# Method for Detect and Extract Forgery from Images

. Hanaa Mohsin Ahmed *( Assist.Prof) Ph.D Sabaa Rakan Salim *

## Abstract:

According the availability of many image editing and processing tools, it is led possible to easily change the information represented by a digital images without leaving any obvious traces of tampering, which led to the problem of verification image. These issues of multimedia security have led to the development of several approaches to tampering detection. Digital image forensics is branch that deals with the identity and authenticity of the images.

The proposed system is the Verification system for images. Where the Verification system used non-blind passive image forensic, and that it has been achieved by using fuzzy gradient based image reconstruction, which is able to detect and extract all types of forgery (Splicing, Image Retouching, Geometrical Transformation, Copy Move Attack, other type) and also able to compute forgery ratio as percentage. The experimental results show that the proposed system achieves accuracy of 100% for detect and extract all type of forgery, with image enhancement capabilities.

**Keywords:**Image tampering; forgery detection; fuzzy process; gradient; poisson**.**

*University of Technology

## 1. Introduction:

Digital Photo images are everywhere, on the covers of magazines, in newspapers, in courtrooms, and all over the Internet. Also editing software for images, such as Adobe Photoshop, GIMP, and Corel Paint Shop are ease available for every person, which it's to enable using different types of forgery like [1]: splicing, image retouching, geometrical transformation, and copy move Attack. This led to the emergence of a problem digital authentication for images. These issues of multimedia security have led to the development of several approaches to tampering detection.

Detect forgery from image has become an important topic of research due to its potential use in a wide range of applications. Digital images have become a very important information carrier in our daily lives. the development taking in the editing software for images, such as Adobe Photoshop, GIMP, and Corel Paint Shop, some of which are available for free, using different type of forgery like [1]: : Splicing " it is a method of tampering images by combining two sources to produce a new image which retains the majority of one image", Image Retouching "is done in most of the magazine covers to give images with a poor quality an enhanced appeal by changing the background", Geometrical transformation "Some images have a portion of the picture altered by some common geometric transformations such as translation, scaling and rotation", A copy move attack "is commonly used to conceal parts of an image or to remove unwanted portions in an image and by using other type of forgery ,and other types of forgery(nosing image ,double JPEG compression) . This led to the emergence of a problem digital authentication for images. These issues of multimedia security have led to the development of several approaches to tampering detection.

Digital image forensics is a new research field that aims to detect tampering in digital images. It has two principal approaches to detect forgery as depicted in Figure (1), first active approach are classified into two categories. The first category is based on digital watermarking. The second category of methods is based on digital signatures [2 and 3]. Second, Passive approach methods are classified into two categories, the first category is based on Blind passive approach [2], the second category of methods is based on Non-blind passive [4].

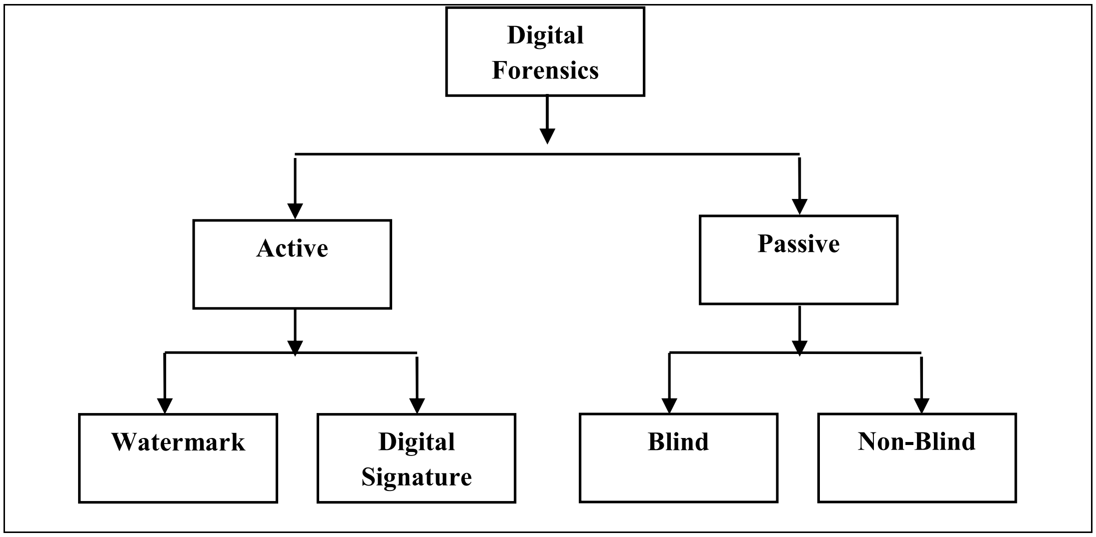


**Figure (1): Types of Digital Image Forensic [3].**

Digital Image Forensics generally can be subdivided into three main branches as in [5 and 2]:

1. Image source identification,
2. Computer generated image recognition, and
3. Image forgery detection.

In this paper fuzzy gradient based image reconstruction has been presented to implement for image to detect and extract forgery from image and also the compute the forgery ratio from image as a percentage .The proposed system detection all kinds of tempering . The scope of this paper focus on a reliable forgery detection system for digital images that will be useful in areas such as journalism, forensic investigation, criminal investigation, insurance processing, surveillance systems, intelligence services and medical imaging. The passive forgery detection is still an active topic of research.

The rest of the paper is organized as follows: Section two reviews the literature review for detect forgery from image forensic, Section three explain fundamental used of proposed system. Section four explain algorithm for proposed system and results and analysis are done in, Section four deals with the conclusion.

## 2- Literature review

Here are a few available techniques digital authentication used against art forgery by depending on using the image processing methods such as removing noise or using mathematics.

In 2004, A.C.Popescu and H.Farid have proposed in [6] a noise inconsistencies detection method based on estimating the noise variances of overlapping blocks by which they tile the entire investigated image. The method uses second and fourth moments of analyzed block to estimate noise variance. The method assumes white Gaussian noise and non-Gaussian uncorrupted image. The method also assumes that kurtosis of the original signal is known, which is mostly not true in practice.

