A Method For Detect Forgery From Images

Dr. Hanaa Mohsin Ahmed
Computer Science Department,University of Technology /Baghdad
Email:salmanhanna2007@yahoo.com
Sabaa Rakan Salim
Computer Science Department, University of Technology /Baghdad
Email: sabaaalhamdany@gmail.com

Revised on: 1/9/2014 & Accepted on: 4/12/2015

ABSTRACT

Due to availability of many image editing and processing tools, it is possible to easily change the information represented by a digital paintings 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 paintings. 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 all type of forgery (Splicing, Image Retouching, Geometrical Transformation, Copy Move Attack, other type) and also able to compute forgery ratio as percentage.

This methodology has its application in a context where the source image is available. The experimental results show that the algorithm can effectively locate the tampered area in multi block size 4X4 of any type, and using fuzzy process is obtained a good result to reduce time consuming for solving image reconstruction and also enhancement reconstruction image .

Keywords: Image Tempering, Forgery Detection, Fuzzy process, Gradient, Poisson.

طريقة للكشف التزوير من الصور

الخلاصة:

نظرا لتوفير العديد من برامج تحرير الصور وادوات معالجتها ,اصبح من الممكن التغير بسهوله على المعلومات التي تحملها اللوحات دون ترك اي اثار واضحه عليها جراء العبث بها والتي ادت الي مشكله التحقق من الصور. ومما ادت هذة القضايا امن الوسائط المتعدده في تطوير طرق الكشف عن التلاعب. الطب العدلي الالكتروني هو الفرع الذي يتعامل مع الهوية والأصالة في الصور والذي يهدف الى كشف العبث في الصور الرقميه .

النظام المقترح هو نظام تحقيق للوحات الفنيه حيث يستخدم طريقة (non-blind passive image forensic) والتي تحققت باستخدام ، إعادة بناء الصورة على أساس التدرج غامض، التي تهدف الى كشف جميع انواع التزوير (التحويل الهندسي، اعادة لمس الصورة، الربط، هجوم نقل نسخة، وغيرها) وايضا القدره على حساب نسبة التزوير كنسبة مئوية، واظهر النتائج التجريبية أن النظام المقترح يحقق دقة 100٪ للكشف عن جميع انواع التزوير، مع القدرة على تحسين الصورة.

https://doi.org/10.30684/etj.33.2B.11
2412-0758/University of Technology-Iraq, Baghdad, Iraq

INTRODUCTION

According to the huge development in the field of imaging acquisition as well as the wide range of imaging modalities, museums started everywhere in the world digitizing their collections in order to archive the cultural heritage, and for preservation, documentation and dissemination purposes.

In the same time 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, enable using different type of forgery like [1] : Splicing " it is a method of tampering images by combining two sources to produce a new 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 . 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 branch that deals with the identity and authenticity of the images. It's has emerged as a new research field that aims to detect tampering in digital images .It has two principal approaches to detect, first active approach are classified into two categories. The first category is based on digital watermarking and second category digital signatures which conceals a watermark or signatures into the image at the capturing end and extracts it at the authentication end to examine whether the image has been tampered with Inserting the watermark either at the time of capturing the image using a specially equipped camera or later by an authorized person is the main drawback of watermarking [2][3][4]. In addition, the subsequent processing of the original image could degrade the image visual quality.

Second, Passive approach methods are classified into two categories, the first category is based on Blind passive approach [3], uses the digital media itself without any side information to ensure its integrity, because it uses statistical analysis without previously adding an authentication code into digital media, to detect the traces of tampering, blind methods use the image function and the fact that forgeries can bring into the image specific detectable changes natural scene image

The second category of methods is based on Non-blind passive [5], in this type investigators have such a data available, data may be available from alternative sources (for instance, earlier versions of a processed image that have been published elsewhere), or could have been stored purposely in advance (most likely the acquired image). Side information about the original scene may also be retrieved from other (trustworthy) images that exist of the same scene. Non–blind approaches in general have the advantage to mitigate some of the forensic investigator's uncertainty respectively and hence to make more informed decisions [6], [7].

