Localisation of spliced region using pixel correlation in digital images

Ashwani Thakur
University Institute of Engineering and Technology
Chandigarh, India
ashwanitr001@gmail.com

Akshita Aggarwal
University Institute of Engineering and Technology
Chandigarh, India
akshitaaggarwal1997@gmail.com

Savita Walia
University Institute of Engineering and Technology
Chandigarh, India
savita_walia@rediffmail.com

Krishan Saluja
University Institute of Engineering and Technology
Chandigarh, India
k.salujauiet@gmail.com

***Abstract*— Image forgery has become the main concern of the society over the past many years due to an increase in the number of false cases of image manipulation leaving a severe impact on the life of a victim. Therefore, it has become necessary to solidly build forgery detection method to overcome image forgery problem. This necessity led to research in this field of image processing and provide detection techniques to check the integrity of images. In this paper, a method for localization of such tampered region is proposed. The proposed method uses unsupervised learning approach to localize the region of image and find whether the region is forged or not. It uses GLCM, a textural feature descriptor that uses pixel correlation in image to extract features from it. Further, for feature matching, Euclidean and Hellinger distance is used and finally, the localization of tampered region is performed. Euclidean and Hellinger distance is calculated separately on each image for comparison of the results. The experimental results showed that Hellinger outperformed Euclidean distance in feature matching and gave better localization results.**

Keywords—splicing forgery, localization, pixel correlation, feature matching, gray level co-occurrence matrix.

I. INTRODUCTION

With the advancement in image processing techniques, tampering with the digital images is becoming easier day by day and leaving no traces thereafter making difficult for humans to detect. This rapid growth leads to an increase in the number of image forgeries which can leave a severe impact on any victim's life whose image has been manipulated and shared on social media. Therefore, it becomes necessary to investigate if image is original or not. Several different researches have been done by authors previously in this field of image forgery. Image forgery detection is mainly divided into two classes which are active methods and passive methods aiming to find the originality of images [1]. In active method, there is prior knowledge about watermark or signature inserted into image while capturing. These are used to check the originality of digital images. This embedded code is taken out from the given image and is checked against the original watermark, if it matches then image is real or authentic otherwise it is not whereas in passive method there is no prior information about any such type of embedded code. In this technique, it is believed that they are some traces left in various form of irregularities in image while tampering the contents of image. These irregularities can be used to find the forgery in image.

There are several techniques for tampering the digital images like retouching, copy-move, splicing, etc. [2]. Retouching refers to change the looks in images like removing the dark circles beneath the eye, changing the skin colour and adding various filters to original photo in order to

Fig. 1. Below spliced (composite) image is a mixture of above two original images.

make it more attractive [3]. Now days, there are different types of applications available for image editing like Snapseed, TouchRetouch, Enlight and many more. This technique is mainly used in film and TV industry to hide all types of blemishes from actor or actresses faces making them more attractive. In copy-move forgery technique, small region or area is copied from the image and pasted into the same image at some other place. This technique is widely used by forgers to manipulate the original image and making false allegations on the other person to prove himself correct by giving false evidence. It is difficult to detect such type of manipulations as region is from same image so patterns like texture, colour, noise remain somewhat similar. Different methods have been proposed by authors in their literature to find copy-move forgery [4][5][6]. Splicing forgery method refers to copy pasting of a region on an image from different one or more images. Fig. 1 represents an example for splicing forgery. Many researchers have proposed method for splicing detection like using textures as a feature for detection [7], using statistical features [8], using inconsistencies in lighting as a feature [9] and many more. It is believed that there are some particular patterns which remain consistent for whole image. Therefore, if any image has been tampered, then its authenticity can be checked against those consistent patterns.