In 2007, Hongmei Gou and etal., [7] Introduced a novel approach for tampering detection and steganalysis on digital images using three sets of noise features. They obtained the de-noising algorithms to obtain the estimates of image noise. The second set of features was obtained by wavelet analysis and the third was obtained by utilizing prediction errors of neighborhood prediction. Using these features a classifier was built to distinguish direct camera output from their tampered or stego versions.

In 2009, another method capable of detecting image noise inconsistencies is proposed in [8]by B.Mahdian and S.Saic. The method is based on tiling the high pass diagonal wavelet coefficients of the investigated image at the highest resolution with non-overlapping blocks. The noise variance in each block is estimated using a widely used median based method and used as homogeneity condition to segment the investigated image into several homogenous sub regions. The shortcoming of the method is that the threshold must be carefully selected; otherwise it is difficult to separate the tampered region from rest of the image.

In 2011, Xunyu Pan et. al. [9] described a novel method for image forgery detection based on the clustering of image blocks with different noise variances.

In 2012, Again Xunyu Pan et. al. [10] described an effective method for exposing image splicing by detecting inconsistencies in local variances. Their method is based on the Kurtosis concentration property of natural image in the band pass filtered domains. The method has limitation as it assumes that splicing region and original image have different intrinsic noise variances. Sonal Sharma et al. [11] introduced a novel methodology based on gradient based image reconstruction to classify images as original or tampered. This methodology has its application in a context where the source image is available (e.g. the forensic analyst has to check a suspect dataset which contains both the source and the destination image).

In 2013, U. M. Gokhale et al. [12] proposed a passive or blind technique for the tampering detection as it does not require a priori information or rely on pre-distribution watermarking or digital signature which is the case with active approaches. The tampering can be detected by comparing the PSNR and SNR of the authentic and tampered image. The region of tampering is localized using the blocks. The method identifies a tampered region when noise has been added locally. Random noise could be added across the entire image to conceal image tampering, and this would not be detected by this method. Ashima Gupta et al. [13] described an effective method to detect doctored JPEG images and further locate the doctored parts, by examining the double quantization effect hidden among the DCT coefficients. These methods detect region duplication forgery by dividing the image into overlapping blocks and then we search for the matching region in the image.

## 3. The Basic Concepts

### 3.1- Fuzzy process

Fuzzy Set Theory is useful in handling various uncertainties in computer vision and image processing applications, or Fuzzy Image Processing, which is a collection of different fuzzy approaches to image processing that, can understand, represent, and process the image. It has three main stages, namely, image fuzzification, modification of membership function values, and defuzzification, [14], shown Figure (2.5).

The fuzzification and defuzzification steps are due to the fact that we do not possess fuzzy hardware. Therefore, the coding of image data (fuzzification) and decoding of the results (defuzzification) are steps that make possible to process images with fuzzy techniques. The main power of fuzzy image processing is in the middle step (modification of membership values .After the image data are transformed from gray-level plane to the membership plane (fuzzification), appropriate fuzzy techniques modify the membership values [15and 14] by:

$$\mu = \begin{cases} 2[\mu_{mn}]^2 & 0 < \mu_{mn} < 0.5 \\ 1 - 2[1 - \mu_{mn}]^2 & 0.5 < \mu_{mn} < 1 \end{cases} \quad , \text{............ (1)}$$

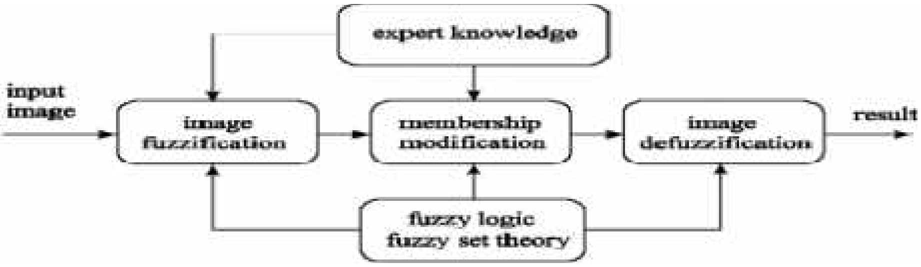


**Figure (2): The general structure of fuzzy image processing [14].**

## 3.2- Normalization

Normalization is a process that changes the range of values in attribute. This involves transforming the data to fall within a smaller or common range such as [−1, 1] or [0.0, 1.0]. Three types of normalization: min-max normalization, z_score normalize and normalization by decimal scaling [11].

Min-max normalization performs a linear transformation on the original date, the formula of Min-max normalization are [16]:

$$NI = (I - Min)\frac{new\,Max - new\,Min}{\text{Max}-\text{Min}} + newMin, \text{ .......................... (2)}$$

*Also to return normalized data to the old values using* min max de-normalization, the formula of Min-max normalization are [16]:

$$Id = (Ir - xmin)\frac{New\ max\text{-}New\ min}{Xmax\ \text{-}Xmin} + Newmin, \text{ .................................. (3)}$$

## 3.3-Poisson Image Reconstruction Using Image Gradients

Image reconstruction from gradient and the Poisson equation solving techniques have been addressed in many related areas such as [17-22], and used for authenticity verification (forgery detection), where the image is converted into gradient map and then is reconstruction the image by taking the gradient map as the input and dissolved in a Poisson equation where they are rebuilt image. A Poisson solver produces the image whose gradients are closest to the input manipulated gradient domain image in a least squares sense, thereby doing a kind of inverse gradient transform by using zero Dirichlet boundary condition. In 2D, a modified gradient vector field [23],[24]:

$G' = [G'x, G'y]$ .......................................(4)

In this process, since the gradient is usually non-integrable, the output cannot be obtained by the direct integration of gradients. Instead, an image whose gradient is close to the targeting gradient is obtained. Let I' denote the image reconstructed from G',

|| □I' – G|| ......................................... (5)

The problem of computing a function f (x,y) whose gradient □f (x,y) is as close as possible to a given gradient field g (x,y) is commonly solved by minimizing the following objective:

$\iint \|\nabla f - G'\|^2 \, dx\, dy$ .....................................(6)

By introducing a Laplacian and a divergence operator, I' can be obtained by solving the Poisson differential equation with fixed boundary condition

$\nabla^2 f = \nabla . G$ ...........................................(7)

For soving the Poisson equation more efficiently, an alternative is to use a rapid Poisson solver, which uses a sine transform (DST) based on the method, to invert the Laplacian operator [25].