Digital Image Forensics generally can be subdivided into three main branches as in [8]:

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

In this paper we presented fuzzy gradient based image reconstruction to implement for image to detect the forgery from image and also the compute the forgery ratio

from image as a percentage ,and the proposed system detection all kinds of tempering . The scope of this paper, a reliable forgery detection system for digital images will be useful in areas such as journalism, forensic investigation, criminal investigation, insurance processing, surveillance systems, intelligence services, and medical imaging and . The passive forgery detection is still an active topic of research and this research deals with devising methods for the same. .

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

Literature Review And Fundamental Used In Proposed System

A- 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 2009, another method capable of detecting image noise inconsistencies is proposed in [9] 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.[10] 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. [11] 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.[12] 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. [13] 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. [14], 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. The proposed method detects region duplication forgery by dividing the image into overlapping blocks and then we search for the matching region in the image.

Fundamental used in proposed system

We explain the fundamental used in verification system :

Fuzzy image processing

Generally speaking by using Fuzzy Set Theory, which 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 defuzzification, [15],shown Figure (1).

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 [16], [15] by:

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

Where

$:\mu_{mn} = \frac{d-mn}{mn-mx}$

$d = dobel(image), mx =$ $\max(\max(image))$,$mn\min(\min(image))$

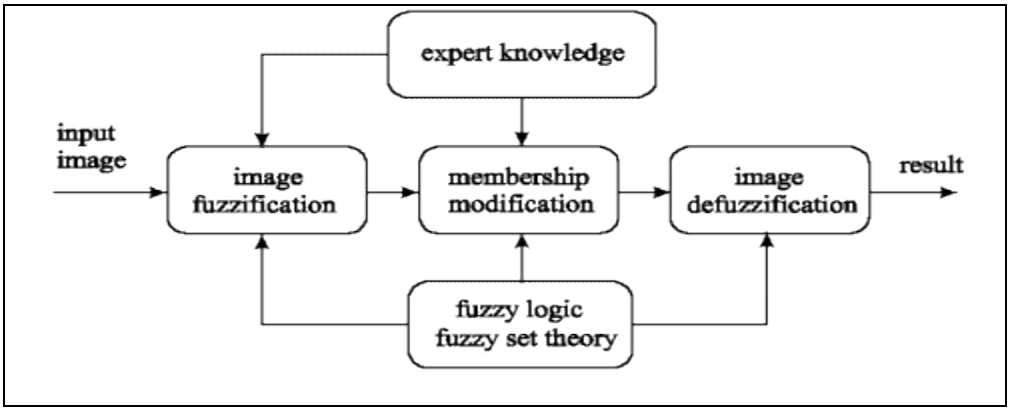

Figure (1): The general structure of fuzzy image processing [17].

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 type of normalization: min-max normalization, z_ score normalize, normalization by decimal scaling.

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

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

Where:

I Original data

Max	Maximum value in original data
Min	Minimum value in original data
New max	Maximum value of new range of data
New min	Minimum value of new range of data
NI	Normalized data

Also to return normalized data to the old values using min max de-Normalization, the formula of Min-max normalization are [17]:

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

Where:

Ir	Normalized data
New max	Maximum value of new range before normalize
New min	Minimum value of ne range before normalize
XMax	Maximum value in normalized data
XMin	Minimum value in normalized data
NI	De-normalized data.

Poisson Image Reconstruction Using Image Gradients

Image reconstruction from gradient fields is a very active research area gradient-based image processing techniques and the Poisson equation solving techniques have been addressed in several related areas such as high dynamic range compression [18], Poisson image editing [19], image fusion for context enhancement [20], interactive photomontage [21], Poisson image matting [22] and photography artifacts removal [23]. The gradient-based image processing techniques and the Poisson equation solving techniques have been addressed in several related areas. In our approach, the image can be reconstructed from its gradients by solving a Poisson equation and hence used for authenticity verification .Where the image is converted into gradient map and then are re-construction the image by takingthe 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.

