

# Passive Copy-Move Image Forgery Detection Method Using MSER and SVD

Ruhi Garg<sup>1</sup>, Navpreet Kaur Gill<sup>2</sup>, Amit Doegar<sup>3</sup>

<sup>1,2,3</sup>Department of Computer Science and Engineering, NITTR, India)

## ABSTRACT

Digital Forensic is a branch of forensic science which is related to computer crime. It deals with the investigation and recovery of material found in digital devices. Digital images and videos are the most important part of digital forensics as they are the prime evidences in law issues or in mass media. So the loyalty of the digital image is important. Due to the rapid increase and easy access of photo editing software tools, it has become easy to duplicate and modify digital image. Copy-move forgery (CMF) is the widely recognized image forgery technique in digital images. In CMF, certain part of the image has been copied and subsequently pasted to another location within the original image to make duplication or cover something. A considerable number of researches already done on the copy-move forgery detection (CMFD) but there's a problem occurs in feature extraction and matching phase. So in the proposed work, we design copy-move forgery detection system using the MSER feature extraction technique and correlation based matching on the feature vector. MSER is the application for the region presented in the image so we can find out the forged region easily. Experimental analysis shows that the proposed work achieves better accuracy on the basis of precision and recall rate compared to similar works.

**Keywords — Cloning, Digital forensics, Correlation matching, SIFT, MSER.**

## I. INTRODUCTION

The rapid growth of technology and easy availability of commercial photo-editing software tools, free or paid, has made digital image tampering much easier. For example, such software has made it easy to manipulate and copy the image's content without (significantly) degrading its quality or with no obvious trace leaving behind to a naked eye [16]. Moreover, the images that are widely shared over the social media on the internet for fun can be easily manipulated to misrepresent their meaning with malicious intention.

As indicated by the Wall Street Journal, out of all colored images published in United States, 10% was in fact manipulated and duplicated [1]. Digital image tampering also been detected in academic papers. For example, according to [2], 15% of the respondents admitted that they were in scientific misconduct such as fabricating, falsifying, manipulating or plagiarizing data in the last three years. Another survey [3] also reported that in Journal of Cell Biology, roughly 20% of accepted manuscripts contain figures which are manipulated inappropriately and 1% of them with fake manipulations.

The credibility of photographs has an indispensable role as these photographs are the prime evidences and used as historical records in wide number of applications such as cyber crime, law enforcement, medical imaging, insurance claims and Journalistic photography.

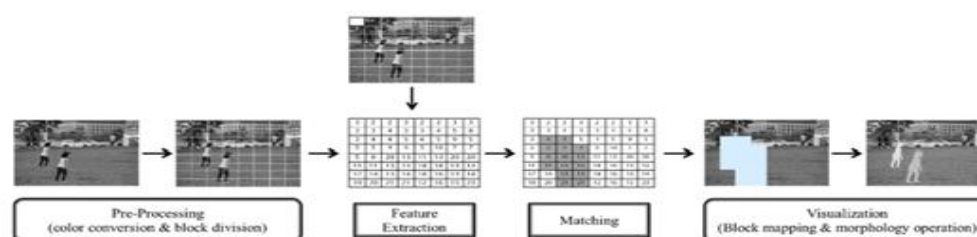


**Figure 1 Example of CMF where number of Iranian missiles is increased [16]**

Image tampering detection techniques are mostly categorised into two classes: active (intrinsic) and passive (non-intrinsic) approaches, according to the presence of additional information. Intrinsic methods require additional information embedded in the digital image to detect image tampering such as digital watermarks and digital signatures. Unlike the intrinsic approach, the non-intrinsic approach does not depend on pre-stored information that is identifier does not have any former data about the digital image.

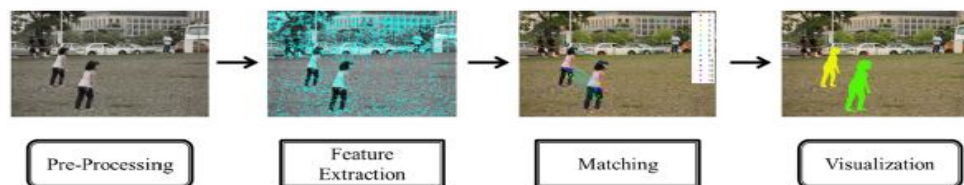
Among passive tampering techniques, CMF is the widely accepted image tampering wherein some region of a image has been copied and pasted to another location in the same image, to hide some responsive or significant information. An example of CMF is depicted in Fig 1. As both the copied and pasted region belongs to the same image, properties like color, texture, noise, etc. remains the same. This correlation makes difficult to detect CMF with the naked human eye. In the literature, many passive CMFD methods have been proposed which are categorised as: block-based methods and keypoint-based methods.

