STM JOURNALS

Journal of Artificial Intelligence Research & Advances
ISSN: 2395-6720 (Online)
Volume 4, Issue 1
www.stmjournals.com

Survey Paper of Image Forensics based on Tampering Detection using Feature Extraction Technique

Saira Baghel[1,*], Priya Pathak[2], Sandeep Gupta[3]
[1]Department of Computer Science and Engineering, Nagaji Institute of Technology and Management, Gwalior, Madhya Pradesh, India
[2]Senior Research Analyst, Department of Computer Science and Engineering /IT, Techies Research, Gwalior, Madhya Pradesh, India
[3]Director, Department of Computer Science and Engineering/IT, Techies Research, Gwalior, Madhya Pradesh, India

Abstract

The digital images (DI) are becoming vital components in the field of statistics forensics and protection. Because of the popularity of picture enhancing tools, DI may be altered. Therefore, it is ought to create forensic strategies that are able to detect tampering in pictures. Image forensic (IF) is a vital part of many investigations. The numerous low-cost effective digital tools have enabled easy picture creation, change and distribution, which make fraudulent picture forgeries simpler than ever. In this paper, we used to feature extraction techniques.

Keywords: *Image forensic, image tampering, feature extraction techniques*

****Author for Correspondence*** E-mail: sairabaghel123@gmail.com

INTRODUCTION

Tampering with picture is not always a new difficulty. In the past, manipulations of the images generated by traditional film cameras required professional knowledge and sophisticated dark-room equipment, which is difficult to perform well for average users. With the advancement in various DI devices, DIs has become ubiquitous today. However, modifying a digital image without any obvious traces is not a difficult task now, with the sophisticated image editing software available, such as Adobe Photoshop, GIMP, and many others. In fact, many forgeries have been dispersed [1]. A famous instance may be found within the 2004 American presidential elections. An extensively circulated image showing the democratic candidate and a famous Hollywood actress sharing an illustration podium changed into, in truth, faux. A popular British newspaper was forced to apologize for publishing photographs showing British soldiers abusing an Iraqi prisoner, which were later proven to be fakes. Apparently, "seeing does no longer believe". It will get worse as counterfeiting techniques become more and more sophisticated. If the tampered pictures are abused, it can give rise to a few huge problems which potentially might also have deep ethical, ethical and medical implications. Therefore, the authentication of DIs will become a vital issue. Digital signature and watermarking have been proposed as a way to authenticate the contents of DIs. However, signature-primarily based and watermark-primarily based techniques require a few pre-processing consisting of signature era and watermark embedding when growing the picture, which could restrict their programs in practice. Thus, they are active methods. Recently, a singular technique for authenticating the contents of virtual pictures has developed fast. The era assumes that the unique picture has a few inherent styles, which might be brought through the numerous imaging devices or processing. These styles are usually consistent with the unique photograph and altered after a few tempering operations. We can recognize the basis of the DI or establish whether a picture is genuine or faux with the aid of detecting the styles.

Image Tampering

To detect image tampering (IT), we should know about IT operation itself first. In, the author divided digital forgery operation into

six exclusive categories: compositing, morphing, re-touching, improving, pc producing and portray. In fact, almost all state-of-the-art tampering detection techniques aim at compositing operation. With powerful image editing tool (e.g. Photoshop or lazy snapping), compositing tampered images (TI) is much easier and can result in much more realistic images. It continually entails the selection, transformation, composition of the picture fragments and the retouching of the final picture. Here, we need to emphasize that a TI approach, a part of the content material of an actual picture is altered. This idea does now not include the ones thoroughly synthesized photographs, e.g. Picture completely rendered by means of computer photos or by means of texture synthesis. In different phrases, a photograph is tampered implies that it ought to incorporate components: the genuine component and the tampered component. All the algorithms introduced later focus on the tampered images defined here [2].

Digital Image Forensics

Since the wild increase in usage of DIs, the crimes involving DI such as image forgery have been increased consequently, and detection of the IT brought many difficulties to forensic investigators and forensic researchers. The major detectable research topics in DI forensics are image authenticity, image correction, steganography, and image processing (IP) and source detection. Image authenticity as the most popular topic in DI forensic category concerns about the reliability of the evidence. Amerini *et al.* proposed a SIFT based algorithm to detect multiple copy-move attacks (CMA) on an image [3].

