, using the same key S to process vector image and have an observation projection for $\tilde{y}$. If the extracted value y is matching with the observed value y ($\hat{y} = \tilde{y}$), the image can be asserted that it's complete.

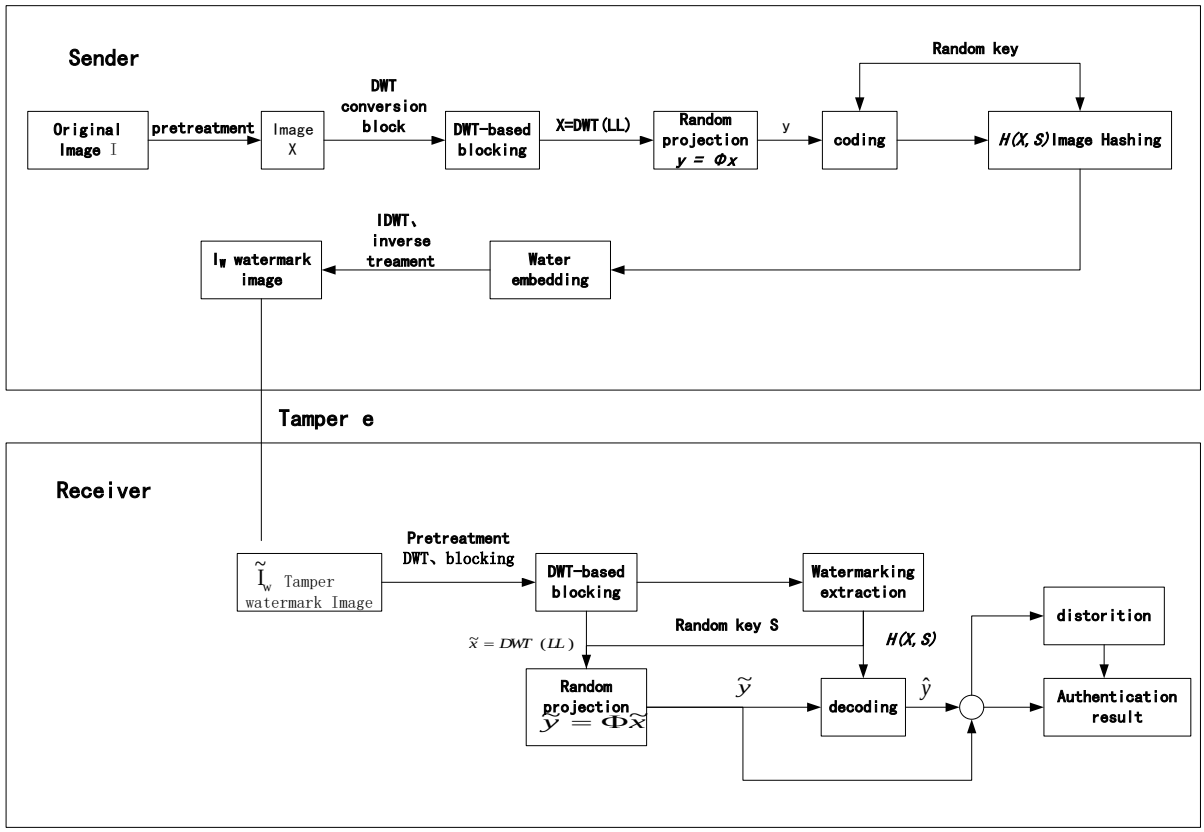


Figure 1 color images reversible watermarking authentication system based on compressed sensing

d. The tamper reconstruction of image block

After the authentication of vector image which use the embedded watermark information, if the image block is subjected to tamper attacking, using compressed sensing to reconstruct tamper block. Figure 3 show the process of tamper reconstruction of image block.

