I.J. Image, Graphics and Signal Processing, **2018, 4, 22-30**
Published Online April 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2018.04.03

Hybridized Technique for Copy-Move Forgery Detection Using Discrete Cosine Transform and Speeded-Up Robust Feature Techniques

Joseph A. Ojeniyi
Department of Cyber Security Science, Federal University of Technology, Minna, Niger State, Nigeria
Email: ojeniyija@futminna.edu.ng

Bolaji O. Adedayo, Idris Ismaila and Abdulhamid M. Shafi'i
Department of Cyber Security Science, Federal University of Technology, Minna, Niger State, Nigeria
Email: bj4lastb@gmail.com, ismi.idris@futminna.edu.org and shafii.abdulhamid@futminna.edu.ng

Received: 10 January 2018; Accepted: 24 February 2018; Published: 08 April 2018

***Abstract*—**As the world has greatly experienced a serious advancement in the area of technological advancement over the years, the availability of lots of sophisticated and powerful image editing tools has been on the rise. These image editing tools have become easily available on the internet, which has made people who are a novice in the field of image editing, to be capable of tampering with an image easily without leaving any visible clue or trace behind, which has led to increase in digital images losing authenticity. This has led to developing various techniques for tackling authenticity and integrity of forged images. In this paper, a robust and enhanced algorithm is been developed in detecting copy-move forgery, which is done by hybridizing block-based DCT (Discrete Cosine Transform) technique and a keypoint-based SURF (Speeded-Up Robust Feature)technique using the MATLAB platform. The performance of the above technique has been compared with DCT and SURF techniques as well as other hybridized techniques in terms of precision, recall, FPR and accuracy metrics using MICC-F220 dataset. This technique works by applying DCT to the forged image, with the main goal of enhancing the detection rate of such image and then SURF is applied to the resulting image with the main goal of detecting those areas that are been tampered with on the image. It has been observed that this paper's technique named HDS has an effective detection rate on the MICC-F220 dataset with multiple cloning attacks and other various attacks such as rotation, scaling, a combination of scaling plus rotation, blur, compression, and noise.

***Index Terms*—**Copy-move image forgery, block-based method, keypoint-based method, DCT, SURF

I. Introduction

The technological world has been evolving at a tremendous pace over the past few decades in terms of development, which has been characterized by the widespread of digital images. These digital images are commonly used to convey information through various mediums such as scientific journals, magazines, newspapers, fashion industries or the internet. They are also used as evidence for different purposes, like crime evidence or court halls [1]. Image forgery can simply be defined as a means of manipulating a digital image in such a way as to hide some useful or important information on the image, which can result to damages on a person reputation or interference with judicial process or creation of a bogus event for propaganda purposes or cause financial loss to an organization or company [2].

When compared to the nature of conventional image forgery, digital image forgery doesn't differ very much. The only major difference is that digital image forgery is concerned with only digital images. With the help of cameras with high digital resolution, personal computers with high processing power and photo editing application that are sophisticated, the manipulation of digital images are becoming simple and easy to perform [3]. The process of making an image forgery has been made simple with the introduction of sophisticated computer editing image software such as Corel Paint Shop, GNU Image Manipulation Program, and Adobe Photoshop, which some of them can be purchased online for free [4].

There are basically three classes of digital image forgery, which is based on the process by which they are created. These categories are Image Retouching, Image Splicing and the Copy-Move Forgery [5].

Image retouching, sometimes called airbrushing, can be referred to a process of manipulating images in order to slightly change the looks of the original image without significant changes. This type of digital image forgery is less harmful when compared to the other two types [6].

Image splicing technique used for the creation of image forgery is more aggressive when compared to image retouching technique. This method can easily be processed by cropping and pasting a portion of an image from the same or different image sources. This technique

is often referred as paste-up, which is created by using digital tools like Adobe Photoshop to stick together with those images. In this particular technique, it combines two or more images, to produce an image forgery [7].

The copy-move forgery technique is much similar to the splicing image technique as both techniques modify a particular portion of the targeted image. But it differs in the aspect of the image source, this technique uses the same target image as its source instead of using a separate image as its source. This technique is difficult and is the most commonly used technique for image forgery. It is used mainly to cover a certain portion of an image, with the goal of removing or adding certain information on the image. The manipulation process involves copying a particular part of the image and moving the particular portion to the desired location and then pasting the copied portion into that location. The blurring of the edge of the copied portion is usually applied, so as to reduce the irregularity between the pasted portion and the original image [8].

In this paper, we will be focusing on just one of the three types of forgery, which is the CMF (copy-move forgery). The Fig. 1 shows a simple example of a copy-move forgery, where the Prime Minister of Canada, William Lyon Mackenzie, removed King George VI from the original photograph with the PM alongside Queen Elizabeth. The image was used on an election poster for the Prime Minister. The goal of this forgery was a political propaganda, as an image of just Mackenzie with the Queen puts him in a more powerful light [9].

