TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.7, July 2014, pp. 5399 ~ 5407
DOI: 10.11591/telkomnika.v12i7.5373

Research of Blind Forensics Algorithm on Digital Image Tampering

Jin Hongying
Computer college of China West Normal University
Shida Road No. 1, ShunQing District, Nanchong, Sichuan, 637002, China
e-mail: jinhongying_cwnu@163.com

Abstract

With rapid development of the internet and the multimedia technology, the digital images tampering with blind forensics technology become a new research direction in the study of information security. The technology is based on the digital image, and it is only to realize image integrity and authenticity of the certification, so it is widely used in the civil fields such as news reports, judicial proof and military fields such as military intelligence analysis. So the research of it has great significance and broad application prospect. In the paper, the exploration and research on the paste tampering and splicing tampering with blind forensics algorithm are made. The blind forensics algorithm based on radial Krawtchouk copy-and-paste invariant moment is proposed. As the current copy-and-paste blind forensics algorithm has low localization accuracy, and poor robustness of the post-processing in solving the problem. Based on sliding window block matching method and the radial Krawtchouk invariant moment, it proposes a copy-and-paste tampering with blind forensics algorithm. The experimental results show that the algorithm can effectively locate the tampered area, and it has very strong robustness of the rotating operation, JPEG compression, Gaussian noise, etc.

Keywords*: blind forensics algorithm, digital image, tampering, research*

1. Introduction

With the rapid development of multimedia and digital technology, digital photos have become the indispensable necessities of life. Traditional film pictures are instead by digital photos, which show that the “digital image era” has arrived. In order to achieve the enhancement purpose of the digital image visual effect, a large number of image processing and editing software, such as Photoshop, ACDSee, libraries have been widely used. However, advanced technology brings the convenience in daily life, at the same time, they also bright some hidden trouble in modern life. With the widely application of the image processing software, the tampering of digital image becomes more convenient, its effect is also very realistic, so some people with malicious motives spread forging digital images in order to achieve ulterior purpose. When tampered with digital image is widely applied to media reports, scientific research and the court, it will no doubt affect the normal order of society and cause damage to personal rights [1-3].

2. Digital Image Forensics

The digital image forensics technology can be divided into active and passive forensics technology. Active forensics technology is embedded in the media in advance indicative information, and make authentication of embedded information. The existing active forensics technology mainly includes digital watermarking and digital signature, etc. These techniques are adopted by the basic thought of embedding or add additional information authenticity and integrity of digital image identification.

2.1. The Digital Signature

The digital signature technology is also known as electronic signature, it is attached according to the cables in electronic form, and the content is used to identify the signature identity data. When use the digital signature to identify the authenticity of digital media, it should

Received December 15, 2013; Revised January 21, 2014; Accepted February 18, 2014

extract the original media data information in advance and keep it in storage, through storing the information to identify the object information to make the identification of the object.

2.2. Digital Watermarking.

Digital watermarking according to its tolerance to image changes, it can be divided into the fragile watermark [4-7], half a fragile watermark and robust watermark [8]. Fragile watermark and fragile watermark are both apply the authenticity and integrity of accurate in the certification, the difference of them is that when containing watermark medium is changed, fragile watermarking are easily damaged, then it is hard to be detected; And semi-fragile watermarking can withstand reasonable certain extent of distortion, and the unreasonable distortion will cause further deteriorate.

Robustness of watermark is hard to remove and has a strong anti-interference ability, and it can also able to withstand all sorts of commonly editing process and watermark attack tools. It is mainly used for copyright information identification of digital works. As for each type of digital watermarking, their basic framework is mainly includes three parts: embedded part, transmission channel, and extracting part. Embedded terminal is embedded with the digital media known as part of the identification information; Transmission channel is the carrier of identification information, it can pass parameters and key information to extracting part; Extraction part can extract information to identify the object, and then according to the extracting accuracy and completeness of the information make the identification and authentication of the objects.

3. Overview of Blind Digital Image Forensics Technology

3.1. Definition and Classification of Blind Digital Image Forensics

Blind digital image forensics refers to the process of using embedded information to identify authenticity of image and obtain evidence; the whole process is independent of any signature or premise information [9]. Despite the current digital image manipulation technology has been very mature, the fake effect of tampering of digital image is not easy to cause visual differences among people, but tampering operation will inevitably cause change in the statistical features of digital image [10].

