A Review on Deep-Learning Approach to Copy-Move Forgery Detection and Source-Target Disambiguation

Krishna Alkeshbhai Brahmbhatt[a]*, Jahnavi Patel[b]

[a]*P.G Scholar, Information Technology Department, L. D. College of Engineering, 380015, India*
[b]*Asst. Professor, Information Technology Department, L. D. College of Engineering, 380015, India*

Abstract

The purpose of the research is to review available copy-move forgery detection approaches and to find an optimal Copy-Move forgery detection algorithm with accurate Source-Target Disambiguation which might also work for n-n Source-Target disambiguation and detection. Hence various approaches are studied out of which the two stage approach with backbone architecture based on VGG16 and Proposal Glue gives best performance for forgery detection and Source-Target disambiguation is performed best by Multibranch CNN including 4-TwinsNet which constitute of four 50-ResNet and Siamese Net. Further a more robust strategy for multi-target detection with Source-Target disambiguation that works on all cases even with the addition of the manipulation attacks like rotation, image blurring, JPEG compression etc.

Keywords: copy-move; forgery; image manipulation; deep learning;, image processing.

1. Introduction

In this digital era, the use of social media and hence use of image manipulation and editing tools have taken over the internet and world. To come across a digitally manipulated and forged picture has become such a common occurrence that 'seeing is believing 'adage does not hold anymore. Moreover, with such wide availability of tools and methods in the market for image forgery that it is very easy to forge an image without any identification through naked eye that the image is manipulated or any trace of being tampered. These tempered images bring a bucket load of problems along with them. Images are often considered trustworthy sources for information and investigation even in the cases of crime Investigation and news media. Various other fields that are affected by forged images are real estate, politics, insurance claims, public hysteria etc.

A digital image can be forged with various manipulations and Copy-move forgery is one such manipulation technique in which a section of image is copied and pasted in the same image widely; it may also include a section of photo being removed from image. In recent years copy move forgery has been one of most studied techniques of image manipulation and the reason for that is It is the easiest photo manipulation technique to perform but it is also one of the toughest techniques to prove that it has been performed, which results in copy move forgery being the most used image manipulation techniques. The purpose of copy-move forgery is generally to hide a particular part of the image using another section of same image or to add extra information to the image in order to contort the original meaning of the image. Hence the detection of copy-move forged image is an important research area in recent years in order to check the authenticity of the content we see online or in magazines which has the power to create a false public opinion or even mass hysteria or May also fuel unnecessary false rumor mill.

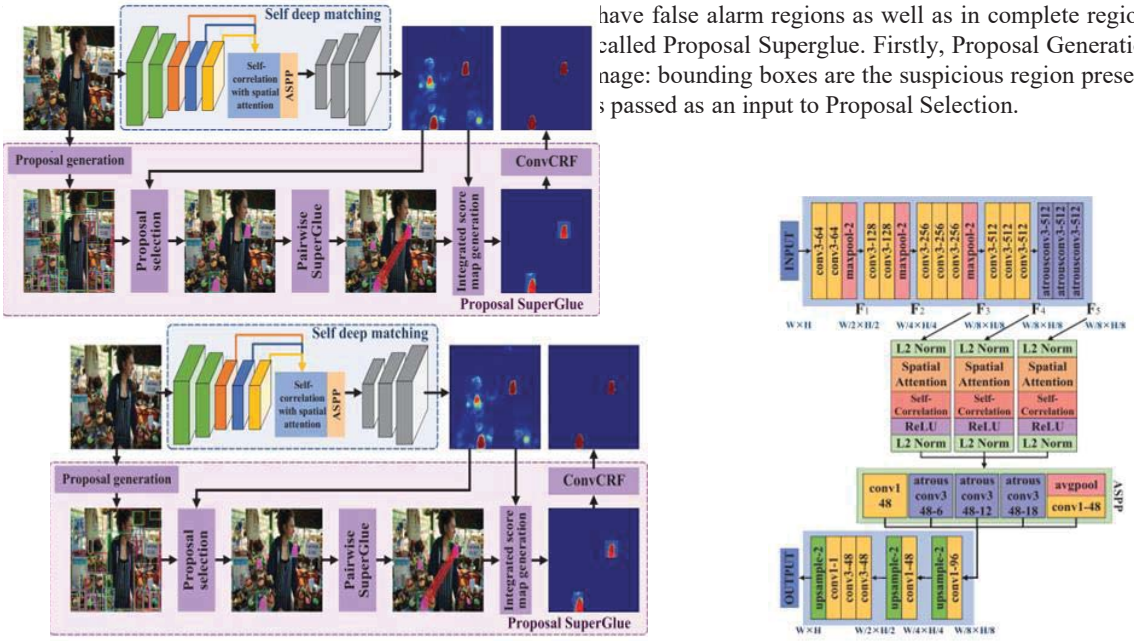
In the recent years many techniques have been researched for copy move forgery detection but a high accuracy detection approach with optimal source-target disambiguation is still a work in progress. Hence it has been of interest for researchers to dabble in. There are mainly two approaches to copy move forgery detection: keypoint based approach and block-based approach. In key point matching approach, the extracted keypoints are matched and in block-based approach the image is divided into blocks, and they are matched. In this paper some of the methods for copy move forgery detection are reviewed in order to find the most optimal approach.