Block-based methods uniformly subdivide the image into small size overlapping or non-overlapping partitions called blocks of fixed size. Then the features are extracted from these sub-divided blocks and compared against each other to determine the similarity between blocks within the image. Once the matched blocks are detected, these blocks represent the manipulation of forgery performed in the image. Many block features have been proposed and utilized in image forensics. Lukas et al. [4] presented a block based matching algorithm based on discrete cosine transform (DCT) for CMFD. Prospec et al. [5] uses principal component analysis (PCA) to decrease the feature vectors. Luo et al. [6] extracted RGB components to represent block features. Li et al. [7] used singular value decomposition (SVD) and discrete wavelet transform (DWT) to detect passive forgery. Mahdian et al. [8] proposed a method based on 24 blur-invariant moments to locate duplicated regions. Memon et al. [9] used Fourier-Mellian transform (FMT) for feature extraction and dimension reduction. Ryu et al. [10] detect forgery using Zernike moments. Lynch et al. [11] used direct block comparison based on block features. In spite of the fact that block-based methods are successful in forgery detection, yet suffer from two fundamental drawbacks: 1) After the pre-processing stage, images are usually sub-divided into fixed size overlapping blocks, hence computational complexity will subsequently increase with increase in image size. 2) Most of the existing block-based methods are rigid to common post-processing operations for instance Gaussian blurring, JPEG compression, etc.



**Fig 2 Stepwise execution of block based method for CMFD [18]**

Lowe et al. [12] proposed a keypoint-based method, named *scale-invariant feature transform* (SIFT) for feature extraction. It initially finds features or interested pixel in a linear scale space and a descriptor vector is allocated. The feature itself is oriented by the dominant gradient direction, which makes it rotation invariant. Besides of its advantages, SIFT is unable to extract affine invariant features. Affine invariance allows analysing the features that undergoes local affine transformations. Substitute to the affine-invariant SIFT is *maximally stable extremal region* (MSER) [13].



**Fig 3 Stepwise execution of keypoint based method for CMFD [18]**

In this paper, we relate MSER with SVD to improve the performance of CMFD system. We observe that using MSER as a feature detection method enhances the accuracy of the extracted features and also make detection system robust against affine invariants. The rest of the paper is organized as follows. Section 2 presented a review of MSER and SVD. Framework of the proposed system and detailed explanation of the system is given in Section 3. Section 4 demonstrates the test results and the corresponding analysis of the experiment. At last Section 5 concludes the paper.

## II. REVIEW OF MSER AND SVD

### 2.1 Maximally Stable Extremal Regions

Maximally stable extremal regions (MSER) are a popular local invariant feature detection method. The MSER algorithm extracts from an image a number of covariant regions, called MSERs: an MSER is a stable connected component of some gray-level sets of the image.

The MSER detector can be informally described as follows [14] [15]; Assume an  $M \times N$  initially empty grid that corresponds to an  $M \times N$  intensity image. We start inserting all pixels of intensity of value 0 to their corresponding locations, then all pixels of intensity value of 1, 2, and so on, until all pixels are reinserted into their corresponding locations, and the image is completely restored. Equivalently, the intensity image is continuously threshold starting with threshold 0 up to 255 with a  $\Delta$  threshold increment. At each threshold, all pixels with values that fall below the current threshold are painted white and the remaining pixels are painted black. As the threshold is increasing, some white regions will show, some will merge, until ultimately all regions will merge into a single large one. In this process, we keep monitoring the size of each white region, i.e. its cardinality  $A(t)$ , as a function of the threshold value  $t$ . Then, an MSER is detected if  $a(t)$  has a local minimum, where:

$$a(t) = |A(t + \Delta) \setminus A(t - \Delta)| / |A(t)|,$$

In this case, the detected MSERs correspond to the bright regions. For dark MSERs, the inverted intensity image is used instead. The formal definition of the MSERs [19] is as follows:

**Definition 1:** Let  $A_1, A_2, \dots, A_{t-1}, A_t, \dots$  be a sequence a sequence of nested extremal regions, i.e.  $A_t \subset A_{t+1}$ . Extremal region  $A_t$  is maximally stable iff  $a(t) = |A(t + \Delta) \setminus A(t - \Delta)| / |A(t)|$  has a local minimum at  $t$ , where  $\Delta$  is the threshold increment.