## 3.4-Discrete Sine Transform

The **discrete sine transform** (DST) is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using a purely real matrix. It is equivalent to the imaginary parts of a DFT of roughly twice the length, operating on real data with odd symmetry (since the Fourier transform of a real and odd function is imaginary and odd), where in some variants the input and/or output data are shifted by half a sample.

Formally, the discrete sine transform is a linear, invertible function F : RN → RN (where R denotes the set of real numbers), or equivalently an N × N square matrix. There are several variants of the DST with slightly modified definitions. The N real numbersx0, ..., xN-1 are transformed into the N real numbers X0, ..., XN-1 according to the formula:

$$X_k = \sum_{n=0}^{N+1} x_n \sin\left[\frac{\pi}{N+1} (n+1)(k+1)\right] \quad \text{.............................................(8)}$$

The inverse of DST is DST multiplied by 2/ (N+1). Like for the DFT, the normalization factor in front of these transform defini-tions is merely a convention and differs between treatments [24].

$$X_k = \frac{2}{N+1} \sum_{n=0}^{N+1} x_n \sin\left[\frac{\pi}{N+1} (n+1)(k+1)\right] \quad \text{.............................................(9)}$$

### 3.5- Absolute Difference

For any two images, the absolute of difference between images is defined as the Absolu Difference, as [24]:

N(x, y) $= |O_1(x,y) - O_2(x,y)|$,............................................ (10)

Where: $O_1(x,y)$ and $O_2(x,y)$ are pixels in the images,

### 3.6-Forgery Ratio

Is a new proposed method to compute forgery ratio as a percentage in test image by using this equation:

Forgery ratio= (number of block difference/total number of block) *100 (11)

### 3.7 Image Quality Measures

Image quality measures are used to evaluate the imaging systems and processing techniques. There are many varieties of these measures, some of existing image quality measures will be presented as [26]:

### 3.7.1 Mean Squared Error (MSE)

To calculate the Mean Squared Error between the original and reconstruction images, The MSE measure is used to compare between two images by describing the degree of similarity between them, it is assumed that one of the images is original and the other is reconstructed , the difference of pixel color in the two images most be known[27]. The formula of MSE is:

MSE= $\frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{jk}-x'_{jk}\right)^2$ .....................................................(12)

### 3.7.2 Peak Signal-to-Noise Ratio (PSNR)

Peak signal-to-noise ratio (PSNR) is one of the most common measures, it is the ratio between maximum possible power and corrupting noise, PSNR is used as measure of quality of reconstruction image,the signal in this case is the original image (cover image) and the noise is the error introduced (reconstructed image).PSNR is defined via the MSE, the high value of PSNR indicates the high quality of the image.[27].The formula of PSNR is:

PSNR=10 $\log_{10}\left(\frac{Max^2}{MSE}\right)$ ........................(13)

Where max is maximum pixel value of image

## 4. The Propsed System

The concept of proposed system is using fuzzy gradient based image reconstruction technique as a system for detect forgery from images as well enable to compute the forgery ratio as a percentage. Figure (3) illustrates the framework of the proposed system.

The proposed system consists of two phases: the first phase named: (DB_phase), which database phase must be connected with the construction of the system (i.e., this phase related to the original image, which is comparable with the image to be detected). The original image is enter to the proposed system to perform the pre-processing for the image by converting it to grey image. The next step will be fuzzification step where the input image crisp value is associated with value between [0, 1] by using normalization, which enter to the process of image reconstruction by using gradient based image reconstruction then apply the intensifier operation to modify the membership values that means apply threshold for membership, which in turn work kind of enhancement on the images and then defuzzification image by using demoralized image. The result is converted to crisp value.After complete the fuzzy process taking the absolute difference between the original image before fuzzification, and the reconstructed image after defuzzification, finally, the original image and the reconstruction image, and the feature of the absolute difference are stored in database. This phase is illustrates in figure (4)

The second phase named: Verification phase to detect and extract forgery. Firstly detecting forgery by enter test image to be determine whether a digital image is original or fake. The same steps in DB phase are repeated except storage step. To determine if the image is fake or not, the absolute differences is segment into non overlapping 4 × 4 blocks for test image and corresponding image in DB. then, if all blocks of absolute differences in test image are equal with corresponding blocks in corresponding image DB then the test image is not fake and vice versa .Also in multi block technique compute forgery ratio as a percentage in test image by using equation (11) . Secondly extract forgery region in test image by comparing each pixel of test image with corresponding pixel for original image to shown of pixel difference which in turn is forgery region. If pixel is not equal with corresponding pixel then putting zero for different pixel, this phase is illustrates in Figure (5).

