An Efficient Forensic Method for Copy–move Forgery Detection Based on DWT-FWHT

Bin YANG [1], Xingming SUN [2], Xianyi CHEN [1], Jianjun ZHANG [1], Xu LI [1]

[1] School of Information Science and Engineering, Hunan University, Changsha, 410082, China
[2] Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing, 210044, China

yewind2002@163.com, sunnudt@163.com, 0204622@163.com, jianjun998@163.com, lixu_csust@126.com

Abstract. *As the increased availability of sophisticated image processing software and the widespread use of Internet, digital images are easy to acquire and manipulate. The authenticity of the received images is becoming more and more important. Copy-move forgery is one of the most common forgery methods. When creating a Copy-move forgery, it is often necessary to add or remove important features from an image. To carry out such forensic analysis, various technological instruments have been developed in the literatures. However, most of them are time-consuming. In this paper, a more efficient method is proposed. First, the image size is reduced by Discrete Wavelet Transform (DWT). Second, the image is divided into overlapping blocks of equal size and, feature of each block is extracted by fast Walsh-Hadamard Transform (FWHT). Duplicated regions are then detected by lexicographically sorting all features of the image blocks. To make the range matching more efficient, multi-hop jump (MHJ) algorithm is using to jump over some the "unnecessary testing blocks" (UTB). Experimental results demonstrated that the proposed method not only is able to detect the copy-move forgery accurately but also can reduce the processing time greatly compared with other methods.*

Keywords

Image forensics, copy–move forgery, duplicated region detection, Discrete Wavelet Transform (DWT), Fast Walsh-Hadamard Transform (FWHT).

1. Introduction

Image security and authentication are playing a critical role in our society. For instance, before they are used as evidence, the trustworthiness of photographs must be authenticated. However, with the rapid advances and availabilities of powerful image processing software, digital images are becoming more and more undependable.

Figure 1(a), for example, was released by Sepah News, the media arm of Iran's Revolutionary Guard, on July 9, 2008. And it was used on the front pages of The Los Angeles Times, The Financial Times, The Chicago Tribune and several other newspapers as well as on BBC News, MSNBC and many other major news Web sites. One day later, The Associated Press received another image, Figure 1(b), from the same source, which appeared to be taken from the same vantage point at almost the same time. Finally, Figure 1(a) was proved to be forged [1]. Digital images are being more and more undependable as a definitive record of an event. It's necessary to develop a set of tools to authenticate digital images.

(a) **(b)**

Fig. 1. An example of copy-move forgery: (a) the forged image with four missiles and (b) the original image with three missiles.

Digital watermarking [2-6] has been proposed as a means not only for authentication, but also for tamper detection. However, this approach has a drawback that a watermark must be inserted into an image first, which would limit this approach to controlled environments, such as surveillance cameras [7]. On the contrary, passive detection techniques [8-13] are developed without the presence of digital watermarks. As such, passive detection techniques are, in theory, applicable to a broader range of operating scenarios [14]. Copy-move forgery, as depicted in Fig. 1, is one of the most common forgery methods. It is usually used to erase or add some special object in the image. The components (e.g., color and light) of the regions copied from the same image will be compatible with the whole image and hard to be detected by Human Visual System (HVS).

In recent ten years, copy-move forgery detection has become a hot topic in the field of image forensic. Many techniques have been proposed to address the problem. The first one has been proposed by Fridrich et al. [15]. They

