Random Forest based Copy-Move Forgery Detection

Chris Templeton
Computer Science

Universidad Virtual Latinoamericana
Venezuela

Awazuddin Shah
Computer Science

Universidad Virtual Latinoamericana
Venezuela

Jawad Khan
Computer Science

Universidad Virtual Latinoamericana
Venezuela

Abstract— Proving the authenticity of images is an important part of image forensics. Copy-move forgery is a method of forgery commonly followed in blind image forensics. We propose the use of a modified Auto Color Correlogram to obtain feature vectors from the forged image. The features extracted are sent as input to a RBF-SVM that gives a score for the possibility of a copy-move situation. We then use a normalized cross correlation for feature matching with the same feature vectors and then produce texture attributes as smoothness and Entropy. Based on the entropy and smoothness we use a linear regression model to classify this and obtain a predicted score. The two outputs obtained are passed as input to a Random forest classifier which classifies the image as either forged or not forged.

Keywords—*copy-move, forgery, random forest*

I. INTRODUCTION

During recent times, image tampering has become extremely feasible due to the easy availability of picture editing software. Such software has made it remarkably easy to manipulate, modulate and modify an image's content while not reducing the quality of the image. These changes do not leave any idea of modification to a user and these images end up on the internet and shared even though it has been modified. Videos and images hold high a level of importance in today's world. They are extremely important in fields like forensics, medical imaging, sports, research publications etc. Forging in these fields can lead to a lot of problems. For example, crime scenes can be forged and can lead to lack of evidence or help the criminal to escape.

Image forgery can broadly be divided into 3 categories:

- 1) Image Splicing
- 2) Image retouching
- 3) Copy-Move forgery.

Image Splicing

Image splicing is a forgery method where two or more images are taken and combined together. This combination generates a new image called the splicing image. Figure (1) shows an example of this.

Figure 1. Image splicing combining two images

Image splicing forgery is hard to detect. This is because it is hard to find out the difference in either the region of the forgery or it's boundary.

Image retouching

Image retouching is another type of forgery. In this method subtle changes are made in the image by modulating changes in color, blur level etc. Another type of modulation is doing operations such as scaling, rotation etc to a part of an image and this creates a new image. Figure 2 shows an example of image retouching.

Figure 2. Image retouching example

Copy-move forgery

In this type of forgery a portion of the image is copied and pasted over another region to hide some information. Figure 3 shows an example of this type of forgery.

Figure 3. Copy-move forgery example

II. RELATED WORK

This paper proposes an approach for copy-move forgery detection.

In general there are two types of copy-move forgery detection algorithms: block-based or keypoint-based. Copy-move forgery methods generally involve comparing regions of interest. This is done by counting a similarity score.

An example of how to count this similarity was proposed by Zhang et al [1].

Block based approaches extract blocks from the image and compare the similarities between blocks to determine blocks having high similarity.

Keypoint based approaches would extract key points in the images as features and compare regions of interest using these key-points. Regions with high similarity were considered forged.

A. Block Based Approaches

Fridrich et al [2] proposed a method to detect forgery using Discrete Cosine Transform (DCT). Lexicographical sorting was done to reduce the cost of computation and pairs of neighboring blocks were considered as possibly forged. A similarity measure was calculated among the blocks. The drawback was an assumption made regarding a lack of postprocessing operations done.

An approach utilizing Discrete Wavelet Transform (DWT) and singular value decomposition (SVD) was proposed by Li et al [3]. They extracted low frequency coefficients by utilizing DWT. Next, they reduced the feature vector by using SVD.

Kang et al [4] proposed an enhancement of the same approach by using an advanced SVD. Myna et al [5] proposed an approach based on DWT and log-polar coordinates. The authors used DWT to obtain reduced dimension representation. The log-polar coordinates were used for mapping to sub-blocks of the image. Phase correlation and exhaustive searching was done to obtain matches between blocks.

Ryu et al [6] proposed an approach using Zernike moments. This algorithm was later on enhanced by Muhammad et al [7] by using an undecimated Wavelet Transform first. Both algorithms were invariant to rotation, blurring, JPEG compression but they were still susceptible to scaling.

An approach using circular blocks were proposed by Cao et al [8]. DCT was used to extract DCT coefficients and then circular blocks were along with this to extract the features. This approach reduced the feature length and showed robustness against noise and blurring. However, the algorithm was still suspect to rotation, compression and scaling.

Another approach using circular blocks was proposed by Li et al [9]. In this, circular blocks were extracted and rotation invariant LBPs are applied to the blocks to extract the features. Next, a gaussian filter was used to obtain low frequency components. These are considered to be more stable for forgery detection. This method was not suited for forgeries with arbitrary angles.

