ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

# An investigation of approaches for image forgery detection

**MandeepKaur[1], Dr.Savita Gupta[2]**

University Institute of Engineering and Technology, Panjab University, Chandigarh, India[1,2]

**Abstract**: Trustworthiness of digital images has a significant role in many areas, but the ease with which they can be manipulated and distributed has brought forth the security aspects. The easy accessibility of sophisticated photo editing tools has made the process of verifying the authenticity and integrity of digital images extremely difficult. There is an urgent need to develop novel image forgery detection techniques and also improve the high false positive rates of the existing methods. The current paper presents an overview of various approaches available in literaturefor tamper detection, along with their strengths and weaknesses. As lot of research has been carried out in the field of *active* and*passive tamper detection*, the focus of this paper is to highlight the role of fusion in the field of image tamper detection. As the research in this direction has been very limited, all methods that detect tampering on the basis of multiple cues (foot prints or tampering traces) are grouped together and are termed as *fusion based approaches*. Image tamper detection techniques can be made more reliable and robust by using fusion of multiple tamper detection tools. A critical review of available fusion is presented to expedite the development of novel image forensic techniques.

**Keywords**: passive-blind methods, image forensics, tamper detection, image forgery, intrusive techniques

## I. INTRODUCTION

Photographs have a crucial role in multiple domains, including: medical imaging, journalistic photography, surveillance systems, forensic and criminal investigation, intelligence services, insurance claims etc. Therefore there trustworthiness and reliability has got great implications. In this digital age, one major challenge is the ready availability of image processing software and editing tools because of which tampering of digital images has become much more easier without leaving any obvious traces. The ease with which the digital content can be manipulated, duplicated and distributed has brought forth the security aspects. Therefore the control over integrity and authentication of a digital image is becoming ever more important. The recommendations and guidelines provided by Scientific Working Group on Imaging Technology (SWGIT) highlight best practices for the analysis of video/images, videography, and photography [Birajdarand Mankar 2013]and thus are very helpful in law enforcement and criminal justice system.

The current image editing tools make it very difficult for naked eye to distinguish a tampered image from an authentic one. There is a need of an automatic classification system that can deal with the problem of image tampering more reliably than human inspection. Digital images can be forged or tampered in number of ways like [Mahdian and Saic 2010] : Copy-move (or copy- paste) forgery: a portion from an image is copied and pasted on another portion of the same image, generally to conceal certain portions of the image, Image splicing: it is a cut and paste operation where a region is cut from one image and pasted onto the another image, Local noise: Additive noise is the main cause of failure of many active or passive tamper detection methods. It is widely used to conceal tampering traces. This is one of, Blur and sharpening: it also commonly used as a tool for concealing the traces of tampering, compression properties: of an image can also be altered in order to affect its quality, Computer graphics and paintings: it can be used to create convincing image forgeries, thus sophisticated methods are needed to distinguish between an image generated through computer graphics and a real photographic images.

Image forgery detection technique aims to verify the authenticity and integrity of a digital image. The objective of this paper is therefore to get an insight of various approaches that are available for image tamper detection as they have great social implication. Several approaches are proposed by the research community verify integrity and detect tampering of multimedia content. Can be broadly classified into Active and Passive technologies [Birajdarand Mankar 2013; Piva 2013] .

In an active approach for tamper detection, some information which is generated at the source side like during the acquisition of a digital image using a camera; is used later to verify the integrity on an image and detect tampering. These are also called intrusive techniques as some extra information is embedded in the image to determine its authentic. In Passive approaches the assessment is made only on the basis of digital content at disposal without any extra information. But lately some practice of using multiple tamper detection tools has also emerged which is found to improve the tamper detection capability and hence improve their detection accuracy and reliability. These techniques are based on the concept of information/data fusion, thus will be termed as fusion based approach.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

A survey of tamper detection techniques in the past covers exclusively active or passive approaches. In [Fridrich 1999] data hiding techniques are discussed. Detailed survey of various Passive blind methods is done in [Birajdarand Mankar 2013; Mahdian and Saic 2010; Piva A. 2013; Sencar and Memon 2007]. The current paper attempts to draw attention towards some fusion based approaches available in literature, citing the latest work in this area with their potential strengths and weakness.

