A Survey on Different Techniques of Tampering and their Detection

Bali Sharma, S. V. Pandit

Abstract **– In today's highly Information Technology era it is important to provide a high level of security to protect highly sensitive and private information. Digital images –Produced from digital cameras can be watermarked either in time domain or in frequency domain. The goal is to produce an efficient, secure and invisible watermarked image using digital watermarking by improving the quality and increasing the heftiness of watermarked image. This can be done by image or secret messages. But detection of originality of the image is done by different techniques which are described in this paper. This work present different types of attacks with different kind of tampering and detection techniques.**

Index Terms**- Digital *Watermarking, Image tampering, Image security*.**

I. INTRODUCTION

At present era peoples used to create, store and distribute data in digital multimedia format by using pen drives, memory cards, CDs/DVDs and hard drives. Multimedia is beneficial for the society in many ways. For example, easy transfer of good quality of images,

data, voice and documents has changed the traditional methods of transfer of data and communication which helps society to overcome the difficulties of fast changing digital world. However, this revolution helps

the pirates to exploit these features for their own intended purpose illegally [1].

Therefore, it is very important to have good authentication methods of digital media to ensure authentications of work and to find out tampering, especially for some cases like national security, medical safety, internet banking and transfer of military information and forensic investigations. In terms of medical use, a major concern among the clinical professionals is that the probability of being modified by attacker, thus, the demand for the authentication and originality is high [2, 3].

Image authentication can be used to ensure that the received image is the original one which is sent by the authorized source.

Nowadays it is common to tamper a medical image by using generic software to elaborate image. Medical image can be attacked by erasing or adding some disease spot on it. If that image is critical pieceof evidence in any legal case or police investigation, this form of tampering might pose a serious problem.

Image tampering is defined as "adding or removing important features from an image without leaving any obvious traces of tampering", [6]. In terms of image processing, tampering can be defined as changing original image information by modifying pixel values to new preferred values so that the changes are not perceivable. This means enhancing an image by tampering the image in order to clearly express the information content of the image should not be taken as tampering, but tampering to deliberately doctor digital images from their time of capture with an intention to change its original information is called digital image tampering. It is also called as image forgery.

Digital technology has become so much advanced that even a learner of digital image processing can create his own digital work. Advancement of technology results in unimaginable creations in digital media, but the fact that is not much realized is loss of copyright protection. Image tampering is done commercially in this 21st century as piece of art making. There exist companies using this technology to retouch images to their client's preferences.

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 commonly known as photo retouch.

Due to the demand of public entertainment and to become limelight in competence, the prime use of these tampering techniques is done in journals.

Fig. 1. Tampering Image of Taj Mahal and Taj Hotel.

From above figures it is clear that these two artistic monuments located at two different places but but due to tempering it is combine and show next to next as they are at same place.

In this paper we describe the design and implementation of a dynamic self-checking mechanism that significantly raises the level of tamper-resistance protection against an adversary with static analysis tools and knowledge of our algorithm and most details of our implementation.

II. Digital Image Watermarking Classification

Some of the important types of watermarking based on different watermarks [3] are given below:

2.1 Visible watermarks

Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the center part of the image.

2.2 Invisible watermark

Invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content and author authentication and for detecting unauthorized copier.

2.3 Fragile watermark

Fragile watermark are also known as tamper-proof watermarks. Such watermark are destroyed by data manipulation or in other words it is a watermarks designed to be destroyed by any form of copying or encoding other than a bit-for-bit digital copy. Absence of the watermark indicates that a copy has been made.

III. Watermarking Architecture

3.1 Embedding

It is also called watermark encoding. The watermark embedding algorithm embeds a watermark in the spatial and transformed domain of image. As shows a generic watermark embedding system. The input parameters for watermark encoder are original image, watermark to be embedded and the secret or public key.