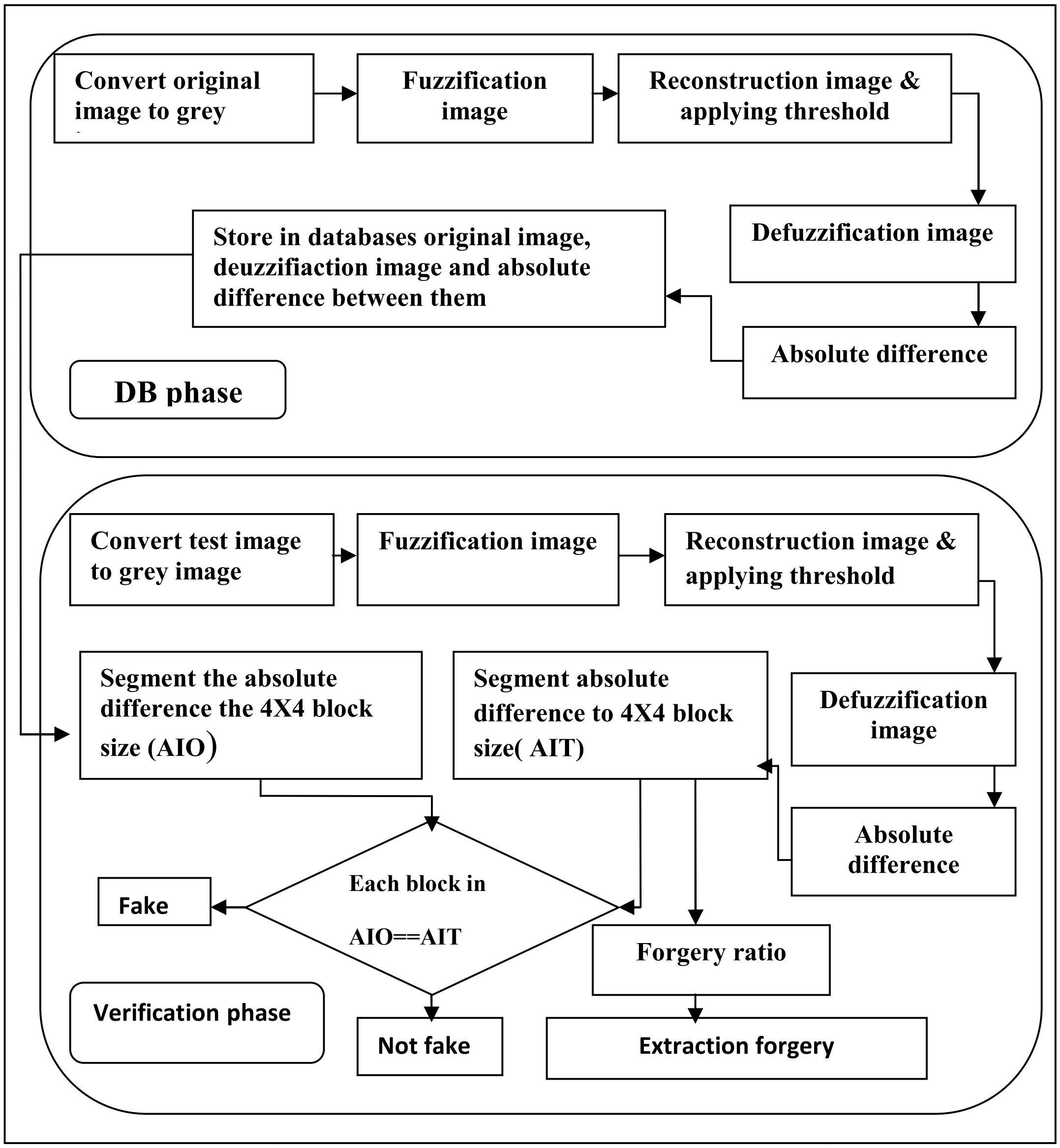

Convert original image to grey
Fuzzification image
Reconstruction image & applying threshold
Defuzzification image
Store in databases original image, deuzzifiaction image and absolute difference between them
Absolute difference
DB phase
Convert test image to grey image
Fuzzification image
Reconstruction image & applying threshold
Segment the absolute difference the 4X4 block size (AIO)
Segment absolute difference to 4X4 block size( AIT)
Defuzzification image
Absolute difference
Each block in AIO==AIT
Fake
Forgery ratio
Verification phase
Not fake
Extraction forgery

**Fig.3: Framework of the Proposed System**

```
Input :original image
Output :saving  absolute difference and original image and reconstruction image
Step 1: read original image.
Step 2: preprocessing image (convert to gray image, resizing image).
Step 3: Fuzzifiction image (normalized image).
Step 4: Reconstruction image by using gradient based image reconstruction.
Step 5: Apply a threshold
Step 6: Defizzification reconstruction image (De-normalized image).
Step 7: Find the absolute difference between original and reconstructed image after Defuzzification A.
Step 8: Store the absolute difference and original image and reconstruction image in DBs.
```

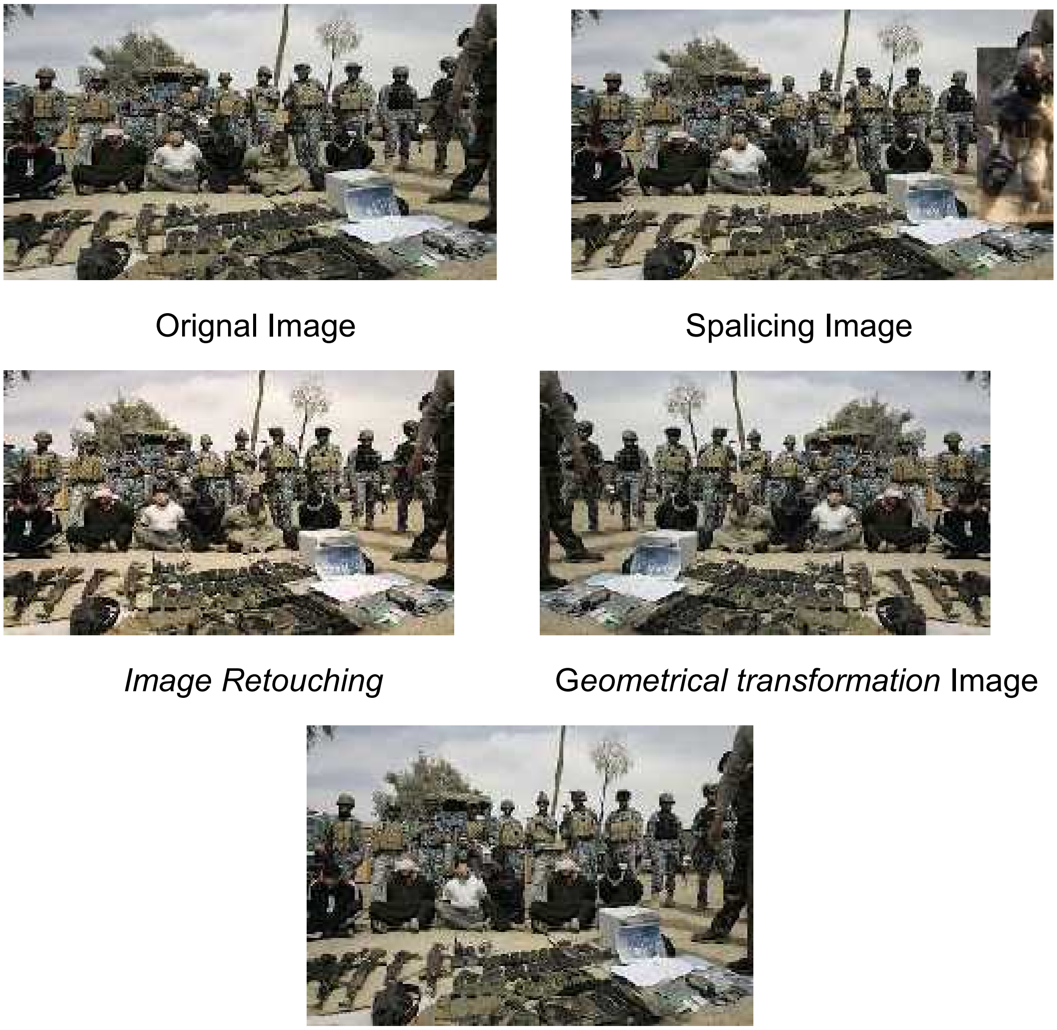
**Figure (4): DB phase (for Database)**

```
Step 1: Input test image.
Step 2: Preprocessing image (convert to gray image, resizing,).
Step 3: Fuzzifiction image (normalized image).
Step 4: Reconstruction image by using gradient based image.
Step 5: Apply a threshold
Step 6: de-fuzzification reconstruction image (De-normalized image).
Step7: Find the absolute difference between original and reconstructed image after De-fuzzification.
Step 8: divided absolute difference for original image in phase one and for test image into multi block each blocks size 4X4.
Step 9: compare each block for test image in corresponding original image to find a match and hence allow or reject the subject accordingly
Step 10: compute forgery ratio.
Step  11: extract forgery
```