Assume that the model of image which is subjected to sparse pulse tamper change into:

$$\tilde{x} = x + e \quad , \tag{8}$$

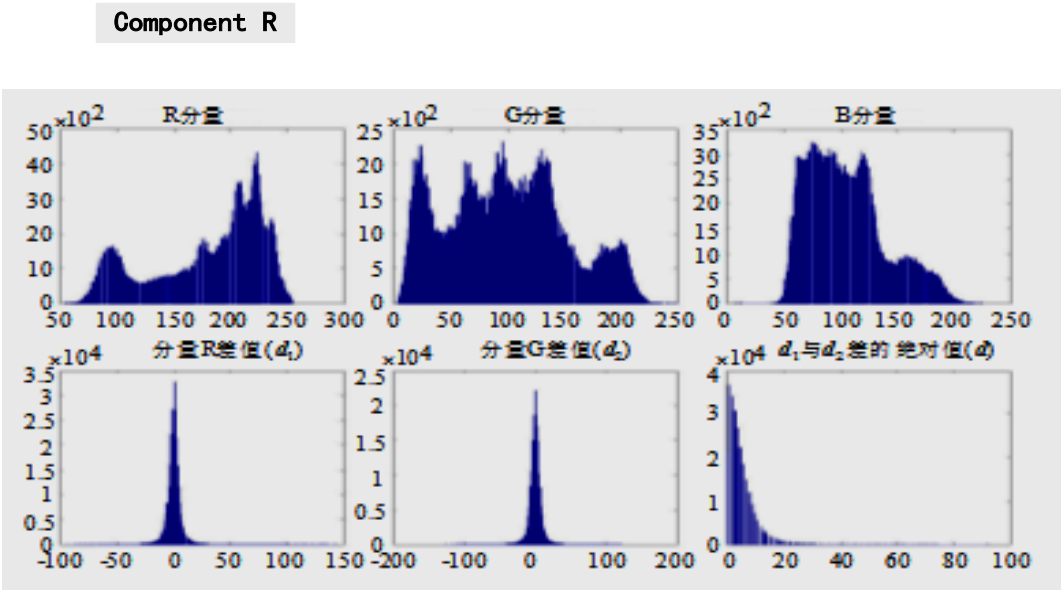


Figure 2 The related histogram of color image (Lena)

Where $e \in R^N$ is K-light noise,noise generated the error of random projection b can be represented as:

