RES MILITARIS Social Science Journal

Evaluation of Key Point-Based Copy-Move Forgery Detection Algorithms

Mamta Gupta[1] Pooja dahiya[2]

guptamamta22985@gmail.com

Affiliation Panipat Institute of Engineering and Technology,Samalkha,Panipat

pujadahiya88@gmail.com

Affiliation Panipat Institute of Engineering and Technology,Samalkha,Panipat

1.1 Abstract

In recent years, the proliferation of digital image manipulation tools has made it easier for individuals with malicious intent to forge images. Copy-move forgery (CMF) is a common technique used in image tampering. Copy-move forgery detection (CMFD) is essential in various fields, including digital forensics, journalism, and law enforcement, as it helps ensure the integrity of digital images by identifying and mitigating attempts to manipulate them for deceptive purposes. Consequently, there is a pressing need for robust and efficient copy-move forgery detection methods. This evaluation provides a comprehensive assessment of the performance of these key-point-based algorithms in detecting copy-move forgeries. This work assesses the performance of the four State-of-the-art SIFT, SURF, BRISK and ORB algorithms on CoMoFoD dataset in terms of accuracy, precision, recall and f1-score.

Keywords: Image forensics, Copy-move forgery detection, SIFT, SURF, BRISK and ORB

1.2 Introduction

Image forensics [1] is a branch of digital forensics that focuses on the analysis and authentication of digital images to determine their integrity, origin, and any potential manipulation or tampering. It involves the use of various techniques and tools to investigate and analyse images, with the goal of uncovering any alterations, forgeries, or deceptive practices related to the visual content. The need for image forensics in recent times has grown significantly due to several factors [2]. With the widespread use of smartphones, digital cameras, and social media platforms, there has been an exponential increase in the creation and sharing of digital images. This has created an environment where image manipulation and forgery have become more prevalent. Digital images play a crucial role in conveying information, and they are often used as evidence in various contexts, including news reporting, legal proceedings, and social discourse. The ability to manipulate images has led to concerns about the authenticity and credibility of visual content.

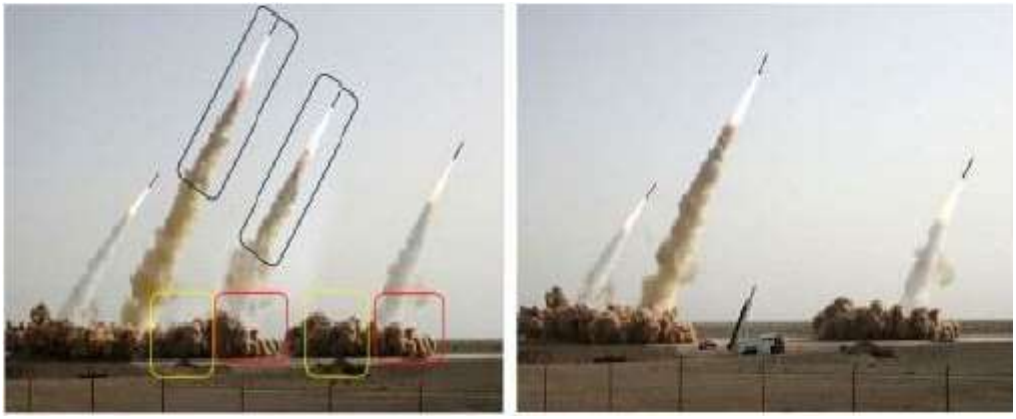

Figure 1: An Example of Copy-Move Forgery [3]

Advances in deep learning and AI have made it possible to create highly realistic and convincing manipulated images and videos, known as deepfakes [4]. These can be used to impersonate individuals, spread false information, or damage reputations. In legal cases, image forensics can be critical for verifying the authenticity of evidence and ensuring that it has not been altered. This is particularly important in criminal investigations and civil litigation.**:** Media organizations and journalists need tools and expertise to verify the authenticity of images and videos used in news stories. Accurate reporting and the prevention of misinformation are essential. Image forensics techniques encompass a wide range of methods, including copy-move forgery detection, image manipulation detection, source camera identification, deepfake detection, and more [5]. These techniques are crucial for ensuring the reliability and trustworthiness of digital images in an increasingly digital and visually-oriented world. As the technology for image manipulation continues to advance, the need for effective image forensics becomes even more critical to maintain trust and transparency in various aspects of society.