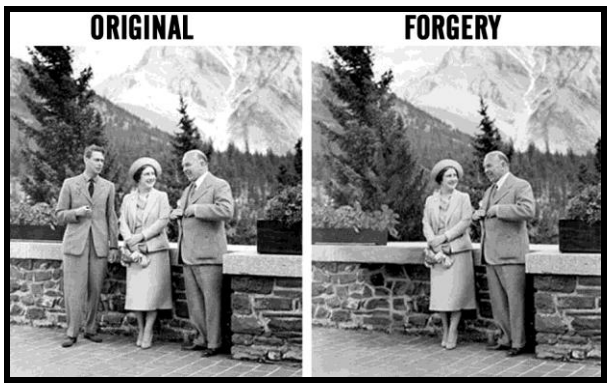

Fig.1. An example of copy-move forgery [9]

When CMF is combined with further attacks, it makes the detection of the manipulated portion in the digital image difficult. This additional attacks can either be intermediate processing operation (geometric transform) or post-processing operation [10] as shown in Fig. 2.

The remaining part of this paper is structured as follows: Section-II presents the copy-move image forgery detection techniques. In Section-III, a related work is presented showing the contribution of various researchers in the detection of CMF, while Section-IV presents the methodology used for the copy-move forgery detection. In section-V, the paper presents the results and discussion of the methodology used. Lastly, Section-VI encompasses the summary and conclusion of the paper and also suggest future work that can be carried out on this paper.

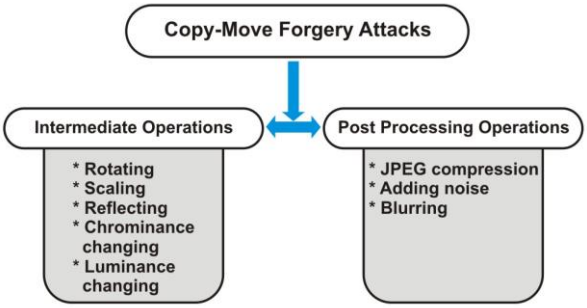

Fig.2. A summary of image processing operation using CMF

II. Copy-Move Forgery Detection Approach

Image forgery detection can be broadly grouped into two approaches depending on if the original image is available or not available. These two groups are active and passive approach [5]. The active detection approach involves the addition of the image details with the goal of determining and describing if the image has been tampered with. These details could be signature, date, name or simply the metadata of the image. This method requires a specific type of hardware to be implemented for it to be cable of authenticating the digital image [11]. There are basically two types of techniques that use the active approach: Digital Signature and Digital Watermarking [12]. The passive detection approach authenticates the images for forgery without requiring the original image signature or watermark, it uses the traces that have been left behind during the manipulation process of the image. This approach simply works by analyzing the binary properties of the digital image, with the purpose of detecting if there are any forgery traces or not. The passive approach has some benefits such as it works mainly on binary information and does not require any kind of previous information or properties about the original image [13].

CMFD (copy-move forgery detection) is a technique that is used in detecting and authenticating if a digital image has been manipulated using CMF [14]. It is easy and effective to manipulate an image in CMF, especially when the source and the targeted image portion are from the same image. This makes it very difficult to detect with a naked eye, as those features such as noise, the temperature of color and illumination properties are commonly matched between the original image and the manipulated portion [15].

The CMFD can be categorized into two approaches based on the segmentation plan, namely the block-based approach and the keypoint-based approach [16]. The block-based approach uniformly partitions the image into blocks, this blocks can either be a smaller non-overlapping or overlapping square shape or partitions of circular shapes [17]. While in the keypoint-based approach, there is no subdivision rather it computes its

feature on image portion that has a high entropy [18]. Table 1 shows a summary of the two approaches. However, our focus is on DCT and SURF techniques.

Table 1. A summary of CMFD Classification

Block-based Approach	Keypoint-based Approach
* DCT (Discrete Cosine Transform)	* SIFT (Scale Invariant Feature Transform)
* Fourier Transform	* Harris Corner Detector
* FWHT (Fast Walsh-Hadamard Transform)	* SURF (Speeded-Up Robust Features)
* DWT (Discrete Wavelet Transform)	
* DyWT (Dyadic Wavelet Transform)	
* Wiener Filter Wavelet	
* PCA (Principle Component Analysis)	

These two detection approaches are briefly discussed in the following subsections.

A. Block-based Approach

This approach involves splitting the image into blocks of either circle or square for analysis in the pre-processing phase. The split blocks can either overlap each other or not depend on the technique used. After the splitting into blocks, the features are extracted from each of those blocks and a comparison is made on each other to determine the similarity of the blocks inside the image. As soon as a match is detected, the blocks represent the CMF manipulation carried on the image [19]. An illustration of the process is shown in Fig. 3. The block-based approach that is commonly used is DCT, Fourier Transform, FWHT, DWT, DyWT and Wiener Filter Wavelet.

The blocked-based approach is generally robust against various post-processing and intermediate operations such as blurring, noise addition and compression in the copied region. But they are not effective in detecting geometrical transformations such as rotation and scaling. This approach is also found to be computationally inefficient, thus requiring more time for it process.

B. Keypoint-based Approach

The keypoint-based approach is different from the block-based approach as it doesn't split the images into blocks in the pre-processing phase as shown in Fig. 4. In this approach extraction of features is by distinctive features like image edges, the image blobs, and image corners. Each of the features is assigned with a set of a descriptor that is generated with the portion surrounding the features. This descriptor assists in increasing the reliability of the feature in relation to the affine transformation. Next, the feature and the descriptors are both categorized and are been matched to with each other, with the goal of identifying duplicate portion in the CMF [20]. The commonly used keypoint-based approaches are SUFF (Speeded-Up Robust Features), HCD (Harris Corner Detector) and SIFT (Scale Invariant Feature Transform) [16].

