Comparative Study of Recent CMFD Techniques: A Review

N Parashar

Department of Computer Engineering and Applications, GLA University Mathura, Uttar Pradesh, India

E-mail: nishtha.parashar@glau.ac.in

Abstract. Due to the ease in manipulation of digital images with various existing photo editing tools and softwares the task of authentication and identifying the reliability of digital image has become a major concern. Copy-move forgery detection (CMFD) is therefore known to be one of the key-domains in the latest digital image authentication study. Copy-move forgery is a passive approach in which a portion of an image is copied and then pasted onto the same image, resulting in a tampered image. In this paper, current developments in CMFD have been surveyed and a comparative evaluation of recent CMFD techniques has been done along with its advantages and limitations. Also, a detailed description of relevant copy-move forgery detection datasets is provided which will help the researchers to decide which dataset to choose for a given CMFD approach.

1. Introduction

In today’s digital world, images are considered as one of the significant means of communication among the people for interaction. Image authentication thus serves as a means of preventing digital images from being misused for unwanted use. It helps in ensuring that the given image is original without any manipulations. Thus, active approach and passive approach are the two approaches used in digital image forensics [1]. Digital watermarking is considered as one of the well-known active approach in which embedding of watermark is performed on the host image. However, the drawback here is that it needs to be embedded in advance on the given image. Therefore, passive methods such as copy-move forgery detection help to address this necessity of pre-processing. Figure 1 demonstrates the detailed classification of both active and passive areas of image forgery detection.

This paper aims to present, together with their advantages and limitations, a comparative evaluation of recent copy-move forgery detection techniques. Also, the detailed list of publicly available datasets is provided which will help the researchers in deciding suitable dataset for the given copy-move forgery detection approach.
2. Copy-Move Forgery
Copy-move forgery detection is a passive technique that involves copying and pasting different image areas onto the same image. Figure 2 contrasts an original image with its tampered counterpart produced by copy-move forgery [2]. At an initial stage, pre-processing of image is being done after that feature extraction is performed and then similarity match between features is accomplished. Figure 3 illustrates a generalised copy-move forgery detection (CMFD) workflow.

The numerous techniques used to detect copy-move forgery can be divided into two categories: block-based methods and key-point-based methods. In block-based methods, input image regions are analyzed to find candidate matches, while correspondence between points is found in key point-based methods [1] [7] [17].

3. Related Work
Due to lack of prior knowledge about the authenticity of the original image forensic methods are considered as blind in nature. Currently, various algorithms have been proposed by the researchers in the domain of detecting copy-move forgery.

J. Zhong et al. [1] developed a two-pass hash function representation and search method to improve the good score and high efficiency in detecting copy-move forgery. X. Wang et al. [2] introduced an adaptive key-point based method to find robust invariant features and screen out the wrong pairs. This method helps detect the use of copy-move forgery in a fast and effective manner. Another effective
approach premised on singular decomposition of value and Kolmogorov Smirnov test was proposed by B. Ahmed et al. [8] which helped in the reduction of false positive rate. G. Gani et al. [10] put forward a DCT and cellular automata-based approach for detecting forgeries under post processing attacks. In this, feature vectors were constructed using cellular automata based on the DCT coefficients. K.B. Meena et al. [11] suggested a tetrolet transform-based CMFD technique that increased accuracy considerably. A tetrolet transform based CMFD technique was proposed by K.B. Meena et al. [11] which improved the accuracy. Y. Zu et al. [12] introduced AR-Net based end to end neural network for enriching the feature representation. C. Chen et al. [3] proposed SIFT based invariant moments calculation and region growing strategy for identifying regions prone to copy-move forgery. Hybrid local feature extraction-based technique was developed by B. Soni et al. [4] which was an enhancement in CMFD methods. H. Huang et al. [5] introduced a key-point based method for finding relevant forensic information from an image using super pixel resolution and Helmert transformation. B. Elhaminia et al. [6] used the concept of Markov Random Field to deal with copy-move forgery detection and achieved an improved precision score. A CMFD method based on Binary Robust Invariant Scalable Key-points and image-blobs and proposed by P. Niyishanka et al. [13] proved to be effective against various post-processing attacks. Discrete Cosine Transform based detection of alteration in image was proposed by E.A. Vega et al. [14]. J.L. Zhong et al. [15] developed a dense moment feature index-based approach for detecting copy-move forgery in videos at the frame and pixel level. A. Roy et al. [16] proposed RLBP and g2NN based approach for addressing the problem of copy-move forgery for an identical but genuine object in an image. X. Tian et al. [18] developed a novel ORB feature extraction based novel similarity metric for effective and fast forgery detection.

