ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

AN EFFICIENT IMPLEMENTATION OF COPY MOVE FORGERY DETECTION ON DIGITAL IMAGES

Vijayaraghavan
Professor
Dept. of Computer Science and Engineering
Shridevi Institute of Engineering and technology
India

ABSTRACT

Copy-move forgery is a specific type of image tampering where a part of the image is copied and pasted on another part generally to conceal unwanted portions of the image. Hence, the goal in detection of copy-move forgeries is to detect image areas that are same or extremely similar. In this paper, we have analyzed review assorted methods proposed to achieve this goal. These methods in general use block-matching procedures, which initially divide the image into overlapping blocks and extract features from each block, assuming similar blocks will yield similar features. Later, a matching step takes place where the aim is to investigate the duplicated blocks based on their feature vectors. A forgery detection decision is made only if similar features are detected within the same distance of features associated to connected blocks. We examine several different block-based features proposed for this purpose in relation to their time complexity and robustness to common processing scaling up/down, compression, and rotation. We have implemented the novel algorithmic approach for testing and case generations for bmp images.

Keywords – Digital Image Processing, Copy Move Forgery Detection

INTRODUCTION

Digital images play a vital role in many fields such as medical, journalism, scientific publication, digital forensics etc. In medical field physicians and researchers make diagnoses based on imaging which is crucial as one is dealing with human life. Digital images are the foremost source of information when we used them as an evidence for any event in the court

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

of law. Digital images are being used in many more applications ranging from military to medical diagnosis and from art to user photography. Now-a-days, digital crime is growing at a faster rate that even surpasses defensive measures. Sometimes a digital media content may be found to be incontrovertible evidence of a crime or of a malevolent action. So, Authenticity of digital images is a major concern now-a-days. Due to the advancement in the availability of powerful digital image processing programs such as Adobe Photoshop, Corel Draw etc, makes it relatively easy to create digital forgeries from same or multiple images. An image can be manipulated easily by means of various available image processing tools. Manipulations of digital images are done with the aim of hiding some meaningful or important information, to create misleading images or to make forged images.

1.1 FORGERY

Forgery may be defined as any modification, alteration or "enhancement" of the image after the image left the camera made with any software, including RAW conversion tools to constitute an altered image But is every altered image a forged one? What if the only things done to the image were standard and widely accepted techniques such as cropping, rotating or applying horizon correction? These and some other techniques do alter the image, but don't necessarily forge it. A forgery is essentially concerned with a produced or altered object. Where the prime concern of a forgery is less focused on the object itself – what it is worth or what it "proves" – than on a tacit statement of criticism that is revealed by the reactions the object provokes in others. Therefore, the whole point of forgery analysis is determining whether any changes were made to alter meaningful content of the image.

DIGITAL IMAGE TAMPERING

Image tampering is defined as adding or removing important features from an image without leaving any obvious traces of tampering. 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.

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

Digital technology has become so much advanced that even a novice of digital image processing is able to create his own digital works. Availability of technology gave power of doing 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 withstand competence, the prime use of these tampering techniques is done in journals. 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. There exist various kinds of tampering techniques used to counterfeit images. Categorization of these tampering techniques to my knowledge has never been published so far. Searching for technical solutions to detect image tampering, researchers have recently started to find new techniques of image tampering by categorizing them in some way. They can be categorized in terms of photography art for example copy-move, background removal, retouch etc.

They can be also categorized in terms of the image processing operations use in the tampering technique like resizing, splicing, rotation etc .The various commonly used image tampering techniques are as follows.

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.

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

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.

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.

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.

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.

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 applying luminance filters like gradient glow, radial glow, etc to the objects that are wished to be highlighted.

Resaving:

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

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.

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.

Graphic rendering:

Computer based graphic rendering software are being used to tamper natural images to make them look superficial.

Figure 1 gives an example, in which it is difficult to identify forensics/manipulated image Figure 2 from original one and in another figure 4, it is cumbersome to find out forged traces from original image as shown in figure 3.

