International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Study and Investigation of Tampering Detection Methods Based on Image Hashing

V. Sumathi, Dr. V. Anuradha

[1]Research Scholar, Department of Computer Science, Sree Saraswathi Thyagaraja College, Pollachi, Tamil Nadu, India

[2]Head (PG), Department of Computer Science, Sree Saraswathi Thyagaraja College, Pollachi, Tamil Nadu, India

ABSTRACT

Technology is growing at outstanding speed. There are numerous ways to be had to govern digital visible content material. This leads people to manipulate images quite simply and fast. When the image cannot be distinguished best by way of visible exam, some felony troubles may stand up. The image this is dispatched on the destination over the network need to be similar to at the supply facet. However it's far very difficult to trust at the received contents without any take a look at, particularly inside the areas where the source image is unknown and one has to use data that is available about the image best. images are considered to be the maximum powerful and sincere media of expression. For a long term, those were typical as proves of evidences in numerous fields which include journalism, forensic investigations, army intelligence, scientific research and guides, crime detection and criminal proceedings, investigation of coverage claims, medical imaging and so forth. As a result, images have almost misplaced their reliability and place as proves of evidences in all fields. This is why digital image tamper detection has emerged as important research vicinity to set up the authenticity of digital pix with the aid of separating the tampered lots from the authentic ones. On this paper, various methods of tampering the image are mentioned and the various detection techniques are surveyed. Subsequently, concluded the comparative take a look at with a few parameters.

Keywords : Image, Tampering, Detection, Active, Passive, Photographs.

I. INTRODUCTION

The digital images are a powerful medium of communication which contains a huge amount of information. Today's images have an important impact on our society. The image authentication and verification is important which are used in many fields such as forensic investigation, criminal investigation, surveillance systems, and intelligence services [1]. Using the various software that are available today, the digital images can be forged without leaving any traces.

A digital image is a numerical representation of a two dimensional image. Digital images are electronic snapshot taken of a scene or scanned from documents such as photographs, manuscript, printed texts, and artwork. Today's technology allows digital media to be altered and manipulated in ways that were simply impossible 20 years ago [1]. In spite of the various professional experts and software tools available worldwide, it is easier to manipulate an image without leaving any clue.

An image is "tampered" means part of the content of a real image is altered. An image is tampered implies that it must contain two parts: 1) Unchanged region 2) Tampered region. Due to the ease of generating and modifying images it is critical to establish trust worthiness for online multimedia information. The assessment of the reliability of an image received through the Internet is an important issue. Images are widespread on today's internet and cause significant social impact, which can be evidenced by the increase of social networking sites with user generated contents. Specifically, methods useful to establish the validity and authenticity of a received image are needed in the context of Internet communications. It uses signature-based approaches. In this, the image hash is associated with the image as header information and must be small and robust against different operations.

In order to perform tampering localization, the receiver should be able to filter out all the geometric transformations (e.g., rotation, scaling) added to the tampered image, in order to align the received image with the one at the sender. An image hash is a distinctive signature which represents the visual content of the image in a compact way (usually just few bytes). The image hash should be robust against allowed operations and at the same time it should differ from the one computed on a different/tampered image. Image hashing techniques are considered extremely useful to validate the authenticity of an image received through a communication channel.

II. LITERATURE REVIEW

Image tampering is defined as “adding or removing important features from an image without leaving any obvious traces of tampering” and thus image tampering is considered as intentional manipulation of images for malicious purposes [5]. There are various techniques for counterfeiting images.

Swati Shivaji Bhosale, Gyankamal J. Chhajed, defines “In this paper authentication and tampering detection of transmitted image is proposed with the use of scale invariant feature transform algorithm to extract the interest point of the image. These points are used to create signature, which further is transmitted along with image and analyzed at the destination for authentication. The voting procedure is performed to determine transformations such as rotation, scale and to align the received image. In this method image is divided into blocks and for the tamper detection comparison of histograms of gradients is used”.

Sebastiano Battiato, Giovanni Maria Farinella, Enrico Messina, and Giovanni Puglisi, defines ‘‘Image hash encodes the spatial distribution of the image features to deal with highly textured and contrasted tampering patterns. A block-wise tampering detection which exploits an histograms of oriented gradients representation is also proposed. A non-uniform quantization of the histogram of oriented gradient space is used to build the signature of each image block for tampering purposes. Experiments show that the proposed approach obtains good margin of performances with respect to state-of-the art methods”.

