Parametric Comparison Between GLCM-BRISK and CHT Copy Move Forgery Detection Techniques

Dr.Amarpreet Singh
Amritsar Group of Colleges, Amritsar, India

Sanjogdeep Singh
Amritsar Group of Colleges, Amritsar, India

***Abstract*: Digital Image forgery has seen an upsurge in the recent times due to advancement in technology, especially in the imaging field. Numerous techniques have been researched upon to counter the issue of image forgery. In the last few decades, techniques such as SURF, SIFT, DCT and many other had been introduced. Apart from these, Circular Harmonic transform(CHT) and Gray Level Co-occurrence Matrix Binary Robust Invariant Scalable Keypoints (GLCM-BRISK) are two prominent methods used for forgery detection purposes. Both of them have different working methodologies with varying accuracy and time of execution.GLCM-BRISK is a latest and novel technique that has been discussed in this paper. Apart from this, paper also makes parametric comparison between GLCM- BRISK and CHT in terms of precision, recall and F-measure.**

KEYWORDS: Copy-move forgery, DWT, GLCM, General architecture, Image Manipulation

I. INTRODUCTION

These days, the use of image processing technology has become quite common. With time, numerous approaches have been designed for the extraction of extremely complicated data from the images. Research, healthcare, pattern recognition, military, etc. are some of the application felids that are using this technology in extensive manner [1]. In copy-move forgery, a certain area of a picture is cut or copied to hide the non-essential parts of an image, and then this part is pasted on some other part. At present, CMF is a leading image tampering method. The advantages and disadvantages of this method depend on the purpose for which it is being used [2]. This method hides the original image information and generates the forged images. The implementation of textured areas is carried out as similar color and noise variation features for generating forged image. It is not possible to detect such extreme changes in the statistical properties of an image manually. In order to reduce different types of anomalies amid the real and pasted areas, blurriness is applied on the edges of the altered image [3]. CMF can be performed easily and makes a major contribution to manipulate an image, especially when both source and target areas belong to the similar picture and have similar features [4]. Hence, it is not possible to detect image tempering with naked eye. The general operated regions in the picture turn out to be grass, foliage or fabric in this type of forgery. These regions can be mixed with the background easily as these regions have similar features such as texture and color [5].Every copy-move forgery correlates the real image part and the pasted part. The segments may not match perfectly but just to some extent as the forgery is generally saved in the lossy JPEG format. Therefore, one of the requirements that a copy-move forgery detection algorithm must have satisfied is that this algorithm should be time efficient by creating few false positives (i.e., detecting inappropriate matching parts) [6].In general, an image represents the real-time event. These days, an image can be tampered easily using the available digital processing tools.Hence, different techniques are developed for validating the genuineness of the acquired image. The image forensics aims to detect the image forgery. Here are the different research gaps:

1. Over the time, different approaches have been developed for the detection of the copy-move forgery. However, most of the template-based approaches leads to increase in the execution time to a large extent. The use of PCA and GLCM-BRISK algorithm for copy move forgery detection discussed in this work will overcome it.
2. The extreme complexity of morphological operation also reduces the detection accurateness. This gap is also fulfilled by the novel method of GLCM-BRISK.

II. LITERATURE REVIEW

Haipeng Chen, et.al (2020) suggested a well-organized cluster based CMFD technique in which SIFT key points and the similar neighborhoods were searched to place the tampered regions [7]. They were matched and grouped into several smaller clusters. The high dimensionality of SIFT caused high time complexity, so this technique helped to reduce that complexity. A new localization algorithm was designed which had used two similarity measures to compare the parallel neighborhoods and to find the manipulated parts of matching pairs.

Kunj Bihari Meena, et.al (2020) recommended a novel Tetrolet transform based approach to detect forged areas in an image [8]. The input picture was separated into overlapped blocks. Tetrolet transform was employed to extract the 4 low and12 high-pass coefficients. The extracted Tetrolet features were matched to recognize the similar blocks. The results acquired after the experiment were demonstrated that the recommended technique was appropriate for detectingthe forged parts in a precise wayeven in post-processing tasks.

Jun-Liu Zhong, et.al (2020) recommended a highly proficient two-pass hashing feature representation for CMFD technique[9]. Firstly, the extraction of corresponding blocks from multiple frequency images was done by presenting the normalized moment transformation. The multiple hashing attribute was concatenated with the presented approach. The two-pass hashing searching algorithm was used efficiently to search and update the adjacent pixel matching. Then the post-processing operations recognized the forgery regions correctly.

