A Survey on Forensic Images for Forgery Detection and Image Authentication

Satish B Pratapur[#1], **Dr. Shubhangi D.C**[*2]
[#] Dept. of computer science & Engineering, Head of the Dept. of Computer Science &Engineering,
[1]Appa Institute of Engg. & Tech., Karnataka, India
[2]Visvesvaraya Technological University, Karnataka, India
satish.pratapur@gmail.com

Abstract— Today's generation, we listen or see crime in our daily routine. The images taken from the crime location for the forensic studies to find the evidence are manipulated using different tools. Analyzing the image in forensic science accurately to obtain information from an image without the prior information of an image is a major subject. To obtain the original details of an image to authenticate or manipulation being done in an image by using different forgery methods (image cloning, image slicing, image retouching etc.) to obtain the duplicate, modified or forged details of an image. In this paper we make a survey of existing methods to develop an exhaustive and invariant method to obtain the minute changes or duplication made in an image with accurate result, high reliability and less complexity.

Keywords— ***Copy-Move, Zernike moment, DCT, PCA, SVD, Image Hash, NMF, Ring partition.***

I. INTRODUCTION

In this digitalization era, we represent most of the information using images. With the widespread use of multimedia the amount of media that is conveyed via digital devices has grown dramatically this has brought up many advantages. However, the development in the image processing field has produced various powerful digital image processing programs, such as Photoshop etc., which makes it relatively easy to create digital image forgeries. This forged image cannot be detected through our naked eyes, for example, if a portion of image is changed (deleted/replaced) using an image editing tool, the change in the image is very difficult to locate and identify by natural human vision system. It is due to the fact that the image editing tools are so intelligent to that level they can submerge changed part into the original image seamlessly.

To find out the image being modified or forged, various method have been developed including source identification &forgery detection where human interpretation is needed, blind approaches(active and passive) using DCT &WLD methods cannot distinguish between malicious tampering and innocent touching, COPY-MOVE forgery detection using SIFT\z vectors, blocked based and key based for small super pixels detection . From the survey of these methods from papers, we have a problem of complexity, detecting small forged area and rotation variant.

For image forgery detection, various methods have been developed including source identification &forgery detection where human interpretation is needed, blind approaches(active and passive) using DCT &WLD methods cannot distinguish between malicious tampering and innocent touching, COPY-MOVE forgery detection using SIFT vectors with robustness and localizing the forgery, forgery using Median filtering with post operations except heavily Gaussian and averaging filtering , Clone detector based on Fourier-Mellin transform of the image blocks, active and passive to detect image forgery but unable detect small forged area of an image, Discrete Cosine Transform for detecting overlapping duplicated region.

SIFT algorithm to detect the cloned regions in the image but stable to changes with respect to changes in illumination, rotation and scaling, near duplication detection based on log-polar coordinates and is invariant with respect to reflection, rotation and scaling, detecting image forgery using Codebook which is generated from the set of images, Zernike moments, ring partition, non-negative matrix factorization, Fourier-Mellin transform for robust hashing technique. In this regard, we have made a literature survey to study the background, ground truths and potentiality of the problems in image forgery detection.

II. LITERATURE SURVEY/ RELATED WORK

A. Image Authentication Using Stochastic Diffusion [1] has two methods for detection of image forgery. The first method considers a binary image watermarking algorithm for hiding an image in a single host image which is based on linearization of the encrypted data. The second method solves the problem of 24-bit image hiding in three host images which generates a near perfect reconstruction after decryption. Both methods make use of a 'hidden code' technique to randomize the order of the embedded bits and the location (in the image plane) of the LSBs which make the embedded information more robust to attack.

In 'image space', the plaintext is considered to be an image p(x,y) of compact support x∊[X,X]; y∊[Y,Y]. Stochastic diffusion is that process compounded in the following encryption/decryption algorithms:

- **Encryption:** $c(x,y)=m(x,y)\otimes_x \otimes_y p(x,y)$ where $m(x,y)=F_2^{-1}[M(k_x,k_y)]$ and kx,ky

$$M(k_x,k_y)= \begin{cases} N^*(k_x,k_y) /|N(k_x,k_y)|^2 , \mid N(kx,ky) \mid\neq 0; \\ N\leftarrow(k_x,k_y), \mid N(k_x,k_y) \mid=0 . \end{cases}$$

The symbols $\otimes_x$ and $\otimes_y$ denote convolution in x and y, respectively, k_x and k_y are the spatial frequencies, F_2^{-1} denotes the two-dimensional inverse Fourier transform and the function $N(k_x,k_y)$ is taken to be the Fourier transform of a cipher n(x,y).

- **Decryption:** $p(x,y)=n(x,y)\Theta_x\ \Theta_y c(x,y)$

Where Θ_x and Θ_y denote correlation in x and y, respectively. For digital image hiding, consider a discrete image array p_{ij} , i =1,2,...,I; j =1,2,...,J of size IXJ and discrete versions of the operators involved, i.e. application of a discrete Fourier transform and discrete convolution and correlation sums.

- **Principal Algorithms:** The principal algorithms associated with the application of stochastic diffusion for watermarking with ciphers are as follows:

Algorithm I: Encryption and Watermarking Algorithm

Step 1: Read the binary plaintext image and compute the size I ⇥ J of the image.

Step 2: Compute a cipher of size I ⇥J using a private key and pre-condition the result.

Step 3: Convolve the binary plaintext image with the preconditioned cipher and normalize the output.

Step 4: Binaries the output obtained in Step 3 using a threshold based on computing the mode of the Gaussian distributed cipher text.

Step 5: Embed the binary output obtained in Step 4 into the host image Least Significant Bit (LSB) to generate the stage-image.

Algorithm II: Decryption and Extraction Algorithm

Step 1: Read the stego-image and extract its lowest 1-bit layer.

Step 2: Regenerate the (non-preconditioned) cipher using the same key used in Algorithm I.

Step 3: Correlate the cipher with the input obtained in Step 1 and normalize the result.

Step 4: Quantize and format the output from Step 3 to construct the original image.

The exposure of the encryption key(s), the encryption algorithm and the embedding technique along with the hidden codes to those other than the intended receiver is practically impossible. By considering the application of stochastic diffusion for encrypting image data prior to embedding it into a host image. Embedding a binary watermark into a host image obtained by binarizing a floating point cipher text, as provides a cryptographically secure solution. This is because binarization is an entirely one-way process. Thus, although the watermark may be encryption key removed from the stego-image, it cannot be decrypted without the recipient having access to the correct.