This paper aims to localize the tampered region of an image using GLCM for feature extraction and further using Euclidean and Hellinger distance for feature matching. This

978-1-5386-9436-7/19/$31.00 ©2019 IEEE

paper describes non-supervised approach to detect the forged region of an image. The rest of paper is organized in the following form. First, all the related work done in splicing forgery detection using texture based features is presented in Section 2. Then Section 3 describes methodology used for detection. Section 4 presents all experimental details and results. Finally, Section 5 gives conclusion.

II. RELATED WORK

Many different models have been proposed in the past for image splicing detection using different features like textural based features, statistical based features, transform domain features, space domain features and many more. In earlier research [10], an author proposed a statistical method, where histogram of approximate run length along the direction of edge gradient is used as a feature to detect image splicing detection. This method used 30-D feature vector for each image and gave 80.58% detection accuracy. In [11], DCT coefficient quantization based markov feature extraction model is used for image splicing detection with 98.5% accuracy for CASIA1 dataset. In this method, information loss is reduced by using DCT coefficient quantization. But on the same hand, additional feature reduction algorithms are also required to eliminate redundancy included by markov model-based features.

In [12], author used color shift inconsistency as a feature to find any manipulation in an image and then further used color temperature distance with threshold value using OSTU algorithm to localise the spliced region. Also, in previous research [13], textural feature Local Binary Pattern (LBP) is used along with spatial rich models (SRM) to detect passive image forgery. In addition to this, it also uses co-occurrence matrices and BEST-q-CLASS feature selection strategy. This approach is applied on IEEE IFS-TC image forensics dataset which contains 10 different forgeries including unaddressed forgeries such as histogram equalization, cropping etc. and produced 98.4% detection accuracy. In [14], multi-scale LBP is used with DCT coefficients on CASIA v1.0, CASIA v2.0 dataset for image splicing detection. On further using 10-fold cross validation for evaluation of SVM classifier with RBF kernel, performance metrics are computed and achieved 97.3% accuracy.

GLCM and HOG is used to extract texture based feature and edge features respectively [15] from color illuminant map. kNN classifier is then used to classify image as forgery if any face pair is indicated as inconsistently illuminated. However, this method is not able to detect all type of composite (spliced) images containing lighting effects. In [16], RBG and HSV color images are used. For each color channel red, green and blue of an image, feature vector is computed. Here color GLCM (CGLCM) and Gabor filters are used for textural feature extraction from an image. It was also found by authors that CGLCM based method gave better precision on small images in comparison to Gabor Filters (GF) method. Moreover, GF produced large size of feature vector as compared to CGLCM. In [7], textural feature GLCM (TF-GLCM) method is proposed to detect splicing forgery and further six different textural features are determined describing the properties of GLCM. TF-GLCM also gave promising results on post-processed images which are collected from CASIA v1.0 and CASIA v2.0 database. Detection accuracy achieved using this method is 98.54% on CASIA v1.0 and 97.73% on CASIA v2.0 with very less features. Furthermore in [17], scene classification is implemented by using graphical feature vector which is extracted using gray level-gradient co-occurrence matrix and then Gower's similarity coefficient model is used to perform similar matching and produced high precision. In addition to this, extension of GLCM to more than 1 scale is done using different methods like pyramid decomposition and Gaussian smoothing [18]. Multi-scale descriptor is further used to evaluate the performance on of the approach five texture dataset. Moreover, in [19] DTCWT is used to decompose the image into multiple directions giving broader information about the features and further GLCM is implemented. Then its statistical properties are calculated and then finally concatenation of the values followed by normalization is done to obtain final feature vector. This approach achieved high classification rate of 99.93% on VisTex test dataset and 98.82% on Brodatz dataset as compared to conventional methods such as DWT, Gabor.

III. METHODOLOGY

The main aim of image forgery is to remove useful information from the image by tampering the contents. The proposed method is inspired from paper [20] and aims to detect such manipulations in the image. This section describes the proposed methodology for the forgery detection in the images. A brief flowchart of the proposed method is illustrated in Fig. 2.