Gul Muzaffer, et.al (2019) suggested the architecture based on DL for detecting and localizing the forgeries in copy-move despite conventional schemes of extracting features [10]. The attributes of image sub-blocks were acquired using aPre-trained AlexNet CNN in this approach. Thereafter, these sub-blocks were matched. At last, false match elimination was carried out.

Nidhi Anna Kurein, et.al (2019) investigated the issues and proposed two major approaches i.e block and keypoints based were used to detect the forgery in copy-move [11]. The Block-based made partition of overlapped image matrix into blocks and also for the extraction of attributes. The key point feature of every image was extracted for the matching. Two algorithms DCT and SIFT for detecting the forgery in copy-move were implemented in the presented approach.

Chengyou Wang, et.al (2019) intended an image CMFD technique to detect the forged images [12]. Two attributes recognized as SURF and PCET were implemented. Image was split into non-overlapped blocks in smooth and texture region.The coefficients of PCET were extracted, when SURF found the key points. False matched points were eliminated dense matched points were found. The RANSAC was combined with a filtering scheme. At last, mathematical morphology and an iterative strategy was used.

Y. Liu (2022) projected a new model which had two phases for detecting the CMF (copy-move forgery) [13]. Initially, the atrous (dilated) convolution was put together with skip matching for augmenting the spatial information and leveraging the hierarchical attributes. Subsequently, Proposal SuperGlue was suggested for eliminating the FA (false-alarmed) regions and remedy imperfect regions. A mechanism was built for enclosing the suspicious areas on the basis of proposal generation and backbone score maps. Eventually, the DL (deep learning) based technique of extracting key-point SuperPoint and matching SuperGlue was exploited to match carry out matching. The experimental outcomes validated that the projected model was effective to detect the forgery in CM (copy-move).

K. M. Hosny (2022) presented a CNN (convolutional neural network) model in order to detect forgery in CM (copy-move) image [14]. This model became lightweight due to the appropriate number of convolution and max-pooling layers. A testing was done quickly and precisely at 0.83 seconds. The presented model was quantified on the benchmark datasets in the experimentation in which accuracy and time was considered as metrics. The experimental results depicted that the accuracy of the presented model was calculated 100%.

A. Murugan (2022) intended an effectual technique to detect forgery in copy-move and locate the tampered regions [15]. For this, the SIFT key-points were clustered and relative neighbourhoods were considered. This technique was implemented to aggregate and match the key-points into several small clusters concerning scale and color. Consequently, the temporal complexity launched with SIFT (scale-invariant feature transform) was lessened. A unique

localization technique method was put forward for analyzing the comparable neighbours of matched pairs in accordance with 2 similarity indices. Afterward, pixel-level tampered areas were discovered by assigning the labels to the tampered regions into pixels. Image processing assisted in manipulating the digital images. In the experimental outcomes, the intended technique was proved applicable to localize the forgery and reliable to detect the forgery in comparison with other methods.

GLCM-BRISK

GLCM is a short for Gray Level Co-occurrence Matrix.It works on the concept of occurring frequency of gray levels of the image in a unit area. This function measures the value of occurrence with entropy, energy, dissimilarity among many other features in a certain spatial association.GLCMalgorithm has been used a number of times before, however the method has not been used along with the BRISK. Due to the usage of a matrix-based function, the algorithm is able to cover almost all the pixels to calculate the intensity in much shorter span of time than (CHT) Circular Harmonic Transformation technique.

BRISK is known for its rotation and scaling invariance. For one or another reason, if GLCM is unable to read or extracts the features for invariance, BRISK will help to process such images. It is a feature point detection algorithm with lower computational cost as compared with CHT (circular harmonic transformation) technique. BRISK achieves the invariance implementing the measure orientation of the keypoint and rotating the pattern by that orientation. Such segregation helps in achieving maximum accuracy and execution speed.

III. Research Methodology

Following are the various steps which are applied for the copy-move forgery detection:

Input Digital Image:The first common step is of loading the manipulated image from the given dataset. In our case it is CoMoFoD dataset which contains around 1200 forged and processed jpg and other image format files. Th is work has used a no of images, however ne sample Image has been presented to avoid the computational complexity of the article. The initial image is in RGB format which is then transformed into grayscale for further operations of processing.