The organization of the paper is as follows: The discussion of Active and Passive approaches is given in section II and III respectively. The section IV cover the fusion based approaches. The discussion and future scope is covered in section V. Conclusion is provided in section VI.
.

## II. ACTIVE APPROACHES

The active approaches basically comprise of the data hiding approach and the digital signature approach. Active approaches were inspired by the idea of granting authenticity to the images generated by digital cameras [Friedman 1993 ; Blythe and Fridrich 2004]

In Data hiding approaches, a secondary data like authentication code is embedded into the image. Therefore these techniques are also called intrusive techniques [Mahdian B. and Saic S. 2010]and are quite popular among research community. In digital watermarking scheme, digital watermark is generated at the source side (e.g.,camera) and inserted in the image. The integrity of mark is verified at the receiving side. These digital watermarks are mostly not separable from the image in which they are embedded. For this reason the watermark also undergo similar transformation as the image. Another major drawback of this scheme is that they must be inserted by the image capturing device itself at the time of recording or later by using a specialized watermark embedding software by an authorized person. Specially equipped cameras or special hardware/ software is therefore needed to insert the authentication code inside the image before it can be distributed. Some watermarks may also degrade the image quality which is may not be acceptable in some applications like medical image diagnosis.

The digital signature approach, unique image features are extracted at the source side which are then encoded to form a digital signatures. These signatures are later used to verify the image integrity. Digital signatures suffer from similar drawbacks as the data hiding scheme.

From the implementation point of view these active approaches need specially equipped camera consisting of a watermarking or a digital signature chip and some private key hard-wired in the camera itself, using which every image captured by the image is authenticated before saving it on its memory card. These schemes were further enhanced by linking the digital image and the hardware through which it was captured enabling image source verification and forgery detection. For this a unique binding can be formed between the embedded watermark or signature and serial number of the camera. But this idea of trustworthy camera may require a standard protocol defined by the manufacturers which can a difficult. This would also constraint the application of such solutions only to very limited scenarios [Piva 2013] .

### *A. Data Hiding Approaches*

Data hiding, also called steganography, offers an interesting alternative to the problem of verifying image integrity and authentication. The embedded signal, known as watermark is inserted into the original image, audio or video. It plays an important role in copyright protection and dealing with problem of piracy of multimedia content. In images the watermark can be embedded in spatial or frequency domain. The embedding generally should be imperceptible under normal observation conditions; this is possible by taking advantage of the masking and other properties of the human visual system.

When an image is tampered, the information or the watermark also gets modified, thus enabling tamper detection. The most common measure to identify the presence of watermark is the correlation between the watermark in the original and tampered image. For the detection of tampering in digital images and its authentication, many data hiding concepts and techniques are proposed [Fridrich 1999] like fragile watermarks, semi-fragile watermarks, robust watermarks, and self-embedding.

Fragile watermarks are designed in such a way that a slight manipulation in the image can easily destroy the watermark. Thus they provide a very high probability of tamper detection. But the digital images being highly redundant in nature, their visual content is usually not modified with minor changes. Therefore such high sensitivity of watermarks may not be desirable in many applications. As compared to this, the semi-fragile watermarks are moderately robust. They are also less sensitive modification in image pixels. The image can be thus regarded as authentic even after the application of certain processing operations like JPEG compression of high quality or changing brightness or contrast. This can be achieved by setting up a threshold in those techniques [Fridrich 1999]. The watermarks that are designed so as to resist any attempt of destroying or removing the digital watermark are called Robust watermarks. One key property of such watermarks is that if a particular image feature is added or removed, which is comparable in size to the watermarking block, the watermark in that block should no longer present, implying tampering in that block. At the same time, image processing operations like gamma correction , image filtering or lossy compression will almost uniformly affect the image blocks carrying the watermark. This enables the detection of malicious image processing operations from innocent changes.