Fig 1: Forged Image

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

Fig 2 : Original Image

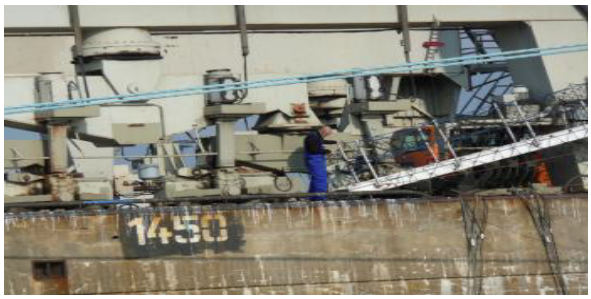


Fig 3: Original Image

Fig 4: Forged Image

1.2 TRADITIONAL WAY TO DETECT FORGERY

To detect the work of a skilled forger, investigators must rely on other methods.

Technique of examination

Thorough examination of the piece is enough to determine authenticity. A sculpture may have been created obviously with modern methods and tools. Some forgers have used artistic methods inconsistent with those of the original artists, such as incorrect characteristic brushwork, perspective, preferred themes or techniques, or have used colors that were not available during the artist's lifetime to create the painting. Some forgers have dipped pieces in chemicals to "age" them and some have even tried to imitate worm marks by drilling holes

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

into objects. While attempting to authenticate artwork, experts will also determine the piece's provenance. If the item has no paper trail, it is more likely to be a forgery.

Other techniques which might indicate that a painting is not authentic include:

- Frames, either new or old, that have been altered in order to make forged paintings look more genuine.
- To hide inconsistencies or manipulations, forgers will sometimes glue paper, either new or old, to a painting's back, or cut a forged painting from its original size.
- Recently added labels or artist listings, onto unsigned works of art, unless these labels are as old as the art itself, suspicion should be aroused.
- While art restorers legitimately use new stretcher bars when the old bars have worn, new stretcher bars on old canvases might be an indication that a forger is attempting to alter the painting's identity.
- Old nail holes or mounting marks on the back of a piece, might indicate that a painting has been removed from its frame, doctored and then replaced into either its original frame or different frame.
- Signatures, on paintings or graphics, that look inconsistent with the art itself (either fresher, bolder, etc.)
- Unsigned work that a dealer has "heard" is by a particular artist.
- Magnetic signatures used in the ink of bank notes are becoming popular for authentication of artworks.
- If examination of a piece fails to reveal whether it is authentic or forged, investigators may
- attempt to authenticate the object using some, or all, of the forensic methods below:
- Carbon dating is used to measure the age of an object up to 10,000 years old.
- "White Lead" Dating is used to pinpoint the age of an object up to 1,600 years old.
- Conventional X-ray can be used to detect earlier work present under the surface of a painting Sometimes artists will legitimately re-use their own canvasses, but if the painting on top is supposed to be from the 17th century, but the one underneath shows people in 19th century dress, the scientist will assume the top painting is not authentic. Also x-rays can be used to view inside an object to determine if the object has been altered or repaired. X-ray diffraction is used to analyze the components that make up

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

the paint an artist used, and to detect pentimenti. X-ray fluorescence (bathing the object with radiation causes it to emit X-rays) can reveal if the metals in a metal sculpture or if the composition of pigments is too pure, or newer than their supposed age. Or reveal the artist's (or forger's) fingerprints.

- Ultraviolet fluorescence and infrared analysis are used to detect repairs or earlier painting present on canvasses.
- Atomic Absorption Spectrophotometry (AAS) and Inductively Coupled Plasma Mass Spectrometry (ICP-MS) are used to detect anomalies in paintings and materials. If an element is present that the investigators know was not used historically in objects of this type, then the object is not authentic.
- Dendrochronology is used to date a wooden object by counting the number of tree rings present in the object. This is of limited use, though, as to date the piece accurately the wood needs to have about 100 rings.
- Stable isotope analysis can be used to determine where the marble used in a sculpture was quarried.
- Thermo luminescence (TL) is used to date pottery. TL is the light produced by heat, older pottery produces more TL when heated than a newer piece.
- A feature of genuine paintings sometimes used to detect forgery is craquelure.

1.3 APPROACHES TO DETECT FORGERY

To determine whether the digital image is authentic or not is a key purpose of image forensics. There are several different types of tampering attacks but the most common and the immediate one is the copy move forgery. Copy move forgery involves concealing or duplicating one region in an image by pasting certain portions of the same image on it.