$$b = \tilde{y} - y = \Phi(\tilde{x} - x), \tag{9}$$

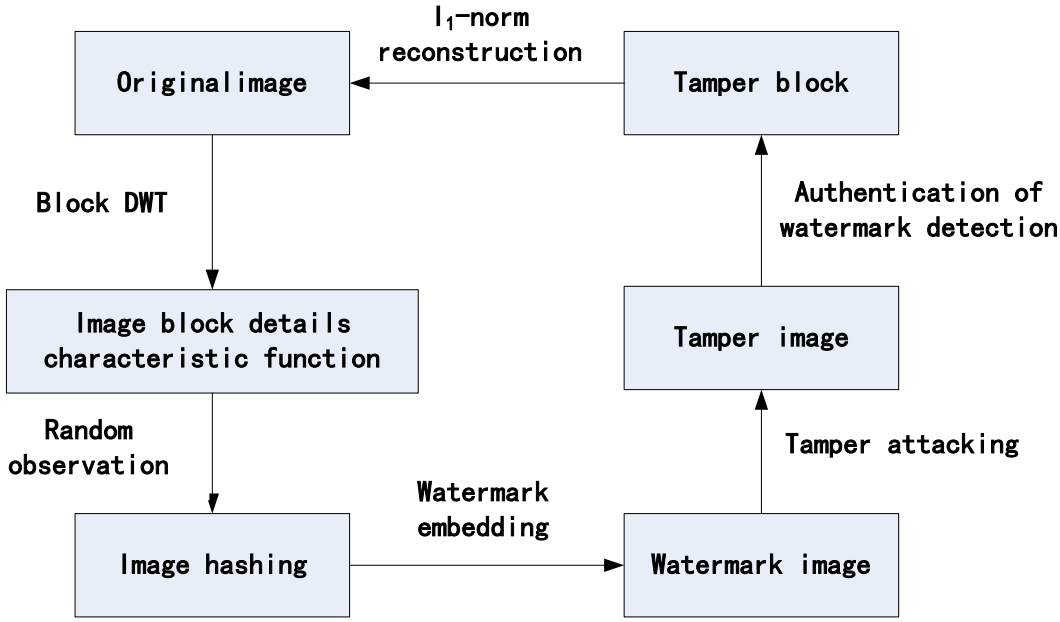


Figure 3 the flow chart of image tamper block reconstruction

Because of the absence of original signal y, the error of random projection b generated by noise can be replaced by follows:

$$\hat{b} = \tilde{y} - \hat{y} = \Phi(x+e) - Q(\Phi x) = \Phi e + \Phi x - Q(\Phi x) = \Phi e + z\,, \tag{10}$$

Where $Q(\cdot)$ represent quantitative operation, z represent the error can bring by quantitative operation. The algorithm use l_1- norm reconstruction in chapter 2 to reconstruct image. For the reconstruction of tamper ,need the follow equation:

$$\hat{e} = min \| e \|_1 \quad s.t. \quad \left\| \hat{b} - \Phi e \right\|_2 \le \varepsilon \quad , \tag{11}$$

Finally, for the evolution of K light tamper e solved expression (11), the compressed sensing theory demand that the value of observation M must meet the follow equation:

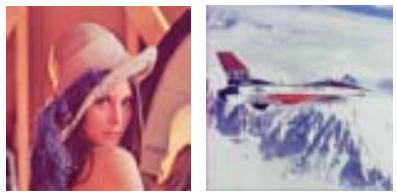
$$M \ge cK \log(N/K) \quad . \tag{12}$$

Where constant c usually dependent on the algorithm of equation (11).

IV. THEEXPERIMENTALRESULTS AND ANALYSIS

The experimental environment demand:Intel(R) Core(TM)2 Duo CPU,1G memory, Win7 operating system, and a experimental platform which installs MATLAB 2012b software.

Two classical images which have the different texture feature, which are 24bit color images(512*512) and the test images, can be obtained from the UCID image library of Columbia University[15].



Lena **Airplane**

Figure 4 original vector color images used in experiment

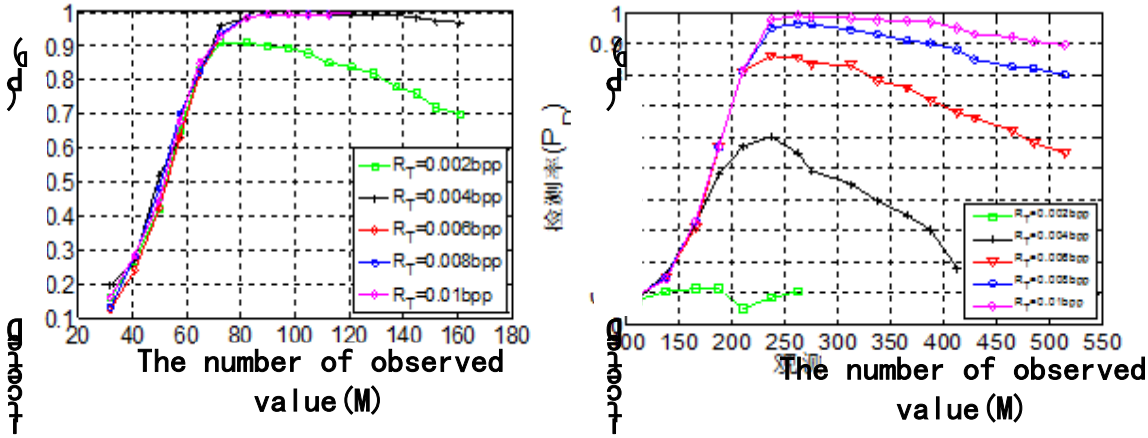
There are two evaluations: true positive detection rate and peak signal to noise ratio. And the evaluations can be used to measure the authentication precision quasi degree of image, as shown in Figure 4.