Hybrid watermarking schemes are also proposed [Deguillaume and Voloshynovskiy 2003] that are capable

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

of providing the key features of both fragile watermarks and robust watermark i.e, accuracy, precise localization and robustness. Another kind of watermarks are the Self-embedding watermarks, which can embedded the image into itself. This enables detection of tampered or cropped regions of the image and also be helpful in recovering the original image content or any missing information.

### *B. Digital Signature Approach*

The digital signature approach uses unique features extracted from the source image which is then encoded to form a signature [Tzeng and Tsai 2001; Lu and Liao 2000]. Digital signature for an image should be designed using robust image features such that it sustains content preserving manipulations like lowpass filtering and JPEG compression but can be helpful in detecting other manipulations done to forge or tamper the content. Like the method proposed in [Xue et. al. 2012], forensic signature is constructed using extracted image feature points and the statistics of feature point neighbourhood. This signature can provide evidence for analyzing the processed history of the received image at a lower computational cost, including geometric transform estimation, tampering detection and localization. This method is capable to trace the processed history of the received image and is also robust to content-preserving manipulations.

The approaches based on traditional cryptography are only useful to protect the security of digital images. But the modern cryptographic scheme, such as DES, AES, MD5, or RSA, can be useful in detecting change from the encrypted data. But these cryptographic schemes cannot help in localizing the tampered area [Lo and Hu 2014].

According to [Lo and Hu 2014] a signature- based scheme can be used to verify the image authenticity. In this scheme, a hash function is first used to generate hash of the digital image, and then the image hash is encrypted using the public key cryptosystem to get the digital signature. A trusted third party can be used to store and protect the digital signature of the image. For image authentication, comparison of the digital signature extracted from the trust third party is done with the signature generated from the image to detect the tampered areas.

## III. PASSIVE APPROACHES

Passive approaches were proposed to overcome the problems encountered in the active approaches. These approaches do not need any extra information (like watermark or digital signature) about the image and thus are termed as passive [Mahdian B. and Saic S. 2010] . The methods used in passive approach are also called 'passive-blind' methods as original image is not needed for verifying the authenticity of the image. Thus nonintrusive methods are used to distinguish authentic images from tampered ones as compared to intrusive and proactive aids such as digital signature attachment or watermark embedding. These approaches are based on the fact that the digital image has some consistent inherent patterns (statistical properties) which are acquired from the distinct phases that are part of the image history [Piva 2013], like the acquisition phase, storage and compression, post processing operations etc. Each phase leaves a unique trace on the image, which works as a digital fingerprint. These patterns/digital fingerprints are altered after tampering operations is performed on the image. It may lead to inconsistency in noise, lightening or compression parameters etc which actually act as footprint. These variations in statistical properties can be detected by applying simple image functions. The human visual system cannot detect such manipulations which are resulted from forgeries of high quality.

The technology, defined as multimedia forensics [Mahdian and Saic 2010;Farid 2009], enables image ,source identification using traces specific to camera, or determine the authenticity of an image by detecting the presence, the absence, or the incongruence of such features inherently tied to the digital content itself. The forensic methods used are also passive-blind methods as the presence of source image is not required for tamper detection. Multimedia forensics descends from the classical forensic science, which studies the use of scientific methods for gaining probative facts from physical or digital evidences.

An elaborated survey of available passive-blind techniques is available in literature, each categorizing the contemporary methods based on different criteria. [Sencar et.al 2005] categorized the techniques into three major areas based on their focus: image source identification, discrimination of synthetic images, and image forgery detection. In [Piva A. 2013] classification of the forensic techniques is done according to the position in the history of the digital image in which the relative footprint is left. Like acquisition-based fingerprints, coding-based traces, and editing-based features. Another comprehensive survey of blind methods for forgery detection and detailed design of classification group is done by Mahdian et al. [Mahdian B. and Saic S. 2010] .It classifies the passive-blind methods based on the footprint they use to detect tampering in images for example: methods that use inconsistency in noise[ Mahdian and Saic 2008], inconsistency in JPEG compression properties (like non alignment of grids, JPEG ghost, double quantization can be used as in [ Huang et. al. 2010]where a methods for detect double compression that occurs due to splicing is proposed . Most of the available passive-blind methods proposed in literature are then fit into these classification groups.

