ISSN: 2456-9348
Vol (01) _Issue (05) Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management

A NOVEL APPROACH FOR IMAGE TAMPERING USING IMAGE HASHING

Amrita Parashar*[1]
[*1]Department of Computer Science & Engineering, ASET, Amity University Madhya Pradesh-474001, India
*Corresponding author: aparashar@gwa.amity.edu
Ph: +91-8878844486

ABSTRACT
Because of effective PCs and propelled picture altering programming devices the pictures control has turned into a basic errand. Validate pictures credibility and altered locales from picture identifying with no data about picture content. An exertion is made to study the current headways being made in the field of advanced picture phony identification and therefore detached strategies for fabrication location are being introduced. In this paper Gaussian, salt and pepper, sprinkle and discover histogram with hash era and after that discover better outcome as look at base work.

Keywords: **-** Tampering, DCT, DWT, SVD and HASH function.

INTRODUCTION

The increasing techniques in image editing and to protect the digital visual data against malicious manipulations makes the use of visual content as evidence material unreliable. It puts question on trust worthiness of digital online multimedia information. Therefore the techniques that are used for validity and authenticity of a received image are needed in context of internet communication. The image authentication process checks the image for its originality. Tampering of image means the part of the real image is altered. Thus the image has two areas, tampered area and unchanged area. In order to perform tampering localization all geometric transformation (e.g. rotation, scaling etc.) should be first filtered out, so that alignment of received image can be done as with the one at the sender. The signature of image implies all the important data related to the image key points which are used for the authentication of received image at destination. The signature of image signature should be much compact, robust against the allowed operations and also it should differ from the one that is computed on tampered image. The tampering detection is the process of finding out tampered areas in image which is based on block wise searching. Image is spilt into different blocks and with gradients histograms representation, the tampering detection and localization is complete. The overall process takes following steps:

1. Feature Extraction: The features of image dataset are extracted and a vocabulary of features is formed, and then it is shared to sender and receiver. At source the features of image that is to be sent are calculated, signature with most robust features is prepared and it is sent with image itself to the destination.

2. Signature Comparison: At destination same procedure is applied for received image to get signature. The both signatures are compared and similarities are found out. With help of similar features data the image alignment is done.

iJETRM
International Journal of Engineering Technology Research & Management

3. Tampering detection: The received image is divided into blocks and HoG for each block is prepared. These histograms are compared with the received histogram data and the tampered area is found [1].

LITERATURE SURVEY

Cai-Ping Yan (2016) et al present that a novel quaternion-based image hashing to detect almost all types of tampering including color-changing, copy-move, splicing, and so on. First, the quaternion Fourier-Mellin transform (QFMT) is used to calculate the geometric hash to eliminate the influence of geometric distortions. Then, a new quaternion image construction approach, which combines both color and structural features benefit, is proposed to implement quaternion Fourier transform (QFT) to calculate the image feature hash to locate the tampered regions [2].

Paweł Korus (2016) et al present that pixel-wise combination is sub-optimal and successful fusion needs to model dependencies between neighboring pixels and exploit the content of the tampered image. Here estimate two different approaches based on the conditional random fields and demonstrate that they can exploit image content and precisely delineate the forgery shape. In contrast to existing approach based on the explicit image segmentation, such technique does not suffer from subtle object eliminate forgeries where valuable segments do not exist [3].

Yi XIE (2015) et al presents that a method of electronic bills against modification based on watermarking technology. Using semi-fragile watermarking to the protect electronic bills; bills can withhold few reasonable minor change, for example moderate image compressing and color-to-grey conversion without warning data. While if these electronic bills are tampered deliberately, these modified bills can be identified and warning information is prompted when detecting watermark [4].

Qing Wang (2015) et al present that a novel probability model based on the first digit statistics of DCT coefficients, to express the changes of statistical properties after manipulation. And we combined Bayes' theorem to detect and locate the tampered regions [5].

Gong Zhenzhen (2015) et al present that a new tamper detection method for clipped double JPEG compression image based on the statistical characteristics of DCT coefficients and block effect caused by double JPEG compression. The offset of the two DCT grids can be obtained by computing the loss of information. Then we will trim image according to offset, and it will be presented to evaluation primary compression quality factor [6].

iJETRM
International Journal of Engineering Technology Research & Management

Bala Mallikarjunarao Garlapati (2015) et al present that a method based on casting Log Co-ordinate Mapping (LCM), in which embedding two watermark segments in two different frequency regions, one for authentication information purpose and other for finding unauthorized source. The LCM method has approving performance against DA-AD conversion attacks [7].

