International Journal of Computing and Applications | **ISSN: 0973-5704**
Volume 13, Number 2, (July-December 2018), pp 337-342

OPTIMIZATION OF SUSPECTED REGION IN COPY MOVE FORGERY USING SLIDING BLOCK PROCESSING AND TEMPLATE MATCHING

Binita Pareek[1] and Mohit Saxena[2]

[1-2]Computer Science Department Apex Institute of Engg, & Tech. Sitapura, Jaipur, Rajasthan.
Email: [1]binita.pareek@gmail.com, [2]mohit.saxena234@gmail.com

Abstract: Image processing has played a vital role in every aspect of human life. The digital era is among us, and the evolution of digital pictures is fashioned for photo professionals and the normal photographer distinctly. With the increase in taking pictures and storing snapshots in digital layout, a brand new and uncharted door is open to the world of digital tampering. This article explores copy-move picture forgeries created digitally via surveying the present research carried out in this field. The overall purpose is to enhance naive tamper detection software that extends the current ways and tactics to be had with a forensic analyst. This paper discusses an analysis of image neighbourhood and offers necessary information for the design of tamper detection tools. The proposed approach deploys the sliding window based block processing and normalized cross correlation parameters as the matching coefficient to optimize the searchable portion in a given spatial domain for the possibility of copy move forgery. The retrieved experimental results tested on standard test images given effective results in domain of prevention and detection of image forgery.

Keywords: Image forensic, copy move forgery, cross- correlation, block processing.

1. INTRODUCTION

During the prior decade, powerful desktops, high-decision digital cameras, and sophisticated photo-modifying software packages have emerged as low priced and available to a huge quantity of people. For this reason, it has emerged as particularly straightforward to create digital forgeries that are hard to differentiate from legitimate portraits. These forgeries, if used within the mass media or courts of law, can have a predominant effect on our society. For example, an image taken for the period of the 2003 Iraq War was released on the entrance page of the A.Times[1]. This photo, however, was once no longer reputable: it was created via digitally splicing together two exclusive pictures. The tampering was once discovered through an editor of the Hartford Courant who seen that some similar individuals appeared twice in the image. Although the manipulation appears to be in simple terms meant to toughen the composition of the picture, the photojournalist accountable for it used to be fired. One other high profile case of a forged digital photo that circulated on the web in early 2004 was once a picture depicting Senator John Kerry and actress Jane Fond a sharing a stage at a peace rally towards the Vietnam war1. The photograph made rather have an effect on, as Senator John Kerry was once strolling for President of US and his involvement within the anti-war movement got here beneath attack[2]. This photo was also created using digitally splicing collectively two separate pictures and used to be uncovered as a forgery when the photographer that took one of the customary photos came ahead. These incidents and many others lead us to question the authenticity of the plethora of digital snapshots that we are exposed to every day. Digital pics provide a new method to symbolize pics and scenes that most useful film and a darkroom would provide before.

In early 2004 a British soldier arrested for producing a forged digital photo depicting detainee abuse, however not than a British newspaper ran the holograph on the quilt of one in all its disorders [4]. Figure 1 depicts a sample of image forgery.

(a) (b)

Figure 1: (a) Original Image, (b) Manipulated Image

2. PRIORARTS

First-order operators are a good primary technique to use in photo processing and forgery detection; however 2nd-order operators offer a designated procedure in the detection of picture forgeries. Second-order operators provide an alternative process for detecting what is considered a part, which enables for more robustness. That is true considering that second-order operators furnish significantly betterface localization established on how they calculate the threshold. Alternatively of calculating apart a few pixels wide, and as a consequence posting the quandary of settling on the core of an area, second-order operators try and protect against [5]. Second-order operators use Laplacian and Gaussian features to calculate the convolutions of the image in question. These tactics are strong against quite a lot of photograph degradations, i.e., Noise, on account that of the Gaussian perform [6]. Marr and Hildreth posed this procedure which considers for zero-crossings after convolution with the Laplacian and the Gaussian features. The Marr part detector first performs Gaussian smoothing earlier than convolving the photo with the Laplacian perform [7]. An instance of a Marr aspect detector of order 5 x 5 is given in [8].