Several key-point based algorithms, such as SIFT (Scale-Invariant Feature Transform) [6], SURF (Speeded-Up Robust Features) [7], BRISK (Binary Robust Invariant Scalable Key-point) [8], and ORB (Oriented FAST and Rotated BRIEF) [9], have been proposed for copy-move forgery detection. Each of these algorithms has its strengths and weaknesses, and their performance can vary depending on factors like image content, scale, and computational resources. This work provides a comprehensive assessment of the performance of these key-point-based algorithms in detecting copy-move forgeries. The contribution of the work lies in its thorough evaluation and comparison of key-point based CMFD algorithms, helping users make informed choices, advancing the state of the art, and identifying areas for further research and improvement in the field of image forensics and tamper detection. This Evaluation can help users optimize these algorithms for their specific needs and can provide researcher a reference point for future algorithm development and comparison.

1.3 Related Work

Copy-move forgery detection methods [10] [11] can be categorized into several types based on the techniques and approaches they use to identify forged regions within an image. include: Key-point-based Methods include SIFT, SIFT detects distinctive key-points and their descriptors in an image, making it robust to changes in scale, rotation, and illumination. Block Matching technique divides the image into blocks and compares them to identify duplicate regions [12]. Discrete Cosine Transform (DCT) can be applied to image blocks, and duplicate blocks are identified by comparing DCT coefficients [13]. Frequency Domain Methods such as FFT-based (Fast Fourier Transform) methods transform the image into the frequency domain and analyse frequency components to detect duplicate regions [14]. Texture Analysis methods [15] such as GLCM (Gray-Level Co-occurrence Matrix calculate texture features from the image and identifies similar texture patterns within the image [16]. Gabor filters can also be used to analyse texture and identify regions with similar texture properties [17]. Deep Learning Approaches [18] [19] such as Convolutional Neural Networks (CNNs) [20] have also been employed for forgery detection. (Principal Component Analysis) can also be used to reduce the dimensionality of image patches and identify similar patches in a lower-dimensional space. The choice of method depends on the specific requirements and characteristics of the image dataset and the expected types of forgeries. Researchers often experiment with various approaches to improve the accuracy and robustness of copy-move forgery detection algorithms.

1.4 Copy-move forgery Detection

Copy-move forgery detection is a technique used in the field of computer vision and digital image forensics to identify and locate regions in an image where portions of the image have been copied and pasted or moved within the same image in order to create a fraudulent or manipulated version of the original image. This type of forgery is often employed to alter the content of an image while attempting to make the changes appear seamless and convincing. Common methods and algorithms used in copy-move forgery detection include SIFT, SURF, and others that are robust to transformations. Machine learning and deep learning techniques have also been applied to improve the accuracy of forgery detection. General working of CMFD algorithms is:

Figure 2: General steps of a CMF detection algorithm

1. **Feature Extraction:** The first step involves extracting distinctive features from the image. These features can include key-points, textures, or other characteristic patterns within the image.
2. **Clustering:** Detected similar regions are often grouped together in clusters, suggesting potential forgery areas.
3. **Feature Matching:** The extracted and clustered features are then compared and matched to identify regions within the image that share similar or identical features. These regions are potential candidates for copy-move forgery.
4. **Validation:** After clustering, further analysis is performed to validate whether the detected regions are indeed forgeries. This step may involve additional techniques to distinguish between genuine duplication (e.g., objects with similar patterns) and malicious copy-move forgery. The final output typically includes information about the location and extent of the forged regions within the image.

As this work provides the systematic evaluation and comparison of four key-point based copy-move forgery detection algorithms (SIFT, SURF, BRISK, and ORB), The algorithms are explained as:

1.4.1 Scale-Invariant Feature Transform (SIFT)

SIFT [21] is a widely used method for detecting and matching key-points in images. It is known for its robustness to scale changes, rotations, and changes in viewpoint. SIFT key-points [22] are described using histograms of gradient orientations in their local neighbourhoods. SIFT begins by detecting key-points or interest points in the image. These key-points are identified based on their uniqueness and stability under various transformations like scaling, rotation, and changes in viewpoint. Key-points are identified at different scales, which allows SIFT to be robust to changes in object size within the image. After detecting key-points, SIFT computes a descriptor for each key-point. The descriptor is a compact representation of the local image information around the key-point. It captures the gradient orientations and magnitudes in the key-point's neighbourhood. SIFT descriptors are invariant to image translation, rotation, and scale changes, making them well-suited for detecting copy-move forgeries, which often involve such transformations.