a. The performance of algorithm detection rate

Under the condition of different degree sparse tamper, the CS-CRAW algorithm simulate the tamper location system for test images. Firstly, the images can be divided into (32*32) pixel block which are not overlapping. Calculating the wavelet transform low frequency coefficient(LL) of block and priority arrange by rows. The calculated results can be expressed by x which meet the elements number(N=256). Making full use of variance σ_s^2 =1000, the algorithm can stimulate tamper when x has K Gaussian noise in random positions. With the help of hashing value H, assume that random measured value y can decode correctly. That is to say,the mean error of the decoded $\hat{y}$ and $\tilde{y}$ which is generated from random projection are equal.

The CS-CRAW algorithm, by the way of reconstructing tamper and comparing estimated tamper position with practical tamper position, evaluate the performance of tamper location. With the change of threshold T, when the per pixel average ration of number and total rate of the observed value meet RT=MR(D)/N, the true positive detection rate ROC curve can be generated. Define zero false reject rate-detection rate(P_D) is the highest value of the true positive rate ROC curve and the zero value of the false positive rate ROC curve. Because of this, the system can detect any conditions of tamper information. The true positive detection rate curve has the different rate of hashing R_T, as shown in figure 5.

Figure 5 (a) show that the different ratio of image hashing R_T corresponding to the different detection rate P_D. With the increasing of the number of observed value, it meet K/N=0.01. Image hashing which is one part of the image generates the different image hashing ratio RT which led to the different detection rate. For a fixed detection rate, with the increasing of the number of observed value, the average ratio of observed value decreases. Improving detection rate P_D is associated with the increasing of the number of observed value, and detection rate reached 1 finally. Under the condition that observed value is smaller than the constraint condition equation (12) and the l_1-norm reconstruction can lead to the bigger false positive rate. It is said that only the small part of tamper location can accord with the realistic cases. Because the tamper e of reconstruction generates more non-zero coefficients which cannot accord with the real tamper. When M meets the equation (12), the detection rate R_D obtains the peak.



(a) K / N = 0.01 **(b) K / N = 0.05**

Figure 5 the true positive detection rate of different hash ratio R_T

As shown in Figure 5, when M nearby 80, detection rate P_D obtain the peak. So, 1% sparse tampers of constant c which equal to 1.72 can be verified. In the low bit rate curve (shown in figure5 (a), RT=0.002bpp), when the observed value got the high value, however, the detection rate decreased. And when the number of the observed value obtains the very small value, the noise e of reconstruction is subjected to serious distortion. So, when reconstructing random observed value, the influence of quantization noise cannot be neglected.

The figure5 (b) shown that under the same experimental conditions, the 5% sparse tamper can be obtained, which can just prove the above issues. When the detection rate P_D nearby $M \geq 250$(c=1.63), the rate can reach the peak. From the equation (12), it can be know that equation (11) need more observed value when the sparsity increasing. So, when figure 5(b) has the same rate as figure 5(a), his number of observed value is smaller than the condition of 1% sparse tamper. And, if detection rates PD reach maximum 1, the larger number of observed value needed for the constitution of the image hashing.

b. Tamper detection location and reconstruction of image

The original image experience wavelet transform by the using of CS-CRAW algorithm. The coefficient of image details characteristics experienced compressed sensing is embedded into vector image. When the image happened sparse noise tamper, the tamper can be detected by the

using of extracted watermark. At the same time, the coefficient of image details characteristics can be used to reconstruct the original image, which obtains the good results, and the detection of noise tamper and reconstruction results have been shown in figure 6.