In 2D, a modified gradient vector field

$$G' = [G'x, G'y] \quad \ldots(4)$$

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 *f*' denote the image reconstructed from G', [24],[12]

$$\| \nabla f' - G \| \quad \ldots(5)$$

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:

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

By introducing a Laplacian and a divergence operator, I' can be obtained by solving the Poisson differential equation with fixed boundary condition [12].

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

Since both the Laplacian and *div* are linear operators, approximating those using standard finite differences yields a large system of linear equations. The full multigrid

method [25] is used to solve the Laplacian equation with Gaussian-Seidel smoothing iterations. For solving the poisson equation more efficiently, an alternative is to use a rapid poisson solver, which uses a sine transform based on the method [26] to invert the laplacian operator. Therefore, the rapid Poisson solver is employed in our implementation. The image is zero-padded on all sides to reconstruct the image.

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:

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

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

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

Absolute Difference

In the present work our approach is to find the absolute difference between the original and the reconstructed image. Subtraction gives the difference between the two images, but the result may have a negative sign and can be lost. The function that finds how different the two images are regardless of the arithmetic sign is the absolute difference:

$$\mathrm{N(x,y)} = \left|O_1(\mathrm{x,y}) - O_2(\mathrm{x,y})\right| \quad \ldots (10)$$

Where

$O_1(x,y)$ and $O_2(x,y)$ are pixels in the original images, $|x|$is the absolute difference operator, and N(x, y) is the resultant new pixel. The absolute difference operator returns +x whether the argument is –x or +x.

6-Forgery Ratio

Is a new method to compute forgery ratio intest image by using the bellow equation

$$\text{Forgery ratio} = \left(\frac{\mathrm{D}}{\mathrm{K}}\right) * 100 \quad \ldots (11)$$

Where D:Number of block difference

K: Total number of block

PROPSED SYSTEM

Idea for proposed system

The concept of proposed system is using fuzzy gradient based image reconstruction technique as a system for detect forgery from painting as well enable to compute the forgery ratio as a percentage.

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.

In the second phase is named: Verification phase, enter test image to be determine whether a digital image (paintings) is original or fake where enter the same steps in first phase except step saving where calculated reconstructed image for test image and absolute difference of test image. Finally determine fake or not by dividing the absolute differences 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 is not fake vice versa, also in multi block technique compute forgery ratio in test 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 implemented using MATLAB (R2011a). Figure (3) illustrates the framework of the proposed system.
We show the algorithm in Schematic diagram below:

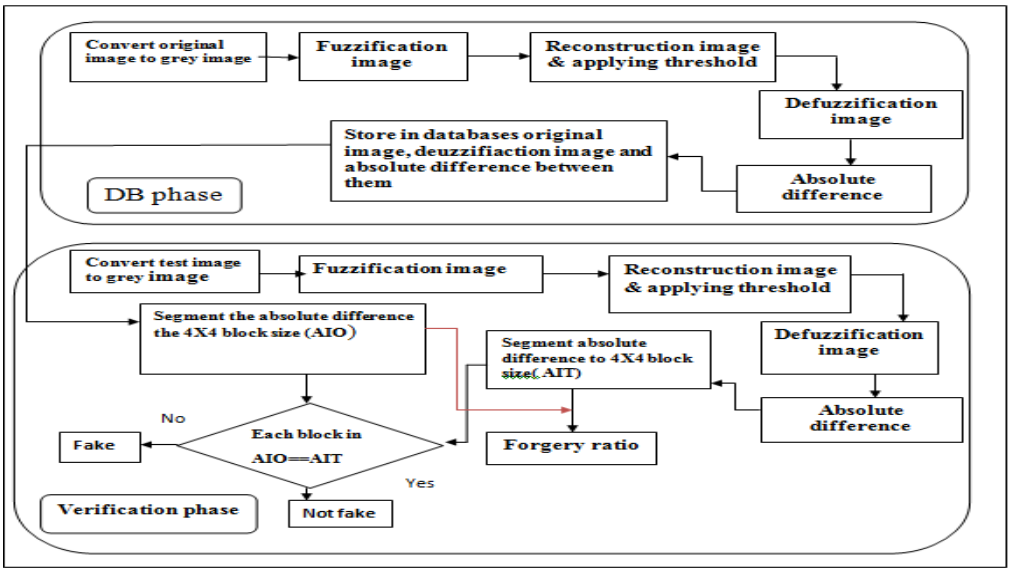

Figure (2): Schematic diagram for DB-phase and Verification Phase

Algorithm Used:

In this section we explain the algorithm for detect forgery in the following phases and step:

Phase one: DB create.
Input :original image
Output : reconstruction image ,absolute difference
process
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.