B. Copy- Move digital image forgery [11] is a specific type of image manipulation, where a part of the image itself is copied and pasted into another part of the same image. Copy-Move forgery is performed with the intention to make an object "disappear" from the image by covering it with a small block copied from another part of the same image. It is very difficult for a human eye to detect, since the copied segments come from the same image, the color palette, noise components, dynamic range and the other properties will be compatible with the rest of the image. Sometimes, even it makes harder for technology to detect the forged image which is retouched with the tools that are available.

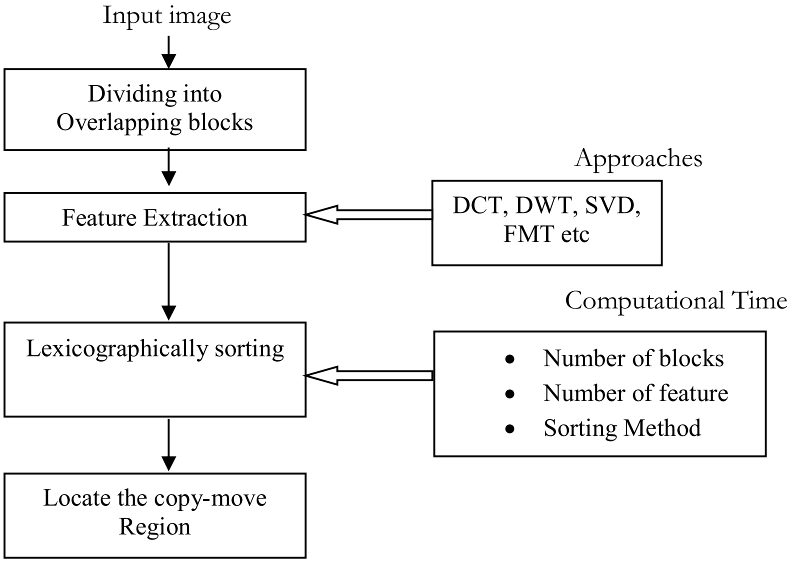


Fig. 1: copy-move forgery detection technique

Photo Image Forgery Detection Techniques is used to identify photo forgeries and to identify forged region by given only the forged image. Photo image forgery is classified in to two categories. The first class is Copy-Move Forgery or Cloning of image forgeries includes images tampered by copying one area in an image and pasting it onto another area. The second class of forgeries is Copy-Create Image Forgery in which copying and pasting areas from one or more images and pasting on to an image being forged.

Effective methodologies for detecting both Copy-Move and Copy-Create type of image forgeries are (i) JPEG Compression Analysis and Algorithm for Forgery Detection

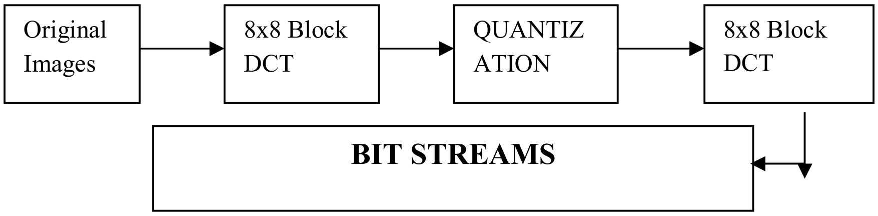


Fig. 2: Block Diagram JPEG Compression

The DCT domain is used to convert a signal into coefficient values with the ability to perform truncating and rounding operations, thus allowing compression of this signal to take place. The first step in JPEG compression process is calculating the DCT of each 8x8 blocks.

(ii) Direction Filter Using JPEG Image Analysis: The main steps of proposed algorithms are based on Image Edge Detection and tampering localization. Following steps explain the process of forgery detection algorithm :(1) Read Input Image (2) Extract edge image using CANNY EDGE Operator (3) Computer X and Y-axis pixel by applying convolution with directional filter to GENERATE SIMILAR type of pixel pyramid. (4) Calculate Horizontal and Vertical projection profile (5) Find boundary pixel values, which differ with Projection profile with X, and Y values (6) Calculate feature map (7) Identify the forgery region (8) Display the Forgery Region (9) Extract the forgery Region.

Direction Filter Technique is successful for JPEG, RGB, Gray Scale, PNG & BMP formats, but JPEG Compression Technique is successful for only for JPEG format.

C. DETECTING IMAGE FORGERY USING BLIND METHODS [2] are regarded as a new direction, in contrast to active methods, they work in absence of any protecting techniques and without using any prior information about the image or the camera that took the image.

To detect the traces of tampering, blind methods use the image function and the fact that forgeries can bring into the image specific detectable changes .Blind methods used the detection of traces of images,

- **Detection of Near–Duplicated Image Regions:** In a common type of digital image forgery, called copy– move forgery, typically with the intention to hide an object or a region and this method brings into the image several near– duplicated image regions which are mostly not identical. So, detection of such regions may signify tampering. This is caused by lossy compression algorithms, such as JPEG, or by possible additional use of retouch tools. Existing near–duplicated regions detection methods mostly have several steps in common: tiling the image with overlapping blocks, Feature representation and matching of these blocks.

- **Detection of Traces of Resampling and Interpolation:** When two or more images are spliced together, to create high quality and consistent image forgeries, almost always geometric transformations such as scaling, rotation or skewing are needed. Geometric transformations typically require a resampling and interpolation step. Therefore, by having sophisticated resampling/interpolation detectors, altered images containing resampled portions can be identified and their successful usage significantly reduced. Existing detectors use the fact that the interpolation process brings into the signal specific detectable statistical changes.

- **Detection of Inconsistencies in Chromatic Aberration:** Optical imaging systems are not ideal and often bring different types of aberrations into the captured images. Chromatic aberration is caused by the failure of the optical system to perfectly focus light of all wavelengths. This type of aberration can be divided into longitudinal and lateral. Lateral aberration happens by a spatial shift in the locations where light of different wavelengths reach the sensor. This causes various forms of color imperfections in the image.

- **Detection of Image Noise Inconsistencies:** A commonly used tool to conceal traces of tampering is addition of locally random noise to the altered image regions. Generally, the noise degradation is the main cause of failure of many active and passive image forgery detection methods. Typically, the amount of noise is uniform across the entire authentic images. Adding locally random noise may cause inconsistencies in the images noise. Therefore, the detection of various noise levels in an image may signify tampering.

Existing copy move forgery and blind methods for image tamper detection. Probably the main drawback of existing methods is highly limited usability and reliability.

