Analysis of Active and Passive Mechanism for Image Forgery Detection

Swati Mishra
Dept. of ECE
Madhav Institute of Technology and Science
Gwalior MP,India

Karuna Markam
Dept. of ECE
Madhav Institute of Technology and Science
Gwalior India

Abstract*—With the expanding accessibility of carefully put away data and the advancement of new multimedia services, security questions are ending up considerably more critical This paper shows a procedure ready to check digital image (DI) with an invisible and undetectable emit data, called the watermark. This procedure can be the premise of a total copyright security system. The procedure initial step comprises in delivering a discharge picture. The initial segment of the mystery dwells in essential data that structures a parallel picture. That picture is then recurrence adjusted. The second piece of the mystery is decisively the frequencies of the bearers. The two insider facts rely upon the character of the copyright proprietor and on the first picture substance. They got picture is known as the stamp. The second step comprises in balancing the adequacy of the stamp as per a concealing basis originating from a model of human observation. That excessively hypothetical basis is adjusted by methods for morphological apparatuses situating in the photo the spots where the measure is assumed not to coordinate. This is trailed by the adjustment of the level of the stamp at those spots. The so shaped watermark is then added to the first to guarantee its security. That watermarking strategy permits the identification of watermarked pictures in a surge of DI, just with the information of the photo proprietor's insider facts.

***Keywords*—image Forgery detection; SIFT; RANSAC;watermarking.**

I. INTRODUCTION

As the fast advancement of interactive media and Internet, computerized content—DI, audio, video, 3D virtual protests et cetera, are broadly utilized as a part of different fields. In any case, these interactive media objects are so effortlessly got, duplicated and appropriated that the computerized data security turns out to be more troublesome. Advanced watermark is an effective strategy for copyright security. As of late, numerous advanced watermark plans have been proposed for security of proprietorship rights on computerized content. In any case, different assaults have been accounted for to pulverize watermarks [1]. Among those attacks, geometric mutilation has been regarded to a standout amongst the most troublesome assaults to oppose, inferable from the synchronization blunders that geometric bending actuate. Consequently, the watermark synchronization process is basic to the vigor of the watermark frameworks. Lately, a few techniques that are impervious to geometric mutilations have been proposed. These plans can be generally delegated format based, invariant change area based, and minute based. Be that as it may, the vigor of each of the three previously mentioned watermark approaches is restricted. For example, another assault called scheme assault can devastate the layout with no earlier learning. The introduction caused by invariant area changes and the discretisation caused by minutes increment the synchronization blunders, which make watermark inserting and location misaligned. Thus, second era watermark conspire was proposed to enhance the strength of watermark to oppose geometrical twisting. This plan removes remarkable component guides which are invariant toward geometric change for watermark synchronization. Some component based watermark approaches are crudely looked into in the accompanying. [1].

Image forgery detection system can be of two types: active and passive1 which are shown in Figure 1. Inactive techniques, detection of forgery is done by authenticating the integrity of a pre-coded data like digital signature or watermarking whereas in passive technique, it depends on the originality of the given digital image which is most widely used in this digital world. Image composition or image splicing, image tampering, and image retouching are different types of passive techniques. There is the need of an efficient and a novel technique to easily distinguish the modified or tampered images from the authentic or original image.[2].

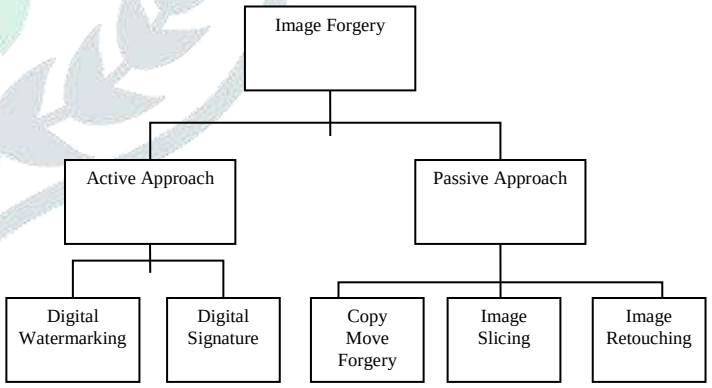

Fig. 1. Different types of image forgery detection.