A. Converting RGB image to gray-scale

In the original image, each pixel is defined by the triplet intensity of Red, Blue and Green color. This triplet of RGB pixel is mapped into a single number result giving each pixel a gray-scale value.

B. Reducing the number of gray-levels

The above method results in 256 gray levels with maximum value 255. With this maximum value, the computation becomes quite complex. So to reduce the complexity, gray level values are reduced to 8. Thus the new gray level values lie in the range of 0 to 7.

C. Dividing the image into sub image of overlapping blocks

The 8 gray level image is further divided into 32×32 size of overlapping blocks and using a sliding window of step size 4. Blocks are traversed in order of left to right and when right end of the image is reached then traversal is from top to bottom and it goes on till the whole image is traversed. The step size of 4 means, next overlapping block selected is after four-pixel values in a horizontal or vertical direction depending on whether the traversal is from right to left or from top to bottom. Fig. 3 illustrates how a window is moved and the next overlapping block is encountered.

D. Calculating the normalized GLCM for each overlapping block

A textural feature based on GLCM is extracted from each block. Corresponding to each block, GLCM is calculated. GLCM is a statistical measure of the spatial relationship between the neighbouring pixels of an image. It recognizes the textural characteristics of an image. It considers how many pixel pairs with certain intensity values are repeated over an image [21]. This textural information between the pixels of an image can be obtained at different values of distance (d) and angle (θ) between them.

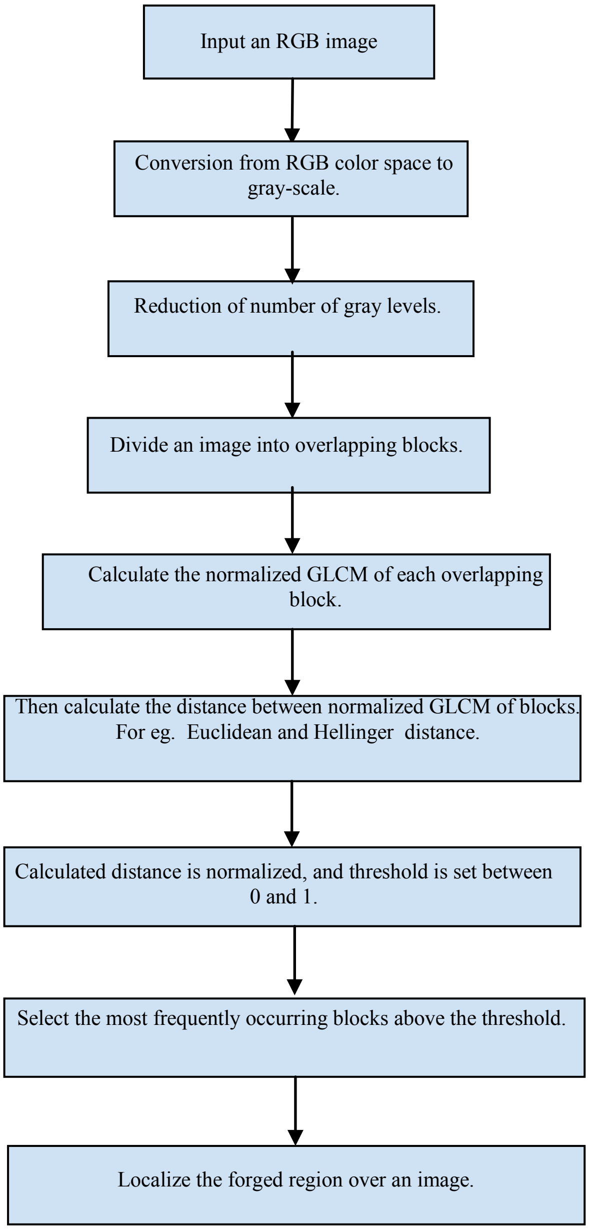

Fig. 2. Brief description of proposed methodology using flowchart.