D. Mesh-based Hashing for Copy Detection and Tracing of Images [4]: the block diagrams of the mesh-based image hashing system and image query system are as shown in below figure

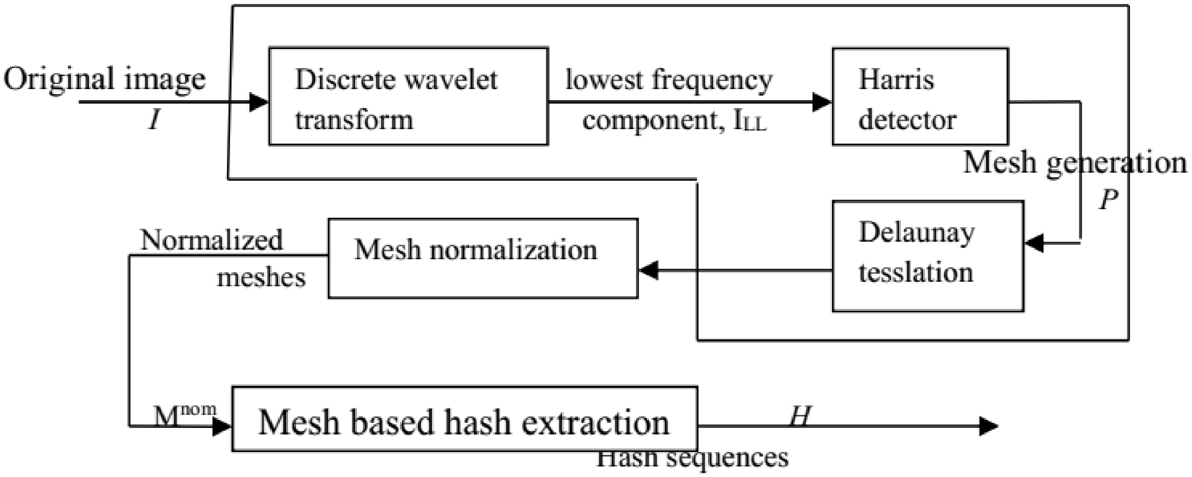


Fig. 3: Block diagram of the mesh-based image hashing system.

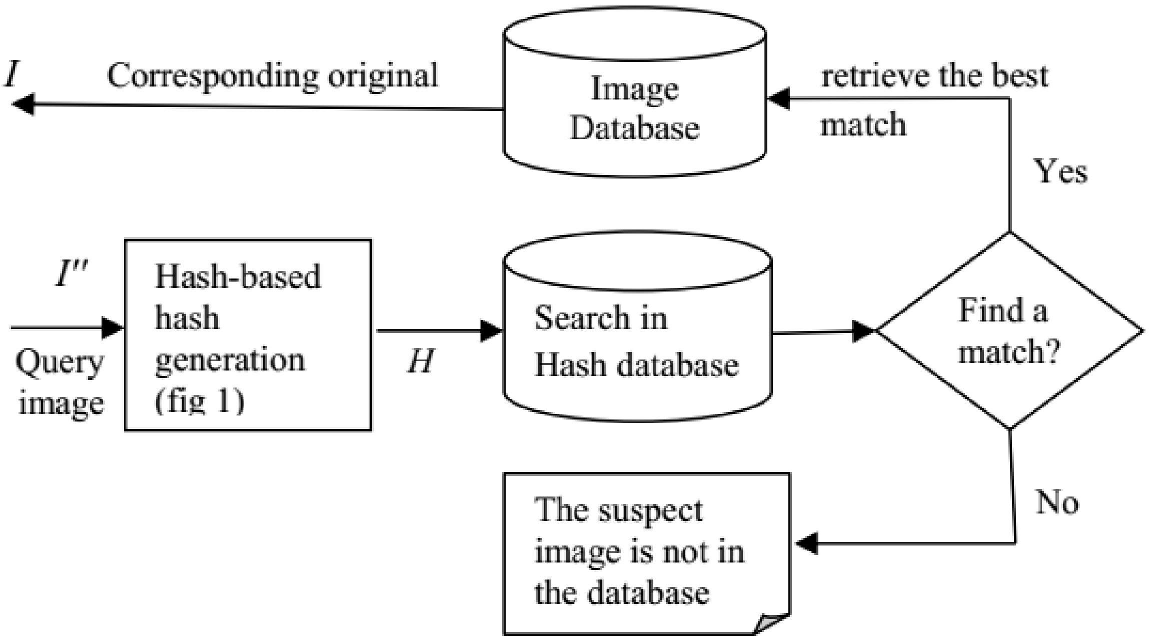


Fig. 4: Block diagram of the image query system: a query enters into the hash database

- **Robust Image Mesh Generation Extraction:** Robust meshes plays an important role in our method since it is a prerequisite in resisting geometrical distortions. To generate meshes, the first step is to detect salient points of an image. Among the ubiquitous feature point extraction methods, Harris detector has been popularly used. However, the original Harris detector is still not robust enough to be used for our purposes. Thus, they propose to improve its robustness by carrying out it in the lowest-frequency subband of the discrete wavelet transform (DWT) domain. Our intention is to filter out noisy points before salient point detection. Once the feature point extraction process is finished, the De- launay tessellation can be used to decompose the image into a set of disjointed triangles. Each triangle (called a mesh hereafter) is regarded as the minimum unit for robust hash extraction.

The overall mesh generation process is summarized as follows: (i) the original image I is discrete wavelet transformed to obtain the lowest-frequency subband signal, ILL; (ii) the set of feature points P are generated by means of applying the Harris detector on ILL; and (iii) Delaunay tessellation is performed using P to obtain a set of meshes M. An example of mesh extraction is shown in Fig. 3, which contains the generated meshes from the original Lenna and its Stirmark attacked Lenna images. By visual inspection, they found that several meshes are consistently extracted. These results validate the effectiveness of mesh extraction from the lowest- frequency subband of an image.

- **Mesh Normalization:** Once the set of meshes in an image has been produced, each original mesh M_k will be normalized as M_k^{nom} k to generate a mesh-based hash H_k, where M_k^{nom} is a right-angled isosceles triangle with the size of 32*32. The aim of normalization is to maintain that all hashes are of the same size for efficient hash comparison. The normalization process is con- ducted by warpping M_k into M_k^{nom} through the processes of affine transform and interpolation.

- **Robust Mesh-based Hashing Image**: It attempts to transfer an image content to a short sequence while preserving distinguishable features in order to facilitate similarity measurement. In this paper, for each normalized mesh M_k^{nom} its robust hash is extracted in the block-DCT domain. First, each triangle M_k^{nom} is flipped and padded with its flipped version to form a 32*32 block. For a pair of blocks, a hash bit, defined as the magnitude relationship between two AC coefficients, is represented as follows:

$$H_k(s)= \begin{cases} 1 & \text{if } |f_i\,(p_1)j| - |f_j(p_2)\,| \geq 0, \\ 0 & \text{otherwise} \end{cases}$$

E. Image Hashing Based on Shape Contexts and Local Feature Points [16:] A novel shape-contexts-based image hashing approach using robust local feature points. The contributions are twofold: The robust SIFT-Harris detector is proposed to select the most stable SIFT key points under various content-preserving distortions. Compact and robust image hashes are generated by embedding the detected local features into shape-contexts-based descriptors.