4. Comparative Evaluation

Based on the survey done on the recent techniques/methods implemented by the researchers the comparative evaluation of the previous state of arts along with its benefits and limitations is provided in Table 1.

| Table 1. Comparative evaluation of existing techniques for CMFD |
|---------------------------------------------------------------|
| **Techniques** | **Benefits** | **Limitations** |
| Two-pass hashing feature illustration and search approach [1] | -Resistant against geometric attacks and post processing attacks.  
-Improved computational efficiency deprived of iterations. | -CMFD results can be further improved, one way is by fusing Deep Neural Network. |
| Fast and effective CMFD method through adaptive keypoint extraction and processing [2] | -False matched pairs are removed.  
-Duplicated regions are localized. | -The source and target areas are not distinguished in the matching pair. |
| Blind CMFD through SVD and KS test [8] | -Forgeries can be detected at pixel level  
-High precision rate is achieved.  
-Reduced false positive rate lesser than 4%.  
-Proved robust for post-processing techniques. | -Larger computational time. |
**CMFD approach using tetrolet transform [11]**

- Much accurate in identifying the size and shape of the forged region.
- Effective results under geometric transformations and post processing.
- Cannot detect forged regions in noisy and distorted images.

**Adaptive Attention and Residual Refinement Network for Copy-Move Forgery Detection [12]**

- At pixel level AR-Net identifies the forged and the respective actual region.
- Prediction mask is refined due to the use of AR-Net.
- Only single mode information is used in AR-Net.

**Rotational CMFD methodology via region growing strategies and SIFT [3]**

- Identifies the orientation difference among various copy-move regions.
- Matched key points and region growing method can be further improved.

**Geometric transformation invariant CMFD via hybrid local features [4]**

- Faster matching due to the use of SURF descriptor.
- Improved results for geometric transformation.
- Multiple forgeries cannot be identified precisely.
- Cannot identify forgery in highly similar regions.

**CMFD for image forensics through super-pixel segmentation and Helmert transformation [5]**

- Cost computation is less.
- Tampered regions are more precisely located due to the use of SLIC algorithm.
- Forged region is not immune to smooth, recurring, and symmetric patterns

**Probabilistic outline for copy-move forgery detection centred on Markov Random Field [6]**

- Improved precision.
- Energy minimization is undertaken using iterative method.
- Over segmentation due to SLIC.

### 5. Datasets

Due to the continuous advancements going on in the field of image forensic research a need of benchmark datasets is always there. A collection of both realistic and tampered images is provided in it which will help in finding more précised results for different techniques. A comprehensive overview of few publicly available datasets can be found in Table 2, which will help the researchers to decide which dataset to choose for a given CMFD approach.

| Dataset                  | Image Size                        | Total Images | Description                                      |
|--------------------------|-----------------------------------|--------------|--------------------------------------------------|
| IMD dataset [1][9]       | Average size of 3000×2300.        | 48           | The copy-move images are tampered from 48 high resolution PNG base images. |
GRIP dataset [2][11] | Images with the size 768×1024 or 1024×768 pixels. | 80 | It contains 80 original images of size 768 × 1024 or 1024 × 768.  
FAU dataset [2] | 3000×2000 pixels | 48 | This dataset is comprised of 48 high-resolution source images.  
MICC-F220 [6][7][13] | The resolution of the image lies between 722×480 to 800×600 pixels | 220 | In this dataset 110 images are original and 110 are manipulated.  
CoMoFoD dataset [7][8] [11] [12] [3] [13] | Varies from 512x512 to 3000x2000. | 200 | Each image is manipulated using 25 different combinations of tampering.  
MICC-F600 [4][6] | Varying from 800x533 to 3888x2592 pixels. | 160 | This dataset constructs the testing images by applying different manipulations on copy-move region.  
MICC-F2000 [4] | 2048 × 1536 images. | 2000 | Out of 2000 images 700 of them are tampered.  