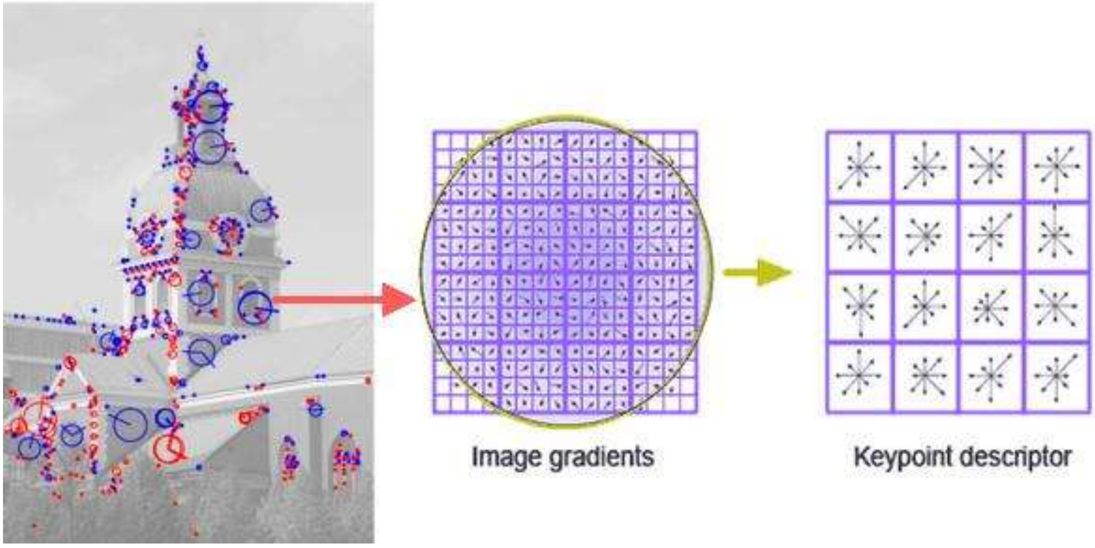

Figure 3: SIFT Key-point detection using image gradients [23]

SIFT then performs key-point matching, where it compares the descriptors of key-points across the entire image to find similar key-points. Key-points with similar descriptors are considered potential matches, suggesting regions in the image that might have been copied and pasted. Geometric Verification: To further validate the potential copied regions, SIFT often employs geometric verification techniques. These techniques consider the spatial arrangement and transformations (e.g., translation, rotation, scaling) between the matched key-points. In copy-move forgery detection, the corresponding key-points should exhibit similar transformations, as the copied regions are expected to undergo similar changes. However, it can be computationally intensive, especially for large images, and may require careful parameter tuning for optimal performance. Researchers continue to explore enhancements and optimizations to improve the accuracy and efficiency of SIFT-based copy-move forgery detection techniques.

1.4.2 Speeded-Up Robust Features (SURF)

SURF [24] begins by detecting interest points, also known as key-points, in the input image. Key-points are identified based on their unique and stable characteristics under various transformations like scaling, rotation, and changes in viewpoint. SURF key-points [25] are detected efficiently by approximating the Hessian matrix determinant using box filters. SURF performs key-point matching to find correspondences between key-points in the input image. Key-points with similar descriptors are considered potential matches, indicating regions in the image that might have been copied and pasted. Detected matches are typically grouped together in clusters. Each cluster represents a set of key-points that likely correspond to a forged region within the image.

