International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Digital Image Tampering-A Threat to Security Management

Sanna Mehraj Kak[1], M. Afshar Alam[2]
[1, 2]Department of Computer Science, SEST, Jamia Hamdard University, New Delhi, India-110062

Abstract—*Present day computerized innovation and the accessibility of progressively capable image preparing tools can undoubtedly control the advanced pictures without leaving evident visual hints of having been altered, so there is a dire need to recognize the genuineness of pictures. In the fields, for example, legal sciences, medicinal imaging, online business, and modern photography, genuineness and honesty of computerized pictures is fundamental. In this exploration work, an extensive review has been embraced for breaking down the danger of digital Image tampering for security. Advanced Photo pictures are all around, on the fronts of magazines, in daily papers, in courts, and everywhere throughout the Internet. Ease with which pictures can be controlled; we should know that seeing does not generally infer accepting. Different strategies and research issues including the altering location and picture verification have been talked about and appropriate suggestions for security situation have been displayed.*

Keywords—*Cloud computing, integrity, tampering, watermarking.*

I. INTRODUCTION

Every now and then pictures have been acknowledged as proof of occasions of the delineated happenings. As a result of strength of computers in the field of education, business and other field, acknowledgment of computerized picture as approved archive has turned out to be visit. The convenience and availability of programming tools [1] and minimal effort equipment, makes it exceptionally uneasy to fashion of altering. All things considered we can't take the integrity and authenticity of images for granted [2]. This questions the quality of digital images offered as medicinal determination, as proof in courts, as daily paper things or as authoritative document in view of trouble in separating unique and changed substance. Computerized crime scene investigation field has grown altogether to battle the issue of image tampering in numerous areas like lawful administrations, medical images, criminology, insight and games [3], [4]. Considerable measure of work is done in the field of image forgery detection.

Image tampering is characterized as "including or removing critical components from a picture without leaving any hints of altering", [5]. In terms of image processing, tamper can be characterized as changing unique picture data by adjusting pixel qualities to new favoured values so that the changes are not distinguishable. This implies upgrading a picture by altering the picture keeping in mind the end goal to plainly express the data of the picture ought not be taken as altered, but rather altering to intentionally change the computerized pictures from their time of catch with an aim to change its unique data is called digital image tampering. It is additionally called as image forgery.

In early years, photography has quickly become the chosen method for making portraits and photographers learned that they can increase their profits by simply retouching their photographs thus to please the customer. Image manipulation has become more common in today's generation with all the available digital cameras and photo editing tools. Shown below are some image manipulations that took place in the history. These have been the most controversial and hence have raised many ethical questions.

Fig. 1. The left image is the splicing of two different images present in the centre and on the right.

The image in Figure 1 shows US Senator John Kerry and film actress Jane Fonda pictured as if they communicated together in an anti-Vietnam gathering. This picture was a forged image in reality and was formed by editing the two pictures from two different places and making them into one image. This photo was a fake in real. It was formed by splicing images of Kerry and Fonda from their performances at two different places in 1971 and 1972.

Fig. 2. The left image is the splicing of two different images present in the centre and on the right.

In this image, General Sherman is seen posturing with his Generals. General Francis P. Blair was pasted to the original image. The photo on the left is another image from the same scene, at which General Blair was not even present.

Sanna Mehraj Kak and M. Afshar Alam, "Digital image tampering-A threat to security management," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 3, pp. 59-62, 2017.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

II. Types of Image Tampering Techniques

There exist different sorts of tampering systems used to fake images. To search for specialized answers for identifying image tamper, scientists have discovered new systems of image tampering by sorting them somehow. They can be arranged as photography art for example copy-move, background removal, modify etc. They can be also ordered as image processing operations utilized as a part of the tampering strategy like resizing, splicing, rotation, etc. [6].

The various commonly used image tampering techniques [7] are as follows:

1. Resize: This operation plays out a geometric change which can be utilized to contract or develop the extent of a picture or some portion of a picture. Image reduction is performed by adding between pixel values in nearby neighbourhood.
2. Copy-move: It is the most prevalent and normal photograph tampering procedure as a result of ease with which it can be completed. It includes duplicating of some area in a picture and moving the same to some other region in the picture. Since the duplicated area is included in a similar picture, in this way the dynamic range and color compatibility stays perfect with rest of the picture.
3. Splicing: It involves replacement of image chunks from one or more images and putting them together on to another image. This is one of the simplest and the most common technique used for image tamper. Thus, splicing can be stated as the result of a paste-up of a number of images.
4. Cropping: It is a method to cut-off boundaries of a picture or lessens the canvas on which a picture is shown. For the most part, this sort of operation is utilized to expel boundary data which is not vital for show.
5. Morphing: It is a picture imitation where one object on a picture is transformed into another object in the other picture.