**Figure (5): Verification phase (detect and extract forgery)**

## 5- Experimental Results

The proposed system is implemented using MATLAB (R2011a). First we applying the proposed system on set of image compute the coefficient performances like (PSNR and MSE) between reconstruction image in DB phase and reconstruction image in verification phase, to evaluate the performance of proposed system. The proposed system is applied on many type of forgery some of them are chosen in below figure (4) .



Orignal Image

Spalicing Image

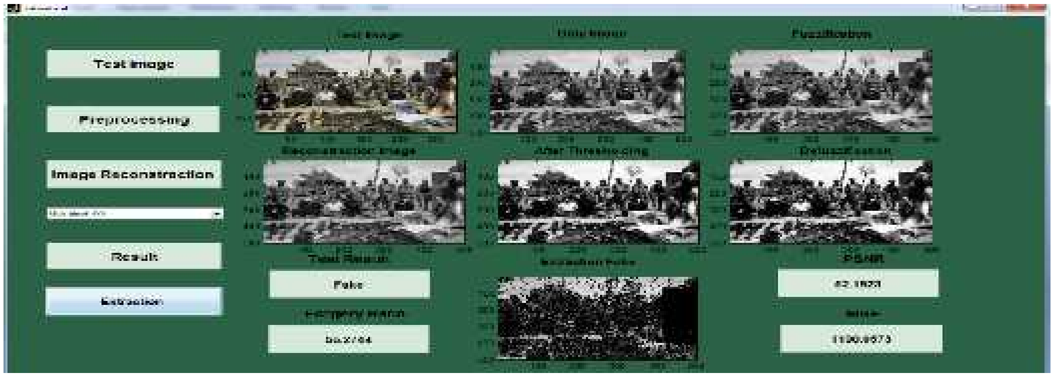
*Image Retouching*

*Geometrical transformation* Image

C*opy Move Attack* Image

**Figure (6) Set of images chosen**

Now will be apply the proposed system on the entire kind of faking image (Splicing Image, Image Retouching, Geometrical transformation, Copy Move attack, Double Compression for image, Noising image) and also applied on original image.



