Optimized Image Authentication Algorithm using Redundant Wavelet Transform Based Sift Descriptors and Complex Zernike Moments

Pooja Vijayakumaran Kallath, Kondaka Lakshmisudha
Department of Information Technology
SIES Graduate School of Technology
Nerul, Navi Mumbai, Maharashtra, India

***Abstract*—Due to the advanced multimedia editing tools and supported by sophisticated hardware, creating image/video manipulations for malicious purposes is increasing which is almost impossible to detect manually. Moreover, to conceal the traces, different post-processing operations are performed. Therefore, authenticity is a growing concern and important for identifying original and forged images. One of the popular image manipulations is copy-move forgery in which one or more regions in the image are duplicated to create a malicious effect within an image. The work in this article presents redundant wavelet transform based complex Zernike moment and Scale Invariant Feature Transform (SIFT) keypoint matching technique for copy-move image forgery operation detection. SIFT is robust against scale and rotation that works on identifying similarity using exhaustive search of SIFT features. After extracting SIFT keypoint features agglomerative hierarchical clustering is employed for grouping and key point matching operation is performed. Finally, block matching operation is evaluated and forged regions in the manipulated images are marked and displayed. This work also presents optimized SIFT key-point feature computations resulting in lower computation time, often one of the requirements in real time deployment. The proposed algorithm performance is evaluated using Precision, Recall, F-Measure and average detection accuracy on popular and publicly available MICC-220 database. The proposed technique demonstrates improved speed-up and detection rate compared to existing approaches.**

Keywords*—Forgery detection; scale invariant feature transform; key point operation; block matching; agglomerative hierarchical clustering

I. INTRODUCTION

In today's world, the widespread use of digital content has led to the manipulations to spread the information with malicious goals and even change people's opinion widely. This forgery creation demands immediate need of digital image authentication and to validate the trustworthiness of source images [1]. Image forensics is the application of domain knowledge to understand image/video content in legal matters. The Scientific Working Group on Digital Evidence (SWGDE) lists best practices that are required to reliably preserve image integrity. Image authentication solution is divided into two types: Active techniques and passive methods (blind). Passive or blind image forensics analyzes the image using statistics and semantics to identify manipulation and without considering embedded data in an image. Passive forgery detection algorithms can be categorized as camera based, pixel-based, geometric-based, physics-based, JPEG artifact-based, and statistical-based techniques.

One of the popular image manipulations is copy-move forgery in which one or more regions in the image are duplicated to create a malicious effect within an image. Copy-move forgery detection algorithm performance is evaluated using either at an image-level or pixel-level. Image/video authentication is employed to verify trustworthiness of the content. Manual authentication mechanism requires huge efforts and labor and sometimes it is error prone. Therefore, automatic image authentication algorithms are required for improved detection rate. As digital media technologies allow for image or video alteration and counterfeiting, having accurate images can be crucial evidence in court. Deep fakes, photo or video editing and many other practices can misrepresent an event that is critical to an investigation. A thorough examination and trustworthy data on the original image is essential. To address this need, image forensics offers a careful review of relevant photos to provide an unbiased assessment of the evidence [2].

Forensic algorithms analyze digital images to determine the accuracy and trustworthiness of the information in several different circumstances. To determine if an image represents a circumstance or location accurately, experts may assess color level anomalies and landmarks to identify the image authenticity. Experts can apply deconvolution to the file to identify a person in the photo that includes a blurred or otherwise obscured identity. Digital images play an important role in people's lives such as news, print media and courtroom evidence [3].

This work presents a technique to verify the credibility and integrity of the images based on a redundant wavelet transform based complex Zernike moment and Scale Invariant Feature Transform (SIFT) key point matching technique for copy-move image forgery operation detection. SIFT is robust against scale and rotation that works on identifying similarity using exhaustive search of SIFT features. However, SIFT is computationally expensive. Hence, this article presents an optimized approach for image authentication. After extracting SIFT key point features agglomerative hierarchical clustering is employed for grouping and key point matching operation is

performed. Finally, block matching operation is evaluated and forged regions in the manipulated images are marked and displayed.