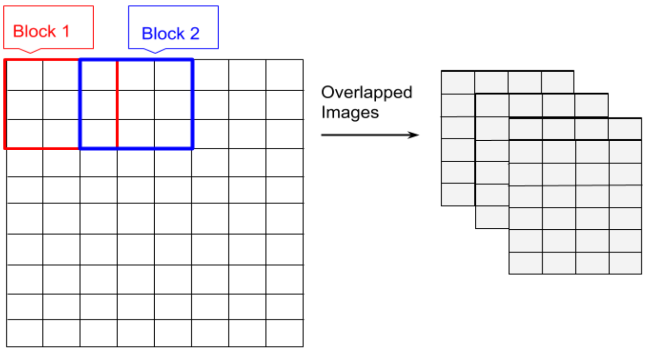

Fig. 3. Illustration of selection of overlapping blocks

The following steps are used to calculate GLCM:

- First, matrix (A) for each block of dimension 32×32 containing pixel value is generated.
- Second, as matrix A contains values from 0 to 7 (8 gray level image) so second matrix B calculated is of size 8×8. Matrix B is calculated as follows:

B (i, j) is an element of matrix B where i and j denote row and column number respectively. B(i, j) value is calculated by counting the number of repeated pair value of (i, j) occurring in matrix A horizontally or vertically. This calculated matrix B is said to be Gray Level Co-occurrence matrix (GLCM). GLCM describes texture information related to the spatial distribution of gray levels in an image. Fig. 4 describes in detail how GLCM is calculated for d=1(neighbouring pixel) and θ=0(horizontal pixel). In the output GLCM, there is value 2 corresponding for the element (1, 1) as two instances of horizontally adjacent pair (0, 0) is present in total for 4×4 image. Similarly, element (2, 3) contains value 1 as only one instance of horizontally adjacent pair (2, 3) is present.

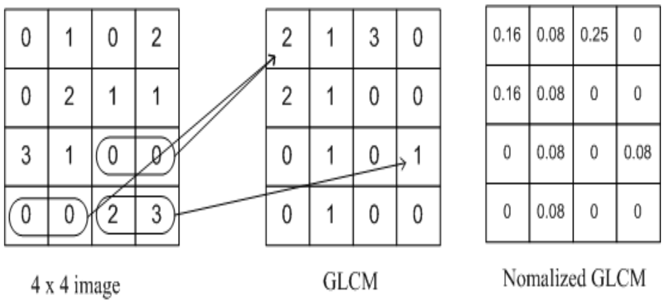

Fig. 4. Steps to calculate the normalized GLCM

E. Calculating distance between GLCM of blocks:

After GLCM is calculated, the next step is to find some dissimilarities between the textural features in the spliced and authentic images extracted using GLCM. This difference is used to mark the distinction between the two images. In the proposed study, one such method used is to calculate the Euclidean distance between the normalized GLCM of the blocks. After the Euclidean distance is calculated, it is normalized by dividing each value with maximum value obtained. Euclidean distance is computed between GLCM on basis of an element by element of the block. First, the difference between the elements of one block with the corresponding elements of the second block is calculated. Then each difference calculated is squared and finally summed together to get the final value whose square-root gives the Euclidean distance.

Other method used is to calculate Hellinger distance between the normalized GLCM and then even further normalizing the distance obtained. Mathematically, Hellinger distance is given by (1). Here, X = (x1,....,xk) and Y = (y1,….,yk) are two discrete probability distributions and the Hellinger distance H (X, Y) is a measure of similarity between these distributions.

$$H(X, Y) = \frac{1}{\sqrt{2}} \sqrt{\sum_{i=1}^{k} \left(\sqrt{x_i} - \sqrt{y_i}\right)^2} \qquad (1)$$

F. Selecting the threshold value:

After calculating the distance between GLCM, the next step is to find the blocks having maximum variation in the GLCM values. To find such blocks, only the blocks having greater value than a specific threshold are considered. With experimentation on different values between 0.0 and 1.0 it was found that 0.3 gives the best results.