2. Literature Review

In [2] paper a two-stage Framework for copy-move forgery is used which includes end to end deep matching and customized key point matching algorithms are used in the pipeline. The copy move forgery detection is performed in two stages; the first stage includes a backbone deep matching network which gives backbone score maps that show the forged regions. The backbone network architecture includes feature extractor for which VGG16 is used but the pooling layer is removed from 4th and 5th convolution block and the 5th block is changed to atrous convolution: it is preferable for the resolution of convolution features as

* Krishna Alkeshbhai Brahmbhatt
E-mail address: krishnabrahmbhatt1503@gmail.com

well as field of view. This generates three large feature maps that are passed to skip matching. The feature maps have low level features with spatial and texture information and high-level features with semantic information both used to find visual similarities. These feature maps are passed to a self-correlation module with spatial attention to generate correlation maps. This process of generating correlation maps from feature maps is known as skip matching. Spatial attention and correlation module try to find correlation between every two features. Correlation maps are passed to Atrous spatial pyramid pooling (ASPP), It contains three parallel atrous convolution layers with 6, 12 and 18 atrous rates average pooling and convolution layer with 1*1 filter. ASPP generates 5 48-channel feature maps which are concatenated and fed to up sampling and convolution layers. The generated



(a) (b)

Fig.1 (a) Proposed Methodology in the paper [2] (b) Architecture of Backbone Architecture [2]

Proposal selection takes output of proposal generation as well as the backbones Score map as input. Proposal selection rejects the proposals with less average scores, selects proposals with high IoU and merge proposals when intersection rates are high. Thresholds are fixed for this average threshold at 0.4, IoU threshold at 0.5 and intersection rates threshold at 0.8. Hence superglue provides high-quality proposals. High quality proposals are further passed to Super Point, It finds interest points and conducts key point matching. Points are matched through super glue using local features. Matching scores of the matching points pixel using a super pixel algorithm SEEDS. This pixel level score map and also integrated score map. The generated score maps are not refined, They have holes and false alarm regions, so in order to refine contour and remove regions with less probability using Convolution Conditional random field (CRF).

Further ablation study of backbone network is performed through step-by-step analysis till self-DM using a synthetic testing dataset with 120,000 images. Different state of the art methods are compared and also the given architecture in combination with 2 deeper networks; ResNet50 and ResNet101 and 3 light-weight networks: MobileNetV2, MobileNetV3, ShuffleNetV2 are tested out of these ResNet50 and MobileNetV3 give best performance. Hence, they were considered for further. They are compared using synthetic dataset. State of the art methods are compared using four data sets: Synthetic testing data set, CoMoFoD (with no attack), CASIA CMFD and MICC-F220.The F1 score for datasets is CASIA-0.7943(detected) and 0.5172(overall) CMFD-0.4782(pixel) and 0.7732(image-level) MICC-F220-0. 8559.The proposed method performs the best in almost all scenarios as shown in the figures.

In [3] methodology for source target disambiguation in copy move forgery detection is proposed. The given methodology works on the simplest scenario of single source single target copy move forgery. Moreover, it works best in the cases where the source and target regions are not overlapping each other and, in the cases, where a single region is returned instead of two different source target regions segmentation algorithms need to be used to distinguish between source and target. Generally, Copy-Move forgeries are performed through geometric transformation of source to target where a matrix represents relation between the two. Further interpolation processes are also performed in order to fit it into a 2D pixel grid resulting in non-invertible transformation. The copy-move forgery is often to followed with post processing such as landing of the borders of the target region in order to make it less obvious. Moreover, the post processing could also be applied globally so if it affects both the source and target. Facts that these post processing leaves are known as boundary artifacts. Proposed methodology exploits the non-invertible property due

to interpolation and the boundary artifacts at the target regions for source target disambiguation.

