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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Digital Image Tampering – A Threat to Security Management

Deepika Sharma[1], Pawanesh Abrol[2]

Research Scholar, Department of Computer Science & IT, University of Jammu, J & K[1]

Associate Professor, Department of Computer Science & IT, University of Jammu, J & K[2]

Abstract: Modern digital technology and the availability of increasingly powerful image processing tools can easily manipulate the digital images without leaving obvious visual traces of having been tampered, so there is an urgent need to identify the authenticity of images. In the fields such as forensics, medical imaging, e-commerce, and industrial photography, authenticity and integrity of digital images is essential. In this research work, a comprehensive study has been undertaken for accessing and analyzing the threat of Digital Image tampering for security. Various methods and research issues involving the tampering detection and image authentication have been discussed and suitable recommendations for security scenario have been presented.

Keywords: tampering detection, authenticity, issues and threats, security management

I. INTRODUCTION

Digital media like digital images and documents should be authenticated against the forgery due to the availability of powerful tools in the field of editing and manipulating these media. Digital imaging has matured to become the dominant technology for creating, processing, and storing pictorial memory and evidence. Though this technology brings many advantages, it can be used as a misleading tool for hiding facts and evidences. This is because today digital images can be manipulated in such perfection that forgery cannot be detected visually. In fact, the security concern of digital content has arisen a long time ago and different techniques for validating the integrity of digital images have been developed. In the fields such as forensics, medical imaging, e-commerce, and industrial photography, authenticity and integrity of digital images is essential. In medical field physicians and researchers make diagnoses based on imaging [1]. The introduction and rapid spread of digital manipulation to still and moving images raises ethical issues of truth, deception, and digital image integrity. With professionals challenging the ethical boundaries of truth, it creates a potential loss of public trust in digital media. This motivates the need for detection tools that are transparent to tampering and can tell whether an image has been tampered just by inspecting the tampered image.

II. TYPES OF IMAGE TAMPERING TECHNIQUES

Image tampering is a digital art which needs understanding of image properties and good visual creativity. One tampers images for various reasons either to enjoy fun of digital works creating incredible photos or to produce false evidence. No matter whatever the cause of act might be, the forger should use a single or a combination series of image processing operations.

Fig. 1 Tampered Image

The various commonly used image tampering techniques are as follows.

a) Copy-move: This is the most common kind of image tampering technique used, where one needs to cover a part of the image in order to add or remove information. Textured regions are used as ideal parts for copy-move forgery. Since textured areas have similar color, dynamic range, noise variation properties to that of the image, it will

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

be unperceivable for human eye investigating for incompatibilities in image statistical properties.

Fig. 2 Copy- Move Forgery

b) Image-splicing: It is defined as a paste-up produced by sticking together photographic images. While the term photomontage was first used for referring to an art form or the act of creating composite photograph can be traced back to the time of camera invention.

c) Resize: This operation performs a geometric transformation which can be used to shrink or enlarge the size of an image or part of an image. Image reduction is performed by interpolating between pixel values in local neighborhoods.

d) Cropping: It is a technique to cut-off borders of an image or reduces the canvas on which an image is displayed. Generally this kind of operation is used to remove border information which is not very important for display.

e) Noising or Blurring: Tampering images with operations described above like image splicing, scaling, rotating can be clear to a viewer in the form of artifacts like improper edges, aliasing defects and tone variations. These obvious traces of tampering can be made imperceptible by applying small amount of noise or blur operations in the portions where the tampering defects are visible [2], [3], [4].

