IMAGE FORGERY DETECTION USING WAVELET BASED SIFT FEATURE

Satyendra Singh, Research Scholar, Satyendra@allduniv.ac.in
Dr. Rajesh Kumar, Assistant Professor,
Department of Electronic and Communication (JK Institute of Applied Physics and Technology),
University of Allahabad, Prayagraj. rajeshkumariitbhu@gmail.com

Abstract

Manipulation in the content of digital images becoming effortless and popular due to freely availability of advance photo editing tools. Content of digital images can be manipulated by using simple steps. Photos are used in many important areas, such as the courtroom, healthcare, magazines, newspapers, etc. The image authenticity and integrity are important. In photo manipulation, copy-move is a very common photo forgery technique. It has a simple process to create forged images. Copy specific content of a photo and paste it into the same photo. We proposed an experimental approach for identification of copy-move photo manipulation using a wavelet-based SIFT (scale invariant feature transform) feature transform. DWT2 db1 is used for segmentation of forge image. The scale invariant feature transform is applied to the segmented image for feature extraction. The extracted features are matched with features of ground truth image. Finally, the experimental setup detected the copy move forgery. The experimental results are shown in terms of average accuracy 97.82%, precision 98.44%, recall 100%, and f-measure 99.21%. The proposed method performs better on the forged image suffering from various geometric attacks like translation, scaling, distortion, and combination.

Keywords: Fake image; Digital image; Copy move forgery; Scale invariant feature transform; Photo forensics

Introduction

Image processing technology is increasing due to the advancement of new technologies. Image is a combination of pixel elements. Each element has a specific location and value. These elements are referred to as pixels and picture elements. We are more familiar with digital images due to the use of images in our daily lives. Photograph are used in various fields such as social media, education, entertainment, courtrooms, etc., the development of digital image processing techniques to improve image visual quality and image editing facilities. With the advancement of image manipulation application software (e.g., CorelDRAW and Adobe Photoshop) (Wang et al., 2019). It is simple to produce altered images. Therefore, authenticity of digital photo has questionable. Fake images are widely used in political campaigns, to spread rumours in society and for photo pranks. The identification of authentic digital images is more difficult for us. In a courtroom without validating the authenticity of photo is not permissible.

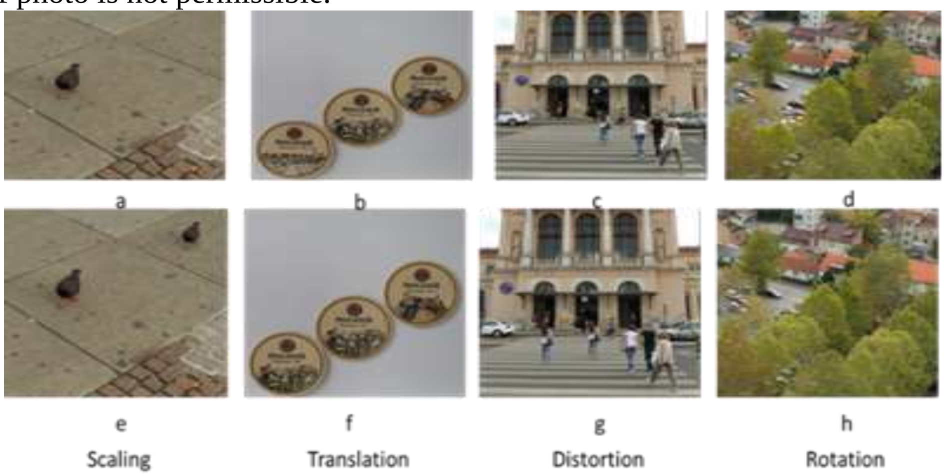

Figure 1: Examples of copy move forged images with transformation such as scaling, translation, distortion and rotation, images (a, b, c, d) are real photo and (e, f, g, h) forged photo and these photos collected from (Tralic et al., 2013).

The authenticity of the digital image is more important (Asghar et al., 2017; Yang et al., 2017; Abd Warif et al., 2016; Alkawaz et al., 2018; Ghorbani et al., 2011; Al-Qershi et al., 2013; Rani et al., 2021; Armas Vega et al., 2021; Kaur et al., 2022). Above Figure 1 demonstrate an example of the real photo and a fake photo with geometrical attacks. Copy move manipulation technique is a very common type of photo forgery (Yang et al., 2018). The aim of this forgery is to hide the original image information. In this experimental work, we used a wavelet-based sift feature to identify copy move photo manipulation. The wavelet is a dwt2 db1 wavelet transform. The input image is divided into four sub bands by the dwt2 db1. The sub-bands are CA, CH, CV, and CD. The CA approximation coefficient matrix and the CH, CV, and CD details coefficient matrices have horizontal, vertical, and diagonal coefficients, respectively. Step second to extract features from the segmented image, SIFT is used. The third step is feature matching. In fourth step detect forge region. The final step is measuring the performance.