This mask incroporates symmetry each horizontally and vertically. That is due to the symmetry of the Gaussian operate which allows for equal steadiness across portions of the Picture being filtered. The vigor of facet detection permits the likelihood of detecting hidden discontinuities, which probably accepted in photograph forgeries [9]. The Marr facet detector follows equivalent symmetry for better dimension matrices of the higher order The following subsection shows a further, however similarly intriguing approaches[10].

The Spectral Analysis approaches use the force of Discrete Fourier Transforms (DFTs) and their capacity to acknowledge brilliance and power levels of a preview. The following system is used to compute the DFT of a given image [11]. Where *f* is the snapshot of measurement M × N represented as a brightness function of each and everypixel.

Lukas analyzed some preliminary test snapshots utilizing the energy of DFTs [12]. This system makes it possible for one to peer areas of the picture that may be manipulated, by means of the amplitude of high frequencies of the image. Dimensional sign, tampering with an area of a image introduces anomalies within the incidence of this sign. If a regional highest within the high-frequency variety is the gift when performing a spectral evaluation, the picture may be a victim of a photo forgery[13]. Farid and Popescu prolong Lukas's spectral evaluation strategy by way of presenting an encouraging method which detects sampling a snapshot [14]. Their processing and filtering the picture in an attempt to obtain high detection accuracy. Entirely analyzing the forgery system and its effect on the victim snapshot enabled Farid and Popescu to boost an entirely customizablemethod[15].

3. BLOCK-BASEDPROCESSING

The spatial processing of processing a given image becomes a hectious task when image size is very big. In such as cases the concept of function handle is usualy deployed to perform a a set of operation for each set of block extracted from a given image. The block processing is usualy deployed in two major pathways[16].

Basically, there are two types of block processing in the field of image processing. First one is the distinct block processing and the second one is the sliding block processing. In the distinct block processing, images are segregated into the multiple blocks and each

one is distinct with respect to another one or we can say that it categorizes distinct blocks that are segregated from the image. It is further considered for processing any sort of image processing operations on the whole image and those operations are being performed by means of the function handle[17].

While in case of sliding block processing, the first of all we define a particular window size for which we want to process block. These are segregated from the image but now the main scenario that deployed in sliding block processing is that blocks are segregated into multiple blocks that exist overlapping between the each particular between the blocks. It can be said that there is region overlap between the consecutive blocks. It means that an element n elements then $n-1$ elements will remain the same that leads to apply an appropriate specific operation on a givenimage[18].

4. TEMPLATE MATCHING

Template matching is conceptually a simple method. We have a template to a photo, where the template is a sub image that contains the form we are looking for. Hence, we center the template on a snapshot factor and depend on what number of points in the template matched these in the photograph. The procedure is repeated for the entire picture, and the factor that resulted in the first-class match, the highest depend on, is deemed to be the point the place the form (given by the template) lies inside thesnapshot[19].

Remember that we want to find the template of a region within the photograph. The template is first placed on the foundation after which matched with the picture to give a rely which reflects how well the template matched that a part of the image at that role. The rely of matching pixels is accelerated by way of one for each factor where the brightness of the template suits the brightness of the photo. That is just like the procedure of template convolution[20]. The change here is that aspects within the image are matched with these in the template, and the sum is of the quantity of matching aspects versus the weighted sum of photography knowledge. The satisfactory suit is when the template is placed on the function the place the rectangle is matched to itself. This process may also be generalized to find, for example, templatesof distinctive size or orientation. In these circumstances, we ought to try the entire templates (at anticipated rotation and size) to examine the high-qualityfit[21].

Formally, template matching may also be outlined as an approach to parameter estimation. The parameters outline the position (and pose) of the template. We can outline a template as a discrete function $T_{x,y}$. This performs values in a window. That is, the coordinates of the aspects $x, y \in W$.