Some of the known image tampering techniques and tamper detection techniques are tabulated in table given below:

Table 1: Image tampering techniques and detection techniques

Image tamper technique	**Image operations/tools used**	**Tamper detection techniques**
copy-move	copy, move,	paste, selection
Exhaustive search, Block matching	(using DCT or PCA),	Autocorrelation
image-splicing	copy, resize, move,	paste, selection
Bispectral analysis, Bicoherence	analysis, Noise variation estimation,	Alpha variance estimation,
Higher order statistics	Re-sampling resize, crop, rotate,	scale, skew, stretch
Expectation and Maximization	(EM) algorithm	double JPEG compression JPEG encoding JPEG artifact estimation (frequency
Analysis	graphic rendering special effect filters Higher order wavelet statistics	digital editing (luminance,

III. IMAGE TAMPERING DETECTION ALGORITHMS

These algorithms use various techniques for tamper detection. These include Principal component Analysis (PCA), Discrete Cosine Transform (DCT), Discrete Wavelet Transforms (DWT), Singular Value Decomposition (SVD) etc. PCA frequently used statistical technique for data dimension reduction. This method divided the image in multiple principal components to analyze different desired components. PCA based algorithms are applied in the areas of Image Color Reduction and Object Orientation. However, the major drawback of PCA is its insensitivity to relative scaling of the original variables. DCT works in frequency domain. It expresses a sequence of finitely data points in terms of a sum of cosine functions oscillating at different frequencies. DCT has numerous applications as in lossy compression of audio (e.g. MP3) and images (e.g. JPEG), image compression etc. However, DCT based methods do not produce well results in case of image blurring and video frame reconstruction applications. DWT is wavelet transform for which the wavelets are discretely sampled. An approximation to DWT is used for data compression if signal is already sampled. It is an efficient approach to lossless compression. As compared to above methods, DWT has numerous drawbacks [5], [6]. Unlike PCA, DWT has high cost of computing. In contrast to DCT, DWT has certain limitations like signal blurring, ringing noise near edge regions in images or video frames, longer compression time, lower quality than JPEG at low compression rates etc.

Another method called Singular Value Decomposition (SVD) is being increasingly used for tampering detection. SVD is a very robust technique. The technique involves refactoring of given digital image in three different feature based matrices. The small set called singular values preserve the useful features of the original image. The advantages of SVD include lesser memory requirement. It has many applications in data analysis, signal processing, pattern recognition, image compression, noise reduction, image blurring, face recognition, forensics, embedding watermarking to an image [8], [9], [10].

IV. RESEARCH ISSUES

Different research issues related to digital images tampering detection are object identification, presence of noise, color or gray level, color combination, contrast, rotation, scaling, shapes, compression details, sharpness etc. In certain cases, original image is available. Comparison of the features of original with the tampered image can ascertain the extent of tampering. However, if the original image is not available, there are different methods to establish the authenticity of the given digital image. In the fields such as forensics, medical imaging, e-commerce, and industrial photography, authenticity and integrity of digital images is essential. In medical field physicians and researchers make diagnoses based on imaging. The introduction and rapid spread of

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

digital manipulation to still and moving images raises ethical issues of truth, deception, and digital image integrity. With professionals challenging the ethical boundaries of truth, it creates a potential loss of public trust in digital media. This motivates the need for detection tools that are transparent to tampering and can tell whether an image has been tampered just by inspecting the tampered image.

There are multiple techniques which can resolve these tampering issues to some extent depending on certain criteria. The methods discussed above are reliable to some extent but possess some limitations. These limitations are overcome by SVD technique. It is a robust technique and is used in many areas. SVD is also used in tampering detection of various transformations, (rotation, scaling, position etc), image compression, noise removal, embedding watermarking etc [11].

V. EFFECT OF TAMPERING IN DIFFERENT AREAS OF SOCIETY

Tampering is normally done to cover objects in an image in order to either produce false proof or to make the image more pleasant for appearance.

In the field of medicine, reports of patients are highly confidential and are always supposed to be authentic. Medical images are produced in most of the cases as proof for unhealthiness and claim of disease. Since medical images are dealing with huge amounts of money, people can get lured to tamper images for claiming medical insurance. Also medical results are generally placed as proofs or alternatives for avoiding punishments in courts. So this type of tampering with medical images disturbs the security of the common individual.

In the field of education, different tampering techniques give us false information which in turns leads to the delivery of incorrect data to the organization. Students carried out large amount of forgery with their documents for their own benefit. This disturbs the security of the management which is an urgent issue to be solved.