Image blind forensics is to use the statistical characteristics changes of image and make the determination of the authenticity, integrity, and primitivism of the image [11-12]. Blind forensics technology has no special requirements for image acquisition device, compared with the active forensics technology, it also do not need to add any image authentication information, so it has important practical value. Blind forensics technology is mainly for image content tampering and for the evidence collection,

Now, the image blind forensics technology can be divided into the following three categories:

1. In view of the image content authenticity discrimination: the main purpose is to judge whether initially acquired images are suffered with some form of processing or tampering.

2. In view of the image source identification: it can judge the image data acquisition device, this kind of technology will connect images with the common features image source, in order to match the images to a particular type of the source device.

3. Analyses the hidden image forensics: As for the integrity of image tampering is an important information security technology branch, so use it as a part of the image forensics. Compared with hidden analysis technology, image hidden deeper analysis forensics need the secret information extraction.

As for digital image tampering operations, the common tampering means are through the copying of original image and masking specific target area of image, thus create the scene which are not in the original image scene or hide some important target, the purpose of this tampering means is the copy-and-paste image tampering [13-14]. The tampering method has many obvious advantages, because the copy-and-paste part of image has no obvious visual difference in terms of brightness, color, noise with the original image, therefore, the tampered image looks realistic, it's hard to judge from the vision. And due to its operation is simple; the current copy-and-paste tampering has a very wide range of applications. In this article, we will put forward a new algorithm to improve the blind forensics detection effect and robustness of the algorithm [15-17].

4. The Model of Copy-and-paste Tampering

Copy-and-paste perform tampering operation in the same image, the operation is usually adopted copying method. The paste and copy part have no intersection or overlap in the image and position deviation is also obvious. From the operation process of copy-and-paste, the tempering image should have the following features:

(1) The same image has the same or similar connected area;

(2) Displacement of the identical or similar area is often greater than a certain threshold value;

(3) The area of these areas is often greater than a certain threshold, which is the area is large enough. During the study, researchers often to simplify the research question, if we make the hypothesis that the tampered image is only one area has been copied and pasted to another area in the image.

4.1. Simple Copy-Mobile-Paste Region Tampering Model

Simply copy-mobile-paste region tampering refers to the area to be copied only after displacement of simple operation, and paste it directly to other area in the image, not after processing operations such as scaling, rotation, therefore, copy area and sticky stick area is equal in the area, just exists position deviation between copy area and paste area. For this type of Tampering, its model is copy-mobile-paste tampering model, just as shown in the Figure 1.

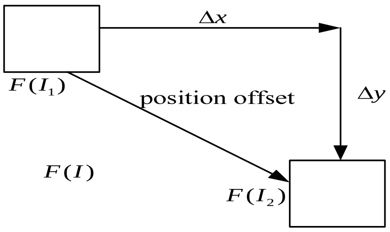


Figure 1. Copy-move-paste Region Tamper Model

As shown in the Figure 1, the origin file is $F(x,y)$, after tampering the file can be expressed as $F^{'}(x,y)$, and the following type can be obtained which is expressed as (1):

$$F^{'}(x,y)=\begin{cases}F(x,y) & (x,y)\notin I_2\\ F(x+\Delta x,y+\Delta y) & (x,y)\in I_2\end{cases} \tag{1}$$

Where the Δx and Δy represent the displacement of the x and y, and the I_1 represents the copied area, I_2 represents the pasted area and the two area is the same, $F(x,y)$ represents the gray value of position (x,y) of the file and $F^{'}(x,y)$ represents the gray value of position (x,y) after tampering.

4.2. Copy-Paste Area Tampering Model through Specific Processing Operations

Through certain processing of copy-and-paste area tamper with the model, also known as copy-transform-mobile-paste tampering model, it refers the copied region after post-processing operation such as scaling, rotation, and then move it pasted into other areas of the image of the tamper with the operation. According to the tampering process, The tampering can not only causes the position offset between copy area and the paste area, at the same time, the two area will meet certain transformation relationship between regions. The tampering model is as shown in Figure 2 and Figure 3.