divided an image into overlapping blocks of equal size firstly. Subsequently, coefficient of each block was extracted by discrete cosine transform (DCT). Finally, the duplicated regions were detected by matching the quantized coefficients which had been lexicographically sorted. Similar to [15], Popescu and Farid [16] proposed a copy-move forgery detection method, the main difference lies in the representation of overlapping image blocks. The authors extracted the coefficient by principal component analysis (PCA) instead of DCT. Since the dimensions of the coefficients extracted by PCA are smaller, Popescu's technique is demonstrated to be more effective. The weakness of [16] is that it cannot detect the rotating copy regions, which limits its scope of application [17]. To improve the robustness of detection, Mahdian et al. [18] developed a method based on blur moment invariants. They can detect the duplicated regions in an image even with the presence of blur, noise or contrast changes in the copied areas. Bayram et al. [17] applied Fourier Mellin Transform (FMT) and 1-D projection of log-polar values in their robust scheme of detecting image forgeries. As an improvement of the DCT-based forgery detection technique, Huang et al. [20] selected parts of the overlapping image blocks by using a threshold p, which can reduce the matching time about (1-p) percent. However, too small threshold p will seriously reduce the matching accuracy. In recent years, Discrete Wavelet Transform (DWT) is used in many forensic approaches to decrease the dimension of image. Khan et al. [11], [19] applied DWT to decrease complexity of copy-move forgery detection. They used Phase Correlation as the similarity criterion to identify the duplicated blocks. Ghorbani et al. [12] orderly combined DWT and DCT to detect the clone area. Although the approach was able to deal with varies clone forgery, it still be time-consuming. Muhammad et al. [13] used Dyadic Wavelet Transform to decrease the dimension of image. Since they directly matched the transformed pixels. Method [13] is confirmed to be only suitable for the image with simple background, and almost ineffective in real forensic. Recently, a new signal processing technique based on 3D models and Google Map was proposed to detect copy-move forgery [21]. However, the drawback of [21] is that it relies on Google Map and only can detect the images of buildings. These detection methods seem to be effective for copy-move forgery, but they are time-consuming and costly. This paper mainly focuses on the operation efficiency of the detection method. In comparison with other methods, the proposed one will be more efficient due to the uses of fast Walsh-Hadamard Transform (FWHT) [22], [23] and DWT [24]. The robustness of JPEG compression with different quality factors, Gaussian blurring and additive white noise in a certain degree is demonstrated by a series of experiments.

The rest of the paper is organized as follows: The proposed forgery detection method is described in Section 2. The experiment results are shown in Section 3. The conclusion is drawn in Section 4.

2. Proposed Method

The essential of a copy-move image forgery detection algorithm is to determine whether a given image contains duplicated regions. Due to the unknown shape and size of the duplicated regions, it is definitely impossible to compare every pairs of region with different shape and size. Matching the overlapping blocks, which was divided into fixed-size in the image, would be time-saving. In order to reduce the processing time and enhance the robustness of blocks matching, some feature extraction transforms such as DCT, PCA should be performed. Even so, the processing time is quite unbearable while handling the high resolution image. Therefore, the purpose of this study was to propose a more efficient approach. At the beginning of the method, the image C is transferred into a grayscale image I, by the formula (1), R, G, B are red channel, green channel, and blue channel of image C, respectively [9].

$$I = 0.2989 \times R + 0.5870 \times G + 0.1140 \times B. \quad (1)$$

To reduce the dimension of the image, Discrete Wavelet Transform (DWT) is performed. Subsequently, the image is divided into overlapping blocks of equal size and, feature of each block is extracted by Fast Walsh-Hadamard Transform (FWHT). Duplicated regions are then detected by lexicographically sorting all features of the image blocks. To make the range matching more efficiently, we skip some "unnecessary testing blocks" by applying the multi-hop jump (MHJ) algorithm. A simple schematization of the whole system is presented in Fig. 2.

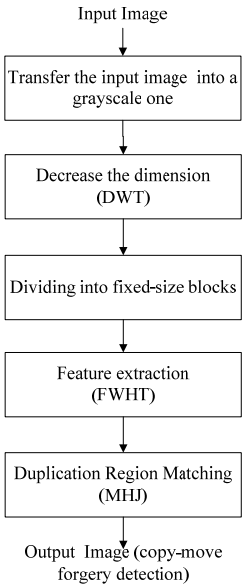

Fig. 2. Overview of the proposed system.