The output of the embedding process is always the watermarked data/image

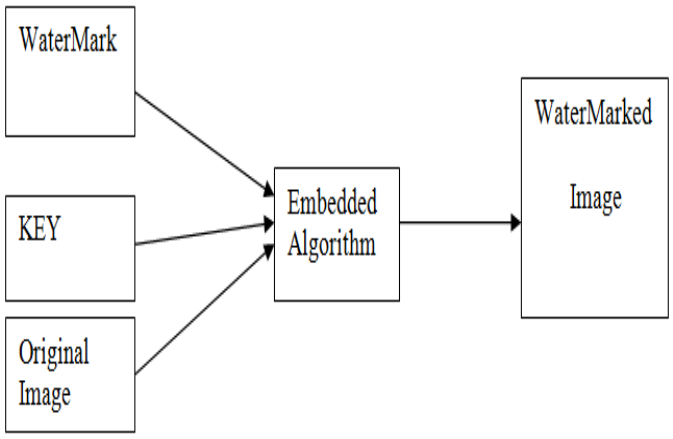

Fig. Embedding of watermark in original Image

3.2 Watermark Detection

This is also called extraction of watermark. It is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If The signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal. A generic watermark detection scheme shown needs a watermarked data and the secret key or public key.

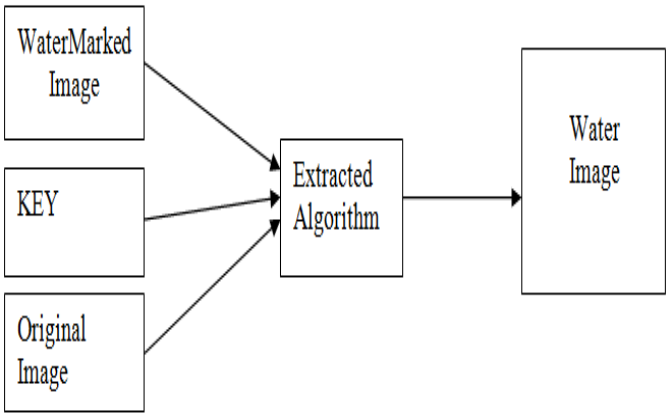

Fig. Generic Watermark Detecting Scheme

For digital color image watermarking following requirements should be satisfied –

- Elements of digital content can be directly manipulated and information can be embedded in them.
- Watermark should be perceptually invisible. Alterations introduced in the image should not reduce its perceived quality.
- Deterioration of the quality of digital content is minimized.
- Watermarks are retained and detectable after the digital content is edited, compressed, or converted. Thus Watermark should be robust as much as possible against attacks or image processing operations that preserve a desired image quality.
- Processing required for watermarking and detection should
be simple.

The Detection of the watermark should not require access to the original image data. This demand is necessary for

avoiding time consuming search in large digital image libraries

IV. WATERMARKING TECHNIQUES

There are two major techniques for watermarking

Spatial Domain – This domain focuses on modifying the pixels of one or two randomly selected subsets of images. Itdirectly loads the raw data into the image pixels.
Some of its main algorithms are:
Least Significant Bit: Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select locations of the image. But these primitive techniques are weak to attacks and the watermark can be easily destroyed. Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications.

SSM Modulation Based Technique: Spread-spectrum techniques are methods in which energy generated at one ormore discrete frequencies is deliberately spread or distributedin time. SSM based watermarking algorithms embed information by linearly combining the host image with a smallpseudo noise signal that is modulated by the embedded watermark.

*Texture mapping coding Technique:*This method is usefulin only those images which have some texture part in it. Thismethod hides the watermark in the texture part of the image.This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage) [2], and cannot be done automatically. This method hides data withinthe continuous random texture patterns of a picture.

Domain – This technique is also called transform
domain. Values of certain frequencies are altered from theiroriginal. There are several common used transform domain methods, such as Discrete cosine transforms (DCT): DCT based watermarking techniques are more robust compared to simple [1] spatial domain watermarking techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc.
Steps in DCT Block Based Watermarking Algorithm

1) Segment the image into non-overlapping blocks of 8x8

2) Apply forward DCT to each of these blocks

3) Apply some block selection criteria (e.g. HVS)

4) Apply coefficient selection criteria (e.g. highest)

5) Embed watermark by modifying the selected coefficients.