II. RELATED WORK

A. Frequency distribution using DWT as (DWT) is concentrated on both time and frequency; this transform gives good frequency and high temporal resolution for low and high frequency components. According to proposed algorithm (DWT) is applied using 'Haar' wavelet on to the image to verify whether the image is smooth or detailed image. This is done by calculating the low frequency energy. This process gives the appropriate frequency energy coefficients to calculate the initial size of the super pixel. B. Extraction of super pixels We gone through many experiments and found that better forgery regions are detected mostly in irregular blocks com- pared to regular blocks regions. However, (SLIC) cannot provide the initial size of the super pixel, the coefficients

collected from (DWT) using 'Haar' wavelet is used to find the super pixel size S.

$$E^{LF} = \sum(|CA_4|) \qquad (1)$$

$$E^{HF} = \sum_i \left(\sum|CD_i| + \sum|CV_i|\right), \qquad i = 1, 2 \ldots, 4 \qquad (2)$$

ELF indicates low frequency energy; EHF indicates high frequency energy. CA gives the fourth approximation coefficients, whereas CD, CH, CV gives the detail coefficients.
Low frequency percentage is calculated as

$$P^{LF} = \frac{E^{LF}}{E^{LF} + E^{HF}} . 100\% \qquad (3)$$

$$S = \begin{cases} \sqrt{0.02 \times M \times N}, P^{LF} > 50 \\ \sqrt{0.01 \times M \times N}, P^{LF} > 50 \end{cases} \qquad (4)$$

Using (4) we can calculate the size of S whereas MxN indicates the size of the input image. This calculation helps SLIC to give the meaningful non-overlapping irregular blocks.

SIFT

The SIFT algorithm combined with improved RANSAC method, by using the rule of the matching distance basically consistent, most non association points were kicked out. The remaining points were used as pre matching points to be iterated by RANSAC method, which reduces the number of iterations and improves the matching efficiency. [3]
For distinguishing interest point from a grey-level picture, SIFT descriptor is utilized which at that point gives particular nearby slope bearings of picture with various power esteems. The description of the image characteristic is then confined in the local neighborhood around each interest point. For matching of the images, SIFT descriptor is used which corresponds to the interest points between different images. The SIFT descriptor is also used in object classification, texture identification etc. There are usually four main steps in SIFT operation.

RANSAC:

Random Sample Consensus (RANSAC) algorithm is used to extract the matched regions. The experimental result of the algorithm which is proposed indicates that, it can extract more accurate results compared with existing forgery detection methods.
The mismatched points are mostly eliminated after the RANSAC selection, however, the remaining matched feature points may themselves exist error. We use the least square method to minimize the error. The objective function is constructed as:

$$f(A) = \sum_{j=1}^{N} \left\| P_j' - AP_j \right\|_2^2$$

where P_j is one of the feature points in the original image, P_j ' is the point in the attacked image that are matched with P_j . Obtain the inverse affine matrix according to the estimated affine matrix A, then make an inverse affine transform to correct the geometrically distorted image.[4]

III. FORGERY DETECTION

Forgery detection (FD) strategies turn out to be significantly more confounded to manage the most recent fabrication procedures. This back to the accessibility of advanced altering apparatuses, modification, and control turn out to be simple and thus fraud recognition turns into a perplexing and undermining issue [5]. Image forgery location can be controlled in different courses with numerous basic activities like relative changes, for example, interpretation, scaling, and so on., remuneration tasks, for example, splendor, hues, differentiate alterations, and so on., concealment task, for example, noise extraction, sifting, pressure, and so forth.,. Furthermore, more mind boggling tasks are additionally conceivable, for example, compositing, mixing, tangling, trimming, photomontage prompting outwardly untraceable ancient rarities in a picture. The programmed and logical strategy for recognizing the produced pictures has turned into a major testing issue for analysts and a similar issue is valid for each media substance.