Statement of the Problem

In digital image manipulation detection, researchers identified lots of copy-move manipulation identification tools that are present in the existing work. We discovered a research gap in existing tools of detecting copy-move manipulation. In large-scale manipulation, experiment is not efficient and gets poor detection results (Chen et al., 2020). Copy-move manipulation identification tools have many challenges, such as contrast adjustment, inpainting, large scale rotation, and additive noise (Mahmood et al., 2018). These challenges are the motivation of many researchers and scientists to work on image forgery detection worldwide.

Objectives of the study

- To identify copy-move manipulation.
- To analyze the performance on geometric attacks such as distortion, scaling, translation, and rotation.

In the proposed experiments, we used the SIFT algorithm because SIFT generates more feature points even in small or smooth parts as compared to the SURF algorithm (Li, et al., 2018).

Review of Literature

In last two decades, research in the field of photo manipulation has increased rapidly. Many researchers and scientists are involved to develop digital image forensics tools. In this section, we will analyse existing work in photo forgery detection and in the field of photo forensics.

(Rao et al., 2016) The authors describe a deep learning-based convolution neural networks that best performs on several copy-move and image splicing datasets. Image inpainting forensic is another field of digital image forensic technique. It is an image repair technique. (Zhu et al., 2018) a CNN based deep learning model to identify image inpainting manipulation. (Lee et al., 2021) created a deep learning tool to detect automatically generated fake face images generated by generative adversarial networks (GAN).

(Ghorbani et al., 2011) propose a model to be developed using an improved discrete cosine transform. The decomposition of quantization coefficients in this paper is based on the DWT. The objective of model is to detect copy-move image forgery. It is not efficient in translation, rotation, and scaling. It works only for simple image forgery. In the future, we shall be working to ensure that extracted features are invariant with rotation, translation, and scaling forgery.

(O'brien et al., 2012) this work, the author proposed a new digital image forensic technique. The focus of this study is geometric inconsistencies. The fake reflections are inserted into a picture to create a manipulated picture. The proposed method is insensitive to some photo editing methods like colour manipulation, resampling, and lossy compression.

(Niyishaka et al., 2020) The authors describe a copy move manipulation detection model. In this experimental work, we use the MICC-F220, MICC-F8multi, and CoMoFoD datasets. improved the performance of present copy move manipulation identification tools like key-point based, and block-based. This method works on transformations (rotation, scaling, translation).

(Wu et al., 2018) introduce a deep learning model called Buster net for copy move manipulation identification. Buster net is an end-to-end trainable deep learning-based neural network. The buster net should better perform on two freely available copy-move forgery datasets CoMoFoD and CASIA. It differentiates between source copies.
(Sadeghi et al., 2018) author analyzed different copy-move manipulation identification techniques and determined which techniques are best performed with different photo attributes like rotation, scaling, translation, and JPEG compression. also highlights the pros and cons of each method. The author differentiates between block based and key point-based methods to identify copy move manipulation and finds that key point-based approaches are better because of good performance and computation time in comparison to block-based approaches.
(Huang et al., 2018) author proposed an experimental work for an image manipulation identification using CNN. This neural network detects splicing forgery too. (Yang et al., 2018) describe a copy-move manipulation identification method. The feature-based SIFT method is used to identify copy-move photo manipulation. The experimental work overcomes the problem of lacking key points in key point selection.
(Li et al., 2018) In this paper, the author suggests a copy-move manipulation tool. The hierarchical key-point matching algorithm is used to detect copy-move manipulation. Proposed tool fails when we have a small or smooth forging region in the fake image.
In Table 1, we show the previous study in comparative manner of photo manipulation and focused on copy-move forger detection approaches.