Major contributions of this article are summarized as:

1) Complex Zernike moment feature extraction for improved detection rate.

2) SIFT key-point feature extraction process is computationally expensive. So, an optimized approach for SIFT key-point descriptor extraction is employed which reduces computation time significantly.

3) The proposed optimized image authentication algorithm demonstrates improved speed-up and detection rate.

The paper is organized as follows. Existing literature and findings are presented in Section II. Section III explains proposed algorithms and various feature extraction steps in detail. Simulation experiments and discussions are presented in Section IV. Finally, Section V discusses the results and presents robustness analysis while Section VI concludes the article.

II. Literature Review

This section describes the most crucial and recent works in the field of copy-move forgery detection. In [4], a new methodology based on SIFT is described that helps us to know and understand if a copy-move attack has taken place. In addition to that, it helps to retain the geometric transformation that performs the process of cloning. The proposed method also estimates the geometric transformation values with improved reliability and detects multiple forgery operations.

The work in [5] uses a high-level algorithm to recognize a unique model of using Hu's invariant moments and Log-polar transformations to minimize feature space dimensionality to one feature per block and parallelly recognizing the CMF among almost the same objects in an image. The qualitative and quantitative outputs obtained demonstrate the effectiveness of the algorithm.

In [6], first the input image is decomposed using steerable-pyramid transform (SPT) and grey level co-occurrence matrix (GLCM) descriptors are extracted from each orientation. These features are then utilized to train optimized support vector machines (OSVM) which also acts as a classifier. GLCM features are extracted from each block. A novel method for forgery detection is illustrated which uses a new integrated version of key point-based counterfeit detection method and SLIC super pixel segmentation algorithm for forgery detection [7]. The proposed algorithm generates super-pixels with the help of Simple Linear Iterative Clustering (SLIC). An algorithm to detect copy-move image forgery in images is developed in [8]. Discrete wavelet transform (DWT) is applied on the given image to be decomposed into four parts LL, LH, HL, and HH. Since the LL section contains most of the information, SIFT is particularly applied on the LL part only to extract the most important features. This helps in finding the best descriptor vector of these key features and furthermore, it helps in identifying the similarities between test and train images. Authors in [9] proposed a dual level keypoint based forgery detection approach. First, SIFT is used to detect keypoints in smooth regions and then, BRIEF and FAST descriptors are combined to detect the critical key points from missing areas. Keypoint matching is performed using the generalized nearest neighbor. Finally, morphological image processing operations are utilized to locate forged areas.

The model in [10] first extracts the textural features from the input image. Robust keypoints are extracted using SIFT from these textual images and keypoint matching is done to conclude if the image is forged or not. From that, suspicious regions are determined. The localization of forged pixels is realized via a Ciratefi based approach. Local tetra pattern (LTrP) based feature extraction is developed in [11] for forgery detection and localization. Firstly, the input image is divided into non-overlapping blocks and then from each individual block LTrP descriptors are extracted.

The novel algorithm proposed in [12] utilizes a fusion of the SIFT and local binary pattern (LBP). Consideration of texture features around the key points detected by the SIFT algorithm can be effective to reduce the incorrect matches and improve the accuracy of copy-move forgery detection. In [13], a stationary wavelet transform (SWT) is applied over the input image to acquire a low approximation band, and crucial features are extracted from the band using block-based discrete cosine transformation (DCT) and singular value decomposition (SVD). The literature survey revealed that main feature extraction is based on Zernike moments and SIFT keypoint feature mapping producing acceptable accuracy rate with higher computation time. Hence, this article proposes use of complex Zernike moments and optimized SIFT keypoint extraction and mapping thereby generating improved detection rate at the same time with lower computation time.