IV. USING TECHNIQUES

Watermarking

A watermark is a distinguishing picture or example in paper that shows up as different shades of gentility/murkiness when seen by transmitted light (or when seen by reflected light, on a dim foundation), caused by thickness or thickness varieties in the paper. Watermarks have been utilized on postage stamps, cash, and other government records to debilitate falsifying. There are two primary methods for creating watermarks in paper; the dandy move process, and the more complex cylinder mould process [6]

Digital Watermarking (DW)

The motivation behind DW is to insert evident data into digital information. The inserted image is generally undetectable or hard to distinguish, yet it can be recognized or extricated by certain extraction calculations. The watermark is hidden in the original data as an integral part of it, and general framework of digital watermarking technology is shown in Figure 1

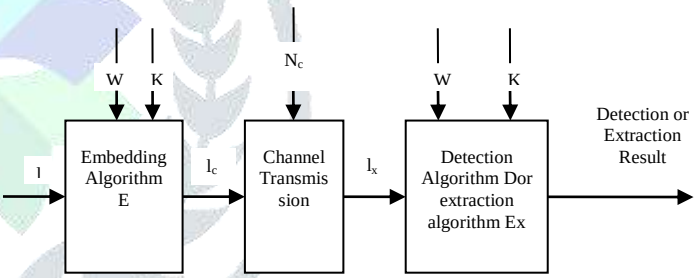

Fig. 1. General framework of digital watermarking.

The digital watermark W is combined with the certain key K, which is embedded into original signal I by the embedding method E, generating the watermarked signal I_w. In the transmission, owing to the interference of noise N_c, the watermarked signal I_w can be transformed into Ir, and the received signal I_r can be evaluated or extracted by applying the detection algorithm D or extraction algorithm Ex. [7]

V. LITERATURE SURVEY

Ahmed Ghoneim, et al. (2018) with the innovation of new correspondence advances; new highlights and offices are given in a brilliant medicinal services system. The features and facilities aim to provide a seamless, easy-to-use, accurate, and real-time healthcare service to clients. As health is a sensitive issue, it should be taken care of with utmost security and caution. This article proposes another medicinal picture FD framework for the social insurance system to confirm that pictures identified with human services are not changed or modified. The framework takes a shot at a commotion guide of a picture, applies a multi-resolution relapse channel on the noise guide, and feeds the yield to help vector-machine-based and outrageous learning-based classifiers. The

commotion delineate made in an edge registering asset, while the sifting and order are done in a center distributed computing asset. In this way, the system works seamlessly and in real time. The bandwidth requirement of the proposed system is also reasonable.[8]

Gonapalli Ramu, et al. (2017) Cloning (duplicate move imitation) is a pernicious altering assault with advanced pictures where a piece of picture is reordered inside the picture to cover the important details of image without any obvious traces of manipulation. This type of tampering attacks leaves a big question of authenticity of images to the forensics. Many techniques are proposed in the past few years after powerful software's are developed to manipulate the image. The proposed plot is included with both the square based and highlight point extraction based systems to separate the manufactured districts all the more precisely. The proposed algorithm mainly involves in matching the tentacles of same features extracted from each block by computing the dot product between the unit vectors. Random Sample Consensus (RANSAC) calculation is utilized to remove the coordinated areas. The experimental result of the algorithm which is proposed indicates that, it can extract more accurate results compared with existing forgery detection methods [10]

Ying Zhang, et al. (2017) This work introduces an approach to localize the tampered region among the images from social media platforms. We propose a joint model to integrate the predictions from a set of features, each of which represents the inherent relation among the pixels within a certain distance to detect the forgery. Within a fixed distance, the feature is adapted from a few basic statistics through a stacked Autoencoder to a proper version in a noise-resistant manner, so that it will be more robust to detect the tampering when the forgery gone through some common social media platform operations. The classifier is trained using a standalone dataset from a benchmarking but is pre-processed properly to simulate its possible imperfections when spreading over the Internet. The approach was tested on images from Facebook, with results showing an encouraging improvement from the prior arts.[11]