ROBUST LOCAL FEATURE POINTS

Scale Invariant Feature Transform Review (SIFT) mainly consists of the following steps:

- **Scale-In variant Points Detection and Localization:** The local feature points detected as the candidates of scale-invariant keypoints are based on the searching for local extrema in a series of difference-of-Gaussian (DOG) images in the scale space. The construction of DOG is proceeded as follows: Image is first convolved with a series of Gaussian kernel functions with consecutively incremental scales. Then, two Gaussian blurred images with nearby scales is produced by using DOG. Essentially, the DOG detector could be attributed to the detector for blob structures in the image content, since it provides a close approximation of the scale-normalized Laplacian of Gaussian

- **Orientation Assignment and Descriptor Generation:** The orientation of each keypoint is determined by the peak of the orientation histogram formed by the gradient orientations within its neighborhood. The corresponding descriptor with 128 dimensions based on gradient histogram within its 16x16 local neighborhood is generated based on the position, scale, and orientation of each keypoint. Since they believed that the robustness of keypoint detector is more important for image hashing, they used the original SIFT descriptor in this work.

- **Robust Keypoints Detection Using Harris Criterion:** To design a robust image hashing against various attacks, robust feature extraction is the most important step. Although the DOG detector of SIFT provides satisfying performances under geometric transforms, its poor robustness against attacks such as additive noise and blurring limits its direct applications in image hashing. To extract robust local features, it is desired to select the most stable keypoints under various distortions and attacks.

- **Detection Evaluation**: This further illustrate the effect of Harris criterion on robust SIFT keypoints selection, defined a robust function to evaluate the performance of SIFT and SIFT-Harris detectors. Let be the set of keypoints detected from the original image and be the set of keypoints detected from its distorted copy where means the cardinality of a set, which is a measure of the number of distinct elements of the set.

  Experimental results show that the proposed image hashing is robust to a wide range of distortions and attacks, due to the benefits of robust salient keypoints detection and the shape-contexts-based feature descriptors. When compared with the current state-of-the-art schemes, the proposed scheme yields better identification performances under geometric attacks such as rotation attacks.

F. Image Authentication Using Zernike Moments and Local Features [17]: By using a robust hashing method for detecting image forgery including removal, insertion, and replacement of objects, and abnormal color modification, and for locating the forged area. Both global and local features are used in forming the hash sequence.

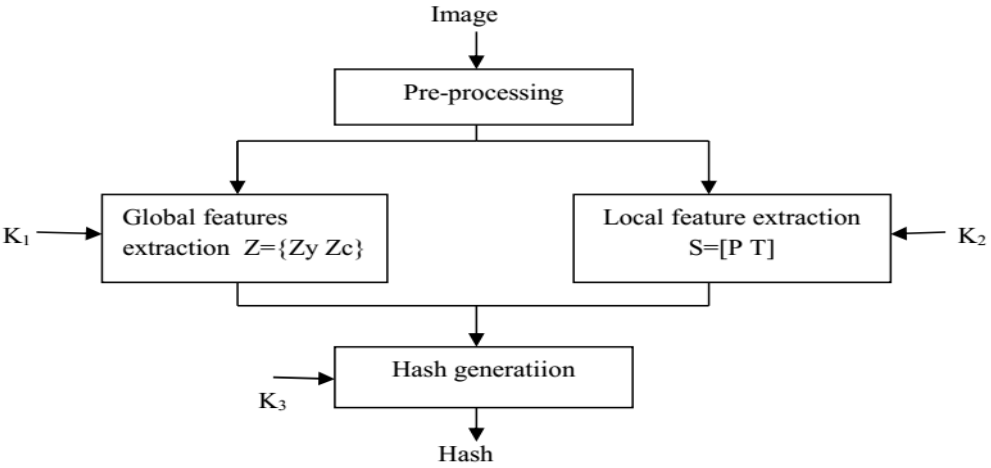


Image
Pre-processing
K1
Global features extraction Z={Zy Zc}
Local feature extraction S=[P T]
K2
Hash generatiion
K3
Hash

Fig. 5: Bock diagram of the image hashing method.

This method combined the advantages of both global and local features. The objective is to provide a reasonably short image hash with good performance, i.e., being perceptually robust while capable of detecting and locating content forgery. They used Zernike moments of the luminance/chrominance components to reflect the image's global characteristics, and extract local texture features from salient regions in the image to represent contents in the corresponding areas. Distance metrics indicating the degree of similarity between two hashes are defined to measure the hash performance. To decide whether a given image is an original/normally-processed or maliciously doctored version of a reference image, or is simply a different image, two thresholds are used. The method can be used to locate tampered areas and tell the nature of tampering, e.g., replacement of objects or abnormal modification of colors.

Probability of collision between hashes of different images approaches nill. Experimental results are presented to show effectiveness of the method by generating short hash length & detect specific forged location in an image especially the ability of distinguishing regional tampering from content-preserving processing.

G. Image Hashing Based on Ring Partition and NMF [19]: It is an efficient image hashing with rotation robustness and good discriminative capability. The key contribution is a novel construction of rotation-invariant secondary image, which is used for the first time in image hashing and helps to make image hash resistant to rotation.

In preprocessing, the input image is converted to a normalized image with a standard size. In the next step, the normalized image is partitioned into different rings, which are then used to construct a secondary image. Then, image hash is finally formed when NMF is applied to the secondary image by NMF coefficients. NMF coefficients are approximately linearly changed by content-preserving manipulations, so as to measure hash similarity with correlation coefficient.

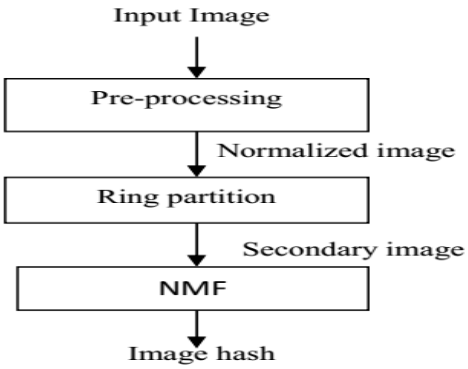


Fig. 5: Block diagram of our image hashing.

- **Preprocessing.** The input image is first mapped to a normalized size mxm by bilinear interpolation to ensure hashes of different size images have the same length and our hashing is resilient to scaling operation. The luminance component Y for representation is taken after color space conversion.
- **Ring partition.** Divide Y into n rings and exploit them to produce a secondary image.. The aim of this step is to construct a rotation-invariant matrix for dimensionality reduction.