Amol V. Dabhade (2015) et al present that The videos sent from one end to other can be tampered maliciously in between. The frames in video can be edited or frames sequence can be altered or even few frames can be deleted, any such malicious alteration is possible. Thus it is very necessary to verify integrity of video data to ensure trustworthiness of the information content. In numerous cases, for example surveillance, medical, forensic investigations it is needed to consider video authenticity [8].

PROPOSED WORK

Image hashing algorithm especially emphases on: robustness and discrimination. This means that we can still extract the same hashing values to confirm the authentication information of the image after conventional attacks. This needs us to extract some deep-level characteristics of the image. These features need to be enough to express the basic content of the image and have strong stability. Also these features need to have the ability of distinguishing the maliciously attacked image or perception significantly different image from the original image. Moreover, the obtained hashing values should be different and random. In other words, the hashing values are statistically independent.

ISSN: 2456-9348
Vol (01) _Issue (05) Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management

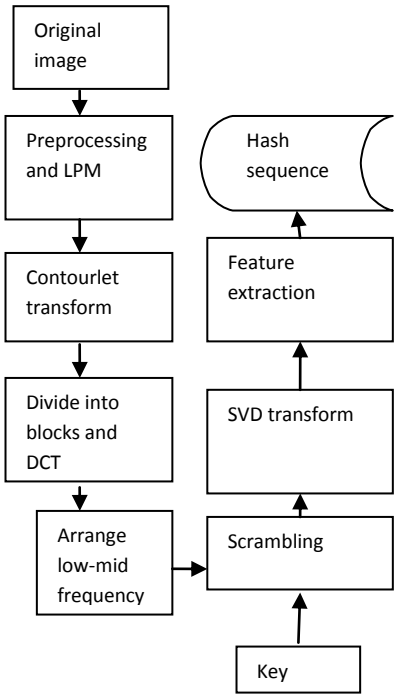


Fig.1 Hash Generation

iJETRM
International Journal of Engineering Technology Research & Management

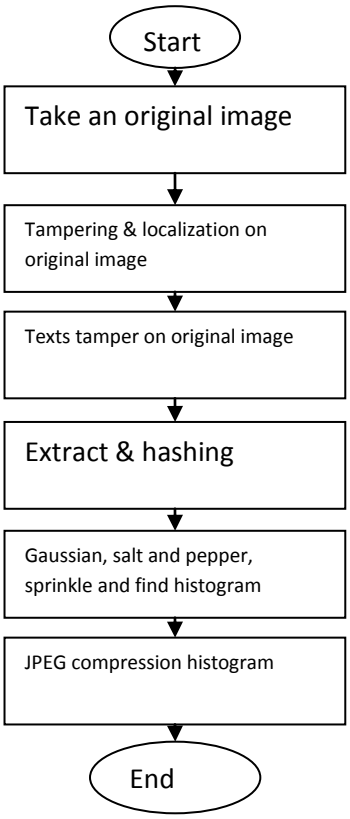


Fig 2. Proposed Work

According to the proposed work first select an original image then apply tampering and localization on original image then text tamper apply on original image after extraction and hashing technique apply. Gaussian, salt and pepper, sprinkle noises apply and find their histogram value last JPEG compression histogram.

ISSN: 2456-9348
Vol (01) _Issue (05) Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management

RESULT SIMULATION

Fig 3. Image Dataset

This image data sets contain five different type images (flower.jpeg, animal.jpeg, baboon.jpeg, lena.jpeg and peppers.jpeg).