Junjie Zhang, et al.(2017) Active detection technology was widely used in the traditional tampering detection. Firstly, those mainstream technologies of active detection were introduced. Then, some necessary improvements for the tampering detection algorithm were proposed in this paper, for example, the steganography information was cross-embedded to enhance the safety of the images, and the chaos function was simplified to enhance the execution efficiency and detection precision of the algorithm. Experimental outcomes about demonstrated that the proposed calculation can enhance the productivity of picture tamper detection.[12]

Paulo Max G. I. Reis (2017) et al present that Audio authentication is an essential project in multimedia forensics stressful strong techniques to hit upon and identify tampered audio recordings. In this text, a brand new method to detect adulterations in audio recordings is proposed by exploiting odd versions inside the Electrical Network Frequency (ENF) signal at last installed in an addressed sound account. These uncommon renditions are because of unexpected section discontinuities as a result of inclusions and concealments of sound pieces amid the altering assignment. First, we recommend an ESPRIT-Hilbert ENF estimator alongside an outlier detector based at the sample kurtosis of the anticipated ENF. Next, we utilize the processed kurtosis as entering for a SVM classifier to recommend the nearness of altering. The proposed scheme, wherein unique as SPHINS, drastically outperforms associated previous tampering detection methods within the performed assessments. We validate our effects the use of the Carioca 1 corpus with a hundred unedited authorized audio recordings of phone calls. [13]

Chi-Man Pun (2016) et. Al. present that TD strategies based on picture hashing were widely studied with non-stop improvements. However, most existing fashions can't generate object-level tampering localization consequences because the forensic hashes connected to the image lack contour records. In this paper, we gift a singular TD version that may generate an accurate, item-level tampering localization quit end result. First, an adaptive image segmentation technique is proposed to phase the picture into closed regions based on strong edges. At that point, the color and capacity feature of the shut territories are separated as a scientific hash. Furthermore, a geometrical invariant tampering localization version named Image Alignment based Multi-Region Matching (IAMRM) is proposed to establish the location correspondence among the obtained and forensic images by exploiting their intrinsic shape statistics. The model estimates the parameters of geometric ameliorations thru a robust image alignment approach primarily based on triangle similarity; additionally, it fits multiple regions concurrently through utilizing manifold rating based on one-of-a-kind graph systems and functions. Experimental consequences display that the proposed IAMRM is a promising method for object-stage TD compared with ultra-modern strategies.[14].

VI. PROPOSE WORK

Problem Statement

Cloning (copy-move forgery) is a malignant altering assault with computerized pictures where a piece of picture is reordered inside the image to conceal the important details of image without any obvious traces of manipulation. This type of tampering attacks leaves a big question of authenticity of images to the forensics.

Propose work:

In this section, a novel watermarking method and SIFT, RANSAC, are compared. In spite of the fact that an extensive number of feature point are gotten by SIFT, some element focuses are as yet not appropriate for watermark data inserting and extraction as far as scale and introduction. In this way, feature point ought to be screened and enhanced before inserting activity. In our propose paper, Random example accord, or RANSAC, is an iterative strategy for evaluating a numerical model from an informational index that contains exceptions. The RANSAC calculation works by distinguishing the exceptions in an informational index and assessing the coveted model utilizing information that does not contain anomalies. By SIFT calculation you can check the coordinating level of key point between the information and other property changed picture by utilizing the key point areas utilizing this code. The motivation behind DW is to implant clear data into digital information. The installed image is normally undetectable or hard to distinguish, yet it can be recognized or separated by certain extraction algorithms.

Proposed ALGORITHM:

1. Browse an host image from dataset
2. Browse an watermark image from dataset
3. Then Embedding process
   Using DWT a 512×512 host image is sub-divided into 4-subbands. Represents the 1st level of DWT decomposition of host picture. Where LL, HL, LH, HH are 4 sub-bands. Here LL represents the high scale low frequency co-efficient set, HL represents the horizontal details of low scale high frequency set, LH represents the vertical details of low scale high frequency set, HH represents the

diagonal details low scale high frequency set of the host image.