The most of existing passive methods suffer from the drawback that they can work on and identify only some specific tampering like noise inconsistency and blocking artifacts introduced due to splicing can detect them separately. But actually the tampering is performed by applying a small set of image editing and processing tools [Piva 2013] .Hence tampered image contains a set of tampering traces. Thus only a part of the available passive blind methods will reveal the presence of tampering others

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

may not. Furthermore, it may happen that the tools search for mutually exclusive traces i,e the positive answer of one algorithm inherently implies the negative answer of another. The tamper detection tool may often give uncertain if not wrong answers, since their performance is far from ideal under which they are normally tested. In most of the cases, the kind of tampering performed is not known before hand and therefore selecting a right kind tool to detect forgery is also difficult. Hence this increases uncertainty in tool outcomes which further affects the reliability of tamper detection softwares.

Thus, deciding the authenticity of a digital image on the basis of a set of forensic tool is not trivial. Thus, the final decision about the forgery can be taken on the basis of fusion of responses obtained from multiple trace detectors [Mahdian B. and Saic 2010; Piva 2013; Barni and Costanzo 2012; Kharrazi et. al. 2006 ; Fontani et. al. 2011a]

## IV. FUSION BASED APPROACHES

Information fusion has a significant role in improving the detection accuracy of a system by enhancing the authenticity, confidence and reliability of data and reducing uncertainty. It can be applied to get single output from multiple inputs which can be heterogeneous, imprecise and incomplete. Thus enhances the decision makers understanding of the data and its implications. The major advantage of performing fusion of multiple tamper detection tools is that it can work on images that subjected to multiple and diverse types of tampering. Thus different forensic tools working in collaboration will enhance detection accuracy and robustness [Barni and Costanzo 2012]. As these tools are based on physical principles and segmentation structures, synergistic fusion remain a major challenge.

There are also some other approaches available for performing fusion of image forensics tools. Decision fusion techniques like linear opinion, voting/ranking methods are also discussed in literature. Amongst the simplest are majority decision and logical disjunction. But these classic decision approaches becomes ineffective as many problems may arise with increase in the number of tools. For example, mutually exclusive response of two or more tools i.e, if one tool detects a tampering trace other(s) will not detect anything. The problem of merging tool responses is addressed in different ways in the literature. Kharrazi et al. [Kharrazi et. al. 2006] has illustrated its implementation in steganalysis in which three main approaches to merge the outputs of several tools are discussed: feature level fusion, measurement level fusion and abstract level fusion. Fusion methods proposed so far usually focus either on the first or on the second method [Barni and Costanzo 2012].

The use decision fusion to address the problem of uncertainty in image forensics has been very limited in the past [Piva 2013; Barni and Costanzo 2012; Fontani et. al. 2011a, Fontani et. al. 2011b]. According to [Barni and Costanzo 2012] most of the existing works, [Hsu and Chang 2008; Chetty and Singh 2010; Hu et. al. 2009] are based on feature fusion approach and one based on hybrid approach is reported in [Bayram et. al. 2006] but still focusing on feature fusion.
At the feature level fusion, features are extracted by each tool, and then a global classifier is trained using subset of these features. At the measurement level output of the tools, which is generally a scalar value, is taken as such and is fused. At abstract level, the tool outcome is thresholded before performing fusion..

Feature level fusion has many potential problems. The most common one is sometimes termed as the 'curse of dimensionality' which is the difficulty in handling situations involving large number of feature. Furthermore, feature selection in most cases is followed by some machine learning that by definition is effective only when a training data set can be prepared that is representative of a large part of the global population of samples. If this can be done for training single detector, creating a representative dataset of all possible image forgeries is practically unfeasible. Moreover the whole system need to be trained each time a new tool is added. These systems also exhibit lack of scalability. The abstract level, suffers from the complementary problem as lots of information is discarded when outputs are thresholded, so the discrimination power of the various tools is not fully exploited.