III. General Tamper Detection Approach

The general steps in tamper detection techniques are:

1. Pre-processing: The aim of pre-processing is to improve the image data that suppress undesirable distortions or improves image features necessary for further detection. The provided image is converted to grey-scale whenever applicable. Other pre-processing techniques include image resizing, dimensional reduction etc. in both key point and block based methods, pre-processing can be applied.

2. Feature Extraction: For block based method, feature vectors can be removed for each and every block whereas for key point based method, feature vectors compute only key points in an image.

3. Matching: After feature extraction, the potential copy-move pairs are recognized by searching blocks with similar features. High similarity between feature descriptors can be inferred as duplicated region.

4. Filtering: A single similarity situation is not enough to state the presence or absence of a duplicated region. Filtering systems are used to reduce the possibility of false matches. And lastly, post-processing can be done to preserve the matches that reveal a common behavior.

IV. Various Image Tamper Detection Algorithms

1. PCA (Principle Component Analysis)

Principal component analysis also called as Karhunen-Loeve or Hotelling transform belongs to linear transforms based on the statistical techniques. This strategy offers a powerful tool for data analysis and pattern recognition which is mainly used in image processing and signal processing [8] as a method for data compression, data dimension reduction or their decorrelation as well. There are multiple algorithms based on neural networks or multivariate analysis that can implement PCA on a certain data sample. PCA is a statistical practice that uses an orthogonal transformation to convert a set of observations of correlated variables into a set of observations of uncorrelated variables called principle component principle modes of variation [9]. The count of principal components is equal or less than the smaller of the number of original variables or the number of observations.

This transformation is defined in such a way that the first principle component has the major variance possible and each successive component in turn has the highest variance possible under the constriction that it is orthogonal to the preceding components. The resulting vectors are in uncorrelated orthogonal basis set. PCA is sensitive to the relative scaling of the original variables.

2. DCT (Discrete Cosine Transform)

DCT is a Fourier related transform similar to Discrete Fourier transform (DFT) but using only real numbers. The DCT's are generally related to Fourier series coefficients of a periodically and symmetrically extended sequence whereas DFTs are related to Fourier series coefficients of a periodically extended sequence. DCTs are equivalent to DFTs, almost twice the length operating on real data with even symmetry whereas in some variants, the input and output data are shifted by half a sample. The DCT helps separate the image into spectral sub-bands of differing importance. The DCT is similar to DFT as it transforms an image or a signal from spatial domain to the frequency domain [10].

The DCT denotes an image as a sum of sinusoids of fluctuating magnitudes and frequencies. The dct2 function computes 2D DCT of an image. The DCT has the property that for a typical image, most of the visually noteworthy evidence about the image is concentrated in just a few coefficients of the DCT. For this reason, DCT is mostly used in image compression applications. For example, the DCT is the centre i.e. the heart of the international standard lossy image compression algorithm known as JPEG.

3. DWT (Discrete Wavelet Transform)

The wavelet transform has acquired wide acceptance in signal processing and image compression. Wavelet transform decomposes a signal into a regular set of basic functions. These basic functions are called wavelets. They are acquired from a single prototype wavelet called mother wavelet by shifting and dilation [11]. The DWT has been introduced as a vastly efficient and flexible method for sub band decomposition of signals. The 2D-DWT is nowadays

Sanna Mehraj Kak and M. Afshar Alam, "Digital image tampering-A threat to security management," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 3, pp. 59-62, 2017.

established as a key operation in image processing. It is multi-resolution analysis and decomposes an image into wavelet coefficients and scaling functions. In DWT, signal energy focuses on to specific wavelet coefficients. This characteristic is useful for compressing images. Wavelets transform the image into a sequence of wavelets that can be stored more proficiently than pixel blocks. Wavelets have irregular edges that are able to render pictures better by eradicating the "blockiness". In DWT, a scheduled representation of the digital signal is acquired using digital filtering techniques. The signal to be analysed is passed through filters with different scales of frequencies implementation and reduction in computation time and resources becomes easy [12]. A 2D-DWT works in a straight forward way by inserting an array transposition between two 1D DWT. The rows of array are first handled with one level of decomposition. This divides the array into two vertical halves with first half storing the average coefficients and the second half storing the detail coefficients. This whole process is repeated again with columns thus resulting in sub bands within the array defined by filter output.