Phase two: Verification phase
Input :test image
Output : result (fake or not fake),forgery ratio
process
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

Results and Discussion

First, we must make it clear why chose the size of block 4X4. We take a sample of the images and applied them of different size blocks and compute the average for sample image, divided absolute difference into multi block size block 2X2, 4X4, 8X8, 16X16 32X32 and 64 X64 compute the PSNR and MSE to seen which size butter with high performances seen the 4X4 is butter size block because is obtained high quality measurement and less time consumption as much as possible in this aspect.

Table (1): multi block

Type of block	Average MSE	Average PSNR	Average Time Consumption
2X2	799.6356	35.8091	6.4666 Sec
4X4	799.7523	33.9043	1.7704 Sec.
8X8	800.2055	32.5479	0.4426 Sec.
16X16	801.8240	31.2038	0.1389 Sec.
32X32	808.6999	29.5274	0.0444 Sec.
64X64	833.9332	27.0576	0.0216 Sec.

and then explain as depicted in Table (2), why using fuzzy process with reconstruction image in proposed system take a sample of images also compute average for time consumption and seen the time consumption with fuzzy less than time without fuzzy.

Table (2): comparative fuzzy with without fuzzy

Type	Average time of numerical Poisson solution
With fuzzification	0.6664 Sec.
Without fuzzification	0.7401 Sec.

The proposed system is applied on many type of forgery some of them are chosen. In below figure (3)

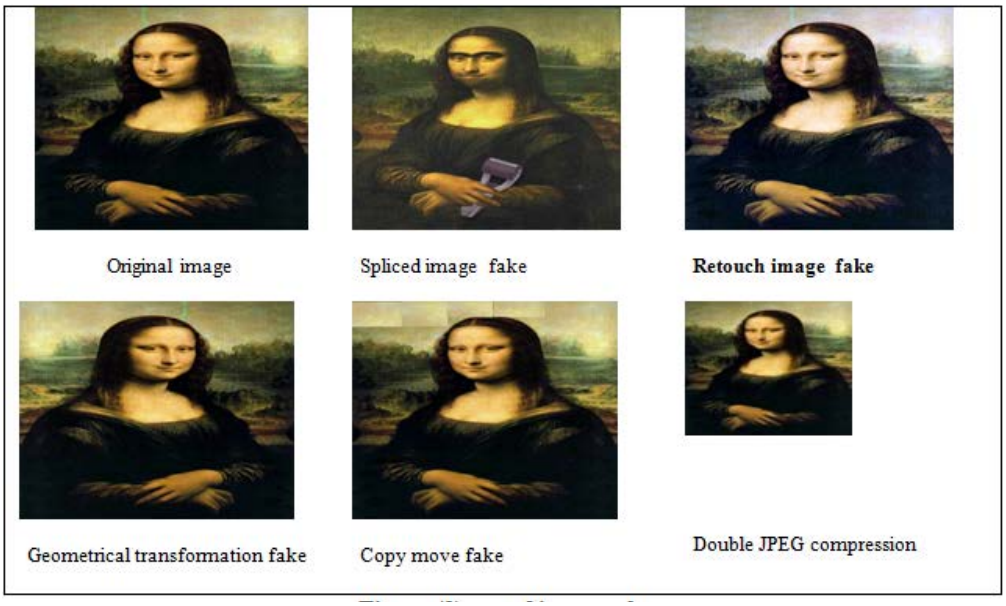

Figure (3) set of images chosen

Now will be apply the proposed system on all the 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 .