Table 1: Comparative study of previous works of copy move manipulation detection techniques

Method	Techniques	Detection Domain	Characteristics
(Yang et al., 2018)	Modified SIFT	Copy-move	This method is robust to detecting forged regions.
(Wang et al., 2019)	SURF and PCET	Copy-move	It takes less computation. Work on a smooth forged region and high brightness.
(Christlein et al., 2012)	SIFT and block-based techniques (DCT, DWT, KPCA, PCA and ZERNIKE)	Copy-move forgery	SIFT is very efficient and it takes little computation. In block-based techniques, the author recommends Zernike due to its small memory footprint.
(Rao et al., 2016)	Deep learning-based CNN	Copy-move and splicing	This method best performs on different public datasets.
(Kuznetsov et al., 2019)	VGG-16 CNN	Splicing	The CASIA dataset classification accuracy for the fine-tuned model was 97.8% and 96.4% for the zero-staged train.
(Abdalla et al., 2019)	Deep learning-based CNN and GAN	Copy-move	The model better performs with accuracy about 95%. In the future, it works on different forgeries.
(Lin et al., 2009)	Radix sort	Copy-move	It is efficient for attacking Gaussian noise and JPEG compression. It is also working on rotation (fixed angles). It is not efficient for small forged regions.
(Hu et al., 2011)	DCT based lexicographical sort.	Copy-move	It reduces false matching rates and maintains detection accuracy.
(Alberry et al., 2018)	SIFT and Fuzzy c-means clustering.	Copy-move	Proposed tool was tested on the MICC-220 dataset and reduced time complexity. It is efficient for different

			attacks such as rotation, scaling, and translation.
(Mahmood et al., 2018)	Stationary Wavelet Transform (SWT) and DCT	Copy-move	It outperforms on geometric attacks like scaling, rotation, blurring, and JPEG compression.
(Abbas et al., 2021)	Deep learning-based model SmallerVGGNet and MobileNet2.	Copy-move	This model is light-weight and provides reliable detection results. In future, it can also be extended to multiple forgeries.

In Table 2 discuss some other existing approaches of scale invariant feature transform (SIFT) based security method for image security.

Table 2: Analysis of existing work scale invariant feature transform based method for image security.

Method	**Approaches**	**Study domain**	**Observations**
(Liu et al., 2019)	SIFT-DCT	Encryption of medical image.	It is robust to geometric attacks. The method is flexible for medical image processing and image transmission security.
(Ahmad et al., 2020)	Wavelet and SIFT features	Watermark for image security.	The method is work for affine transformation. The watermark security is guaranteed in frequency domain. The proposed tool needs to store SIFT feature information as a carrier photo.
(Fang, et al., 2022)	SIFT and Bandelet-DCT	Zero-water marking for medical image.	The proposed algorithm is well performed on both geometric attacks common attacks.
(Bhatti et al., 2020)	Arnold transform and Chaotic encryption, Quaternion Fourier Transform (QFT)	Enhancement of watermark security in color images.	Experimental algorithm has better performance. The Clifford algebra to analyse the photo information.

Research Methodology

To perform the program in the proposed experiment, we used the Windows 11 operating system, a core i5 Intel processor with 8 GB of RAM, and MATLAB 2017b software. The (Tralic et al., 2013) dataset has been used in the proposed experimental work. The dataset has original and fake photos with geometric attacks.

The DWT2 db1 and SIFT algorithms have been used in the experiment.

DWT2 – DWT2 has three different variants, such as Daubechies (db) 1, (db) 2 and Haar wavelet (Kumar et al., 2017). In this experimental work, we used a dwt2 db1 to segment the input photo. The input photo has segmented into four subparts. The segmented parts are CA, CH, CV, and CD. The approximation coefficient CA and the detailed coefficient CH, CV, and CD represent the horizontal coefficient, vertical coefficient, and diagonal coefficient, respectively. To the further process, we applied the SIFT algorithm.

SIFT – photo has many important interest points, which can be extracted by feature extraction methods such as SIFT and SURF. The scale invariant feature transform is a familiar feature descriptor algorithm in the field of photo manipulation identification. SIFT matches, describes, and

detects local features of an image. The detected features by the SIFT algorithm are invariants with many geometric attacks scaling, translation, rotation. In the SIFT algorithm, there are some important steps that follow. Find the location scale of each key-point. key-point scale and localization, orientation assignment for each key-point, and determining key-point descriptors (Lowe et al., 1999).
The SIFT algorithm-based method is complete in five important steps (1) Space extrema detection, (2) Key point localization, (3) Orientation Assignment, (4) Key point descriptor and (5) Feature Matching.

1. Space extrema detection
In this step, SIFT features are extracted in different image locations and scales. Gaussian blur is used to achieve scale space extrema and use the gaussian function. the input image I(x, y) and gaussian function G(x, y, σ).

$$L(x, y, \sigma) = G(x, y, \sigma)\times I(x, y) \qquad (1)$$

In equation (1) L is the convolution of the input image I.