Digital image forensics has two principal approaches to detect forgery as shown in Fig 1; first one is active approach which includes watermarking and stenography. These are implemented at the time of image acquisition. Active approach requires a special hardware implementation to mark the authenticity of the digital image, like embedding the digital signature in the image or encrypting the image. The water marking consist of hiding certain information in an image at the time of image acquisition and to check the authenticity of the image, embedded

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

information is extracted from the image and verified with the original watermarks. Hence, this method relies on the source information before hand. Second one is passive approach which does not require any prior information about the image and only depends on traces left on the image by different processing steps during image manipulation. There are two methods of passive approach. First one is image source identification, which identifies the device used for the acquisition of the digital image.

It tells that the image is computer generated or digital camera image. In this method the location of forgery in image cannot be determined.

Second one is tampering detection; it detects the intentional manipulation of images. Image manipulation is denoted as tampering when it aims at modifying the content of the visual message. There are various techniques to manipulate digital image by copy-move forgery, image composition and tampering image features.

Copy-Move image forgery is the widely used technique to edit the digital image. Copy-move simply requires the pasting of image blocks in same image and hiding important information or object from the image. Thus this changes the originality of the image and puts at stake the authenticity of that image. As the copied blocks are from same image they have same properties as the other blocks of image and therefore makes it very difficult to detect forgery. The copied content of image which is used to perform forgery is called snippet.

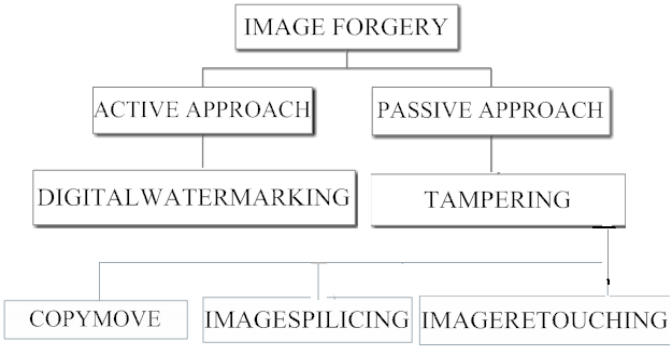


Fig 5: Principal Approaches to Detect Forgery

Active approach:

The active approaches are mainly based on digital watermarking and signature. Watermarking can be performed either in spatial or frequency domain. In spatial

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

domain, watermark is directly embedded into the pixel such as LSB (Least Significant Bit).

The problem with this method is easy detection of watermarked data. Frequency domain enhances better data security when compared to spatial domain due to its complex calculations. So, this technique involves conversion of image from spatial to frequency domain by use of transform such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT) etc. Then the watermark symbol is embedded into the frequency domain coefficients Figure 6 represents the general process of embedding watermarking technology in an image. . Water marking techniques are classified further based on robustness, fragile and semi fragile referred in [3].

Robust watermarking:
Watermark stands with the image even after processing such as translation, rotation, scaling and compression are applied to the image. This method is used to protect the copy right of digital media.

Fragile watermarking:
The slight change or modification on the image may lead to invalid image. By this, authenticity of image can be verified.

Semi fragile watermarking:
It is intermediate between first and second method. It can distinguish between malicious (modification, cropping etc.) and non malicious attacks (compression, smoothening etc.)

Passive Approach
The passive approach does not rely on pre-registration/pre embedded information but uses the image processing techniques for authenticity detection. Passive approach which does not require any prior information about the image and only depends on traces left on the image by different processing steps during image manipulation.

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

There are two methods of passive approach. First one is image source identification, which identifies the device used for the acquisition of the digital image. It tells that the image is computer generated or digital camera image. In this method the location of forgery in image cannot be determined. Second one is tampering detection; it detects the intentional manipulation of images. Image manipulation is denoted as tampering when it aims at modifying the content of the visual message. There are various techniques to manipulate digital image by copy-move forgery, image composition and tampering image features. Copy-Move image forgery is the widely used technique to edit the digital image. Copy-move simply requires the pasting of image blocks in same image and hiding important information or object from the image. Thus this changes the originality of the image and puts at stake the authenticity of that image. As the copied blocks are from same image they have same properties as the other blocks of image and therefore makes it very difficult to detect forgery. The copied content of image which is used to perform forgery is called snippet.