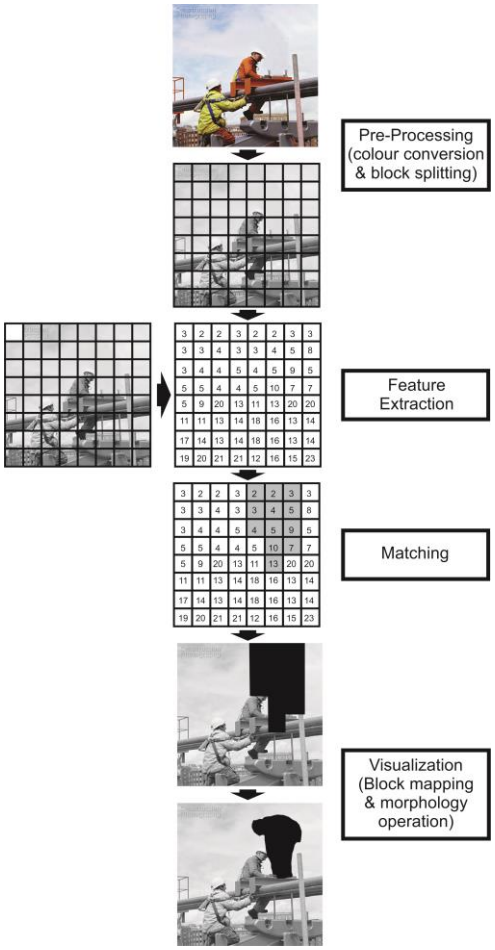

Fig.3. The Block-based approach process for CMFD [16]

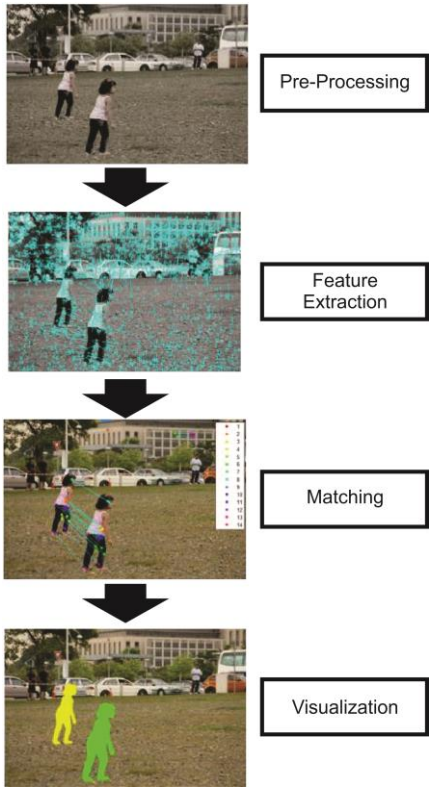

Fig.4. The Keypoint-based approach process for CMFD [16]

The keypoint-based approach is capable of easily tackling the issue of geometric transformation, but the drawback is that it cannot effectively deal with the noise and compression addition in the region that is duplicated. This approach is faster than the block-based approach due to the high computational complexity that it has. To effectively make use of the advantages of both approaches, this paper implemented both approaches by hybridizing the block and keypoint-based approaches.

III. Related Works

The first DCT technique was proposed by Fridrich *et al*. [21], in which he used the technique for overlapping blocks. When comparing this technique with other block-based techniques, it was discovered that it has a better performance. Huang *et al*. [22] proposed a technique using a robust detection algorithm, which was based on the DCT technique. The authors tried to enhance the challenges facing square block approach, by using a circular block technique instead of the conventional square blocking technique. This technique was able to detect multiple CMF in an image and has a robust feature to noise and blurring addition as well as having a low computational complexity. However, it was only tested with the post-processing operation. It also has a large blurring radius. Cao *et al*. [23] enhanced the DCT coefficient, by truncation of the higher frequency of coefficient thereby leading to a reduction of feature dimension and this technique is also robust to blurring, jpeg compression, and AWGN distortion. But like the other previous work, it was only tested with post-processing operation and it has a reduced detection rate when used to detect blur section. In the paper by Zhao and Guo [24], they made use of SVD (Singular Value Decomposition), which was applied to the DCT block process. It is able to detect multiple CMF in an image and also it was robust in term of noise and blurring addition. However, this technique was only tested in the post-processing operation. Kumar *et al*. [25] proposed a technique that tries to modify the matching process, so as to improve the computation time. This technique was effective as it has a highly robust against Gaussian noise, jpeg compress and a little amount of scaling and rotation. But, it was not capable of effectively detecting forgery when the image has been rotated or scaled. Fracastoro *et al*. [26] also made use of the DCT technique by designing an image encoder (SDCT) to enhance the performance of the DCT, which uses binary decision tree in achieving its results. It is able to detect multiple CMF in an image and is also has an enhanced detection rate for noise and blurring addition but, it is not capable of effectively detecting forgery when the image size was very large and the computational time was slow.

