A Keypoint Based Technique To Detect & Localize Copy Move Forgery In Digital Images

Navdeep Kanwal, Akshay Girdhar, Lakhwinder Kaur, Jaskaran Singh Bhullar

Abstract: Images were used to be most authentic source of information at one time but with the advancement in the technology, it is very easy now days to manipulate them. This paper deals with such manipulation in general and specifically for copy-move forgery attack on the digital images. The paper present a technique for identification of copy-move forgery and its localization by using keypoints extracted through ORB (oriented FAST and rotated BRIEF) features followed by region based extraction. The proposed techniques takes an edge over the block based forgery detection techniques due to their high computational load. Localization of the forgery in the images has been done by using region based approach using statistical moment features. The technique has been evaluated qualitatively and quantitatively in the last and has been evaluated against the existing state-of-the-art methodologies. The proposed technique achieves a high precision of 96.67% and thus can be used to detect and localize copy-move forgery in the images.

Index Terms: Copy-move forgery, ORB, keypoints, Region grow, forgery localization, image moments, forgery attack

1 INTRODUCTION

Digital pictures can be noticeable everywhere in newspapers, criminal proceedings as evidence and in the whole internet, one of the primary sources of information today. The ongoing evolution of digital photography and specialized software available for image manipulation (e.g. photoshop etc.) led to an enormous number of manipulated images without any clue of being tampered, as we call it a digital offense. In most of the cases a person cannot evaluate if a multimedia message or an image is genuine or not. Therefore there is a need of significant research in tampering detection techniques to determine the authenticity. Digital image forensics is an area in which images from a specific scenario are analyzed to detect credibility and authenticity via several means [1]. A famous example of image tampering has happened in 2004 when democratic candidate in American presidential election and a famous Hollywood actress sharing a stage was just tampered The existence of forgery can be determined by implementing the active and passive approaches of forgery detection [2] .

1.1 Active Approach

Pre-extracted or pre-embedded data about an image is required to detect forgery in this approach [3]. Digital watermarking, digital signature and steganography are the main components of an active approach, each of which can be implemented in the image acquisition phase. Digital watermarking is the technique to hide text or a mark inside the original image that may be validated for the authenticity and integrity of the image whenever there is doubt of image manipulation. The digital watermarks can be Invisible-Robust watermark, Visible watermark, Invisible-Fragile watermark or Dual watermark [4].

- *Navdeep Kanwal is currently pursuing Ph D in Computer Science & Engineering in I.K.G. Punjab Technical University, India. Email: navdeepkanwal@gmail.com*
- *Akshay Girdhar is Professor, IT, at GNDEC, Ludhiana, India*
- *Lakhwinder Kaur is Professor, CSE, at Punjabi University, Patiala, India*
- *Jaskaran Singh Bhullar is Professor, App. Sci., at MIMIT, Malout, India*

At the time of capturing, a watermark must be added which will restrict this strategy to digital cameras that are particularly designed for this purpose and this is the major limitation of digital watermarking [5]. Cryptography implies to keep messages confidential, and the digital signature is like a tool of cryptography [6]. Steganography may also be a form of digital signature, in which the important information is to be placed secretly into an image in such a way so that this is not accessible in general.

1.2 Passive Approach

No historical information about an image is needed in case of the passive or blind approach for forgery detection [7]. Such approaches can be further classified into dependent and independent forgery [8]. Dependent forgery includes copy-move and copy-paste (splicing). Copy and paste an image fragment into the same image at some other location is referred to as copy-move forgery whereas copy and then paste the fragment of one image onto some other image is called splicing or copy-paste forgery. Copy-Move forgery can be identified by using three procedures i.e. Brute force matching, Block-based methods and Keypoint based methods. The brute force strategy involves an exhaustive search on the image and may be clubbed with autocorrelation [1]. The image is used as an array in it and an exhaustive search to determine matching segment with circularly shifted versions, and autocorrelation is performed to determine location change [3]. In the block based techniques, the image may fragmented into overlapping or non-overlapping blocks and afterwards, rather than detecting the entire duplicated region, the forgery is detected as connected image blocks that are copied and moved [9], [10]. The block-based strategy uses algorithms including Principle Component Analysis (PCA), Singular Value Decomposition (SVD), Discrete Wavelet Transform (DWT) [11] and Discrete Cosine Transform (DCT)[12]. The block based techniques involve a lot of block comparisons causing slow detection speed. In order to avoid the computational issue of block based approach, keypoint based technique is proposed. Speed-up Robust features (SURF), Scale Invariant feature Transform(SIFT)[13] and Harris corner Detector [3] are keypoint-based methods that may be used to identify copy-move image forgery.

