Multi-Scale Fusion for Improved Localization of Malicious Tampering in Digital Images

[1]Prof. Akshay Agrawal, [2]Wrujuta P. Dhavale, [3]Jyoti V. Khandagale, [4]Sampada K.Kulkarni

[1]Asst. Professor, [2,3,4]UG Student, [1,2,3,4]Computer Engg. Dept. Shivajirao S.Jondhle College of Engineering & Technology, Asangaon, Maharshatra, India.

[2]wrujutad@gmail.com, [3]jvkhandagale@gmail.com, [4]sampda.kul05@gmail.com

Abstract--A sliding window-based analysis is most influencing mechanism for tampering localization in passive image authentication. Using existing forensic detectors, primarily designed for a full-frame analysis, to obtain the detection scores for each image region. The main problem with a window based analysis is its impractically low localization resolution stemming from the need to use large analysis windows. This project addresses to investigate a multi-scale analysis approach that joins multiple tampering maps, resulting from the analysis with different windows, to obtain a single and more reliable tampering map with better localization resolution. Here three different techniques for multi-scale fusion are used, and their feasibility is verified against various reference strategies. Considering a popular tampering scenario with mode-based first digit features to distinguish between singly and doubly compressed regions. The results clearly indicate that the fusion strategies can successfully combine the benefits of small-scale and large-scale analyses and improve the tampering localization performance.

Keywords — Digital image forensics, tampering localization, result fusion, multi-scale analysis, first-digit-features, energy minimization, Markov random fields.

I. INTRODUCTION

The increasing easy editing digital photographs has spread out an urgent need for reliable authentication mechanisms, capable of precise localization of potential malicious fraud. Though proactive image protection schemes will deliver precise identification of the tampered regions and even restore their original appearance with very high-quality [6]-[7], they can only be exploited in an exceedingly strictly controlled environment, since they use a carefully designed digital watermark that needs to be available as side information.

The rapidly developing field of digital image forensics aims to deliver passive authentication mechanisms that analyze intrinsic fingerprints introduced on various stages of the image acquisition pipeline [1]-[8]. As a result, such techniques can be applied to existing, non-watermarked pictures. However, since they are engineered on the foundations of machine learning and statistical signal analysis, reliable detection of forensic features provides precise tampering localization a challenging problem.

The analysis is performed on the example case of a popular tampering scenario involving splicing of JPEG pictures that produces regions with totally different compression history. The forensic features of choice are the mode-based first digit features (MBFDF) [11]. While recent studies have already demonstrated that MBFDF can be used successfully for sliding window-based localization, a much more detailed analysis is conducted with densely sampled compression levels and emphasis on multi-scale localization.

II. LITERATURE SURVEY

Sequential floating forward search approach selects the most descriptive features which are then used in a linear regression classifier for discriminating authentic from manipulated images. In both cases, the statistical model is used to find out everything from basic image manipulations like resizing and filtering to discriminating photographic from computer-generated images and detecting hidden messages. And To achieve the aim of localization, the SVM has been trained by means of image portions whose size was compliant with that of search window used for forgery localization[3].

III. AIMS AND OBJECTIVES

Though proactive image protection schemes can deliver precise identification of the tampered regions and even restore their original appearance with very high-quality, they can only be exploited in a strictly controlled environment, since they use a carefully designed digital watermark that needs to be available as side information. The increasing easy editing digital photographs has spread

out an urgent need for reliable authentication mechanisms, capable of precise localization of potential malicious fraud.

The above attempts result in tampering of images. Image tampering has grown widely and these images are being used for malicious reasons. Most of existing localization methods are essentially extensions of conventional full-frame detectors operating on a sliding window basis.

The main aim is to smooth the tampered image given as an input by using approaches like Energy Minimization, Top-down and bottom-up techniques and obtain the binary mask for the original image.

1. To select and image as an input for recognizing the tampered region.
2. Using the L0 smoothing approach and converting the image into a 64*64 block for further processing.
3. Energy minimization or the Bayesian approach the tampered region is detected.
4. Making cluster using K-means by implementing the Bottom-up and Top-down approaches.
5. Making cluster using K-means by implementing the Bottom-up and Top-down approaches.
6.To classify the tampered region using SVM technique.
7.To obtain the binary mask for the original image.