A. Base Result

Fig 4. Menu Bar

iJETRM
International Journal of Engineering Technology Research & Management

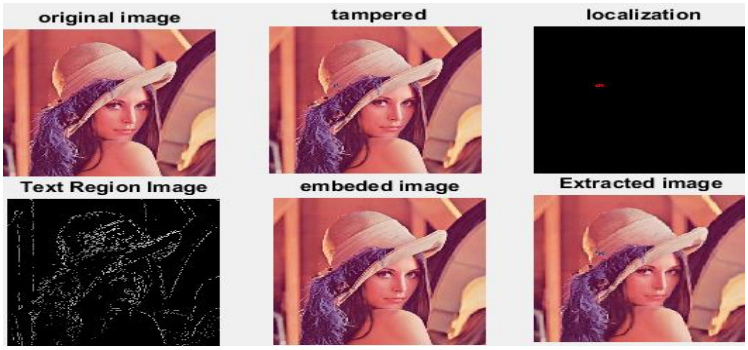


Fig 5. Original Image Various Solutions

In this figure show various functions and their solution (tampered, localization, Text region image, embedded image and extraction image).

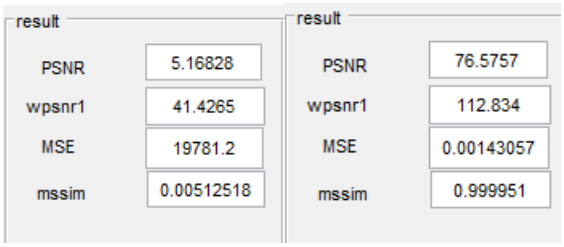


Fig 6. (a) Base embedded result and (b) Base extraction result

This figure show base embedded result and base extraction result (PSNR, WPSNR1, MSE and MSSIM).

B. Proposed result

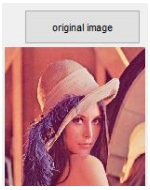


Fig 7. Select original Image

First select original image from image data set here Lena.jpeg image select

iJETRM
International Journal of Engineering Technology Research & Management

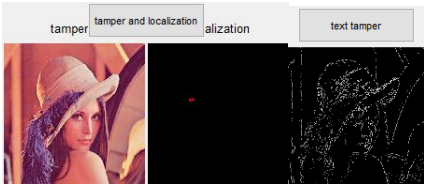


Fig. 8 Tamper and localization

Apply tamper and localization on original image and then apply text tamper.

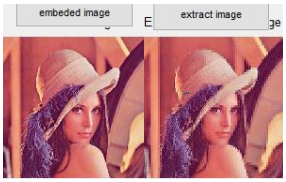


Fig. 9 Embedded and Extract Image

Find embedded and extraction image according to proposed technique.

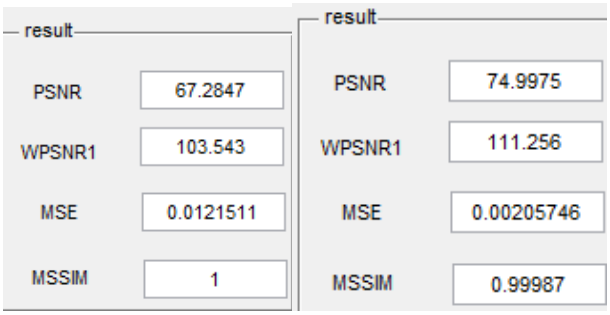


Fig 10. (a) Proposed embedded result and (b) Proposed extraction result

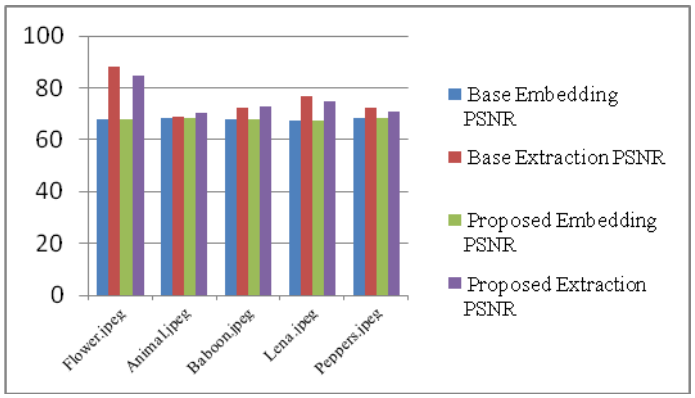
This figure show proposed embedded result and proposed extraction result (PSNR, WPSNR1, MSE ans MSSIM)

iJETRM
International Journal of Engineering Technology Research & Management

C. Comparison base and proposed result

Table1. Comparison between base (embedding and extraction) PSNR and proposed (embedding and extraction) PSNR