2.1 Discrete Wavelet Transformation (DWT)

Discrete Wavelet Transformation (DWT), a multi-level decomposition technique, is localized in space and in frequency. The localization feature both in space and fre

quency, in turn, leads to a number of useful applications such as data compression, detecting features in images, and removing noise and so on [24]. In the proposed approach, Haar wavelet is performed to reduce the dimension of the image, and then four sub-bands are output. As is well known, low frequency sub-band concentrates most of the image energy, whose size is only $1/4^j$ of the original image, where j is a positive integer. Consequently, the size of a forged $M\times N$ image is reduced to $M\times N/4^j$.

2.2 Dividing into Fixed-size Blocks

It is impossible to compare every pairs of region with different shape and size, while detecting duplicated regions in an image. Like most of overlapping blocks methods [15-18], [20], we divided the image into $a\times a$ pixels fixed-sized overlapping blocks (here we assume that the size of the blocks is smaller than the duplicated region to be detected). Blocks are slid by one pixel along the image from the upper left corner right down to the lower right corner. For a $M\times N$ pixels image, the sliding will generate $(M-a+1)\times(N-a+1)$ such blocks. As the size of the forged image is reduced to $M\times N/4^j$, the approach will generate k blocks where $k=(M/2^j-a+1)\times(N/2^j-a+1)\approx M\times N/4^j$.

2.3 Fast Walsh-Hadamard Transformation (FWHT)

The Walsh–Hadamard transform (WHT) is a non-sinusoidal, orthogonal transformation technique that decomposes a signal into a set of basis functions. These basis functions are Walsh functions, which are rectangular or square waves with values of +1 or –1. Tab. 1 is the first eight Walsh functions example.

Index	Walsh Function Value
0	1 1 1 1 1 1 1 1
1	1 1 1 1 -1 -1 -1 -1
2	1 1 -1 -1 -1 -1 1 1
3	1 1 -1 -1 1 1 -1 -1
4	1 -1 -1 1 1 -1 -1 1
5	1 -1 -1 1 -1 1 1 -1
6	1 -1 1 -1 -1 1 -1 1
7	1 -1 1 -1 1 -1 1 -1

Tab. 1. The first eight Walsh functions.

WHT returns sequency values which is a more generalized notion of frequency and is defined as one half of the average number of zero-crossings per unit time interval. Each Walsh function has a unique sequency value. The returned sequency values could be used to estimate the signal frequencies in the original signal. WHT is quite useful for reducing bandwidth storage requirements and spread-spectrum analysis in many applications such as image processing, filtering, and power spectrum analysis.

The WHT has a fast version, the fast Walsh–Hadamard transform (FWHT). The FWHT for an $n\times n$ matrix $\boldsymbol{X}$ is defined as:

$$Y=\frac{1}{n}WAL_n\times X\times WAL_n \tag{2}$$

where WAL_n represents an $n\times n$ Walsh functions matrix. For example, the matrix of first eight Walsh functions which presented in Tab. 1 is:

$$WAL_8=\begin{bmatrix}1&1&1&1&1&1&1&1\\1&1&1&1&-1&-1&-1&-1\\1&1&-1&-1&-1&-1&1&1\\1&1&-1&-1&1&1&-1&-1\\1&-1&-1&1&1&-1&-1&1\\1&-1&1&-1&-1&1&1&-1\\1&-1&1&-1&-1&1&-1&1\\1&-1&1&-1&1&-1&1&-1\end{bmatrix}.$$

More detail of FWHT could be found in literatures [22] and [23].

Many copy-move forgery detection techniques such as [15] and [20] extracted the feature of an image by applying discrete cosine transform (DCT). However, due to FWHT only use addition and subtraction, which is simpler than the DCT. The FWHT runs more efficiently than the DCT. In our approach, we extract the feature of each block by FWHT instead of DCT. Each $a\times a$ block is transformed by FWHT and reshaped into a row vector $\vec{a}$. A $k\times a^2$ matrix, H, is then formed, where k is the number of blocks. Each row corresponds to one position of the sliding block. To make the algorithm more robust [15], [20], each FWHT coefficient will be quantized by a quantization factor q and then rounded to the nearest integer.