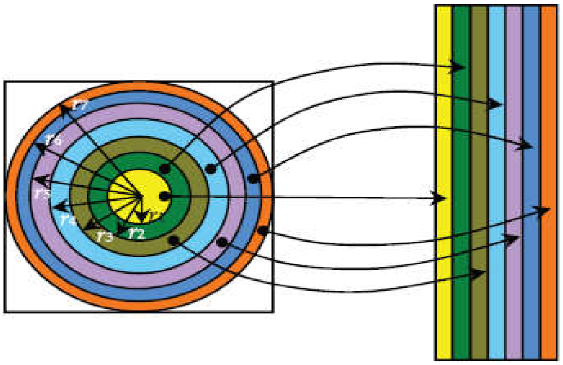


Fig 6: Ring Partition & Secondary Image

- **NMF.** The NMF is applied to V, and then the coefficient matrix C is available. Concatenate the matrix entries and obtain a compact image hash. Thus, the hash length is

  L= nK, where n is the number of rings and K is the rank for NMF.

  Experiment for illustrating the efficiency with 346 images.

H. Image Hashing with Ring Partition and Invariant Vector Distance [20]: In this image hashing algorithm is used for enhancing rotation robustness and discriminative capability.

The proposed image hashing is a four-phase procedure. To obtain stable feature extraction, initially input image is first preprocessed to generate a normalized image. The normalized image is divided into different rings which are kept unchanged even after image rotation. Further, the stable statistical features are extracted from image rings. Lastly to form a compact image has, the invariant distances between feature vectors are used. These four phases are detailed as follows.

- **Preprocessing:** To illustrate effects of commonly-used digital manipulations to images, three operations, i.e., bi-linear interpolation, Gaussian low-pass filtering and color space conversion, are exploited to produce a normalized image for feature extraction. An input image is first converted to a standard N × N image by bi-linear interpolation, so as to make our hashing resistant to image resizing, as well as to ensure they have the same hash length of those images with different sizes. And then, Gaussian low-pass filtering is applied to the resized image, which can reduce the influence of minor modifications, such as noise contamination or filtering. In general, it can be done by a symmetric convolution mask.

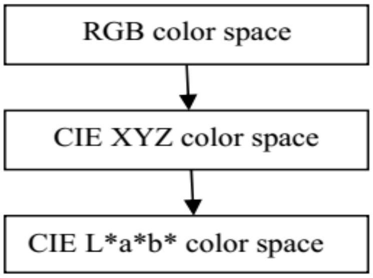


Fig 7: Diagram of Color Space Conversion

- **Ring Partition:** Generally, rotation operation takes image center as the origin. This means that the region in the inscribed circle of an image is still the same after rotation. By extracting stable features from image rings, this property gives us an opportunity to design image hashing resistant to rotation. The normalized image is divided into a set of rings with equal area since pixel numbers of all image rings are expected to be the same.

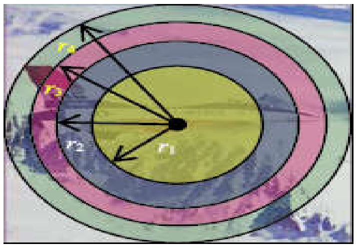


Fig. 8: Schematic partition with four rings.

- **Statistical Features:** Since pixels of image ring are unchanged after rotation, statistical features extracted from Rk (k = 1,2,...,n) can resist image rotation. To efficiently capture visual content of each ring, four statistics are chosen for representation, i.e., mean, variance, skewness, and kurtosis

  The extracted from image rings in perceptually uniform color space, i.e., CIE L∗a∗b∗ color space are the statistical features which are rotation invariant and stable, since ring partition is unrelated to image rotation.

I. Forgery Detection in CopyMove and Spliced Images [13]: It uses the sharped edge detection and the copy-move/splicing detection. Before presenting the proposed method, this part firstly shows the related theories in brief including multiscale using DWT, edge detection, dilation and RDM in which the first three are used in sharpness detection and the last is suggested for feature extraction in copy-move/splicing detection.

- **Multiscale using DWT:** With a 2D image f(x,y), two dimension DWT will produce one separable scaling function $\phi(x,y)$ and three separable directionally sensitive wavelets $\psi^{H}(x,y)$, $\psi^{V}(x,y)$, $\psi^{D}(x,y)$ corresponding to variations along the horizontal edges, vertical edges and diagonals, respectively. These functions are defined in (1), (2), (3) and (4).

$$\phi\ (x,y)= \phi(x)\ \phi(y)\ (1)$$

$$\psi^{H}(x,y)= \psi(x)\ \phi(y)\ (2)$$

$$\psi^{V}(x,y)= \phi((x)\ \psi(y)\ (3)$$

$$\psi^{D}(x,y)= \psi(x)\ \psi(y)\ (4)$$

where *$\phi(x)$, $\phi(y)$* are one dimension scaling functions and $\psi(x)$, $\psi(y)$ are one dimension wavelet functions.

- **Egde Detection:** Sharpness of edges can be traces of pasting information from other region. Therefore, edge detection is the first step to search the suspicious regions and the regions having edges with highest sharpness are collected, considered and tested. Laplacian operator is applied to the three sub-bands LH, HL and HH to select only edges for further processing steps by a convolution between each sub-band and a 3x3 Laplace kernel.

- **Dilation for Filling Gaps:** Ordinary, at positions of pasting, the borders will be smoothed by some software tools or Photoshop so not all of edges are detected continuously in LH, HL and HH. Therefore, dilation is proposed to bridge the gaps and make the boundary smooth, which helps to address the forged regions easier.

- **Extract Features using Run Difference Method:** Run Difference Method (RDM) is a feature extraction method in which features of size and prominence of texture elements are considered. From distribution of gray-level difference (DGD), RDM calculates five feature vectors including large difference emphasis, sharpness, the second moment of DGD, the second moment of distribution of the average gray level difference (DOD) and long distance emphasis.