Table-1 comparative Study.

Sr no	Paper Title	Author's Name	Algorithm used	Problem	Solution	Future Work
1	Image Forgery Detection	Hany Farid	1. the expectation/maximization (EM) algorithm. 2. sequential floating forward search algorithm.	Digital watermark must be inserted at the time of recording.	The expectation/maximization (EM) algorithm is used to solve the problems.	Develop an algorithm so that the color filter array interpolation can be regenerated by simply placing an image onto its original lattice
2	Splicing Forgeries Localization through the Use of First Digit Features	Irene Amerini ,Rudy Becarelli, Roberto Caldelli, Andrea Del Mastio	1. forgery localization algorithm.	Tampering localization in a full-frame image	Forgery localization algorithm used to work with full-frame image	Future works will concern the reduction of such a search window size. After that, these tiles have been compressed once or twice to build the positive or the negative dataset.
3	Image Forgery Localizationvia Block-Grained Analysis of JPEG Artifacts	Tiziano Bianchi, Alessandro Piva	1. double JPEG localization algorithm	maximizatio n problem has to be separately solved for each of the 64 DCT coefficients within a block.	forensic algorithm that can reveal a tampering at a local level, without any prior information about the location of the manipulated area, in the presence of double JPEG compression, either aligned or non-aligned	Future research will be devoted to methods that can cope with simple image editing operations.
4	Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis	Zhouchen Lina, Junfeng Heb, Xiaoou Tanga, Chi-Keung Tangb	1. CRF(Conditional random field) based algorithm.	problem in computational fine-grained algorithm to detect tampered JPEG images	CRF based algorithms used to overcome the problem	Improve the accuracy of the approach by detecting the tampered images.
5	Multi-Clue Image Tampering Localization	Lorenzo Gaborini, Paolo Bestagini, Simone Milani, Marco Tagliasacchi, Stefano Tubaro	1.tampering detection algorithm. 2.tampering localization algorithm. 3.image forgery localization algorithm based on PRNU	Forensic tools usually focus on one specific kind of forgeries.	To implement Color Filter Array (CFA) interpolation strategy, to detect local tampering.	Future works will be devoted to fine-tune the fusion strategy, as well as to integrate forensic tools.
6	Multi-Scale Fusion for Improved Localization of Malicious Tampering in Digital Images	Paweł Korus, Jiwu Huang	1.SIMPLE algorithm. 2. Bottom-up and top-down fusion algorithm	It is critical to correctly exploit the dependencies between different scales of analysis.	By using proper fusion techniques best performance can be achieved.	

IV. PROPOSED SYSTEM

1. It deals with multiscale analysis in digital image forensics.
2. A popular forgery method is considered in which, as a result of content replacement, some fragments of the JPEG image have different compression history and exhibit either single or double compression artifacts[8].
3. A detailed analysis of the multi-scale localization problem based on MBFDFs is evaluated.

Which consists of:

a) Localization Using First Digit Feature:

Our feature space contains 180 features - the MBFDFs of all 9 digits from first 20 AC coefficients. Classification is performed by a SVM classifier with a radial basis function (RBF)[6] kernel and trained to yield probability estimates of the decisions.

b) Detailed Analysis of Candidate Maps:

Here, two tampering scenarios are considered which are corresponding to the presence of double JPEG compression either inside or outside of the tampered regions, in short referred to as the double-inside or single-inside scenarios, respectively. Regardless of the scenario, the expected candidate maps indicate tampered regions with scores≈1 and pristine regions with scores ≈ 0. Hence, for the single inside scenario the candidate scores will correspond to 1 - classification scores

c) Exploiting Inter-Scale Dependencies:

The candidate maps are characterized by strong correlations both between the neighbours in the image plane, and between various scales of analysis. Exploitation of the latter dependencies is the key to successful multi-scale fusion.

d) Determining Candidate Map Reliability:

Small scale analysis yields less reliable candidate maps, which may unnecessarily introduce noise to the fusion process. Additionally, large scale analysis may produce empty candidate maps if the tampered region is smaller than the analysis window. Since such candidate maps do not contribute information useful for tampering localization, ideally they should be ignored by the fusion procedure. Here, an algorithm that allows to quickly estimate whether a candidate map is useful or not is used.