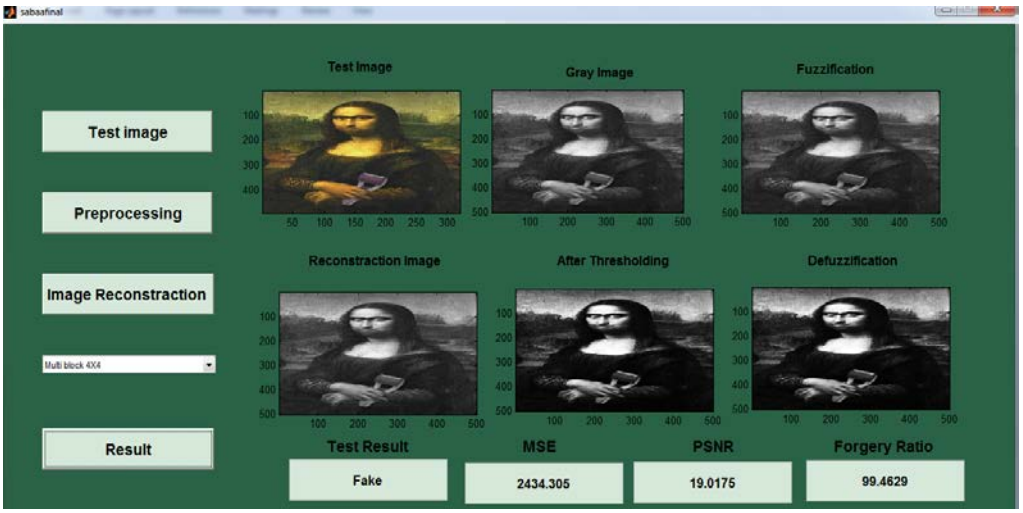

Figure (4): Applying Proposed System for Splicing Image.

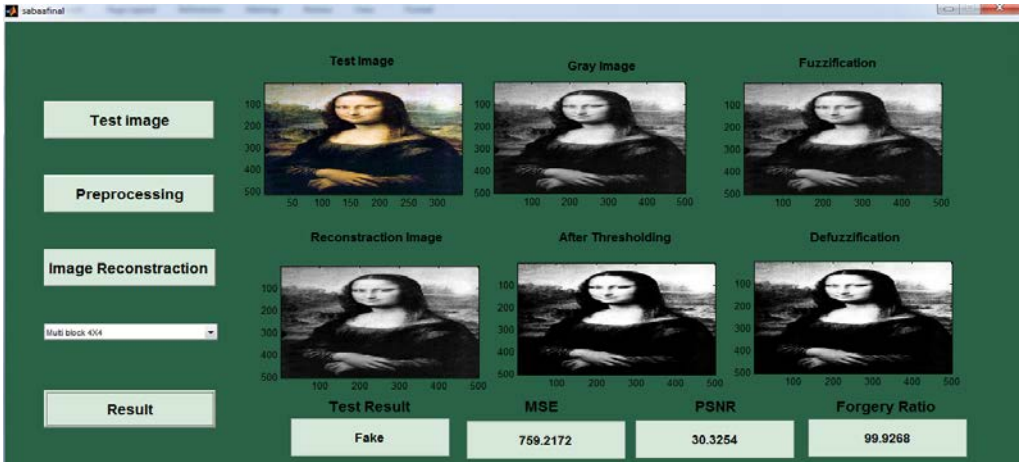

Figure (5): Applying proposed system for Image Retouching.