Bo *et al*. [27] proposed a technique using SURF technique in enhancing the robustness of the interest points and descriptors, which improves the detection rate. This technique was able to detect rotation, scaling, and noise. However, it was unable to effectively detect naturally similar features and has a high computational time. Hamid *et al*. [28] also made use of the SURF technique and were able to compare the performance of SURF and SIFT techniques, which the result showed SURF having a better performance. It was able to detect rotation, scaling, and noise. Also, it has a better accuracy time but, the research showed that SURF has a higher false positive rate. Raj and Joseph in their paper [29], segmented the copied area into patches and an evaluation was carried on this patches based on their matching. This increased the detection of CMF and also reduced the issues related to partial matching and it was able to detect CMF that where rotated or scaled. However, it was unable to effectively detect naturally similar features, as that is one of the major issues with SURF techniques.

Several research has shown that hybridization of CMFD techniques tend to perform better compare to when those techniques are used alone. For instance, the combination of DCT and DWT by Katharotiya *et al*. [30] shows that forged region are detected more accurately when compared to using each of the techniques alone, though this technique wasn't able to detect CMF that were either rotated or scaled. Also, the combination of SURF and SIFT technique produced a better and more accurate performance in the CMFD compared to when used individually, however, this technique was limited to also the problems associated to keypoint-based approaches [31]. When combining a block-based and keypoint-based approach, there is a higher and better accuracy in detection, as both problems associated with those approaches will reduce the false positive in detection. A typical technique that combines both approaches using SIFT and DWT is a technique proposed by Hashmi et al. [32].

IV. Methodology

In this paper, the CMFD has been studied and implemented by hybridization of two commonly used CMFD, which are DCT and SURF techniques. The goal of the hybridizing both techniques is to enhance the detection accuracy of CMF from the issues of scaling, rotation, similar naturally region and time complexity for both better detection performance. To enhance the detection performance an algorithm is designed with the above technique and the algorithm is evaluated using performance metrics of precision, recall, FPR (False Positive Rate) and accuracy. The results obtained from the above method is been compared with other related work results obtained.

The Fig. 5 shows the flowchart of the algorithm that is been implemented and the detailed explanation is broken down into twelve steps. The name given to this algorithm is HDS (Hybridized Detection System), which hydrides the DCT and SURF techniques.

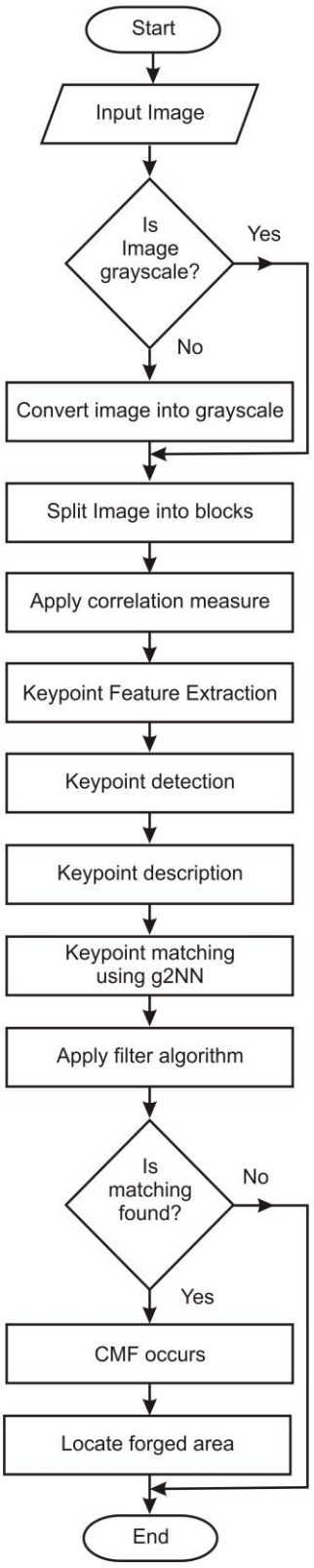

Fig.5. Flowchart for HDS algorithm

Step 1: Input image

This step is basically where the suspected image is been inputted into the model with the goal of detecting if the image is a forgery or not.

Step 2: Check if image is grayscale

This stage is responsible for checking if the inputted image is a grayscale image, if the image is already in a grayscale there will be no need to covert the image to a grayscale and if it is in RGB, the image will be sent for conversion to grayscale.

Step 3: Convert image to grayscale

The RGB image is converted based on equation 2.1 stated earlier. The goal of this conversion is to increase the detection performance of the image.

Step 4: Split image into blocks

Divide the M×N image to be tested into overlapping blocks. The image is scanned from the upper left corner to the lower right corner, sliding a block over the image. This results in blocks.

Step 5: Apply Correlation measure

For each block, apply the Radon transform in various directions, which are specified by a set of angles. This measure is applied to the image with the aim of making it robust against the various post-processing operations (compression, blur addition, and noise addition) on the copied region.

Step 6: Apply Keypoint feature extraction

The keypoint feature extraction is applied on the resulting image, for the purpose of extracting the keypoints from the image. This helps in the keypoint detection, the point descriptor, and the feature description matching.