Image	Base PSNR		Proposed PSNR	
	Embedding	Extraction	Embedding	Extraction
Flower.jpeg	67.8746	88.2312	67.8781	84.7623
Animal.jpeg	68.3256	68.7809	68.4337	70.4429
Baboon.jpeg	67.9192	72.1411	67.9758	72.6669
Lena.jpeg	67.2558	76.8176	67.2839	74.9822
Peppers.jpeg	68.1559	72.3061	68.249	70.8284



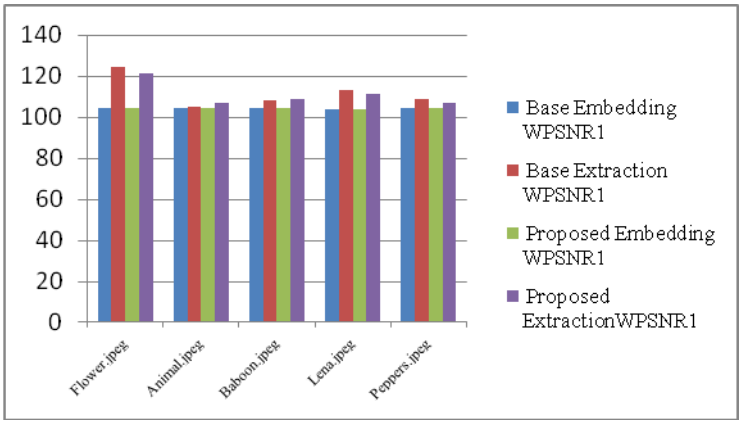
Graph 1.: Graph comparison between base (embedding and extraction) PSNR and proposed (embedding and extraction) PSNR

ISSN: 2456-9348
Vol (01) _Issue (05) Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management

Table2 COMPARISON BETWEEN BASE (EMBEDDING AND EXTRACTION) WPSNR1 AND PROPOSED (EMBEDDING AND EXTRACTION) WPSNR1

Image	Base WPSNR1		Proposed WPSNR1	
	Embedding	Extraction	Embedding	Extraction
Flower.jpeg	104.133	124.489	104.136	121.021
Animal.jpeg	104.584	105.039	104.692	106.701
Baboon.jpeg	104.177	108.399	104.234	108.925
Lena.jpeg	103.514	113.076	103.542	111.24
Peppers.jpeg	104.414	108.564	104.507	107.087



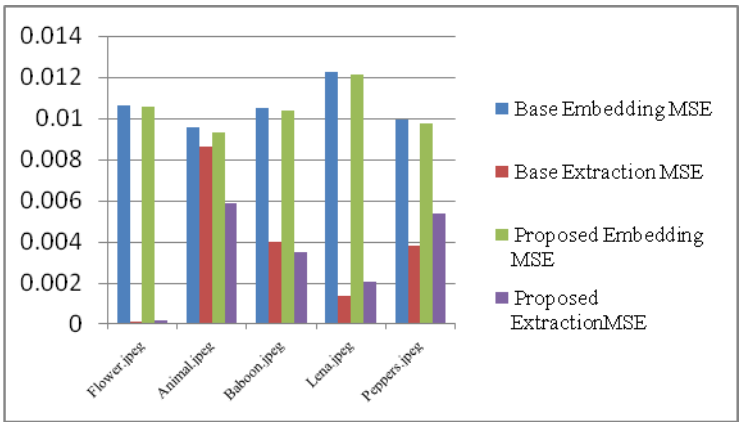
Graph 2. Graph comparison between base (embedding and extraction) WPSNR1 and proposed (embedding and extraction) WPSNR1

ISSN: 2456-9348
Vol (01) _Issue (05) Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management

Table3 COMPARISON BETWEEN BASE (EMBEDDING AND EXTRACTION) MSE AND PROPOSED (EMBEDDING AND EXTRACTION) MSE

Image	Base MSE		Proposed MSE	
	Embedding	Extraction	Embedding	Extraction
Flower.jpeg	0.0106078	0.000101278	0.0105991	0.000217195
Animal.jpeg	0.00956132	0.00860968	0.00932625	0.00587206
Baboon.jpeg	0.0104994	0.00397162	0.0103633	0.00351874
Lena.jpeg	0.0122322	0.00135306	0.0121533	0.00206472
Peppers.jpeg	0.00994231	0.00382354	0.00973158	0.00537327