The above images shows that the tamper area can be detected accurately by the way of extracting the watermark information and the authentication when the images experienced sparse noise tamper. Making full use of image characteristics coefficient, the image can be reconstructed. As shown in figure 6(a) Lena, the SNR(signal to noise ratio) between reconstructed image and original image is 39.66dB and the SNR of figure 6(b) is 39.11dB. The CS-CRAW algorithm can divide image into pixel block(32*32) which are not superimposed. Every pixel blocks experience the wavelet transform and the characteristic coefficient of image wavelet can be embedded into other pixel blocks. If the tamper has happened on the image, the tamper blocks can be reconstructed by the using of the embedded coefficient and compressing sensing .

The figure 7 shows that the location of cutting area can be detected accurately by the way of extracting watermark information when the images have experienced the single block cutting. And the the characteristic coefficient of cutting area can be used to reconstruct the original images. Figure 7(a) is contradistinctive figure of experimental results. And the SNR between reconstructed images and original images is 42.57dB and the SNR of figure 7(b) is 41.24dB.

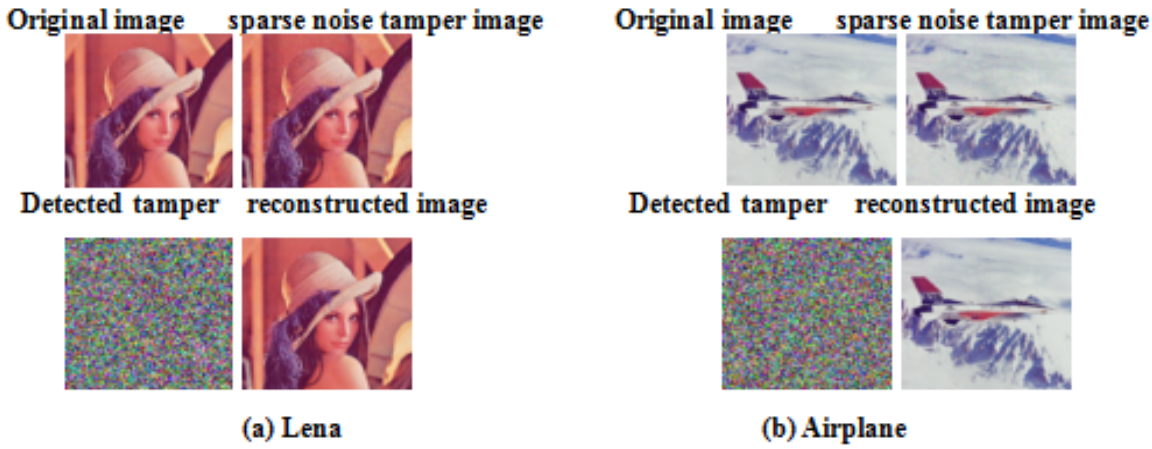


Figure6 the noise tamper detection and reconstruction of image

The figure7 shows that the cutting area can be detected accurately by the way of extracting watermark information and authentication when image experienced many departments cutting. Making use of characteristic coefficient of cutting area to reconstruct the cutting area, the image can be reconstructed finally. Figure 8(a) is the contrast diagram of image experimental results. The SNR between reconstructed image and original image is 40.63dB. And the SNR in figure 8(b) is 39.74dB.

