

Blur-Invariant Copy-Move Forgery Detection Technique Utilizing Hu's Invariant Moments for Video Forensics

B. Prabhakar

Department of ECE, JNTUH College of Engineering, Jagtial, Telangana, India.

Abstract - With the increase in interchange of data, there is a growing necessity of security. Considering the volumes of digital data that is transmitted, they are in need to be secure. Among the many forms of tampering possible, one widespread technique is Copy Move Forgery (CMF). This forgery occurs when parts of the video frame are copied and duplicated elsewhere in the same video frame. There exist a number of algorithms to detect such a forgery in which the primary step involved is feature extraction. The feature extraction techniques employed must have lesser time and space complexity involved for an efficient and faster processing of media. Also, majority of the existing state of art techniques often tend to falsely match similar genuine objects as copy move forged during the detection process. To tackle these problems, the paper proposes a novel algorithm that recognizes a unique approach of using Hu's Invariant Moments and Log-polar Transformations to reduce feature vector dimension to one feature per block simultaneously detecting CMF among genuine similar objects in an video frame. The qualitative and quantitative results obtained demonstrate the effectiveness of this algorithm.

Keywords—copy move forgery; Hu's moments; Log-polar transformations; region duplication forgery;

I. INTRODUCTION

With the advancements in imaging technologies, the digital video frames are becoming a concrete information source. Meanwhile, a large variety of video frame editing tools have placed the authenticity of video frames at risk. The ambition behind the video frame content forgery is to perform the manipulations in a way, making them hard to reveal through the naked eye, and use these creations for malicious purposes. For instance, in 2001, after the 9/11 incident, several videos of Osama bin Laden over the social media were found counterfeited through the forensic analysis [1]. In the same way, in 2007, an video frame of tiger in forest forced the

people to believe in the existence of tigers in the Shanxi province of China. The forensic analysis, however, proved the tiger to be a "paper tiger" [2]. Similarly, in 2008, an official video frame of four Iranian ballistic missiles was found to be doctored, as one missile was revealed to be duplicated [3].

Hence, the famous saying "seeing is believing" [4, 5] is no longer effective. Therefore, ways that can ensure the integrity of the video frames especially in the evidence centered applications are required. In recent years, an exciting field, digital video frame forensics, has emerged which finds the evidence of forgeries in digital video frames [6]. The primary focus of the digital video frame forensics is to investigate the video frames for the presence of forgery by applying either the active or the passive (blind) techniques [2]. The active techniques such as watermarking [7] and digital signatures [6] depend on the information embedded a priori in the video frames.

However, the unavailability of the information may limit the application of active techniques in practice [8]. Thus, passive techniques are used to authenticate the video frames that do not require any prior information about them [9–10].

II. LITERATURE REVIEW

Fridrich et al [1] proposed the first CMFD algorithm using exact match technique where every pixel was counted as a feature and robust CMFD algorithm using DCT coefficients as features of the blocks. Huang et al [2] improved the DCT algorithm to compute the results faster. Farid and Popescu [3] proposed an algorithm to detect CMFD using considerably less feature vector dimension using Principle Component Analysis (PCA) algorithm. Kang et al [4] proposed an algorithm to curb copy move forgery using Singular Value Decomposition (SVD) algorithm which was effectively robust against induced noise. Zhang et al [5] used Discreet Wavelet Transform (DWT) to reduce the complexity of the program as compared to the other existing schemes. Yang et al [6] used

Dyadic Wavelet Transform by decomposing the forged video frame into four sub-bands and removing the low frequency components in it. Muhammad et al [7] proposed a similar algorithm using DyWT which was capable of utilizing both low and high frequency components in an video frame to eliminate as many false positives as possible. Rahul et al [8] proposed a blur invariant CMFD technique using SWT-SVD algorithm. A method using Fourier Mellin Transform was developed in [9] which proved to be efficient in detecting forgery in highly compressed video frames. Guangjie et al [10] proposed an algorithm using Hu's invariant moments [11], proving its robustness against several post processing techniques. Huang et al [12] proposed an algorithm using DWT and SVD for robust feature extraction. The PCA algorithm was further developed by Sunil et al [13] to increase its robustness to JPEG compression and noise using DCT-PCA algorithms. PCA is mainly used to reduce the feature vector dimension in the given matrix.