6) Apply inverse DCT transform on each block

*Discrete wavelet transforms (DWT):*Wavelet Transform isa modern technique frequently used in digital image processing, compression, watermarking etc. The transformsare based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude ofDWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL).

V. IMAGE TAMPERING TECHNIQUES

Image tampering is a digital art which needs understanding of image properties and good visual creativity. Image can be tempered for various reason either for fun or to make image attractive or to produce false evidence or to destroy evidence in legal cases or in police investigations. No matter whatever the cause might be, the forger should use a single or a combination series of image processing operations. 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 be unperceivable for human eye investigating for incompatibilities in image statistical properties.

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 [7].

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. Image zooming is achieved by interpolation. Scaling is used to change the visual appearance of an image, to alter the quantity of information stored in a scene representation for example to make an object look bigger with respect to the background image objects.

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. By enlarging the borders of the tractor, blur artifacts are clearly apparent which indicates that the forger has used blur tool to cover the edge variations due to tampering.

f) Apply luminance nonlinearities: In order to highlight parts of an image or to make a digital image more photo realistic, luminance nonlinearity technique is used. This is done by varying contrast, brightness and windows level or a pplying luminance filters like gradient glow, radial glow, etc to the objects that are wished to be highlighted.

g) Resaving: After tampering an image, saving can be done by the forger in two ways, either by saving the image using a lossy or lossless compression algorithm. If the image is saved with JPEG compression, it is possible that the image pixels are further tampered by the quantization of DCT (Discrete cosine transform) coefficients done during JPEG compression, which is normally visible as block artifact in lossy compressed JPEG images.

h) Double JPEG compression: If a JPEG image is tampered and compressed again with JPEG compression with a different quality factor, then it is likely to find periodic artifacts in the histogram of the DCT coefficients of compressed image.

VI. IMAGE TAMPERING DETECTION TECHNIQUES

Principal components analysis

Principal components analysis (PCA) is a mathematical technique to identify patterns in large sets of data like image data by transforming the data to a new coordinate system. The origin of the transformed coordinate system is the mean of the original data and the transformed axes are always orthogonal to each other. The transformed variables in the new coordinates are called principal components. The first principal component is always the greatest variance of the data set; second greatest variance is the second principal component and so on. This kind of representation highlights the similarities and differences in large data sets. One of the main advantages of identifying patterns in high dimension sets is to reduce the data by choosing only the patterns that are most important.

Principal components analysis on the acquired pixel blocks of data from the tampered image represent the data such that identical patterns or pixel blocks can be highlighted and thus by searching for matches in the new transformed data we can find parts forged by copy-move technique. The initial multidimensional image block data is obtained by copying the rows of the acquired image blocks of the image f(x,y) as mentioned in the data acquisition in to the columns of a matrix F i.e. each column in matrix F represents each acquired image block that is being investigated. To find the PCA of a multi-dimensional data, first each column of matrix F is made zero mean by subtracting each element of the column with the mean of the column. Covariance matrix C=FF of this data is calculated. as Covariance matrix gives the similarity measure between the image blocks.

Autocorrelation (AC) method for copy-move

Another technique which is mostly used for pattern recognition and for finding repetitive features is autocorrelation. Copy-move detection based on autocorrelation function is proposed in [5]. Autocorrelation function is defined as correlation of a signal or part of signal with itself. 2D correlation for an image with width Nx pixels and height Ny pixels is given as.

$$A(i,j) = \sum_{x=1}^{Nx} \sum_{y=1}^{Ny} \frac{f(x,y)\, f(x+1, y+1)}{NxNy}$$

f(x,y) is image function
(i,j) representing location of the pixel,

The idea behind using autocorrelation for copy-move image tamper detection is that, the resulting image after autocorrelation of an image and a region taken from it will consist of higher correlation values (average power or mean square) exactly in the position from where the region is derived. Thus copy-move regions give higher correlation values when auto correlated with the tampered image.