Pre-Processing:It is the preliminary step which converts the image into grayscale and further decomposed, transformed a per the need. The general procedure carried out in the step is to convert RGB pixels in grayscale within a spectrum of 0-255. Important features of the image such as brightness, entropy, color contrast is analyzed. It also assists in reduction of noise levels from the image.

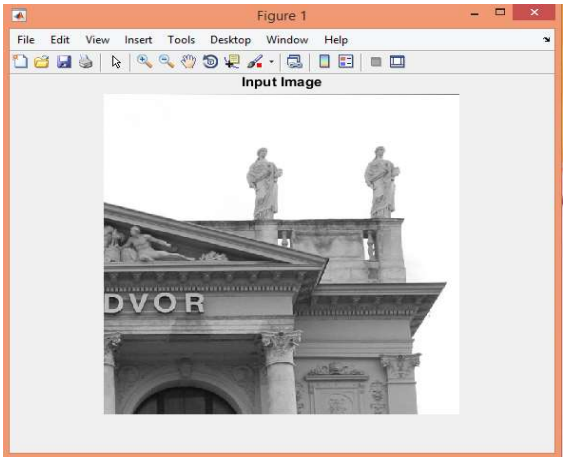

Fig 2: Input image (Manipulated Image)

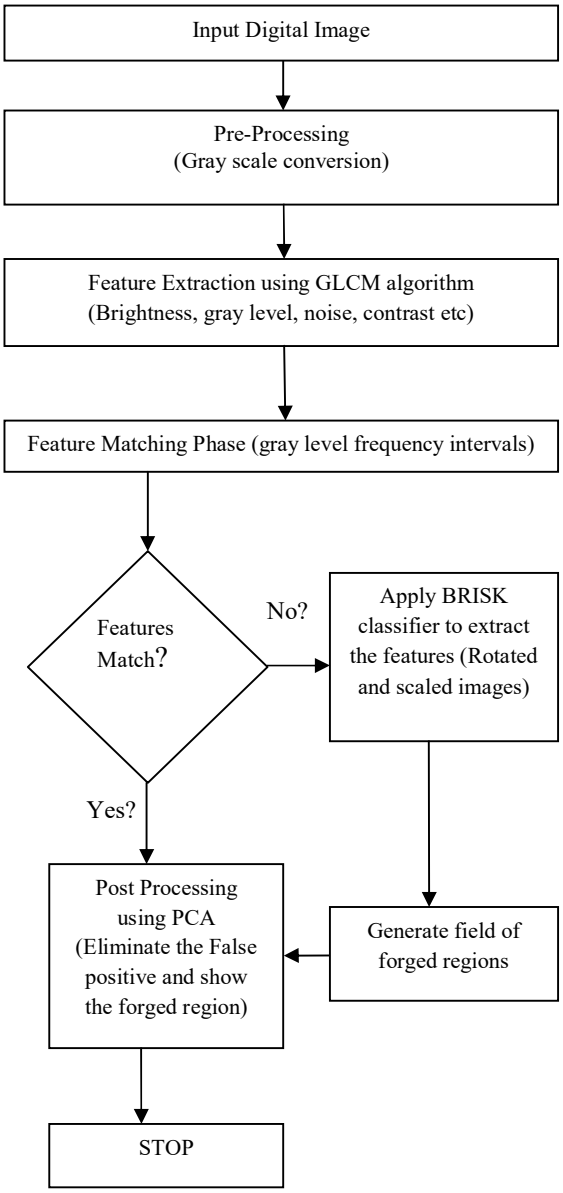

Fig1: Proposed Flowchart

***Feature extractionwith GLCM*:** The attributes such as energy, dissimilarity, correlationis extracted from the input image in the first stage by matching grayscale levels and heir occurring frequency. The highest matching keypoints will be matched. These features are used for detecting the forgery. The procedure in which abstractions of image information is acquired is known as feature detection. The grayco-matrix function is applied for developing a GLCM. This function computes the value of occurrence of pixel using the intensity value *i* in a specific spatial association to a pixel having the value *j*. The pixel of interest and the pixel to its immediate right are used to describe the spatial association by default. However, the spatial relationships can be identified within two pixels. In the resultant GLCM, every element (*i,j*) is the addition of the number of times that the pixel that has value *i* which is occurred in the specified spatial association with value *j* within the input image.The value 1 is comprised in the element (1,1) in the output GLCM as the input image has only one example in which the values 1 and 1 is assigned to two horizontally adjacent pixels. The value 2 is comprised in element (1,2) of GLCM as there two examples in which the values 1 and 2 is defined for two horizontally adjacent pixels.The value 0 is comprised in the element (1,3) in the GLCM since, the values 1 and 3 is assigned for two horizontally adjacent pixels as they have not any instance. The input image is

processed, the image for other pixel pairs (*i,j*) is scanned and the sums in the corresponding elements of the gray-level co-occurrence matrix are recorded with the help of grayco-matrix.