B. Keypoint based approaches

Keypoint based approaches eliminate the block division in the preprocessing stage of the algorithm itself. Distinctive features such as blobs, corners, edges etc are extracted using key points. A descriptor is then produced for a region around the features developed using the key-points. These regions are then used for the comparison to extract the similarity score.

Pun et al [10] proposed an approach where feature matching was done using Coefficient maps and thresholding. Pre-processing was done using DWT and segmentation.

Li et al [11] proposed a segmentation based approach to detect forgery. In this, small independent patches were extracted and the matching was done utilizing a transform matrix.

A method utilizing BSFN clustering was proposed by Liu et al [12]. The algorithm did not use any preprocessing method and instead utilized pixel sized regions of interest and then clustered them using BFSN. The algorithm showed robustness against scaling and rotation.

Keum et al [13] proposed a method to detect forgery using SIFT that was proposed by Lowe et al [14] as the method for key-point extraction. The regions were divided using mean shift clustering. The matching of regions were done using pattern entropy.

A method was proposed by Hashmi et al [15] wherein DWT was used to preprocess the image, key points were then obtained using SIFT and comparison of regions were done using the feature vectors. This method was robust to rotation and scaling. Jaber et al [16] proposed a method to detect forgery by using a mirror reflection invariant feature descriptor proposed by Guo et al [17]. Region matching was done using RANSAC algorithm proposed by Fischler et al [18] and hysteresis thresholding

III. PROPOSED APPROACH

A. Datasets

We use two popular databases to aid us with our experimental accuracy. First, we use the IMD database proposed by Christlein in [19] and then with the CoMoFoD database proposed by Tralic et al [20]. In total, we used 2000 images for training using the small image category of CoMoFoD and testing was done on 300 images.

B. Autocolor Correlogram

Auto Color Correlogram (ACC) was introduced by Tungkasthan et al [21] as a combination of correlogram and color relation. It was used for spatial color indexing. We however, modify it to extract features. The ACC takes into consideration all pixels of a particular color C_j that exist at a particular distance from all pixels of Color C_i to compute a mean color. Equation (1) shows how this is done.

$$ACC(i, j, k) = \mu_{C_i v C_j}^{(k)}(I) \quad (1)$$

Here, $I(x, y)$ is image we are checking with x ranging from 1 to M and y from 1 to N . This image is quantized in $C_1, C_2, \dots, C_m$ colors and k is the minimum of M or N . VC_j gives the R,G,B value of the color under consideration. The mean is calculated based on (2).

$$\mu_{C_i v C_j}^{(k)}(I) = \frac{\prod_{C_i v C_j x}^{(k)}(I)}{\prod_{C_i C_j}^{(k)}(I)} \quad (2)$$

Here, x can be either r, g or b . The denominator tells us the total of color C_j pixel color values that are separated by a distance of ' k ' from color C_i pixels. We determine N as the number of pixels where C_j is at a distance k from C_i and is represented by (3).

$$N = \prod_{C_i C_j}^{(k)}(I) = (P(X_1, Y_1) \epsilon C_i | P(X_2, Y_2) \epsilon C_j) \quad (3)$$

The image is divided into a set of blocks and the above steps are developed to obtain a spatial relation between the various colors for each pixel in the block.

These are stored as features and are repeated for each block. Each vector is stored as a row in a matrix. Therefore, each row corresponds to a particular block.

We use a SVM with a RBF kernel to provide probabilities based on each block's features as to whether the image may be forged or not. A score for forgery is calculated. This score is stored as SSVM.

C. Normalized Cross Correlation Score

The Normalized Cross Correlation (NCC) was proposed by Lewis et al [22] as a feature matching tool. Mathematically, NCC is represented by (4).

$$C(x, y) = \frac{\sum_{y'=0}^{h=1} \sum_{x'=0}^{w=1} T(x', y') I(x + x', y + y')}{\sqrt{\sum_{y'=0}^{h=1} \sum_{x'=0}^{w=1} T(x', y')^2 \sum_{y'=0}^{h=1} \sum_{x'=0}^{w=1} I(x + x', y + y')^2}} \quad (4)$$

Here x', y' are co-ordinates of the template T and x, y of the Image. The height and width are given by h, w respectively.

To this, we calculate two texture features as smoothness (S) and entropy (E). S is calculated in (5) and E in (6).

$$S = 1 - \frac{1}{1 + F} \quad (5)$$

Here, F is equal to the difference between C and the squared multiple correlation coefficient [23] that can be obtained from a linear regression model developed after the cross correlation done.

$$E = -(\log(S) + e^{-S}) \quad (6)$$

The entropy is passed as input to a linear regression model that gives a score as to whether the image has been forged or not as SNCC.