It is observed that these equations are also the solution of the minimization difficulty given by[8],

$$\min e = \sum_{x,\, y \in W} (I_{x+i,\, y+j} - T_{x,\, y})^2 \qquad (1)$$

That is, maximum probability estimation is identical to picking the template position that minimizes the squared error (the squared values of the diversities between the template facets and the corresponding snapshot points). The role the place the template pleasant fits the picture is the estimated position of the template within the photo[22].

The equation depicting the minimal energy on further solving leads to,

$$\begin{aligned} \min e &= \max\{\text{corr}\ (I, T)\} \\ &= \sum_{x,\, y \in W} I_{x+i,\, y+j} \times T_{x,\, y} \end{aligned} \qquad (2)$$

Which is equivalent to Normalized cross correlation being given as[9],

$$\text{NXX} = \frac{\sum_{x,\, y \in W} (I_{x+i,\, y+j} - \bar{I}_{i,\, j})(T_{x,\, y} - \bar{T}_{i,\, j})}{\sqrt{\sum_{y \in W} (I_{x+i,\, y+j} - \bar{I}_{i,\, j})^2 x,}} \qquad (3)$$

A. Proposed Methodology

In this article we target to make an automated system to define a region of suspect using Normalized Cross Correlation coefficient and block processing operation. The distinct and sliding block processing methods are adopted as described below:

1. Consider an input image $I(x, y)$.
2. Segregate $I(x, y)$ into multiple blocks of size wxw using distinct (sliding) block processing method.

3. For each block from distinct (sliding) block, let T(x, y) defines the template.
4. Apply Normalized cross correlation for all the distinct block locations i, j over the image I.
5. Threshold NCC coefficient matrix D(i, j) using a threshold value of .93.
6. Set the intensity values as zero of those D(i, j) location's whose number of match is found less than two and else is set to unity.
7. Mask up input image I(x, y) by multiplying it with D(i, j).

The deployment of step 1 to 7 finally darkens up non suspected region and visualizes only the suspected portion of input image I for possibility of copy move forgery.

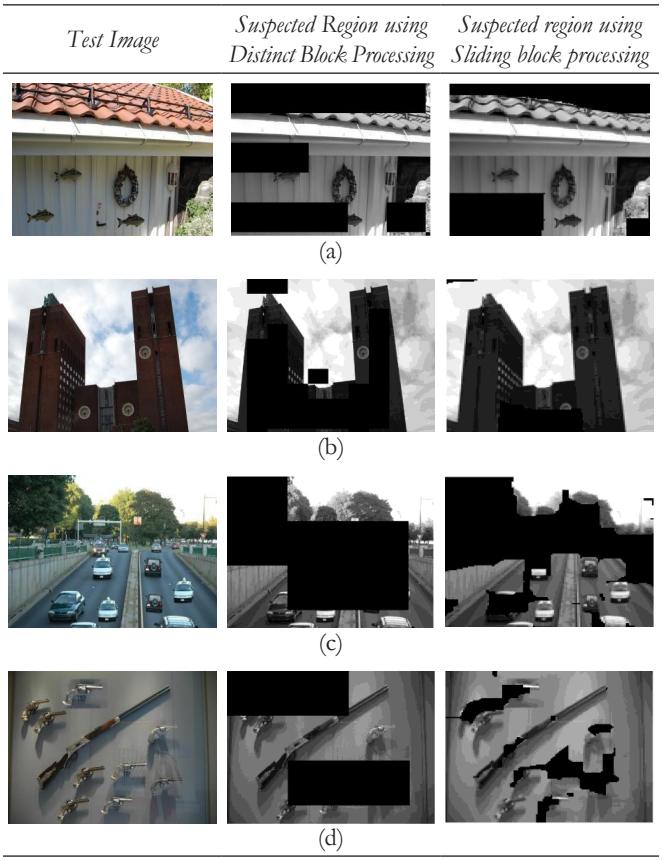

Figure 2: Extraction of optimized region of forgery using distinct and sliding block processing. Three set of test images (a), (b) and (c) are investigated for an automated detection of forged portions. Left most column represent the original image, middle column shows the non-masked region as forged portion and right most shows the non-masked region obtained using sliding block processing operation.