HI

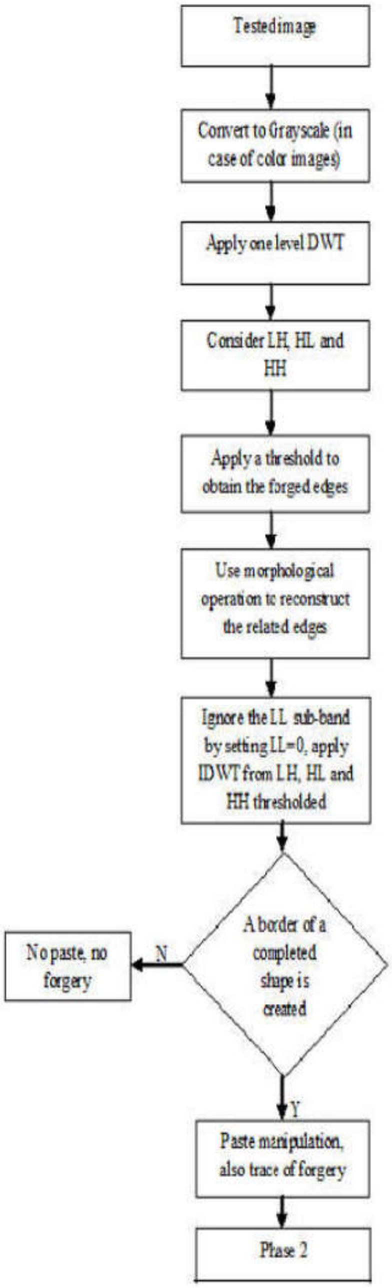

Tested image
Convert to Grayscale (in case of color images)
Apply one level DWT
Consider LH, HL and HH
Apply a threshold to obtain the forged edges
Use morphological operation to reconstruct the related edges
Ignore the LL sub-band by setting LL=0, apply IDWT from LH, HL and HH thresholded
A border of a completed shape is created
N
No paste, no forgery
Y
Paste manipulation, also trace of forgery
Phase 2

Fig. 9: Forgery confirmation based on boundary suspicious region

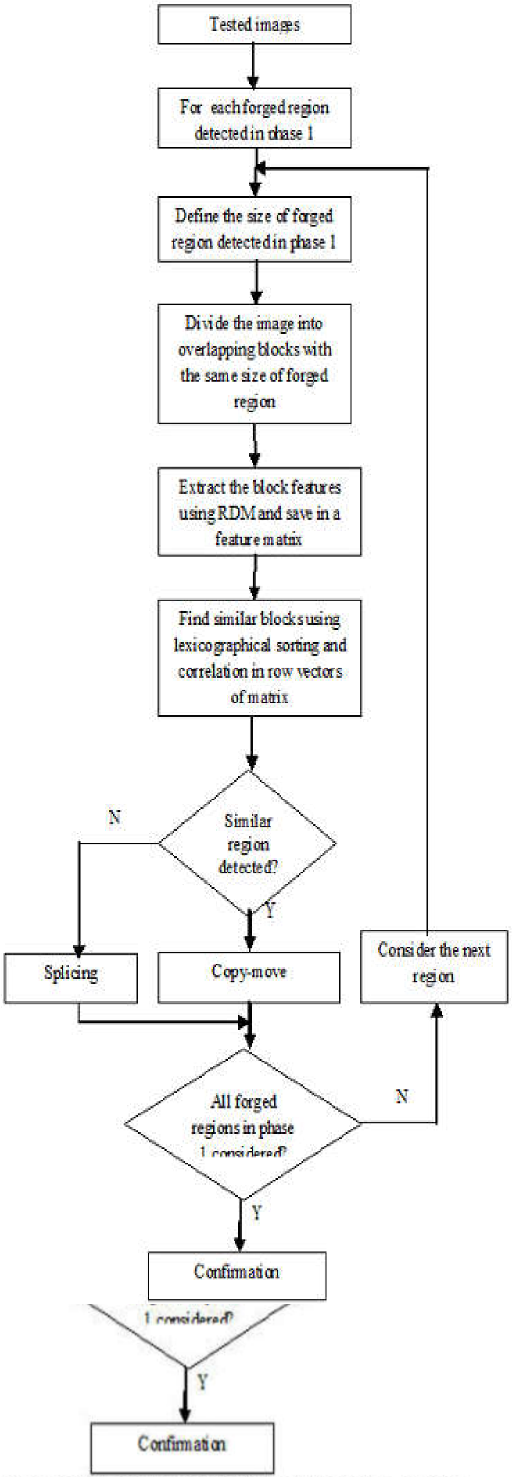

Tested images
For each forged region detected in phase 1
Define the size of forged region detected in phase 1
Divide the image into overlapping blocks with the same size of forged region
Extract the block features using RDM and save in a feature matrix
Find similar blocks using lexicographical sorting and correlation in row vectors of matrix
Similar region detected?
N
Y
Splicing
Copy-move
Consider the next region
All forged regions in phase 1 considered?
N
Y
Confirmation
1 considered?
Y
Confirmation

Fig 10: The confirmation in kind of forgery: of the copy-move, splicing or both copy-move and splicing

The algorithm is tested in three different kinds of images in which the first kind is copy-move images from benchmark_data and two remains are spliced images and copy-move/spliced images by Photoshop with good results.

J. Hash Using Texture and Shape Feature [3]: In this image hash generation method, image authentication and tampering detection process. It has two modules as shown below:

➢ **Hash generation:** the block diagram of hash generation is as shown below and the steps are as follows

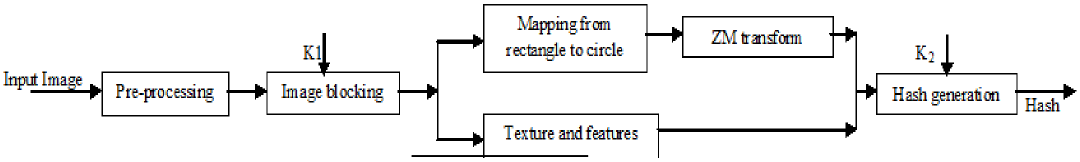


Fig. 11: Hash generation

- **The input image is pre-processed:** The pre-processing include re-sizing and color space conversion. The image is resized to a standard size using bi-linear interpolation. Then the color space of the image is transformed from RGB to YCbCr. And Y component and the difference value between Cb and Cr components |Cb - Cr| constitute the pre-processed images.

- **Image blocking:** The pre-processed images are partitioned into non-overlapped blocks randomly by secret key K1. Each block is resized using bi-linear interpolation. These blocks are mapped to a circle by equal interval sampling in polar coordinate system.

- **Shape feature extraction:** Zernike moments of blocks after mapping from rectangle to circle are calculated. Because the shape features can be obtained from a small number of low frequency coefficients, the order n does not need to be large. And with the increase of n, the calculation complexity and numbers of Zernike moments are increased greatly.

- **Texture features extraction:** the texture features of all blocks including skewness, kurtosis, and Tamura coarseness and contrast features are computed and rounded.

- **The final hash sequence** is obtained by pseudo-randomly permuting the texture and shape features obtained in the previous step by secret key K2.

➢ **Image authentication and tampering detection**

This module is shown in below figure is used to detect whether the received image is authentic or tampered. If tampered, the tampered regions in the image are marked. The steps are as follows.