The algorithm takes the localization mask of the forged image as input. The process perform source target disambiguation using interpolation artifacts works on the hypothesis formed that if the Copy move forgery process through geometric transformation is performed in the forward direction from source to target it gives the similar results to the image we already have at hand but on the other hand if the process is performed in the backward direction that is if the target is moved to source then the resulting image would be significantly different than the image we have at hand as there is no interpolation on the source. Hence it would be easy to identify which way is the forward way and which is the backward resulting in easily identifying source and target. For the implementation purpose we have used by bilinear kernel for interpolation. Sometimes only the interpolation artifacts are not enough in order to recognize source and target from each other. In such cases the second branch that is the branch that works on identifying the boundary artifacts is useful, moreover there is also a chance that the interpolation is very weak or not present at all due to either intense post processing process or rigid translation. The boundary artifact analysis works on the hypothesis that the target region would always have boundary artifacts in order to hide it or to make it less obvious, but source region would have no such arteffects hence the presence of this artifact is used in order for this ambiguation between source and target.

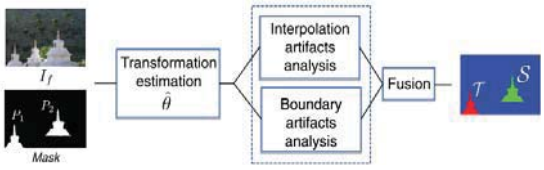


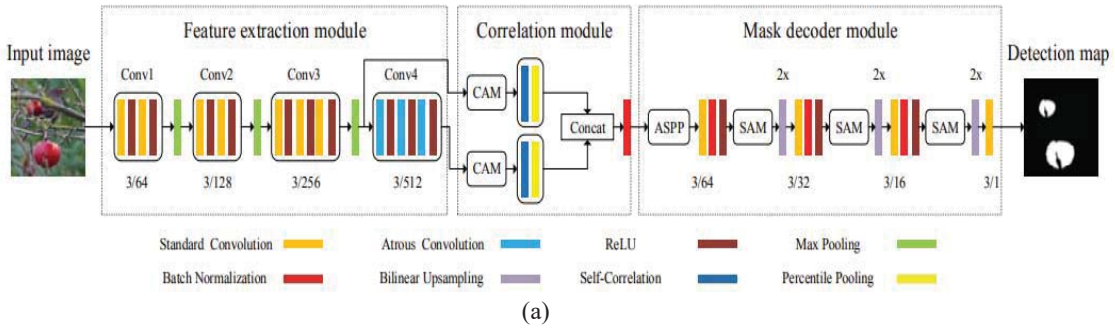
Fig.2 Scheme of the proposed CM disambiguation system. [3]

For the purpose of interpolation artifact analysis and boundary artifact analysis multibranch CNN networks are proposed: A parallel for branch module 4-Twins net which is used for interpolation artifact analysis and Siamese network for boundary artifact analysis. the output of both the networks are merged in a score level fusion module. Proposed architecture as a whole is referred to as DisTool. Architecture of the proposed 4 twins' network is shown in the figure. Before implementing the two networks, preliminary steps are carried out in order to identify the focus of attention (FOA), while the preliminary steps are similar for both the networks in the Siamese network the focus of attention is divided into four parts in order to get better results. Scores are generated based on a weighted sum the weights are assigned based on the reliability of both the network in specific scenarios. The four twins' network is more accurate in case of a more rigid translation while Siamese networks work better in the case of less rigid translation.

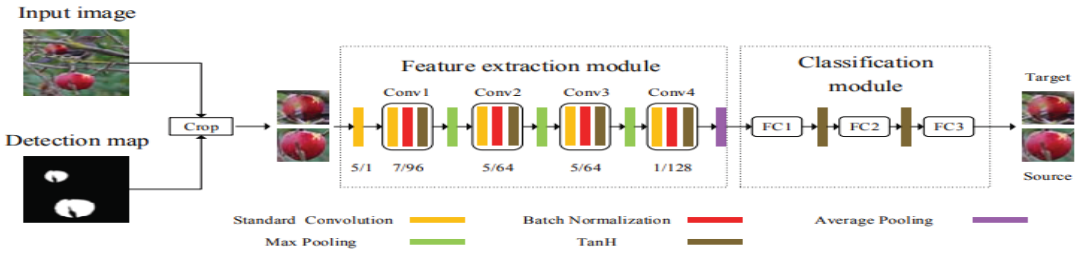
For evaluation purposes the four data sets are considered which includes a synthetically made dataset which further has three subsets in it which contains images with only rotation or only resizing or rigid translation. The methodology is also tested on USCISI, CASIA and GRIP data sets. The results were for Synthetic dataset SYN-T(28000 Images) for SYN-T-Rigid-97.00 accuracy, SYN-T-Rotation-97.90 accuracy and SYN-T-Resize-97.60 accuracy. for other already available datasets also results were comparatively better than previous approaches.

In [4] paper the proposed methodology is developed based on Busternet; busternet is a a dual branch parallel neural network with branches ManiDet and SimiDet -ManiDet is used in order to detect the manipulated regions and SimiDet is used to detect the similar copy move forged region. Hence with the help of results from both of them we can correctly disambiguate between source and target regions, but it has often been observed that the results from the internet are not much accurate because of the parallel branching structure hence in this paper a serial structure for the disambiguation is proposed.