Step 7: Keypoint detection

This step involves finding the points that are stable for geometric transformation and illumination transformation as keypoints. This defines some particular intensity around that region, such as the corner. This keypoint is used for deriving the descriptor.

Step 8: Generation of keypoint description

These keypoint descriptions, build descriptor (feature vector) for each keypoint based on the relationship between the surrounding pixels. This descriptor is used to classify the keypoint and the combination of both the keypoint and descriptor defines the feature.

Step 9: Use g2NN for keypoint matching

The keypoint features obtained are been compared with each other with the assistance of corresponding descriptors. For this keypoint matching, a g2NN (generalized 2 nearest neighbor) is used. This matching technique is used in the detection of multiple CMF in one image due to the repetition processing.

Step 10: Apply filtering algorithm

The filtering algorithm is been used for the reduction of the false positive, which will arise during the matching process. For example, removing of matches between spatially close areas. There are similar intensities between

neighboring pixels that might lead to false positive, which is the reasons for using the filter algorithm. This filtering algorithm involves the combination of HAC (hierarchical agglomerative clustering) and RANSAC (Random Sample Consensus algorithm).

Step 11: Check if matching is found

This step checks the image if it is forged or not. It simply considers an image been CMF if there are two or more clusters that have at least three pairs of matched points link one cluster to one another.

Step 12: Located forged region

Lastly, the CFM region is been located and marked.

To evaluate the performance of the hybridized algorithm, the Precision, Recall, FPR and accuracy performance metrics are been used. The HDS algorithm is implemented using MATLAB tool, the tool is used for the computation and visualization and it is tested on a standard MICC-F220 dataset.

V. Results and Discussion

The following results were obtained after implementation of the HDS algorithm and are thus shown below. Firstly the implemented technique is tested on the standard MICC-F220 dataset, along with some other images containing rotation, scaling and a combination of both.

The Fig. 6 shows results of some of the forged images from the MICC-F220 dataset. The first row represents the original image, row two represents the forged image (that has the rotation, scaling and combination of both attacks) and the last row represents the detection results using the HDS algorithm. The results indicate that the hybrid implemented is able to detect the various types of forgery effectively.

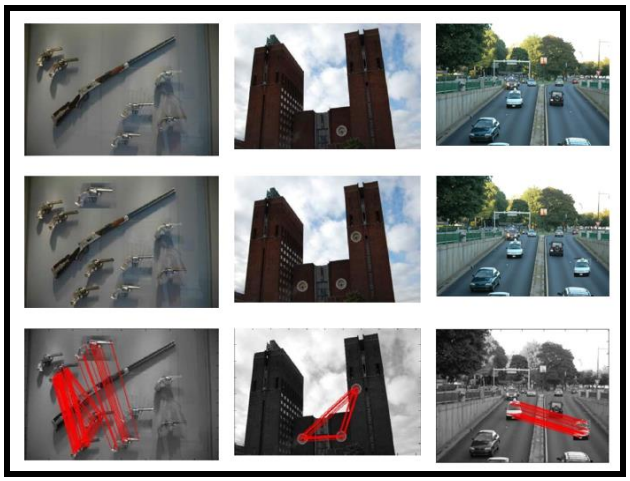

Fig.6. Results of HDS algorithm on some of the forged images

To have an effective detection rate, the threshold value t_v is adjusted and the result computed in Table 2. It can be seen from the results in Table 2, that as the threshold value begins to increase from a value of 0.3 to 0.5, the FPR also increases and the TPR (true positive rate) increases as well. As the value continues to increase to a value of 0.5 to 0.8, the FPR begins to decrease and the TRP begins to decrease. This indicates that the threshold value 0.5 has the best performance results and this value (0.5) is been adopted for the research.

Table 2. Training phase results to determine the threshold value t_v

t_v	TPR (%)	FPR (%)
0.3	89.09	4.55
0.4	90.91	5.45
0.5	97.27	6.36
0.6	96.36	6.36
0.7	92.73	5.23
0.8	88.18	4.32

The Table 3 shows the result obtained when the implementation was carried out using the hybridized technique. From the results, it shows that the total number of TP (True Positive) is 107, while that of the TN (True Negative) is 103 and the FP (False Positive) and FN (False Negative) are 7 and 3 respectively.

Table 3. Results obtained from the HDS Algorithm

Number of original image	Number of tampered image	TP	TN	FP	FN
110	110	107	103	7	3

For the performance of the hybrid technique, the results obtained in Table 3 are used in evaluating the HDS technique using performance metrics stated earlier and the result computed and tabulated in Table 4.

Table 4. Results from the Evaluation of the hybridized Technique

Precision	Recall	FPR	Accuracy
0.938596	0.972727	0.063636	0.954545
93.86%	97.27%	6.36%	95.45%

The precision metrics show that it was able to correctly detect 93.64% of the image that was not forged. In regards the recall metrics, it shows that it was able to correctly detect 97.28% of the forged image in the dataset used. Also, the FPR shows that it detected 6.36% as wrongly forged and also shows that 2.73% of the image that had forgery were not detected as a forged image. It can be seen that the accuracy rate of the hybridized technique is high, which implies that this technique can comfortably detect the various type of CMF attacks that might be applied to the image. The precision is also high as well, which is also an indication that the technique can positively predict the value of CMFD. The detection of the forged image is also high as shown in the recall value. The ratio of CMFD fallout is low as indicated in the FPR column.

