VERIZONA PUBLISHER
Publishing Your Ideas

www.verizonaonlinepublishing.com
Vol: 1, Issue: 1

Journal of Electronics and Communication Engineering Research

Active Image Forgery Detection: State of the Art and Possible Enhancements

Maryam Pahlavan Nodeh

Department of Computer Science, SanabadGolbahar Institute of Higher Education, Golbahar, Iran

***Corresponding author:** Maryam Pahlavan Nodeh, Department of Computer Science, SanabadGolbahar Institute of Higher Education, Golbahar, Iran; E mail: pahlavan.maryam@sanabad.ac.ir

Article Type: Review, **Submission Date**: 20 April 2016, **Accepted Date:** 21 April 2016, **Published Date:** 11 May 2016.

Citation: Maryam Pahlavan Nodeh (2016) Active Image Forgery Detection: State of the Art and Possible Enhancements. J. Elec. Commu. Eng. Resol 1(1): 11-13.

Abstract

Hundreds of thousands of digital images and image contents are produced, stored, and distributed in every minute worldwide through various digital cameras, social media, and image sharing platforms. While most of images could be real and they indicate a certain source of evidence, some others could be easily tampered and cause several detriments to us. This begs the question: How we can tackle the problem of digital image forgery detection? Detection of tampering with digital images is still an active research for the image processing and computer vision community. Over the past decade, there have been vast expansions in the designing and developing of image forgery detection algorithms. All these algorithms are divided into two categories: (1) Active, and (2) Passive. Using the Active approaches, we create and embed data or information as a cipher key into the original images to protect them against a forgery. In the Passive algorithms we only investigate some local image features such as statistical anomalies, correlations and compressions to detect forgeries.

Keywords: Image forgery detection, Image encryption, Digital forensic.

Introduction

We are living in an Internet of Things (IoT) era where security of computerized information such as digital images and video streams are becoming more important than ever. The expressive potential of images and the ease in their storage, transmission, and distribution are more and more exploited to convey information. Together with a bunch of undoubted benefits, the availability of digital images brings a major drawback. With the development of low cost and powerful image editing tools, the craft of tampering visual content is no more restricted, so they could be easily altered without leaving any traceable effect. The detection of image forgery is really important because digital images can be used as legal evidence in many areas such as forensics investigations. To ensure trustworthiness, image authentication strategies have emerged to verify the content and prevent forgery.

Image forgery detection methods in computer vision are quite able to authenticate the entire content of images and protect them against tampering. A reliable images forgery detection system will be useful in many areas such as surveillance systems, medical imaging, criminal investigation, journalism, visa and immigration documents, insurance processing, and forensic investigations.

The forgery detection techniques that are developed for digital images are mainly classified into two major categories: Active and Passive [1-3]. Using the Active algorithms we would like to insert data or signature at the time of digitizing. In contrast to the Active approaches, the Passive algorithms operate in the absence of any data or signature, investigating local features such as statistical anomalies, correlations, compressions, and measurements of objects in the existence image to detect a forgery.

In this paper, we are going to study and review the Active algorithms in digital image forgery detection, providing insights and tendencies for possible future enhancements. The main objectives of the current contribution are as follows:

To extract current knowledge and so far progresses in Active image forgery detection techniques.

To review the state of the art of Active image forgery detection algorithms.

To provide better insight and tendencies in the research area, so we can plan several future enhancements to advance the level of the progress and impact of the active forgey detection strategies.

We do hope that this work will serve as a guide for image forgery detection. The rest of the paper is arranged as following. Section 2 covers the literature review. Section 3 presents discussions and outlooks.

Literature Review and Taxonomy

In this section, we will first review the state of the art of active image forgery detection and present a taxonomy of different algorithms developed in the research body.

In 1998 Podilchuk et al. [4] proposed Two perceptual schemes the challenge is to introduce a digital watermark that does not alter the perceived quality of the electronic content, while being extremely robust to attack.They proposed two watermarking techniques (robustness and transparency) for digital images that are based on utilizing visual models which have been developed in the context of image compression. Equally important, the

watermark should not alter the perceived visual quality of the image. Two perceptual schemes have been proposed: the IA-DCT and IA-W approaches. The IA-DCT algorithm offers the advantage of being able to watermark partially decompressed JPEG bit streams. The results show that the DCT framework of the IA-DCT scheme is quite robust to JPEG compression as well as other types of common image transformations.