III. Proposed Method for Speech Dysfluencies Classification

This work presents redundant wavelet transform based Zernike moment and optimized scale invariant feature transform (SIFT) key point matching technique for copy-move image forgery operation detection. SIFT is robust against scale and rotation that works on identifying similarity using exhaustive search of SIFT features. After extracting SIFT key point features agglomerative hierarchical clustering is employed for grouping and key point matching operation is performed. Finally, block matching operation is evaluated and forged regions in the manipulated images are marked and displayed. The proposed algorithm performance is evaluated using Precision, Recall, F-Measure and detection accuracy and compared with existing copy-move forgery detection approaches.

A. Architecture of MFCC and FBE based Dysfluencies Classification

The detailed steps followed during the development of advanced image authentication algorithm using redundant wavelet transform based SIFT Descriptors and Zernike Moments are outlined below. Fig. 1 illustrates the architecture of the proposed optimized SIFT keypoint feature based algorithm.

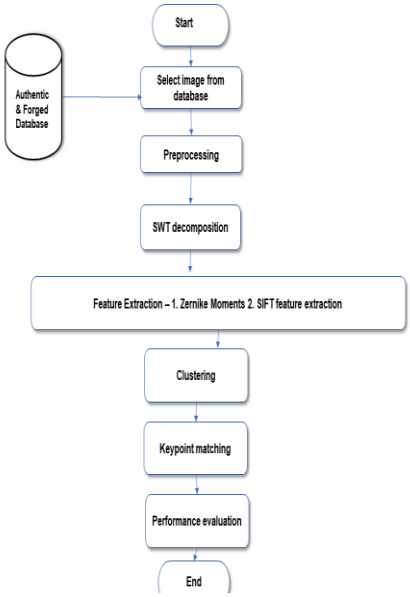

Fig. 1. Workflow diagram of system architecture.

1) Database collection: Collect the image authentication database. The dataset consists of Original and forged images using copy-move forgery operation. Total forged images are represented as $F_T = 1,2,\dots,N$, whereas total original images with $A_T = 1,2,\dots,M$.

2) Redundant wavelet transform decomposition: Apply 4-level redundant wavelet transform decomposition on the original and forged images as follow:

$$A_{j,k_1,k_2} = \sum_{n_1}\sum_{n_2} h_0^{2j}(n_1 - 2k_1)h_0^{2j}(n_2 - 2k_2)A_{j-1,n_1,n_2}$$

$$D^1_{j,k_1,k_2} = \sum_{n_1}\sum_{n_2} h_0^{2j}(n_1 - 2k_1)g_0^{2j}(n_2 - 2k_2)A_{j-1,n_1,n_2}$$

$$D^2_{j,k_1,k_2} = \sum_{n_1}\sum_{n_2} g_0^{2j}(n_1 - 2k_1)h_0^{2j}(n_2 - 2k_2)A_{j-1,n_1,n_2}$$

$$D^3_{j,k_1,k_2} = \sum_{n_1}\sum_{n_2} g_0^{2j}(n_1 - 2k_1)g_0^{2j}(n_2 - 2k_2)A_{j-1,n_1,n_2} \quad (1)$$

Where $A_{j,k_1,k_2}, D^1_{j,k_1,k_2}, D^2_{j,k_1,k_2}, D^3_{j,k_1,k_2}$ are the low-frequency sub-band (LL), high-frequency sub-band (LH), high-frequency sub-band (HL) and diagonal (HH) sub-band of the redundant wavelet transform respectively [14].

3) Compute Zernike moments: Compute the discrete form of the Zernike moments for an image with the size $N \times N$ as follows:

$$Z_{n,m} = \frac{n+1}{\lambda N}\sum_{c=0}^{N-1}\sum_{r=0}^{N-1} f(c,r)V_{n,m}(c,r)$$

$$= \frac{n+1}{\lambda N}\sum_{c=0}^{N-1}\sum_{r=0}^{N-1} f(c,r)R_{n,m}(\rho cr)e^{jm\Theta cr} \quad (2)$$

where, n = Zernike moments order, m is the repetition, λN is a normalization factor, centroid for angle is shown as θ, c indicates centroid column number and r denotes row number. In the above equation, (c; r) represents the coordination of the image while f (c; r) is the image function. The translation vector is represented as V, j is the index of input ROI [15].