Find the key points by the Difference of Gaussian (DOG) and subtract the two successive photos at the same level.

$$\begin{aligned} D(x, y, \sigma) &= (G(x, y, \sigma) - G(x, y, \sigma))\times I(x, y) \\ &= L(x, y, k\sigma) - L(x, y, \sigma). \end{aligned} \qquad (2)$$

In equation (2) σ is the size of scale space.

2. Key points localization
In the key point localization step, illuminate low-contrast key points. The poor contrast key point is removed if this function value is less than a threshold and only specific feature points has obtained.

3. Orientation assignment
In this stage, assign orientation to each key point. The local image region is described in a way invariant to the affine transform (scale, rotation, and translation). Around each feature point, its magnitude and gradient direction are calculated. For each points the magnitude m(x, y) and orientation Θ(x, y) are computed as

$$m(x, y) = \sqrt{\left(L(x+1, y) - L(x-1)\right)^2 + \left(L(x, y+1) - L(x, y-1)\right)^2} \qquad (3)$$

$$\Theta(x, y) = \tan^{-1}\left(\frac{L(x,\ y+1)-L(x,\ y-1)}{L(x+1,\ y)-L(x-1,\ Y)}\right) \qquad (4)$$

Equation (3) is used for calculating gradient modulus and equation (4) for gradient magnitude.

4. Key point descriptor
The calculated gradient data has been used to generate key point descriptors. Number of key points are multiplied by 128 and it create a 16×16 neighborhood around the key points that next divided 16 subblocks of size 4×4 and each sub-block have 8 bins orientation. So finally, 4×4×8 = 128 bins.

5. Feature Matching
In this step, we store the key points of the sample image and match them with the tested image. The SIFT algorithm matches key points using a best-bin-first search method.

Proposed work has been used both wavelets transform and SIFT algorithm. SIFT has used to extract features from segmented part CA(LL). The extracted features of image are invariant to rotation, scaling, translation, noise, and distortion.

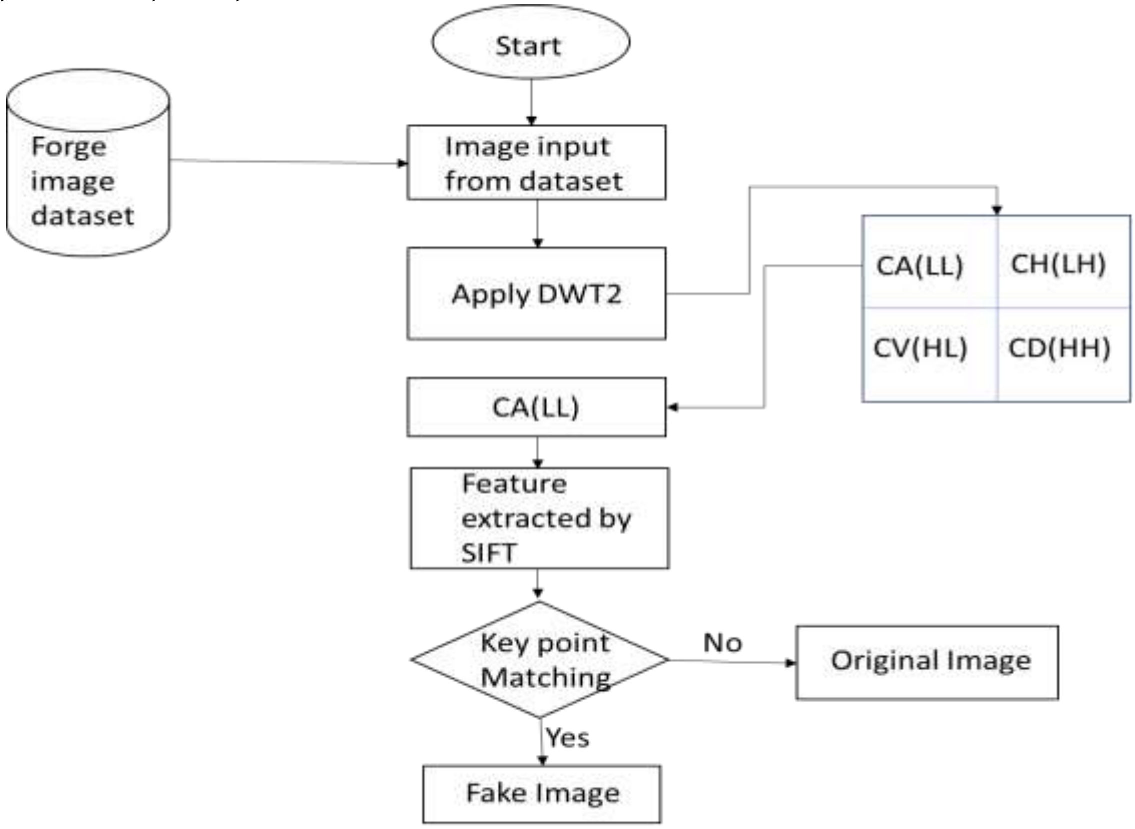

Figure 2:Flow chart of the proposed method

In the experimental approach, according to Figure 2, first read the image and apply DWT2 for image segmentation. Then SIFT is used for feature extraction and match extracted features. If feature is matched, then draw a line between matching points then resulted image is fake image and feature is not matched then resulted image is original.