Afterwards, an effective technique known as Binary Robust Invariant Scalable Keypoints (BRISK) has been implemented for the detection of image manipulation using multiscale corner features in 2D grayscale input image. This technique is invariant to rotation and scaling issues. Low storage memory and faster response time are the two major advantages of this technique. The command line function for this technique is represented is:

Points =detectBRISKFeatures(I);

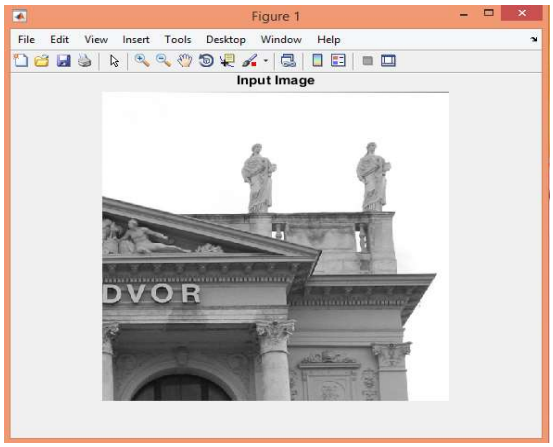

Fig 3: Grayscale image

Figure 3 shows the input image after processing. This is a grayscale image.

Apply PCA Algorithm:The valuable information from each image block is extracted using PCA algorithm. It is a multivariate method which is adopted for the analysis of data table. This data table characterizes various correlated variables based on their quantity. This algorithm aims to extract the valuable information from the table so that new orthogonal variables can be represented. These variables are referred as principal components.The approach displays instances based on the similarity of observations while the variables as points within maps. The data is placed mainly corresponding to every variable if a specified data matrix includes p variables and n samples. The data occurs in the middle after the generation of principal components which does not affect the spatial relations of data or the variances. The first principal component (Y_1) is given by the linear combination of variables X_1, X_2, ..., Xp. The first principal component can be represented as:

$$Y_1 = a_{11}X_1 + a_{12}X_2 + \cdots + a_{1p}X_p \qquad \ldots (1)$$

As matrix, it can be represented as:

$$Y_1 = a_1^T X \qquad \ldots (2)$$

The first principal component is measured to discover the highest possible variance. The variance of Y_1 can be generated by the selection of big values for weights, represented as $a_{11}, a_{12}, \ldots a_{1p}$,. The weights are measured with the limitation such that the sum of squares is 1, to avoid such condition.

$$a_{11}^2 + a_{12}^2 + \cdots + a_{1p}^2 = 1 \qquad \ldots (3)$$

The second principal component is measured in the similar manner to prevent the occurrence of correlation in the direction of the first principal component. The next maximum variance makes use of this second principal component.

$$Y_2 = a_{21}X_1 + a_{22}X_2 + \cdots + a_{2p}X_p \qquad \ldots (4)$$

This process continues till the measurement of p principal components. These components correspond to the original number of variables. Corresponding values are achieved for the sum of variances of all principal components and the sum of variances of all variables in this point. Hence, the changesin all real variables with respect to the principal components can be represented as:

$$Y = XA$$

Keypoint matching:The matching of keypoints is done with each other for the recognition of same points in the similar image. The identical regions are discovered in an image using the value of threshold which is chosenheuristically. But the blocks made with the help of GLCM output are known to be the most appropriate features of the image as the pixel doesn't have any kind of informatics value of the feature. Similarity matching is performed within the pixels, once the required pixels are obtained,the pixels of the dissimilar blocks be detected as the forgery pixels.

Suspected region identification:The only position of forgery areas is the matching attribute points. An approach based on block related to region localization has been implemented when every matching keypoint is replaced with unmatched keypoints. The keypoints will be compared with the other blocks to evaluate forgery pixels from the image. Further the morphological operation is applied to which mark the forgery part on the image.Figure 4 demonstrates an image with detected forged areas. In this image, the marking of mismatched image components is carried out with the black color.