III. PROPOSED METHOD

We now propose a novel algorithm to reduce the feature vector dimension and simultaneously making the algorithm more effective in differentiating between similar objects in video frame and actual copy move forgery detection using Hu's invariant moments and log-polar transformations. This algorithm can be discussed in detail as follows:

Algorithm 1: Proposed Method

Input: Copy Move Forged video frame.

Output: Binary video frame showing the regions of duplication.

- Input the forged video frame of size $M \times N$, convert it to grey scale.
- Divide the video frame into overlapping blocks of size $B \times B$.
- Calculate Hu's invariant moments for each of the divided blocks in step 2 up to 7th order.
- Apply the log-polar transformation over each of the Hu's invariant moment order.
- Use 'format long' to check on every value up to its respective 15th decimal.
- Calculate the sum of all 7 invariant moments produced for each block and write this value into a new linear column matrix.

- Add two additional columns to the matrix formed in step 5 indicating the location of the corresponding block's first pixel.
- Lexicographically sort the formed matrix.
- Now check if adjacent rows first value is the equal up to 15th decimal digit.
- If the values match, check the number of times a value is repeating. Also, compute the Euclidean distance between the matching blocks.
- Apply user specified threshold to eliminate false matches.
- Create a binary video frame with one's in the duplicated regions as a result of detecting the forgery.

The previous state of art CMFD process using Hu's invariant moments used moment values up to 4th order as features of each block, mainly because of the reason that the value of Hu's invariant moments above 4th order generally tend to go beyond 10-6 units reducing its impact over generation of features. Generation of four invariant moments sufficed the purpose of distinguishing the block among others. In this paper, we propose an algorithm where all the computed Hu's moments are summed to produce one feature value that can distinguish the block from other blocks. Summing up to only 4th order moments leads to several false matches. Therefore, in order to reduce false matches to the maximum extent, we produce 7 invariant moments and apply log-polar transform to convert the values beyond 10-6 units to significant floating values.

The accuracy of identifying blocks can further be increased by using 'long format' variables which could display and compute the values generated up to 15th decimal number. Here, if the feature value's matches with one another up to 15th decimal we can have a benefit of doubt that they are duplicated regions. False matches among these are further curbed by calculating Euclidian distance among the matched blocks. The idea here is that, if a cluster of blocks are copied from a region and are duplicated in the same video frame, the distance between corresponding copied and duplicated block must be the same for every matched pair. A user-specified threshold is applied onto the video frame to eliminate singular false positives and the remaining matched regions are marked as copy-moved.

Certain feature extraction algorithms such as Scale Invariant Feature Transform (SIFT) or Speeded up Robust Features (SURF) are commonly used for CMFD purposes. These algorithms mark the features on objects present in the video frame which provides an advantage of having more robustness towards post processing techniques and geometrical transformations over the pasted region. Since, these algorithms concentrate their key features over objects and drastic pixel flow changes in the video frame, they often tend to confuse between copy move forgery and genuine similar products in the same video frame. Using Hu's invariant moments and log-polar transformations to calculate one

feature value per block can reduce the chance of false representation over two or more genuine similar products. Hu's moments are sensitive towards the slightest changes in the pixel values which helps us distinguish between similar products since it's practically impossible to have two or more genuine elements in an video frame with exactly the same corresponding matching pixels due to the influence over environmental factors, illumination factors and many more. Moments have well known applications in video frame processing, computer vision, machine learning and other related fields which are normally used to derive invariants with respect to specific transformation classes.