Sujoy Roy Qibin Sun, defines “This is primarily because of the difficulty in meeting two contradictory requirements. First, the hash should be small and second, to detect localized tampering, the amount of information in the hash about the original should be as large as possible. The desynchronization of the query with the original further aggravates the problem. Hence a tradeoff between these factors needs to be found. This paper presents an image hashing approach that is both robust and sensitive to not only detect but also localize tampering using a small signature ($< 1kB$).

To our knowledge this is the first hashing method that can localize image tampering using a small signature that is not embedded into the image, like in watermarking”.

AR. Guru Gokul, N. Kumaratharan, & Dr. D. Balasubramanian, defines “ Digital images are powerful and widely used communication medium in many fields like medical imaging, digital forensics, surveillance, journalism, etc. The availability of sophisticated digital image technology has given rise to image forgery. The forgeries are very difficult for a human eye to detect. Passive tampering detection method aims to detect the tampering areas in the digital images without any prior knowledge of the original images. The available tampering detection technique uses 8 x 8 blocks to detect the tampered region. However, all the pixels involved in the block are not compared, which again leads to a forgery. To mitigate these effects, a new progressive passive copy-paste tampering detection technique is proposed. Experimental results show that the proposed technique overcomes the foresaid technique which enhances the tampering detection method”.

Minati Mishra, Flt. Lt. Dr. M. C. Adhikary, defines “Today, digital images have completely replaced the conventional photographs from every sphere of life but unfortunately, they seldom enjoy the credibility of their conventional counterparts, thanks to the rapid advancements in the field of digital image processing. The increasing availability of low cost and sometimes free of cost image editing software such as Photoshop, Corel Paint Shop, Photoscape, PhotoPlus, GIMP and Pixelmator have made the tampering of digital images even more easier and a common practice. Now it has become quite impossible to say whether a photograph is a genuine camera output or a manipulated version of it just by looking at it. As a result, photographs have almost lost their reliability and place as proves of evidences in all fields. This is why digital image tamper detection has emerged as an important research area to establish the authenticity of digital photographs by separating the tampered lots from the original ones. It gives a brief history of image tampering and a state-of-the-art review of the tamper detection techniques".

Digital Image tampering is very much similar in nature to that of the conventional photo fakeries where the conventional photographs are replaced by their digital counterparts. One of the key characteristics of a digital image is; it is easier to modify or manipulate a digital image in comparison to its conventional counterpart.

III. IMAGE HASHING

An image hash is a short signature of the image that preserves its semantic information under allowable changes made to it while at the same time differentiates it from a different image (either distinct or tampered). That is, it should be robust to allowable modifications (like small rotations, compression, scaling, addition of noise etc) and sensitive to distinct images or illegal manipulations to the original like tampering. Hashes find application in verifying the authenticity of protected content.

A typical image hashing method consists of two steps: (1) Hash Generation and (2) Verification. The image hashing generation method and tampering detection method are proposed.

Different hash based approaches have been recently proposed in literature. Most of them share the same basic scheme: i) a hash code based on the visual content is attached to the image to be sent; ii) the hash is analyzed at destination to verify the reliability of the received image. An image hash is a distinctive signature which represents the visual content of the image in a compact way (just few bytes). The image hash should be robust against allowable operations and at the same time it should differ from the one computed on a different/tampered image.

An image hash is a short signature of the image that preserves its semantic information under allowable changes made to. That is, it should be robust to allowable modifications (like small rotations, compression, scaling, addition of noise etc) and sensitive to distinct images or illegal manipulations to the original like tampering. A common approach of image hashing is extracting features which have perceptual importance and should survive compression. The authentication data are generated by compressing these features or generating their hash values. The user checks the authenticity of the received content by comparing the features or their hash values to the authentication data. In order to perform tampering detection, the receiver should be able to filter out all the geometric transformations added to the tampered image by aligning the received image to the one at the sender.