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution. It captures location as well as frequency information. An image comprises of pixels that are organised in 2D matrix each pixel representing the digital equivalent of image intensity. In spatial domain adjacent pixel values are highly correlated and hence redundant. In order to compress images, these redundancies existing among pixels needs to be eliminated. DWT processor transforms the spatial domain pixels into frequency domain information that are represented in numerous sub-bands, each representing different time scale and frequency points. One of the prominent features of JPEG2000 standard, providing it the resolution scalability, is the use of the 2D-DWT to convert the image samples into a more compressible form. The JPEG 2000 standard proposes a wavelet transform stage since it offers better rate or distortion (R/D) performance than the traditional DCT.

4. SIFT(Scale Invariant Feature Transform)

Scale-invariant feature transform (SIFT) is an algorithm to detect and define the local features in images. In an image, interesting points on the object can be extracted to obtain "feature description" of the object. This description, extracted from a training image, can then be used to identify the object when attempting to locate the object in a test image containing many other objects. To perform reliable recognition, it is important that the features extracted from the training image be detectable even under changes in image scale, noise and illumination. Such points usually lie on high-contrast regions of the image, such as object edges.

It is used to match the image that is based on feature key points i.e. scale and rotation invariance. The SIFT algorithm is the most frequent algorithm used for image extraction. It is used to find the key points on the image. SIFT includes the SIFT descriptor and SIFT detector. Another important characteristic of these features is that the relative positions between them in the original scene shouldn't change from one image to another. For example, if only the four corners of a door were used as features, they would work regardless of the door's position; but if points in the frame were also used, the recognition would fail if the door is opened or closed. Similarly, features located in articulated or flexible objects would typically not work if any change in their internal geometry happens between two images in the set being processed. However, in practice SIFT detects and uses a much larger number of features from the images, which reduces the contribution of the errors caused by these local variations in the average error of all feature matching errors.

SIFT keypoints of objects are first extracted from a set of reference images [13] and stored in a database. An object is recognized in a new image by individually comparing each feature from the new image to this database and finding candidate matching features based on Euclidean distance of their feature vectors. From the full set of matches, subsets of keypoints that agree on the object and its location, scale, and orientation in the new image are identified to filter out good matches. The determination of consistent clusters is performed rapidly by using an efficient hash table implementation of the generalized Hough transform. Each cluster of 3 or more features that agree on an object and its pose is then subject to further detailed model verification and subsequently outliers are discarded. Finally the probability that a particular set of features indicates the presence of an object is computed, given the accuracy of fit and number of probable false matches. Object matches that pass all these tests can be identified as correct with high confidence

Huang et al. [14] used SIFT for calculating local statistical features of an image. Best-bin-first nearest-neighbour for matching keypoints is used for the proposed algorithm. It is rotation and scale invariant but lacks in performance.

Scale Invariant Feature Transform is a digital image descriptor for image-based matching and recognition. The descriptors along with related image descriptors are mainly used for computer vision related to point matching between different views of a 3-D scene and viewbased object recognition [15]. The SIFT descriptor is invariant to translations, rotations and scaling transformations in the image domain and also robust to moderate perspective transformations and illumination variations. Thus SIFT descriptor is very useful in practice for image matching and object recognition under real-world conditions. The SIFT descriptor comprises a method for detecting interest points from a grey-level image at which statistics of local gradient directions of image intensities are accumulated to give a summarizing description of the local image structures in a local neighborhood around each interest point, with the intention that this descriptor should be used for matching corresponding interest points between different images. Later, the SIFT descriptor has also been applied at dense grids (dense SIFT) which have been shown to lead to better performance for tasks such as object categorization, texture classification, image alignment and biometrics . The SIFT descriptor has also been extended from grey-level to color images and from 2-D

Sanna Mehraj Kak and M. Afshar Alam, "Digital image tampering-A threat to security management," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 3, pp. 59-62, 2017.

spatial images to 2+1-D spatio-temporal video. A SIFT feature is a selected image region (also called keypoint) with an associated descriptor. Keypoints are extracted by the SIFT detector and their descriptors are computed by the SIFT descriptor. It is also common to use independently the SIFT detector (i.e. computing the keypoints without descriptors) or the SIFT descriptor (i.e. computing descriptors of custom keypoints). SIFT detector.

SIFT Detector: A SIFT keypoint is a circular image region with an orientation. It is described by a geometric frame of four parameters: the keypoint center coordinates x and y, its scale and its orientation. The SIFT detector uses as keypoints image structures which resemble "blobs". By searching for blobs at multiple scales and positions, the SIFT detector is invariant to translation, rotations, and rescaling of the image. The keypoint orientation is also determined from the local image appearance and is covariant to image rotations. Depending on the symmetry of the keypoint appearance, determining the orientation can be ambiguous. In this case, the SIFT detectors returns a list of up to four possible orientations, constructing up to four frames for each detected image blob.