In the initial step, input the image from the stored copy move forgery dataset. In the next step, a 2D wavelet transform is applied to input photo and segments it into four important subparts. The subparts are details coefficient (CH, CV, CD), horizontal coefficient CH, vertical coefficient CV, and diagonal coefficient CD, respectively and approximation coefficient CA. These coefficients have been recorded in a 2D array like in Figure 3.

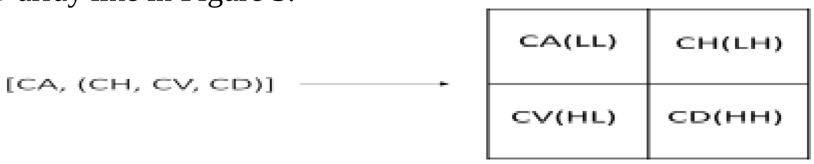

Figure 3: Segments of dwt2

In the further steps, SIFT is applied to a segmented block (CA), which has more information. The SIFT algorithm extracts key-points from block image. In feature matching step, the extracted features match with the help of the best bin search method. After matching the feature points, they labelled these matched features. The merge region process is performed after the completion of the feature point labelling process. Upon the completion of the important steps above, we get the final resultant detected image.

Results and Discussion

In this section results of proposed work have been analyzed. the results of each tested image demonstrate in Figure 5 below measure the performance of the proposed method. In this experiment, we measured accuracy, recall, precision, and F-measure. The results of developed method have been compared to the available performance in terms of recall, accuracy, F-measure, and precision. Figure 5 shows experimental result.

The common criteria for measuring the performance of copy move manipulation detection approach in terms of recall, accuracy, f-measure, and precision, are as follows (Badr et al., 2020; Malviya et al., 2016):

True positive (Tp) – manipulated photo claimed to be original.

True negative (Tn) – original photo claimed to be original.

False positive (Fp) – predicted that the original image had been manipulated.

False negative (Fn) – fake image claimed to be real.

Precision: - the probability that a detected fake is actually a fake, evaluated as

$$\mathrm{P} = \frac{Tp}{Tp+Fp} \quad (5)$$

Recall: - The chance of spotting a fake image, represented by the letter "R," is calculated as

$$R = \frac{Tp}{Tp+Fn} \quad (6)$$

Accuracy: - Accuracy is the capability of a technique to measure an accurate value

$$Accuracy = \frac{Tp+Tn}{Tp+Tn+Fp+Fn} \quad (7)$$

F-measure: - The range of the F-measure score, from best to worst, is 1 to 0. It is described as a weighted average of recall and precision.

$$F - measure = \frac{(2*(RP))}{R+P} \quad (8)$$

Equations (5), (6), (7) and (8) are formula to calculate precision, recall, accuracy and F-measure respectively.