4. After select area for tempered process
5. Then Tempering
6. After that Extract with tempered

The extraction technique is depicts in. To extract the mark picture from the embedded or watermarked picture the original 512×512 picture is used, hence this is an informed DW technique.

$$W' = \frac{[f'(m,n) - f(m,n)]\sqrt{|(m,n)^2 - f_{avg}(m)^2|}}{\alpha[f(m,n) - f_{avg}(m)]}$$

Read the watermarked image.
Read matrix (a secret key) which is sent with image.
Subtract Matrix from watermarked Image in matrix subtraction form.
Now generate two different images from theses matrices form.
The output images are Original image and watermarked image.

7. Calculate parameter is Accuracy

$$Accuracy(A) = \frac{TP+TN}{TN+TP+FN+FP}$$

8. Calculate Specificity

$$Specificity(Sp) = \frac{TN}{TN+FP}$$

9. Calculate Sensitivity,

$$Sensitivity(S) = \frac{TP}{TP+FN}$$

10. Calculate FPR , FNR

FPR= 1- specificity (FPR: False Positive Rate)
FNR= 1- sensitivity (FNR: False Negative Rate)

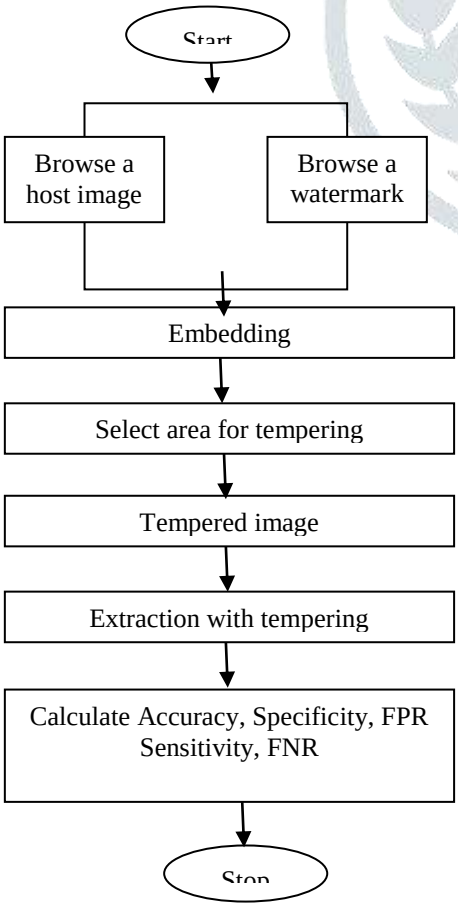

Fig. 1 Flow chart on Propose work

VII. RESULT ANALYSIS

MATLAB is used to test the images where we had tested 80 images with resolutions between 1000 x 900 and 1200 x 1000.

Fig. 2 First, We 'Run' our code and then obtain this type of menu bar.
In this menu bar there are 6 steps.

Fig. 3. Browse an Host image from dataset.

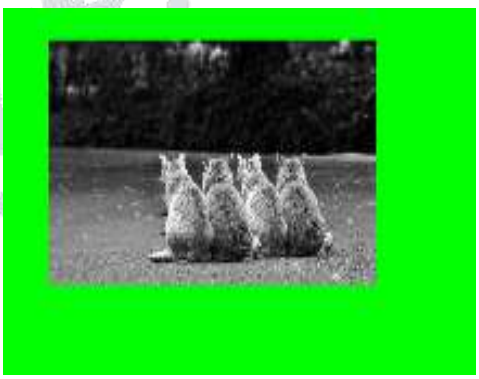

Fig. 4. Browse a Watermark image from dataset.

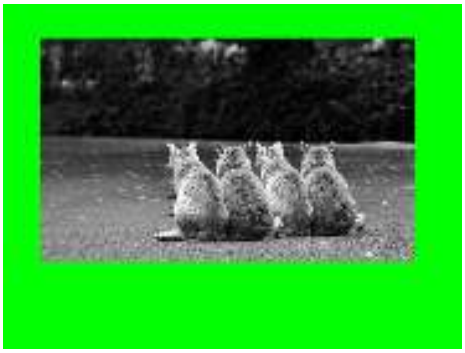

Fig. 5. Embedding

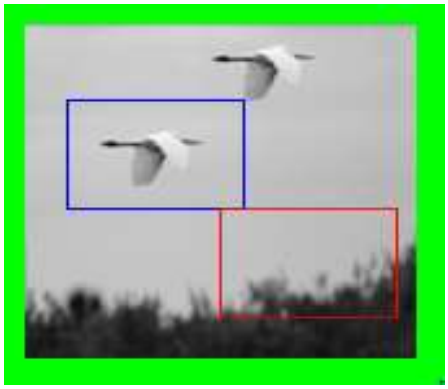

Fig.6. Tempering process.