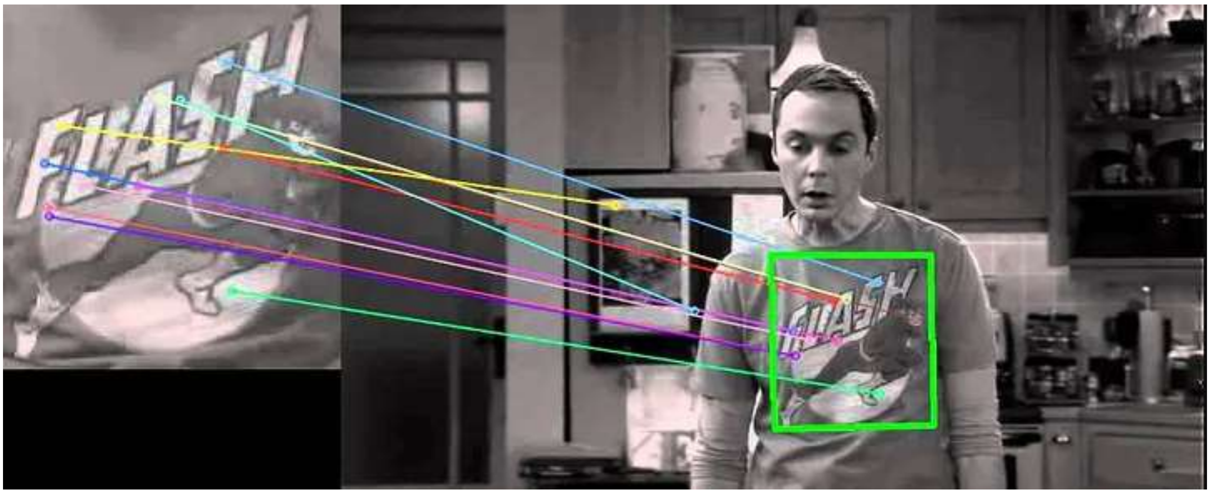

Figure 4: Key-point detection using SURF algorithm [26]

Clusters can be used to identify the specific regions of the image that have been manipulated through copy-move forgery. The output of SURF includes information about the location and extent of the copy-move forgeries within the image. This information is often represented as bounding boxes or masks highlighting the forged areas. SURF benefits from the computational efficiency of the SURF algorithm, making it suitable for processing large images and real-time applications. However, like any forgery detection technique, it may require parameter tuning and careful consideration of factors like false positives and computational resources. Researchers continually explore enhancements and optimizations to improve the accuracy and efficiency of SURF-based copy-move forgery detection methods.

1.4.3 Oriented FAST and Rotated BRIEF (ORB)

ORB [27] is a real-time key-point detector and descriptor that combines the FAST (Features from Accelerated Segment Test) key-point detector with the BRIEF (Binary Robust Independent Elementary Features) descriptor [28]. It is known for its computational efficiency. ORB is a feature detection and description method that can be used in the context of CMFD. ORB play a role in this process by helping to detect and describe key-points within the image, which are essential for identifying duplicated or forged regions. ORB is known for its computational efficiency and robustness to various transformations, making it a valuable tool for CMFD tasks. It can efficiently detect key-points and compute binary descriptors, making it suitable for real-time applications. However, like any forgery detection technique, it may require careful parameter tuning and validation to ensure accurate results. Researchers often experiment with various approaches to improve the accuracy and robustness of ORB-based CMFD methods.

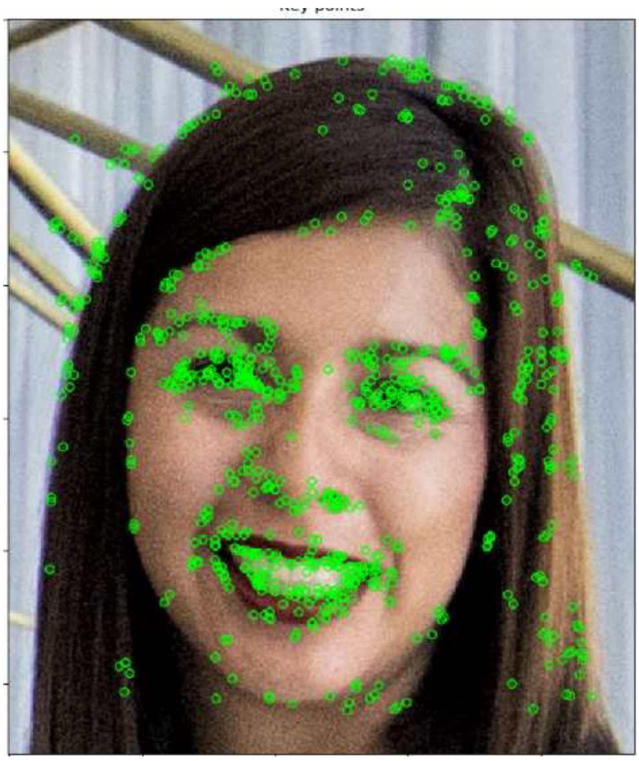

Figure 5: Detected key-point (interest points) in ORB algorithm

ORB detects key-point (interest points) in the image Figure 5. These key-point are locations in the image where there are distinctive patterns or features. Once key-point are detected, ORB computes descriptors for each key-point. These descriptors capture local image information in the neighbourhood of each key-point. ORB descriptors are binary strings, making them compact and efficient for matching. ORB matches key-point between different regions of the image, looking for regions that exhibit similar patterns. Key-point with similar descriptors are considered potential matches, suggesting regions in the image that might have been copied and pasted. To validate potential copied regions, geometric verification can be applied. This involves analysing the spatial arrangement and transformations (e.g., translation, rotation, scaling) between the matched key-point. In CMFD, the corresponding key-point in copied regions should exhibit similar transformations.