4) Scale-invariant feature transform (SIFT) feature extraction: SIFT descriptors are rotation and scaling invariant and are computed using the following steps.

5) Scale-space extrema detection: A Gaussian function G(x; y; σ) and input image, I(x; y) are convolved to obtain scale-spaced image L(x; y; σ) :

$$L(x,y,\sigma) = G(x,y,\sigma) * I(x,y)$$

$$G(x,y,\sigma) = \frac{1}{2\pi r^2}e^{-\frac{x^2+y^2}{2\sigma^2}} \quad (3)$$

6) Keypoint localization: The keypoint selection from extrema is obtained by rejecting the points along image edges or having low contrast values and expressed as:

$$D(x) = D + \frac{\partial D^T}{\partial x} + \frac{1}{2}x^T + \frac{\partial^2 D}{\partial x^2}x \quad (4)$$

7) Keypoint descriptor generation: The SIFT keypoints with a histogram array of 4 X 4 and number of orientation bins as 8, produces 128-dimensional descriptor.

8) Clustering: SIFT keypoint descriptors are extracted from approximate sub-band of the SWT decomposition and are grouped using agglomerative hierarchical clustering. Typical linkage methods utilized for the clustering approach are median, centroid or ward.

9) Key point matching: SIFT keypoint matching is a principal step in which firstly keypoints from the input image are read and compared with the keypoints of images.

10)Block matching and marking forged region: Finally, block matching operation is evaluated and forged region in the manipulated images are marked and displayed.

11)Performance evaluation: The proposed algorithm performance is evaluated using Precision, Recall, F-Measure and detection accuracy.

Precision = True-Positives / (True-Positives + False-Positives)

Recall = True-Positives / (True-Positives + False-Negatives)

F-Measure = (2 * Precision * Recall) / (Precision + Recall)

Detection rate = (TruePositives + True-Negatives) /(True-Positives +True-Negatives + False-Positives + False-Negatives)

IV. Simulation Results

This section presents a variety of experiments conducted using the proposed algorithm. To assess the effectiveness of the developed technique for image authentication, MICC-F220 database is employed. This popular and publicly available image dataset has forged and authentic natural 220

images: 110 are manipulated images and 110 are authentic. The pixel resolution of these images varies from 722 X 480 to 800 X 600 pixels and almost 1.2% of the whole image is covered by the forged patch. The simulation experiments were conducted on Intel® Core™ i-54, 9400F CPUU @ 2.90 GHz processor with 8GB RAM running MATLAB 2021a.

As the input image pixel resolution varies, we have resized the input image size to 300 X 300. In order to extract finer details four-level redundant wavelet transform decomposition is utilized. Zernike moments are extracted with the settings as order of 4 and repetition of moments 2. The proposed optimized forgery detection algorithm utilizes Harris threshold of 5 and number of windows as 2. We have set the sigma value as 9 and 3 neighbourhood computation. The forged region detection is performed individually on each color component and finally combined to generate final output.

The performance of the proposed optimized image forensic algorithm is described by the computation of precision, recall, F-score and detection rates. Precision and recall are two important parameters employed to identify forgery detection algorithm accuracy. F-Measure represents a measure of test accuracy and is the harmonic mean of precision and recall. The results reported in this paper are an average of 10 trials. The proposed image authentication algorithm performance is evaluated using Precision, Recall, F-Measure and detection accuracy.

1) Experimental results and analysis using standard and proposed optimized forgery detection approach: Firstly, the effectiveness and the accuracy evaluation of the proposed technique, we present experimental results and analysis using conventional SIFT key-point feature extraction approach and proposed optimized image forensic algorithm. For fair comparison for both experiments MICC-F220 DATABASE is employed. The detection performance is measured on irregular shaped duplicated regions as it influences the overall detection rate. The first set of experiments is carried out without any post-processing operation on the original and manipulated image.