6. Conclusion
In recent years, copy-move forgery detection has been one of the dominant areas of research. This paper aims at exploring various CMFD techniques. A comparative study of recent techniques has been made providing the advantage of choosing one technique over another along with its limitations. Also, description of relevant datasets for copy-move forgery detection is being provided which will help the researchers in the selection of the relevant datasets for efficient results for a given CMFD technique.

References
[1] J. Zhong and C. Pun, “Two-pass hashing feature representation and searching method for copy-move forgery detection”, Information Sciences, Vol. 512, pp. 675-692, 2019.
[2] X. Wang et al., “A fast and high accurate image copy-move forgery detection Approach”, Multidimensional Systems and Signal Processing, Vol. 31, pp. 857–883, 2019.
[3] Mahrishi M., Morwal S. (2020) “Index Point Detection and Semantic Indexing of Videos—A Comparative Review”. In: Pant M., Kumar Sharma T., Arya R., Sahana B., Zolfagharinia H. (eds) Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing, vol 1154. Springer, Singapore.
[4] B. Soni, P. K. Das and D.M. Thounaojam, “Geometric transformation invariant block-based copy-move forgery detection using fast and efficient hybrid local features”, Journal of Information Security and Applications, Vol. 45, pp. 44-51, 2019.
[5] H. Huang and A.J. Ciou, “Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation”, EURASIP Journal on Image and Video Processing, Vol. 68, 2019.
[6] B. Elhaminia, A. Harati and A. Taherinia, “A probabilistic framework for copy-move forgery detection based on Markov Random Field”, Multimedia Tools and Applications, Vol. 78, pp. 25591–25609, 2019.
[7] P. Niyishaka and C. Bhagvati, “Copy-move forgery detection using image blobs and BRISK feature”, Multimedia Tools and Applications, Vol. 79, pp. 26045–26059, 2020.
[8] B. Ahmed, T. A. Gulliver and S. Zahir, “Blind copy-move forgery detection using SVD and KS test”, SN Applied Sciences, Springer, 2020.
[9] K.B. Meena and V. Tyagi, “A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature Transforms”, Multimedia Tools and Applications, Vol. 79, pp. 8197–8212, 2020.

[10] G. Gani and F. Qadir, “A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata”, Journal of Information Security and Applications, Vol. 54, 2020.

[11] K.B. Meena and V. Tyagi, “A copy-move image forgery detection technique based on tetrolet transform”, Journal of Information Security and Applications, Vol. 52, 2020.

[12] Y. Zhu, C. Chen, G. Yan, Y. Guo and Y. Dong, “AR-Net: Adaptive Attention and Residual Refinement Network for Copy-Move Forgery Detection”, IEEE Transactions on Industrial Informatics, Vol. 16, pp. 6714 – 6723, 2020.

[13] P. Niyishaka and C. Bhagvati “Copy-move forgery detection using image blobs and BRISK feature”, Multimedia Tools and Applications, Vol. 79, pp. 26045–26059, 2020.

[14] E.A. Vega, E.G. Fernandez, A.L.S. Orozco and L.J.G. Villalba “Copy-move forgery detection technique based on discrete cosine transform blocks features” Neural Computing & Applications, 2020.

[15] J.L. Zhong, C. M. Pun and Y.F. Gan, “Dense moment feature index and best match algorithms for video copy-move forgery detection”, Information Sciences, Vol. 537, pp. 184-202, 2020.

[16] A. Roy, R. Dixit, R. Naskar and R.S. Chakraborty, “Copy-Move Forgery Detection with Similar But Genuine Objects”, Vol. 755, pp. 65-77, 2020.

[17] K. Sunitha, A. N. Krishna, “Efficient Keypoint based Copy Move Forgery Detection Method using Hybrid Feature Extraction”, International Conference on Innovative Mechanisms for Industry Applications, pp. 670-675, 2020.

[18] X. Tian, G. Zhou and M.Xau, “Image copy-move forgery detection algorithm based on ORB and novel similarity metric”, IET Image Processing, Vol.10, pp. 2092-2100, 2020.