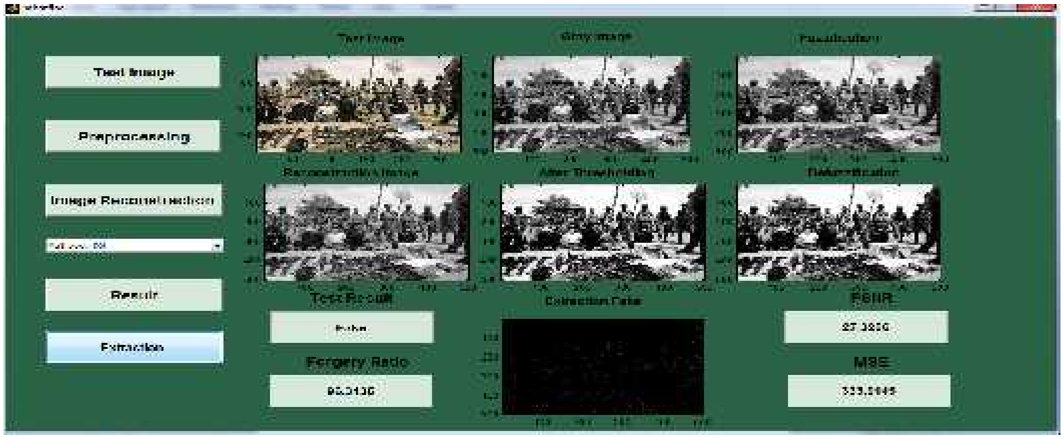
Test Result: Fake

Forgery Ratio: 56.2764

PSNR: 62.1523

MSE: 1100.8573

**Figure (7): Applying Proposed System for Splicing Image.**



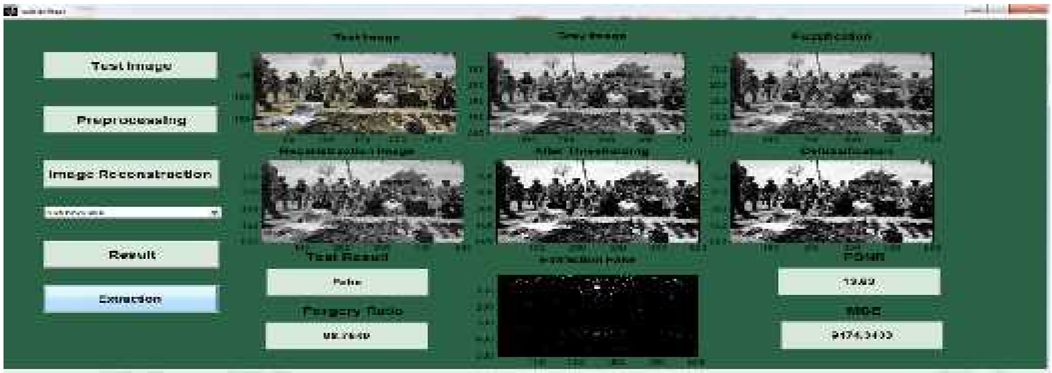
Test Result: Fake

Forgery Ratio: 96.3136

PSNR: 27.3830

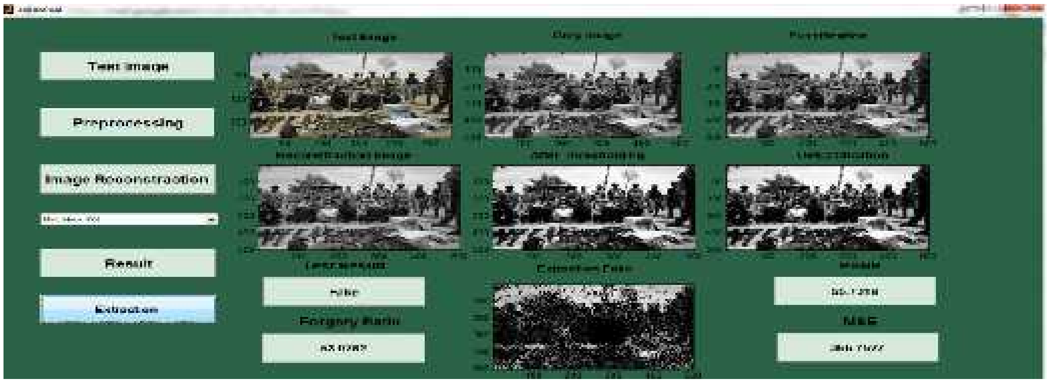
MSE: 333.5646

**Figure (8): Applying proposed system for Image Retouching.**



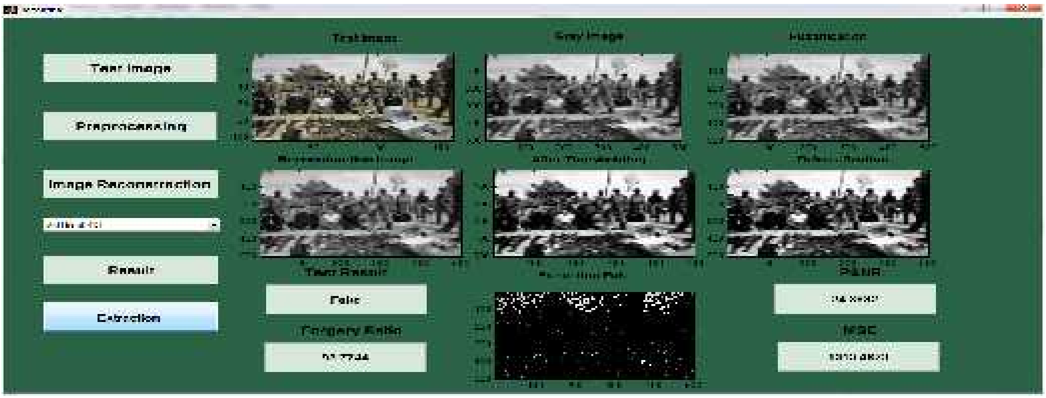
Test Result
False
Forgery Ratio
[illegible]
PSNR
19.89
MSE
9174.3433

**Figure (9):Applying proposed system for Geometrical Transformation**



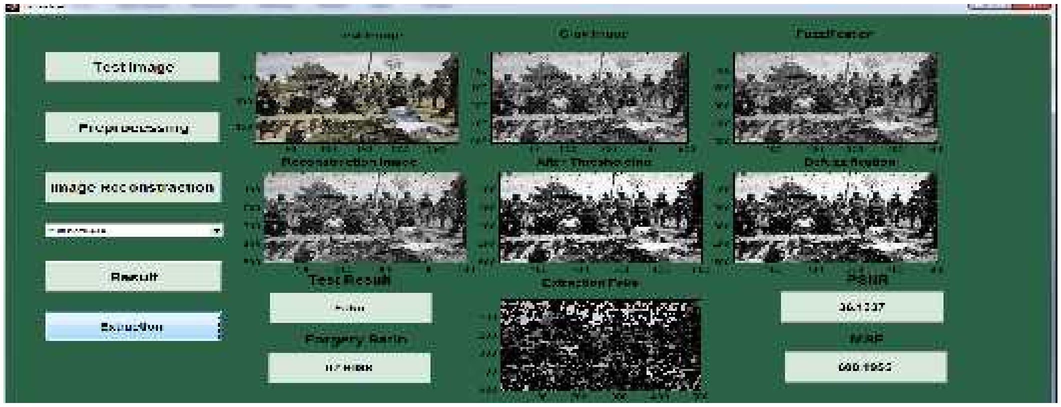
Test Result
False
Forgery Ratio
[illegible]
PSNR
[illegible]
MSE
[illegible]

**Figure (10):Applying proposed system for Copy Move Attack.**



Test Result
False
Forgery Ratio
[illegible]
PSNR
[illegible]
MSE
[illegible]

**Figure (11): Applying proposed system for Double JPEG compression.**



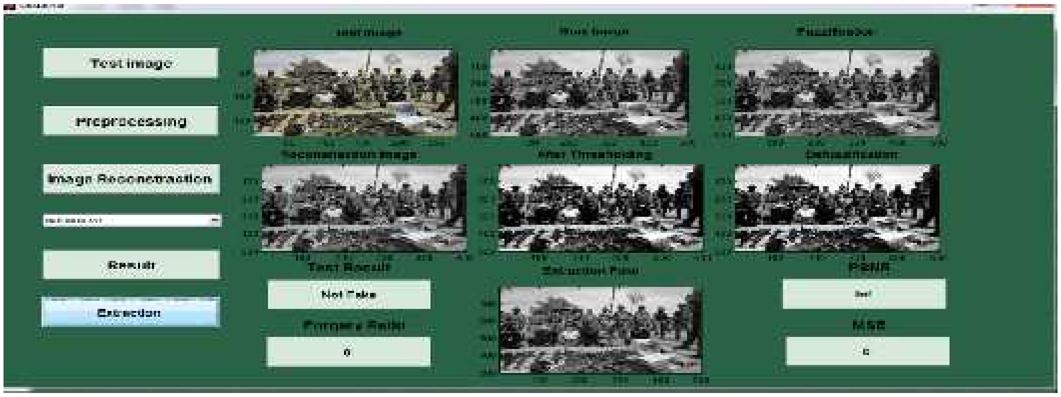
Test Result: Fake

Forgery Ratio: [illegible]