Fig. 7. Selected area of tempered

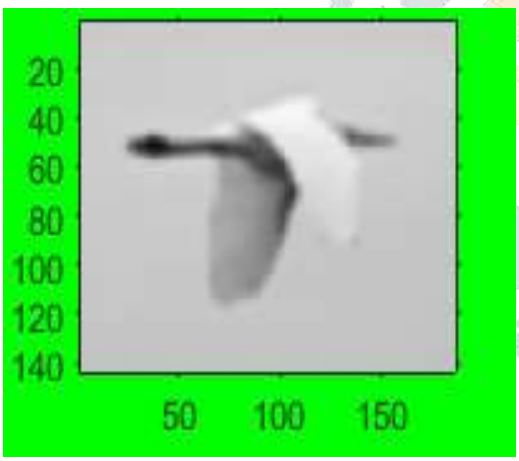

Fig. 8. Tempered image

Fig. 9. Extraction with temper

Table 1. Comparison on Base Accuracy and Propose Accuracy

Base Accuracy	Propose Accuracy
98.0200	99.1700

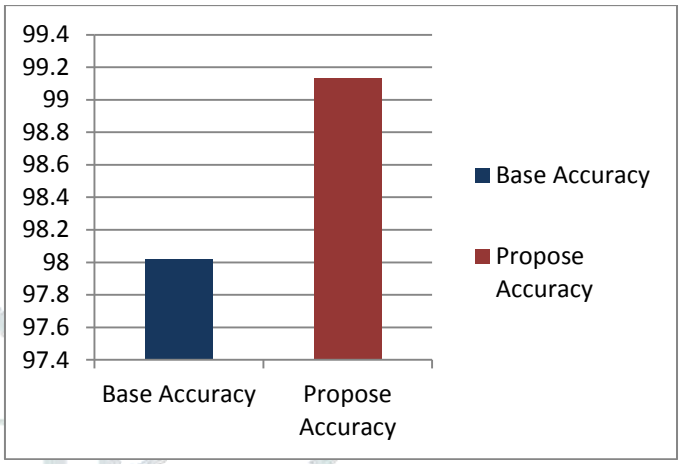

Fig. 10. Comparison Graph on Base Accuracy and Propose Accuracy

Table 2. Comparison on Base SPECIFICITY and Propose SPECIFICITY

Base SPECIFICITY	Propose SPECIFICITY
92.5781	95.4893

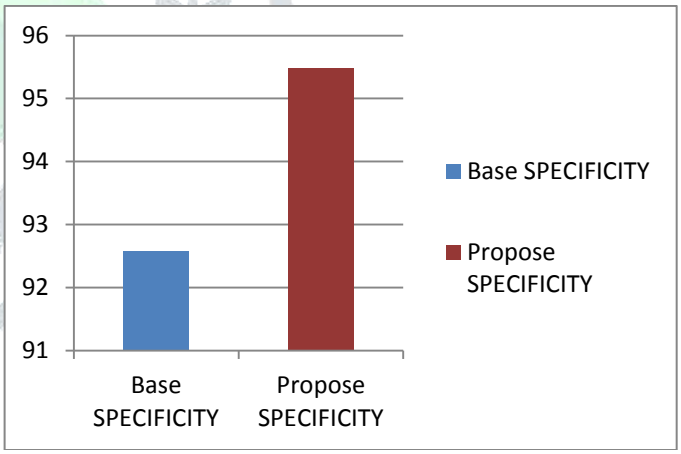

Fig. 11. Comparison Graph on Base SPECIFICITY and Propose SPECIFICITY

Table 3. Comparison on Base SENSITIVITY and Propose SENSITIVITY

Base SENSITIVITY	Propose S SENSITIVITY
95.2510	96.5057