This technique extracts and matches the image features to identify a similar local region on the image and then makes a hierarchical cluster of the extracted features to recognize the duplicate areas. In case the image is classified as unauthentic, the geometrical transformation will be identified to discover the original area and the copy-moved area. Gou *et al.* introduced a source identification technique with the ability of recognizing various post-processing operations on the scanned image. Utilizing the noise analyses through wavelet analysis, neighborhood detection and image de-noising, made this approach capable of detecting the model of scanner used to scan the image and type of the image source (scanner, digital camera or computer generated). Chen *et al.* introduced a source digital camera identification technique with integrity verification capability based on photo response non-uniformity noise (PRNU) imaging sensor fingerprint. The PRNU is generated through the maximum likelihood principle derived from normalized model of the sensor output and then compare to a regenerated experimental dataset. Yuan introduced a unique approach for detection of median filtering (MF) in DIs [4]. The key points of this method were the capability of MF detection for low resolution, JPEG compressed images, and tampering detection (TD) in case a MF part is inserted in a non-MF image and vice versa. Mahdian and Saic studied the addition of locally random noise to TI regions for anti-forensic purposes and introduced a segmentation technique for dividing the DI into various partitions based on homogenous noise levels. Their novel approach utilized tiling the high pass wavelet coefficients at the highest resolution with non-overlapping blocks, to estimate the local noise level and median based method to estimate the standard noise level of the image.

TYPES OF IMAGE FORGERY

Image forging is specially categorized into three kinds; specifically image retouching, image splicing and CMA.

Image Retouching

It may be considered as a much less dangerous form of DIe forgery [5]. Retouching is not anything however making use of a few IP algorithms to beautify or to lessen fine features of an image. But it does not considerably change the photograph. This type of forging is specially utilized by magazine picture editors to make the picture more attractive, still knowing that this kind of photograph amendment is morally incorrect (Figure 1).

Fig. 1: *Example Image Retouching.*

Image Splicing (IS)
This technique is more violent than soft image retouching. IS is an image-forging technique that includes a composite/merging of two or more photographs, the pictures are blended to create a fake picture (Figure 2). Copy-paste forgery (CPF) is done via taking a place of the source picture and pasting it onto any other (target) picture, consequently generating a faux one. It may be very probable that this method introduces inconsistencies between the characteristics of the authentic and created ones. There are multiple methods to identify cut and paste forgery, some of the techniques will be discussed later in this paper.

Copy-Move Attack (Cloning)
It is an extra or much less just like IS retaining, the fact that both modify certain areas of a picture. It is a specific picture manipulation, in which a bit of the image itself is copied and inserted into a few different parts of the same image. In copy-move forgery (CMF), the object is made disappeared from the unique picture. One of the distinguishing characteristic of CMF is that it performs covering of the small block of photo replicated from any other part of the picture. The duplicated location can be manipulated with an arbitrary variety of processing equipment to seamlessly blend the forged and the unique contents. Blurring is generally carried out along the border of the changed vicinity to reduce the impact of irregularities between the original and pasted area. Since the copied segments or chunks come from the identical picture, the color palette, dynamic range, noise constituents, and the opposite features could be tuneful with the relaxation of the picture; for that reason, it is miles very tough to discover, for a human eye. Sometimes, even it makes more difficult for era to hit upon the forgery, if the image is retouched with the gear that is available (Figure 3).

Application Forensics
The forensic investigation of applications is quite advantageous as these applications usually store specific evidences. Identifying and collecting these evidences demands for prior research on the application behavior. Yasin *et al.* studied internet download manager (IDM) activities, recorded the effects on different files such as log files, Windows registry and history from artifacts point of view [6]. This study demonstrated approaches and told to detect different attributes of download requests like URL, download time and login credentials. Garfinkel (Garfinkel, 2012b) shared the experience of construction of a Korean reference data set (KRDS) based on National Software Reference Library RDS (NSRL RDS), and developed a model for both, effective importing of NSRL data sets and adding Korean specific data sets.

