www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 1 January 2015, Page No. 10187-10190

A Compressive Survey on Active and Passive Methods for Image Forgery Detection

Nikhilkumar P. Joglekar[1], Dr. P. N. Chatur[2]

[1] Government College of Engineering, Amravati 444 604, Maharashtra, India
nikhil.joglekar1@gmail.com

[2] Government College of Engineering, Amravati 444 604, Maharashtra, India
chatur.prashant@gmail.com

Abstract: ***In digital computing world representing information in visual forms has become very important. Due to improvement in computing and network technologies, in past few years we have seen a considerable rise in the accessibility and transmission of digital images using imaging technologies like digital cameras, scanners. This technology is also used for manipulating digital images and creating different forgery in image which is very difficult to identify. In tampering of digital images involved copying one part of image into other part of image, any types of image manipulation operation is consider as a forgery in image. Simple way to image forgery is manipulated image without leaving any perceptible traces; as a result, the authenticity of images can't be taken for granted. There are no of operation in which we can change the image contain, like scaling, rotating, cropping. Preserving image authenticity is very complex because easily availability and free downloading image editing software. So detecting image forgery is difficult and challenging task. A lot of research has been going on this area and one of the problems is unavability of original image for evaluation. In this paper we studied active and passive or blind approaches to detect forgery in digital image.***

Keywords: Image Processing, Image Tampering, Copy-move Detection

1. Introduction

1.1 **Problem Definition**

Digital images are the foremost source of information in today's digital world. Due to their ease of acquisition and storage they are the fastest means of information convey. Images can be used as an evidence for any event in the court of law. The images broadcasted in any TV news are accepted as the certificate for the truthfulness of that news. Digital images are being used in many applications ranging from military to medical diagnosis [1] and from art piece to user photography. Hence the digital image forensics emerges as fast growing need of the society. Thus the images are required to be authentic.

In today's scenario due to advancement of computers and availability of low-cost hardware and software tools it is very effortless to manipulate the digital images without leaving the visible traces of manipulation. It has become difficult to trace these manipulations. As consequences, the integrity and authenticity of digital images is lost. This modification of images can be used for some malicious purpose like to hide some important traces from an image. Thus modified images are used to transmit incorrect information. In order to identify the integrity of the images we need to identify any modification on the image. Digital Image Forensic is that branch of science that deals at exposing the malicious image manipulation[8].

Digital image forgery detection technique generally classified into two categories, first one is active technique and second one is passive technique. There are some drawback in active technique in which embedding some information in image either during creation or before it broadcasting to public. As compared with blind technique we couldn't add any data or modified image. Below we discussed about these two image forgery detection method.

2. Literature Review

2.1 Active Authentication

There are many tools that can be easily create or manipulate the digital image. As a result, authenticity of image can't be taken granted, now a day digital image is used for legal photographic evidence in that case we can't easily trust on any digital document. Manipulation of image consists of many processing operation like scaling, rotating, blurring, brightness adjusting, change in contrast, etc. or any combination of these operation. Doctoring image means pasting one part of image into other part of image, skillfully without living any trace. One important tool for authenticity of digital image is digital signature watermarking.

2.1.1 Digital Signature

Digital signature is some sort of cryptographic is a mathematical scheme for demonstrating the authenticity of digital document. Digital signature is used for detecting image forgery or tampering. In digital signature a robust bits extracted from the original image. In this method image is divided into blocks of 16*16 pixels. A secret key k is used to generate N random matrices with entries uniformly distributed in interval [0, 1]. A low pass filter is applied on each random matrix to obtained random smooth pattern. System generate digital signature by applying signing process on digital image. Signing process contain following steps:

1) Decompose the image using parameterized wavelet feature.
2) Extract the SDS
3) Cryptographically hash the extracted SDS, , generate the crypto signature by the image senders private key.
4) Send the image and its associated crypto signature to the recipient.

Digital signature is simple and basic approach for digital image authentication.

2.1.2 Watermarking

Watermarking is also used for image forgery detection. Several watermarking techniques have been proposed. One uses a checksum schema in that it can add data into last most significant bit of pixels [3]. Others add a maximal length linear shift register sequence to the pixel data and then identify the watermark by computing the spatial cross-correlation function of the sequence and the watermarked image. These watermarks are designed to be invisible, or to blend in with natural camera or scanner noise. Visible watermarks also exist. In addition to this, a visually undetectable watermarking schema is also available which can detect the change in single pixels and it can locate where the change occur [3]. Embedding watermarks during creation of digital image it may limits its application where digital image generation mechanism have built-in watermarking capabilities. These active techniques have some limitation because they required some human intervention or specially equipped cameras. To overcome this problem a passive authentication has been proposed.