(a) The received image is passed the same steps (a) to (d) as mentioned in hash generation

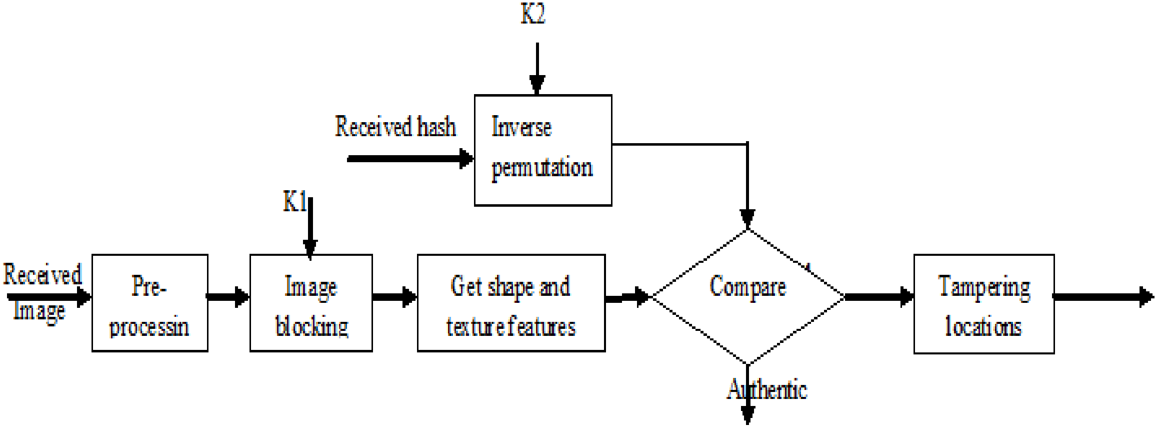


Fig. 12: Image authentication and tamper detection

(b) Using the secret key K2, inverse permutation is applied to the received hash to get the intermediate hash. The error sequence He is defined as He = |H1 −H2|. Then the distance D between the hash of the received image and input image is defined as in below equation.

$$D(H1,H2) == \sqrt{\sum_{He(k)\in\Gamma max} (He(k))^2}$$

If D is smaller than the threshold T, the received image is not tampered and is authenticated. Otherwise, it is considered as tampered, and the following steps (c) and (d) are used to find the tampered blocks.

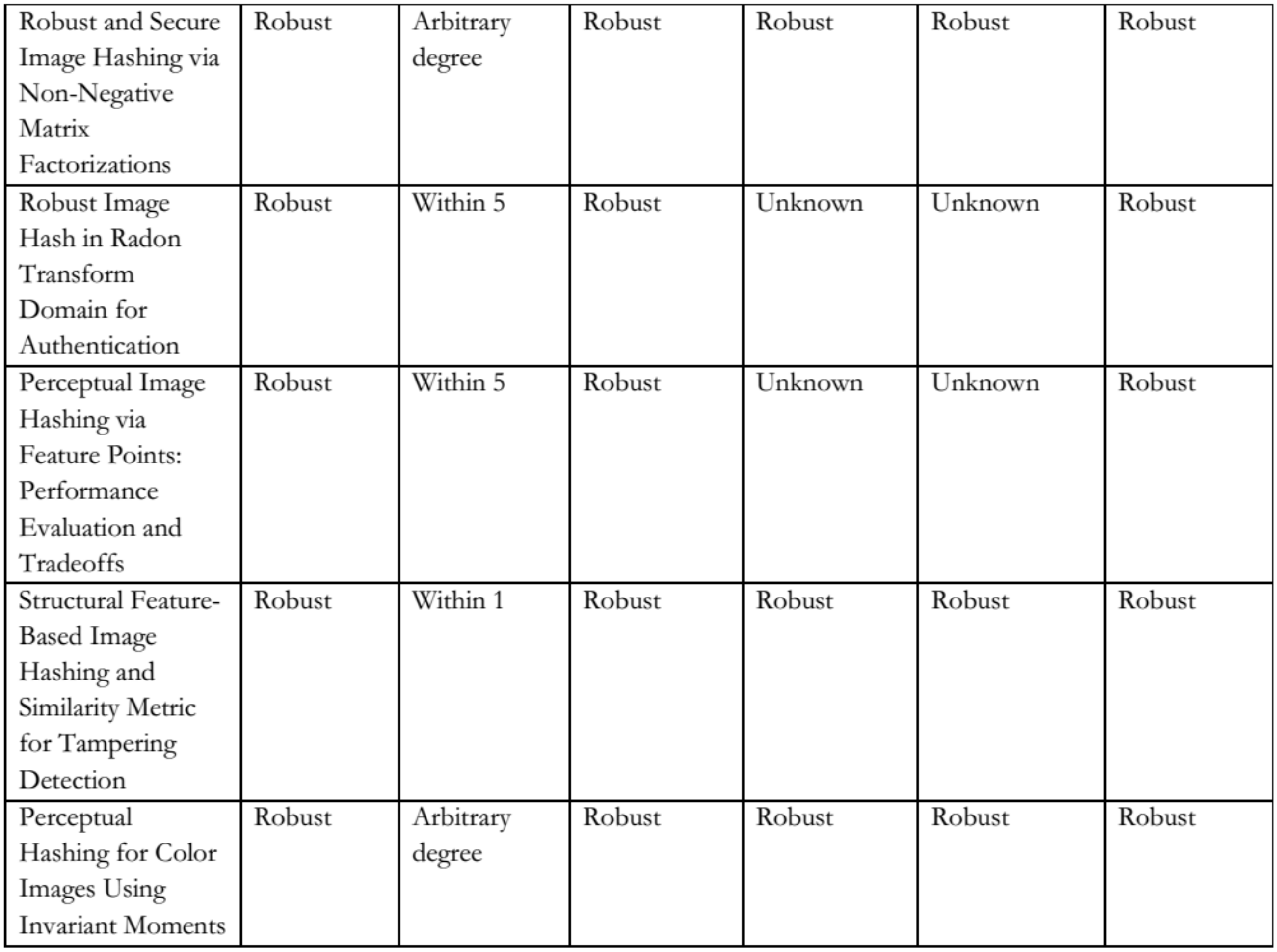
(c) An error vector is calculated as the distance between the hash bits of the received image blocks and that of corresponding input image block.

$$E(i) = \sqrt{\sum_{k=1}^{2Tn+4} (Hi1(k) - Hi2(k))^2} \qquad i = 1,\ldots,p2.$$

(d) Each entry of the vector E is compared with a block threshold τ. If any entry is greater than τ, the corresponding block is considered as tampered.