Copy-move:

In a Copy-Move forgery, a part of the image itself is copied and pasted into another part of the same image. This is usually performed with the intention to make an object "disappear" from the image by covering it with a segment copied from another part of the image. Textured areas, such as grass, foliage, gravel, or fabric with irregular patterns, are ideal for this purpose because the copied areas will likely blend with the background and the human eye cannot easily discern any suspicious artifacts. Because the copied parts come from the same image, its noise component, color palette, dynamic range, and most other important properties will be compatible with the rest of the image and thus will not be detectable using methods that look for incompatibilities in statistical measures in different parts of the image. To make the forgery even harder to detect, one can use the feathered crop or the retouch tool to further mask any traces of the copied-and-moved segments. 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.

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

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.

1.5 DETECTION OF COPY-MOVE FORGERY

A copy-move forgery introduces a correlation among the original image area and the pasted content. It is often necessary to perform post-processing of snippet of the image before pasting to create a convincing forgery. An efficient forgery detection method needed to be robust to post-processing operations, such as scaling, rotations, JPEG compression and Gaussian Noise addition.

In our work we are using the combination of both block-based and key point-based technique for feature extraction . By employing this strategy we are able to detect those forgeries which may be missed by using previous techniques.

IMPLEMENTATION SCENARIO AND WORK DONE

- Combining block based method(DCT) and feature based method(SIFT) in order to improve the efficiency to detect the forgery
- Implementation of the algorithmic approach on BMP Images.
- Comparative Analysis with JPEG noisy results
- Performance analysis of BMP copy move forgery
- Performance analysis of proposed algorithm to determine the accuracy rate.
- Comparing proposed algorithm with PCA, DCT, SIFT

PROPOSED ALGORITHM (HYBRID APPROACH MAKING COMBINATIONS OR OPTIONS FROM THE CLASSICAL APPROACHES)

1. Divide the tampered image into overlapping blocks of 16x16 pixels. Block shift can be 2,4,..etc. Convert Image rgb to gray
2. For each block compute a feature vector (DCT or PCA).
3. Place the feature vectors as the rows of a matrix and then lexicographically sort the rows.
4. Since similar blocks should have similar feature vectors so neighbors in the sorted matrix are considered to be pairs. (**PROPOSED : CLUSTERING)**
5. for each pair compute the similarity between their feature vectors. If the

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

similarity is > th0 declare them to be as a "matched pair" otherwise discard them.

(IDENTIFICATION OF OUTLIERS BASED ON THE SIMILARITY MEASURES OR POINTS)

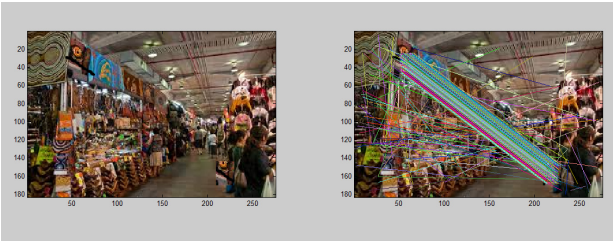
6. for each matched pair, compute the shift vector between them i.e. how far they are apart in the image. If the norm of the shift vector > th1 then keep them otherwise discard them. This prevents neighboring blocks matched with each other.

(PROPOSED) [FREQUENCY INTENSITY IDENTIFICATION AND LOCALIZATION)

7. for each shift vector, count how many times it has occurred. If the frequency of a shift vector is >th3 then keep all the associated matched pairs otherwise discard them. This is because when a region is copied and moved all the blocks in them move with the same homogeneous motion.

8. The matched blocks remaining after all the above steps are the potential areas where copy-move forgery may have taken place.

OUTPUT SCREENSHOTS



In the specified figure and output screenshot, it is apparent that the localization is performed on the test image. The copy move forgery is easily detected on the image alongwith the candidate points and pixels.

PERFORMANCE ANALYSIS

The proposed work is working efficiently in case of BMP Images. We have analyzed and implemented the same algorithmic approach on JPEG images. It is giving less optimal results in terms of more noisy localization and compromise in the accuracy.

The JPEG images are not efficient in terms of the localization in the images after detection of copy move.

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

CONCLUSION AND SCOPE OF FUTURE WORK

In this research work, the major focus is pointed on the copy move forgery detection on the digital images. Copy-move forgery is a specific type of image tampering where a part of the image is copied and pasted on another part generally to conceal unwanted portions of the image. Hence, the goal in detection of copy-move forgeries is to detect image areas that are same or extremely similar. In this paper, we review several methods proposed to achieve this goal. These methods in general use block-matching procedures, which first divide the image into overlapping blocks and extract features from each block, assuming similar blocks will yield similar features. Later, a matching step takes place where the aim is to find the duplicated blocks based on their feature vectors. A forgery detection decision is made only if similar features are detected within the same distance of features associated to connected blocks. We have examined the several different block-based features proposed for this purpose in relation to their time complexity and robustness to common processing scaling up/down, compression, and rotation. We have also included comparative results for better evaluation. The technique and algorithmic approach is efficient in terms of the results and complexity, still there is scope of the future work for further enhancement of the results.