Fig. 2 to 5 illustrate experiment results for copy- move forgery detection using the proposed algorithm for four sample images from the database. In each figure, the first row (from left to right) depicts the original image, SLIC image and SIFTS keypoint feature extraction. Second row (from left to right) shows labelled feature points, merged points after morphological operation, and detected forged regions are shown. As it is evident from these figures that the proposed optimized technique effectively detects and locates forged areas. Moreover, it convincingly visualizes and detects irregular shape manipulated areas and objects.

As illustrated in these Fig. 2 to 5, first the input image is decomposed using a four-level redundant wavelet transform. The four-level decomposition primarily assists in extracting fine details from the forged image. This in turn enhances the detection and localization estimation. As shown in the second figure of the first row, the simple linear iterative clustering based super pixel segmentation (SLIC) algorithm convincingly improves input segmentation into different regions. The SIFT key-point feature extraction process and final detection result is dependent on the SLIC generated output.

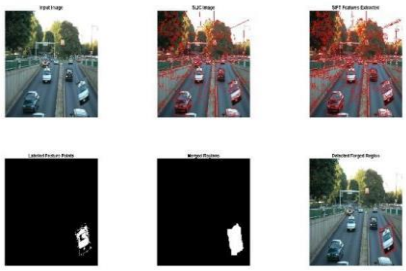

Fig. 2. Copy- move forgery detection results using the proposed algorithm obtained using image sample 1.

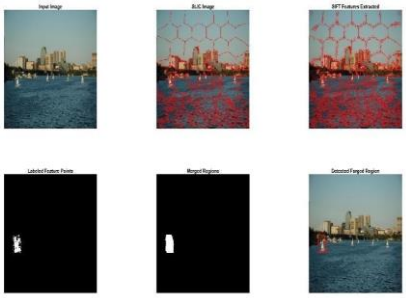

Fig. 3. Copy- move forgery detection results using the proposed algorithm obtained using image sample 2.

Fig. 4. Copy- move forgery detection results using the proposed algorithm obtained using image sample 3.

Fig. 5. Copy- move forgery detection results using the proposed algorithm obtained using image sample 4.

V. DISCUSSIONS

This work presents comparison between conventional SIFT key-point feature extraction and modified feature extraction technique in terms of various performance evaluation parameters. In the conventional SIFT key-point feature extraction approaches typically Harris threshold is set at 10 and number of windows for computation is 4. The computation time for detection of SIFT key-point features and further processing like localization is considered as one of the major concerns in case of real-time detection. Table I shows the evaluation results using these parameters for precision, recall, F-measure and execution time for five images.

As it can be observed from Tables I and II that the execution time of the optimized image forensic algorithm is significantly reduced compared to the conventional approach. The speedup obtained in this case is almost twice. Additionally, precision and F-measure parameters are slightly improved in the proposed technique. This experimental evaluation signifies improved performance of the optimized algorithm over the conventional SIFT key-point feature extraction technique. The average precision and F-Measure value is 0.9806 and 0.9904 for the conventional SIFT feature extraction approach whereas it is 0.987 and 0.9938 for the proposed method. Fig. 6 and 7 depict the effect of Harris threshold and number of window computation on the average detection accuracy respectively.

A. Robustness Analysis

To conceal the traces of copy-move forgery operation the malicious user usually performs various post-processing operations. The prime intent of these post-processing operations is to make forged areas hard to detect and localize. Therefore, it is imperative to evaluate the robustness of the proposed image forensic technique against different post-processing operations. In this study, three different post-processing operations and its robustness is analyzed: rotation attack, scaling attack, and contrast enhancement.