The serial network can be divided into two sub parts: a Copy-Move forgery detection network (CMFDNet) and Source-Target Region Distinguishment Network (STRDNet). In the case of CMFD net the changes done to SimiDet for better performance as Simi date uses VGG16 and hence generates lower resolution features; include double level self-correlation and Atrous convolution to generate high resolution features. Also, the 4th pooling layer is removed to increase the resolution as each pooling layer divides the resolution by half. Also include double level self-correlation for finding relations between each two features and Atrous convolution to resolves the reduction in field of view filters due to pooling layer removal. The atrous convolution is only used for the fourth layer and not the rest in order to not increase the cost of GPU and balance in the batch size so as to keep training efficient. Self-Correlation module is followed by percentile pooling to remove irrelevant information from the score maps. The self-correlation module is followed by Mask Decoder module ASPP in order to take care of the multiscale features. In this module at the end a standard convolution and a softmax layer is used to find the final detection map which has both the source and target region.



(a)



(b)

Fig.3. (a) Copy-Move Similarity Detection Network (b) Source-Target Distinguishment Network [4]

This detection map generated from the CMFD module Is used in order to crop the source and target from the actual input image. The way it is cropped is such that the smallest area containing the source and target and 15 pixels surrounding it. Cropped parts are passed to a feature extraction module containing for convolution groups first 3 followed by a max pooling and the last followed by an average pooling. Once the features are extracted there passed to a cost classification module having three fully connected layers with tanh activation function that classify is between tapered region and untampered region. Tampered region would be the target and the untampered would be the source.

For evaluation purposes a new synthetic data set (100100 images) was created and was used 8:1:1 for training testing and validation respectively. Evaluation was also done for CASIA v2.0(12614 images), CoMoFoD (200 images) and COVERAGE (200 images) data set for different state of the art methods. For data set are as follows CASIA v2.0-0.538, CoMoFoD-0.511 and COVERAGE-0.677 and for synthetic dataset-0.692 and for krocknecker convolution-0. 679.Evaluation in the case of the images under 6 well known attacks used to hide the forgery for different parameters was also considered. Comparison with the Busternet which was the base for the proposed methodology was also performed based on the correctly distinguished images and correctly classified images are synthetic data set(5394 images), CASIA v2.0(278 images), CoMoFoD(67 images) and COVERAGE(48 images).It was also tested for various attacks such as JPEG compression (JC), image blur (IB), Gaussian noise addition (GNA), color reduction (CR), contrast adjustments (CA), and brightness change (BC) with the proposed architecture performing better on all of the cases.

In [5] paper deep learning CNN model that is scale invariant to overcome. The inefficiency in performance due to scaling or rotation of manipulated objects. The method works with multi-scaled images this helps in feature extraction on multiple levels and hence gives an advantage of robustness in scaling. the architecture proposed in the paper can be divided into three parts: encoder phase, Decoder phase and classification phase. In encoder the input images of 256*256 dimensions are scaled multiple times up to 16*16 dimensions and all the 5 levels are taken as input. These images Convolution layer batch normalization and ReLu and down sampled using max pooling but max pooling is not good for segmentation and hence these max pooling is concatenated with activated feature space, continued till lowest scale input dimension. Convolution layer has padding same and stride 1. For visualization and segmentation corresponding to each max pooling up sampling is done. It is followed by convolution layer batch normalization and ReLu.The activated feature space is concatenated with the out of first up sampled layer. classified requires single Depth features space for training hence a 1*1 convolution with stride one and padding same Followed by sigmoid activation function So the image pixels are divided into two parts black and white for authentic and forged pixels. to evaluate the classifiers prediction a loss function is also used lower the value better the prediction; binary cross entropy loss function is used.

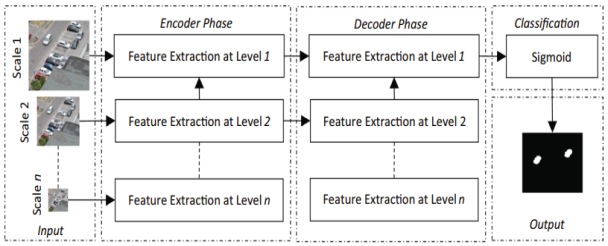


Fig.4. Architecture of proposed model for copy-move forgery detection using deep learning CNN model [5]

Evaluation purposes two data sets:CoMoFoD and CMFD are considered: for 3 kernel size, 6 post processing attacks With various parameters and comparison with various state of art methods. The ratio for training validation and testing is 70,20,10 respectively.