1.3 Image Forgery Detection Framework

In the CMFD framework, keypoint and block-based techniques

are two alternatives for image preprocessing phase [14]. This phase is used to enhance the features of an image by removing unwanted distortions (i.e. noise etc.). The most frequently used procedure in this phase is the conversion of RGB color channel to grayscale. Afterwards, in the feature extraction phase, block-based techniques subdivide an image into square or circular blocks and then relevant features(i.e. Intensity, texture, DCT, DWT, log-polar transform) can be extracted from these blocks and compare with each other to examine the similar type of blocks [8]. Block division is eliminated in case of keypoint based approach. Then depending on the extracted features matching techniques can be implemented and sometimes post-processing operations may be required for tampering, which includes manipulations such as localization of copy-move forgery[3].

2 LITERATURE REVIEW

SIFT-based technology is the most prevalent keypoint based technique in CMFD [15] and it was first proposed and designed as robust keypoint extractor against scale and rotation transformation [8]. To identify the copy-move forgery in digital images, An effective and reliable technique based on feature matching is suggested in [16]. The advantage of the technique is that it provides good performance on compressed images for rotation, scaling and other post image processing operations, but it is not appropriate for identifying the small-size tampered areas. In other paper three procedures presented by the author [17] includes keypoint clustering and matching with the texture evaluation. The goal is to find variations of a copied part, for example bunch of points, at that point to validate results and dispense with false positives, the surfaces of similar areas are analyzed. The results demonstrate great detection accuracy and less number of false matches but have failed in the homogeneous region because the homogeneous region has no key points. The author of [18] describes a different technique that focuses on the image SIFT feature where the Best-Bin-First algorithm is used for keypoint matching. These algorithms are reliable against post-processing and the detection accuracy is very high. In other technique, a particular image is divided into four sections namely LL, LH, HL and HH by implementing DWT [19]. Then SIFT is applied on LL section because it contains majority of the information to excerpt the image features for finding the image descriptor and then to find whether the given image is forged by finding the similarities between various descriptor vectors. High detection accuracy (94%) and decreased computational complexity in order to be compared with other techniques [20]. However, the suggested method is used to identify only copy move tampering. Another technique to deal with copy move forgery is proposed by [21] in which SIFT characteristics are compared initially and analogous feature points are then paired. Then, to eliminate falsely matched points, a distance evaluation is performed. It extracts the normalized RGB color feature of matched point neighbor-hoods and comparisons are made between pairs generated by the prior phase. Ultimately revised Gabor texture feature is used by implementing statistical methods to rid of the remaining false matched pairs and final identification results are displayed. The test findings indicate that the technique is resistant to complicated geometric transformation but that effectiveness needs to be improved in a large image with an enormous amount of key points. In 2011, [22] proposed to enhance the SIFT strategy by introducing hierarchical clustering to the SIFT key points and suggested a SIFT-based detection technique that detects geometric transformations used in a copy-move forgery and then estimates them. The advantage of this methodology is that the efficient matching with g2NN is efficient in dealing with multiple cloning but in the case of the highly uniform texture area, improvements are necessary. Authors in [23] presents a keypoint-based strategy for the identification of copy-move forgery to improve the efficiency of the SIFT technique. For the purpose, a rapid method is proposed in [24] to detect copy-move forgery based on SURF (Speed up Robust Features). The SURF descriptors helps to get invariance towards rotation, scaling, etc but the manipulated area and its border are not automatically located and it was a major drawback of the proposed algorithm. Author of [25] introduced techniques that combine SURF with DWT and DyWT. The primary goal for this strategy is to acquire distinctive and robust technique for detecting forgery of copy-move images and to be prepared to maintain multiple attacks as well. We can say from the outcomes achieved that the suggested algorithm has a better precision rate as well as a recall rate. Recently in 2019, using the k-nearest neighbor and SURF technique author [26] introduced a technique for digital images to identify copy-move forgery. It provides lower computational costs and producing the algorithm more appropriate for larger images. Authors in [27] have also suggested a technique to identify copy-move forgery using keypoints. ORB (Oriented Fast and Rotated Brief) is highly rapid binary descriptor introduced in 2011 [28]. ORB is invariant to rotation and noise-resistant and an alternate for SIFT and SURF. Higher effectiveness and performance compared to other common features of ORB. Four separate measures to resolve the problem of wrong consistency and robustness in the detection of forgeries are included in a paper [29] i.e. Identify the pyramid scale space, remove the ORB scaled function, equate it to the feature and then eradicate the wrong compatibility. Not just the duplicated areas are identified in the proposed technique, but geometric transformations and post-processing in forged areas are also determined. The procedure for tampering detection of high-resolution images is still time-consuming, which was the primary drawback of this technique using ORB keypoints.