2.4 Duplicated Regions Matching

In the matching step, each pair of sub-block is tested whether they are similar. A simple way is an exhaustive search to every possible pairs of blocks. Such an approach is obviously time consuming and the computational cost is $O(N^2)$. In order to make the matching more efficient, we skip some "unnecessary testing blocks". Thus, the computational cost is reduced to $O(\log_2 N)$. Figure 3 is an example of copy-move forgery, a region $R(x, y)$ (the top-left corner's coordinate of the corresponding block is noted as x, y) is copied and pasted as the region $R'(x', y')$ in the same image, where $x'=x+\Delta x$ and $y'=y+\Delta y$. The distance between the original and pasted regions is $d=(\Delta x,\Delta y)$.

As can be seen, all the reciprocal spatial distances between original blocks (B_i) in region R and the corresponding pasted blocks (B_i') are the same. Therefore, these pairs of original and the pasted blocks $(B_n,B_n'),(B_{n+1},B_{n+1}'),...,(B_m,B_m')$ can be confirmed as duplication forgery without further testing; we named such blocks

as "unnecessary testing blocks" (UTB). The advantage of our approach is that we skip as much as possible UTB in the copy-move regions by performing multi-hop jump (MHJ) algorithm. Figure 4 is an example of matching two regions *R1, R2* by MHJ. The block number of the first row is the position of the top-left corner point of each block. Blocks are lexicographically sorted by their features which were extracted by FWHT.

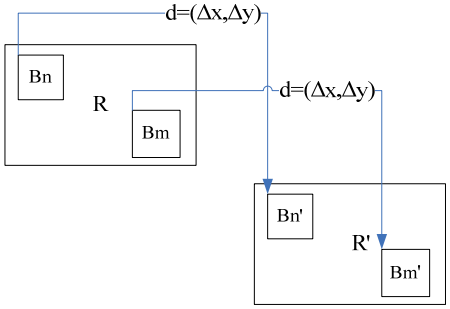

Fig. 3. Region R is copied and pasted as R'. Each block (B_i) in region R has the same distance to the corresponding one (B_i') in the pasted region R'.

Subsequently, they are arranged in a row for the convenience of matching. The second row in the figure is the distance of the block number correspondence to each pair blocks; we abbreviate such distance as *BNd*. As shown in figure, many pair blocks have the same *BNd* which are unnecessary to be tested. The MHJ algorithm iteratively repeats the following steps on the matrix H which contains the vectors of FWHT coefficients:

Step 1. Initialing the match pointer *p(BNd)* to the first line of matrix H with the current *BNd*. We empirically determined appropriate jump distance n to $\lfloor k/16 \rfloor$, where k is the number of rows of matrix. Finally, an array $u(i)$ that records the number of *BNd* is generated, and initialized to 0.

Step 2. The pointer jump n pair blocks forward, if the pointer reach the last row of the matrix H, the algorithm is over.

Step 3. Comparing the new *BNd'* and the original *BNd*. If *BNd* = *BNd'*, then $u(BNd) = u(BNd) + n$, and the algorithm proceed to the *Step 2*. Otherwise, the algorithm proceeds to the *Step 4*.

Step 4. The pointer $p(BNd)$ jump $\lfloor n/2 \rfloor$ pair blocks backward, and set n to $\lfloor n/2 \rfloor$. If the jump distance n is equal to 0, the jump distance n is set to $\lfloor k/16 \rfloor$ again. Finally, the algorithm proceeds to the *Step 2*.

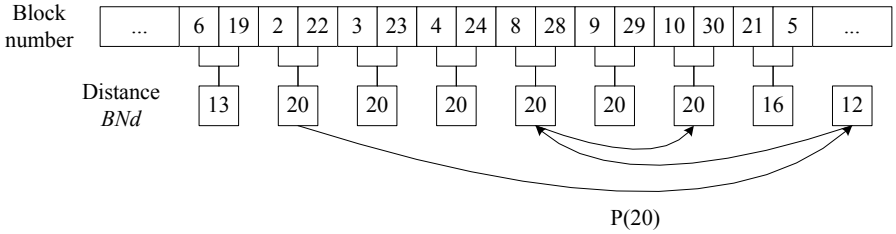

Fig. 4. An example of matching two regions R_1, R_2 by MHJ.