2.2 Passive Authentication

Passive or blind forgery detection technique uses the received image only for assessing its authenticity or integrity, without any signature or watermark of the original image from the sender. It is based on the assumption that although digital forgeries may leave no visual clues of having been tampered with, they may highly likely disturb the underlying statistics property or image consistency of a natural scene image which introduces new artifacts resulting in various forms of inconsistencies. These inconsistencies can be used to detect the forgery. This technique is popular as it does not need any prior information about the image. Existing techniques identify various traces of tampering and detect them separately with localization of tampered region.

2.2.1 Improved DCT-based

An improved DCT (discrete cosine transform)-based technique was proposed in [4] to discover copy-move forgery in digital images. The original image is sub-divided into fix number of blocks, and then DCT is computed on that image. The DCT coefficients are lexicographically sorted, and compared with different blocks. DCT-based technique is robust against JPEG compression, additive white Gaussian noise, or blurring distortion [9],[13]. DCT-based technique is also used to detect multiple copy-move forgery in same image.

Cao et al [5] proposed new improved DCT-based technique for locating duplicated regions in image. The task for finding copy-move forgery in image is to find large similar region in image. Since the duplicate region is unknown in terms of their size and shape, if we compare each and every possible pairs pixel by pixel, the computational complexity become much higher, and it is difficult to handle [9]. It is more practical to divide input image into some fixed size small region to reduce computational complexity and time and finding duplicate region present in image. In order to efficient detection of duplicate region in image, some appropriate and robust features Features have to be extracted from each block. A good features extraction can not only represent the whole blocks, but also reduce the dimension of feature vector [5]. The method uses circle block for representing DCT coefficient's array.

According to the above discussion, the duplicate region detection framework is given as follows:

(1) Dividing the suspicious image into number of fixed-size small blocks.

(2) DCT is applied to each block to generate the quantized coefficients.

(3) Representing each quantized block by a circle block and extracting appropriate features from each circle block.

(4) Searching similar block pairs.

(5) Finding correct blocks and output them.

It can detect even multiple copy move forgeries in the same image and also is relatively robust to some common distortions

2.2.2 Noise pattern based

Noise pattern based image forgery detection method was proposed in [6]. Noise present in an image and found that original image has different noise pattern is associated with that regions. However, a tampered image, where two regions has exactly same noise pattern, because they are copied and paste part. In this method input image is segmented into number of small segment of size m*n in such a way that each object is fully contained in a single segment, and the segment is almost homogeneous [6],[10]. After segmentation of image, then we estimated image noise. Though many different denoising algorithms exist in the literature, which can be used for noise estimation, each algorithm focuses on a particular type of noise [8],[13]. After noise estimation we analyzing noising pattern for each image segment. Then finally find the image is tampered if the noise patterns of at least two segments are similar.

2.2.3 Approximate run length based

A new method was proposed which is based on approximate run length (ARL) to detect CMF. The edge-gradient array of a given image is calculated, and then the approximate run length is computed along the edge-gradient orientation. Zhao et al used chrominance spaces with RLRN (run-length run-number) for CMF detection [7]. The input image is transferred into YCbCr color mode. Then RLRN is used to extracted features from the de-correlation of a chrominance channels. Support vector machine (SVM) was used for classification purpose [8],[12]. This method gave better performance with JPEG image format than the TIFF image format.

2.2.4 Weber local descriptor

Fig.1 shows the block diagram of proposed method. In first step it converts given image into YCbCr color space. In image forgery generally image tampering do in color space and it is default to trace in color space. YCbCr color space stored color into luminance and chrominance. The Human eye is less sensitive to luminance and chrominance. Even after tampering image look like an original image, some tampered traces are left in the chrominance channels. In second steps, the chrominance component is used for extracting feature in the form of weber local descriptor. Multi scale weber local descriptor is introduce where the histograms from different operators of variation (P, R) are concatenated and used to represent the image features; P is the count of the neighbors, and R is the spatial-scale for the operator. In last step Support vector machine is used for classify the input image is original or forged.

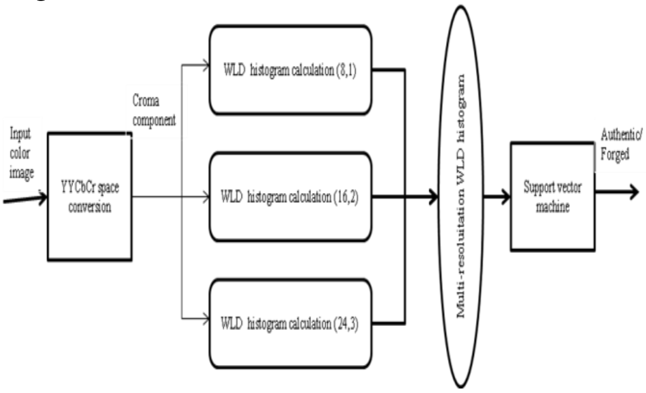

Figure 1: Block diagram of WLD.