3 PRESENT WORK

The accuracy has been constantly questioned in re-enacting source and details in digital images. Because of its implications in almost every area, it introduced the necessity for image forgery detection and location. The present paper proposes a methodology for detection of copy move forgery in the images, as explained in following sections and elaborated in Fig. 1.

4 PROPOSED METHODOLOGY

4.1 Preprocessing

An Image may be a 24-bit RGB image or 8-bit gray image. The proposed methodology uses 8-bit images for further processing, so the image under consideration is pre-processed to transform it into gray image. It can be achieved by using (1)

$$0.2989 * R + 0.5870 * G + 0.1140 * B \quad (1)$$

4.2 Feature Extraction

Numerous techniques are used for image keypoint extraction, such as Scale-Invariant Transforming Function (SIFT), Speed Up Robust Feature (SURF) and ORB (Oriented FAST and Rotated BRIEF). Although the SIFT keypoint detector and descriptor is more than ten years old and it has been substantially successful for many tasks. But indeed, it is not always effective in scenarios like biometric authentication systems and in other unreliable real-time scenarios [30]. Therefore, to improve efficiency and reduce computation cost, SIFT technology is replaced with SURF in some of the scenarios. An alternative for SIFT and SURF is ORB, a very fast binary descriptor based on a BRIEF (Binary Robust Independent Elementary Features) descriptor and a FAST (Features from accelerated segment test) keypoint detector, and that's why labelled it as Oriented FAST and Rotated BRIEF. Considering their better performance and effectiveness for computational cost, both of these techniques have been selected. Due to its increased speed and efficiency, and low memory requirements compared to the SURF and SIFT descriptors, ORB descriptor is considered as better. A definite orientation element is applied to FAST by using the intensity centroid cloud mechanism, which utilizes a reliable measure of corner orientation [30].

oFAST: FAST Keypoint Orientation

FAST detector and its variants (FAST-ER, FAST-9 and FAST-12) are the strategies used to identify the keypoints in real-time systems effectively but there was a lack of orientation component. oFAST is the effectively determined orientation applied to the FAST. FAST points in the image are first identified by determining the intensity threshold between the core pixel and the pixels in a circular ring around the core.

Due to less robustness of FAST, the intensity centroid(IC) strategy is applied here [31]. IC has been an effective procedure for corner orientation that assumes the intensity of corner is an offset from its center and is used to measure the orientation vector. The patch moments used to identify the centroid can be described as in (2).

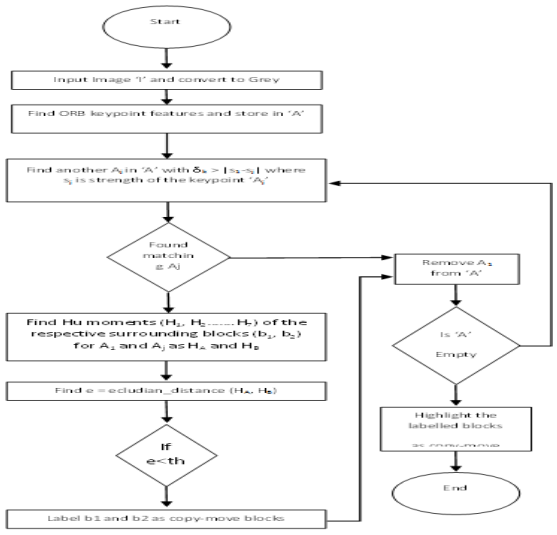


***Fig. 1**. Proposed Methodology*

$$\boldsymbol{m_{pq}} = \sum_{x,y} \boldsymbol{x^p\, y^q I(x,y)} \quad (2)$$

where, m_{pq} is $(p+q)^{th}$ order moment of an image and its intensity is I(x,y) which varies with x and y coordinates. Thus, we can identify the centroid by using the moments in (2) as in (3).