As many copy-move forgery would rotate and/or blur the image part before pasting it over to reduce the visual artifacts. The *BNd* of every pair blocks will not be exactly equal. In our approach, a threshold t is defined, the blocks whose *BNd* difference does not exceed the threshold t are considered to be replication. Since a duplicated region will consist of many smaller blocks, each of these blocks will have the same offset [16]. To reduce the impact of some isolate blocks which are naturally similar, we defined a threshold. Only when the number of similar blocks is greater than the threshold p, those blocks can be determined to have a copy relationship. Furthermore, to make our approach more robust in some environment such as sky and lake, we ignore the blocks whose distances are minor than a threshold D.

The detail of matching algorithm goes as follows:

Step 1. The rows of the matrix H are lexicographically sorted. The sorted list of the feature vectors of blocks $B_1, B_2, \ldots, B_m$, are denoted as $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_m$, respectively. Each block B_i has a block number N_i which is marked by its top-left corner point in the block.

Step 2. The *BNd* of the i-th pair blocks is calculated as shown in (3).

$$BNd_i = \left| N_i - N_{i-1} \right|. \tag{3}$$

Step 3. Perform the MHJ algorithm. For any $BNd_i > D$, calculate the number of blocks pair $u(i)$ whose *BNd* difference does not exceed the threshold t.

Step 4. For any $u(i) > p$, marks the corresponding blocks in special color in the image.

3. Experimental Results

In this section, we evaluate the quantitative performance of the proposed copy-move detection method on a set of forgery images with duplicated regions.

3.1 Settings for Forgery Detection

We evaluated our approach and tested on the Tampered Image Detection Evaluation Database (TIDED)V2.0 generated by the Institute of Automation at Chinese Academy of Sciences (CASIA)[25]. It consists of 7492 authentic and 5124 tampered color images with JPEG, BMP, or TIFF format. The images in this database are of different sizes, varying from 240×160 to 900×600 pixels. Furthermore, the detection performance has been compared to the result obtained with our implementation of other approaches [11], [12], [15], [16] and [20].

The experiments were carried out on the Matlab R2007a and manipulated by Photoshop CS2 in a computer of CPU 2.4 GHz with memory 2 GB. The output of the method was a duplication map, in which likely duplicated regions were shown. Parameters of the method were set to $a = 8$ (block size), $p = 30$ (threshold for the number of similar blocks), $t = 24$ (threshold for blocks distance difference), $D = 40$ (threshold for blocks image distance). In the DWT step, the experiment image was performed DWT with the positive integer $j = 1$ (i.e. only one level DWT was performed, and sub-band $3 \times 1 + 1 = 4$ is created). After the DWT processing, the image size was only 1/4 of the original image.

Detection performance was measured in terms of correct alarm rate (CAR) and false alarm rate (FAR), where CAR is the fraction of tampered images correctly identified as such, while FAR is the fraction of identifying an original image as a tampered one [18]. They can be represented as:

$$\text{CAR} = \frac{\text{the number of the images detected as forged being forged}}{\text{the number of the forged images}}, \quad (4)$$

$$\text{FAR} = \frac{\text{the number of the images detected as forged being original}}{\text{the number of the original images}}. \quad (5)$$

3.2 Visual Test on Duplicated Regions

In all cases, the copy-move tampering was realized in the image to conceal or clone an object. Several different images, which were considered to be challenging for copy-move forgery detection with different size of copied area, were used in our experiment.

The first example is presented in Fig. 5. Figure 5(c) is the duplication map of the proposed method applied to the tempered image shown in Fig. 5(b). In this example, no further manipulations are conducted with the duplicated regions. The tampered image is saved in TIFF format without compression. The output shows that the proposed method could detect the duplicated regions correctly.

Figure 6 is an example of replication green plants to conceal a building. Figure 6(c) shows the duplication map generated by applying the proposed method to Fig. 6(b).