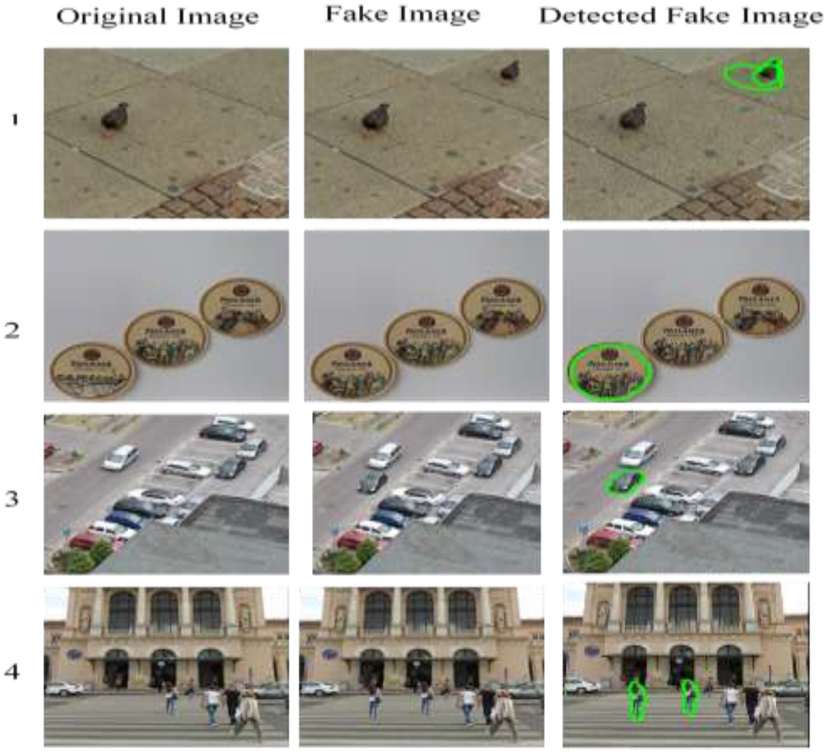

Figure 4: Results of proposed approach of copy move manipulation detection, image 1 with scaling transform, image 2 translation, image 3 combination and 4 with distortion transform.

The results of the developed method compared with other existing methods are shown in Table 3.

The comparison of the proposed method in terms of accuracy, precision, recall and f-measure.

Table 3:comparison of result of proposed method with existing techniques

Methods	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)
(Goel et al., 2021)	96	89	100	94

(Warif et al., 2017)	91.39	95.83	86.55	90.95
(Hashmi et al., 2013)	94	95.83	92	93.87
Proposed approach	**97.82**	**98.44**	**100**	**99.21**

Proposed copy-move manipulation detection techniques test on images collected from dataset Tralic D. et al, [11]. Table 3 shows the result of proposed approach on each test images. Experimental results written in table 3 and we calculate the value of recall, precision, accuracy and F-measure as quality parameters. From above experimental results for image 1 in figure 4 the value of measuring matrices accuracy is 98.51%, precision is 98.50%, recall is 100%, and F-measure is 99.24%. For image 2 in figure 4 the value of measuring matrices accuracy is 95.74%, precision is 95.78%, recall is 100% and F-measure is 97.84%. For image 3 in figure 4 the value of matrices accuracy is 98.79%, precision is 98.79%, recall is 100% and F-measure 99.39%. For image 4 in figure 4 the value of matrices accuracy is 98.62%, precision is 98.61%, recall is 100% and F-measure is 99.30%. In this experiment total 20 images have been tested.

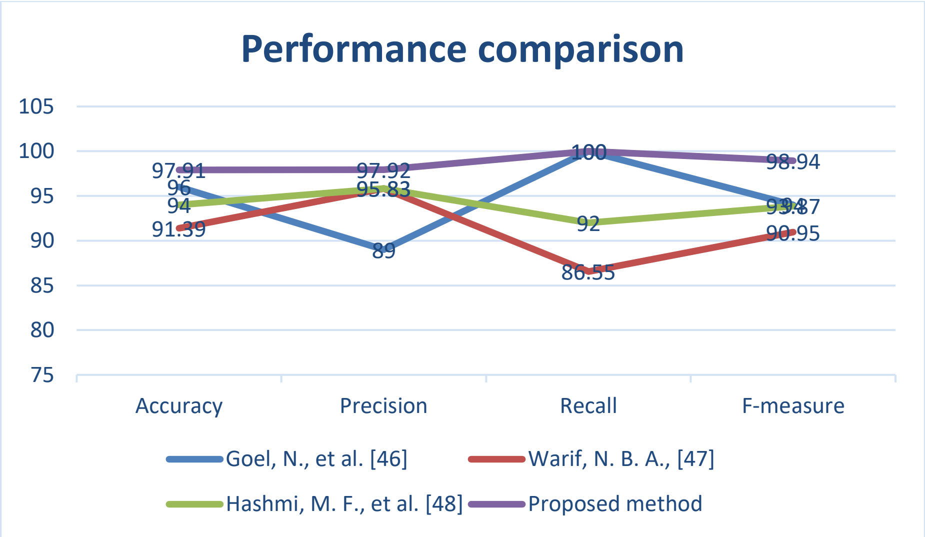

Figure 5: Performance comparison of proposed method with existing methods

Figure 5 demonstrates the comparison of the performance of proposed experimental work with other existing methods. The developed technique is well performed in comparison to existing techniques.

Conclusion

Experimental results coming from Figure 5 and Table 3 demonstrate that the experimental approach well performed to detect copy move manipulation in terms of measuring metrics. The proposed approach also performs better in scaling, combination, translation, and distortion transformed images. Therefore, the wavelet based SIFT method is robust and good for identification of copy-move infected images. Proposed system performs better in terms of detecting any type of copy-move image forgery. Thus, from the Table 3, we can say that the proposed system gives better results as compared to existing techniques in the literature. In the future, we will improve this method to identify other types of image forgeries by applying artificial intelligence and soft computing approaches.