D. Random Forest Classifier

The two outputs are passed as input to a random forest classifier which determines if the image has been forged or not. Figure 4 shows the pipeline of the proposed model.

Figure 4. Pipeline of proposed work

IV. EXPERIMENTAL ANALYSIS

The proposed method was tested and compared using first the IMD and CoMoD databases.

The proposed method was compared against the method proposed by Huang et al [24], Cao et al [8] along with SIFT, SIFT-HOG and SURF.

Table 1 corresponds to the accuracy comparison for the algorithms tested using IMD database under rotation attacks. Table 2 corresponds to the accuracy comparison using IMD database with additive noise.

Table 3 corresponds to the accuracy comparison using IMD database with JPEG compression.

Table 1 corresponds to the accuracy comparison for the algorithms tested using CoMoD database under rotation attacks.

Table 5 corresponds to the accuracy comparison using CoMoD database with additive noise.

Table 6 corresponds to the accuracy comparison using CoMoD database with JPEG compression.

Method	Accuracy
SIFT	88.64
SURF	87.48
SIFT-HOG	91.51
Huang et al [24]	95.43
Cao et al [8]	94.81
Proposed	95.48

Table 1. Accuracy comparison using IMD rotation

Method	Accuracy
SIFT	85.45
SURF	86.01
SIFT-HOG	88.74
Huang et al [24]	96.83
Cao et al [8]	96.91
Proposed	96.89

Table 2. Accuracy comparison using IMD with noise

Method	Accuracy
SIFT	86.36
SURF	86.45
SIFT-HOG	87.78
Huang et al [24]	95.48
Cao et al [8]	95.37
Proposed	96.65

Table 3. Accuracy comparison using IMD with JPEG compression

Method	Accuracy
SIFT	88.42
SURF	87.78
SIFT-HOG	91.61
Huang et al [24]	95.31
Cao et al [8]	94.67
Proposed	95.31

Table 4. Accuracy comparison using CoMoD rotation

Method	Accuracy
SIFT	86.15
SURF	86.41
SIFT-HOG	88.14
Huang et al [24]	97.13
Cao et al [8]	96.94
Proposed	97.17

Table 5. Accuracy comparison using CoMoD with noise

Method	Accuracy
SIFT	84.51
SURF	86.16
SIFT-HOG	87.59
Huang et al [24]	96.03
Cao et al [8]	96.57
Proposed	96.71

Table 6. Accuracy comparison using IMD with JPEG compression

CONCLUSION

A method to detect Copy-Move forgery was proposed. First the image is subject to ACC and feature vector obtained is passed as input to a RBF-SVM and a prediction score is calculated.

Next, the image is subject to NCC and the feature vector is passed as input to a linear regression model to obtain an entropy value as output. Both the outputs obtained are passed as input to a random forest classifier that classifies the image to two classes: forged or not forged.

The proposed method showed great accuracy, much better than older methods and slightly better than recent state of the art methods. Novelty was in the ensemble of the algorithms and in the calculation of the entropy.

