ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
April 2016,
Vol. 9, No. (1):
Pgs. 12-16

Neuro-Fuzzy based First Responder for Image forgery Identification

GAURAV KUMAR SINGH GAHARWAR[1, 2], V. V. NATH[3] and RAINA GAHARWAR[4]

[1]Research and Development, Raksha Shakti University, Ahmedabad, India.
[2]School of Business and Law, Navrachana University, Vadodara, India.
[3]Institute of Management, Nirma University, Ahmedabad, India.
[4]G. H. Patel Department of COMPUTER SCIENCE and Technology,
Sardar Patel University, Vallabh Vidyanagar, India.

http://dx.doi.org/10.13005/ojcst/901.03

(Received: February 11, 2016; Accepted: March 14, 2016)

ABSTRACT

Image forgery is always been sought after field of digital forensics, as it becomes very convenient now to edit/forge any image with many desktop based and online tools available. Also, to prove authenticity of any image in the court of law, there is a need of algorithm which can used to check forgery of any image, irrespective of its forgery type. Proposed model in the paper aims to provide neuro-fuzzy based algorithm which utilizes capabilities of best algorithms for each type and provides accurate result about the forgery in the image. It also provides analysis about type of forgery in the image along with the area forgered in the image.

Keywords: Image forgery, Copy-move forgery, Image splicing, Image retouching, Lightning condition, Neuro-fuzzy approach, ANN**.**

INTRODUCTION

Image forgery

Image forgery is to manipulate the content of an image in such a way that either it hide an important part of the image or represents wrong information. Image forgery is very common of digital crimes carried out. The most familiar targets of these forgeries are photographs, legal or administrative documents and financial documents line checks. Nowadays it becomes effortless to manipulate any digital image with readily available software like Adobe Photoshop. Digital image forgery can be identified into two categories viz. cloning in which an area of the image is pasted on the same image, and composition in which an area of the image contain area from some other image.

Fig 1 show how and image can be easily forged where Wong Su En from DAP-China forged a photograph receiving knighthood from Queen Elizabeth-II.

Different types of Image forgeries

Image forgeries can be categorized into copy-move forgery, image splicing, image retouching, and lightning condition.

"In copy-move forgery, the area copied belongs to the same image, the dynamic range and color remains will be same as the other part of image. Copy-move forgery is usually done to either hide some part of the image of to show some part of the image multiple times."[1] This is most common type of image forgeries.

"Image splicing forgery involves composition or merging of two or more images changing the original image significantly to produce a forged image."[1] Whenever images with similar looking background are merge, then becomes extremely difficult to find forgered image.

"In Image Retouching, the images are less modified. It just enhances some features of the image. There are several subtypes of digital image retouching, mainly technical retouching and creative retouching."[2]

"Many times the image splicing is done with such a precision that it is visually impossible to identify different lightning conditions in the combined image. To the extent that the direction of the light source can be estimated for different objects/people in an image, inconsistencies in the lighting direction can be used as evidence of digital tampering."[3]

Different Image forgery identification techniques

There are different methods suggested by different researchers for solving different types of forgeries, viz copy-move forgery, image splicing, image retouching, and lightning condition.

Copy-move forgery identification methods can be categorized into either block based method or keypoint based method[4] Block based methods gives accurate result for identifying image forgery in any jpg image but also takes lot more time then keypoint based methods[5] And forgery covered under geometric transformations like rotation and scaling are better suited for the keypoint based methods while methods like exhaustive block search method can find almost any type of copy-move forgery[4]

Image splicing forgery detection algorithm divided into two categories: detection algorithm based on authenticity of the local area and detection algorithm based on source inconsistency[4] There are many algorithms proposed by different researchers for exploiting inconsistency local characteristic of an forgered image. It is extremely difficult for any image forger to hide these inconsistencies. Also, image source in always ideal, it has its own inconsistencies, these inconsistencies are then pass on to all the images taken from that source. Consistency in the inconsistencies of source is used for identifying image splicing forgery.