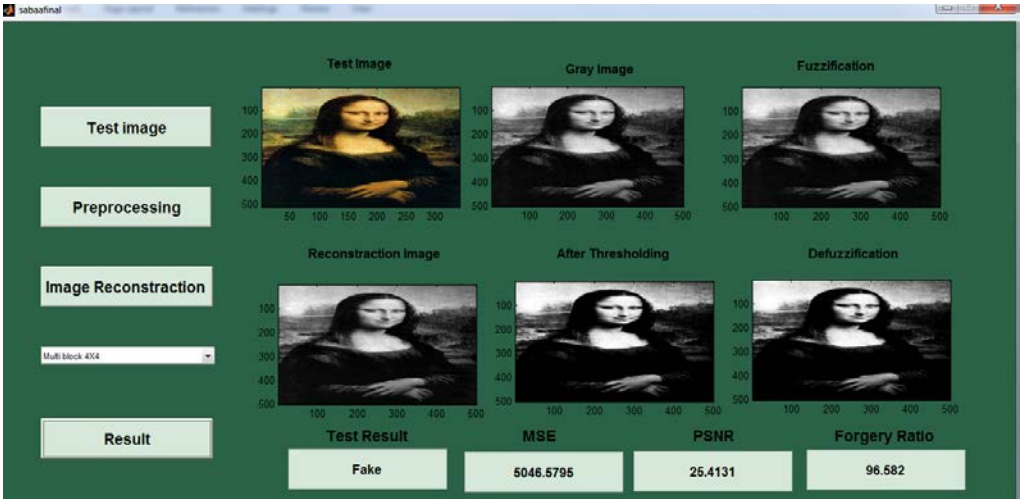

Figure (6):Applying proposed system for Geometrical Transformation

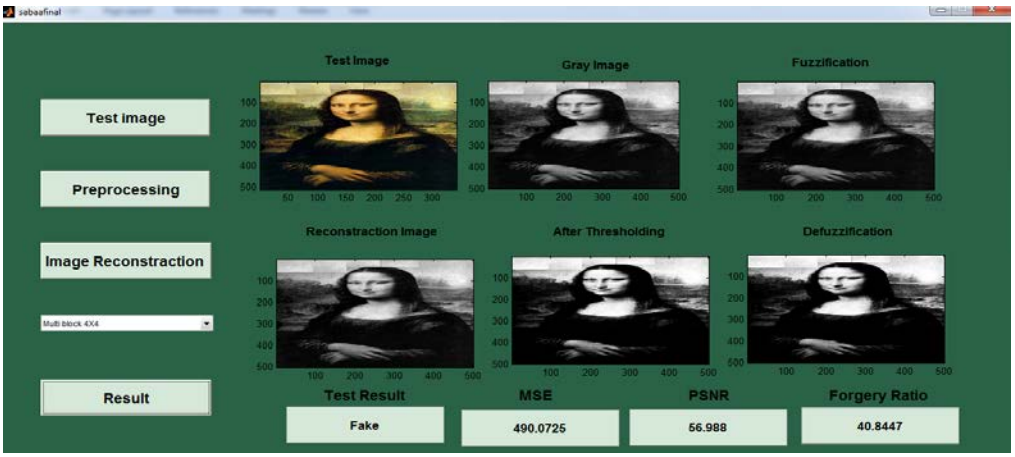

Figure (7):Applying proposed system for Copy Move Attack.

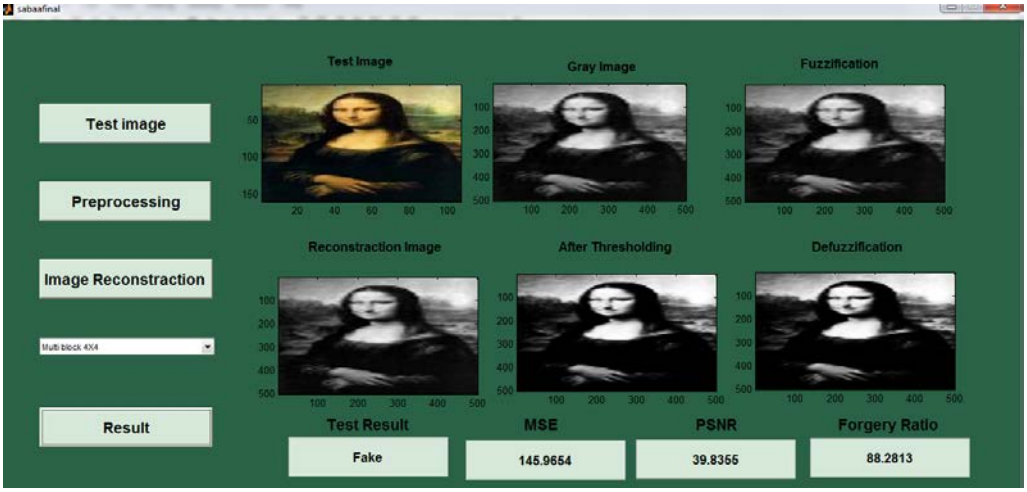

Figure (8): Applying proposed system for Double JPEG compression.