(a) (b) (c)

Fig. 5. Shown are the original version of the test image (a), its forged version (b) and the constructed duplication map (c).

(a) (b) (c)

Fig. 6. Shown are the original version of the test image (a), its forged version (b) and the constructed duplication map (c).

(a) (b) (c)

Fig. 7. Shown are the original version of the test image (a), its forged version (b) and the constructed duplication map (c).

The tampered image in this case is saved in JPEG format with quality factor 80. The output shows that the proposed method is affected by the compression in the image. A few duplicated blocks have not been detected in a medium quality JEPG format image. However, since most of duplicated blocks are detected, it's easy to determine the duplicated regions.

Figure 7(c) shows the duplication map created by applying the proposed method to Fig. 7(b). In this example, the black pillar is erased by the floor tiles. To test the robustness of the proposed method, 1.5% Gaussian noise is added in the image additionally. The tampered image in this case is saved in JPEG format with quality factor 90. The result indicates that the proposed method performs well also in the case of processing an additive Gaussian noise distorted image.

3.3 Comparison with Other Methods

Table 2 shows the detection performance and the processing time on average (in seconds) for the experiment images. For comparison, Khan et al.'s [11], Ghorbani et al.'s [12], Fridrich et al.'s [15], Popescu's [16] and Huang et al.'s [20] detection methods were implemented and applied to the same forgery image set. The input parameters required by the three methods were set as follows:

$b = 8$ (block size), $N_n = 5$ (number of neighborhood rows to search in the lexicographically sorted matrix), $N_f = 30$ (threshold for the minimum frequency), and $N_d = 22$ (threshold to determine a duplicated block). In [11], another threshold needed: $t = 0.8$ (threshold of phase correlation). In [15], two more parameters were needed: $e = 0.01$ (fraction of the ignored variance along the principle axes after PCA is computed) and $Q = 256$ (number of the quantization bins). In [20], another factor was needed: $p = 0.25$ (the first p percent DCT coefficients are saved for matching.). To make the comparison fair and rational, those parameters of similar function were set to the same value in these methods. Moreover, only one level Haar DWT is performed to the DWT based methods.

Method	CAR (%)	FAR (%)	Times (s)
Khan et al.'s [11]	82.55	11.88	61.86
Ghorbani et al.'s [12]	84.33	10.50	56.32
Fridrich et al. [15]	93.70	4.70	202.38
Popescu and Farid [16]	89.03	4.31	45.63
Huang et al.[20]	93.27	4.16	135.12
The proposed method	93.89	4.16	27.22

Tab. 2. CAR, FAR values (%) and processing time (average time, per image) for each method.

The results indicate that the proposed method works more efficiently compared with other methods. This could be attributed to the usage of DWT-FWHT and the MHJ algorithm. In addition, the CAR of the proposed method exhibits the best performance due to the use of threshold p. The FWHT coefficients of some isolate blocks may be much similar by coincidence. We ignore such isolate blocks in our method, while the compared methods do not. In DWT step, the experiment image size is reduced to a quarter of the original. Since the FWHT only uses addition and subtraction which is simpler than the DCT does, the proposed method has a better performance in feature extraction process by using FWHT. Furthermore, by applying the MHJ algorithm, the match pointer could jump over some "unnecessary testing blocks" which greatly reduces the processing time in matching step. The computational cost is reduced from $O(N^2)$ to $(\log_2 N)$. As demonstrated in Tab. 2, the processing time of the methods that used DWT is significantly less than that of the methods without DWT. The performances of method [11] and [12] are relatively poor, since they have not considered the isolate blocks. Method [16] also obtained a remarkable score in processing time by using PCA. However, it can not detect the copy regions which were slightly rotated. Hence the CAR of [16] is modestly lower than that of the [15]. Method [20] gets a relative high accuracy, but the processing time is still high. And its processing time is reduced with the decreasing of the factor p; nevertheless the detection accuracy would be reduced.