The problems of fusion at feature level and abstract level can be overcome by performing measurement level fusion [Barni and Costanzo 2012]. Here the task of feature selection, training, classification and decision making is delegated as responsibility of individual tool. The fusion framework will thus remain more general and extendable. This will also prevent the loss of important information regarding the tool response confidences as occurs in the case of fusion performed at abstract level. For these reasons there is a need to design alternative reliable and robust fusion techniques in the area of digital image forensics.

In [Barni and Costanzo 2012], a decision fusion framework based on the fuzzy theory is proposed. Fuzzy logic has been used in many control applications in which robustness to noise and imprecise and incomplete information is a critical requirement. The proposed framework is designed to cope with the uncertainty introduced by image forensic tools by using multiple tools to detect image forgery and merging their outcome in final decision making. The approach uses not only tool response but also tool reliability into consideration. Similarly in [Fontani et. al. 2011a ], a fusion framework based on the Dempster-Shafer's theory is proposed. It is a framework for reasoning under uncertainty that also allows the representation of ignorance. The proposed method performs fusion at measurement level. One of the key features of this framework is that the knowledge about

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

compatibility between tools and their performances is exploited before making a decision about authenticity of an image. Also new tools can be easily integrated to the framework. The fusion framework can determine if an image is tampered or not and can generate response that can be binary (y/n) as well as some soft interpretation of the same. This helps in analysis of images where decision making is difficult due to conflicting data.

A comparison of both fusion techniques [Barni and Costanzo 2012; Fontani et. al. 2011a ] with SVM and other fusion based system like binary OR is given in [Fontani et. al. 2011b], where both show comparable results and superiority over other fusion methods. These are the first proposals based on fusion of the forensic tool outcomes. Fusion approaches can be designed that take in account certain parameters like reliability and certainty of each tool which is part of the framework. More effective tools are required that can work in real applications without a strong participation of a human operator.

## V. Discussion and Future Scope

One of the important issues that comes from the digitization
of images is the fact that the digital content is very easy to modify and counterfeit by sophisticated image processing tools/softwares. Some of these modifications cannot be easily perceived by human visual abilities, which leads to disputes. For example, a tampered medical image may lead to incorrect interpretation by doctors, a falsified news photograph or counterfeit secret image may lead to an unnecessary war between two countries. Reliable image tamper detection schemes are therefore necessary and important to counter such fraudulent acts. The paper presents a brief survey of various approaches available for tamper detection in digital images. A key limitation of available tamper detection methods is the inability to distinguish malicious tampering and genuine processing operations that are performed on the image (like red-eye correction). Another challenge is to find such statistical features that are robust enough to resist the various post processing operations [Birajdar G. K. and Mankar V.H 2013].

Developing a tool that can detect all kind of traces, there different permutations combinations and different extent of manipulation is practically impossible. One solution to this problem is, to apply a set of tools and then fuse the tool outcomes. But there are many critical issues pertaining to fusion like heterogeneity of input, type of input image, tampering traces, reliability of individual tools etc which remains an open issue for research.

The fusion framework based on fuzzy logic proposed in [Barni and Costanzo 2012]suffers from the problem of exponential growth of if–then rules whenever a new tool is added to the framework. Similarly, the framework in [Fontani et. al. 2011a]which is based on DS Theory has high worst case time complexity. There is scope of improvement in these frameworks. Also in most of the cases the suspicious tampered region was known in advance. There is a need to design methods for the case where the suspicious tampered region is not known. Another limitation for researchers in this area is the lack of common image database for testing, training and evaluation of forensic methods. The existing methods show considerably high false positive rates due to the variety of image characteristics and contents when applied to real applications.

## VI. Conclusion

In this paper, we provided the various approaches for tamper detection of digital images. Along with the active and passive approach on which lot of research has been done, the paper also highlights some fusion based approaches that synergistically merge response of multiple tools and can work on multiple footprint detection schemes, thereby improving the reliability and robustness of current image tamper detection techniques. We hope it will motivate the researchers working in this area to design novel image tamper detection techniques and also improve accuracy of the existing methods.