Fig. 8, 9 and 10 depict average accuracy, precision and F1-Measure computed using rotation attack, scaling attack and contrast enhancement respectively. It is evident from these figures that the proposed optimized forgery detection technique has the capability to perform better even when the forged image suffers from rotation, scaling and contrast enhancement post processing operations. The average accuracy is above 96% in all post-processing attacks proving enhanced detection and localization performance of the proposed algorithm. Finally, the proposed optimized image forensic approach is compared with existing state-of-the-art techniques. As shown in Table III, the proposed algorithm outperforms existing approaches in terms of precision, recall and average accuracy rate.

TABLE I. PERFORMANCE EVALUATION USING CONVENTIONAL SIFT KEY-POINT FEATURE EXTRACTION APPROACH

Image number	Execution time (s)	Precision	Recall	F-Measure
Image 1	0.4835	0.9838	1	0.9918
Image 2	0.4928	0.9729	1	0.9887
Image 3	0.4734	0.9837	1	0.9899
Image 4	0.4674	0.9823	1	0.9903
Image 5	0.4985	0.9802	1	0.9914
Average	0.4735	0.9806	1	0.9904

TABLE II. PERFORMANCE EVALUATION USING OPTIMIZED SIFT KEY POINT FEATURE EXTRACTION APPROACH

Image number	Execution time (s)	Precision	Recall	F-Measure
Image 1	0.2383	0.9913	1	0.9918
Image 2	0.2467	0.9838	1	0.9928
Image 3	0.2414	0.9867	1	0.9939
Image 4	0.2725	0.9848	1	0.9956
Image 5	0.2469	0.9884	1	0.9926
Average	0.2492	0.987	1	0.9938

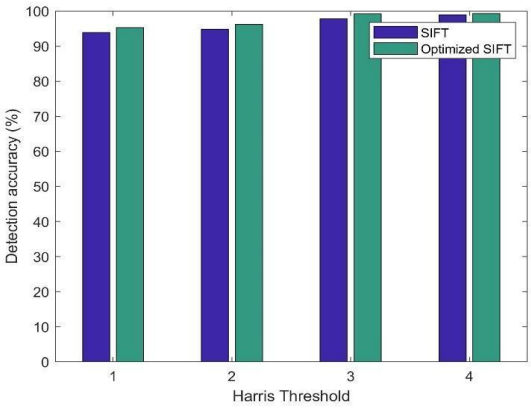

Fig. 6. Detection rate using Harris threshold using conventional SIFT and proposed optimized SIFT algorithm.

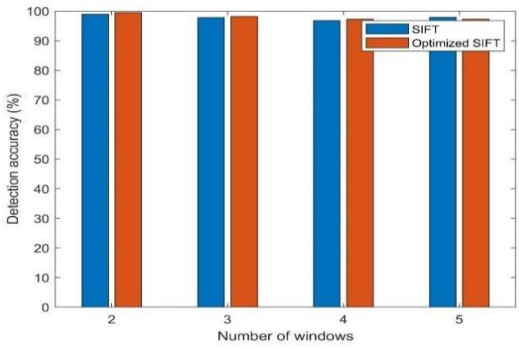

Fig. 7. Effect of number of windows on the detection rate using conventional SIFT and proposed optimized SIFT algorithm.

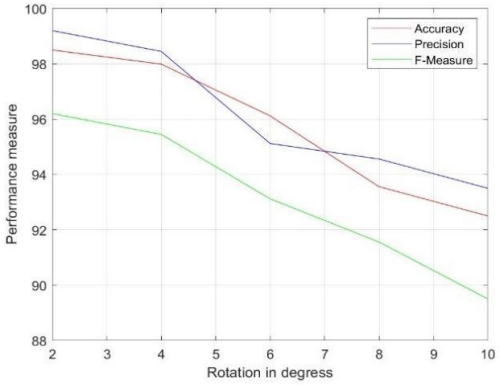

Fig. 8. Average accuracy, precision, and F1-measure computation using rotation attack with 2, 4, 8 and 10 degree rotation.