1.4.4 Binary Robust Invariant Scalable Key-point (BRISK)

BRISK [29] is designed to be both robust and efficient. It employs a scale-space pyramid and detects key-point in different scales. BRISK key-point are described using binary strings. BRISK can play a role in this process by helping to detect and describe key-points within the image, which are crucial for identifying duplicated or forged regions [30]. BRISK detects key-points (interest points) in the image. These key-points are locations in the image where there are distinctive patterns or features. Key-point Description: Once Key-points are detected, BRISK computes descriptors for each Key-point. These descriptors capture local image information in the neighbourhood of each Key-point. BRISK descriptors are binary strings, which makes them compact and efficient for matching. BRISK matches Key-points between different regions of the image, looking for regions that exhibit similar patterns. Key-points with similar descriptors are considered potential matches, suggesting regions in the image that might have been copied and pasted. To validate potential copied regions, geometric verification can be applied. This involves analysing the spatial arrangement and transformations (e.g., translation, rotation, scaling) between the matched Key-points. In CMFD, the corresponding Key-points in copied regions should exhibit similar transformations.

A comparison of the four CMFD algorithms SIFT, SURF , BRISK and ORB is presented in Table 1. As the suitability of these algorithms for a specific CMFD task depends on factors like the nature of the images, computational resources, and the level of robustness required. All three algorithms are widely used in computer vision and image processing, but the choice depends on the specific application and its requirements.

Table 1: comparison of the SIFT, SURF, BRISK and ORB algorithms

Aspect	SIFT	SURF	BRISK	ORB
Scale Invariance	Yes (Built-in)	Yes (Built-in)	Yes (Built-in)	Yes (Built-in)
Rotation Invariance	Yes (Built-in)	Yes (Built-in)	Yes (Built-in)	Yes (Built-in)
Key-point Detection Speed	Moderate	Fast	Fast	Fast
Key-point Descriptor Size	128-dimensional vector	64-dimensional vector	Binary string (256 or 512 bits)	Binary string (256 bits)
Descriptor Matching Speed	Moderate	Fast	Fast	Fast
Sensitivity to Scale Changes	Less sensitive	Sensitive	Less sensitive	Less sensitive
Sensitivity to Rotation Changes	Less sensitive	Sensitive	Less sensitive	Less sensitive
Sensitivity to Illumination	Sensitive	Sensitive	Less sensitive	Sensitive

Computational Efficiency	Moderate	Fast	Fast	Fast
Applicability	Wide range of applications	Real-time applications	Real-time applications	Real-time applications
Suitable for Large Datasets	Yes	Yes	Yes	Yes
Binary Descriptors	No	No	Yes	Yes
Geometric Transformations	Supports complex transformations	Limited support for rotation and scale	Supports complex transformations	Supports limited transformations (rotation)
Robustness to Noise	Good	Good	Moderate	Good

1.5 Experimental Analysis

we conducted the evaluation using the CoMoFoD dataset [31], which comprises 200 images of copy-move forgeries and 200 unaltered images, all with dimensions of 512x512 pixels. Figure 6 shows a sample image copy move forgery from the CoMoFoD dataset which original image on the left, and the binary mask in the middle showing the differences, and the forged image in the right.