G. Localise the forged area on image:

The blocks obtained in the above steps are finally plotted over an image. The plotted area results in the identification of the forged area on the image.

IV. EXPERIMENTAL RESULTS

This section presents the performance analysis of the proposed method on images from publicly available datasets i.e. CASIA v1.0 and CASIA v2.0 dataset [22]. CASIA v1.0 contains 800 authentic images and 921 forged images of JPEG format. All the images (authentic and spliced) considered for experimentation is of fixed size 384×256 and no post-processing is performed on any image. In CASIA v1.0 dataset, among 921 forged images, there are 461 images on which copy-move forgery operation has been performed and rest of 460 images are composite (copy and paste operation from one image to other) images. CASIA v2.0 contains 7,491 authentic and 5123 forged images of varying sizes from 240 × 160 to 900 × 600 pixels and of different format i.e. JPEG, BMP, and TIFF.

During experimentation for detecting the splicing forgery, RGB image of size 384×256 is taken as input which contains 256 gray levels. 256 gray levels of image are further converted to 8 gray levels. This image is further divided into overlapping blocks of dimension 32×32. Therefore, total blocks obtained by using a sliding window of step size 4 are 6144. GLCM is calculated for each overlapping block. As image is reduced to 8 gray levels, so GLCM calculated also consists of 8 levels only, i.e. dimension of GLCM is 8×8. For experimentation, normalized GLCM is calculated for d=1 and theta = 0 on the different forged images. Furthermore, Euclidean and Hellinger distance is calculated between the GLCM of blocks by setting different values of threshold between 0 and 1, and then again normalising the distance obtained and finally analysing the best threshold value for the proposed method. Experimentation is performed by taking different values of threshold such as 0.3, 0.5, 0.7 and 0.9. It was found that 0.3 as threshold value, gives best possible results for localisation of spliced region.

In Fig. 5, experimental results are shown on the four images for both the Euclidean and Hellinger distance. First column shows the spliced image, second column shows the Euclidean results and third column shows the Hellinger results. Forged region is localised by red color rectangles over an image. In case of Euclidean distance, false positives (region which is not forged) are also detected to some extent whereas Hellinger distance detected forged region correctly.

V. CONCLUSION

In this paper, method for localisation of spliced region using pixel correlation is proposed. Overlapping blocks are considered in the proposed method. Next, textural feature descriptor i.e. GLCM is used to extract the features from the images. Many different textural features can be extracted using GLCM, by changing the values of distance (d) and angle (θ) between the pixels. Then, Euclidean and Hellinger distances are calculated separately on the images to perform feature matching and finally localising the tampered region. The proposed methodology is tested on CASIA v1.0 and CASIA v2.0 dataset. Finally, the results are compared and it is observed through experimental results that Hellinger distance performed better than Euclidean distance because in case of Hellinger, even small changes can be observed due to square-root of pixels in calculation of Hellinger distance.

In the future work, supervised learning such as SVM classifier will be used to automate the process of image forgery detection. Also, the effect of other color components of image like chrominance and luminance will be explored for spliced forgery detection.

REFERENCES

[1] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digit. Investig., vol. 10, no. 3, pp. 226–245, 2013.

[2] M. A. Qureshi and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," Signal Process. Image Commun., vol. 39, pp. 46–74, 2015.

[3] H. Shah, P. Shinde, and J. Kukreja, "Retouching Detection and Steganalysis," International Journal of Engineering Innovation & Research , vol. 2, no. 6, pp. 487–490, 2013.

[4] T. Mahmood, Z. Mehmood, M. Shah, and T. Saba, "A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform," J. Vis. Commun. Image Represent., vol. 53, pp. 202–214, 2018.

[5] A. Novozámský and M. Šorel, "JPEG compression model in copy-move forgery detection," Proc. 7th Int. Conf. Image Process. Theory, Tools Appl. IPTA 2017, vol. 2018–Janua, pp. 1–6, 2018.