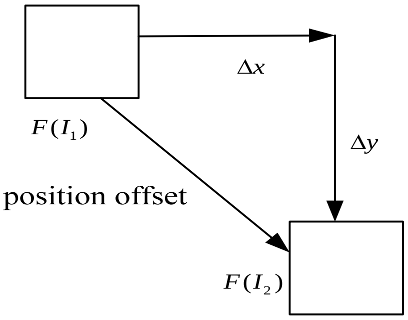


Figure 2. Copy-rotate-paste Region Tamper Model after Certain Operation

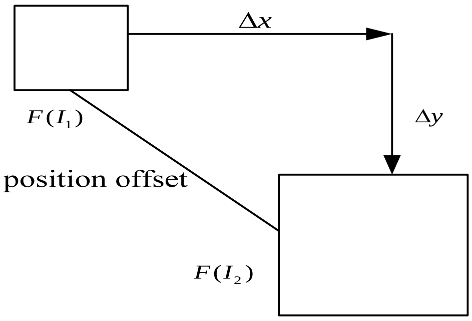


Figure 3. Copy-zoom-paste Region Tamper Model after Certain Operation

According the model, the origin picture $F(x,y)$ and tempered picture $F^{'}(x,y)$ can be expressed as (2):

$$F^{'}(x,y)=\begin{cases}F(x,y) & (x,y)\notin I_2\\ T(F(x+\Delta x,y+\Delta y)\times h(x,y)+n(x,y) & (x,y)\in I_2\end{cases} \quad (2)$$

Where, $F(x,y)$ denotes origin picture and $F^{'}(x,y)$ denotes tempered picture, he I_1 represents the copied area, I_2 represents the pasted area. In the model, when the picture is zoomed, the area is not the same, and the T represents the transform of the zoom and rotation. $h(x,y)$ and $n(x,y)$ represents the other operations.

5. Radial Krawtchouk Copy and Paste Blind Forensics Algorithm of Invariant Moments

5.1. Algorithm Theory

Aiming at a kind of common image forensics copy-and-paste tampering, it proposes a blind forensics algorithm based on radial Krawtchouk moment invariants. The main idea of the detection algorithm is local matching. In the first step, it uses the wavelet transform to extract the low frequency component of image, and then it the extract invariant radial Krawtchouk moment of low frequency component and the feature vector of composition characteristic matrix are dictionary sorted. It can realize the matching of characteristics pieces together coupled with similar threshold, blocks of spacing and the area threshold, it finally debugs mathematical morphology to determine the final copy-and-paste tampering area.

Three Points of Algorithm are as below:

(1)Through DWT processing with the suspect image, and extracting image of low frequency subband, it can greatly reduce the number of image block, and the low frequency is not sensitive to noise at the same time, which can enhance the extracted features robustness.

(2) The main ideas of copy-and-paste tamper detection is local matching, that is make wavelet subband block in low frequency of the image, and then make the image feature extraction, and then match all of the extracted image features, when the matching error is less than a certain threshold, it can be considered a success match, it is the core of the algorithm.

(3) As for the selection of image content features. The radial Krawtchouk moment invariant feature of image block, copy-and-paste tamper with the detecting images, because Krawtchouk moments is based on classical discrete Krawtchouk polynomial. Radial Krawtchouk can well describe the image feature invariant moment, and has the good distinguish identification features. Second, the radial Krawtchouk invariant moment also has rotation invariance, the tamper is through with the copy-and-paste method, and it can reprocess the operation. For instance as one of the most common copy-rotation-displacement-paste mode, it not only can enhance the visual effect of modification, and harder to detect, because some algorithm can not resist rotation operation performance. Therefore, the radial Krawtchouk has good description of image rotation invariant moment features for image tamper detection. Based

on the above analysis, in the paper, it selects the radial Krawtchouk moment invariant feature image block, and image copy-and-paste tampering method with blind forensics algorithm. Flow chart of the algorithm is as shown in the Figure 4.