Table 1. Average test result using performance measures precision, recall, accuracy, TNR, FNR, F1-score and MCC value on different datasets [5]

Dataset	P	R	A	TNR	FNR	F1	MCC
CMFD	0.9892	0.9982	0.9878	0.7764	0.0018	0.9936	0.8329
CoMOoFoD	0.9863	0.9962	0.9839	0.8247	0.0038	0.9909	0.8578

Table 2. Average test result using performance measures precision, recall, accuracy, TNR, FNR, F1-score and MCC value on CoMoFoD dataset on different post-processing operations [5]

These abbreviations stand for—F: Only translation without post-processing, BC1-BC3: Brightness change, CA1-CA3: Contrast Adjustment, CR1-CR3: Color Reduction, IB1-IB3: Image blurring, JC1-JC9: JPEG Compression and NA1-NA3: Noise addition

Post-processing	P	R	A	TNR	FNR	F1	MCC
F	0.9863	0.9961	0.9838	0.8215	0.0039	0.9909	0.8558
BC1	0.9862	0.9961	0.9837	0.8186	0.0039	0.9908	0.8537
BC2	0.9860	0.9961	0.9835	0.8152	0.0039	0.9907	0.8510
BC3	0.9852	0.9961	0.9827	0.8029	0.0039	0.9903	0.8419
CA1	0.9864	0.9961	0.9840	0.8261	0.0039	0.9910	0.8589
CA2	0.9865	0.9962	0.9841	0.8293	0.0038	0.9910	0.8613
CA3	0.9858	0.9963	0.9835	0.8279	0.0037	0.9907	0.8607
CR1	0.9863	0.9961	0.9838	0.8213	0.0039	0.9909	0.8556
CR2	0.9863	0.9961	0.9838	0.8212	0.0039	0.9909	0.8556
CR3	0.9863	0.9961	0.9838	0.8214	0.0039	0.9909	0.8556
IB1	0.9861	0.9964	0.9838	0.8221	0.0036	0.9909	0.8575
IB2	0.9862	0.9964	0.9840	0.8217	0.0036	0.9910	0.8579
IB3	0.9862	0.9964	0.9841	0.8195	0.0036	0.9910	0.8560
JC1	0.9862	0.9962	0.9838	0.8277	0.0038	0.9909	0.8595
JC2	0.9860	0.9962	0.9835	0.8268	0.0038	0.9907	0.8573
JC3	0.9864	0.9963	0.9841	0.8287	0.0037	0.9910	0.8610
JC4	0.9867	0.9962	0.9843	0.8300	0.0038	0.9911	0.8611
JC5	0.9865	0.9961	0.9840	0.8298	0.0039	0.9910	0.8604
JC6	0.9865	0.9962	0.9841	0.8281	0.0038	0.9910	0.8602
JC7	0.9863	0.9961	0.9837	0.8261	0.0039	0.9909	0.8573
JC8	0.9863	0.9961	0.9837	0.8245	0.0039	0.9909	0.8570
JC9	0.9871	0.9961	0.9846	0.8456	0.0039	0.9913	0.8710
NA1	0.9869	0.9962	0.9846	0.8269	0.0038	0.9913	0.8600
NA2	0.9868	0.9961	0.9843	0.8278	0.0039	0.9911	0.8598
NA3	0.9868	0.9961	0.9843	0.8273	0.0039	0.9912	0.8593

In [6] paper a key point matching-based algorithm is used for copy move forgery detection. The proposed methodology in the paper consists of four steps: preprocessing, key point calculation, key point matching and morphological processing and LCS.Proposed methodology focuses on features from textured regions as well as a smooth region so in order to perform it properly different feature extraction is used for both scenarios. So different preprocessing needs to be performed for both approaches. For preprocessing of textured areas include removing unsharp edges and noise. The RGB image is converted to grayscale image. Moreover, unsharp masking technique is used to remove blurring and get a sharp image. For pre-processing of smooth regions, the wiener filter is used for adaptive noise removal and also mention that blurring is used for removing noise. Local neighborhood is used for local mean and variance for pixel.

For feature extraction phase, for textured region feature extraction Features from accelerated segment test (FAST) and Binary robust independent elementary features (BRIEF) descriptors are used and for smooth region feature extraction SIFT descriptors are used. In case of FAST Bresson Ham circle of radius 3 with 16 pixels along its circumference is used to find the neighbourhood and pixels below above right and left of this neighbourhood are checked. If 3 pixels out of this 4 are darker than it is checked further if 12 pixels are darker out of the 16 It is considered. Then BRIEF is used for binary feature descriptors finding.256 dimensions descriptors are generated after smoothing. For SIFT different smoothing version and difference of gaussian (DOG), also taylor series on scale space is applied for transformation invariance.