$$\boldsymbol{C} = \left(\frac{\boldsymbol{m_{10}}}{\boldsymbol{m_{00}}}, \frac{\boldsymbol{m_{01}}}{\boldsymbol{m_{00}}}\right) \quad (3)$$

We have to get a vector from the corner's center O to the centroid $\overrightarrow{\text{OC}}$ and the patch orientation is determined in (4).

$$\boldsymbol{\theta} = \boldsymbol{atan2(m_{01}, m_{10})} \quad (4)$$

In this equation, atan2 represents quadrant-aware form of arctan. Centroid gives consistently good orientation, also against the maximum noise in the image. The intensity centroid (IC) performs much better in comparison with BIN and MAX method for retrieving the orientation of falsely tilted or rotated noisy patches [28].

rBRIEF: Rotation-Aware Brief

Another feature descriptor is BRIEF which uses simple binary tests among pixels in a smooth image patch while rotation invariance is missing in BRIEF descriptor. Therefore, another step of learning is incorporated in r-BRIEF (Rotation aware BRIEF) for finding less correlated binary test [31], and it is the second component of ORB. BRIEF [32] descriptor is bit string description of the image patch created from a series of binary intensity tests to ensure an effective BRIEF rotation operator. Take a smoothened image patch p and the binary test τ has been determined as in (5).

$$\tau(p; x, y) = \begin{cases} 1 : p(x) < p(y) \\ 0 : p(x) \geq p(y) \end{cases} \quad (5)$$

where the intensity of p is represented by p(x) at point x. The feature, considered as the patch function can then be describe n binary tests as a vector by:

$$f_n(p) = \sum_{1 \leq i \leq n} 2^{i-1}\, \tau(p; x_i, y_i) \quad (6)$$

Several forms of test distributions are taken into consideration in [32],[28] that uses a Gaussian distribution near to the center of the patch and selects the length of a vector n = 256. For a given set of features of n binary tests at a specific location (x_k, y_k), the 2n matrix should be expressed as in (7).

$$S = \begin{pmatrix} x_1 \dots \dots \dots x_n \\ y_1 \dots \dots \dots y_n \end{pmatrix} \quad (7)$$

Now, we have to compute the "steered" version S_θ of S:

$$S_\theta = R_\theta S \quad (8)$$

here, θ represents patch orientation and R_θ is the corresponding rotation matrix. Finally, the steered BRIEF operator can be published as

$$\boldsymbol{g_n(p, \theta) = f_n(p) | (x_i, y_i) \in S_\theta} \quad (9)$$

4.2 Keypoint Matching

After extracting all the keypoints, their parameters are stored in an array A. This array is then sorted lexicographically against the strength of the keypoints. The array is scanned to find another A_j in 'A' with $\delta_k > |s_1 - s_j|$ where s_j is strength of the keypoint 'A_j', $\delta_k = t * \max\{s_1, s_j\}$, j=1,2,… …size(A).

4.3 Extraction of Region of Interest (ROI)

After finding the matching keypoints, the algorithm works to detect and localize the forged area in the image. Region growing technique is used in the proposed technique to extract

region of interest i.e. forged area. Statistical Hu moments have been used for this. The method will find Hu moments (H_1, H_2…….H_7) of the respective surrounding blocks (b_1, b_2) for A_1 and A_j as H_A and H_B. Euclidian distance between different blocks will be calculated. If the computed euclidian distance is lesser than a predefined threshold, the respective blocks will be counted as matched blocks and will be highlighted as forged portions. The above steps will be repeated for all the matching blocks. Fig. 1 represents proposed methodology.