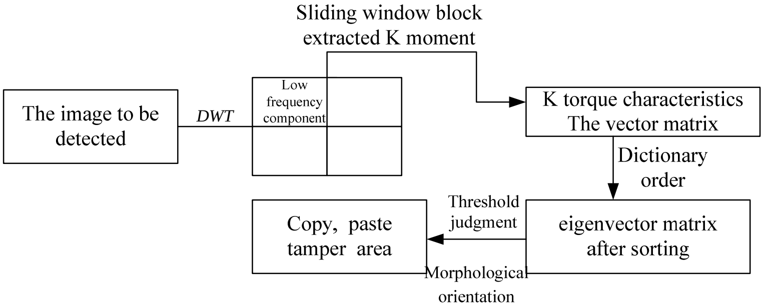


Figure 4. Flow Chart of the Algorithm

5.3. Application of Discrete Wavelet Transform in Reducing the Amount of Image Data

Detection based on block matching algorithm in solving the key problems, mainly have two points: one is to reduce the time complexity; the other is how to extract the feature. In the paper, testing image with discrete wavelet Transform [15] (DWT, Discrete Wavelet Transform) is proposed . Wavelet transform is a kind of time domain, frequency domain or airspace - frequency domain transformation; have at the same time domain and frequency domain localization properties. In the algorithm of wavelet, the feature extraction performed in low frequency part, it can greatly reduce the number of image block, low frequency is not sensitive to noise at the same time, which can enhance robustness of the extracted features.

In the recent years, wavelet analysis has been developed very rapidly, its application areas including image processing, computer recognition, signal processing, and many other fields, discrete wavelet decomposition (DWT) can decompose the two-dimensional image signal into a low frequency approximation subband and level of detail, vertical and diagonal details and three high frequency subband. The Low frequency approximation subband means the maximum scale of the optimal approximation of the original image through wavelet decomposition under the minimum resolution, its statistical characteristics is similar to original image, and most of the energy is focued on the subband image; While the high frequency subband is mainly image detailed information in different resolution and different scales, the lower the resolution is, there will be the higher contains information. Images after wavelet multi-resolution decomposition in the low frequency part will still keep the overview of the source image and space features, the loss of high frequency detail information can be neglected. The image after discrete wavelet decomposition results as shown in figure 3-4. And discrete wavelet transform can be regarded as using low frequency filter and high frequency filter to decompose the image into low frequency and high frequency coefficient, as for two-dimensional signal, discrete wavelet decomposition and reconstruction process can be expressed as shown in Figure 5.