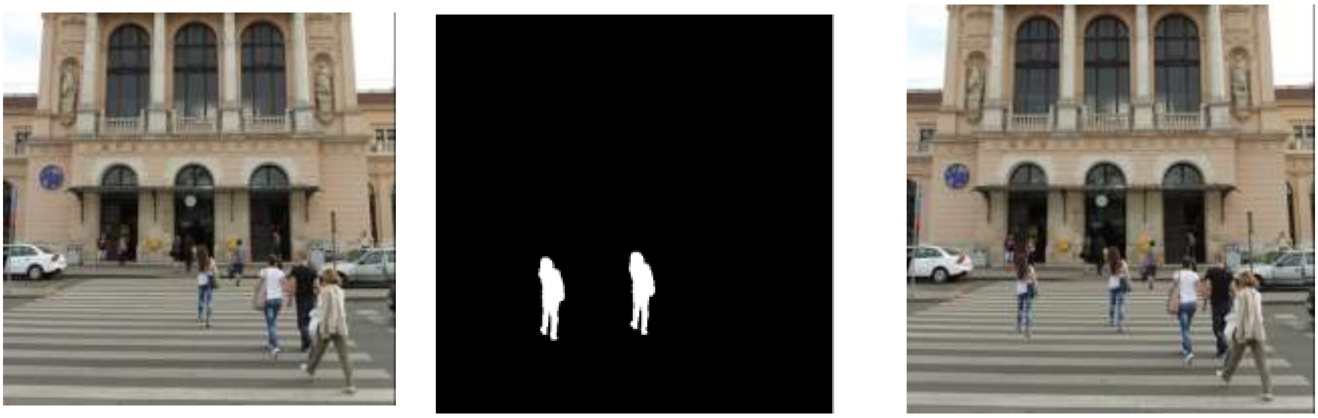

Figure 6: A sample image copy move forgery from the CoMoFoD dataset

The computational environment utilized for our experiments featured an Intel i5 processor, 8.00 GB of RAM, and MATLAB R2021B running on the Windows 10 operating system. To gauge the effectiveness of the key-point based methods, we employed four metrics at the image level, namely accuracy, precision, recall, and the F1 Score. The comparative results of these four methods are presented in Table 2, showcasing the computed metrics.

BRISK achieved a high accuracy rate (87.5%), indicating that it correctly identified copy-move forgeries and genuine images in a substantial portion of the dataset. The precision score for BRISK is also excellent (97.0%), indicating that when it flagged an image as a forgery, it was very likely to be correct. The recall score (89.0%), while strong, suggests that BRISK captured the majority of the actual copy-move forgeries in the dataset but missed a small percentage.

Table 2: Evaluation Results of the copy-move forgery detection algorithms

Method	Accuracy	Precision	Recall	F1
BRISK	87.5	97.0	89.0	92.8
HoG	70.3	78.3	81.5	83.2
SIFT	83.7	84.0	83.7	89.7
SURF	82.4	62.7	92.5	74.3

The F1 score (92.8%), which balances precision and recall, is quite high, indicating overall robust performance. ORB achieved a relatively lower accuracy (70.3%) rate compared to BRISK, indicating that it had a lower overall correctness in classifying images. The precision score suggests that when ORB flagged an image as a forgery, it was correct in a significant proportion of cases (78.3%). The recall score of (81.5%) indicates that ORB captured a substantial portion of the actual forgeries but missed some.

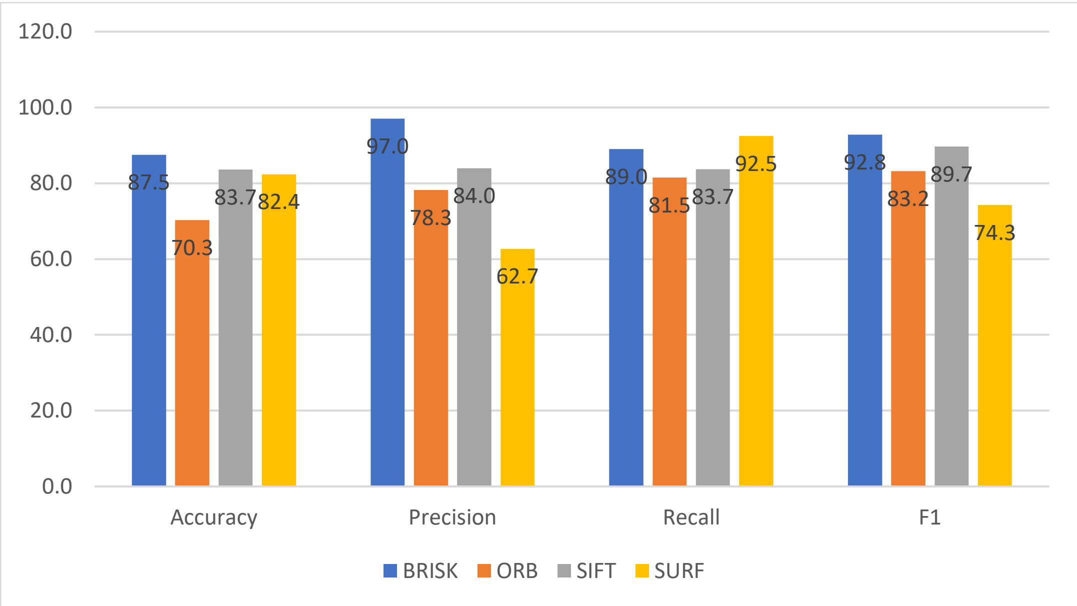

Figure 7: Comparative evaluation of the algorithms in terms of accuracy, precision, recall, and the F1 Score.