In the field of agriculture, tampering is also done with the different images used during the training of the farmers which results to the misguidance to the agricultural students. This type of forgery imbalance the security management which is to be solve soon.

In the field of e-commerce, most of the transactions are carried out through internet whether it is money transfer, Shopping purpose, bill payment etc. In this, Security of the customer's details is the prime focus of the government. But many unauthorized users manipulate the data which results in serious crime. This corrupted or disturbed security management leads to serious crime. So in the era of digital technology, tampering is a major threat to the technology which requires immediate attention.

VI. CONCLUSION

In this era of digital computing, the interest and necessity of representing information in visual forms has become very important. Due to considerable improvement in computing and network technologies, and the availability of better bandwidths, the past few years have seen a considerable rise in the accessibility, sophistication, and transmission of digital images using imaging technologies like digital cameras, scanners, photo-editing, and software-packages. However, this technology is also being used for manipulating digital images and creating forgeries that are difficult to distinguish from authentic photographs. Thus the problem of establishing image authenticity has become more complex with easy availability of digital images and free downloadable image editing softwares leading to diminishing trust in digital photographs.

REFERENCES

[1] P. Abrol, D. Padha, and Kusam, "Detecting Forgery in Digital Images: A Review",*Researcher, A Multidisciplinary J.JU*, pp. 170-180, vol.1, no. 1, 2008.
[2] P. Abrol, D. Padha, P. Lehana, "Application of Aura in Identification of Textural Objects"*Int. PCTE J. Computer Science*, pp. 92-98,vol.5, no. 1, 2008.
[3] L. Weiqi, Q.U Zhenhua, P. Feng, and H. Jiwu, "A survey of passive technology for digital image forensics",*J. Frontiers of Computer Science*,vol.1, no.2,pp.166-179,2007.
[4] Kusam, P. Abrol, D. Padha, "Digital Tampering Detection Techniques: A Review",in *Proc. 3rd Nat. Conf. on Computing for Nation Development INDIA Com, ICAM, New Delhi*, pp. 549-556, 2009.
[5] Iwata, M. Hori, T. Shiozaki, and A. Ogihara, "Digital watermarking method for tamper detection and recovery of JPEG images", in *Proc.Conf.Information Theory and its Applications (ISITA), International Symposium*,pp. 309 – 314, 2010.
[6] H. Amira, R. Rhouma, and S. Belghith, "An Eigen value based Watermarking scheme for tamper detection in gray level images", in *Proc. 7th Int. Multi Conference on Systems, Signals and Devices*, pp.1-5, IEEE, 2010.
[7] L. Kang, and X. Cheng, "Copy-move Forgery Detection in Digital Image",in *Proc.3rd Int. Congress on Image and Signal Processing*,pp. 1-5, IEEE, 2010.
[8] G. Gul, I. Avcibas, and F. Kurugollu, "SVD based image manipulations detection",in*Proc.17th Int. Conf. Image Processing*, pp. 1765-1768, 2010.
[9]O. N. Osmanli, "ASingular Value Decomposition Approach forRecommendations Systems, M.Sc. thesis,Dept. of Computer Engineering, Middle East Technical University, 2010.
[10] M. E.Wall, A. Rechtsteiner, and L. M. Rocha, "Singular Value Decomposition and Principal Component Analysis",*J.A Practical Approach to Microarray Data Analysis, Computer and computational division*, pp. 91-109, 2003.
[11] Y. He, T. Gan, W. Chen, and H. Wang, "Adaptive Denoising by Singular Value Decomposition", *IEEE J.Signal Processing Letters*, vol. 18, no. 4, pp 215 – 218, IEEE,2011.

BIOGRAPHIES

Deepika Sharma is the Research Scholar in the Department of Computer Science and IT, University of Jammu. She has done MCA. She has been working in the area of Digital Image Tampering detection and removal techniques. She has presented papers in different Science Conferences and journals.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Dr. Pawanesh Abrol has been working as Associate Professor in the Department of Computer Science and IT, University of Jammu. His research interest includes Image Authentication, Cloud Computing applications and Visualization Techniques. He has more than 39 research publications in different national and international Journals and proceedings.