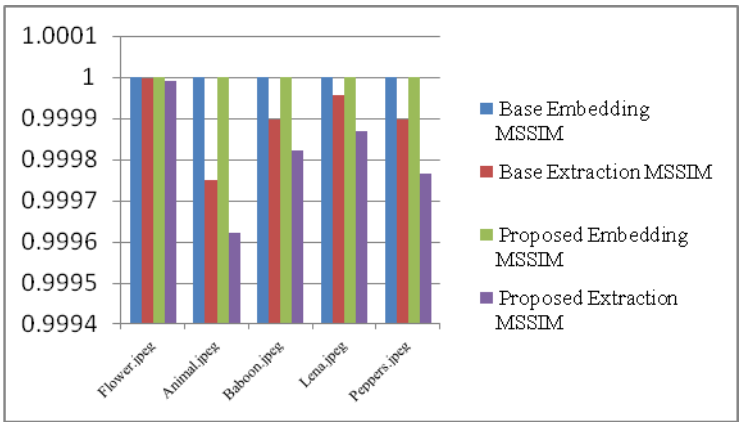


Graph 3. Graph comparison between base (embedding and extraction) MSE and proposed (embedding and extraction) MSE

iJETRM
International Journal of Engineering Technology Research & Management

Table4 COMPARISON BETWEEN BASE (EMBEDDING AND EXTRACTION) MSSIM AND PROPOSED (EMBEDDING AND EXTRACTION) MSSIM

Image	Base MSSIM		Proposed MSSIM	
	Embedding	Extraction	Embedding	Extraction
Flower.jpeg	1	0.999997	1	0.99999
Animal.jpeg	1	0.999749	1	0.999622
Baboon.jpeg	1	0.999897	1	0.999822
Lena.jpeg	1	0.999957	1	0.99987
Peppers.jpeg	0.999999	0.999896	0.999999	0.999766



Graph 4. Graph comparison between base (embedding and extraction) MSSIM and proposed (embedding and extraction) MSSIM

CONCLUSION

Digital imaging has experienced tremendous growth in present decades, and digital camera images have been used in increasing various applications. Now a day's various software's are presented that are used to manipulate image so that the image is look like as original. Images are used as authenticated proof for any crime and if these images do not remain genuine then it will be problem create. Detecting these kinds of forgeries has become serious problem at present. To define whether a digital image is original or doctored is a big challenge. To find the tampering marks in a digital image is a difficult task. In this paper Gaussian, salt and pepper, sprinkle and find histogram with hash generation and then find better result as compare base work.

iJETRM
International Journal of Engineering Technology Research & Management

References

[1]. Swati Shivaji Bhosale and Gyankamal J. Chhajed," Authentication and Tampering Detection of Transferred Image", International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 6, June – 2014, pp: 835-839.
[2]. Cai-Ping Yan, Chi-Man Pun and Xiao-Chen Yuan," Quaternion-based Image Hashing for Adaptive Tampering Localization", 2016 IEEE.
[3]. Paweł Korus and Jiwu Huang," Evaluation of Random Field Models in Multi-modal Unsupervised Tampering Localization", 2016 IEEE International Workshop on Information Forensics and Security (WIFS)
[4]. Yi XIE, Yixin CHEN, and Yulin WANG," Tamper Detection of Electronic Bills based on Semi-Fragile Watermarking", 2016 First International Conference on Multimedia and Image Processing, pp:41-44.
[5]. Qing Wang, Rong Zhang and Ke Qing," Passive Detection of Tampered JPEG Image Based on First Digit Statistics", 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2015 IEEE, pp: 401-404.
[6]. Gong Zhenzhen, Niu Shaozhang and Han Hongli," Tamper Detection Method for Clipped Double JPEG Compression Image", 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2015 IEEE, pp: 185-188. Intelligence, Modelling and Simulation, pp: 325-331.
[7]. Bala Mallikarjunarao Garlapati, Srinivasa Rao Chalamala and Krishna Rao Kakkirala," Tamper Detection in Speech based Access Control Systems using Watermarking", 2015 Third International Conference on Artificial
[8]. Amol V. Dabhade, Yogesh J. Bhople, K. Chandrasekaran and Swapan Bhattacharya," Video Tamper Detection Techniques based on DCTSVD and Multi-Level SVD", 2015 IEEE