World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:6, No:11, 2012

Efficient Copy-Move Forgery Detection for Digital Images

Somayeh Sadeghi, Hamid A. Jalab, and Sajjad Dadkhah

Open Science Index, Computer and Information Engineering Vol:6, No:11, 2012 publications.waset.org/10220.pdf

***Abstract*—Due to availability of powerful image processing software and improvement of human computer knowledge, it becomes easy to tamper images. Manipulation of digital images in different fields like court of law and medical imaging create a serious problem nowadays. Copy-move forgery is one of the most common types of forgery which copies some part of the image and pastes it to another part of the same image to cover an important scene. In this paper, a copy-move forgery detection method proposed based on Fourier transform to detect forgeries. Firstly, image is divided to same size blocks and Fourier transform is performed on each block. Similarity in the Fourier transform between different blocks provides an indication of the copy-move operation. The experimental results prove that the proposed method works on reasonable time and works well for gray scale and colour images. Computational complexity reduced by using Fourier transform in this method.

***Keywords*—Copy-Move forgery, Digital Forensics, Image Forgery.

I. Introduction

IMAGE as a communication media became very popular immediately after invention of photography and plays critical role in real life, but from time to time image does not tell the truth. With the entrance of digital data in current years and improvement of human computer knowledge, expansion of digital images increased and validity of digital data faces a big problem [1]. Availability of the digital image processing tools such as Photoshop or GIMP which are available free makes it easy to change features of images which are flexible to manipulation; these powerful tools caused suspicions on the integrity of digital images that we face every day in our life [2]. Consequently, digital image forgery invented to find out the integrity of the image, and it became an important issue as people tried to change the content of the image and present the forged image as original one to achieve their illegal purposes.

Digital image forgery is important because of the usage of digital images in many social areas like courts when they are used as evidence, or in medical field to help physician makes decisions base on digital images. Digital Image Forensics can be subdivided into three branches as image source identification; Computer generated image recognition and Image forgery detection, and base on latest technology, digital image forgery categorized in three groups; Copy-Move, Image splicing and Image retouching. Copy-Move forgery or Region-Duplication forgery is the most important type of forgery, in Copy-Move some part of the image copies and pastes into another part of the same image to create a new thing or to hide an important scene [2]. Image splicing is the procedure of creating a fake image by cutting one part of an image and paste it to another image. It works on combining few images to create one tampered image. One of the problems is that, when the backgrounds in the images are different the objects in result may appear unclear [3]. Image Retouching doesnt obviously change the image, so it can be considered as the less corrupting type of digital image forgery, it just enhance some features of image. It is famous among magazine photo editors and most of magazine covers use this technique to change some features of an image but it is ethically wrong [3].

With the creation of digital image forgery, many researchers developed different techniques to detect forgery, detection of Copy-Move forgery is difficult compare to other forgeries because the source and destination of forgery is same image, also the original image segment and the pasted one have same important properties such as dynamic range, noise component and colour palette. An example for this type of forgery can be seen in Fig.1, where (a) shows the original image and (b) shows the tampered image [4].

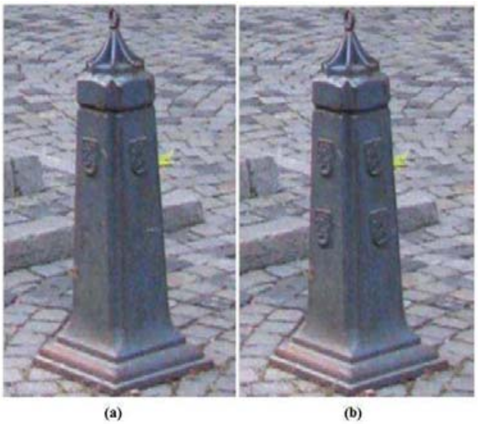

Fig. 1: Sample of Image Forgery

In this paper, we propose a novel method for identifying the location of copy-move tampering and authenticating an image by applying Fourier transform. The image is first converted to gray scale image and reduced in size based on the resize criterion value. Fourier transform applied on image to perform correlation, and correlation can be used to locate features within an image, and finally it helps to find similar correlations

S. Sadeghi is with the Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia. (email: ssomayeh@siswa.um.edu.my)

H.A Jalab is with the Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia. (email: hamidjalabb@um.edu.my)

S.Dadkhah is with the Faculty of Computer Science and Information System, University Technology Malaysia 54100 Kuala Lumpur, Malaysia (email: dsajjad2@live.utm.my)

values in image and convert the result value to a matrix of real numbers and shows location of matched blocks.