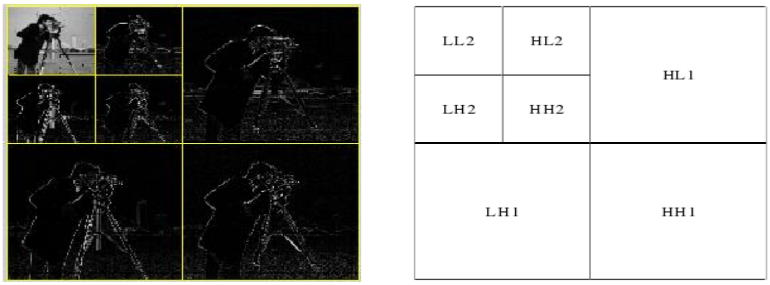


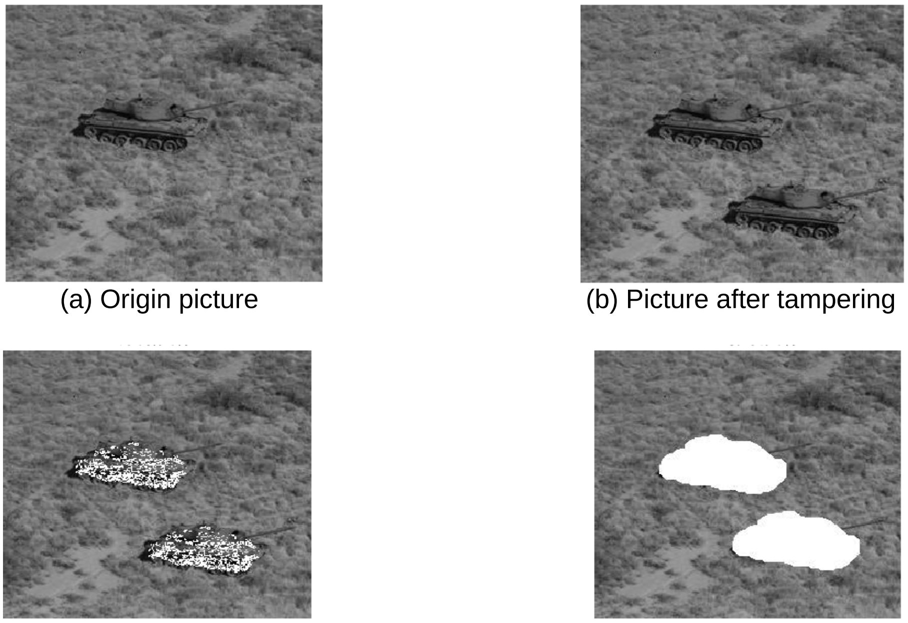
Figure 5. Discrete Wavelet Transform

In the paper, it proposes copy-and-paste tampering with blind forensics algorithm, firstly it through discrete wavelet transform (DWT) as pre-processing for the figure, and extract the discrete wavelet wrap the low-frequency subband as optimal approximation of the image, through the above the scattered wavelet transform analysis, it can be found the that the size of the low frequency component of original image can be reduced to a quarter of j (j is for wavelet decomposition series), through the processing it can achieve the goal of would of reducing the amount of image data. Then, based on the wavelet coefficients, line slide block and the block to can be extracted to the radial Krawtchouk window, and then in turn it can turned into subsequent match action.

6. Results of Experiment and Analysis

In the experiment, in order to validate the effectiveness of the algorithm, in the first step, we select the gray level of 256 in the experiment and the size of images is 512×512 as the experimental images, if the image is RGB type of image, it can be converted to grayscale images. In the selection of image threshold, according to the experimental method, the selection of similarity threshold is set as R = 0.003; the size of the image block is 8×8, the spacing block threshold is L = 12; Image area threshold is S > 512×512×0.85%. In the experiments, we select pictures tank as test images, and test this algorithm respectively in copy - displacement - paste, adding noise, copy-rotation-displacement-paste, mirroring operations and JPEG lossy compression cases, and the accuracy of experimental testing, the error rate and the analysis of misjudgment rate are calculated.

6.1. Copy - displacement - paste Tamper Detection



(a) Origin picture

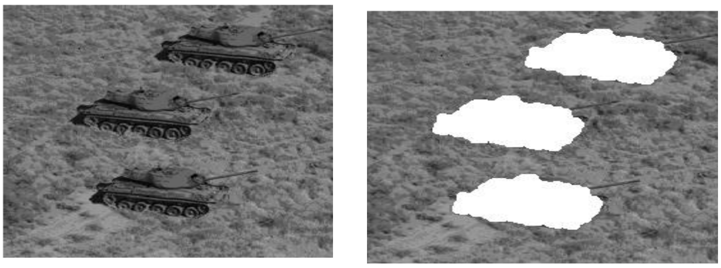
(b) Picture after tampering

(c) Preliminary detection image

(d) Results after morphological processing

Figure 6. Origin Detection Results

As can be seen through the results of experiment, the algorithm about joining tampering with images after Gaussian noise detection effect is good as shown in the Figure 7, with the increase of noise intensity, the area of the test match gradually narrowed.



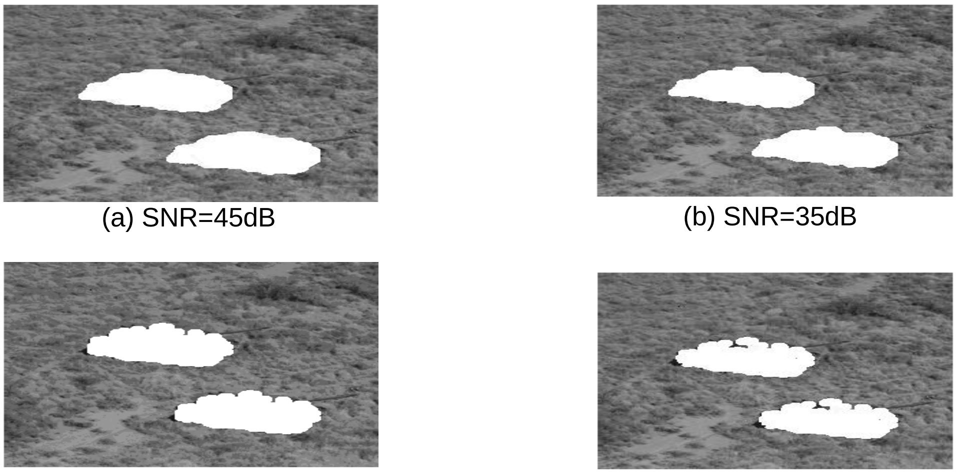
(a) Picture after tampering (b) Detection image

Figure 7. Multi-copy-paste Detection

6.2. Tamper Detection of Adding Noise

In order to test and verify the robustness of algorithm, different post-processing operations are performed according to the tampering image, such as adding different levels of Gaussian , Noise (SNR = 45 dB, 35 dB, 25 dB, 15 dB), the test results as shown as in figure 8 , respectively.