5 RESULTS AND DISCUSSIONS

The proposed technique has been evaluated using MatLab software (version 2016b) on a machine using i7-7700K CPU, 16 GB of RAM, Windows 10 (64-bit). The proposed technique is evaluated qualitatively and quantitatively. The technique has been evaluated on COMFOD (reference) dataset. Table 1 summarize the details of COMFOD dataset.

5.1 Qualitative Results

Visual results for the proposed technique on some images of COMFOD dataset [33] are presented in the Table 1. First column represents original image whereas second column of the Table 1 represents images forged through copy-move attack. Third column of the figure is highlighting the actual copy-move binary portions in the image. Last fourth column of the figure represents the results obtained after applying proposed technique on the images. The copy-move portions in the images are duly highlighted by white and black color respectively. A visual analysis of the results shown in Table 1 validate the performance of the proposed technique, as it actually detect the forged portion and its position in the image. It is evidently visible that the technique successfully detect and localize the forgery of every shape and size.

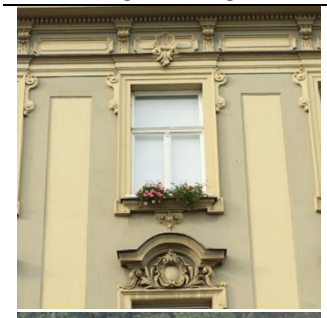
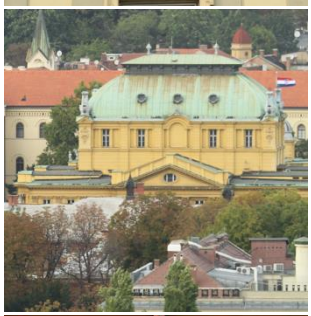
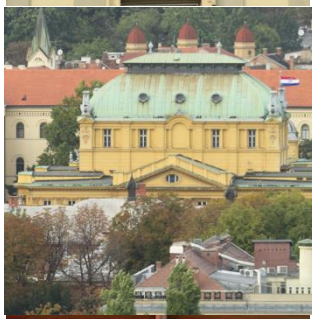
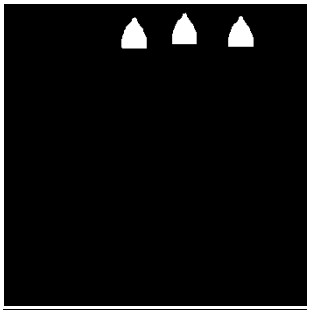
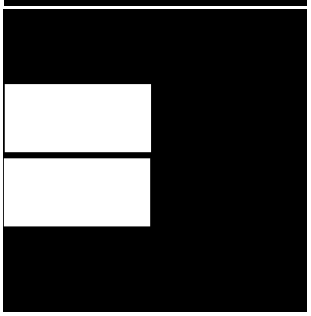
5.2 Quantitative Results

The proposed technique is also evaluated quantitatively on the basis of True positives, True Negatives, False Positives, False Negatives and Precision. Precision of a detection technique may be calculated by using (10).

$$Precision = 100 \times \frac{TP+TN}{TP+FP+TN+FN} \quad (10)$$

TABLE 1

QUALITATIVE ANALYSIS OF THE PROPOSED TECHNIQUE

Original Image	Copy Move Image	Forgery Binaries	Forgery detected
			
			
			

where the number of tampered pixels detected as forged is TP (true positive), the number of manipulated pixels detected as original points is FN(false negative). The number of original image pixels detected as forged is FP (false positive), and the number of original image pixel detected as original pixels is TN (true negative). Table 2 demonstrates that for all types of images the system is highly accurate. For high-detailed images, however, the accuracy rate is slightly lower. Another insight from this table is that the output of the calculation depends on the number of keypoints in the picture. The first seed point for beginning the area was found to grow because of more keypoints in more detailed images including trees. Seed point selection depends on number of ORB points captured for a respective image. There are few keypoints in the picture such as the 'gate' with less color changes and the seed point extraction took 3.31 seconds. The region growing is important for the successful adoption of the technology. As the methodology contrasts Hu moments to find the tampered and original component of the picture, it takes more time for a region to expand. The same is shown in the table. Time taken for localization of the forged area in the image depends on size of area copied. The results in the table establishes this fact.