PSNR: 36.1337

MSE: 600.1955

**Figure (12): Applying Proposed System for Noising Image.**



Test Result: Not Fake

Forgery Ratio: 0

PSNR: Inf

MSE: 0

**Figure (13): Applying Proposed System for original Image**

Also will be take another samples of images in different types of forgery and will be apply on proposed system as depicted in Table (1),

Table (1): applying proposed system on sample image

| ***Type of image*** | | ***PNSR*** | ***MSE*** | **Forgery ratio** |
|---|---|---|---|---|
| Not Fake ( original ) | Image 1 | 0 | infinity | 0 |
| | Image 2 | 0 | infinity | 0 |
| | Image 3 | 0 | infinity | 0 |

| | | | | |
|---|---|---|---|---|
| Splicing image | *Image 1* | 0.0026911 | 99.0348 | 1.5869 |
| | *Image 2* | 0.033542 | 96.8657 | 9.4238 |
| | *Image 3* | 0.0091659 | 102.1848 | 5.3162 |
| Image retouching | *Image 1* | 1503.7426 | 24.9311 | 97.9248 |
| | *Image 2* | 759.2172 | 30.3254 | 99.9268 |
| | *Image 3* | 3164.1986 | 26.1355 | 93.3594 |
| Geometric transformation | *Image 1* | 4537.628 | 18.4231 | 98.1689 |
| | *Image 2* | 5046.5795 | 25.4131 | 96.582 |
| | *Image 3* | 2454.2694 | 26.3863 | 96.3623 |
| Copy move attack | *Image 1* | 43.2064 | 40.2234 | 30.6396 |
| | *Image 2* | 490.0725 | 56.988 | 40.8447 |
| | *Image 3* | 21.3842 | 68.0189 | 18.4326 |

Table (2) is the compression of the proposed method to Babak M. & Stanislav S.[8], Xunyu Pan , Xing Zhang& Siwei Lyu[9], U. M. Gokhale, Y.V.Joshi[12], Mohasin N., Prof. Yoginath R.& , Dnyaneshwar J[28], Ashima G. , Nisheeth S.,& ,S.K Vasistha3[11] , and Sonal S. & Preeti T.[13], according to Types of detection, Methods use, Enhancement image, and Detection accuracy. We find that only 5, and our proposed system can detect all types of forgery, and our proposed method enhance image quality, with 100% detection accuracy.

Table (2): Comparison of different methods

| | Types of detection | Methods use | Enhancement image | Detection Accuracy |
|---|---|---|---|---|
| [8] | Geometric transformations | Detecting Periodic properties in the image | No | % 95 - 100 |
| [9] | Splicing image | The clustering of image blocks with different noise variances. | No | high detection accuracy |
| [12] | identifies a tampered region when noise has been added<br>locally | Noise Estimation Using Filtering and SVD | No | High detection accuracy |
| [28] | Copy move attack and geometric transformation | SIFT algorithm to detect image forgery | No | High detection accuracy |
| [11] | All types of forgery | Gradient based image reconstruction | No | High detection accuracy |
| [13] | Copy move attack | Using DCT transformation | No | High detection accuracy |
| Our method | All types of forgery | Fuzzy gradient based image reconstruction. | Yes | 100 % |

## Conclusions

This paper proposed a new fuzzy gradient based image reconstruction, it is able to detect and extract all type of general forgery like Splicing, Image Retouching, Geometrical Transformation, and Copy Move Attack, also enable to detect other type of forgery like Double JPEG Compression and Noising Image . The proposed system compute the forgery ratio from image as a percentage also extract the forgery . The fuzzy process achieved the features for the system. Firstly, enhancement the image reconstruction, secondly, reduce the time consumption as much as possible. Using the min max normalization function instead of other known membership functions, which led to the success of the selection, it was for the first time of using normalization function as a membership function .New suggested method of computing forgery ratio as a percentage by using this suggested method is also enable to determine the test image fake or not. The practical implementation of the proposed system has shown the ability to detected paintings with 100 % of accuracy and the results are excellent .The drawback of the proposed system takes a large space in the memory storage in databases.

The possible future works take several directions including: Applying of the proposed system for video forgery detection. Applying the proposed system on different applications such as military, forensic, media, etc., applying Slant let transformation or other transformations to reduce size that is imply to reduce storage and in same time enhance image.

## References:

[1] R.E.J. Granty, T.S. Aditya, S.S. Madhu, ″Survey on passive methods of image tampering detection″, Proc. of the International Conference on Communication and Computational Intelligence, Page(s): 431 – 436, 2010.

[2] Amanpreet Kaur and RichaSharma,"Optimization of Copy-Move Forgery Detection Technique" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2`013 .

[3] *Osamah M. Al-Qershi and Khoo Bee Ee*,"Passive Detection of Copy-Move Forgery in Digital Images: State-of-the-art",Volume 231, Issues 1-3, Pages 284–295, September 10, 2013

[4] Dr. AbdulMonem S. Rahma and Dr. LumaFaikJalilKhalil,"A Proposed Method for Detecting Fake Art by Using B-Spline Curves", ,ENG. And Tech. journal,2011.

[5] Somayeh Sadeghi, Hamid A. Jalab, and SajjadDadkhah, ″Efficient Copy-Move Forgery Detection for Digital Images″, World Academy of Science, Engineering and Technology , pp. 755-758, 2012.

[6] A. C. Popescu and H. Farid, “Statistical Tools for Digital Forensics,” 6th Intl. Work. on Info. Hiding & LNCS, vol. 3200, pp. 128–147, May 2004.