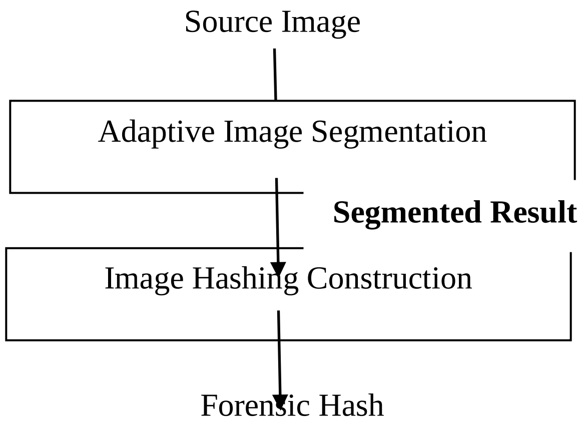

Figure 1: - Image Hashing Construction

Image hashing is a technique that represents the visual content of the image in a compact signature, which should be robust against a wide range of content-preserving attacks but sensitive to malicious manipulations. An image hash is a distinctive signature that represents the visual content of the image in a compact way. The image hash should be robust against common operations and be different from one computed on a different/tampered image. Image hashing techniques are considered extremely useful to validate the authenticity of an image received through a communication channel.

In our image hashing method includes two stages as shown in Figure. 1: first, the image is divided into closed regions using a novel adaptive image segmentation method; second, the color and position features of each closed region are obtained to generate the forensic hash. There are many more such cases of digital image tampering available and the list is increasing every second with addition of newer cases.

IV. TAMPER DETECTION METHODS

Image tampering again can be performed either by making changes to the context of the scene elements or without the change of the context. In the second case, the recipient is duped to believe that the objects in an image are something else from what they really are but the image itself is not altered [11]. Digital image tamper detection techniques can be broadly classified into two groups such as

i. Active Detection Methods.
ii. Passive Detection Methods.

The active techniques require a pre-processing step and suggest embedding of watermarks or digital signatures to images so as to authenticate them. The major difficulty with this method is that it requires the watermark to be embedded at the time of image capturing and for this; all digital cameras should have a standard inbuilt watermark.

On the other hand, the passive detection techniques do not require pre embedding of any watermark or digital signatures to the images and hence are commonly used for the purpose of tamper detection in digital images.

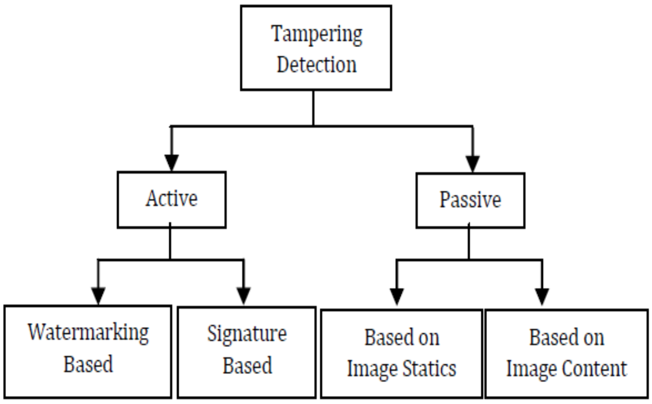

Figure 2 : Tampering Detection Methods

4.1. Active Detection Methods

Active taper detection techniques due to their inherent limitation, though, are not as common as those of the passive techniques still these are considered to be most efficient image authentication methods and a lot of research has been done in this field. These active image authentication techniques are commonly classified into two categories: the first method uses a fragile watermark, which localizes and detects the modifications to the contents. While the rate of tamper detection is very high for these methods they cannot distinguish between the simple brightness, contrast adjustments and replacement or addition of scene elements. Increasing the gray scales of all pixels by one would indicate a large extent of tampering by this method, even though the image content remains unchanged for all practical purposes [23]. The second method uses a semi-fragile watermarking, that only detects the significant changes in the image while permitting content-preserving processing.

The fragile watermark though has good localization and security properties but cannot differentiate forgeries such as addition or removal of parts of image, from the innocent image processing operations such as brightness or contrast adjustments.

The hybrid watermark can be used to accurately pinpoint changes as well as distinguish forgeries from other innocent operations. Active tamper detection and authentication schemes and developed a number of fragile, semi-fragile, robust, public as well as private key based watermarks for copyright protection, authentication and tamper detection [25-29] out of which, some either failed to effectively address the problems or sacrifice tamper localization accuracy of the original methods while few of them were proved to be highly efficient and effective.