As can be seen through the experiment, the detection effect of algorithm about joining tampering images after adding Gaussian noise is good, but with the increasing of noise intensity, the area of the test match is gradually narrowed.



(a) SNR=45dB (b) SNR=35dB

(c) SNR=25dB (d) SNR=15dB

Figure 8. Detection Results of Adding Gaussian Noise

6.3. Evaluation Index Calculation of the Algorithm

In the paper, copy-and-paste tampering with the algorithm of blind forensics evaluation index has been introduced; in the specific calculation the error rate and misjudgment rate of each picture, on the first step, it randomly select from a rectangle in the copy, and paste it into same image in the region of disjoint, the sizes of copy area are the 32×32, 64×64, 96×96 and 128×128. We tamper with the images with some post-processing operations, such as adding Gaussian noise, JPEG compression, the statistics of its accuracy under specific post-processing operations and misjudgment rate.

1) Processing accuracy and misjudgment rate, error rate

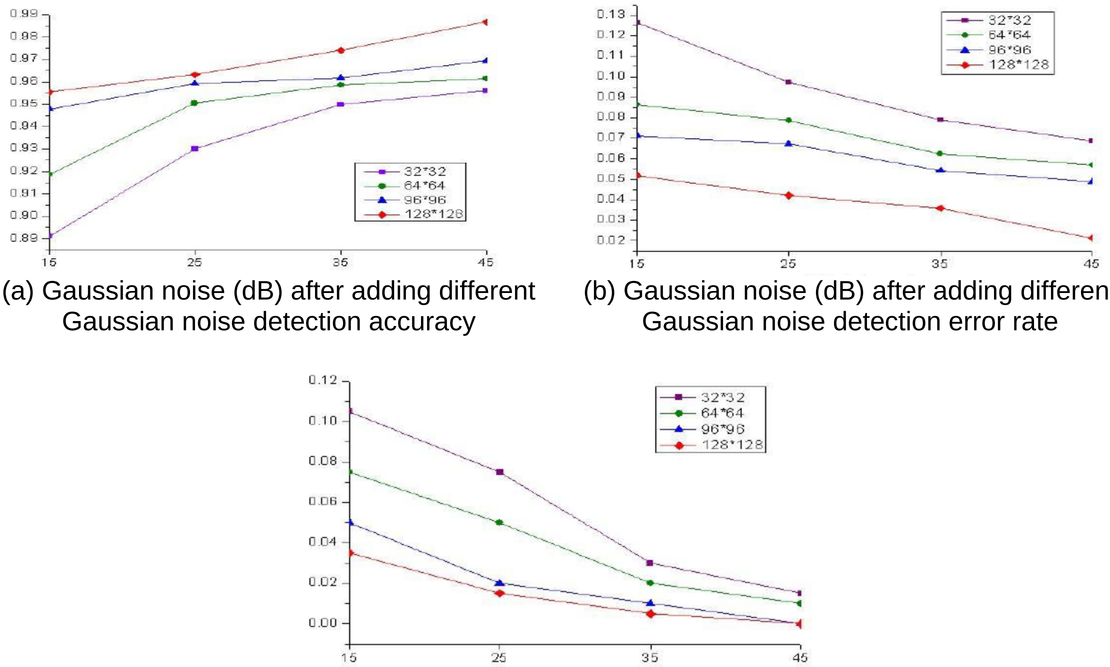
In the replication area under the condition of processing operations, paste the image directly to another area, the detection effect of the tampered image of error rate and false are as shown in Table 1, and through the Figure 9, the intuitive results with the change of the tamper with the area, the change of detection results are shown.

Table 1. Accuracy, Inaccuracy and Misdiagnosis Rate of Copy-paste Tamper

Tampering aera	Accuracy	Error rate	Misjudgment rate
32×32	0.9644	0.0677	0
64×64	0.9723	0.0519	0
96×96	0.9794	0.0405	0
128×128	0.9903	0.0172	0

2) Accuracy and misjudgment rate, error rate after joining different intensity of Gaussian noise

Join in the image with Gaussian noise of 15 dB, 25 dB, db 35, 45 dB, respectively, using the respectively Chapter algorithm in the detecting image tampering with accuracy and error rates. Figure 9, a) is accuracy rate, b) is the error rate, c) is false rate.