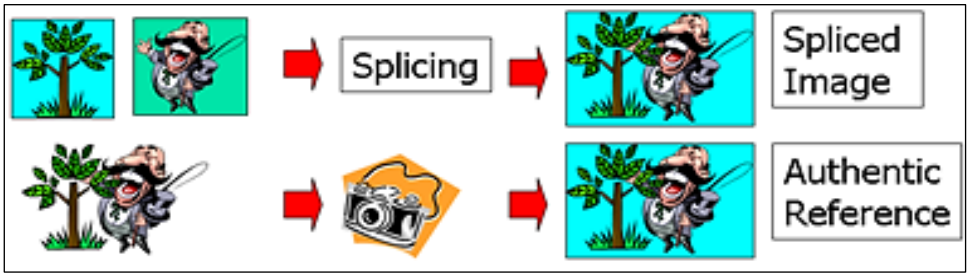

Fig. 2: *Example Image Splicing.*

Fig. 3: *Copy-Move Forgery.*

Lallie and Briggs explored three well-known peer-to-peer network clients (BitTorrent, µTorrent and Vuze) and analyzed their artifacts on Windows registry using the effects created by installation and working with these clients [7]. Damshenas *et al.* outlined the significance of web browsers in forensic investigation and proposed a methodology for evidence collection and analysis from web browsers log files [8]. Lewthwaite and Smith looked into the Limewire artifacts remained in Windows registry and other log files. They also developed a tool, AScan, to identify and recover evidences from unallocated spaces and slack spaces of hard disk drives. Fellows described the significance of recovering the WinRAR temporary files and studied the behavior of WinRAR in creating these temporary files. The results of this research indicated that there is a chance to detect and recover the evidence file from deleted temporary folders while the original file is protected by cryptographic solutions.

LITERATURE SURVEY

Sepideh *et al.* advocated a brand new automated approach for discriminating unique and TIs based totally on "JPEG ghost detection" approach that is a separation of format-founded completely IF approach [9]. The inconsistency of great factors indicates that the picture is a composite one created from at the least special cameras and therefore its miles a manipulated picture. Our classification set of rules first extracts the ghost border. Then the picture is assessed as authentic or tampered companies by thresholding a distance in characteristic area.

It became very easy today to capture and create DIs [10]. It is no longer a more expensive affair, as maximum of the handheld electronic gadgets together with cell telephones are ready with virtual cameras. Today, there are ample PC and cell apps to be had which might be evolved to govern captured pictures. One can easily take a picture, manipulate it with the installed app and make it viral through the internet. Hence, this DIs should not be interpreted as they speak. DS are the good proof of events and places. Hence, these DIs can be presented as evidence before a court of law. It turns into very critical in such cases then, to show the DIs in query to be unique. DI forensics performs a crucial function in such instances. DI forensics is a department of virtual forensics which offers with examining the DIs for their integrity and authenticity. In this paper, we present a DI forensic technique that may locate one of such IT. As snap shots can be tampered in a number of ways, in this paper, we cope with a common case known as copy-paste tampering.

Fahmy and Fahmy proposed an approach which makes use of the reality that, the copied or tampered components will no longer contain the ideal digital fingerprint of the areas it copied to [11]. The method is based on finding distinct blocks between the solid fingerprint and its corresponding mom camera fingerprint. Dissimilarity is measured through searching for blocks within the stable fingerprint photograph, having the M biggest Euclidian distance from their opposite numbers inside the mom camera fingerprint. A binary image is then built to mark the ones M likely tampered places. Morphological labeling and dilation techniques are used to take away isolated holes and superficial peaks. Cases of weakly correlated pix also are handled, through constructing a common binary image identifying tampered locations.

Paweł and Jiwu recommended to apply maximal entropy random stroll on a graph for tampering localization in DI forensics [12]. Our approach serves as an additional post-processing step after conventional sliding-window analysis with a forensic detector. Strong localization belongings of this random walk will spotlight important areas and attenuate the heritage, even for noisy reaction maps. Our assessment indicates that the proposed approach can drastically outperform both, the typically used threshold-based selection, and the recently proposed optimization-based totally approach with a Markovian prior. The intention of the paper by Thai *et al.* is to advise an accurate technique for estimating quantization steps from a picture that has been previously JPEG-compressed and saved in lossless layout [13]. Discrete cosine transform (DCT) coefficient is characterized by way of the statistical model that has been proposed in our previous works. The evaluation of quantization effect is carried

out inside a mathematical framework, which justifies the relation of nearby maxima of the wide variety of integer quantized forward coefficients with the proper quantization step. From the candidate set of the genuine quantization step given by means of the preceding analysis, the statistical model of DCT coefficients is used to provide the finest quantization step candidate.