The F1 score (83.2%), while lower than BRISK, still reflects a reasonable balance between precision and recall. SIFT achieved a high accuracy rate (83.7%), similar to BRISK, indicating strong overall performance in classification as shown in Figure 7. The precision score of (84.0%) suggests that SIFT's forgery classifications were highly accurate. The recall score indicates that SIFT captured most of the forgeries (83.7%) in the dataset but missed a small percentage. The F1 score is relatively high (89.7%), signifying a balanced performance between precision and recall. SURF achieved a good accuracy rate (82.4%), though slightly lower than BRISK and SIFT. The precision score for SURF is lower compared to the other methods only (62.7%), suggesting that it may have more false positives. The recall score is high, indicating that SURF captured a significant portion of the actual forgeries (92.5%). The F1 score, while reasonable, is lower than the other methods (74.3%), reflecting a trade-off between precision and recall, with some false positives. In summary, BRISK stands out as the method with the highest accuracy, precision, and F1 score, indicating strong performance in copy-move forgery detection. SIFT also performs well overall, with high accuracy and a balanced F1 score. ORB and SURF show good but comparatively lower performance, with slight trade-offs between precision and recall. The choice of method should consider the specific requirements and trade-offs in your CMFD application.

1.6 Conclusion and Future Scope

These key-point-based methods play a crucial role in feature-based image matching and copy-move forgery detection, as they provide distinctive points in an image that can be used to identify regions with similar content, potentially indicating forgery. The choice of method depends on factors like computational efficiency, robustness to various transformations, and the specific application requirements. This paper provides an evaluation of the performance of these key-point-based algorithms in detecting copy-move forgeries. This work assessed the performance of the four State-of-the-art SIFT, SURF, BRISK and ORB algorithms on CoMoFoD dataset in terms of accuracy, precision, recall and f1-score. The comparative results reveal distinct performance characteristics among the algorithms, with BRISK emerging as the top performer, achieving high accuracy, precision, and an impressive F1 Score. SIFT also demonstrates strong overall performance, while ORB and SURF exhibit good but comparatively lower performance, with specific trade-offs between precision and recall. The work serves as a benchmark for the state-of-the-art in copy-move forgery detection, shedding light on areas for further research and enhancement in the field of image forensics and tamper detection. Incorporating deep learning techniques, such as CNNs or recurrent neural networks (RNNs), into copy-move forgery detection can be a promising avenue for further research, as deep learning models have demonstrated remarkable capabilities in various computer vision tasks and may enhance detection accuracy.

1.7 References

[1]. Ferreira, W. D., Ferreira, C. B., da Cruz Júnior, G., & Soares, F. (2020). A review of digital image forensics. Computers & Electrical Engineering, 85, 106685.

[2]. Mayer, O., & Stamm, M. C. (2019). Forensic similarity for digital images. IEEE Transactions on Information Forensics and Security, 15, 1331-1346.

[3]. Alberry, H. A., Hegazy, A. A., & Salama, G. I. (2018). A fast SIFT based method for copy move forgery detection. Future Computing and Informatics Journal, 3(2), 159-165.

[4]. Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. ACM Computing Surveys (CSUR), 54(1), 1-41.

[5]. Verdoliva, L. (2020). Media forensics and deepfakes: an overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910-932.

[6]. Amiri, E., Mosallanejad, A., & Sheikhahmadi, A. (2021). Copy-Move Forgery Detection by an Optimal Keypoint on SIFT (OKSIFT) Method. Journal of Computer & Robotics, 14(2), 11-19.

[7]. Akar, F. U. N. D. A. (2022). A HYBRID COPY-MOVE FORGERY DETECTION METHOD WITH FAST AND SURF.

[8]. Velmurugan, S., & Subashini, T. S. (2022, March). Binary descriptors for Copy-Move Forgery Detection in Digital Photographs. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1345-1352). IEEE.

[9]. Xue, Z., Tian, L., & Li, C. (2021). Passive Image Copy–Move Forgery Detection Based on ORB Features. In Recent Developments in Intelligent Computing, Communication and Devices: Proceedings of ICCD 2019 5 (pp. 312-317). Springer Singapore.

[10]. Teerakanok, S., & Uehara, T. (2019). Copy-move forgery detection: A state-of-the-art technical review and analysis. IEEE Access, 7, 40550-40568.

[11]. Zhang, Z., Wang, C., & Zhou, X. (2018). A Survey on Passive Image Copy-Move Forgery Detection. Journal of Information Processing Systems, 14(1).