The word 'extremal' refers to the property that all pixels inside the MSER have either higher (bright extremal regions) or lower (dark extremal regions) intensity than all the pixels on its outer boundary. The MSER is controlled by four main parameters, namely the threshold increment  $\Delta$ , the minimum and maximum size of each region, and the maximum area variation defined by the stability function  $a(t)$ . There are no optimal values for these four parameters. The lower the value of  $\Delta$ , the more accurate (but the slower) the algorithm becomes. Typically,  $\Delta$  is selected in the range of 4–7.

## 2.2 Singular value decomposition

Singular Value Decomposition (SVD) [17] is a dimension reduction technique which is known for its three important characteristics: robust to scaling, rotation invariant and high stability. While SVD is used for dimension reduction, it also proved itself for noise reduction, image compression and other areas. The algorithm for SVD is given by the below stated formula:

Let  $M$  be an  $m \times n$  image matrix of rank  $r$ , its SVD is given by the formula:

$$M = U\Sigma V^T$$

Where  $U$  is a  $m \times m$  matrix of the orthonormal eigenvectors of  $MM^T$ ,  $V^T$  is the transpose of a  $n \times n$  matrix containing the orthonormal eigenvectors of  $M^TM$ ,  $\Sigma \in \mathbb{R}^{m \times n}$  is a  $m \times n$  diagonal matrix of the singular values which are the square roots of the eigen values of  $M^TM$ , divided in the form of equation:

$$\Sigma = \begin{bmatrix} \Sigma_r & 0 \\ 0 & 0 \end{bmatrix}$$

Where  $\Sigma_r$  is a square diagonal matrix in  $\mathbb{R}^{r \times r}$ ,  $\Sigma_r = \text{diag}(\sigma_1, \sigma_2, \sigma_3, \dots, \sigma_r)$ .  $r$  is the rank of  $M$  that is equal to number of non-negative singular values. The positive diagonal entries in  $\Sigma_r$  are called the singular values of  $M$   
 $\sigma_1 \geq \sigma_2 \geq \sigma_3 \geq \dots \geq \sigma_r > 0$

As small singular values are responsive against noise while the largest singular value (LSV) contains most energy of each image block and has a good stability even when images suffer from minor distortions. Because of this property of SVD is incorporated in our algorithm.

## III. THE PROPOSED ALGORITHM

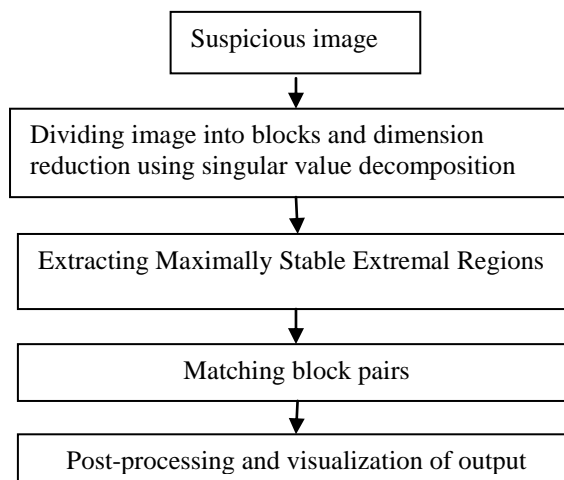
The aim of forgery detection is to determine whether an image contains a forgery or not. In CMF, regions or subpart of an image is copied, so detection algorithm should be capable to detect these regions. If algorithm try to detect forgery by comparing each pixel of image to its corresponding pixels, then computationally it becomes impossible to compare. To overcome the above stated problem, proposed method adopt blocking method in which the input image undergoes division into fixed size overlapping blocks and examine whether pairs of blocks are copied or not. Feature extraction and matching stage plays an important role in forgery detection because a good feature can not only represent the whole image, but also has robustness against post-processing operations, which makes detection algorithm to have lower computational complexity with high accuracy.