For the future scope of work, the following techniques can be associated :

- Genetic Algorithms
- Simulated Annealing
- Neural Networks
- Ant Colony Optimization
- Combinatorial Optimization Solution Methodology
- Swarm Intelligence

REFERENCES

[1] Ashima Gupta, Nisheeth Saxena and S.K.Vasistha, " Detecting Copy move Forgery using DCT," International Journal of Scientific and Research Publications, Vol.3(5), 2013

.[2] Hieu Cuong Nguyen and Stefan Katzenbeisser, " Detection of copy move forgery in Digital images using Radon transformation and phase correlation,"

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

Eighth International Conference on Intelligent information hiding and Multimedia Signal Processing, IEEE, pp.134-137, 2012

[3] A.C.Popescu and H.Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Technical Report, TR2004-515, Department of computer Science, Darmouth College, pp.758-767, 2006

[4] Swapnil H.Kudke,A.D.Gawande, "Copy-Move Attack Forgery Detection by Using SIFT," International Journal of Innovative Technology and Engineering (IJITEE), Vol 2(5), 2013

[5] M. Sridevi, C. Mala and Siddhant Sanyam, "Comparative Study of Image Forgery and Copy-Move," International Journal of computer science Issues, Vol.8(4), 2011

[6] Ashima Gupta, Nisheeth Saxena, S.K Vasistha, "Detecting Copy Move Forgery using

DCT," International Journal of Scientific and Research Publications, Vol.3(5), 2013

[7] B.L.Shivakumar and Dr.S.Santhosh Baboo, "Automated Forensics Method for Copy-Move Forgery Detection based on Harris Interest Points and Sift Descriptors," International Journal of Computer Applications, Vol.27(3), 2011

[8] Swapnil H.Kudke and A.D.Gawande, "Copy-Move Attack Detection by Using SIFT," International Journal of Innovation Technology and Exploring Engineering, Vol.2(5), 2013

[9] B.L.Shivakumar and Lt.Dr.S.Santhosh Baboo, "Detection of Region Duplication Forgery in Digital Images Using SURF," International Journal of computer science Issues, Vol.8(4), 2011

[10] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Albert Del Bimbo, Luca Del Tongo, Giuseppe Serra, "Copy-Move Forgery Detection and Localization by Means od Robust Clustering with J-Linkage, Signal Processing: Image Communication Journal, Vol.28(6), 2013

[11] Preeti Yadav, Yogesh Rathore and Aarti Yadu, "DWT Based Copy-Move Image Forgery Detection," International Journal of Advanced Research in Computer Science and Electronics Engineering, Vol.1(5), 2012

[12] Sevinc Bayram, Husrev Taha Sencar and Nasir Memon, "A Survey of Copy Move Forgery Detection Technique, IEEE Western New York Image Processing Workshop, 2008

ISSN (Print) 2321-3280
ISSN (Online) 2319-4618

International Journal of Reviews, Surveys and Research (IJRSR)

Current Issue - Volume 3 Issue 2 May 2014

(Approved and Registered with Govt. of India)

[13] Luo Juan and Oubong Gwun, "A Comparison of SIFT, PCA-SIFT AND SURF," International Journal of Image Processing, Vol.3(4), 2011

[14] Amanpreet Kaur and Richa Sharma , "Optimization of Copy-Move Forgery Detection Technique," International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3(4), 2013

[15] I.Amerini,L.Ballan,R.Caldelli,A.D.Bimbo,and G.Serra, "A SIFT-based Forensics Method for Copy-Move Attack Detection and Transformation Recovery," IEEE Transaction on Information Forensics and Security, Vol.6, no.3, pp.1099-1110, 2011.

[16] V.Christlein,C.Riess,J.Jordan, C.Riess,and E.Angelopoulou, "An Evaluation of popular Copy-Move Forgery Detection Approaches," IEEE Transactions on Information Forensics and Security, Vol.7, pp.1841-1854, 2012