In 2011, Li et al. [5] proposed a new reversible watermarking algorithm based on PEE which stands for Prediction-error expansion. Their algorithm focused on highly correlated regions and pixels, and it was able to better exploit the spatial redundancy to achieve an improved performance compared with conventional PEE. In 2011, Tafti et al [6] investigated several statistical values for active image forgery detection and eventually embedded those values into the spatial domain to prevent image forgery. In 2011, Tafti et al [7] performed a kind of same method by embedding the data into the frequency domain rather than the spatial domain. In 2012 Subramanyam et al. [8] proposed a novel technique to embed a robust Watermark in the JPEG2000 compressed encrypted images using three different existing watermarking schemes. They defined Digital asset management systems (DAMS) for tamper detection or ownership declaration or copyright management purposes. This planalsopreservesthevery private nature of contentastheembeddingisdoneonunreadabledata. In 2013, He et al. [9] proved that using geometrical disorder stable watermarking algorithms and according to improvement and changeable on the pillar graphs can resistance to geometrical assaults and signal processing assaults. In order tomeasureelectronickeydifferences and similarities betweenthe originalandtheextraction qualitative measurement methodswere used.

In 2013, Shaukat et al. [10] showed digital watermarking algorithms that proposed on the chotiac map. Those are proved that the logistic guide was utilized for finding implanting positions of disorderly watermark era and a novel watermarking plan was proposed. The logistic guide is utilized to distinguish the positions for installing the watermark in the host picture. In that plan, the first flag was not presupposed amid the extraction process. In 2013, Tafti et al. [11] combined several computational algorithms, such as SVD and cellular automata to encrypt an image in the spatial domain, making a digital image robust against forgery.In 2014, Hassannia [12] et al. developed two active image forgery detection techniques based on the cellular automata methodology. In 2015, Hu et al. [13] showed an image forgery detection plan was proposed to successfully recognize an altered background or foreground picture utilizing image watermarking and alpha mattes. This strategy can precisely distinguish traded foreground images, traded background images, altered foreground images, and altered background images, and can identify forgery images made utilizing image matting or image in painting. Moreover, the proposed system utilizes versatile limits, making it suitable for useful applications. In 2015, Rohani et al. [14] developed a method using LU decomposition and one dimensional cellular automata to enhance their previous platform [15] designed using SVD.

Based on the literature review, we come up with taxonomy of active digital image forgery detection algorithms. Taxonomy of active image forgery detection algorithm is shown in Figure 1. As you see in this figure, all active image forgery detection algorithms have been divided into two major categories namely: 1) Digital Signature in which a kind of digital signature must be inserted into an image as the image is recording, and 2) Digital Watermarking in which a symbol, data, or a watermark should be inserted in to an image at the time of storing.

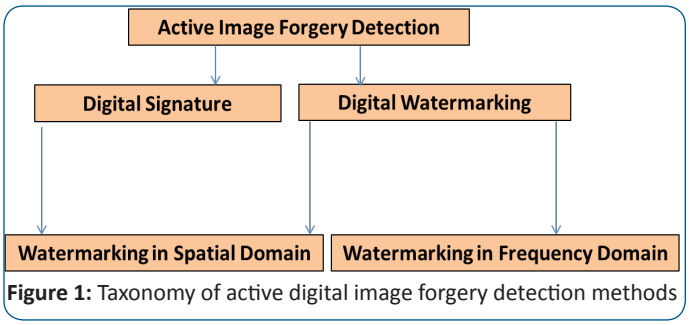

Figure 1: Taxonomy of active digital image forgery detection methods

Discussion and Outlook

This report demonstrates the state of the art and review the current progresses in active algorithm developed for digital image forgery detection. Not all active image forgery detection approaches are accurate and robust enough in detecting a forgery, since they all need to work at the time of recording or storing the image. In addition, not all digital images are suitable for active image forgery detection techniques.Images combined with text data (e.g., electronic documents) that includes complete structure may not suit for such algorithms. The accuracy and quality of the active image forgery detection algorithm is based on several factors, such as type of the watermark, statistical data, embedding data in frequency or spatial domain.

From the software application side, we can make a web service library as an open access framework for digital image forgery detection, and make it available to the research community all around the world to collaborate each other developments. Similar works are presented in [16-18].