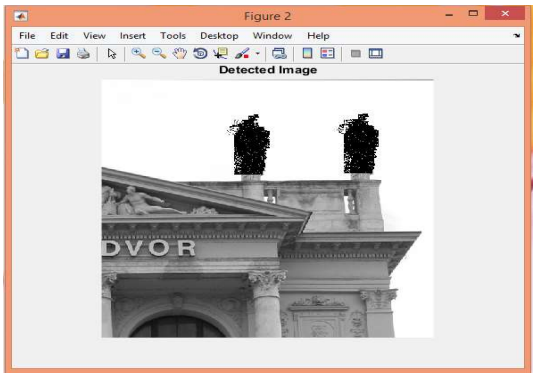

Fig 4: Output image with detected forged areas

Parametric Comparison

In this section, parametric comparison has been conducted between the two techniques of forgery detection i.e., GLCM-BRISK and CHT. The parameters taken into account are precision, recall rate and F-measure.The comparisons are made using CoMoFoD dataset for computation purpose. This dataset comprises of 1200 forged and processed images.The results are obtained implementing the research work in MATLAB R2015 a v8.5.0.197613. Following are the various parameters for the performance Analysis: -

a) **Precision**: In pattern recognition, information retrieval and binary classification, precision (also called positive predictive value) is the fraction of relevant instances among the retrieved instances.

$$Precision = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

Precision				
Level	**CHT**	**GLCM**	**Impact**	**% Change**
Image Level	0.92	0.98	0.06	6.52%
Pixel Level	0.92	0.98	0.06	6.52%

Table 1: Precision comparison between CHT and GLCM-BRISK

b) **Recall**: Recall is the fraction of relevant instances that have been retrieved over the total amount of relevant instances.

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative}$$

Recall				
Level	**CHT**	**GLCM**	**Impact**	**% Change**
Image Level	0.93	0.98	0.05	5.38%
Pixel Level	0.92	0.98	0.06	6.52%

Table 2: Recall comparison between CHT and GLCM-BRISK

c) **F-Measure:** It is calculated as the harmonic mean of precision and recall, giving each the same weighting. It allows a model to be evaluated taking both the precision and recall into account using a single score, which is helpful when describing the performance of the model and in comparing models

$$F - score = \frac{TP}{TP + 1/2(FN + FP)}$$

F-Measure				
Level	**CHT**	**GLCM**	**Impact**	**% Change**
Image Level	62.90	93.54	30.64	48.71%
Pixel Level	72.58	95.16	22.58	31.11%

Table 3:F-measure comparison between CHT and GLCM-BRISK

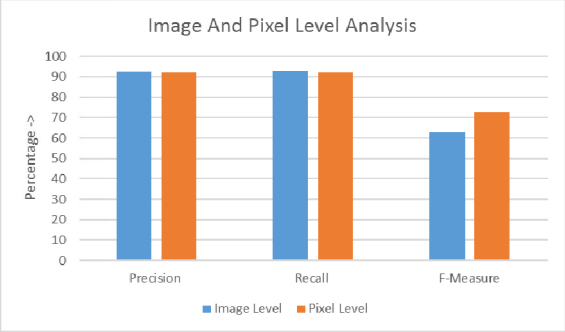

Fig 5: Image and Pixel Level Analysis of CHT

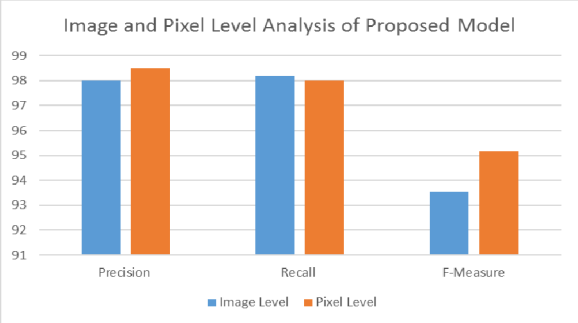

Fig 6: Image and Pixel Level Analysis of GLCM-BRISK method

VI. Result and Discussion

As it is clear from the results depicted in the above tabular data that the performance of GLCM-BRISK is better than its counterpart CHT. When it comes to precision, there is a percentage improvement of 6.52 both at image level and pixel level. The recall rate on image level shows improvement of 5.38% and pixel level revealed improvement of 6.52%. Drastic improvements have also been observed in F-measure with a percentage increase of 48.71 at image level and 31.11 percent at pixel level.