The rest of paper is organized as follows. In next section, the related work is reviewed. In section 3, the details of the proposed method are presented with the general flowchart of the program. Section 4 presents the experimental results and discussion. Final conclusions are drawn in last section.

II. Related Work

Copy-move forgery is a very general and important type of forgeries because the source and destination of the forged image is same. In this type of forgery, some part of the image copies and pasts on other part of the same image to cover and important scene for illegal purposes [5]. Consequently detection of copy-move forgery invented to search the copied regions and their pasted ones, but detection may vary base on whether there has been any post-processing on copied part before paste it to another part. Usually attackers will do some operations such as rotation, filtering, JPEG compression, resizing and noise addition to the original part before pasting, and these operations make it difficult to detect copy-move forgery, therefore forgery detector should be robust to all manipulations [2].

To accomplish this task several copy-move forgery detection techniques have been proposed. Fridrich, Soukal, and Jan Luk in [5] described Copy-Move forgery base on similarity. They believed there is a relationship between the original image parts and pasted one, and this relationship can be used for a successful detection of copy-move. Since the tampered image will possibly be saved in the JPEG format, the image parts might match approximately not accurately. As a result, they found there are some requirements for detection algorithm, which are: 1. Algorithm must permit for an approximate match of small image parts. 2. When there is possibility of false positive, it should work in a reasonable time. 3. Another thing is that the forged parts should be a connected component rather than a collection of individual pixels.

Accordingly, they have developed a technique for detection based on exact match, and it works to find segments in the image which match exactly. This technique is useful for forensic analysis, but its applicability is limited [5]. In 2003, Fridrich analyzed the exhaustive search and proposed a block matching detecting method based on discrete cosine transform (DCT) and lexicographic sort used for detecting the forged areas [5]. Mahdian and Stanislav in [6] proposed a method based on blur moment invariant which is robust to all manipulations but the main disadvantage of this method was detection time which takes 45 minutes for a 256x256 pixel image to detect which area has been duplicated.

An efficient non-intrusive method is proposed in [7], in this method image is divided into sub blocks and a separate noise image is created by using noise pattern of each sub blocks, these noise images are used to approximate the overall noise of the image which is useful later to guess the noise pattern of different blocks. Finally blocks with similar noise histogram are suspected to duplicated area. This method can segment an image into complete objects more accurately compare to previous methods but it cant work on different images as detection can happen only if the background of the image is simple. Detection based on DCT was proposed by Jie, Huaxiong, Gao and Hai (2011), in this method Fridrichs method based on DCT has improved by reducing false matching rate. This method works by comparing image block features and find out if number of matched blocks in certain region is more than threshold. In order to improve the accuracy of matching a lexicographical sorting algorithm based on distance proposed. It is robust to post image processing like adding noise and blurring, but it is not robust to rotation [8]. Reference [7] shows a new solution proposed based on dyadic wavelet transform usage. It is robust to post processing but this method also has its drawbacks, it works only on images with simple background.

According to XiaoBing KANG and ShengMin WEI [9] , in proposes detection based on Singular value decomposition (SVD) can be done easily even when tamperer does some manipulations such as additional noise, scaling or rotation to image part before pasting to another part, and it works well for lossy format such as JPEG, detection based on SVD happens by dividing image into overlapping blocks and apply SVD on each block base on SVD formula in (1) where A is image matrix and U is a (m x m) orthogonal matrix, V is an (n x n) orthogonal matrix and S is an (m x n) diagonal matrix with singular values on the diagonal.

$$A = USV^T \tag{1}$$

From SVD, singular values will extract and arranged in a matrix, then it needs to change features in each block into k-d tree and search for similar blocks for each query using (2) where u and v are values of orthogonal matrixes.

$$D(UN) = (\sum_{i=1}^{n}(u_i - v_i)^2)^{\frac{1}{2}} \tag{2}$$

At this time, blocks similarity matching will be done to find similar blocks. The main idea of this step is that a duplicated region consists of many neighbouring duplicated blocks. If two similar blocks can be fined in the analyzed space and if their neighbourhoods are also similar to each other, there is a high probability that they are duplicated and they are tagged as duplication area, then the output of the method is a duplicated regions map which showing the image regions that are expected duplicated. Based on their experimental results, their proposed method gives robustness against post processing like blur filtering, Gaussian noise addition, etc. Detection time for this method for a 256 x 256 colour image is 120 second which is better compare to existed method in [6].