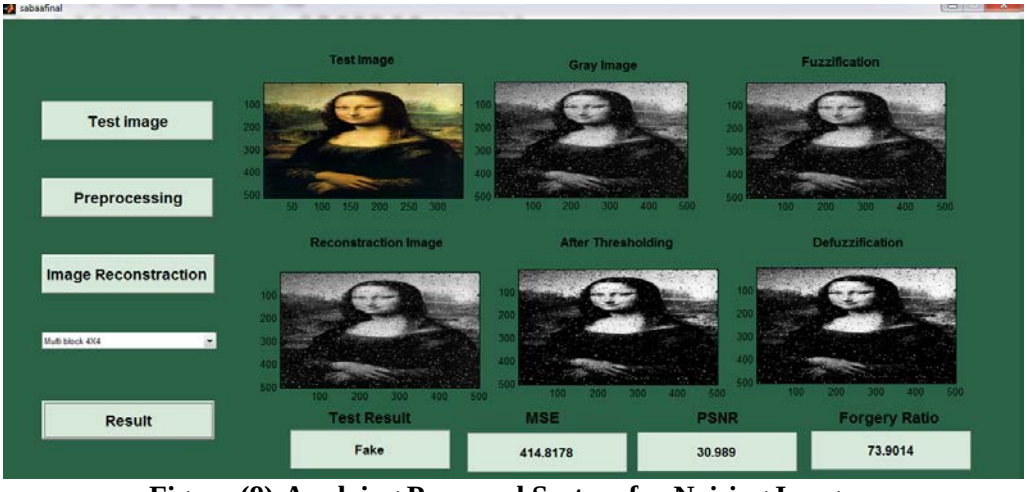

Figure (9):Applying Proposed System for Noising Image.

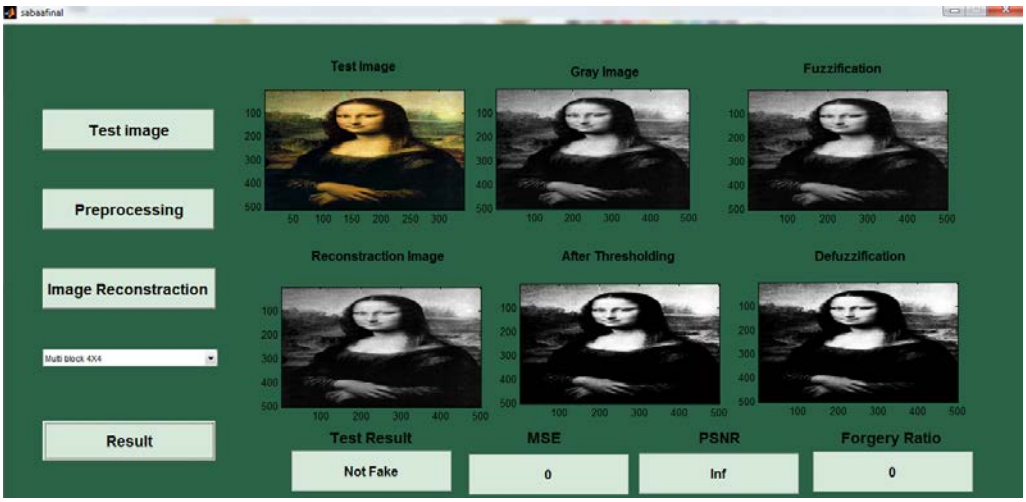

Figure (10): Applying Proposed System for original Image

Table (3) is the compression of the prosed method to Babak M. & Stanislav S.[18], Xunyu Pan , Xing Zhang& Siwei Lyu[19], U. M. Gokhale, Y.V.Joshi[20], Mohasin N., Prof. Yoginath R.& , Dnyaneshwar J[21], Ashima G. , Nisheeth S.,& ,S.K Vasistha[15] , and Sonal S. & Preeti T.[22], according to Types of detection, methods use, Enhancement image, and Detection accuracy. We find that only [14], and our proposed system can detect all types of forgery, and our proposed method enhance image quality, with 100% detection accuracy.