WLD is a local descriptor and it is based on fact of human sensitivity of a sample is relies on the change of original stimulus of intensity [11]. WLD is a texture descriptor and is used for extract feature from image. It has many advantages such as edge detection and it is robust to illumination. WLD is describing below for feature extraction purpose. WLD is based on weber law and it has two main components: differential excitation and orientation [11]. WLD is calculated on these two components and then a histogram is calculates. Final result is send to support vector machine [12] were it is classified the input image according WLD histogram output and it classify the image into forged or original image. This method contain more accurate compares with other method , and it is insensitive to noise and illumination.WLD is suitable for splicing detection in image and take less time to detect forgery in image. This technique contain heights accuracy than others technique.

3. Conclusion

brief survey on forgery detection method was presented. This survey covers both active method as well as passive method for detection of image forgery. It will help researchers to explore new idea and new solution to find forgery in image. An attempt has been made to introduce various techniques that represent improvement in forgery detection method. Still there are some drawbacks in each method and that must be eliminating to obtained efficient result. In active method both digital signature and watermarking technique data embedded into image and it is not sufficient to detect forgery in image. In DCT-based method contain high computational complexity. DCT-based method is inapplicable in high texture and small forged region. Likewise ARL method less computational complexity but it does not possess effective accuracy rate. In WLD method is suitable for copy-move as well as splicing detection and its accuracy is heights among all passive methods.

Current research in forgery detection is mainly limited to image tampering detection technique and it can be extended to audio and video. The validation of performance measures, such as accuracy, robustness, security is a major concern. This is because of the lack of established benchmarks. One of the major limitations of current forgery detection method is that there is no way to distinguish between malicious tampering and innocent retouching.

References

[1] B.L. Shivakumar and S. S. Baboo, “Detecting copy-move forgery in Digital images: A survey and analysis of current methods”, Global Journal of Computer Science and Technology, vol. 10, no. 7, 2010.

[2] Guillermo Ruiz∗, Edgar Chavez† and Eric S. Tellez, “Towards Self-Indexing Relational Databases”, 1550-4069/13 $26.00 © 2013 IEEE.

[3] X. Zhao, J. Li, S. Li, and S. Wang, “Detecting digital image splicing in chroma spaces”, Digital Watermarking, pp. 12–22, 2011.

[4] Y. Huang, W. Lu, W. Sun, and D. Long, “Improved DCT-based detection of copy-move forgery in images”, Forensic science international, vol. 206, no. 1–3, pp. 178–184, 2011.

[5] Y. Cao, T. Gao, L. Fan, and Q. Yang, “A robust detection algorithm for copy-move forgery in digital images”, Forensic Science International, vol. 214, no. 1–3, pp. 33–43, Jan. 2012.

[6] N. Muhammad, M. Hussain, G. Muhammad, and G. Bebis, “A non-intrusive method for copy-move forgery detection”, Advances in Visual Computing, LNCS, Springer, pp. 516–525, 2011.

[7] Z. He, W. Sun, W. Lu, and H. Lu, “Digital image splicing detection based on approximate run length’”, Pattern Recognition Letters, pp. 1591–1597, 2011.

[8] H. Ling, H. Cheng, Q. Ma, F. Zou, and W. Yan, "Efficient image copy detection using multiscale fingerprints," IEEE Magazine of Multimedia, vol. 19(1), pp. 60-69, 2012.

[9] H. Farid, "Image forgery detection - a survey," IEEE Signal Processing Magazine, vol. 5, pp. 16–25, March 2009.

[10] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," Signal Processing: Image Communication, vol. 25, pp. 389-399, 2010.

[11] J. Chen, S. Shan, C. He, G. Zhao, M. Pietikainen, X. Chen, and W. Gao, ‘WLD: A robust local image descriptor’, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 9, pp. 1705–1720, 2010.

[12] N. Cristianini and J. Shawe-Taylor, *An Introduction to Suppor Vector Machines and Other Kernel-based Learning Methods*, Cambridge University Press, 2000.

[13] A. Popescu and H. Farid, Exposing digital forgeries by detecting duplicated image regions, Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.

Author Profile

N. P. Joglekar received his B.Tech. degree in Computer Science and Engineering from Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded, Maharashtra, India in 2013, pursuing M.Tech degree in Computer Science and Engineering from Government College of Engineering, Amravati, Maharashtra, India. His research interest includes image processing. At present he is engaged in finding passive method for detecting image forgery using weber local descriptor.

Dr. P. N. Chatur has received his M.E degree in Electronics Engineering fromGovernment College of Engineering Amravati, Maharashtra, India and Ph.D. degree from Amravari University. He has published twenty papers in international journals. His area of research includes Artificial Neural Network, Data Mining, Data Stream Mining and Cloud Computing. Currently, he is Head of Computer Science and Engineering & Electronics Engineering Department at Government College of Engineering Amravati, Maharashtra, India. At present he is engaged with large database mining analysis and stream mining.