[7] Hongmei Gou, AshwinSwaminathan, and Min Wu ,” Noise Features for image tampering detection and steganalysis ,” in IEEE International Conference on Image Processing, Sun Antono,Texas,2007.

[8] BabakMahdian and StanislavSaic, “Using noise inconsistencies for blind image forensics”, Image and Vision computing, vol.27, no10, pp.1497-1503, 2009.

[9] Xunyu Pan, Xing Zhang and SiweiLyu, “Exposing Image forgery with Blind Noise Estimation” in proceedings of 13th ACM workshop on Multimedia and security, pp. 15-20, September 29-30, 2011,Buffalo, New York, USA.

[10] Xunyu Pan, Xing Zhang and SiweiLyu, “Exposing image splicing with inconsistent local noise variances.” in IEEE International Conference on Computation Photography (ICCP) , pp. 1-10, April 2012.

[11]Sonal Sharma and Preeti Tuli ," Design of Classifier for Detecting Image Tampering Using Gradient Based Image Reconstruction Technique", International Journal Of Computational Engineering Research (IJCER) ,Vol. 2 Issue.5,2012.

.[12] U. M. Gokhale, Y.V.Joshi,” Noise Estimation Using Filtering and SVD for Image Tampering Detection”, International Journal of Engineering Science and Innovative Technology (IJESIT), pp. 46-53, vol. 2, no. 1, 2013,

[13] Ashima Gupta1, Nisheeth Saxena2 ,and S.K Vasistha3,"Detecting Copy move Forgery Using DCT", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013 1 ISSN 2250-3153.

[14 ]Tarun Mahashwari, and AmitAsthana," Image Enhancement Using Fuzzy Technique", INTERNATIONAL JOURNAL OF RESEARCH REVIEW IN ENGINEERING SCIENCE & TECHNOLOGY( IJRREST), (ISSN 2278–6643), 2013.

[15]Nitin Kumar Kansal, MrsAnjuBala, “Fuzzytechniques for image enhancement,” Master of Engineering report, Thapar University, Patiala 147004. June 2010

[16] Jiawei Han, MichelineKamber, and Jian Pei,3d edition ,"DATA MINING CONCEPT AND TECHNIQUES" ,EISILIVER,2012.

[17] R. Fatta, D. Lischinski, M. Werman, “Gradient domain high dynamic range compression” ACM Transactions on Graphics 2002;21(3):249-256.

[18] P. P´erez ,M. Gangnet , A. Blake, “ Poisson image editing” ACM Transactions on Graphics 2003;22(3):313-318.

[19] R. Raskar, A. Ilie ,J.Yu, “ Image fusion for context enhancement and video surrealism”, In: Proceedings of Non-Photorealistic Anima-tion and Rendering ’04, France, 2004. p. 85-95.

[20]A. Agarwala , M. Dontcheva, M. Agrawala , S. Drucker, A.Colburn, B. Curless, D Salesin , M. Cohen M, “ Interactive digital photo-montage. ACM Transactions on Graphics” 2004;23(3):294-302.

[21] J. Sun, J. Jia, CK. Tang , HY Shum , “Poisson matting. ACM Transactions on Graphics” 2004;23(3):315-321.

[22]A. Agrawal , R. Raskar, SK. Nayar , Y. Li, “Removing flash artifacts using gradient analysis” ACM Transactions on Graphics 2005;24(3):828-835.

[23] Pravin Bhat1 Brian Curless1 Michael Cohen1,2 C. Lawrence Zitnick2, "Fourier Analysis of the 2D Screened Poisson Equation for Gradient Domain Problems", University of Washington ,Microsoft Research.

[24] Sonal Sharma, PreetiTuli , Design of Classifier for Detecting Image Tampering Using Gradient Based Image Reconstruction Technique, International Journal Of Computational Engineering Research (Ijceronline.Com) Vol. 2 Issue.5.

[25] W. Press, S. Teukolsky, W. Vetterling, B. Flannery “Numerical Recipes in C: The Art of Scientific Computing” Cambridge University Press; 1992.

[26] Muna Ghazi Abdul Sahib, "Authenticated Image Documents Using Secret Sharing Technique ", University of Technology,2013.

[27] E. A. Silva , K. Panetta and S.S. Agaian," Quantifying image Similarity using measure of enhancement by entropy" ,processing of SPIE, Mobile Multimedia/Image Processing for Military and Security Applications, vol. 6579, Paper #6579-32, April 2007.

[28]Mohasin N. Shaikh, Yoginath R. Kalshetty, Dnyaneshwar J. Ghanawajeer, "A SIFT FOR COPY-MOVE ATTACK DETECTION & TRANSFORMATION RECOVERY", International Journal of Advanced Engineering Research and Studies E-ISSN2249–8974

# طريقة لكشف واستخراج التزوير من الصور

أ.م.د.هناء محسن احمد * سبأ راكان سالم*

## المستخلص

نظرا لتوفير العديد من برامج تحرير الصور وادوات معالجتها ,اصبح من الممكن التغير بسهوله على المعلومات التي تحملها الصور دون ترك اي اثار واضحه عليها جراء العبث بها والتي ادت الي مشكله التحقق من الصور . ومما اثرت هذة المشاكل على امن الوسائط المتعدده في تطوير طرق الكشف عن التلاعب. الطب العدلي الرقمي هو الفرع الذي يتعامل مع التعرف identity التخويل authenticity للصور والذي يهدف الى كشف العبث في الصور الرقميه . النظام المقترح هو نظام تحقق لللوحات الفنية حيث يستخدم طريقة (non-blind passive image forensic)والتي تحققت باستخدام ، إعادة بناء الصورة على أساس التدرج الغامض، التي تهدف الى كشف واستخراج جميع انواع التزوير (الربط، اعادة لمس الصورة، التحويل الهندسي، هجوم نقل نسخة، وغيرها) وايضا القدره على حساب نسبة التزوير كنسبة مئوية، واظهر النتائج التجريبية أن النظام المقترح يحقق دقة 100٪ للكشف واستخلاص جميع انواع التزوير، مع القدرة على تحسين الصورة.

*الجامعة التكنولوجية