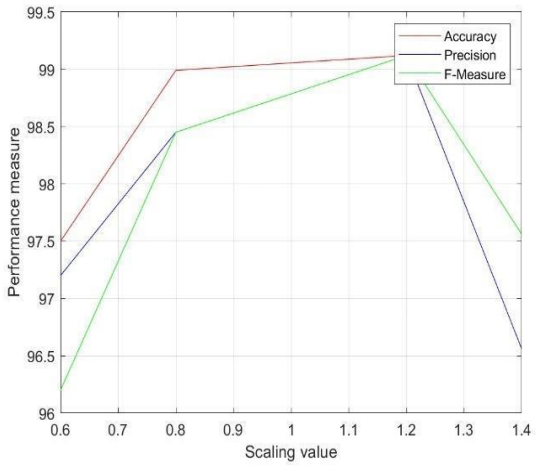

Fig. 9. Average accuracy, precision, and F1-measure evaluation using scaling attack with 0.6, 0.8, 1.2 and 1.4 scaling value.

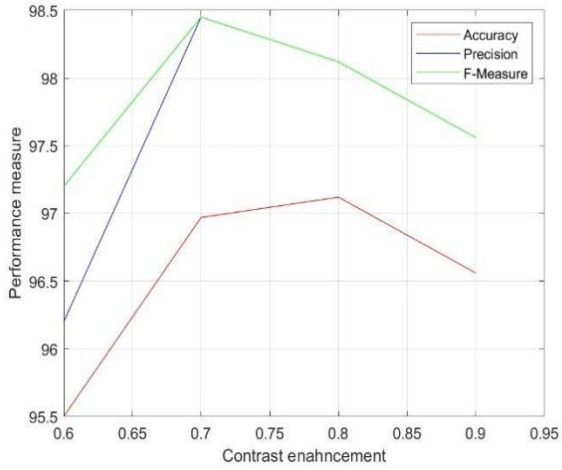

Fig. 10. Average accuracy, precision, and F1-measure values obtained using different contrast enhancement parameters.

Overall recent proposed methods based on SIFT and feature level image authentication have higher computational complexity although, there are performance improvement techniques using different feature fusion resulting in higher dimensional feature vector. To overcome these issues this paper presents optimized SIFT based image authentication solution. The proposed approach lowers the computational cost and speed up is achieved in this study.

TABLE III. COMPARISON OF PROPOSED ALGORITHM

Method	Precision	Recall	F-measure	Accuracy
[15	96	89	100	94
[16]	91.39	95.83	86.55	90.95
[17]	94	95.83	92	93.87
[18]	93.9	90.44	87.75	92.20
[19]	92.8	88.7	91.15	94.45
Proposed	98.53	100	99.13	98.87

VI. CONCLUSIONS

In today's world, widespread use of multimedia contents has given rise to the manipulations of multimedia content with malicious purposes demanding the necessity of robust authentication techniques. This work presents redundant wavelet transform based complex Zernike moment and optimized scale invariant feature transform (SIFT) keypoint matching technique for copy-move image forgery detection. SIFT is robust against scale and rotation that works on identifying similarity using exhaustive search of SIFT features. After extracting SIFT keypoint features agglomerative hierarchical clustering is employed for grouping and key point matching operation is performed. Finally, block matching operation is evaluated and forged regions in the manipulated images are marked and displayed. The proposed algorithm is evaluated using the popular and publicly available database MICC-F220. As observed, the proposed optimized SIFT algorithm achieves speedup of almost twice over the standard SIFT technique. Experimental evaluation illustrates improved performance of the proposed technique as compared to other similar methods available in the literature. In future, the work can further be explored using statistical descriptors to improve image authentication accuracy.

REFERENCES

[1] Kaur, G., Singh, N. & Kumar, M., "Image forgery techniques: a review", Artificial Intelligence Review, Volume - 56, pp. 1577–1625, 2023.

[2] Warif, N.B.A., Idris, M.Y.I., Wahab, A.W.A. *et al.* "A comprehensive evaluation procedure for copy-move forgery detection methods: results from a systematic review", Multimedia Tools and Applications, Volume - 81, pp. 15171–15203, 2022.