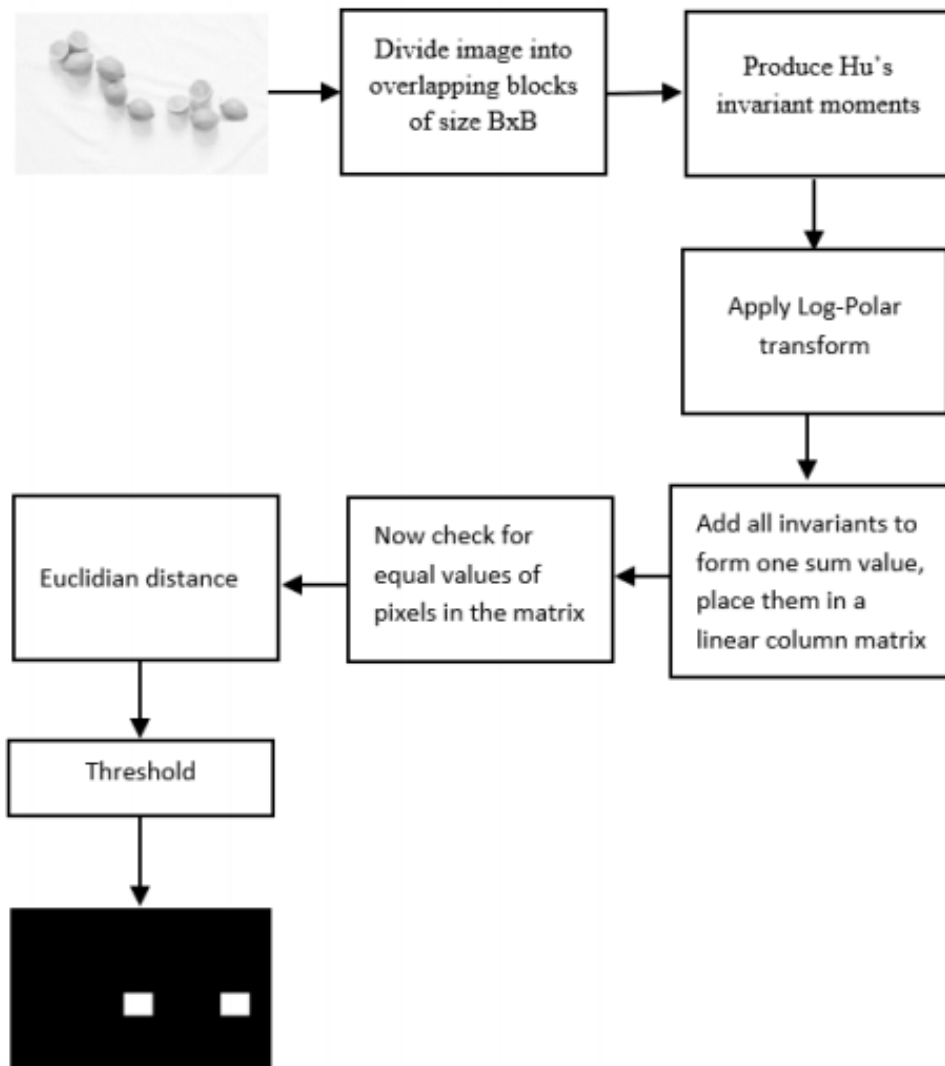


Fig. 1: Proposed block diagram for copy move forgery detection.

IV. EXPERIMENTAL RESULTS

A set of 105 video frames from the official database MICC-F220, as well as other grey scale video frames obtained by manual forging process were chosen for the experimental analysis. The video frames were chosen from diversified environments, varied illumination factors, weather conditions and a varied range over pixel clarity. We chose the standard size of the video frame to be 256 x 256 and used a constant block size of 8 x 8 in order to attain the best possible results in

terms of precision and accuracy. All the experiments were conducted in MATLAB 2016a software with long format variables associated in the program.

The qualitative results obtained are visually demonstrated in Fig 2. Now we make an attempt to quantitatively measure the effectiveness of the proposed Algorithm 1. To measure the performance Accuracy (A), we define Accuracy [8] as

$$Accuracy = \frac{Number\ of\ correctly\ detected\ copy - moved\ pixels}{Number\ of\ pixels\ actually\ copy - moved} \times 100\%$$

The performance accuracy (A) was calculated for different forgery sizes ranging from 10% to 40% of the video frame, meaning that, 40 % of the video frame was copied and duplicated in another region of the same video frame. Table -1 shows a comparative analysis of the results obtained by the proposed algorithm with the existing state of art techniques

with a varied duplication size from 10% to 40%. The highest Performance Accuracy (A) observed and the average Performance Accuracy Values calculated are lucidly displayed for a comprehensive analysis of the effectiveness of proposed algorithm as compared to the existing state of art techniques.










Samples	Original Image	Forged Image	Forgery detected
image 1			
Image 2			
Image 3			

Fig 2. Results obtained through Algorithm 1.