In recent years, DIs is widely used in many applications and for multiple purposes [14]. The number of tools and software of DI editing is also increasing day-by-day which makes it easy to manipulate the actual information of an image. Therefore, it is important to ascertain the authenticity of the image under use. There are many ways in which a forger can tamper an image, out of which the most popular way is CMF. This kind of forgery is used to both conceal an item and replicate it via copying and pasting it on any other place of the same picture. The algorithm makes use of characteristic vectors extracted from the Gabor response of each overlapping block of the picture.

In the work of Hazem's paintings, a semi-fragile watermarking scheme, for grayscale picture authentication and TD, is proposed [15]. The proposed watermarking scheme is primarily based on enforcing a changed DWT quantization- based set of rules by embedding a random watermark bit collection into the DWT domain, the usage of an increased-bit multiscale quantization-based totally method with adjusted watermarked place. Here, the watermark bit is extended into three similar bits and embedded in a multistage style into the DWT low-frequency subbands of the 2d DWT ranges (LL2, LLHL1 and LLLH1). An adjustment of the quantized coefficients is supplied, based totally on enhancing their values to fall in more comfy locations in the quantization C program language period. Several designed standards were used to choose the received photo through classifying it into: authenticated, by the way or maliciously attacked with excessive accuracy in finding and categorize attacks.

In recent years, more data are created in digital form allowing easy control over storage and manipulation due to the technology progress [16]. Unfortunately, this progress may have dragged along a lot of risks, especially the ones related to the security of digital files. In unique, digital forgery turns into a fear for lots of businesses because it has end up less difficult to create fake pictures without leaving any apparent perceptual tampering of traces. A precise form of picture forgery operation called "replica-flow" is taken into consideration one of the maximum hard problems inside the case of forgery detection. For this example, part of the picture is copied and pasted on some other vicinity of the equal picture to hide unwanted items in the scene.

In the proposed method, a picture is first decomposed into three coloration additives [17]. LBP histograms are then calculated from overlapping blocks from every component. If the retained block-pairs are present in all the three color additives, they are decided on as number one applicants. 8- Connected community clustering is then applied to refine the candidates. The proposed method shows significant improvement in reducing the false positive rates over some recent related methods.

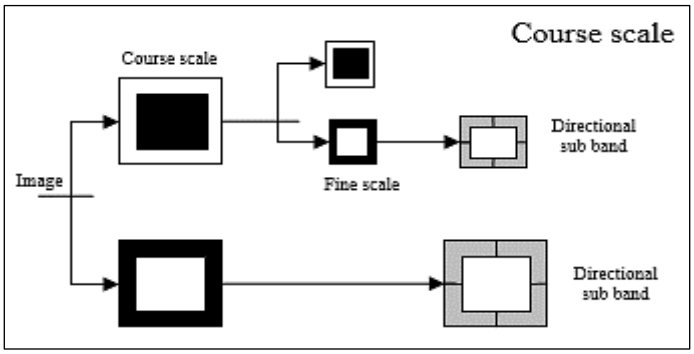

Fig. 4: *Two Level Contourlet Decomposition.*

FEATURE EXTRACTION TECHNIQUES

Countourlet Transform (CT)

It allows for exceptional and flexible number of guidelines at each scale. CT is built by joining two awesome decomposition degree (Do MN, 2004), a multi-scale decomposition followed by means of way decomposition [18]. In essence, a wavelet like remodel is used for side (points) detection, and then a neighborhood directional remodel for contour segments detection. The double filter bank combination is named PDFB as present in Figure 4.