Fast and accurate active image forgery detection techniques still needed in the research area. Combining the methods with passive approaches is also possible and it will enhance the accuracy of the work. Moving from the algorithms to application areas would be a great practical way to examine the accuracy of the proposed methods on real business data, such as medical images, microscopy images [19,20] and etc. Applying the algorithms on bigger datasets available on the Internet will proof their accuracy in a better way.

References

1. Farid H. Image forgery detection. Signal Processing Magazine. IEEE. 2009; 26(2):16-25.
2. Birajdar GK, Mankar VH. Digital image forgery detection using passive techniques: A survey. Digital Investigation. 2013; 10(3):226-245.
3. Kaur A, Malhotra S. Review Paper on Re-Sampling Detection in Digital Image Forensics Using Peak Value Identification Classifier. International Journal. 2015; 3(4).
4. Podilchuk CI, Zeng W. Image-adaptive watermarking using visual models. Selected Areas in Communications, IEEE Journal. 1998; 16(4):525-539.
5. Li X, Yang B, Zeng T. Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. Image Processing, IEEE Transactions. 2011; 20(12):3524-3533.

6. Tafti AP, Malakooti MV, Ashourian M, Janosepah S. August. Digital image forgery detection through data embedding in spatial domain and cellular automata. In Digital Content, Multimedia Technology and its Applications (IDCTA). 2011: 7th International Conference. IEEE. p. 11-15.
7. Tafti AP, Janosepah S. Digital images encryption in frequency domain based on DCT and one dimensional cellular automata. In Informatics Engineering and Information Science. Berlin Heidelberg: Springer. 2011; p. 421-427.
8. Subramanyam AV, Emmanuel S, Kankanhalli MS. Robust watermarking of compressed and encrypted JPEG2000 images. Multimedia, IEEE Transactions. 2012; 14(3):703-716.
9. He X, Zhu T, Yang G. A geometrical attack resistant image watermarking algorithm based on histogram modification. Multidimensional Systems and Signal Processing. 2015; 26(1):291-306.
10. Jamal SS, Shah T, Hussain I. An efficient scheme for digital watermarking using chaotic map. Nonlinear Dynamics. 2013; 73(3):1469-1474.
11. Tafti AP, Maarefdoust R. Digital Images Encryption in Spatial Domain Based on Singular Value Decomposition and Cellular Automata. International Journal of Computer Science and Information Security. 2013; 11(4):121.
12. Tafti AP, Hassannia H. Active Image Forgery Detection Using Cellular Automata. In Cellular Automata in Image Processing and Geometry. Springer International Publishing; 2014. p. 127-145.
13. Hu WC, Chen WH, Huang DY, Yang CY. Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes. Multimedia Tools and Applications; 2015. p. 1-22.
14. Far MAM, Rohani F, Behravesh E. An Active Algorithm to Gray-scale Digital Image Forgery Detection based on Cellular Automata and LU Decomposition. J Comput Sci Softw Dev. 2015; 1(001).
15. Malakooti MV, Tafti AP, Rohani F, Moghaddasifar MA. RGB digital image forgery detection using Singular Value Decomposition and One Dimensional Cellular Automata. In Computing Technology and Information Management (ICCM). 2012: 8th International Conference. IEEE. p. 483-488.
16. Tafti AP, Hassannia H, Piziak D, Yu Z. SeLibCV: A Service Library for Computer Vision Researchers. In Advances in Visual Computing. Springer International Publishing; 2015. p. 542-553.
17. Tafti AP, Hassannia H, Yu Z. siftservice. com-Turning a Computer Vision algorithm into a World Wide Web Service. arXiv preprint arXiv:1504.02840. 2015.
18. He Q, Zhao B, Chang L, Su J, You I. PSSRC: A Web Service Registration Cloud Based on Structured P2P and Semantics. International Journal of Data Warehousing and Mining (IJDWM). 2016; 12(2):21-38.
19. Rohani F, Hassannia H, MoghaddasiFar MA, Sagheb E. Human cell detection in microscopic images through discrete cosine transform and Gaussian mixture model. Computational Biology and Bioinformatics. 2014; 2(4):52-56.
20. Rohani F, Far MAM, Bavojdan FF. From Business Process Management to Flexible Image Analysis Applications: A Case Study.