### 3.1 Algorithm Framework

Framework of the proposed method is explained below:

1. Convert the loaded input image as a gray image of size  $M \times N$ .
2. Converted gray scale image is divided into fixed size overlapping blocks.
3. Reducing dimension space using SVD.

4. Extracting MSER features from each MSER region.
5. Matching similar MSER features.
6. Isolated regions are removed and visualized the forged region.



**Fig 4 Flowchart of the proposed method**

### 3.2 Implementation details:

Detailed explanation of detection algorithm is given below:

**Step 1:** Pre-processing of input image

*Color Conversion:* The input image should be a gray scale image  $I$  of the size  $256 \times 256$ . If not, then first converted to a grayscale image using the standard formula:

$$Y = 0.299R + 0.587G + 0.114B$$

Where  $R$ ,  $G$ ,  $B$  are three color channels,  $Y$  is its luma component.

*Binarization:* The gray scale image is converted into binary forms to find out the region based on the connectivity of the component.

*Resizing:* The proposed forgery detection system is made for images of size  $256 \times 256$ . So in this step, the image size is made compatible for the detection algorithm. The images are resized to  $256 \times 256$  in size.

**Step 2:** Singular Value Decomposition (SVD) is used for sub-dividing the image into blocks and for dimension reduction.

In this step, input image is sub-divided into  $8 \times 8$  blocks followed by dimension reduction. The basic concept of SVD is to represent an image with size  $m \times n$  as a two-dimensional  $m \times n$  matrix. In this paper, image size used is  $256 \times 256$ . SVD is applied to this matrix to obtain the  $U$ ,  $\Sigma$  and  $V$  matrices, where matrix  $U$  is an  $m \times n$  orthogonal matrix. Matrix  $V$  is an  $n \times n$  orthogonal matrix and  $\Sigma$  is a  $m \times n$  diagonal matrix with singular values (SV) on the diagonal. Let  $M$  be an image matrix with  $M \in \mathbb{R}^{M \times N}$  of rank  $r$ , its SVD is given by the formula:

$$M = U\Sigma V^T.$$

**Step 3:** Feature Extraction

Now on the decomposed image, MSER is applied to extract features. Each  $8 \times 8$  sub divided block is assumed as an input image and a maximally stable region is detected from each block. This region is referred as a feature. Likewise, features are extracted from the whole image. The algorithm used for Feature Extraction is explained below:

```

Load Image I
Convert the input image I into gray scale. In this paper, range of S is 0-255.
  for i = 1 to all row of I
    for j = 1 to all row of I
      1. Find connectivity of components
      2. Check the neighborhood relation of components
      3. Define threshold of connectivity
         if connectivity size > Threshold
           region ( i, j) = I
           define the boundary of the region
MSER(I) = maximum stable boundary of region
    end
  store all MSER for an image
  end
end

```

**Fig 5 MSER Algorithm used for feature extraction**

#### Step 4: Matching

After the feature extraction, correlation based matching is performed. Correlation is a mathematical measurement of two or more features that indicate the level of change. The algorithm used for Matching is explained below:

```

-Load MSER feature set according to blocks
-Calculate size of MSER feature set as row and column
  for i = 1 to all row r
    for j = 1 to all row c
      load feature of each blocks
-Find distance (D) between block features and MSER
feature sets
  if D is minimum
    matching_ratio (blocks) = maximum
  else
    matching_ratio (blocks) = D
  end
-Find the position of maximum matching pints
- Represent as a copy-part, denote that points
  end
end

```

**Fig 6 Matching Algorithm used in the proposed method**

#### Step 5: Post-processing and visualization of the forgery

Morphological operations like area open technique, Filling, Boundary and region properties is applied to fill the holes in marked regions and remove the isolated blocks. Forgery, if present, is displayed in the form of patch.