The performance of the hybridized technique is done using a comparative analysis of the results gotten from similar implementation. The Table 5 and Fig. 7 shows

HDS technique been compared to DCT and SURF techniques. It can be seen that the hybridized technique performed better when compared with the DCT and SURF separately.

Table 5. Comparative analysis of our technique with existing DCT and SURF

Technique used	Precision (%)	Recall (%)	FPR (%)	Accuracy (%)
DCT [25]	82.00	76.00	24.00	80.00
SURF [29]	89.32	83.64	10.00	86.82
HDS	93.86	97.27	6.36	95.45

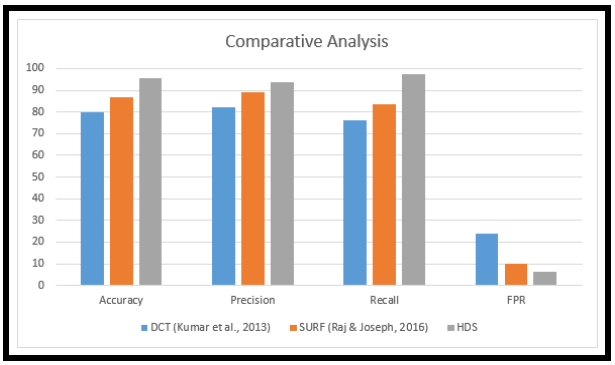

Fig.7. Comparative analysis of our technique with existing DCT and SURF

In the aspect of precision rate, it can be seen that the hybridized technique has the highest precision rate. This simply means it was able to correctly detect more images that were not forged when compared to the remaining two techniques (DCT and SURF). Also, the hybridized technique has the highest recall rate when compared to the rest of the two technique, which implies that it was able to detect more images that were classified as being forged. In terms of FPR, the hybridized technique had the lowest FPR rate, which indicates that it detected fewer images as wrongly forged images. Lastly, in terms of accuracy, the hybridized technique has a higher value than the other two techniques, which also implies that the hybridized technique was able to properly detect when an image is either forged or not forged. This shows that it has a higher correct classification rate when compared with the remaining two techniques.

The Table 6 and Fig. 8 compares the HDS technique with other existing hybridized techniques that have been used, which shows the technique performing better.

Table 6. Comparative analysis of our technique with existing hybridized technique

Technique used	Precision (%)	Recall (%)	FPR (%)	Accuracy (%)
DyWT + SIFT [33]	88.89	80.00	10.00	85.00
PCA +SIFT [34]	93.04	97.27	7.27	95.00
DWT+SURF [35]	77.17	64.55	19.27	72.60
DyWT+SURF [36]	77.06	76.36	22.94	76.71
HDS	93.86	97.27	6.36	95.45

The HDS algorithm can be seen in Table 6 to have a higher precision rate when compared to the four other hybridized algorithms. This implies that it is capable of detecting more images that are classified as not forged. While the recall and accuracy values are also higher when compared to the four other hybridized algorithms and the HDS algorithm maintains the lowest FPR as well. This comparative indicates the HDS algorithm has a higher detection accuracy when compared to the remaining four hybridized algorithms.

Looking closely at Figure 8, it can be shown that in terms of the four evaluation performance metrics used (accuracy, precision, recall, and FPR) in this paper. The HDS algorithm has higher detection accuracy in the detection of copy-move forgery.

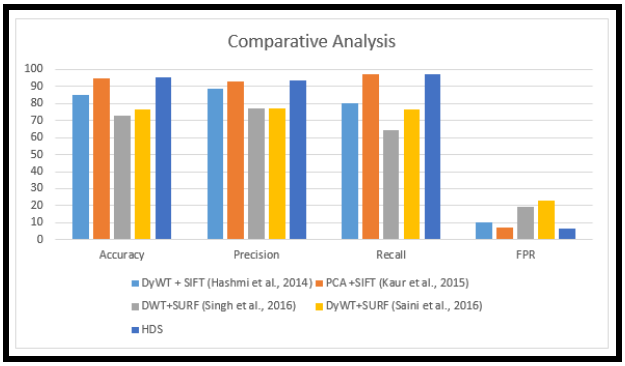

Fig.8. Comparative analysis of our technique with existing hybridized technique

VI. Conclusion

In conclusion, for a successful detection of CMF, the system must be able to detect forgery of all types of attacks associated with it (such as scaling, rotation, and blurring attacks). This paper has thoroughly assessed the various categories of forgery and developed an algorithm with the sole purpose of enhancing the performance and robustness in the detection of the common copy-move forgery. The paper developed an HDS technique that hybridizes DCT and SURF techniques. The efficiency of the hybridized technique has been shown that its detection rate and accuracy is far higher than the previously available methods. The goal of hybridizing both techniques is to be able to compensate the lapses found in each of the techniques. The hybridize technique has a better accuracy rate and it is robust to most of the attacks and preprocessing techniques that are associated with CMF

This paper was able to address some of those issues associated with CMF, however, there will be a need for improvement in the detection of other forms of image formats in jpeg format. This technique was basically designed for detection and doesn't proffer solution for prevention approach, which could serve as an area of future work. This work can also be extended to detect CMF in a video as well. This paper provided a hybridized algorithm for the detection copy move image forgery. It

also enhanced the previous accuracy and detection rate by hybridizing two common methods of detection, which are DCT and SURF.