5. EXPERIMENTAL SETUP AND RESULTS

The whole experimentation work is carried out on test image taken from *CoMoFoD* database of image forensics. The simulation implementation of proposed approach is framed in Image Processing Toolbox of Matlab 2013a, operation on a Windows-8 platform, running at 2.3 GHz. In this work test image is divided into multiple sub-blocks using both distinct and sliding window based methods. A part of test image is further investigated for the possibility of its domination in copy move forgery using Normalized Cross Correlation Coefficient. Figure 2 depicts the experimental outcome showing the optimization of suspected portion of test image.

From the table above it is obvious that some part of image is blackened in middle and right most column. These marker positions define the unsuspected region in the input image. In the further step of experimentation the non-mark positions are tested for detection of copy move forgery as shown by Figure 3. It represents the various locations of forgery as evaluated using normalized cross correlation coefficient with a threshold of 0.93.

It is apparent from above results that distinct block processing is lesser efficient to indicate the template location while sliding block processing methodology results to give a relevant view of suspected portions in the input image.

6. CONCLUSION

The digital technologies are highly impacted by various sorts of attacks. In image processing domain there are multiple type of forgeries that can be applied on an image. In this article we have investigated the performance of distinct and sliding block processing approaches so as to optimise the region of search for detection of forgery existing in an image. The experimental results prove that sliding block processing approach is more efficient than distinct block processing to retain the forged locations. Thus it can be concluded that proposed approach for detection of copy move forgery gives enhanced performance and can impart as a vital section in framework of forgery detection. The scale and rotation in variance is most drilling issue that will be focussed in our further research.

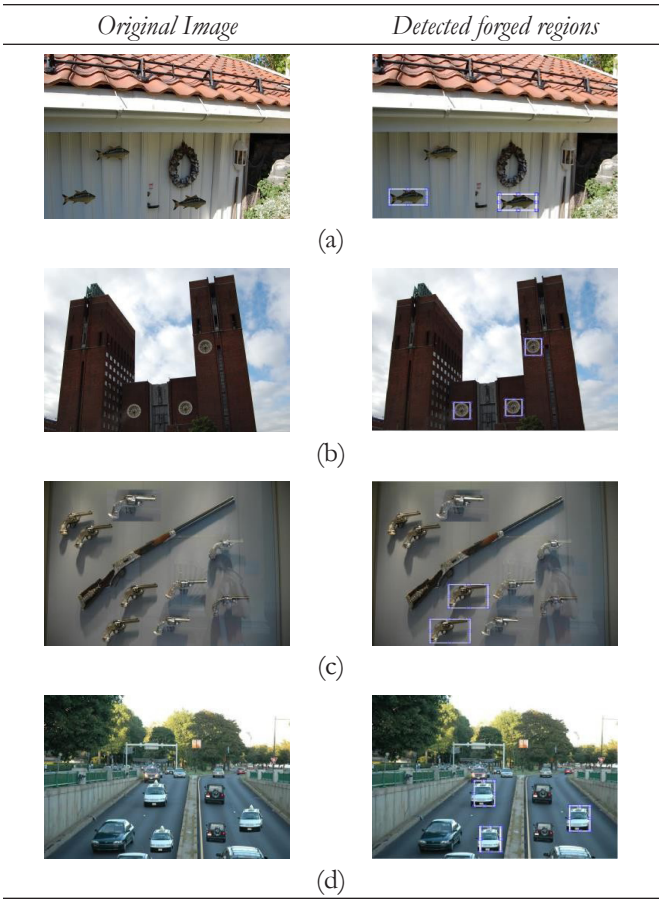

Figure 3: For a set of four test images (a), (b), (c) and (d). Left column represent the original test images and right column show the copy-move forged regions.