It is notice that, all the experiment methods are hard to detect the images with the extremely similar scene, such as pure sky, floor, etc. Methods [15], [16] and [20] obtain an acceptable FAR (about 4%) by ignoring the isolate block. On the contrary, the FAR of [11] and [12] is greater than 10% due to the interference of naturally similar blocks.

4. Conclusion

Copy-move forgery is a common type of forgery where some regions of an image are replaced with other regions from the same image. The doctored regions always are subjected to various image transformations in order to conceal the tampering. Conventional techniques of detecting copy–move forgery usually suffer from the problem of time-consuming.

We have proposed an automatic and efficient forensic method for copy-move forgery detection based on DWT-FWHT. It can work in case of complete absence of digital watermarks or signatures. To make the method more efficient compared with previous works, the proposed method uses DWT to reduce the image size, and extracts the feature in the overlapping blocks by FWHT instead of the DCT. To speed up the method, MHJ algorithm is used in the matching process.

The experimental results show that the proposed method can accurately and quickly detect the duplicated regions. And the processing time is reduced significantly as against other classic methods, while the accuracy still remains at a high level. The method works well in spite of the presence of blur, noise and JPEG compression in a certain degree. However, the proposed method is weak in

detecting images which have undergone the attack of transforming. In future, we would like to deal with problem such as rotation and scales.

Acknowledgement

This work is supported by the NSFC (61232016, 61173141, 61173142, 61173136, 61103215, 61373132, and 61373133), National Basic Research Program 973 (2011CB311808), 2011GK2009, GYHY201206033, 201301030, 2013DFG12860, SBC201310569 and PAPD fund.

References

[1] In an Iranian image, a missile too many. [Online] Cited 2012-08-23. Available at: http://thelede.blogs.nytimes.com/2008/07/10/in-an-iranian-image-a-missile-too-many/

[2] COX, I., MILLER, M. L., BLOOM, J. A., KAUFMAN, M. Digital watermarking. *Journal of Electronic Imaging*, 2002, vol. 11, no. 3, p. 50-55.

[3] COLTUC, D. Improved capacity reversible watermarking. In *2007 ICIP IEEE International Conference on Image Processing.* 2007, p. 249-252.

[4] YANG, Y., SUN, X., YANG, H. A contrast-sensitive reversible visible image watermarking technique. *IEEE Transactions on Circuits and Systems for Video Technology,* 2009, vol. 19, no. 5, p. 656-667.

[5] LUO, H., SUN, X., YANG, H., XIA, Z. A robust image watermarking based on image restoration using SIFT. *Radioengineering*, 2011, vol. 20, no. 2, p. 525-532.

[6] TAN, L., SUN, X., SUN, G. Print-scan resilient text image watermarking based on stroke direction modulation for Chinese document authentication. *Radioengineering*, 2012, vol. 21, no.1, p. 170-181.

[7] FARID, H. Image forgery detection. *Signal Processing Magazine, IEEE*, 2009, vol. 26, no. 2, p. 16-25.

[8] SHIVAKUMAR, B. L., BABOO, S. S. Automated forensic method for copy-move forgery detection based on Harris interest points and SIFT descriptors. *International Journal of Computer Applications*, 2011, vol. 27, no. 3, p. 9-17.

[9] PENG, F., NIE, Y., LONG, M. A complete passive blind image copy-move forensics scheme based on compound statistics features. *Forensic Science International*, 2011, vol. 212, no. 1, p. 21-25.

[10] HWEI-JEN LIN, CHUN-WEI WANG, YANG-TA KAO Fast copy-move forgery detection. *WSEAS Trans Sig Proc.*, 2009, p. 188-197.

[11] KHAN, S., KULKARNI, A. An efficient method for detection of copy-move forgery using Discrete Wavelet Transform. *International Journal on Computer Science and Engineering*, 2010, vol. 2, no. 5, p. 1801-1806.

[12] GHORBANI, M., FIROUZMAND, M., FARAAHI, A. DWT-DCT (QCD) based copy-move image forgery detection. In *18th International Conference on Systems, Signals and Image Processing (IWSSIP 2011)*. Sarajevo, 2011, p. 1-4.