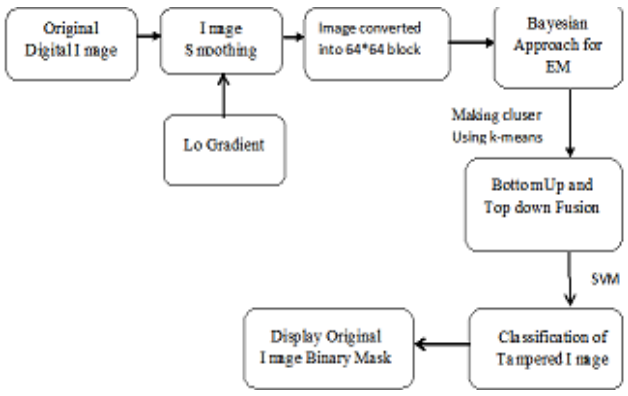

Fig 1: Proposed System

V. ALGORITHM

1. Smoothing of image

```
Begin
Set offset=0;
Set numRead=0;
While
(offset < bytes.length && (numRead=in.read())>=0);
        offset += numRead;
if (offset < bytes.length)
 throw exception=could not read the file+file name;
set RenderedImage=NULL;
ImageIO.write(image,"jpeg",newFile("smoothimage.jpg"));
End
```

2. Clustering

```
Begin
Set co=0;
Set mean=0;
Read the smoothed image using BufferedImage
Get the width and height of the image as follows
int height=img.getHeight();
    int width=img.getWidth();
for (int i = 0; i < height; i++) {
        for (int j = 0; j < width; j++) {
increment co;
int pixel=img.getRGB(j, i);
int red = (pixel >> 16) & 0xff;
int green = (pixel >> 8) & 0xff;
int blue = (pixel) & 0xff;
Print the custer number
End
```

3. Energy minimization

```
Begin
Set width=sourceImage.getWidth();
Set height = sourceImage.getHeight();
Calculate the size of the image as width * height;
if (data == null || picsize != data.length) {
Set data=new picsize;
Set magnitude= new picsize;
Find out the threshold edges
          for (int i = 0; i < picsize; i++)
{
 data[i] = data[i] > 0 ? -1 : 0xff000000;
           }
Find out the luminance
          Math.round(0.299f * r + 0.587f * g + 0.114f * b);
Display edges
Stop.
```

VI. MATHEMATICAL MODEL

Fusion by energy minimization:

Step1: A Bayesian approach to tampering localization would involve finding the optimal tampering map $t^{\wedge}$that maximizes the posterior probability given a set of candidate maps:

$$t^{\wedge} = argmax_{t\in[0,1]^N} P\left(t\middle|c^{(s)}: s = 1,2,\dots,S\right) \quad (1)$$

Step2:Then, ignoring the irrelevant constant term, the problem can be rewritten as:

$$t^{\wedge} = argmax_{t\in[0,1]^N} P\left(c^{(s)}: s = 1,2,.,S\middle|t\right)P(t) \quad (2)$$

Step3: Due to analytical tractability issues, full independence of the observations for individual authentication units is commonly assumed, leading to a simpler formulation:

$$t \quad = argmax_{t\in[0,1]^N} \prod_{i=1}^{N} P(c^{(s)}: s = 1,2\dots.,s|t_{i)}P(t). \quad (3)$$

Step4: It is found out to be more practical to assume interscale independence of the candidate scales at this point, and introduce a simpler heuristic mechanism for exploiting these dependencies at a later stage. Then, the problem becomes:

$$t^{\wedge} = argmax_{t\in[0,1]^N} \prod_{i=1}^{N}\prod_{s=1}^{S} P\left(c_i^{(s)}\middle|t_i\right)P(t) \quad (4)$$