REFERENCES

[1] M. Acedo. (2016, on 29th January, 2017). *5 Smart Ways To Use Digital Images In The Classroom*. Available: http://www.teachthought.com/the-future-of-learning/technology/5-smart-ways-use-digital-images-classroom/

[2] M. Sridevi, C. Mala, and S. Sanyam, "Comparative Study of Image Forgery and Copy-Move Techniques," in *Advances in Computer Science, Engineering & Applications: Proceedings of the Second International Conference on Computer Science, Engineering and Applications (ICCSEA 2012), New Delhi, India*. vol. 1, D. C. Wyld, J. Zizka, and D. Nagamalai, Eds., ed New York: Springer Science & Business Media, 2012, pp. 715-723.

[3] S. Sahu,S. Kumar Nanda, and T. Mohapatra, " Digital Image Texture Classification and Detection Using Radon Transform," *International Journal of Image, Graphics and Signal Processing(IJIGSP)*, vol. 5, pp. 38-48, 2013

[4] E. Burns. (2016, on 27th January, 2017). *Photo Editing Apps You Can Get for Free*. Available: http://www.digitaltrends.com/computing/best-free-photo-editing-software/

[5] S. K. Mankar and A. A. Gurjar, "Image Forgery Types and Their Detection: A Review," *International Journal of Advanced Research in Computer Science and Software Engineering* vol. 5, pp. 174-178, 2015.

[6] Full Sail. (2017, on 29th January, 2017). *Enhance Perfection With a Photo Retouching Career* Available: http://www.theartcareerproject.com/photo-retouching/657/

[7] T. H. Park, J. G. Han, Y. H. Moon, and I. K. Eom, "Image Splicing Detection Based on Inter-Scale 2D Joint Characteristic Function Moments in Wavelet Domain," *EURASIP Journal on Image and Video Processing*, vol. 2016, pp. 30-39, 2016.

[8] J. Brown. (2016, on 29th January, 2017). *Pentagon Is Developing Tech That Detects Fake Photos*. Available: http://www.vocativ.com/356956/pentagon-doctored-photos/

[9] B. George. (2016, on 29th January, 2017). *12 Historic Photographs that were actually Doctored (14 HQ Photos)*. Available: http://thechive.com/2012/02/07/12-historic-photographs-that-were-actually-doctored-14-hq-photos/

[10] A. Dixit, and R. K. Gupta, " Copy-Move Image Forgery Detection a Review," *International Journal of Image, Graphics and Signal Processing(IJIGSP)*, vol. 8, pp. 29-40, 2016.

[11] H. Kaur and K. Kaur, "A Brief Survey of Different Techniques for Detecting Copy-Move Forgery," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, pp. 875-882, 2015.

[12] M. Al-Hammadi, "Copy Move Forgery Detection In Digital Images Based On Multiresolution Techniques," MSc, Computer Engineering, Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh., 2013.

[13] G. K. Saini, and M. Mahajan,, " Improvement in Copy - Move Forgery Detection Using Hybrid Approach," *International Journal of Modern Education and Computer Science(IJMECS)*, vol. 8, pp. 56-63, 2016.

[14] S. Kumar, J. V. Desai, and S. Mukherjee, " Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors," *International Journal of Image, Graphics and Signal Processing(IJIGSP)*, vol. 7, pp. 38-44, 2015.

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

[16] N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, R. Ramli, R. Salleh, S. Shamshirband, *et al.*, "Copy-Move Forgery Detection: Survey, Challenges and Future Directions," *Journal of Network and Computer Application*, vol. 75, pp. 259-278, 2016.

[17] A. Gupta, N. Tiwari, M. Chawla, and M. Shandilya, "An Image Encryption using Block based Transformation and Bit Rotation Technique," *International Journal of Computer Applications*, vol. 98, 2014.

[18] J. Zheng, Y. Liu, J. Ren, T. Zhu, Y. Yan, and H. Yang, "Fusion of block and keypoints based approaches for effective copy-move image forgery detection," *Multidimensional Systems and Signal Processing*, vol. 27, pp. 989-1005, 2016.

[19] R. Krishnamoorthy and G. Devasena, "A Block-Based Feature Extraction Approach for Texture Classification with Orthogonal Polynomials," in *5th National Conference on Computational Methods, Communication Techniques & Informatics (NCCCI 2017)* New Delhi, India, 2017, pp. 16-20.

[20] V. Anand, M. F. Hashmi, and A. G. Keskar, "A Copy Move Forgery Detection to Overcome Sustained Attacks Using Dyadic Wavelet Transform and SIFT Methods," in *Intelligent Information and Database Systems: 6th Asian Conference, Aciids 2014, Bangkok, Thailand*. vol. 8397, N. T. Nguyen, B. Attachoo, B. Trawiński, and K. Somboonviwat, Eds., ed Switzerland Springer International Publishing, 2014, pp. 530-542.

[21] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in *Digital Forensic Research Workshop*, Cleveland, Ohio, USA, 2003.