[3] Simranjot Kaur, Rajneesh Rani, Ritu Garg, and Nonita Sharma, "State-of-the-art techniques for passive image forgery detection: a brief review", International Journal of Electronic Security and Digital Forensics, Volume -14, Issue - 5, pp. 456-473, 2022.

[4] Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, "A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery," in *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, Sept. 2011.

[5] K. Tejas, C. Swathi and M. Rajesh Kumar, "Copy Move Forgery using Hu's Invariant Moments and Log-Polar Transformations," *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, 2018, pp. 1229-1233.

[6] S B G Tilak Babu, Ch Srinivasa Rao, "An optimized technique for copy–move forgery localization using statistical features", ICT Express, Volume 8, Issue 2, Pages 244-249, 2022.

[7] Rathi, K., Singh, P., "Copy Move Forgery Detection by Using Integration of SLIC and SIFT", In: Jeena Jacob, I., Gonzalez-Longatt, F.M., Kolandapalayam Shanmugam, S., Izonin, I. (eds) Expert Clouds and Applications. Lecture Notes in Networks and Systems, vol 209, 2022.

[8] M. F. Hashmi, A. R. Hambarde and A. G. Keskar, "Copy move forgery detection using DWT and SIFT features," *2013 13th International Conference on Intelligent Systems Design and Applications*, Salangor, Malaysia, 2013, pp. 188-193, doi: 10.1109/ISDA.2013.6920733.

[9] Fatima, B., Ghafoor, A., Ali, S.S. *et al.* "FAST, BRIEF and SIFT based image copy-move forgery detection technique" Multimedia Tools and Applications, Volume - **81**, Pages- 43805–43819, 2022.

[10] Tahaoglu, G., Ulutas, G., Ustubioglu, B. *et al.* "Ciratefi based copy move forgery detection on digital images", Multimedia Tools and Applications *Volume*- **81**, pages -22867–22902, 2022.

[11] Ganguly, S., Mandal, S., Malakar, S. *et al.* "Copy-move forgery detection using local tetra pattern based texture descriptor", Multimedia Tools and Applications, 2023, https://doi.org/10.1007/s11042-022-14287-9.

[12] Marziye Shahrokhi, Alireza Akoushideh and Asadollah Shahbahrami, "Image Copy–Move Forgery Detection Using Combination of Scale-Invariant Feature Transform and Local Binary Pattern Features", International Journal of Image and Graphics, Vol. 22, No. 05, pages-2250048, 2022.

[13] Kumar, S., Mukherjee, S. & Pal, A.K, "An improved reduced feature-based copy-move forgery detection technique", Multimedia Tools and Applications, Volume - 82, pages - 1431–1456, 2023.

[14] Mahmoud, Khaled & Husien, Arwa. (2016). Copy-Move Forgery Detection Using Zernike and Pseudo Zernike Moments. The International Arab Journal of Information Technology (IAJIT). 13. 930-937.

[15] Goel, N., Kaur, S., & Bala, R. (2021). Dual branch convolutional neural network for copy move forgery detection. IET Image Processing, 15(3), 656-665.

[16] Warif, N. B. A., Wahab, A. W. A., Idris, M. Y. I., Salleh, R., & Othman, F. (2017). SIFT-symmetry: a robust detection method for copy-move forgery with reflection attack. Journal of Visual Communication and Image Representation, 46, 219-232.

[17] Hashmi, M. F., Hambarde, A. R., & Keskar, A. G. (2013, December). Copy move forgery detection using DWT and SIFT features. In 2013 13th international conference on intellient systems design and applications (pp. 188-193). IEEE.

[18] Richa Singh ; Sandeep Verma ; Suman Avdhesh Yadav ; S. Vikram Singh. Copy-move Forgery Detection using SIFT and DWT detection Techniques. 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), 10.1109/ICIEM54221.2022.9853192.

[19] S B G Tilak Babu, Ch Srinivasa Rao, "An optimized technique for copy–move forgery localization using statistical features" ICT Express 8 (2022) 244–249.