Image retouching algorithms work on analyzing image histogram to identity contrast enhancement. Irregularities from the histogram can

Fig. 1: Image source: http://www.nkkhoo.com/2010/07/10/ex-dap-member-forged-knight-award/

be considered as the evidence of image retouching forgery. With histogram analysis algorithm can also localize the forgery area[4] Image retouching is frequently done highlight certain part of an image, e.g. one might modify the color of faces in the photograph.

Lightning inconsistency is one of the obvious techniques to identify image forgery. Many algorithms use 2-D surface normals, and lateral chromatic aberration. Many algorithms use Peak/ Gap bin detection method for identifying lighting inconsistencies[4] Whenever there is huge mismatch in the contrast of different parts of an image, this type of forgery can be a great possibility.

Limitations with existing techniques

There are many different types of image forgeries and many different algorithms are given by researchers to detect forgery. In single forgery type also many algorithms are there working on completely different principles. The result is also inconsistent and different if different algorithms are applied on same forgered image. There is no single method/algorithm for image forgery identification.

Due to which there is always a need of expert to identify first type of forgery and then apply appropriate algorithm to check forgery. As it is subjective assessment by expert about the type of forgery, this becomes a grey area in image forgery identification. There is a need of an algorithm which can predict any type of forgery in an image.

Proposed model

The proposed system will utilize advantages of different algorithms. The forged image is sent to different algorithms which then analyzed result is then given in the form of whether the image is forgered according to that algorithm of not. The fuzzification of this true-false values are done before inputting to input layer of the Artificial Neural Network (ANN). Inside the ANN different weights are assign to different connections and accordingly knowledge has been generated at the output layer of ANN. Lastly defuzzification of the output knowledge is been done to provide yes-no answer to the user.

Inherent property of any computer system is its speed and accuracy and with the better hardware coming to market every month, the speed will be ever increasing in future. With better speed the expert system will leverage the benefits of many algorithms and provide user accurate result which can withstand in the court of the law. Also, model utilizes capabilities of best of the forgery detection algorithms with the help of ANN. If ANN is trained correctly then most of the forgeries can be identified effortlessly.

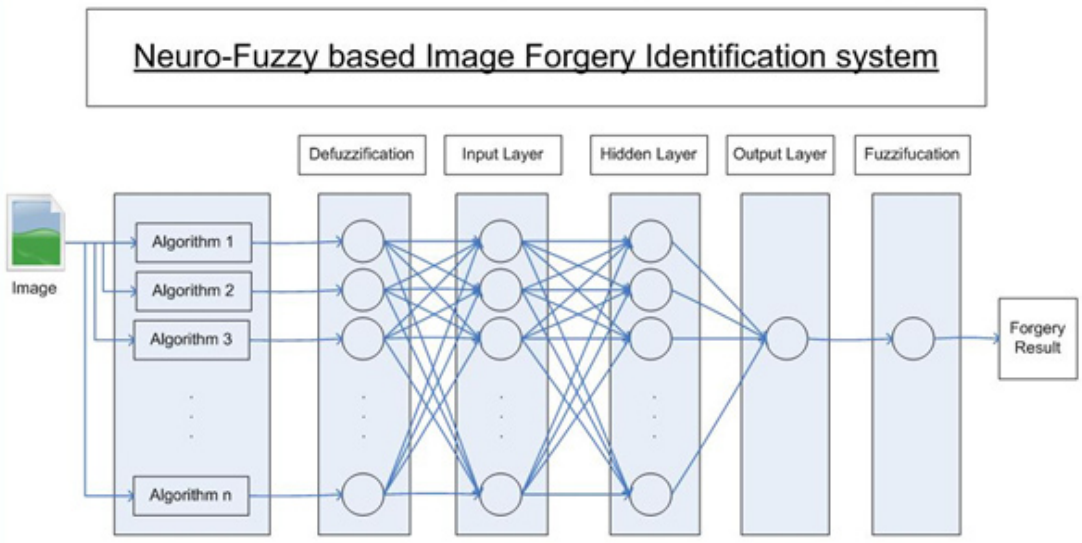

Fig. 2:

Neuro-fuzzy approach

Learning capabilities of neural networks is great for numerical data but real world, which is not always numeric data, deals largely with fuzzy data. On the other hand fuzzy logic has a good interpretation capability. Neuro-fuzzy is a hybrid approach to leverage the capabilities of both neural networks and fuzzy logic. The output of one system can be supplied as the input of the other system. The cooperative neuro-fuzzy model corresponds to the case that one system is used to adapt the parameters of the other system[6]. Neuro-fuzzy model takes the form of either a fuzzy neural network or a neuro-fuzzy system. A hybrid neuro-fuzzy system does not use multiplication, addition, or the sigmoidal function, but uses fuzzy logic operations such as t-norm and t-conorm.

A fuzzy neural network is a neural network equipped with the capability of handling fuzzy information, where the input signals, activation functions, weights, and/or the operators are based on the fuzzy set theory[7]. A neuro-fuzzy system is a fuzzy system, whose parameters are learned by a learning algorithm. It has a neural network architecture constructed from fuzzy reasoning, and can always be interpreted as a system of fuzzy rules. Learning is used to adaptively adjust the rules in the rule base, and to produce or optimize the membership functions of a fuzzy system. Structured knowledge is codified as fuzzy rules. Expert knowledge can increase learning speed and estimation accuracy. Both fuzzy neural networks and neuro-fuzzy systems can be treated as neural networks, where the units employ the t-norm or t-conorm operator instead of an activation function. The hidden layers represent fuzzy rules.

Advantages of proposed model

The proposed system will be developed in the domain of digital forensics and serve as first responder in the case of identifying forgery or tempering in the image. Data collected during this process is used to train the neurons for improving the process for successive executions.

The proposed system will not eliminate than need of expert, but it will assist an expert by automating first responder processes so expert can focus on more important tasks where his involvement is highly required. Human resource is most critical resource in any organization for performing certain task, in digital forensics the situation is more critical due to less availability of experts. So, it becomes more important not to use these experts for routine task like first responder process and this routine task can be performed by intelligent computerized systems like expert system.

CONCLUSION

The proposed expert system will combine the power different image forgery algorithms for verifying authenticity of the image on the hand. The simple to use tool will facilitate novice to find out forgery from the image in the absence of forensic expert. The simple to use system will not only provide result in simpler format but also due the processing with multiple algorithms it will provide more accurate analysis of any image.

REFERENCES

1. G. K. S. Gaharwar, V. V. Nath, and R. D. Gaharwar, "comprehensive study of different types image forgeries," in *International conference on Recent Advances in Engineering Science and Management*, New Delhi, 2015, pp. 345-350.
2. P. Sabeena Burvin and J. Monica Esther, "Analysis of Digital Image Splicing Detection," *IOSR Journal of Computer Engineering*, **16**(2); 10-13 (2014).
3. Micah K. Johnson and Hany Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," *ACM Multimedia and Security Workshop*, (2005).
4. Gauravkumarsingh Gaharwar, V. V. Nath, and Raina Gaharwar, "Comprehensive Study of Contemporary Image forgery Identification Techniques," *International Journal of Computer Science and Information Technology*, **6**(6); 5413-5416 (2015).

5. V S Kulkarni and Y V Chavan, "Comparison of methods for detection of Copy-Move Forgery in Digital Images," *Spvryan's International Journal of Engineering Sciences & Technology*, **1**(1): (2014).
6. Stephan I Gallant, "Connectionist expert systems," *Communications of the ACM*, **31**(2); 152-159 (1988).
7. W. Pedrycz and A F Rocha, "Fuzzy-Set Based Models of Neurons and Knowledge-Based Networks.," *IEEE Trans. Fuzzy Systems*, **1**(4): 254-266 (1993).