Grey Level Co-Occurrence Matrix (GLCM)

The approach makes use of an image GLCM and it offers a simple approach to seize the spatial dating among two points in a texture pattern. It is calculated from normalized iris image applying pixels as primary data. All factors inside the GLCM are an estimation of the pixel intensities pair joint possibility in predetermined relative positions inside the photo. The (i, j) though element of the matrix, is generated by using finding the opportunity that if the pixel region (x, y) has gray stage Ii, then the pixel region (x+dx, y+dy) has a gray level intensity Ij. The specific features taken into consideration in this research are defined as follows [19]:

$$Energy = \sum_i \sum_j p(i,j)^2$$

$$Contrast = \sum_{n=0}^{N_g} n^2 \left[\sum_{i=1}^{N_g} \sum_{j=1}^{N_g} p(i,j) \|i-j\| = n \right]$$

$$correlation = \frac{\sum_i \sum_j (ij) p(i,j) - \mu_x \mu_y}{\sigma_x \sigma_y}$$

$$Homogeneity = \sum_i \sum_j \frac{1}{1 = (i-j)^2} p(i,j)$$

$$Autocrrelation = \sum_i \sum_j (ij) p(i,j)$$

$$Dissimilarity = \sum_i \sum_j |ij| . p(i,j)$$

$$Inertia = \sum_i \sum_j (i-j)^2 . p(i,j)$$

Here $\mu_r, \mu_v, \sigma_r, \sigma_v$are mean and standard deviation along X and Y axis.

Gabor Filter (GF)

A GF is created for the duration of modulating a cosine/sine wave with a Gaussian. Sine wave modulation with Gaussian affords localization in area, even though with loss of localization in frequency. An actual element is identified through a cosine modulated with Gaussian and an imaginary part is defined through a sine moderated with a Gaussian. The imaginary and real filters are also called as the even and odd symmetric components respectively. The filter centre frequency is identified through sine/cosine wave frequency. The filter bandwidth is specified by the Gaussian width. A 2D GF over an image domain is represented as [20]:

$$G(x,y) = e^{-\pi\left[\frac{(x-x_0)^2}{\alpha^2} + \frac{(y-y_0)^2}{\beta^2}\right]} e^{-2\pi i[u_0(x-x_0)+v_0(y-y_0)]}$$

Where, (x_0, y_0) specify position in the image (α, β) specify the effective and length and (u_0, v_0) specicy modution

Haar Encoding (Wavelet Method)

It extensively utilized the wavelet transform (WT) to extract functions from the iris region [21]. Both Haar wavelet and Gabor transforms are considered as the mother wavelets. From multi-dimensional filtering, a feature vector with 87 dimensions is computed. Since each dimension has real value ranging from –1.0 to +1.0, characteristic vector is sign quantized so that any high quality cost is represented through 1 and poor cost is represented by means of fee zero. It compared the Gabor transform and HaarWT use, and present that HaarWT recognition rate was slightly better than Gabor transform (i.e. by 0.9%).

Histogram of Orientation (HOG)

In this phase, HOG, is used for shape feature extraction by using intensity gradients distribution or edge directions. This method consists of three steps: (i) the thickened signature line image is divided into small connected regions called cells; (ii) each cell is computed the HOG coefficients; and (iii) the HOG features are constructed by concatenating all HOG coefficients. These features can be improved by normalization technique. This technique is employed to standardize HOG coefficients of each cell with

its nearest neighbor, which has four histograms to form one block feature [22].

Pyramid Histogram of Orientation (PHOG)
PHOG was firstly proposed by Bosch *et al.* and has been effectively used to object classification in present years. Because the PHOG method results in a much lower number of features compared with GF, the procedure of feature selection by the AdaBoost method is not required. This descriptor is generally inspired by two different sources: (1) the use of the pyramid representation, and (2) the HOG. The distance among two PHOG picture descriptors then reflects the extent to which the images include comparable shapes and correspond of their spatial layout [23].

Discrete Wavelet Transform (DWT)
The DWT based on coding of sub-band, is created to yield a wavelet transform fast computation (Figure 5). It is easy to put in force and decreases the computation time and assets want. The 2-D DWT of size N1xN2 of photograph characteristic s(n1, n2) can be expressed as [24]:

$$W_{\varphi}(j_0, k_1, k_2) = \frac{1}{\sqrt{N_1 N_2}} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} s(n_1, n_2) \varphi_{j_0,k_1,k_2}(n_1, n_1)$$

$$W\ (j_0, k_1, k_2) = \frac{1}{\sqrt{N_1 N_2}} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} s(n_1, n_2) \Psi^{i}{}_{j_0,k_1,k_2}(n_1, n_1)$$

Where i={H, V, D} point to the wavelet purpose track index. As in 1-D case.j_0Shows shows any starting scale, which may be treated as j_0=0. Above two different equations are 2-D DWT.