V. Conclusion

The copy-move forgery detection is the technique applied to detect forgery portion from the image. This research is based on the copy-move forgery detection using block based technique. In this work, the GLCM-BRISK algorithm is used for the textual feature analysis and mean value of the features will be given as input to the PCA algorithm for the feature reduction. The results obtained show significant improvements as compared to CHT technique in terms of precision, recall rate and F-score. The results shows comprehensive and significant improvement of GLCM-BRISK model over CHT in context to the detection of copy move forgery.

References

[1] X. Kang, and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics", 2008, in International Conference on Computer Science and Software Engineering, volume 3, issue 10, pp. 92630.

[2] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," 2008, in Pacific-Asia Workshop on Computational Intelligence and Industrial Application, volume 2, issue 15, pp. 2726.

[3] G. H. Li, Q. Wu, D. Tu, and S. J. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWTand SVD," 2007, in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, volume 23, issue 15, pp. 17503.

[4] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," 2011, in 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), volume 12, issue 4, pp. 14.

[5] I. Amerini et al., "A SIFT-based forensic method for copymove attack detection and transformation recovery", 2011, IEEE Trans. Inf. Foren. Sec., volume 6, issue 3, pp. 1099111

[6] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy move forgery in digital images," 2003, in Proceedings of the Digital Forensic Research Workshop, volume 17, issue 3, pp. 58.

[7] Haipeng Chen, Xiwen Yang, YingdaLyu, "Copy-Move Forgery Detection Based on Keypoint Clustering and Similar Neighborhood Search Algorithm", 2020, IEEE Access, vol. 8, issue 12, pp 45-50

[8] Kunj Bihari Meena, VipinTyagi, "A copy-move image forgery detection technique based on tetrolettransform", Journal of Information Security and Applications, volume 52, issue 34, June 2020, article 102481

[9] Jun-Liu Zhong, Chi-Man Pun, "Two-pass hashing feature representation and searching method for copy-move forgery detection", Information Sciences, volume 512, issue 15, February 2020, pages 675-692

[10] Gul Muzaffer, GuzinUlutas, "A new deep learning-based method to detection of copy-move forgery in digital images", 2019, Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT), volume 6, issue 23, pp. 50-65

[11] Nidhi Anna Kurien, S Danya, Diya Ninan, C Heera Raju, Jisa David, "Accurate And Efficient Copy-Move Forgery Detection", 2019, 9th International Conference on Advances in Computing and Communication (ICACC), volume 4, issue 14, pp 345-355

[12] Chengyou Wang, Zhi Zhang, Qianwen Li, Xiao Zhou, " An Image Copy-Move Forgery Detection Method Based on SURF and PCET", 2019, IEEE Access, volume 7, issue 12, pp. 170032 – 170047

[13] Y. Liu, C. Xia, X. Zhu and S. Xu, "Two-Stage Copy-Move Forgery Detection with Self Deep Matching and Proposal SuperGlue," in *IEEE Transactions on Image Processing, vol. 31, pp. 541-555,* 2022

[14] K. M. Hosny, A. M. Mortda, M. M. Fouda and N. A. Lashin, "An Efficient CNN Model to Detect Copy-Move Image Forgery," in *IEEE Access, vol. 10, pp. 48622-48632, 2022*

[15] A. Murugan, M. ArsathA, M. Anandarajand M. Naveenkumar, "Similar Neighbourhood Search and Key-Point Clustering in Forgery Detection," 2022 *International Conference on Applied Artificial Intelligence and Computing (ICAAIC), pp. 1375-1380, 2022*

Author Biography

Dr.Amarpreet Singh has completed his PhD. Currently he is working as a professor in Amritsar Group of Colleges Amritsar, Punjab, India. He has published number of research papers in various international/ national journals and conferences. His area of interest is Network Security and Digital Image Processing. He can be contacted at amarpreet.cse@acetedu.in

Sanjogdeep Singh has completed Bachelor of Technology in CSE degree from Punjab Technical University. Currently he is studying Master of Technology. His area of interest is Digital Image Processing. He can be contacted at er.sanjogdeep@gmail.com. The link to his ORCid is https://orcid.org/0000-0002-1478-9917