For feature matching a generalization of Lowe's matching technique named g2NN is used.it can also detect multiple copies. It is ratio of di and di+1 where d stands for Euclidean distance. A threshold is decided for ratio for matching. If the matched points are not too close to each other than morphological processing is applied. If normalized area is 40 percent of max the considered otherwise, they are considered outliers. Further localization is improved. Noise is removed through median filtering. super pixel segmentation is performed through linear spectral clustering (LSC). Segmentation is considered meaningful only if SSIM is higher than 0.6.Evaluation is performed on MICC-F220 with CPU time.

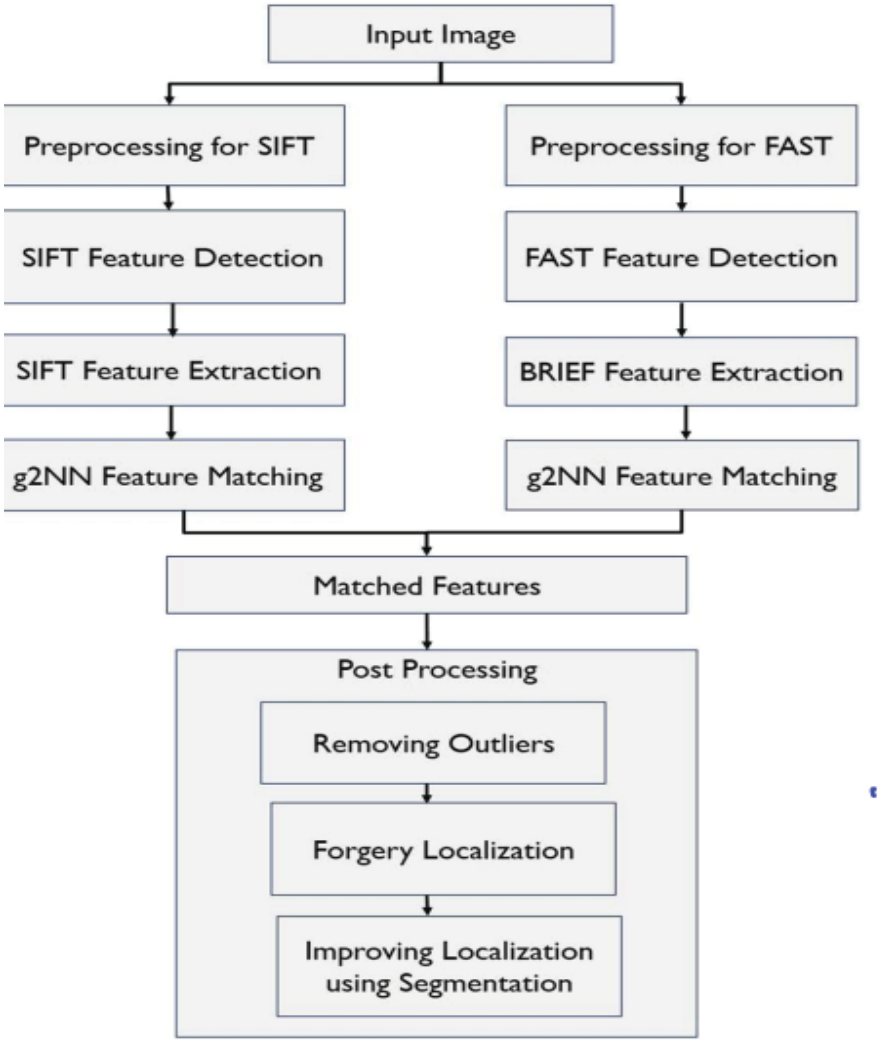


Fig 5. (a) Block diagram of proposed system [6]

Table 3. Performance measurement for 6 selected images [6]

Images	Pun et al. [18]	Ryu et al. [23]	Cao et al. [6]	Proposed
F-Measure				
Image 1	0.5052	0.1153	0.077	0.9626
Image 2	0.8244	0.9143	0.3767	0.9663
Image 3	0.6414	0.0044	0.0326	0.8567
Image 4	0.3241	0.0604	0.0444	0.725
Image 5	0.8317	0.0051	0.0397	0.9508
Image 6	0.6104	0.2646	0.0372	0.94864
Precision				
Image 1	1	0.0612	0.04	0.9476
Image 2	0.9966	0.8428	0.2325	0.9837
Image 3	1	0.0024	0.0173	0.9967
Image 4	1	0.082	0.0281	0.9853
Image 5	0.998	0.0026	0.0.0452	0.9164
Image 6	1	0.2239	0.0462	0.9023
Recall				
Image 1	0.3379	1	1	0.978
Image 2	0.7029	0.9991	0.9927	0.9495
Image 3	0.4721	0.024	0.2821	0.7513
Image 4	0.1934	0.0478	0.1067	0.5735
Image 5	0.7129	0.1582	0.0354	0.9878
Image 6	0.4393	0.3234	0.0325	1
CPU-time (in seconds)				
Image 1	30.335	33.339	97.148	5.622
Image 2	19.300	30.506	46.794	6.367
Image 3	15.613	33.590	63.938	8.4039
Image 4	16.336	30.845	35.470	7.236
Image 5	73.439	33.335	50.346	10.345
Image 6	61.478	44.672	79.345	11.457