The DWT compared to other transforms is characteristics of frequency or time used in various application fields. The DWT sub band flow chart for DI is presented in Figure 5, where L represents to component of low frequency, H represents too high frequency and the number 1 and 2 represent the decomposition level of the DWT. The sub image LL is element of low frequency, it is the approximate usual image sub image; sub image HL is the component of low frequency in horizontal course and the high in vertical route, it manifests the long-established picture horizontal aspect. LH sub image is the factor of high frequency in horizontal course and in the vertical direction, it manifests the original image vertical edge; sub image HH is the component of high frequency, it manifests the original image oblique edge. It is present that original image energy is contained in the LL2 low frequency region.

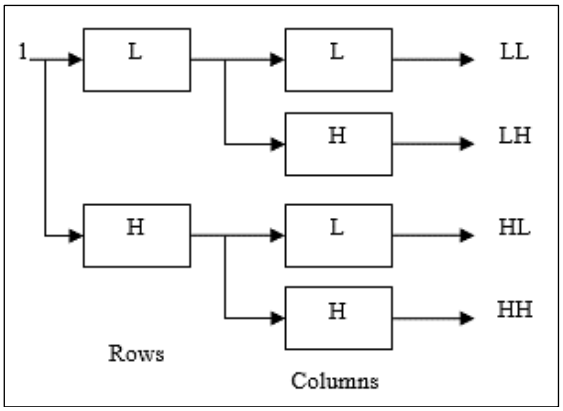

Fig. 5: *Discrete Wavelet Sub-Band Decomposition.*

Patch-Based Features
The different popular characteristic type is the patch based feature kind, which makes use of look as cues. This feature has been in use since more than two decades, and edge-based features are relatively new in comparison to it. Moravec searched for neighborhood maxima of minimum depth gradients, which he known as corners and selected a patch around those corners. His work was improved by Harris, who made the new detector less sensitive to noise, edges, and anisotropic nature of the corners proposed.

In this feature kind, there are two principal variations:

1) Patches of square shapes that contain the feature obstacles describing the features of the gadgets. Usually, these capabilities are known as the local functions.
2) Irregular patches wherein, every patch is homogeneous in terms of depth or texture and the exchange in those functions are characterized via the boundary of the patches. These features are commonly called the region-based features. [25]

Classifiers

Artificial Neural Network

The ANNs are layers of neurons, each computing an activation characteristic according to weights connected to the hyperlinks amongst neurons. The ANN architecture includes an own family of features (the activation functions), and the community schooling lets in selecting one such decision function. In precise, this circle of relatives is defined via the complexity of the neural network: number of hidden layers, quantity of neurons in these layers, and topology of the people. Optimal weights usually minimize a blunders characteristic for the particular network architecture [26].

Support Vector Machine (SVM)

First, the sample data vectors are projected onto a completely high-dimensional area. The dimension of this space is significantly larger than the original data space. Second, the set of rules reveals a hyper plane on this new space with the most important margin (linearly) setting apart training of facts. Classification accuracy normally calls for a sufficiently high dimensional goal area. This scalar product may be defined by using introducing a kernel feature (x.X')=K(x, x'), where x and x'are a pair of vectors in the low-dimensional area for which the kernel characteristic K corresponds to a scalar product in a high dimensional space.

PROBLEM STATEMENT

In today's state of affairs, due to advancement of computers and the supply of low-value hardware and software program tools its miles very handy to operate the DI without leaving the visible strains of manipulation. It has emerged as difficult to trace those manipulations. How much can we trust DI? The distinction among real and manipulated pictures has emerged as harder to differentiate, and may simplest be detected by using digital forensic specialists.

The IFs capstone assignment goals to create an online software program provider that plays the paintings of forensic analysts, and visualizes and analyzes the feasible manipulations that could had been carried out on an image. Our purpose is to empower absolutely everyone to perform IF evaluation, and help boom our religion in digital content.