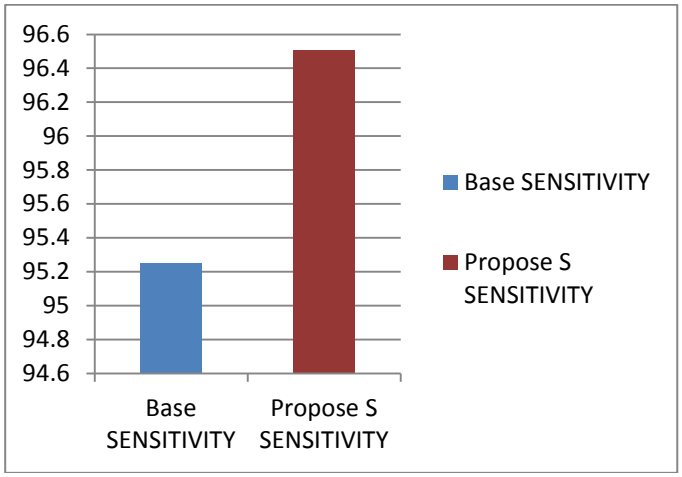

Fig. 12. Comparison Graph on Base SENSITIVITY and Propose SENSITIVITY

Table 4. Comparison on Base FPR and Propose FPR

Base FPR	Propose FPR
7.4219	4.5107

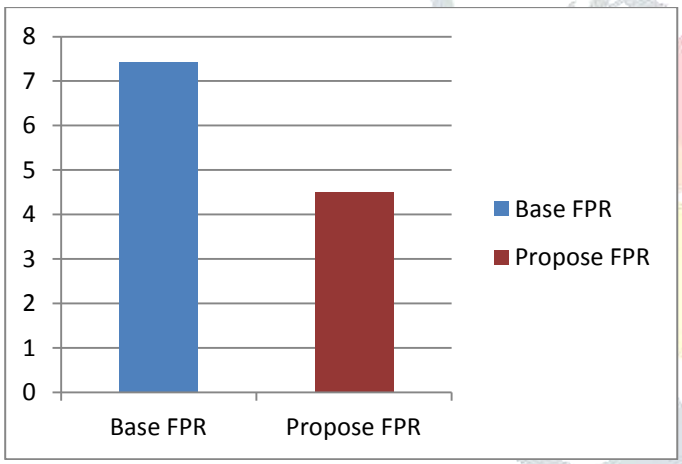

Fig. 13. Comparison Graph on Base FPR and Propose FPR

Table 5. Comparison on Base FNR and Propose FNR

Base FNR	Propose FNR
3.9013	2.9695

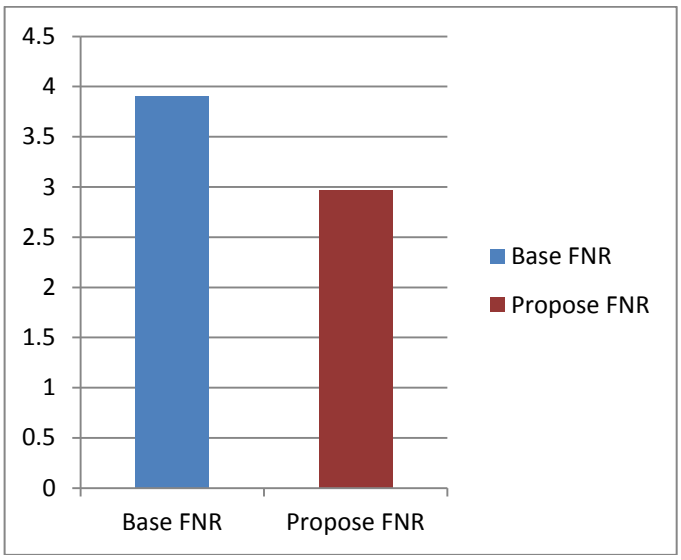

Fig. 14. Comparison Graph on Base FNR and Propose FNR

Conclusion

We analyzed both active and passive mechanism and we came into a conclusion that active mechanism gives more accuracy, specificity and better value for FNR. The active mechanism is high sensitive the n passive mechanism.