3. Summarization

Sr no.	Title of paper	Publication details	Proposed Method	Tools and technology	Datasets	Research possibility
1. [2]	Two-Stage Copy-Move Forgery Detection With Self Deep Matching and Proposal SuperGlue .	Published in IEEE Transactions on Image Processing, Volume 31, 2022	A two stage approach with backbone architecture with deep matching and superglue with convCRF.	VGG16,Atrous convolution, Spatial attention, Self correlation, split matching, SuperPoint, superglue, convCRF	MICC-F220 CoMoFoD CASIA SYNTHETIC	The backbone architecture can be worked on and further multi target CMFD.
2. [3]	Copy Move Source-Target Disambiguation Through Multi-Branch CNNs	Published on IEEE Transactions on Information Forensics and Security, Volume 16,2022,	Geometric transformation followed by 4-twinsNet and Siamese network.	Geometric transformation, 4-Twins Net, Siamese Net, FOA	USCISI Grip CASIA SYN-Ts	Neuro- fuzzy network with back propagation can be used, multi-target detection, robustness by forger perspective.

3. [4]	A serial image copy-move forgery localization scheme with source/target distinguishment	Published on IEEE Transactions on Multimedia, Volume 23, 2021	A BusterNet with Atrous convolution and correlation and mask decoder with classification module.	BusterNet, Atrous Convolution, Mask Decoder, Classification module, Self Correlation.	Synthetic CASIA V2.0 CoMoFoD COVERAGE	Better source target disambiguation and robustness checking using various attacks.
4. [5]	Detection of Copy-Move Forgery in Digital Image Using Multi-scale, Multi-stage Deep Learning Model	Published on Springer in Neural Processing Letters, Volume 54, 2022	A encoder module with a decoder module with classification with sigmoid function.	Encoder, Decoder, sigmoid function	CMFD CoMoFoD	a segmentation using dictionary learning can be used with the proposed deep learning technique for a better result.
5. [4]	CNN-Transformer Based Generative Adversarial Network for Copy-Move Source/Target Distinguishment	CNN-Transformer Based Generative Adversarial Network for Copy-Move Source/Target Distinguishment	A generator and discriminator based deep learning approach for source target disambiguation	Generator, Discriminator, transformer	USCISI, CoMoFoD, CASIA2	The GAN can be improved and is supported by multi-branch CNN.
6. [5]	Disentangling copy-moved source and target areas	Published on Applied Soft Computing Volume 109, 107536, Elsevier on September 2021	An image component statistical deviation using GMM and log likelihood and histogram.	GMM, Empirical histogram, likelihood	CASIA2	without statistical modeling GMM but directly with the pixel values more advanced distance measures such as Wasserstein or MMD (Maximum Mean Discrepancy
7. [6]	FAST, BRIEF and SIFT based image copy-move forgery detection technique	Published on Springer in Multimedia Tools and Applications , 2022	SURF and FAST with BRIEF with pre-processing with G2nn matching and post processing.	SURF, FAST, BRIEF, G2NN , LCS	Synthetic	Multi-target detection and Source-Target disambiguation can also be performed.
8. [7]	A novel copy-move forgery detection algorithm via two-stage filtering	Digital Signal Processing, Elsevier, Volume 113, June 2021, 103032	A key point detection algorithm followed by key point Matching; Delaunay triangulation algorithm and 2 stage filtering scheme Grid-Based Filter and the Clustering-Based Filter	Delaunay triangulation, Grid-Based Filter and the Clustering-Based Filter	IMD CMHD CoMoFoD	Improving clustering based filter by relaxing angular constraint of group building and merging smaller groups nearer to each other.