[12]. Soni, B., Das, P. K., & Thounaojam, D. M. (2019). Geometric transformation invariant block based copy-move forgery detection using fast and efficient hybrid local features. Journal of information security and applications, 45, 44-51.

[13]. Armas Vega, E. A., González Fernández, E., Sandoval Orozco, A. L., & García Villalba, L. J. (2021). Copy-move forgery detection technique based on discrete cosine transform blocks features. Neural Computing and Applications, 33, 4713-4727.

[14]. Abd Warif, N. B., Wahab, A. W. A., Idris, M. Y. I., Ramli, R., Salleh, R., Shamshirband, S., & Choo, K. K. R. (2016). Copy-move forgery detection: survey, challenges and future directions. Journal of Network and Computer Applications, 75, 259-278.

[15]. Ardizzone, E., Bruno, A., & Mazzola, G. (2010, October). Copy-move forgery detection via texture description. In Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence (pp. 59-64).

[16]. Teerakanok, S., & Uehara, T. (2018, July). Copy-move forgery detection using GLCM-based rotation-invariant feature: a preliminary research. In 2018 IEEE 42nd annual computer software and applications conference (COMPSAC) (Vol. 2, pp. 365-369). IEEE.

[17]. Mokhtari Ardakan, M., Yerokh, M., & Akhavan Saffar, M. (2019). A new method to copy-move forgery detection in digital images using Gabor filter. In Fundamental Research in Electrical Engineering: The Selected Papers of The First International Conference on Fundamental Research in Electrical Engineering (pp. 115-134). Springer Singapore.

[18]. Alom, M. Z., Taha, T. M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M. S., ... & Asari, V. K. (2018). The history began from alexnet: A comprehensive survey on deep learning approaches. arXiv preprint arXiv:1803.01164.

[19]. Agarwal, R., & Verma, O. P. (2020). An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. Multimedia Tools and Applications, 79(11-12), 7355-7376.

[20]. Wu, J. (2017). Introduction to convolutional neural networks. National Key Lab for Novel Software Technology. Nanjing University. China, 5(23), 495.

[21]. Bellavia, F., & Colombo, C. (2020). Is there anything new to say about SIFT matching?. International journal of computer vision, 128(7), 1847-1866.

[22]. Hazgui, M., Ghazouani, H., & Barhoumi, W. (2021). Evolutionary-based generation of rotation and scale invariant texture descriptors from SIFT keypoints. Evolving Systems, 12(3), 591-603.

[23]. Bandara, R. (2017, August 30). Bag-of-features descriptor on SIFT features with opencv (BOF-SIFT). CodeProject. https://www.codeproject.com/Articles/619039/Bag-of-Features-Descriptor-on-SIFT-Features-with-O

[24]. Bay, H., Ess, A., Tuytelaars, T., & Van Gool, L. (2008). Speeded-up robust features (SURF). Computer vision and image understanding, 110(3), 346-359.

[25]. Ignat, A., & Păvăloi, I. (2021). Keypoint Selection Algorithm for Palmprint Recognition with SURF. Procedia Computer Science, 192, 270-280.

[26]. Tyagi, D. (2020, April 7). Introduction to surf (speeded-up robust features). Medium. https://medium.com/data-breach/introduction-to-surf-speeded-up-robust-features-c7396d6e7c4e

[27]. Rublee, E., Rabaud, V., Konolige, K., & Bradski, G. (2011, November). ORB: An efficient alternative to SIFT or SURF. In 2011 International conference on computer vision (pp. 2564-2571). Ieee.

[28]. Liu, Y., Zhang, H., Guo, H., & Xiong, N. N. (2018). A fast-brisk feature detector with depth information. Sensors, 18(11), 3908.

[29]. Singh, N. P., & Singh, V. P. (2020). Efficient Segmentation and Registration of Retinal Image Using Gumble Probability Distribution and BRISK Feature. Traitement du Signal, 37(5), 855-864.

[30]. Tralic, D., Zupancic, I., Grgic, S., & Grgic, M. (2013, September). CoMoFoD—New database for copy-move forgery detection. In Proceedings ELMAR-2013 (pp. 49-54). IEEE.

[31]. Hersbach, H., Bell, B., Berrisford, P., Hirahara, S., Horányi, A., Muñoz-Sabater, J., ... & Thépaut, J. N. (2020). The ERA5 global reanalysis. Quarterly Journal of the Royal Meteorological Society, 146(730), 1999-2049.