Active tampering detection methods are generally considered as watermarking methods. This method can be applied in two domains, spatial and frequency domain. In Spatial domain techniques we directly work with image pixels, these techniques are Least Significant Bit, Predictive coding techniques, Correlation based techniques and Patchwork techniques. In LSB technique watermark in embedded into LSB of pixels of image [19]. Predictive coding technique takes the advantage of correlation between adjacent pixels [20]. In correlation based technique random noise is added into image and at the receiver if correlation between image and noise is above threshold then image is considered as tampered image.

4.2. Passive Detection Method

Passive tampering detection methods are based on Detecting splicing by visual cues, Detection of inconsistencies in local noise, Cyclostationary Approach etc. In detection of splicing by cues method abnormality present at boundary of object is detected to detect tampering [26]. Detection of inconsistencies in local noise method various noise levels in image is used to detection tampering [27]. Image has hidden cyclostationary property which is transformed by scaling therefore cyclostationary properties can be used to detect tampering [28].

The passive methods are regarded as evolutionary developments in the area of tamper detection. In contrast to the active authentication techniques these methods neither require any prior information about the image nor necessitate the pre embedding of any watermark or digital signature into the image. The underlying assumption that is the basis of these schemes is, though the carefully performed digital forgeries do not leave any visual clue of alteration, they are bound to alter the statistical properties of the image. The passive techniques try to detect digital tampering in the absence the original photograph as well as without any pre inserted watermark just by studying the statistical variations of the images.

4.2.1. Splicing

One of the types of image tampering is splicing or composition or photomontage. In such a forgery, elements from multiple images are often juxtaposed in a single image to convey an idea that could not have been conveyed by any of the original images. Such an idea usually does not reflect reality, and so such spliced images can be very damaging.

Digital splicing of two or more images into a single image is another commonly used image manipulation technique. When performed carefully, the borders between the spliced regions can be visually imperceptible. It is a popular way to distort the semantic content of an image so as to fool the viewer to misbelieve the truth behind a scene. Image splicing is a fundamental operation in image forgery and is characterized by simple cut-and-paste operation that takes a part of an image and puts it onto either the same or another image without performing any post-processing smoothing operation such as edge blurring, blending to it. By Image tampering, it generally means splicing followed by the post-processing operations so as to make the manipulation imperceptible to human vision

4.2.2. Copy-Move

Another common type of image forgery is the copy-move (or region duplication or cloning) forgery. In this type of forgery, regions from the same image are copied and pasted (with possible transformations) in the same image. This is usually done with the intent of hiding certain content present in the original image or duplicating certain content not actually present in the image. Copy-move forgeries are usually detected by searching for matching regions in the image, although recent research has taken a more SIFT-based approach, concentrating on matching key points (as in object detection) rather than blocks, in order to allow for various image transformations that can be used to create more convincing forgeries.

4.2.3. Image Retouching

Image Retouching can be regarded to be the much less harmful type associated with digital image forgery. Image retouching does not really considerably modify an image, however rather, improves or even decreases certain feature of an image. This method is well-liked by magazine photo editors. It can probably be asserted just about all magazine cover would utilize this technique to improve particular features of the image so that it can be more attractive; disregarding the truth that this kind of enhancement is morally wrong.

4.2.4. Cloning

To clone or copy and paste a part of the image to conceal an object or person is one of the most commonly used image manipulation techniques. When it is done with care, it becomes almost impossible to detect the clone visually and since the cloned region can be of any shape and size and can be located anywhere in the image, it is not computationally possible to make an exhaustive search of all sizes to all possible image locations.

V. CONCLUSIONS

A lot of research has been done on active as well as passive tamper detection techniques and still a lot of work is going on worldwide to successfully detect tampering in digital images. In this paper we have reviewed the two popularly used passive detection techniques, splicing and cloning. A survey of a recent study is explored including an examination of the various approaches in detecting image tampering. This area of research is relatively new and only a few sources exist that directly relate to the detection of image forgeries. Active or Passive, or blind, approaches for detecting image tampering are regarded as a new direction of research. In recent years, there has been significant work performed in this highly active area of research. These approaches do not depend on hidden data to detect image forgeries, but only utilize the statistics and/or content of the image in question to verify its genuineness.

VI. REFERENCES

[1]. S. Battiato, G. M. Farinella, E. Messina,G. Puglisi, "Robust Image Alignment for Tampering Detection, IEEE Transactions On Information Forensics And Security, Vol. 7, No. 4, August 2012.