#### IV.EXPERIMENTAL RESULTS AND ANALYSIS

Intel CORE™i5 and Matlab R2016b platform was used to carry all the experiments. Copy-move forged images were taken from benchmark dataset MICC-F220. This dataset contains 220 images of size 722 × 480 to 800 × 600. Experiment was carried on total 110 images, out of which 55 were forged and 55 were original images. Experimental analysis shows that accuracy of detecting forged images is approximately same with accuracy of detecting untampered images.

##### 4.1 Performance assessment

To practically implement the forgery detection, detection method must have both the capabilities: the first is that it should be capable to differentiate between forged and original images. Addition to this, the accuracy to correctly locate the duplicated area must be significant. The above mentioned parameters results in strong evidence to expose digital forgeries. Therefore, to achieve practical implementation, we assess the performance of the proposed method at both levels: at image level and at pixel level. At image level, the whole concentration is on the fact that whether a forged image is get detected or not and at pixel level, accuracy evaluation is centred. We keep a record of the some critical measures which are the number of correctly detected forged images  $T_P$ , the number of images that have been falsely detected as forged  $F_P$ , and the falsely matched forged images  $F_N$ . From these we compute the measures Precision (p) and recall (r) which is defined as follows:

$$p = \frac{T_P}{T_P + F_P} \tag{i}$$

$$r = \frac{T_P}{T_P + F_N} \tag{ii}$$

Where precision (p) denotes the probability that a detected tampering is truly a tampering and recall shows the probability that a doctored image is detected.

##### 4.2 Discussion of Results

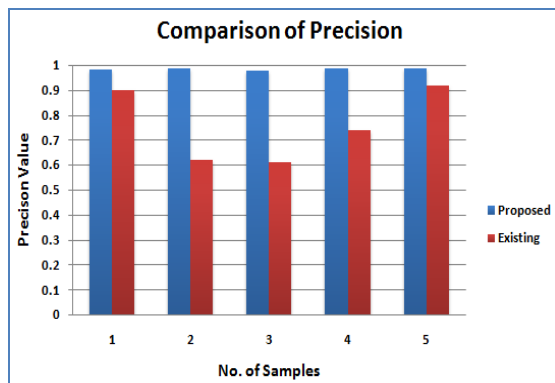
Pre-processing stage is performed in order to convert suspicious image to gray scale and for resizing. After the pre-processing, loaded image is sub-divided into fixed size blocks and feature vector space is reduced using SVD. Keypoints are extracted using MSER and visualization of forged image is displayed. Experiment is performed with different images of benchmark dataset MICC-F220 to show the effectiveness of the proposed system as depicted in figure 7.



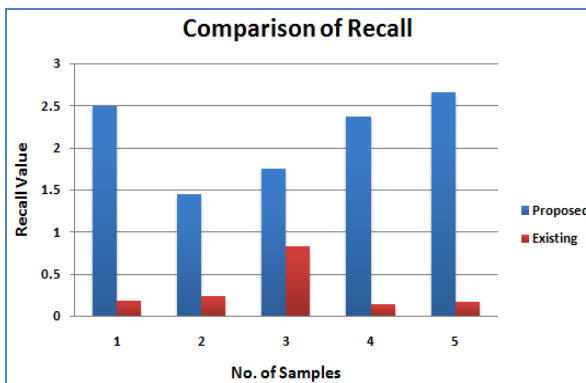
Fig 7 MSER Algorithm used for feature extraction

#### 4.2.1 Performance Results of Proposed Detection System and comparison with existing methods

Results have been compared with the Existing techniques on the basis of Precision and Recall to validate the results. Different graphs have been plotted for different matrices which are shown below and the graphs will prove that our technique will outperform the existing techniques in both the matrices.



**Graph 1 Comparison between Proposed and Existing Technique [19] in terms of Precision**



**Graph 2 Comparison between Proposed and Existing Technique [19] in terms of Recall**

## V. CONCLUSION

Copy-Move Forgery detection techniques still suffer from large number of issues and till now there is no unified Algorithm which can detect every type of forgery. As a result of it, the MSER feature detection algorithm has been implemented to resolve some of the issues. The implemented method shows robustness against geometric transformations and the proposed method shows robustness against geometric transformations and the proposed technique shows improvement in results in terms of Precision and recall as compared to existing techniques. The prime drawback of the existing methods is Automation that is the answers can be interpreted with the intervention of human only. Second drawback is that if we talk about copy-move forgery, then the use of these methods is computationally expensive. Thirdly as these techniques are applied to images only, we can extend the research on audios and videos. Fourthly at present there is no technique which can identify between the malicious forgery and just the retouching like artistic manipulation. The most challenging tasks is to develop a unified algorithm having capacity to detect any type of forgery.