In this paper, we propose a detection algorithm based on Fourier transform to extract transformed image matrix, and find location of similar blocks in the image using inverse Fourier transform.

III. Proposed Method

When a forgery occurs in a digital image, it shows that statistical characteristics of image have changed; therefore it is obvious that statistical characteristics of forged area are different from original area. For detecting forged area, the statistical characteristics of each small sections of the image calculated and compared with each other. Fig. 2 shows the general procedures of detecting copy-move forgery in digital images [10].

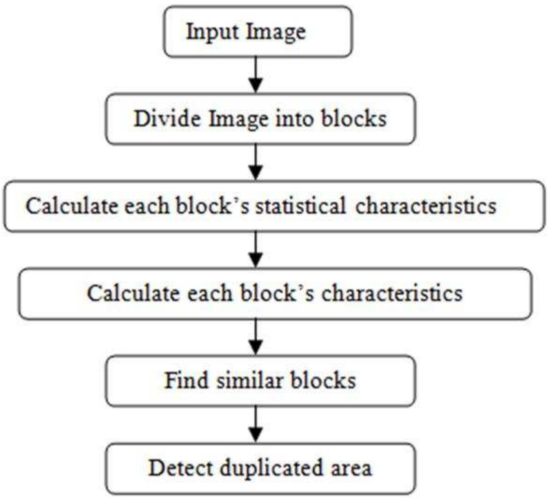
Input Image
Divide Image into blocks
Calculate each block's statistical characteristics
Calculate each block's characteristics
Find similar blocks
Detect duplicated area

Fig. 2: Copy-move forgery detection procedure

Most of detection techniques focused on block matching, and the procedure is common by dividing image into same size blocks and extracting image features by different techniques, afterwards searching for similar block to find which region is duplicated base on block matching, this is happen if many similar blocks in a specific distance can be fined, and these suspected blocks are connected to each other to identify tampered area. The proposed method works by resizing image to specific resize scale and convert the input image to gray scale image if it is colour to reduce time of detection. We have defined block size as a square with K x K pixels and assumed to be smaller than the size of the duplicated regions which have to be detected. Here we have defined block size 20 by default to divide image based on block size to same size overlapping blocks, and number of blocks calculated from (M x K + 1)(N x K + 1) where (M, N) are image pixels and K is the size of the block we have defined before. Fourier transform applied on image to extract features of each blocks, when Fourier transform of the image calculated, a function is created with the intensity signal across the image, and function is decomposed into a sum of orthogonal basis functions by using Fourier transform. f (m, n) is a function of two discrete spatial variables m and n, and the two-dimensional Fourier transform of f (m, n) is defined by the relationship in (3)

$$F(\omega_1,\omega_2)=\sum_{m=-\infty}^{\infty}\sum_{n=-\infty}^{\infty}f(m,n)e^{-j\omega_1 m}e^{-j\omega_2 n} \qquad (3)$$

The variables $\omega 1$ and $\omega 2$ are frequency variables, and F ($\omega 1$, $\omega 2$) is frequency-domain representation of f (m, n). F ($\omega 1$,$\omega 2$) is a complex-valued function that is periodic both in $\omega 1$ and $\omega 2$, with period 2π and period range $-\pi \leq \omega_1$, $\omega_2 \leq \pi$. Fourier transform applied on image blocks to perform correlation, subsequently the correlation of the blocks computed to locate features within image, then correlation are sorted in a lexicographically order because it can make matching more effective, and sorted correlation stored in a matrix named Q with the size of (M - K + 1) x (N - K + 1) x K2. After all blocks sorted properly, the algorithm continues into the matching step by testing each pair of blocks whether they are matching. For each row in matrix Q, correlations values are computed for the block matching to current row with the blocks matching to rows around the current row, if the computed maximum correlation value exceeds threshold which is block-matching threshold, then two blocks are duplicated. When similar blocks detected then the inverse of a transform is performed on a transformed image to produce the original image, and the inverse of two-dimensional Fourier transform of the image is done by (4)

$$F(m,n)=\frac{1}{4\pi^2}\int_{\omega_1=-\pi}^{\pi}\int_{\omega_2=-\pi}^{\pi}F(\omega_1,\omega_2)e^{j}\omega_1 m e^{j}\omega_2 n d\omega_1 d\omega_2 \qquad (4)$$