Detection algorithm for image-splicing technique

Most imaging devices introduce some form of luminance and geometric nonlinearities. If a composite image is formed by splicing two images with different image statistics, it is very likely to introduce discontinuity or un-natural correlations at the point of splicing. If this composite is made from images with different luminance or noise properties, the un-natural correlations can be found out by studying horizontally and vertically the noise and luminance characteristics of the image.

Detection techniques based on bispectral analysis are proposed in papers [4] and based on inspecting luminance nonlinearities and noise variations are proposed in [5].

If two images with different SNR are spliced together or super imposed, detection of forgery can be done by just scanning the tampered image for noise variations. Several SNR estimation techniques have been reported by various researcher s [8] and a search to identify the best estimator has been studied and reported in [9]. Since noise is often described by its variance and can be studied by computing higher order image statistics, noise variation detection based on second and fourth order moments proposed by Mr. Rolf Matzner and Ferdinand Englberger [8] has been selected for implementation in this thesis work. Detection technique based on second and fourth order moments noise estimator described in the next section has been proposed in [5] for estimating local variations of noise in an image.

Fountain Codes & Hashing Function

In [9] original image is break into blocks then by the use of the fountain code generation algorithm one can

supply sufficient amount of code in the channel so that if some of the packet get effected by the noise then the image will be effective generate with the help of the other packets which are successfully received. This is quite effective in generating the information then embedded it in the packets by the use of the hash function that specify at which part embedding need to be done. Then analytically derive formulas for the reconstruction success bounds, and validate them experimentally with Monte Carlo simulations and a reference image authentication system.

CONCLUSION

In this paper, we studied the various types of watermarking techniques on the basis of various parameters like Human Perception, Robustness etc. On the basis of human perception, we can divide the watermarking into two parts:

Visible and Non Visible Watermarking.
Then this paper focuses on the different type of tampering which is done on the images. Finally different techniques of tampering detection are shown. There are lot of improvement need to do as the image get tampered easily and detection or correction is done upto certain extents only

REFERENCES

[1] T. Narasimmalou, R. Allen Joseph, 2012 "Robustdiscrete Wavelet Transform Based Steganography" in International Journal of Power Control Signal and Computation IJPCSC Vol. 4. No.2. pp.102-108 ISSN: 0976-268X

[2] R.Kalpanasonika, S. Akila Agnes A Scrutiny on Digital Watermarking Techniques Volume 3, Issue 12, December 2013ISSN: 2277 128XInternational Journal of Advanced Research inComputer Science and Software Engineering

[3] Gaurav ChawlaRavi SainiRajkumar Yadav Classification of Watermarking Based upon Various Parameters" International Journal of Computer Applications & Information TechnologyVol. I, Issue II, September 2012(ISSN: 2278-7720).

[4] T. –T. Ng and S. –F. Chang, "A model for image-splicing", IEEE International Conference on Image Processing, pp. 1169-1172, 2004.

[5] A. C. Popescu and H. Farid, "Statistical tools for digital forensics", 6th International Workshop on Information Hiding, Toronto, Canada, 2004.

[6] J. Fridrich, D. Soukal and J. Lukas, "Detection of Copy-move forgery in digital images", in Digital Forensic Research Workshop, 2003.

[7] G. Palmer, "A Road Map for Digital Forensic Research", Technical Report DTR-T0010-01, DFRWS, 2001.

[8] D. R. Pauluzzi and C. Norman, "A Comparison of SNR Estimation Techniques for the AWGN Channel", IEEE Transactions on Communications, Vol. 48(10), pp. 1681-1691, 2000. IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 3, MARCH 2013

[9] Paweł Korus and Andrzej Dziech Efficient Method for Content Reconstruction With Self-Embedding IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 3, MARCH 2013