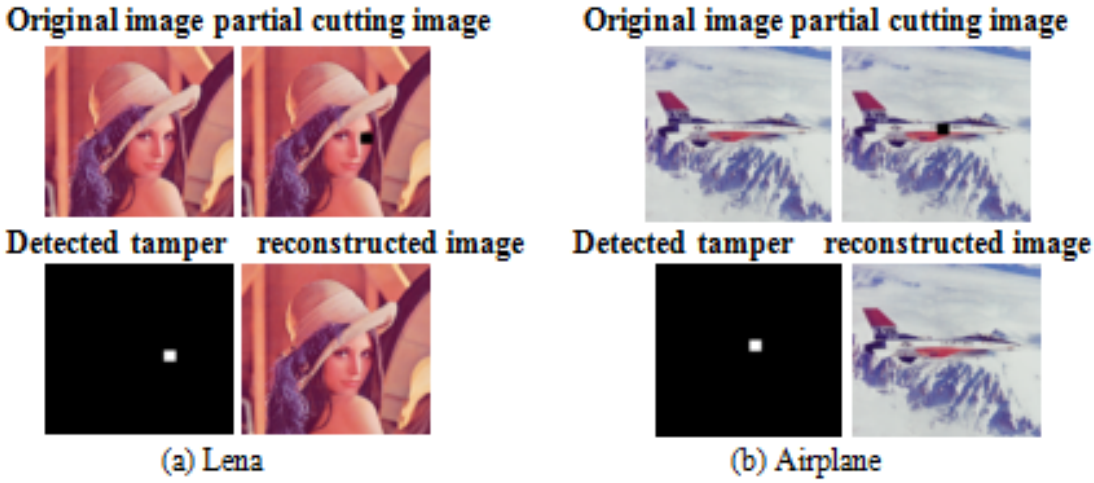


Figure7 single block cutting tamper detection and reconstruction

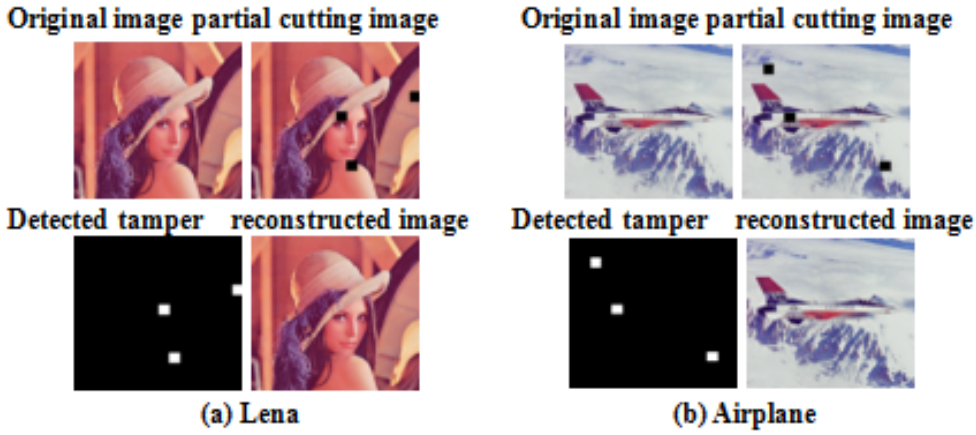


Figure 8 many departments cutting detection and reconstruction of image

V. CONCLUSIONS

The paper puts forward color image reversible watermarking authentication algorithm based on compressed sensing. Firstly, the low frequency coefficient of gray image of vector color image experienced compressed sensing and random projection and generated the watermark. The details characteristics of image can be completely expressed by watermark information. Then embedded watermark can be adjusted by the absolute value of difference between difference histogram of components. For a high image quality, the CS-CRAW algorithm only considers the embed of two components (R, B) and ignores the embed of green color component which is the most sensitive for human visual system(HVS). The results show that the authentication of image needn't the original image and blind detection can extract the watermark information in the receiver for the authentication. If authenticating the image without and tampers, the original image can be recovered without any loss. When image experiences the sparse noise pulse, the original image can be reconstructed by the way of watermarking location of tamper and the compressing sensing. The CS-CRAW algorithm can be used in the tamper location of vector image and the reconstruction of sparse noise tamper. And the algorithm obtains very good effects and improves the robustness of watermark algorithm resistance sparse noise and resistance tailoring.

ACKNOWLEDGEMENTS

This work is partially supported by the National Natural Science Foundation of China (No. 61363078), the Natural Science Foundation of Gansu Province of China (No. 1212RJZA006, No. 1310RJYA004). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] Kamran, Asifullah K, Sana A M, “A high capacity reversible watermarking approach for authenticating images, Exploiting down-sampling, histogram processing, and block selection”, Information Sciences, VOL. 256, NO.1, 2014, pp.162-183.