REFERENCES

- [1] Gowda, S.N. and Yuan, C., 2018, December. ColorNet: Investigating the importance of color spaces for image classification. In *Asian Conference on Computer Vision* (pp. 581-596). Springer, Cham.
- [2] Fridrich, A.J., Soukal, B.D. and Luk, A.J., 2003. Detection of copy-move forgery in digital images. In *Proceedings of Digital Forensic Research Workshop*.
- [3] Kang, L. and Cheng, X.P., 2010, October. Copymove forgery detection in digital image. In *Image and Signal Processing (CISP), 2010 3rd International Congress on* (Vol. 5, pp. 2419-2421). IEEE.
- [4] Myna, A.N., Venkateshmurthy, M.G. and Patil, C.G., 2007, December. Detection of region duplication forgery in digital images using wavelets and log-polar mapping. In *Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on* (Vol. 3, pp. 371-377). IEEE.
- [5] Muhammad, G. and Hossain, M.S., 2011, August. Robust copy-move image forgery detection using undecimated wavelets and Zernike moments. In *Proceedings of the Third International Conference on Internet Multimedia Computing and Service* (pp. 95-98). ACM.
- [6] Cao, Y., Gao, T., Fan, L. and Yang, Q., 2012. A robust detection algorithm for copy-move forgery in digital images. *Forensic science international*, 214(1), pp.33-43.
- [7] Li, L., Li, S., Zhu, H., Chu, S.C., Roddick, J.F. and Pan, J.S., 2013. An efficient scheme for detecting copymove forged images by local binary patterns. *Journal of Information Hiding and Multimedia Signal Processing*, 4(1), pp.46-56.
- [8] Pun, C.M., Yuan, X.C. and Bi, X.L., 2015. Image forgery detection using adaptive oversegmentation and feature point matching. *IEEE Transactions on Information Forensics and Security*, 10(8), pp.1705-1716.
- [9] Li, J., Li, X., Yang, B. and Sun, X., 2015. Segmentation-based image copy-move forgery detection scheme. *IEEE Transactions on Information Forensics and Security*, 10(3), pp.507-518.
- [10] Gowda, S.N., 2017. Human activity recognition using combinatorial Deep Belief Networks. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops* (pp. 1-6).
- [11] Keum, J.S., Lee, H.S. and Hagiwara, M., 2012, November. Mean shift-based SIFT keypoint filtering for region-of-interest determination. In *Soft Computing and Intelligent Systems (SCIS) and 13th International Symposium on Advanced Intelligent Systems (ISIS), 2012 Joint 6th International Conference on* (pp. 266-271). IEEE.
- [12] Gowda, S.N., 2016, September. Innovative enhancement of the Caesar cipher algorithm for cryptography. In *2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Fall)* (pp. 1-4). IEEE.
- [13] Lowe, D.G., 1999. Object recognition from local scale-invariant features. In *Computer vision, 1999. The proceedings of the seventh IEEE international conference on* (Vol. 2, pp. 1150-1157). Ieee.
- [14] Hashmi, M.F., Hambarde, A.R. and Keskar, A.G., 2013, December. Copy move forgery detection using DWT and SIFT features. In *Intelligent Systems Design and Applications (ISDA), 2013 13th International Conference on* (pp. 188-193). IEEE.
- [15] Gowda, S.N., 2016, October. Using Blowfish encryption to enhance security feature of an image. In *2016 6th International Conference on Information Communication and Management (ICICM)* (pp. 126- 129). IEEE.

- [16] Jaber, M., Bebis, G., Hussain, M. and Muhammad, G., 2013, July. Improving the detection and localization of duplicated regions in copy-move image forgery. In *Digital Signal Processing (DSP)*, 2013 18th International Conference on (pp. 1-6). IEEE
- [17] Guo, X., Cao, X., Zhang, J. and Li, X., 2010. Mift: A mirror reflection invariant feature descriptor. *Computer Vision/ACCV 2009*, pp.536-545.
- [18] Gowda, S.N. and Yuan, C., 2020. StegColNet: Steganalysis based on an ensemble colorspace approach. *arXiv preprint arXiv:2002.02413*.
- [19] Fischler, M.A. and Bolles, R.C., 1981. Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. *Communications of the ACM*, 24(6), pp.381-395.
- [20] Christlein, V., Riess, C., Jordan, J., Riess, C. and Angelopoulou, E., 2012. An evaluation of popular copymove forgery detection approaches. *IEEE Transactions on information forensics and security*, 7(6), pp.1841-1854.
- [21] Gowda, S.N. and Sulakhe, S., 2016, April. Block based least significant bit algorithm for image steganography. In *Proceedings of the Annual International Conference on Intelligent Computing, Computer Science & Information Systems, Pattaya* (pp. 16-19).
- [22] Tralic, D., Zupancic, I., Grgic, S. and Grgic, M., 2013, September. CoMoFoDNew database for copy-move forgery detection. In *ELMAR, 2013 55th international symposium* (pp. 49-54). IEEE.
- [23] Gowda, S.N., 2017, July. An intelligent fibonacci approach to image steganography. In *2017 IEEE Region 10 Symposium (TENSYP)* (pp. 1-4). IEEE.
- [24] Lee Rodgers, J. and Nicewander, W.A., 1988. Thirteen ways to look at the correlation coefficient. *The American Statistician*, 42(1), pp.59-66.
- [25] Gowda, S.N., 2016, December. Advanced dual layered encryption for block based approach to image steganography. In *2016 International Conference on Computing, Analytics and Security Trends (CAST)* (pp. 250-254). IEEE.
- [26] Huang, Y., Lu, W., Sun, W. and Long, D., 2011. Improved DCT-based detection of copy-move forgery in images. *Forensic science international*, 206(1), pp.178-184.
- [27] Gowda, S.N. and Vrishabh, D.N., 2017, April. A secure trigonometry based cryptography algorithm. In *2017 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0106-0109). IEEE.