[6] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 3, pp. 507–518, 2015.

[7] X. Shen, Z. Shi, and H. Chen, "Splicing image forgery detection using textural features based on the grey level co-occurrence matrices," IET Image Process., vol. 11, no. 1, pp. 44–53, 2017.

[8] Saba Mushtaq, Ajaz Hussain Mir, "Forgery Detection Using Statistical Features", *International Conference on Innovative Applications of Computational Intelligence on Power Energy and Controls with their Impact on Humanity (CIPECH14)*, 28 & 29 November 2014.

[9] M. K. Johnson and H. Farid, "Exposing Digital Forgeries by Detecting Inconsistencies in Lighting," ACM Multimed. Secur. Work., no. 1, pp. 1–10, 2005.

[10] Z. He, W. Sun, W. Lu, and H. Lu, "Digital image splicing detection based on approximate run length," Pattern Recognit. Lett., vol. 32, no. 12, pp. 1591–1597, 2011.

[11] J. G. Han, T. H. Park, Y. H. Moon, and I. K. Eom, "Quantization-based Markov feature extraction method for image splicing detection," Mach. Vis. Appl., vol. 29, no. 3, pp. 543–552, 2018.

[12] Peng Sun, Yubo Lang, Shu Fan, Zhe Shen, Lei Liu, Daguo Shan, Silong Peng, Exposing Splicing Forgery Based on Color Temperature Estimation, Forensic Science International https://doi.org/10.1016/j.forsciint.2018.04.049.

[13] S. Farooq, M. H. Yousaf, and F. Hussain, "A generic passive image forgery detection scheme using local binary pattern with rich models," Comput. Electr. Eng., vol. 62, pp. 459–472, 2017.

[14] A. Shah and E. S. El-Alfy, "Image Splicing Forgery Detection Using DCT Coefficients with Multi-Scale LBP," 2018 Int. Conf. Comput. Sci. Eng. ICCSE 2018 - Proc., pp. 1–6, 2018.

[15] L. Baby and A. Jose, "Digital Image Forgery Detection Based on GLCM and HOG Features," Neurocomputing, vol. 3, pp. 426–430, 2014.

[16] M. Benčo and R. Hudec, "Novel method for color textures features extraction based on GLCM," Radioengineering, vol. 16, no. 4, pp. 64–67, 2007.

[17] S. Chen, C. Wu, D. Chen, and W. Tan, "Scene classification based on gray level-gradient co-occurrence matrix in the neighborhood of interest points," Proc. - 2009 IEEE Int. Conf. Intell. Comput. Intell. Syst. ICIS 2009, vol. 4, pp. 482–485, 2009.

[18] F. Roberti de Siqueira, W. Robson Schwartz, and H. Pedrini, "Multi-scale gray level co-occurrence matrices for texture description," Neurocomputing, vol. 120, pp. 336–345, 2013.

[19] P. Yang and G. Yang, "Feature extraction using dual-tree complex wavelet transform and gray level co-occurrence matrix," Neurocomputing, vol. 197, pp. 212–220, 2016.

[20] D. Cozzolino, G. Poggi, and L. Verdoliva, "Splicebuster: A new blind image splicing detector," " in IEEE Workshop on Information Forensics and Security (WIFS), 2015, Rome, 2015, pp. 1–6.

[21] Y. Q. Shi, C. Chen, and W. Chen, "A natural image model approach to splicing detection," " in Proc. ACM Workshop on Multimedia and Security, Dallas, TX, Sep. 2007, pp. 51–62.

[22] "CASIA Image Tempering Detection Evaluation Database (CAISA TIDE)," National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science, Corel Image Database. [Online]. Available: http://forensics.idealtest.org. [Accessed: 19-Aug-2017].