Where $\omega 1$ and $\omega 2$ are frequency variables, and and F ($\omega 1$, $\omega 2$) is frequency-domain representation of f (m, n).

IV. Experimental Result

The proposed method has been implemented using Matlab 7.9. Experimental environment is on a personal computer of 2.00GHz processors with 1GB memory. The block size is 20 x 20 pixels. Tests have been performed on various images with different size of duplication region and different formats. In the first experiment, several copy-move tampered images have been examined with proposed algorithm.

Fig.3 demonstrates an ordinary forgery, in Fig.3 (b) tampered image shown in which some part of the leaves copied and pasted on the trunk to cover it, and result of detection shown in Fig.3 (c).

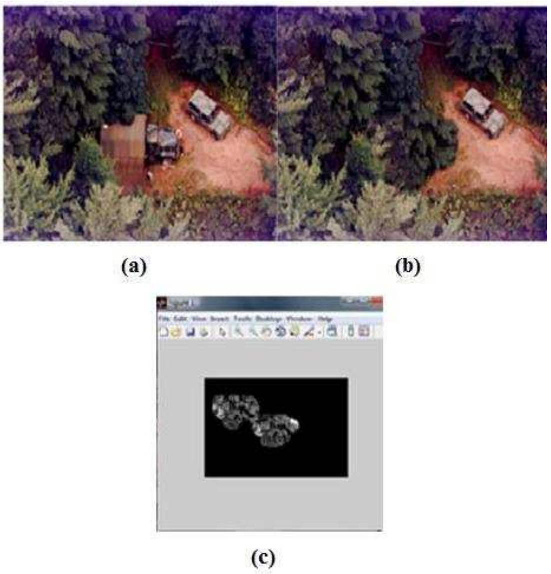

Fig. 3: (a) Original Image, (b) Tampered Image, (c) Detection Result

Lena gray scale image tampered and Fig.4(b) illustrates the tampered image where some part of the hair has been copied and pasted on the hat to cover some part of the hat, and Fig.4(c) shows the detection map.

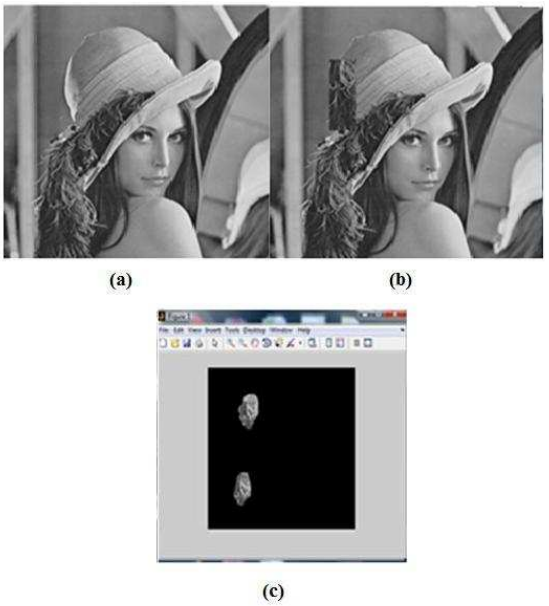

Fig. 4: (a) Original Image, (b) Tampered Image, (c) Detection Result

Fig.5 shows another forgery which is obvious, original image is tampered by hiding the man in the image and created tampered image in Fig.5 (b) along with detection result in Fig.5(c).