TABLE 2

QUANTITATIVE EVALUATION OF THE PROPOSED TECHNIQUE

Image	Leafs	Gate	Books	Bird	Building
Number of Keypoints	13637	3965	5570	7755	8936
Time to seed pixel	11.41s	3.31s	4.61s	6.77s	7.34s
Number of Forged Pixels	14878	12194	27460	13182	2216
Localization Time	10.4s	8.47s	35.48s	21.66s	0.49s
Precision of Localization	96.12	89.11	96.67s	92.92	97.16

5.3 Comparison with existing techniques

To prove the superiority of proposed technique over the state-of-the-art techniques, performance comparison has been presented in Table 3 by comparing precision of various existing techniques and proposed technique. It is evident from the Table that proposed technique is a better approach for copy-move forgery detection in comparison to state-of-the-art techniques.

TABLE 3

PERFORMANCE EVALUATION OF PROPOSED TECHNIQUE W.R.T. EXISTING STATE OF THE ART TECHNIQUES

Technique	Precision
Amerini et al. [15]	70%
Li et al. [34]	54.46%
Chen et al. [27]	70.19%
Proposed Technique	96.67%

6. CONCLUSION

The identification of copy-move forgery is a problem in the rapidly expanding world of technology. The paper provides a strategy for identifying forgery by way of keypoints. To extract features in a picture, ORB keypoints are used. Such keypoints are sorted to get the seed point, further by an adaptive level. The adaptive threshold refers to the avoidance of unwanted comparisons. Region based methodology for growing areas shall be used to extract areas which surround the seeds. The region(s) were automatically extracted based on the Hu moment characteristics by the technique. The procedure is computationally effective methodology in contrast with block based techniques. The outcomes have been assessed subjectively and quantitatively. Result assessment approves the vigor of the strategy for recognition and confinement of the copy move falsification against varying forgery shapes and orientation. The proposed procedure has additionally been evaluated against current state of the art methodologies where the proposed method outflanks every one of them by accomplishing a precision of 96.67%. The outcomes and evaluation exhibited in the paper builds up that strategy might be utilized for detection and localization of copy-move fabrication in the digital images. Future research in the field may concentrate on recognizing imitation in profoundly compacted pictures. The use of proposed method for recognizing phony in videos can be investigated.

7 ACKNOWLEDGMENT

I.K.G. Punjab Technical University, Kapurthala for giving opportunity to do research on this topic.

8 REFERENCES

[1]. T. Qazi et al., "Survey on blind image forgery detection," IET Image Process., vol. 7, no. 7, pp. 660–670, 2013.

[2]. M. Kaur and S. Gupta, "A fusion framework based on fuzzy integrals for passive-blind image tamper detection," Cluster Comput., vol. 22, no. 5, pp. 11363–11378, 2019.

[3]. N. K. Gill, R. Garg, and E. A. Doegar, "A review paper on digital image forgery detection techniques," in 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2017, pp. 1–7.

[4]. M. Chandra, S. Pandey, and R. Chaudhary, "Digital watermarking technique for protecting digital images," in 2010 3rd International Conference on Computer Science and Information Technology, 2010, vol. 7, pp. 226–233.

[5]. H. Farid, "Image forgery detection," IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16–25, 2009.

[6]. M. S. Murty, D. Veeraiah, and A. S. Rao, "Digital signature and watermark methods for image authentication using cryptography analysis," Signal Image Process. An Int. J., vol. 2, no. 2, pp. 170–179, 2011.

[7]. C. N. Bharti and P. Tandel, "A survey of image forgery detection techniques," in 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp. 877–881.

[8]. N. B. A. Warif et al., "Copy-move forgery detection: Survey, challenges and future directions," J. Netw. Comput. Appl., vol. 75, pp. 259–278, 2016.

[9]. S. Bayram, H. T. Sencar, and N. Memon, "A survey of copy-move forgery detection techniques," in IEEE Western New York Image Processing Workshop, 2008, pp. 538–542.

[10]. B. L. Shivakumar and L. D. S. S. Baboo, "Detecting copy-move forgery in digital images: a survey and analysis of current methods," Glob. J. Comput. Sci. Technol., 2010.

[11]. G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in 2007 IEEE international conference on multimedia and expo, 2007, pp. 1750–1753.

[12]. Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," Forensic Sci. Int., vol. 206, no. 1–3, pp. 178–184, 2011.