III COMPARATIVE STUDY OF DIFFERENT HASHING ALGORITHM

Algorithm	Image scaling	Image rotation	Guassian low-pass filtering	Gamma correction	Brightness adjustment	Contrast adjustment
Secure and Robust Hash-Based Scheme for Image Authentication	Sensitive	Sensitive	Robust	Unknown	Sensitive	Sensitive
Robust Image Hashing for Tamper Detection Using Non-Negative Matrix Factorization	Robust	Sensitive	Robust	Robust	Robust	Robust
Lexicographical Framework for Image Hashing with Implementation Based on DCT and NMF	Robust	Within 1	Robust	Robust	Robust	Robust
RASH: Radon Soft Hash Algorithm	Robust	Arbitrary degree	Robust	Robust	Robust	Robust
Robust Perceptual Image Hashing via Matrix Invariants	Robust	Arbitrary degree	Robust	Robust	Robust	Robust
Robust and Secure Image Hashing	Robust	Within 20	Sensitive	Robust	Sensitive	Unknown



Robust and Secure Image Hashing via Non-Negative Matrix Factorizations	Robust	Arbitrary degree	Robust	Robust	Robust	Robust
Robust Image Hash in Radon Transform Domain for Authentication	Robust	Within 5	Robust	Unknown	Unknown	Robust
Perceptual Image Hashing via Feature Points: Performance Evaluation and Tradeoffs	Robust	Within 5	Robust	Unknown	Unknown	Robust
Structural Feature-Based Image Hashing and Similarity Metric for Tampering Detection	Robust	Within 1	Robust	Robust	Robust	Robust
Perceptual Hashing for Color Images Using Invariant Moments	Robust	Arbitrary degree	Robust	Robust	Robust	Robust

Table1: Hashing Algorithms against Common Content-Preserving Operations

Robustness performances of some typical hashing algorithms against common content-preserving operations are summarized in Table1, where “Unknown” represents that such robustness result has not been reported in the literature and some state-of-the-art algorithms are robust against image rotation with arbitrary degree. However, these algorithms are not good enough in discrimination. Therefore, more efforts on developing high-performance algorithms with rotation robustness and good discrimination are in demand.

CONCLUSION

Their experiments show that the hashing is robust against content-preserving operations. The hashing is much better than all these algorithms in classification performances with respect to robustness and discrimination. The literature survey indicates that there are certain drawbacks and there exists scope for improvements in the methods those we came across in the literature survey. The main drawback with various existing copy move forgery and blind methods mentioned above is highly limited usability, reliability and rotation variant. But it should be noted that the area is growing rapidly and results obtained promise a significant improvement in forgery detection in the never ending competition between image forgery creators and image forgery detectors.

REFERENCES

[1] AbdulRahman I, Al-Rawi and Jonathan M. Blackledge, "Image Authentication Using Stochastic Diffusion", in proceedings of 15th Intl. conf. on Computer Modeling and Simulation, 2013.

[2] B.L.Shivakumar, Lt. Dr. S.Santhosh Baboo, "Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods", Vol. 10, Issue 7, Ver. 1.0, Sept., 2010.

[3] Babak Mahdian _, Stanislav Saic "A bibliography on blind methods for identifying image forgery", Elsevier vol. 25,Issue 6, pp. 389–399, July 2010

[4] C.S. Lu, C.Y. Hsu, S.W. Sun, and P.C. Chang, "Robust Mesh-Based Hashing for Copy Detection and Tracing of Images", Proc. IEEE Intl. Conf. Multimedia and Expo, Vol.1, pp. 731-734, 2004.

[5] E.Agnes, S. Devi Mahalakshmi, Dr. K. Vijayalakshmi, "A Forensic Method for Detecting Image Forgery Using Codebook", Intl. Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 3, March 2013.

[6] F. Khelifi and J. Jiang, "Perceptual image hashing based on virtual watermark detection", IEEE Trans. Image Processing, Vol. 19, No. 4, pp. 981–994, Apr. 2010.

[7] Gang Cao Yao Zhao Rongrong Ni Lifang Yu Huawei Tian, "Forensic Detection Of Median Filtering In Digital Images", ICME 2010

[8] R. Sandler and M. Lindenbaum, "Nonnegative Matrix Factorization with Earth Mover's Distance Metric for Image Analysis", IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 33, No. 8, pp. 1590-1602, Aug. 2011.

[9] Swaminathan, Y. Mao, and M. Wu, "Robust and Secure Image Hashing", IEEE Trans. Information Forensics and Security, Vol. 1, No. 2, pp. 215-230, June 2006.

[10] 3hS.Xiang, H. J. Kim, and J. Huang, "Histogram-based image hashing scheme robust against geometric deformations", in Proc. ACM Multimedia and Security Workshop, New York, 2007, pp. 121–128.

[11] S.Murali1, Govindraj, Prabhakara H. S and Basavaraj S. Anami, "Comparison And Analysis Of Photo Image Forgery Detection Techniques", International Journal on Computational Sciences & Applications (IJCSA), Vol. 2, No.6, Dec. 2012.

[12] Supakorn Prungsinchai, Fouad Khelifi and Ahmed Bouridane, "Fourier-Mellin Transform for Robust Image Hashing", IEEE 4th Intl. conf. on Emerging Security Technologies,2013.

[13] Tu Huynh-Kha, Thuong Le-Tien, Synh Ha-Viet-Uyen ,Khoa Huynh-Van,Marie Luong "A Robust Algorithm of Forgery Detection in CopyMove and Spliced Images", Intl, Journal of Advanced Computer Science and Applications, Volume 7,No 3, 2016.

[14] Tushant A. Kohale, at.al., "Detection of Post operated Copy Move Image Forgery by Integrating Block Based and Feature Based Method", Intl, journal of advanced research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014.

[15] V. Monga and B.L. Evans, "Perceptual Image Hashing via Feature Points: Performance Evaluation and Tradeoffs", IEEE Trans. Image Processing, Vol. 15, No.11, pp. 3452-3465, Nov. 2006.

[16] Xudong Lv and Z. Jane Wang, "Perceptual image hashing based on shape contexts and local feature points", IEEE Trans. Inf. Forensics Security, Vol.7, No. 3, pp. 1081–1093, June 2012.

[17] Y. Zhao, S. Wang, X. Zhang, and H. Yao, "Robust Hashing for Image Authentication Using Zernike Moments and Local Features", IEEE Trans. Information Forensics and Security, Vol. 8, No. 1, pp. 55-63, Jan. 2013.

[18] Z. Tang, S. Wang, X. Zhang, W. Wei, and S. Su, "Robust Image Hashing for Tamper Detection Using Non-Negative Matrix Factorization", J. Ubiquitous Convergence and Technology, Vol. 2, No. 1, pp. 18-26, 2008.

[19] Zhenjun Tang, Xianquan Zhang, and Shichao Zhang, "Robust Perceptual Image Hashing Based on Ring Partition and NMF ", IEEE Trans. Knowledge and Data, Vol. 26, No. 3, March 2014.

[20] Zhenjun Tang, Xianquan Zhang, Xianxian Li, and Shichao Zhang, "Robust Image Hashing With Ring Partition and Invariant Vector Distance", IEEE Trans. On Information Forensics And Security, Vol. 11, No. 1, January 2016