RESEARCH METHODOLOGY

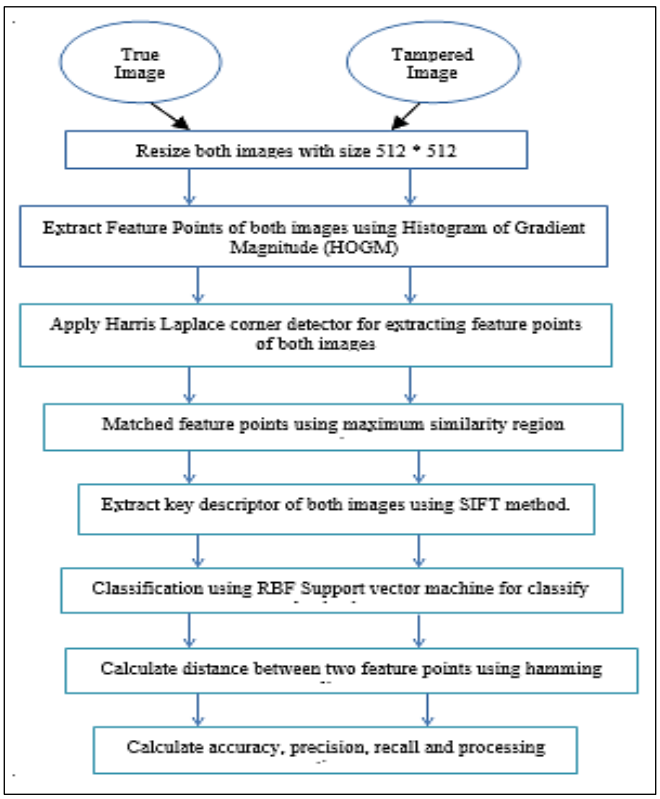

Fig. 6: *Flow Chart of Research Methodology.*

Scope of the Study

The trustworthiness of pictures has an essential function in lots of regions, inclusive of: forensic research, criminal investigation, surveillance structures, intelligence offerings, clinical imaging, and journalism. The artwork of making image fakery has a long records. But, in these days of virtual age, it is viable to very without problems trade the information represented by way of a picture without leaving any obvious strains of tampering. Despite this, no system but exists which accomplishes correctly and as it should be the IT detection challenge.

Objective

The aims and objectives of this research are as follows:

1. Propose and analyze TD techniques based on feature extraction using histogram of gradient magnitude (HOGM).
2. Propose and analyze tamper corner detection techniques (Scale-Invariant Feature Transform (SIFT), Shi-Tomasi, and Harris detectors).
3. Propose and analyze distance techniques such as hamming distance for tampering localization.
4. Incorporate a SVM for tampering localization.
5. Propose and analyze an adaptive algorithm for detecting cloning in regions with different textures.

CONCLUSION

Image forensic is a growing research area that has received great benefits from the research community over the past era. An introduction about the IT has been presented and the existing researches are ordered according to the techniques implemented. This review overlay the way to the potential researchers to know about the various techniques available for IT. We have discussed various types of attacks that can be launched against an IT system. We have mainly highlighted strategies that may be used to elicit the contents of a CMF template thereby compromising the facts. The embedded information will be used as the 'second authentication item to verify whether the image template in the database is genuine or already has been tampered. We will also improve accuracy, precision and recall of our system, and detect tampered area for enhancing security of image.

REFERENCES

1. LUO Weiqi, QU Zhenhua, PAN Feng, *et al.* A Survey of Passive Technology for Digital Image Forensics. © Higher Education Press and Springer-Verlag 2007.
2. Wei Wang, Jing Dong, Tieniu Tan. A Survey of Passive Image Tampering Detection. Springer.
3. Amerini I, Ballan L, Caldelli R, *et al.* A SIFT-Based Forensic Method for Copy-Move Attack Detection and Transformation Recovery. *IEEE Trans Inf Forensic Secur*. 2011; 6(3): 1099–1110p.
4. Yuan HD. Blind Forensics of Median Filtering in Digital Images. *IEEE Trans Inf Forensic Secur*. 2011; 6(4): 1335–1345p.
5. Burvin PS, Esther JM. Analysis of Digital Image Splicing Detection. *IOSR Journal of Computer Engineer (IOSR-JCE)*. 2014; 16(2): 10–13p.
6. Yasin M, Cheema AR, Kausar F. Analysis of Internet Download Manager for Collection of Digital Forensic Artefacts. *Digital Investigation*. 2010; 7(1–2): 90–94p.
7. Lallie HS, Briggs PJ. Windows 7 Registry Forensic Evidence Created by Three Popular BitTorrent Clients. *Digital Investigation*. 2011; 7(3–4): 127–134p.
8. Mohsen Damshenas, Ali Dehghantanha, Ramlan Mahmoud. A Survey on Digital Forensics Trends. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*. 2014.
9. Sepideh Azarian-Pour, Massoud Babaie-Zadeh, Amir Reza Sadri. An Automatic JPEG Ghost Detection Approach for Digital Image Forensics. 978-1-4673-8789-7/16/$31.00 _c 2016 IEEE.
10. Anil Dada Warbhe, Dharaskar Rajiv V, Thakare Vilas M. Digital Image Forensics. *An Affine Transform Robust Copy-Paste Tampering Detection. IEEE*. 2016.
11. Fahmy MF, Fahmy OM. A New Morphological Based Forgery Detection Scheme. 978-1-4673-9652-3/16/$31.00 ©2016 IEEE.