[2] Wang X, Pang K, Zhou X, et al. “A visual model based perceptual image hash for content authentication”, IEEE Transactions on Information Forensics and Security, VOL.10, NO.1, 2015, pp.1336-1349.

[3] Lo C C, Hu Y C. “A novel reversible image authentication scheme for digital images”, Signal Processing, VOL. 98, NO.5, 2014, pp.174-185.

[4] Farid H. “Exposing digital forgeries in scientific images”, Proceedings of the 8th workshop on Multimedia and security, Geneva, Switzerland, ACM, 2006, pp.29-36.

[5] Johnson M K, Farid H. “Detecting photographic composites of people” Proceedings of the 6th International Workshop on Digital Watermarking, IWDW 2007. Guangzhou, China, Springer Berlin Heidelberg, 2008, 5041 LNCS: 19-33.

[6] Swaminathan A, Mao Y, Wu M., “ Robust and secure image hashing”, IEEE Transactions on Information Forensics and Security, VOL.1, NO.2, 2006, pp.215-230.

[7] Monga V, Evans B L. “Perceptual image hashing via feature points: performance evaluation and tradeoffs”, IEEE Transactions on Image Processing, VOL. 15, NO.11, 2006, pp.3452-3465.

[8] Donoho D L. “Compressed sensing”, IEEE Transactions on Information Theory, VOL. 52, NO.4, 2006, pp.1289-1306.

[9] Candès E J, Romberg J, Tao T. “Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information”, IEEE Transactions on Information Theory, VOL. 52, NO.2, 2006, pp.489-509.

[10] Kundur D, Hatzinakos D. “Digital watermarking for telltale tamper proofing and authentication”, Proceedings of the IEEE, Vol. 87, No.7, 1999, pp.1167-1180.

[11] Celik M U, Sharma G, Saber E, et al. “Hierarchical watermarking for secure image authentication with localization”, IEEE Transactions on Image Processing, VOL. 11, NO.6, 2002, pp.585-595.

[12] Valenzise G, Tagliasacchi M, Tubaro S, et al. “A compressive-sensing based watermarking scheme for sparse image tampering identification”, Proceedings of the 2009 IEEE International Conference on Image Processing, ICIP 2009, Cairo, Egypt, IEEE, 2009 ,pp.1265-1268.

[13] Zhang X, Qian Z, Ren Y, et al. “Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction”, IEEE Transactions on Information Forensics and Security, VOL. 6, NO.4 , 2011 ,pp.1223-1232.

[14] Sheikh M, Baraniuk R G. “Blind error-free detection of transform-domain watermarks”, Proceedings of the 2007 IEEE International Conference on Image Processing, ICIP 2007, San Antonio, TX, United states, IEEE, 2007, 5, pp.453-456.

[15] Schaefer G, Stich M. “UCID-an uncompressed colour image database” , Proceedings of SPIE, Storage and Retrieval Methods and Applications for Multi-media, San Jose, CA, United states, The International Society for Optical Engineering, 2004, 5307, pp.472-480.

[16] Wenqing ,Chen, Tao Wang and Bailing Wang, “Design of digital image encryption algorithm based on mixed chaotic sequences", International Journal on Smart Sensing and Intelligent Systems, VOL. 7, NO.4, pp. 1453-1469, 2014.

[17] Yanmin LUO, Peizhong LIU and Minghong LIAO, “An artificial immune network clustering algorithm for mangroves remote sensing”, International Journal on Smart Sensing and Intelligent Systems, VOL. 7, No. 1, pp. 116-134, 2014.

[18] Daode Zhang et al., “Research on chips defect extraction based on image-matching”, International Journal on Smart Sensing and Intelligent Systems, VOL. 7, NO.1, 2014, pp.321-336.