Our Future work is how we merge two algorithms for getting better results.

References

[1] Haijun LUO1 , Xingming SUN1 , Hengfu YANG2 , Zhihua XIA1, "A Robust Image Watermarking Based on Image Restoration Using SIFT". RADIOENGINEERING, VOL. 20, NO. 2, JUNE 2011

[2] Rajeev Rajkumar1*, Sudipta Roy1 and Kh. Manglem Singh2, "A Robust and Efficient Copy-Move Forgery Detection Technique based on SIFT and SVD". Indian Journal of Science and Technology, Vol 10(14), DOI: 10.17485/ijst/2017/v10i14/110034, April 2017 ISSN (Print) : 0974-6846 ISSN (Online) : 0974-5645

[3] 22. Lowe D. "Distinctive image features from scale-invariant keypoints", cascade filtering approach. IJCV. 2004; 1–28

[4] Wuyong Zhang Jianhua Chen* Rongshu Wang Xiaolong Wang Tian Men, "Affine Correction Based Image Watermarking Robust to Geometric Attacks". 2016 17th International Conference on Parallel and Distributed Computing, Applications and Technologies978-1-5090-5081-9/16 $31.00 © 2016 IEEE

[5] Asif Hassan1 ,Dr. V.K. Sharma, "Passive Forgery Detection and Analysis-A Survey". International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 03, Issue 01; January - 2017 [ISSN: 2455-1457]

[6] Anuja Dixit1 and R. K. Gupta, "Copy-Move Image Forgery Detection using Frequency-based Techniques: A Review". International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.9, No.3 (2016), pp.71-88 http://dx.doi.org/10.14257/ijsip.2016.9.3.07.

[7] Yunpeng Zhang, Chengyou Wang, Xiaoli Wang * and Min Wang, "Feature-Based Image Watermarking Algorithm Using SVD and APBT for Copyright Protection". Future Internet 2017, 9, 13; doi:10.3390/fi9020013

[8] Ahmed Ghoneim, Ghulam Muhammad, Syed Umar Amin, and Brij Gupta, "Medical Image Forgery Detection for Smart Healthcare". IEEE Communications Magazine • April 2018 0163-6804/18/$25.00 © 2018 IEEE

[9] Gonapalli Ramu, S.B.G. Thilak Babu, "Image forgery detection for high resolution images using SIFT and RANSAC

algorithm". Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES 2017) IEEE Xplore Compliant - Part Number:CFP17AWO-ART, ISBN:978-1-5090-5013-0, 978-1-5090-5013-0/17/$31.00 ©2017 IEEE

[10] Kang Hyeon RHEE, "Forgery Image Detection of Gaussian Filtering by Support Vector Machine Using Edge Characteristics". 978-1-5090-4749-9/17/$31.00 ©2017 IEEE

[11] Ying Zhang, Vrizlynn L. L. Thing, A Multi-Scale Noise-Resistant Feature Adaptation Approach For Image Tampering Localization over Facebook". 2017 IEEE 2nd International Conference on Signal and Image Processing, 978-1-5386-0969-9/17/$31.00 ©2017 IEEE

[12] Junjie Zhang, Jun Tan , Yun Cheng, "Research on digital image tampering detecting algorithm of remote healthcare platform". 2017 4th International Conference on Information Science and Control Engineering, 978-1-5386-3013-6/17 $31.00 © 2017 IEEE

[13] Paulo Max G. I. Reis, Joao Paulo C. L. da Costa, ˜ Senior Member, IEEE, Ricardo K. Miranda, Student Member, IEEE and Giovanni Del Galdo, Member, IEEE," ESPRIT-Hilbert based audio tampering detection with SVM classifier for forensic analysis via electrical network frequency", IEEE TRANSACTIONS ON INFOMATION FORENSICS AND SECURITY, 2017.

[14] Chi-Man Pun, Senior Member, IEEE, Cai-Ping Yan, and Xiao-Chen Yuan, Member, IEEE," Image Alignment based Multi-Region Matching for Object-level Tampering Detection", 2016 IEEE