12. Paweł Korus, Jiwu Huang. Image Forensics based on Maximal Entropy Random Walk. IEEE. 2015.
13. Thanh Hai Thai, R´emi Cogranne, Florent Retraint, *et al.* JPEG Quantization Step Estimation and Its Applications to Digital Image Forensics. IEEE. 2016.
14. Raichel Philip Yohannan, Manju Manuel. Detection of Copy-Move Forgery Based on Gabor Filter. 978-1-4673-9916-6/16/$31.00 ©2016 IEEE.
15. Hazem Munawer Al-Otum. Semi-Fragile Watermarking for Grayscale Image Authentication and Tamper Detection Based on an Adjusted Expanded-Bit Multiscale Quantization-Based Technique. ELSEVIER. 2014.
16. Takwa Chihaoui, Sami Bourouis, Kamel Hamrouni. Copy-Move Image Forgery Detection Based on SIFT Descriptors and SVD-Matching. 978-1-4799-4888-8/14/$31.00 ©2014 IEEE.
17. Motasem AlSawadi, Ghulam Muhammad, Muhammad Hussain, *et al.* Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering. 978-1-4799-2578-0/13 $31.00 © 2013 IEEE.
18. Christophe Ambroise, Fouad Badrean, Sylvie Thira, *et al.* Hierarchical Clustering of SOM for Cloud Classification. *Neuro Computing*. Jan 2000; 30: 47–52p.
19. Amir Azizi, Hamid Reza Pourreza. A Novel Method for Iris Feature Extraction Based on Contourlet Transform and Cooccurrence Matrix. *IADIS International Conference Intelligent Systems and Agents*. 2009; 53–60p.
20. Adegoke B, Omidiora E, Ojo JA. *et al.* Iris Feature Extraction: A Survey. *IISTE*. 2013; 4(9): 7–13p.
21. Li Ma TT, Yunhong W, Dexin Z. Efficient Iris Recognition by Charactering Key Local Variation. *IEEE Trans Image Process*. 2004; 13(6): 739–750p.
22. Dalal N, Triggs B. Histograms of Oriented Gradients for Human Detection. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. 2005; 1: 886–893p.
23. Anna Bosch, Andrew Zisserman, Xavier Munoz. Representing Shape with a Spatial Pyramid Kernel. *CIVR'07*. Jul 9–11, 2007; 401–408p.
24. Mohankumar C, Madhavan J. Content Based Image Retrieval Using 2-D Discrete Wavelet with Texture Feature with Different Classifiers. *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*. Ver. IV. Mar–Apr 2014; 9(2): 01–07p.
25. Prasad Dilip K. Survey of the Problem of Object Detection in Real Images. *IJIP*. 2012; 6(6): 441–466p.
26. Maria De Marsico, Alfredo Petrosino, Stefano Ricciardi. Iris Recognition through Machine Learning Techniques: a Survey. 10.1016/j.patrec.2016.02.001,2015 Elsevier.

Cite this Article

Saira Baghel, Priya Pathak, Sandeep Gupta. Survey Paper of Image Forensics Based on Tampering Detection Using Feature Extraction Technique. *Journal of Artificial Intelligence Research & Advances*. 2017; 4(1): 33–42p.