[22] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," *Forensic science international*, vol. 206, pp. 178-184, 2011.

[23] Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm for copy-move forgery in digital images," *Forensic science international*, vol. 214, pp. 33-43, 2012.

[24] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," *Forensic science international*, vol. 233, pp. 158-166, 2013.

[25] S. Kumar, J. Desai, and S. Mukherjee, "A fast DCT based method for copy move forgery detection," in *2013 IEEE Second International Conference on Image Information Processing (ICIIP)*, Shimla, India, 2013, pp. 649-654.

[26] G. Fracastoro, S. M. Fosson, and E. Magli, "Steerable Discrete Cosine Transform," *IEEE Transactions on Image Processing*, vol. 26, pp. 303-314, 2017.

[27] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in *International Conference on Multimedia information networking and security (MINES)*, Nanjing, China, 2010, pp. 889-892.

[28] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "A Comparison between using SIFT and SURF for characteristic region based image steganography," *International Journal of Computer Science Issues*, vol. 9, pp. 110-116, 2012.

[29] R. Raj and N. Joseph, "Keypoint Extraction Using SURF Algorithm for CMFD," *Procedia Computer Science*, vol. 93, pp. 375-381, 2016.
[30] A. Katharotiya, S. Patel, and M. Goyani, "Comparative analysis between DCT & DWT techniques of image compression," *Journal of Information Engineering and Applications*, vol. 1, pp. 9-17, 2011.
[31] R. C. Pandey, S. K. Singh, K. Shukla, and R. Agrawal, "Fast and robust passive copy-move forgery detection using SURF and SIFT image features," in *2014 9th International Conference on Industrial and Information Systems (ICIIS)*, Gwalior, India, 2014, pp. 1-6.
[32] M. F. Hashmi, A. R. Hambarde, and A. G. Keskar, "Copy move forgery detection using DWT and SIFT features," in *2013 13th International Conference on Intelligent Systems Design and Applications (ISDA)*, Malaysia, 2013, pp. 188-193.
[33] M. F. Hashmi, V. Anand, and A. G. Keskar, "Copy-move image forgery detection using an efficient and robust method combining un-decimated wavelet transform and scale invariant feature transform," *Aasri Procedia*, vol. 9, pp. 84-91, 2014.
[34] H. Kaur, J. Saxena, and S. Singh, "Simulative Comparison of Copy-Move Forgery Detection Methods for Digital Images," *International Journal of Electronics, Electrical and Computational System*, vol. 4, pp. 62-66, 2015.
[35] M. Singh and E. H. Singh, "Detection of Cloning Forgery Images using SURF + DWT and PCA," *International Journal of Latest Engineering Research and Applications (IJLERA)*, vol. 1, pp. 1-10, 2016.
[36] G. K. Saini, M. Mahajan, and P. Mohali, "Study of Copy Move Image Forgery Detection Based On Surf Algorithm," *International Journal of Modern Electronics and Communication Engineering (IJMECE)* vol. 4, pp. 46-49, 2016.

Authors' Profiles

Joseph A. Ojeniyi, is a lecturer in the Department of Cyber Security Science, School of Information and Communication Technology, Federal University of Technology (FUT) Minna, Nigeria. He received his PhD in Cyber Security Science from the same University, M.Sc. in Computer Science from University of Ibadan, Nigeria and a B.Tech. in Mathematics/Computer Science from FUT Minna, Nigeria. He has been appointed as a reviewer to several indexed Journals. He currently serves the chairman of the Conference Organizing Committee of the faculty, 'ICTA 2018'. His area of interest is in Digital Forensics, Deep Learning and Cyber Physical Systems.

Bolaji O. Adedayo, he is pursuing the master of technology from the Federal University of Technology, Minna, Niger State, Nigeria. He received his Bachelor of Engineering in Electrical/Computer Engineering from FUT Minna, Niger State, Nigeria in 2007. His area of interest is digital image forensic.

Idris Ismaila, is a Senior Lecturer at the Department of Cyber Security Science, Federal University of Technology, Minna, Niger State, Nigeria. He has a Bachelor of Technology from FUT Minna, Niger State, a Master of Science from University of Ilorin, Kwara State and a Doctor of Philosophy form Universiti Teknologi, Malaysia. His area of interest is in Digital Forensic.

Abdulhamid M. Shafi'I, he received his PhD in Computer Science from UTM Malaysia, M.Sc. in Computer Science from BUK Kano, Nigeria and a B.Tech. in Mathematics/Computer Science from FUT Minna, Nigeria. He has been appointed as an Editorial board member for UPI JCSIT, JITE:Research and IJTRD. He has also been appointed as a reviewer to several ISI and Scopus indexed Journals. Presently he is a Senior Lecturer in the Department of Cyber Security Science, FUT Minna, Nigeria.

How to cite this paper: Joseph A. Ojeniyi, Bolaji O. Adedayo, Idris Ismaila, Abdulhamid M. Shafi'i," Hybridized Technique for Copy-Move Forgery Detection Using Discrete Cosine Transform and Speeded-Up Robust Feature Techniques", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.10, No.4, pp. 22-30, 2018.DOI: 10.5815/ijigsp.2018.04.03