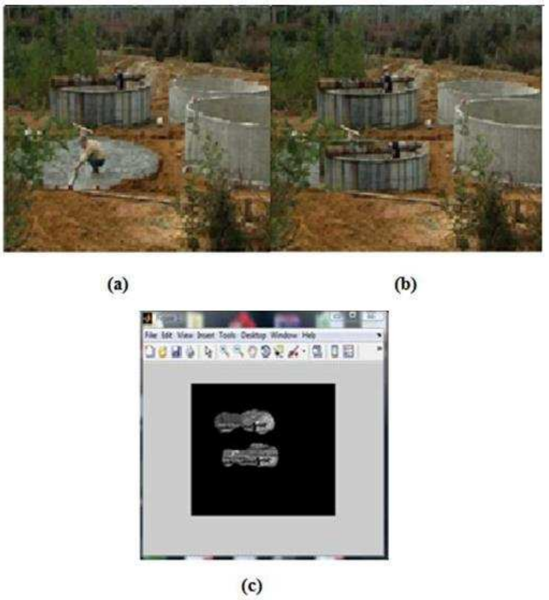

Fig. 5: (a) Original Image, (b) Tampered Image, (c) Detection Result

In time performance, the complexity time of the proposed algorithm is better compared with existing methods [6]. Kang and Wei explained in their experimental results [6] they have tested a gray scale image with dimension 256 x 256 and block size 20, the detection time was 60 seconds, and compare with our algorithm for the same image detection time is 8 seconds. Another image has been test, based on Kang and Wei algorithm, the average runtime of the their algorithm for one colour channel of a 256x256 image when block size B=20, is approximately 120 seconds, and compare to our algorithm for the same size of colour image it takes 11 seconds to find duplicated areas.

V. Conclusion

With the rapid progress of image processing technology, detection of digital image forgery is an interesting research topic in forensics science. In this paper, a specific type of forgery which is Copy-move forgery investigated and an efficient detection method proposed based on Fourier transform. The procedure of detection starts by dividing image into same size overlapped blocks and apply Fourier transform on each block, finally demonstrate the location of similar blocks by using inverse Fourier transform. Proposed method is able to locate duplicated areas in reasonable time compare to existing methods, and computational complexity reduced. Our future work is to enhance our method to detect duplicated area more accurately and improve it to be able to detect another kind of forgery which is image splicing.

Acknowledgment

The authors would like to thank University of Malaya for their educational and financial support.

References

[1] J. Fridrich, “Methods for tamper detection in digital images,” *Proceeding of ACM Conference on Multimedia and Security*, p. 1923, 1999.

[2] C. L. Jing, “Image copy-move forgery detecting based on local invariant feature,” *Journal of Multimedia*, vol. 7, 2012.

[3] Q. S. W. Chen and W. Su, “Image splicing detection using 2-d phase congruency and statistical moments of characteristic function,” *E. J. Delp and P. W. Wong, editors, Proceedings of SPIE: Security and Watermarking of Multimedia Content IX*, vol. 6505, p. 65050, 2007.

[4] D. T. G. Li, Q. Wu and S.Sun, “A sorted neighborhood approach for detecting duplicated regions in image forgeries based on dwt and svd,” *Proceedings of IEEE International Conference on Multimedia and Expo*, pp. 1750–1753, 2007.

[5] a. J. L. J. Fridrich, D.Soukal, “Detection of copy-move forgery in digital images,” *Proceeding of Digital Forensic Research Workshop*, pp. 55–61, 2003.

[6] S. S. B. Mahdian, “Detection of copymove forgery using a method based on blur moment invariants,” *Proceedings of fifth International conference on Forensic Science International*, p. 180189, 2007.

[7] M. G. M. Najah, H. Muhammad and B. George, “Copy-move forgery detection using dyadic wavelet transform,” *Eighth International Conference Computer Graphics, Imaging and Visualization*, pp. 103–108, 2011.

[8] G. Q. H. Jie, Z. Huaxiong and H. Hai, “An improved lexicographical sort algorithm of copy-move forgery detection,” *Second International Conference on Networking and Distributed Computing*, pp. 23–27, 2011.

[9] S. W. X. Kang, “Identifying tampered regions using singular value decomposition in digital image forensics,” *International Conference on Computer Science and Software Engineering*, 2008.

[10] X. P. Z. H. Z. Zhang, Y. Ren and S. Zhang, “A survey on passive-blind image forgery by doctor method detection,” *Proceedings of the Seventh International Conference on Machine Learning and Cybernetics*, 2008.