[13] MUHAMMAD, N., HUSSAIN, M., MUHAMMAD, G., BEBIS, G. Copy-move forgery detection using Dyadic Wavelet Transform. In *Eighth International Conference on Computer Graphics, Imaging and Visualization (CGIV 2011)*. 2011, p. 103-108.

[14] XIAOYING, F., COX, I. J., DOERR, G. Normalized energy density-based forensic detection of resampled images. *IEEE Transactions on Multimedia,* 2012, vol. 14, no. 3, p. 536-545.

[15] FRIDRICH, J., SOUKAL, D., LUKÁŠ, J. Detection of copy-move forgery in digital images. In *Proc. Digital Forensic Res. Workshop.* Cleveland (USA), Aug. 2003.

[16] POPESCU, A. C., FARID, H. Exposing digital forgeries by detecting traces of resampling. *IEEE Transactions on Signal Processing,* 2005, vol. 53, no. 10, p. 758-767.

[17] BAYRAM, S., SENCAR, H. T., MEMON, N. An efficient and robust method for detecting copy-move forgery. In *IEEE International Conference on Acoustics, Speech and Signal Processing ICASSP 2009*. 2009, p. 1053-1056.

[18] MAHDIAN, B., SAIC, S. Detection of copy-move forgery using a method based on blur moment invariants. *Forensic Science International*, 2007, vol. 171, no. 2, p. 180-189.

[19] KHAN, S., KULKARNI, A. Reduced time complexity for detection of copy-move forgery using Discrete Wavelet Transform. *International Journal of Computer Applications,* 2010, vol. 6, no. 7, p. 1087-1418.

[20] HUANG, Y., LU, W., SUN, W., LONG, D. Improved DCT-based detection of copy-move forgery in images. *Forensic Science International*, 2011, vol. 206, no. 1-3, p. 178-184.

[21] KIMA, H. J., LIMA, S., MOONA, J., KIMB, B., JUNG, E .S. A photographic forensic case study: Myths, principles and techniques. *Mathematical and Computer Modelling*, 2012, vol. 55, no. 1-2, p. 3-11.

[22] BEAUCHAMP, K. G. *Applications of Walsh and Related Functions - With an Introduction to Sequency Theory*. Academic Press, 1984.

[23] BEER, T. Walsh Transforms. *American Journal of Physics*, 1981, vol. 49, no. 5, p. 466-472.

[24] AMARA, G. An Introduction to Wavelets. *IEEE Computational Science and Engineering*, 1992, vol. 2, no. 2, p. 50-61.

[25] CASIA, Image Tampering Detection Evaluation Database. http://forensics.idealtest.org, 2010

About Authors ...

Bin YANG (corresponding author) was born in Guangdong, China, 1979. He received his MS. from the South China University of Technology in 2007, and he is currently pursuing his PhD in Computer Science and Technology at the School of Computer and Communication of Hunan University, China. His research interests include information security, digital image forensic, digital watermarking and image processing.

Xingming SUN received his BS in Mathematics from Hunan Normal University, China, in 1984, MS in Computing Science from Dalian University of Science and Technology, China, in 1988, and PhD in Computing Science from Fudan University, China, in 2001. He is currently a professor in Nanjing University of Information Science and Technology, China. His research interests

include network and information security, digital watermarking, digital forensic and natural language processing.

Xianyi CHEN was born in Hubei, China, 1986. He received his M.S. degree in college of mathematics and econometrics, Hunan University in 2008, and is currently pursuing his Ph.D. degree in the School of Information Science and Engineering from Hunan University, China. His research interests include multimedia security, digital watermarking, data hiding and image processing.

Jianjun ZHANG received his MS. from Yunnan Normal University in 2000, and he is currently pursuing his PhD in Computer Science and Technology at the School of Computer and Communication, Hunan University, China. His research interests include information security, digital image forensic, digital watermarking and image processing.

Xu LI is currently pursuing his PhD in Computer Science and Technology at the College of Information Science and Engineering, Hunan University, China. His research interests include probability theory and image processing.