(a) Gaussian noise (dB) after adding different Gaussian noise detection accuracy

(b) Gaussian noise (dB) after adding different Gaussian noise detection error rate

(c) Gaussian noise (dB) after adding different Gaussian noise detection misjudgment rate

Figure 9. Accuracy, Inaccuracy and Misdiagnosis Rate of Adding Gaussian Noise with Different Intensities

In the chapter, the results of copy-and-paste tampering algorithm detection effect have been quantitative analyzed. The experiments are mainly aim for copy-displacement-paste, and add Gaussian noise, JPEG compression. Spin Turn, mirror and other tamper with the type test, as can be seen from the experimental detection images. In the paper, it the obvious test results of put forward the algorithm has been achieved. Then, the quantitative analysis is obtained, this chapter mainly calculates error rates and misjudgment rate of detection accuracy in each tampered algorithm, further results show the effectiveness of the algorithm and the algorithm has good performance. According to the experiment, the algorithm for Gaussian noise, JPEG compression and other post-processing to tamper with the image of the operation have very strong robustness, especially for rotating post-processing tampering, it has strong detection accuracy.

6. Conclusion

In the study, it firstly introduces the copy-and-paste tamper with the model, combined with the model, a radial Krawtchouk copy-and-paste tampering with blind forensics algorithm of invariant moments is proposed. Experiments show that the proposed algorithm can effectively locate the tampering of copy-and-paste area, and solve the problem of the similar operating algorithm which is unable for resist rotation, and it also has very strong robustness with the JPEG lossy compression and Gaussian noise and so on.

References

[1] Zhu BB, Swanson MD, Tewfik AH. When seeing isn't believing. *IEEE SignalProcessing Magazine,* 2004; 21(2): 40-49.

[2] Wu Qong. Facing the truth detection blind digital image forensics method research. University of defense technology 2008.

[3] NT Chang SF, Lin CY, et al. Passive-blind Image Forensics. *Multimedia Security Technologies for Digital Rights,* WZeng, Yu H, Lin C Y(eds.), Elsvier. 2006.

[4] Lanh TV, Chong KS, Emmanuel S, et al. *A Survey on Digital Camera Image Forensic Methods.* Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, China. 2007: 16-19.

[5] Zhou Linna, Mr Wang. Digital image forensics technology, Beijing: Beijing university of posts and telecommunications press. 2008.

[6] Yao Zuoliang, Wu Qiong, Li Guohui, Tu Dan. *A recoverable and active digital signature approach for image: RADS.* In Proceedings of IEEE conference. Beijing, China. 2004: 541-546.

[7] Zhong Hua, jiao li cheng. A digital signature scheme for image content verification. *Journal of computers,* 2003: 26(6): 708-708.

[8] Yang Yixian Niu Xin Xin. Digital watermarking theory and technology. Beijing: higher education press. 2006.

[9] Rey C, Dugelay J. A survey of Watermarking Algorithms for Image Authentication. Eurasip *Journal on Applied Signal Processing,* 2002; 6:613-621.

[10] Yeung MM, Mintzerf. *An Invisible Watermarking Technique for Image Verification.* International Conference on Image processing. Santa Barbara, CA, USA. 1997; (2): 680-683.

[11] Fridrich J. *Security of Fragile Authentication Watermarks with Localization.* 4th Conference on Security and Watermarking of Multimedia Contents. San Jose, CA, USA. 2002: 691-700.

[12] Fridrich J. Methords for Detecting Changes in Digital Images. *Multimedia and Security Workshop at ACM Multimedia.* Orlando, Florida, USA. 1999: 29-33.

[13] Lin C, Chang S. Semi-Fragile Watermarking for Authenticating JPEG Visual Content. *Security and Watermarking of Multimedia Contens*. San Jose, CA, USA. 2000: 40-51.

[14] Van Schyndel RG, Tirkel AZ, *Osborne CF. A digital watermark.* Proc. Int.Conference in Image processing. 1994; (2): 86-90.

[15] Cheng En, Zhang Rong-Xin, Yuan Fei. Automatic Detection and Assessment System of Water Turbidity based on Image Processing. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2013; 11(3): 1506-1513.

[16] Xiong Jie. Digital Medical Image Enhanced by wavelet Illumination-Reflection Model. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2013; 11(1): 19-27.

[17] Ye Tian, Change Zheng, Qiuhong Ke. A Bubble Detection Algorithm Based on Sparse and Redundant Image Processing. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2013; 11(6): 2983-2990.