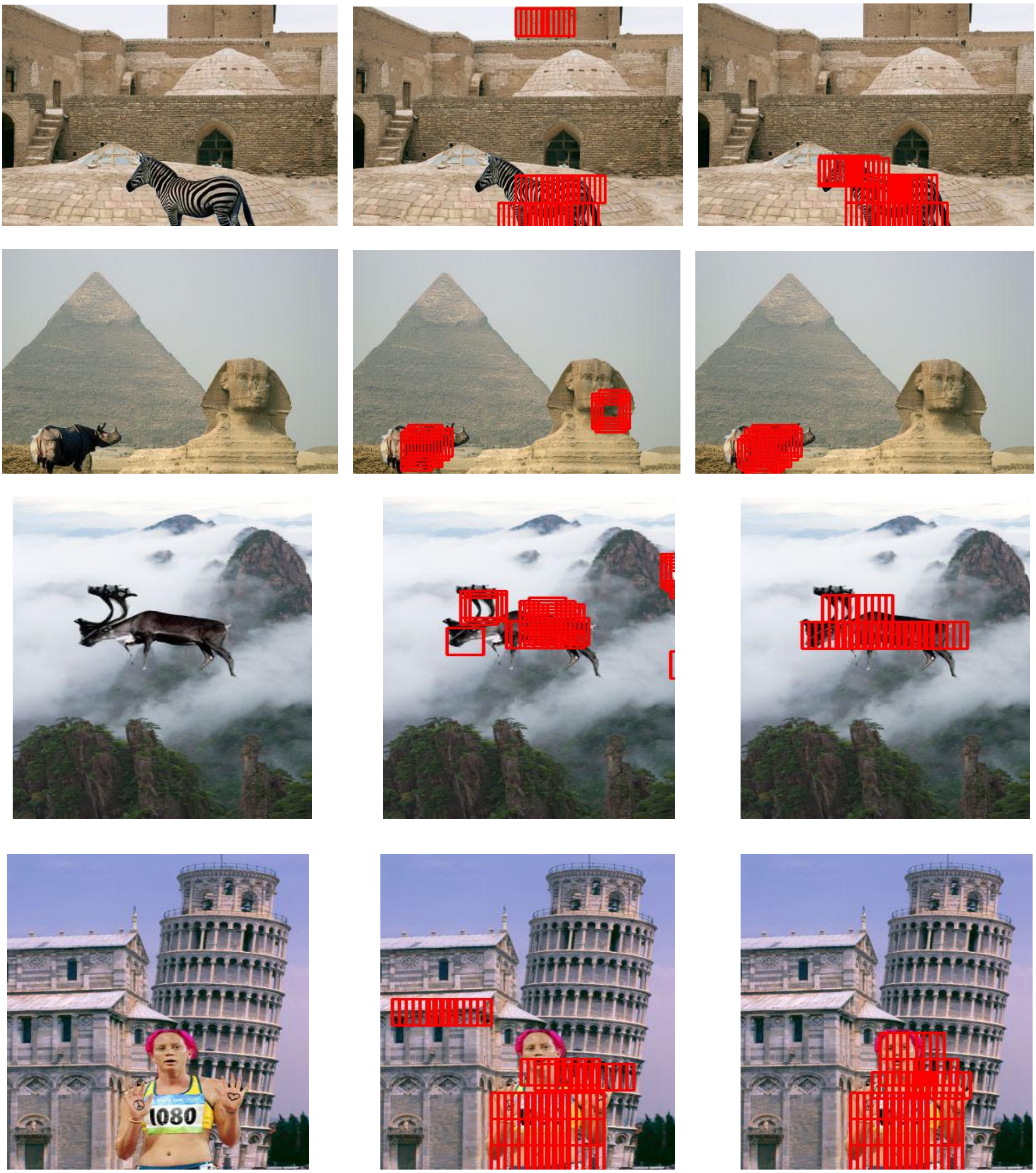

Fig. 5. Experimental results of the proposed methodolgy.Red color rectangles indicates the forged region. First column is of spliced image, second column shows Euclidean results and third column shows Hellinger results over an image.