Table-1. Performance Accuracy (A) comparison

Method	No. of Frames	Accuracy - Highest	Accuracy - Average
PCA [3]	10	96.7870	96.7588
	20	96.9130	96.9095
	30	97.1671	97.1436
	40	97.7945	97.7645
SVD [4]	10	97.6309	97.6092
	20	98.1880	98.1576
	30	98.4924	98.4754
	40	98.8730	98.8311
DCT [1]	10	97.8672	97.2254
	20	97.4396	97.4123
	30	97.6434	97.5978
	40	98.0624	98.0232
DWT [5]	10	98.0857	98.0838
	20	98.1490	98.1464
	30	98.2210	98.2171
	40	98.2840	98.2780
DyWT [7]	10	98.0027	97.9892
	20	98.3641	98.3471
	30	98.5950	98.5455
	40	98.7889	98.7091
Zernike [6]	10	98.8179	98.8015
	20	98.9674	98.9372
	30	99.4017	99.3908
	40	99.4398	99.4199
SWT-SVD [8]	10	99.0626	99.0362
	20	99.1391	99.1316
	30	99.4366	99.4204
	40	99.4492	99.4307

Proposed Algorithm	10	99.5369	99.4549
	20	99.4569	99.4100
	30	99.4200	99.3876
	40	99.4173	99.3821

V. CONCLUSION

Passive forensics technology of digital video frame is one of the rapidly growing fields of research. Our brief review of video frame CMFD technologies indicates that the research is still in the phase of vigorous development and has a huge potential for the future research and development applications. Two classical models of copy-move forgery and two frameworks of CMFD technologies are presented at first. Then, block-based and key point-based CMFD methods are reviewed from different aspects, respectively, including the classical CMFD technologies and the state-of-the-art algorithms for CMFD in recent several years. The performance evaluation criterions and frequently used datasets for evaluating the performance of the CMFD schemes are collected. The future directions of this topic are given at last. With the help of the advanced technologies, some CMFD schemes with high performance are expected to become standard tools in the future. We also hope that this survey will provide related information to scientists, researchers, and relevant research communities in this field. The investigation on video frame forensics is still a continual, sustainable process and it will continue to explore forensics technologies with high accuracy and robustness.

VI. REFERENCES

- [1]. Fridrich, A. J., Soukal, B. D., & Lukáš, A. J. (2003). Detection of copy-move forgery in digital video frames. In in Proceedings of Digital Forensic Research Workshop.
- [2]. Huang, Y., Lu, W., Sun, W., & Long, D. (2011). Improved DCTbased detection of copy-move forgery in video frames. *Forensic science international*, 206(1-3), 178-184.
- [3]. Farid, A.P., Popescu, A.C.: 'Exposing digital gorges by detecting duplicated video frame region'. Technical report, Hanover, Department of Computer Science, Dartmouth College, USA, 2004.
- [4]. Kang, X., & Wei, S. (2008, December). Identifying tampered regions using singular value decomposition in digital video frame forensics. In *Computer Science and Software Engineering, 2008 International Conference on* (Vol. 3, pp. 926-930). IEEE.
- [5]. Zhang, J., Feng, Z., & Su, Y. (2008, November). A new approach for detecting copy-move forgery in digital video frames. In *Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on* (pp. 362-366). IEEE.
- [6]. Yang, J., Ran, P., Xiao, D., & Tan, J. (2013). Digital video frame forgery forensics by using undecimated dyadic wavelet transform and Zernike moments. *J. Comput. Inf. Syst*, 9(16), 6399-6408.
- [7]. Muhammad, G., Hussain, M., & Bebis, G. (2012). Passive copy move video frame forgery detection using undecimated dyadic wavelet transform. *Digital Investigation*, 9(1), 49-57.
- [8]. Dixit, R., Naskar, R., & Mishra, S. (2017). Blur-invariant copymove forgery detection technique with improved detection accuracy utilising SWT-SVD. *IET Video frame Processing*, 11(5).
- [9]. Bayram, S., Sencar, H. T., & Memon, N. (2009, April). An efficient and robust method for detecting copy-move forgery. In *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on* (pp. 1053-1056). IEEE.
- [10]. Liu, G., Wang, J., Lian, S., & Wang, Z. (2011). A passive video frame authentication scheme for detecting region-duplication forgery with rotation. *Journal of Network and Computer Applications*, 34(5), 1557-1565.
- [11]. Li, Y. (1992). Reforming the theory of invariant moments for pattern recognition. *Pattern recognition*, 25(7), 723-730.
- [12]. Huang, D. Y., Huang, C. N., Hu, W. C., & Chou, C. H. (2017). Robustness of copy-move forgery detection under high JPEG compression artifacts. *Multimedia Tools and Applications*, 76(1), 1509-1530.