References

1. Wang, C., Zhang, Z., Li, Q., & Zhou, X. (2019). An image copy-move forgery detection method based on SURF and PCET. *IEEE Access*, *7*, 170032-170047.
2. Asghar, K., Habib, Z., & Hussain, M. (2017). Copy-move and splicing image forgery detection and localization techniques: a review. *Australian Journal of Forensic Sciences*, *49*(3), 281-307.
3. Yang, F., Li, J., Lu, W., & Weng, J. (2017). Copy-move forgery detection based on hybrid features. *Engineering Applications of Artificial Intelligence*, *59*, 73-83.
4. 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.

5. Alkawaz, M. H., Sulong, G., Saba, T., & Rehman, A. (2018). Detection of copy-move image forgery based on discrete cosine transform. *Neural Computing and Applications*, *30*(1), 183-192.
6. Ghorbani, M., Firouzmand, M., & Faraahi, A. (2011, June). DWT-DCT (QCD) based copy-move image forgery detection. In 2011 18th International Conference on Systems, Signals and Image Processing (pp. 1-4). IEEE.
7. Al-Qershi, O. M., & Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic science international*, *231*(1-3), 284-295.
8. Rani, A., Jain, A., & Kumar, M. (2021). Identification of copy-move and splicing based forgeries using advanced SURF and revised template matching. *Multimedia Tools and Applications*, *80*(16), 23877-23898.
9. 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*(10), 4713-4727.
10. Kaur, N., Jindal, N., & Singh, K. (2022). An improved approach for single and multiple copy-move forgery detection and localization in digital images. *Multimedia Tools and Applications*, 1-31.
11. 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.
12. Chen, H., Yang, X., & Lyu, Y. (2020). Copy-move forgery detection based on keypoint clustering and similar neighborhood search algorithm. *IEEE Access*, *8*, 36863-36875.
13. Mahmood, T., Mehmood, Z., Shah, M., & Saba, T. (2018). A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform. *Journal of Visual Communication and Image Representation*, *53*, 202-214.
14. Yang, B., Sun, X., Guo, H., Xia, Z., & Chen, X. (2018). A copy-move forgery detection method based on CMFD-SIFT. *Multimedia Tools and Applications*, *77*(1), 837-855.
15. Li, Y., & Zhou, J. (2018). Fast and effective image copy-move forgery detection via hierarchical feature point matching. IEEE Transactions on Information Forensics and Security, 14(5), 1307-1322.
16. Rao, Y., & Ni, J. (2016, December). A deep learning approach to detection of splicing and copy-move forgeries in images. In 2016 IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 1-6). IEEE.
17. Zhu, X., Qian, Y., Zhao, X., Sun, B., & Sun, Y. (2018). A deep learning approach to patch-based image inpainting forensics. Signal Processing: Image Communication, 67, 90-99.
18. Lee, S., Tariq, S., Shin, Y., & Woo, S. S. (2021). Detecting handcrafted facial image manipulations and GAN-generated facial images using Shallow-FakeFaceNet. Applied soft computing, 105, 107256.
19. Ghorbani, M., Firouzmand, M., & Faraahi, A. (2011, June). DWT-DCT (QCD) based copy-move image forgery detection. In 2011 18th International Conference on Systems, Signals and Image Processing (pp. 1-4). IEEE.
20. O'brien, J. F., & Farid, H. (2012). Exposing photo manipulation with inconsistent reflections. ACM Trans. Graph., 31(1), 4-1.
21. Niyishaka, P., & Bhagvati, C. (2020). Copy-move forgery detection using image blobs and BRISK feature. Multimedia Tools and Applications, 79(35), 26045-26059.
22. Wu, Y., Abd-Almageed, W., & Natarajan, P. (2018). Busternet: Detecting copy-move image forgery with source/target localization. In Proceedings of the European conference on computer vision (ECCV) (pp. 168-184).
23. Sadeghi, S., Dadkhah, S., Jalab, H. A., Mazzola, G., & Uliyan, D. (2018). State of the art in passive digital image forgery detection: copy-move image forgery. Pattern Analysis and Applications, 21(2), 291-306.
24. Huang, N., He, J., & Zhu, N. (2018, August). A novel method for detecting image forgery based on convolutional neural network. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 1702-1705). IEEE.
25. Yang, B., Sun, X., Guo, H., Xia, Z., & Chen, X. (2018). A copy-move forgery detection method based on CMFD-SIFT. Multimedia Tools and Applications, 77(1), 837-855.
26. Li, Y., & Zhou, J. (2018). Fast and effective image copy-move forgery detection via hierarchical feature point matching. IEEE Transactions on Information Forensics and Security, 14(5), 1307-1322.
27. Yang, B., Sun, X., Guo, H., Xia, Z., & Chen, X. (2018). A copy-move forgery detection method based on CMFD-SIFT. *Multimedia Tools and Applications*, *77*(1), 837-855.
28. Wang, C., Zhang, Z., Li, Q., & Zhou, X. (2019). An image copy-move forgery detection method based on SURF and PCET. *IEEE Access*, *7*, 170032-170047.