## References

[1] Birajdar andMankar 2013. Digital image forgery detection using passive techniques: A survey, J. Digital Investigation, Elsevier, 10,3, (2013), 226-245 .
[2] Mahdian B. and Saic S. 2010. A bibliography on blind methods for identifying image forgery, J. Signal Processing: Image Communication, Elsevier, 25, 6, (2010), 389–399.
[3] Piva A. 2013.An Overview on Image Forensics, ISRN Signal Processing, Article ID 496701, (2013), 22 pages
[4] Fridrich. 1999. Methods for Tamper Detection of Digital Images, Multimedia and Security Workshop at ACM, Florida, (1999), 29-33,
[5] Sencar and Memon 2007, Overview of State-of-the-Art in Digital Image Forensics, In. Proceedings WSPC, (2007), 1-20.
[6] Friedman. 1993. Trustworthy digital camera: restoring credibility to the photographic image, IEEE Transactions on Consumer Electronics, 39,4, (1993), 905–910
[7] Blythe and Fridrich. 2004. Secure digital camera, In Proceedings of the Digital Forensic Research Workshop, (2004), 17–19.
[8] Deguillaume et al. 2003. Secure hybrid robust watermarking resistant against tampering and copy attack, J. Signal Processing, Elsevier, 83, 10, (2003),2133-2170.
[9] Tzeng and Tsai. 2001. A new technique for authentication of image/video for multimedia applications, In Proceedings of Workshop on Multimedia and Security, ACM Press, New York, USA, (2001), 23–26.
[10] Lu and Liao. 2000. Structural digital signature for image authentication: an incidental distortion resistant scheme, In Proceedings of ACM workshops on Multimedia, ACM Press, New York, USA, (2000), 115–118.
[11] Xueet. al. 2012. Image forensic signature for content authenticity analysis, J. of Visual Communication and Image Representation, 23, 5, (2012), 782-797.
[12] Lo and Hu 2014. A novel reversible image authentication scheme for digital images. J. Signal Processing, 98, (2014), 174-185.
[13] Farid. 2009. Image forgery detection. IEEE Signal Processing Magazine, 26, 2, (2009), 16–25.
[14] Mahdian and Saic. 2008. Detection of resampling supplemented with noise inconsistencies analysis for image forensics. International Conference on Computational Sciences and its Applications, IEEE Computer Society, Perugia, Italy, (2008), 546–556.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940



[15] Huang et. al. 2010. Detecting Double JPEG Compression With the Same Quantization Matrix, IEEE Transactions on Information Forensics and Security, 5, 4, (Dec. 2010), 848-856.
[16] Barni and Costanzo 2012. A fuzzy approach to deal with uncertainty in image forensics. J. Signal Processing-Image Communication, Elsevier, (2012), 1-13.
[17] Kharrazi et. al. 2006. Improving steganalysis by fusion techniques: a case study with image steganography. IEEE Transactions on Data Hiding and Multimedia Security, (2006), 123–137.
[18] Fontaniet. al. 2011a. A Dempster-Shafer framework for decision fusion in image forensics, IEEE International Workshop on Information Forensics and Security, (2011),1-6.
[19] Fontaniet. al. 2011b. Two Decision Fusion Frameworks for Image Forensics, In proceedings of the Annual GTTI Meeting, Taormina, Italy, (2011).
[20] Hsu and Chang 2008. Statistical fusion of multiple cues for image tampering detection, In proceedings of the 42nd Asilomar Conference on Signals, Systems and Computers, (2008), 1386-1390.
[21] Chetty and Singh 2010. Nonintrusive Image Tamper Detection Based on Fuzzy Fusion. International Journal of Computer Science and Network Security, 10, 9, (2010), 86-90.
[22] Hu et. al. 2009. D-S Evidence Theory Based Digital Image Trustworthiness Evaluation Model, In proceedings of the International Conference on Multimedia Information Networking and Security, 1, (2009), 85-89.
[23] Bayramet. al. 2006. Image manipulation detection. J. of Electronic Imaging, 15, 4, (2006), 1-17.