## REFERENCES

- [1] C. Amsberry, Alterations of photos raise host of legal, Ethical issues. Wall Street Journal, Jan 1989.
- [2] J. K Tjldink, R. Verbeke, and Y. M Smulders, Publication pressure and scientific misconduct in medical sciences, Journal Empir. Respository, (9)5,2014, 64-71.
- [3] Hany Farid, Exposing digital forgeries in scientific images, ACM multimedia and security workshop, 2006.
- [4] J. Fridrich, D. Soukalm, and J. Lukas, Detection of Copy-Move Forgery in Digital Images, Digital Forensic Research Workshop, 2003, pp. 19-23.
- [5] Alin C Popescu, and Hany Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Department of Computer Science, Dartmouth College, Technical Report TR2004-515,2004.
- [6] W. Luo, J. Huang, and G. Qiu, Robust detection of region-duplication forgery in digital images, International Conference on Pattern Recognition, 4, 2006, 746-749.





- [7] Leida Li, shushing Li, and Hancheng zhu, An efficient scheme for detecting copy-move forged images by local binary patterns, *Journal of Information Hiding and multimedia signal processing*, 1(4), 2013, 46-56.
- [8] Babak Mahdian, and Stanislav Saic, Detection of copy-move forgery using a method based on blur moment invariants, *Forensic Science International*, 2(171), 2007, 180-189.
- [9] Sevinc Bayram, Husrev Taha Sencar, and Nasir Memon, An Efficient and Robust Method for Detecting Copy-Move Forgery, *IEEE Conference on Acoustics, Speech and Signal Processing*, 2009, 1053-1056.
- [10] Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee, Detection of Copy-Rotate-Move Forgery Using Zernike Moments, *International Workshop on Information Hiding*, Springer, 6387, 2010, 51– 65.
- [11] Gavin Lynch, Frank Y. Shih, and Hong-Yuan Mark Liao, An Efficient Expanding Block Algorithm for Image Copy-Move Forgery Detection, *Information Sciences*, Elsevier, 239, 2013, 253-265.
- [12] David G. Lowe, Distictive Image Features from Scale-Invariant Keypoints, *International Journal of Computer Vision*, Springer, 2(60), 2004, 91-110.
- [13] J. Matas, O. Chum, M. Urban, and T. Pajdla, Robust wide Baseline Stereo from Maximally Stable Extremal Regions, *Image and Vision Computing*, 10(22), 2004, 761-767.
- [14] Ron Kimmel, Cuiping Zhang, Alexander M. Bronstein, and Michael m. Bronstein, Are MSER Features Really Interesting ?, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 11(33), 2011.
- [15] Ehab Salahat, Hani Saleh, Safa Salahat, Andrzej Sluzek, Mahmoud Al-Qutayri, Baker Mohammad, and Mohammad Ismail, "Extended MSER Detection, *IEEE International Symposium on Industrial Electronics*, 2015.
- [16] Yanjun Cao, Tiegang Cao, Li Fan, and Qunting Yang, A Robust Detection Algorithm for Copy-Move Forgery in Digital Images, *Forensic Science International*, Elsevier, 1-3(214), 2012, 33-43.
- [17] Jie Zhao, and Jichang Guo, Passive forensics for copy-move image forgery using a method based on DCT and SVD, *Foresic Science International*, 233, 2013, 158-166.
- [18] Nor Bakiah Abd Warif, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Roziana Ramli, Rosli Salleh, Shahboddin Shamshirband, and Kim-Kwang Raymond Choo, Copy-Move Forgery Detection : Survey, Challenges and Future Directions, *Journal of Network and Computer Applications*, Elsevier, 75, 2016, 259-278.
- [19] Edoardo Ardizzine, Alessandro Bruno and Giuseppe Mazzola, "Copy-Move Forgery Detection by Matching Triangles of Keypoints," *IEEE Transactions on Information Forensic and Security*, vol. 10. No. 10, 2015.