Step5: In practice it is often more convenient to represent the MRF in terms of Gibbs potentials, and reformulate the problem into energy minimization [15]. Gibbs potentials use probabilities in the form:

$$p(t) = Z^{-1}e^{-U(t)} = Z^{-1}e^{-\sum v_c^{(t)}} \quad (5)$$

where Z is a normalizing constant, and U is an energy function defined as a sum of potentials v_c on cliques

Step6: Finally, by taking a negative logarithm of (Step4), the multi-scale fusion problem can be solved by minimizing the following energy function:

$$\frac{1}{S}\sum_{i=1}^{N}\sum_{s=1}^{S} E_r\left(c_i^{(s)}, t_i\right) + a\sum_{i=1}^{N} t_i + \beta\sum_{i=1}^{N}\sum_{j\in\bowtie_i}^{i} |t_i - t_j| \quad (6)$$

VII. EXPECTED OUTPUT

When an image is browsed, it gets displayed and then we perform image smoothing on it. Image smoothing smoothes or blurs the image and helps in finding out the tampered region in the image. After the smoothing clusters of the image are found out on the basis of color bags. Energy minimization is performed on the basis of clusters formed. The image obtained after energy minimization would be further read into two different angles by using Top-Down and Bottom-Up approaches to check for tampering of the image. The tampered image would further be corrected and the binary mask for the original image would be obtained as the final output.

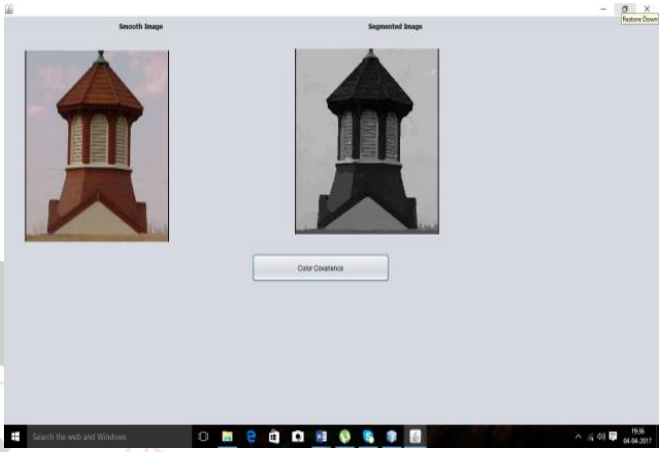

Fig 2: Smoothing and segmentation of image.

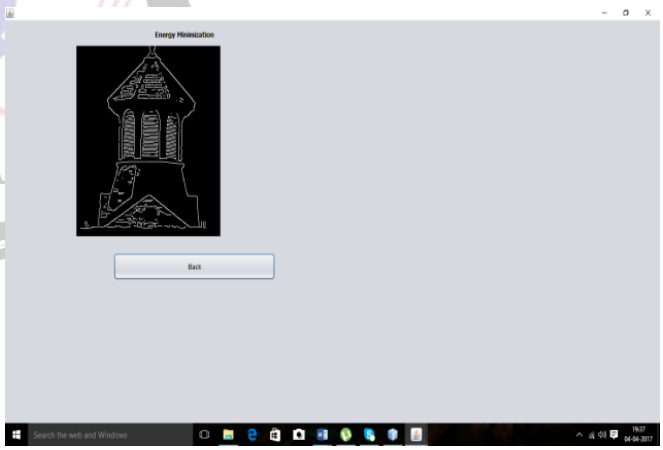

Fig 3: Energy Minimization.

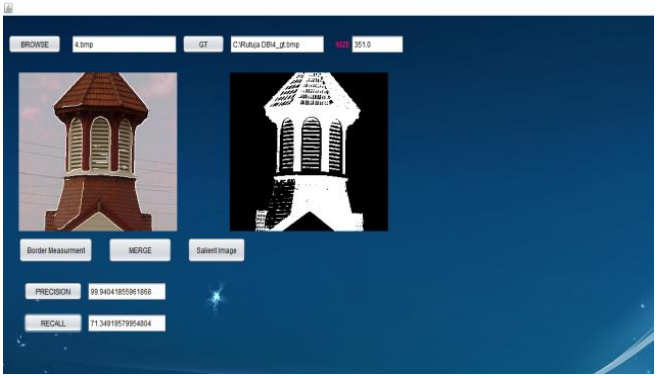

Fig 4: Binary mask of salient region with precision and recall.