[13]. S. Bharathi, R. Sudhakar, and V. E. Balas, "Hand Vein-based Multimodal Biometric Recognition," Acta Polytech. Hungarica, vol. 12, no. 6, pp. 213–229, 2015.

[14]. V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," IEEE Trans. Inf. Forensics Secur., vol. 7, no. 6, pp. 1841–1854, 2012.

[15]. I. Amerini, L. Ballan, R. Caldelli, A. Bimbo, G. Serra, and , IEEE, "Del and 'A sift-based forensic method for copy-move attack detection and transformation recovery,' Information Forensics and Security, on, vol. no. 3, pp. , .," vol. 6, pp. 1099–1110, 2011.

[16]. H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008, vol. 2, pp. 272–276.

[17]. E. Ardizzone, A. Bruno, and G. Mazzola, "Detecting multiple copies in tampered images," in 2010 IEEE International Conference on Image Processing, 2010, pp. 2117–2120.

[18]. X. Pan and S. Lyu, "Detecting image region duplication using SIFT features," in 2010 IEEE International Conference on Acoustics, Speech and Signal Processing, 2010, pp. 1706–1709.

[19]. M. F. Hashmi, A. R. Hambarde, and A. G. Keskar, "Copy move forgery detection using DWT and SIFT features," in 2013 13th International conference on intellient systems design and applications, 2013, pp. 188–193.

[20]. J. Zhang, Z. Feng, and Y. Su, "A new approach for detecting copy-move forgery in digital images," in 2008 11th IEEE Singapore International Conference on Communication Systems, 2008, pp. 362–366.

[21]. B. Liu and C.-M. Pun, "A SIFT and local features based integrated method for copy-move attack detection in digital image," in 2013 IEEE International Conference on Information and Automation (ICIA), 2013, pp. 865–869.

[22]. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3 PART 2, pp. 1099–1110, 2011.

[23]. H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in European conference on computer vision, 2006, pp. 404–417.

[24]. X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in Multimedia information networking and security (MINES), 2010 international conference on, 2010, pp. 889–892.

[25]. M. F. Hashmi, V. Anand, and A. G. Keskar, "A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms," in 2014 International Conference on Computer and Communication Technology (ICCCT), 2014, pp. 147–152.

[26]. K. H. Paul, K. R. Akshatha, A. K. Karunakar, and S. Seshadri, "SURF Based Copy Move Forgery Detection Using kNN Mapping," in Science and Information Conference, 2019, pp. 234–245.

[27]. C.-C. Chen, W.-Y. Lu, and C.-H. Chou, "Rotational copy-move forgery detection using SIFT and region growing strategies," Multimed. Tools Appl., pp. 1–16, 2019.

[28]. [E. Rublee, V. Rabaud, K. Konolige, and G. R. Bradski, "ORB: An efficient alternative to SIFT or SURF.," in ICCV, 2011, vol. 11, no. 1, p. 2.

[29]. Y. Zhu, X. Shen, and H. Chen, “Copy-move forgery detection based on scaled ORB,” Multimed. Tools Appl., vol. 75, no. 6, pp. 3221–3233, 2016.
[30]. A. Vinay, C. A. Kumar, G. R. Shenoy, K. N. B. Murthy, and S. Natarajan, “ORB-PCA based feature extraction technique for face recognition,” Procedia Comput. Sci., vol. 58, pp. 614–621, 2015.
[31]. A. Vinay, A. S. Cholin, A. D. Bhat, K. N. B. Murthy, and S. Natarajan, “An Efficient ORB based Face Recognition framework for Human-Robot Interaction,” Procedia Comput. Sci., vol. 133, pp. 913–923, 2018.
[32]. M. Calonder, V. Lepetit, C. Strecha, and P. Fua, “Brief: Binary robust independent elementary features,” in European conference on computer vision, 2010, pp. 778–792.
[33]. D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, “CoMoFoD - New Database for Copy-Move Forgery Detection,” Proc. 55th Int. Symp. ELMAR-2013, no. September, pp. 25–27, 2013.
[34]. J. Li, X. Li, B. Yang, and X. Sun, “Segmentation-based image copy-move forgery detection scheme,” IEEE Trans. Inf. Forensics Secur., vol. 10, no. 3, pp. 507–518, 2015.