29. Christlein, V., Riess, C., Jordan, J., Riess, C., & Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on information forensics and security*, *7*(6), 1841-1854.
30. Rao, Y., & Ni, J. (2016, December). A deep learning approach to detection of splicing and copy-move forgeries in images. In 2016 IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 1-6). IEEE.
31. Kuznetsov, A. (2019, November). Digital image forgery detection using deep learning approach. In *Journal of Physics: Conference Series* (Vol. 1368, No. 3, p. 032028). IOP Publishing.
32. Abdalla, Y., Iqbal, M. T., & Shehata, M. (2019). Copy-move forgery detection and localization using a generative adversarial network and convolutional neural-network. *Information*, *10*(9), 286.
33. Lin, H. J., Wang, C. W., & Kao, Y. T. (2009). Fast copy-move forgery detection. WSEAS Transactions on Signal Processing, 5(5), 188-197.
34. Hu, J., Zhang, H., Gao, Q., & Huang, H. (2011, September). An improved lexicographical sort algorithm of copy-move forgery detection. In 2011 Second International Conference on Networking and Distributed Computing (pp. 23-27). IEEE.
35. 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.
36. Mahmood, T., Mehmood, Z., Shah, M., & Saba, T. (2018). A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform. *Journal of Visual Communication and Image Representation*, *53*, 202-214.
37. Abbas, M. N., Ansari, M. S., Asghar, M. N., Kanwal, N., O'Neill, T., & Lee, B. (2021, January). Lightweight deep learning model for detection of copy-move image forgery with post-processed attacks. In 2021 IEEE 19th World Symposium on Applied Machine Intelligence and Informatics (SAMI) (pp. 000125-000130). IEEE.
38. Liu, J., Li, J., Chen, Y., Zou, X., Cheng, J., Liu, Y., & Bhatti, U. A. (2019). A robust zero-watermarking based on SIFT-DCT for medical images in the encrypted domain. *Comput. Mater. Continua*, *61*(1), 363-378.
39. Ahmad, R. M., Yao, X., Nawaz, S. A., Bhatti, U. A., Mehmood, A., Bhatti, M. A., & Shaukat, M. U. (2020, June). Robust Image Watermarking Method in Wavelet Domain Based on SIFT Features. In Proceedings of the 2020 3rd International Conference on Artificial Intelligence and Pattern Recognition (pp. 180-185).
40. Fang, Y., Liu, J., Li, J., Cheng, J., Hu, J., Yi, D., ... & Bhatti, U. A. (2022). Robust zero-watermarking algorithm for medical images based on SIFT and Bandelet-DCT. *Multimedia Tools and Applications*, *81*(12), 16863-16879.
41. Bhatti, U. A., Yu, Z., Li, J., Nawaz, S. A., Mehmood, A., Zhang, K., & Yuan, L. (2020). Hybrid watermarking algorithm using clifford algebra with Arnold scrambling and chaotic encryption. *IEEE Access*, *8*, 76386-76398.
42. Kumar, M., Jindal, M. K., & Sharma, R. K. (2017). Offline handwritten Gurmukhi character recognition: analytical study of different transformations. Proceedings of the National Academy of Sciences, India Section A: Physical Sciences, 87(1), 137-143.
43. Lowe, D. G. (1999, September). Object recognition from local scale-invariant features. In Proceedings of the seventh IEEE international conference on computer vision (Vol. 2, pp. 1150-1157). Ieee.
44. Badr, A., Youssif, A., & Wafi, M. (2020, June). A robust copy-move forgery detection in digital image forensics using SURF. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
45. Malviya, A. V., & Ladhake, S. A. (2016). Pixel based image forensic technique for copy-move forgery detection using auto color correlogram. *Procedia Computer Science*, *79*, 383-390.
46. Goel, N., Kaur, S., & Bala, R. (2021). Dual branch convolutional neural network for copy move forgery detection. IET Image Processing, 15(3), 656-665.
47. 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.
48. 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.