[2]. S. Battiato, G.M. Farinella, E.Messina, And G. Puglisi, "Robust Image Registration And Tampering Localization Exploiting Bag Of Features Based Forensic Signature," In Proc. ACM Multimedia (Mm'11), 2011.

[3]. S. Xiang, H. J. Kim and J. Huang, Histogram-based image hashing scheme robust against geometric deformations, Proc. of the ACM Multimedia and Security Workshop, ACM Press, 2007, pp. 121-128.

[4]. S. S. Kozat, K. Mihcak and R. Venkatesan, Robust perceptual image hashing via matrix invariants, Proc. of IEEE Conference on Image Processing (lCIP'04), Singapore, Oct. 24-27, 2004, pp. 3443-3446.

[5]. V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

[6]. T.-Y. Lee, S.-D. Lin.: Dual Watermark for Image Tamper Detection and Recovery. In Pattern Recognition 41 pp. 3497--3506. (2008).

[7]. Henry Farid "Image forgery detection survey " , IEEE SIGNAL PROCESSING MAGAZINE, March 2009. 2] M.Ali Qureshi, M. Deriche "A review on copy move forgery detection techniques" IEEE 2014.

[8]. N.Anantharaj "Tampering and Copy move forgery detection using shift Feature, 2014.

[9]. Sahar Qasim Seleh," Tampering and Copy move Forgery Detection using shiftfeature"2012.

[10]. V. Christlen,C. Riess, J.Jordan,C.Riess, and E.Anegelopouou "An Evaluation of popular Copy Move Forgery detection approach" Dec, 2012 19] R.Achanta , A. Shaji, K. Smith, A. Lucchi, P.Fua, and S. Susstrunk,"SLICsuperpixel compared to stateof the arts superpixelmethod", 2012 20] I. Amerini, L. Ballan,R.Caldelli, A. Del Bimbo,AND g. Serra, "A State based forensic method for copy move attack detection and transformation recovery",2011.

[11]. Tong, Xiaojun, et al. "A novel chaos-based fragile watermarking for image tampering detection and self-recovery." Signal Processing: Image Communication 28.3 (2013): 301-308.

[12]. Dadkhah, Sajjad, et al. "An effective SVD-based image tampering detection and self-recovery using active watermarking." Signal Processing: Image Communication 29.10 (2014): 1197-1210.

[13]. W. Lu, A. L. Varna, and M. Wu, "Forensic hash for multimedia information," in Proc. SPIE Electronic Imaging Symp.—Media Forensics Security, 2010.

[14]. W. Lu and M.Wu, "Multimedia forensic hash based on visual words," in Proc. IEEE Computer Soc. Int. Conf. Image Processing, 2010, pp.989-992.

[15]. S. Roy and Q. Sun, "Robust hash for detecting and localizing image tampering," in Proc. IEEE Computer Soc. Int. Conf. Image Processing, 2007, pp. 117-120.

[16]. N. Khanna, A. Roca, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, "Improvements on image authentication and recovery using distributed source coding," in Proc. SPIE Conf. Media Forensics Security, 2009, vol. 7254, p. 725415.

[17]. J. Fridrich and M. Goljan, Robust hash functions for digital watermarking, IEEE Proceedings International Conference on Information Technology: Coding and Computing, pp.178-183, 2000.

[18]. F. Lefebvre, J. Czyz, and B. Macq, A robust soft hash algorithm for digital image signature, Proceedings of International Conference on Image Processing, vol. 2, pp. 14-17, September 2003: II - 495-8.

[19]. E. L. Lehmann and J. P. Romano, Testing Statistical Hypotheses, 3rd ed., New York, USA, Springer, pp. 590-599, 2005.

[20]. Bianco, S., Mazzini, D., Pau, D., Schettini, R.: Local detectors and compact descriptors for visual search: a quantitative comparison. Digital Signal Process. 44, 1-13 (2015).

[21]. Jegou, H., Perronnin, F., Douze, M., Sánchez, J., Pérez, P., Schmid, C.: Aggregating local descriptors into a compact codes. IEEE Trans. Pattern Anal. Mach. Intell. 34(9), 1704-1716 (2012).

[22]. Janan, F., Brady, M.: Shape description and matching using integral invariants on eccentricity transformed images. Int. J. Comput. Vis. 113(2), 92-112 (2015