VIII. CONCLUSION

We have tried to implement the paper "Paweł Korus, Jiwu Huang", "Multi-Scale Fusion for Improved Localization of Malicious Tampering in Digital Images", IEEE Trans. Image Process., March 2016 and according to the implementation the conclusion is, a detailed analysis of the multi-scale fusion problem in the context of JPEG splicing forgeries. The fusion of candidate maps obtained on multiple scales of analysis can improve the tampering localization performance of sliding window-based detectors by combining the benefits of small-scale and large-scale analysis. Here three novel fusion methods that exploit the dependencies between successive scales of analysis. Firstly, by using an energy-minimization approach, which uses a MRF to model the previous information regarding the tampering maps. Secondly, with the two dual heuristic strategies, referred to as bottom-up and top-down fusion, which exploits the expected dependencies between the tampered regions in small and large-scale analysis. The smoothened image helps in detecting the clusters present in the image and further more the energy minimized image gives us a outline of the completely connected regions in the input image. The salient region hence obtained is useful for determining the precise location of the object.

REFERENCES

[1] H. Farid, "*Image forgery detection*," IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16–25, Mar. 2009

[2] I. Amerini, R. Becarelli, R. Caldelli, and A. Del Mastio, "*Splicing forgeries localization through the use of first digit features*," in Proc. IEEE Int. Workshop Inf. Forensics Secur., Dec. 2014, pp. 143–148.

[3] Z. Lin, J. He, X. Tang, and C.-K. Tang, "*Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis*," Pattern Recognit., vol. 42, no. 11, pp. 2492–2501, 2009

[4] T. Bianchi and A. Piva, "*Image forgery localization via block-grained analysis of JPEG artifacts*," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1003–1017, Jun. 2012.

[5] L. Gaborini, P. Bestagini, S. Milani, M. Tagliasacchi, and S. Tubaro, "*Multi-clue image tampering localization*," in Proc. IEEE Int. Workshop Inf. Forensics Secur., Dec. 2014, pp. 125–130

[6] P. Korus and A. , "*Efficient method for content reconstruction with self-embedding*," IEEE Trans. Image Process., vol. 22, no. 3, pp. 1134–1147, Mar. 2013.

[7] S. Sarreshtedari and M. A. Akhaee, "*A source-channel coding approach to digital image protection and self-recovery*," IEEE Trans. Image Process., vol. 24, no. 7, pp. 2266–2277, Jul. 2015.

[8] M. C. Stamm, M. Wu, and K. J. R. Liu, "*Information forensics: An overview of the first decade*," IEEE Access, vol. 1, pp. 167–200, May 2013

[9] W. Wang, J. Dong, and T. Tan, "*Exploring DCT coefficient quantization effects for local tampering detection*," IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 1653–1666, Oct. 2014.

[10] S. Duncan and S. Sameer, "*Approaches to multisensor data fusion in target tracking: A survey*," IEEE Trans. Knowl. Data Eng., vol. 18, no. 12, pp. 1696–1710, Dec. 2006

[11] X. Wang, J.-H. Cho, K. Chan, M. Chang, A. Swami, and P. Mohapatra, "*Trust and independence aware decision fusion in distributed networks*," in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops, Mar. 2013, pp. 481–486

[12] Z. Chair and P. K. Varshney, "*Optimal data fusion in multiple sensor detection systems*," IEEE Trans. Aerosp. Electron. Syst., vol. AES-22, no. 1, pp. 98–101, Jan. 1986.

[13] R. Polikar, "*Ensemble based systems in decision making*," IEEE Circuits Syst. Mag., vol. 6, no. 3, pp. 21–45, Sep. 2006.