9. [8]	AR-Net: Adaptive Attention and Residual Refinement Network for Copy-Move Forgery Detection	IEEE Transactions on Industrial Informatics, Volume 16, issue 10, 2020	AR-NET with channel and position attention with Adaptive Attention mechanism and ASPP and Residual Refinement module.	AR-NET, ASPP, Residual Refinement module, Adaptive attention mechanism	CASIAII	A multi-modes architecture for more information as opposed to single stream architecture of now
10. [9]	Copy Move Forgery Detection based on double matching	Journal of Visual Communication and Image Representation, Elsevier, Volume 76, April 2021, 103057	Key-point detection with double matching first LIOP generated key points with Delaney triangle second adding triangles iteratively and Localization by DBSCAN.	LIOP, Atrous Convolution, Delauney triangulation, DBSCAN	MICC-F220	DBSCAN can be updated atrous convolution and self correlation for better feature generation.
11. [10]	Single and Multiple Copy–Move Forgery Detection and Localization in Digital Images Based on the Sparsely EncodedDistinctive Features	Arabian Journal for Science and Engineering, Springer, Volume 45,April 2020	Uses SURF with BRISK descriptors and matching with 2NN and hamming distance followed by DBSCAN and noise clustering.	SURF, BRISK, 2NN, hamming distance, DBSCAN	MICC-F220 MICC-F2000 CoMoFoD	The technique needs to increase robustness from available attacks.
12. [11]	Copy-Move Forgery Detection Exploiting Statistical Image Features	Digital Image Forensics Journal, Springer, chapter 4, 2019	Using Mean and variance similarities between blocks made by Discrete wavelet transform.	Statistical transformation, DWT, Euclidean distance	USCISI + CoMoFoD SELF FORGED for testing	For block based methods a combination of DCT and FFT is used and can be combined with

4. Conclusion

In this paper recent advances in the field of copy move forgery have been studied in order to get an idea to find an optimal approach for forgery detection as well as source target disambiguation which is the process of recognising source from target.It was observed that backbone architecture with proposal superglue gives the best performance for detection of copy move forgery while a multi-branch CNN approach gives best results for source target disambiguation.The use of image processing based method is a step towards a accurate detection of manipulated images and helps in detecting forgeries that are not easily detected by naked human eye.

References

1. “COPY-MOVE-FORGERY-EXAMPLE.JPG”.
2. 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, doi: 10.1109/TIP.2021.3132828.
3. M. Barni, Q. -T. Phan and B. Tondi, "Copy Move Source-Target Disambiguation Through Multi-Branch CNNs," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1825-1840, 2021, doi:10.1109/TIFS.2020.3045903.
4. B. Chen, W. Tan, G. Coatrieux, Y. Zheng and Y. -Q. Shi, "A Serial Image Copy-Move Forgery Localization Scheme With Source/Target Distinguishment," in IEEE Transactions on Multimedia, vol. 23, pp. 3506-3517, 2021, doi:10.1109/TMM.2020.3026868.
5. Jaiswal, A.K., Srivastava, R. Detection of Copy-Move Forgery in Digital Image Using Multi-scale, Multi-stage Deep

Learning Model. Neural Process Lett 54, 75–100 (2022). https://doi.org/10.1007/s11063-021-10620-9

6. Fatima, B., Ghafoor, A., Ali, S.S. et al. FAST, BRIEF and SIFT based image copy-move forgery detection technique. Multimed Tools Appl (2022). https://doi.org/10.1007/s11042-022-12915-y
7. Jixiang Yang, Zhiyao Liang, Yanfen Gan, Junliu Zhong,A novel copy-move forgery detection algorithm via two-stage filtering,Digital Signal Processing,Volume 113,2021,103032,ISSN 1051 2004, https://doi.org/10.1016/j.dsp.2021.103032.
8. Y. Zhu, C. Chen, G. Yan, Y. Guo and Y. Dong, "AR-Net: Adaptive Attention and Residual Refinement Network for Copy-Move Forgery Detection," in IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6714-6723, Oct. 2020, doi: 10.1109/TII.2020.2982705.
9. Qiyue Lyu, Junwei Luo, Ke Liu, Xiaolin Yin, Jiarui Liu, Wei Lu,Copy Move Forgery Detection based on double matching,Journal of Visual Communication and Image Representation,Volume 76,2021,103057,ISSN 1047-3203, https://doi.org/10.1016/j.jvcir.2021.103057
10.]Bilal, M., Habib, H.A., Mehmood, Z. et al. Single and Multiple Copy–Move Forgery Detection and Localization in Digital Images Based on the Sparsely Encoded Distinctive Features and DBSCAN Clustering. Arab J Sci Eng 45, 2975–2992 (2020). https://doi.org/10.1007/s13369-019-04238-2
11. Roy, A., Dixit, R., Naskar, R., Chakraborty, R.S. (2020). Copy-Move Forgery Detection Exploiting Statistical Image Features. In: Digital Image Forensics. Studies in Computational Intelligence, vol 755. Springer, Singapore. https://doi.org/10.1007/978-981-10-7644-2_4
12. Y. Zhang *et al*., "CNN-Transformer Based Generative Adversarial Network for Copy-Move Source/Target Distinguishment," in *IEEE Transactions on Circuits and Systems for Video Technology*, 2022, doi: 10.1109/TCSVT.2022.3220630.
13. Ludovic Darmet, Kai Wang, François Cayre,Disentangling copy-moved source and target areas,Applied Soft Computing,Volume 109,2021, 107536,ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2021.107536.