SIFT Descriptor: A SIFT descriptor is a 3-D spatial histogram of the image gradients in characterizing the appearance of a keypoint. The gradient at each pixel is regarded as a sample of a three-dimensional elementary feature vector, formed by the pixel location and the gradient orientation. Samples are weighed by the gradient norm and accumulated in a 3-D histogram h, which (up to normalization and clamping) forms the SIFT descriptor of the region. An additional Gaussian weighting function is applied to give less importance to gradients farther away from the keypoint center. Orientations are quantized into eight bins and the spatial coordinates into four each

5. SVD (Singular Value Decomposition)

Singular Value Decomposition (SVD) is being progressively used for tamper detection. It is a robust technique. The technique includes refactoring of given digital image in three different feature based matrices. The small set called singular values preserve the valuable features of the original image. The advantages of SVD include lesser memory requirement. It has many applications in data analysis, pattern recognition, signal processing, image compression, image blurring, face recognition, forensics, embedding watermarking to an image [16].

V. CONCLUSION

Copy paste forgery is among the main challenges in digital image forensics. Over the years, tremendous work has been done. Main focus has been on copy-move and copy-paste. It is studied that block-based methods tend to work efficiently than key-point based method. The result thus proved is very effective and any tamper in the image compared to plain image is very hard to distinguish. The difference sometimes varies less than 1% making it difficult to notice change. A method for forgery detection in digital image based on SIFT is mentioned in this paper. This SIFT based technique is dependent on feature extraction using key point detection and feature description which are invariant to scaling and rotation.

REFERENCES

[1] G. Liu, J. Wang, S. Lian, and Z. Wang, "A passive image authentication scheme for detecting region-duplication forgery with rotation," *Journal of Network and Computer Applications*, vol. 34, no. 5, pp. 1557–1565, 2010.
[2] N. Sebe, Y. Liu, Y. Zhuang, T. Huang, and S.-F. Chang, "Blind passive media forensics: motivation and opportunity," Multimedia Content Analysis and Mining, Springer, Berlin/Heidelberg, pp. 57–59, 2007.
[3] B. Mahdian and S. Saic, "Blind methods for detecting image fakery," *IEEE Aerosp. Electron. Syst. Mag*., vol. 25, pp. 18–24, 2010.
[4] B. L. Shivakumar and S. S. Baboo, "Detecting copy-move forgery in digital images: a survey and analysis of current methods," *Global J. Comput. Sci. Technolgy*, vol. 10, pp. 61–65, 2010.
[5] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in Digital Forensic Research Workshop, 2003.
[6] V. A. K Raj, "Digital image tamper detection tools," University of Applied Science Germany, September 2015.
[7] D. Sharma, P. Abrol, "Digital image tampering – A threat to security management," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, issue 10, 2013.
[8] H. H. Barret, *Foundations of Image Science*, John Wiley & Sons, New Jersey, U.K., third edition, 2004.
[9] R. C. Gonzales and R. E. Woods, *Digital Image Processing*, Prentice Hall, second edition, 795 pages, 2002, ISBN 0-201-18075-8.
[10] A. Alice Blessie, J. Nalini, and S. C. Ramesh, "Image compression using wavelet transform based on the lifting scheme and its implementation," *IJCSI International Journal of Computer Science* Issues, vol. 8, issue 3, no. 1, pp. 449-453, 2011.
[11] D. Zhang, G. Lu, W. Li, L. Zhang, and N. Luo, "Three dimensional palmprint recognition using structured light imaging," *2nd IEEE International Conference on Biometrics: Theory, Applications and Systems*, BTAS 2008, pp. 1-6.
[12] Ms. Yamini S. Bute, Prof. R.W. Jasutkar, "Implementation of discrete wavelet transform processor for image compression," *International Journal of Computer Science and Network (IJCSN)*, Vol. 1, issue 3, 2012.
[13] D. G. Lowe, "Object recognition from local scale-invariant features," *Proceedings of the International Conference on Computer Vision*. 2. pp. 1150–1157, 1999.
[14] D. Sharma and P. Abrol, "Digital image tampering – A threat to security management," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, issue 10, 2013.
[15] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, vol. 60, issue 2, pp. 91–110, 2004.
[16] G. Gul, I. Avcibas, and F. Kurugollu, "SVD based image manipulations detection," in *Proc.17th Int. Conf. Image Processing*, pp. 1765-1768, 2010.