Table (3): Comparison of different methods

	Types of detection	**Methods used**	**Enhancement image**	**Detection Accuracy**
[27]	Geometric transformations	Detecting Periodic properties in the image	No	% 95 - 100
[12]	Splicing image	The clustering of image blocks with different noise variances.	No	high detection accuracy
[15]	identifies a tampered region when noise has been added 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
[14]	All types of forgery	Gradient based image reconstruction	No	High detection accuracy
[16]	Copy move attack	Using DCT transformation	No	High detection accuracy
Our method	All types of forgery	Fuzzy gradient based image reconstruction.	Yes	100 %

CONCLUSION

This paper proposed a new fuzzy gradient based image reconstruction, its enable to detect forgery from all type of images forgery and compute the forgery ratio from images as a percentage .

The fuzzy process achieved the features for the system. Firstly, their works on enhancement the image reconstruction, secondly, reduce the time consumption as much as possible.

This paper proposed a new fuzzy gradient based image reconstruction, its enable to detect all type of general forgery in 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 and compute the forgery ratio from image as a percentage .

The fuzzy process achieved the features for the system. Firstly, their works on 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 disadvantage of the proposed system takes a large space in the memory storage in databases.

REFERENCE

[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] D. Kundur and D. Hatzinakos, “Digital Watermarking for Telltale Tamper Proofing and Authentication,” in *Proceedings of the IEEE*, 1999, vol. 87, pp. 1167–1180

[3] 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 2013 .

[4] 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.

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

[6] Matthias Kirchner, "Notes on Digital Image Forensics and Counter-Forensics", September 2011 / October 2012.p 13-16.

[7] Kalpana M. and M.M. Bartere ,"Methodology for Evidence Reconstruction in Digital Image Forensics", Computer Engineering and Intelligent Systems Vol.4, No.13, 2013.

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

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

[10] 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.

[11] 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.

[12] 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.

[13] 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,

[14] 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.

[15] Tarun Mahashwari and Amit Asthana," Image Enhancement Using Fuzzy Technique", International Journal Of Research Review In Engineering Science & Technology (IJRREST), ISSN 2278–6643, 2013.

[16] Nitin Kumar Kansal, Mrs Anju Bala, "Fuzzy techniques for image enhancement," Master of Engineering report, Thapar University, Patiala, 147004. June 2010.

[17] Jiawei Han, Micheline Kamber, and Jian Pei," Data Mining Concept And Techniques", Third Edition , ElSILIVER , 2012.

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

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

[20] 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.

[21] 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.

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

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

[24] 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.

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

[26] R. Raskar, K. Tan, R. Feris , J. Yu, M. Turk “Non-photorealistic camera: depth edge detection and stylized rendering using multi-flash imaging” ACM Transactions on Graphics 2004;23(3):679-688.

[27] Babak Mahdian and Stanislav Saic, "Detection and Description of Geometrically Transformed Digital Images", Media Forensics and Security. Edited by Delp, Edward J., III; Dittmann, Jana; Memon, Nasir D.; Wong, Ping Wah. Proceedings of the SPIE, Volume 7254 (2009), pp. 72540J-72540J-9 (2009).

[28] Mohasin N. Shaikh, Yoginath R. Kalshetty, and Dnyaneshwar J. Ghanawajeer, "A SIFT FOR COPY-MOVE ATTACK DETECTION & TRANSFORMATION RECOVERY " ;International Journal of Advanced Engineering Research and Studies E-ISSN2249–8974,2013 .