References

[1] H. Farid, "Digital doctoring: how to tell the real from the fake," *Significance*, Vol. 3, No. 4, pp. 162–166, 2006.

[2] B. Zhu, M. Swanson, and A. Tewfik, "When seeing isn~t believing [multimedia authentication technologies] ," *IEEE Signal Processing Magazine*, Vol. 21, No. 2, pp. 40–49, 2004.

[3] G.L. Friedman, "Trustworthy digital camera: restoring credibility to the photographic image," *IEEE Transactions on Consumer Electronics*, Vol. 39, No. 4, pp. 905–910, 1993.

[4] P. Blythe and J. Fridrich, "Secure digital camera," in *Proceedings of the Digital Forensic Research Workshop (DFRWS '04)*, pp. 17–19, 2004.

[5] M. Barni and F. Bartolini, *Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications*, Signal Processing and Communications, Marcel Dekker, 2004.

[6] Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Water- Marking and Steganography*, Morgan Kaufmann, San Francisco, Calif, USA, 2nd edition, 2008.

[7] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, pp. 120–126, 1978.

[8] J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Fla, USA, 1st edition, 1996.

[9] H. Farid, "Image forgery detection," *IEEE Signal Processing Magazine*, Vol. 26, No. 2, pp. 16–25, 2009.

[10] T. Van Lanh, K.S. Chong, S. Emmanuel, and M.S. Kankanhalli, "A survey on digital camera image forensic methods," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '07)*, pp. 16–19, July 2007.

[11] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," *Signal Processing: Image Communication*, Vol. 25, No. 6, pp. 389–399, 2010.

[12] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in *Proceedings of the 8th workshop on Multimedia & Security*, S. Voloshynovskiy, J. Dittmann, and J. J. Fridrich, Eds., pp. 48–55, ACM, Geneva, Switzerland, September 2006.

[13] L.T. Van, S. Emmanuel, and M.S. Kankanhalli, "Identifying source cell phone using chromatic aberration," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '07)*, pp. 883– 886, Beijing, China, July 2007.

[14] K.S. Choi, E.Y. Lam, and K.K.Y. Wong, "Automatic source camera identification using the intrinsic lens radial distortion," *Optics Express*, Vol. 14, pp. 11551–11565, 2006.

[15] E. Dirik, H. T. Senear, and N. Memon, "Digital single lens reflex camera identification from traces of sensor dust," *IEEE Transactions on Information Forensics and Security*, Vol. 3, No. 3, pp. 539–552, 2008.

[16] Anil Dada Warbhe, R.V. Dharaskar, V.M. Thakare, Computationally Efficient Digital Image Forensic Method for Image Authentication, Procedia Computer Science, Volume 78, 2016, Pages 464-

470, ISSN 1877-0509,http://dx.doi.org/10.1016/j.procs.2016.02.089.

[17] Alessandro Piva, "AnOverview on Image Forensics," ISRN Signal Processing, Vol. 2013, Article ID 496701, 22 pages, 2013. doi:10.1155/2013/496701.

[18] T.K. Huynh, K.V. Huynh, Thuong Le-Tien and S. C. Nguyen, "A survey on Image Forgery Detection techniques," *The 2015 IEEE RIVF International Conference on Computing & Communication Technologies - Research, Innovation, and Vision for Future (RIVF)*, Can Tho, 2015, pp. 71-76.

[19] Toqeer Mahmood, Tabassam Nawaz, Aun Irtaza, Rehan Ashraf, Mohsin Shah, and Muhammad Tariq Mahmood, "Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images," Mathematical Problems in Engineering, Vol. 2016, Article ID 8713202, 13 pages, 2016. doi:10.1155/2016/8713202.

[20] G. Cao, Y. Zhao, R. Ni and X. Li, "Contrast Enhancement-Based Forensics in Digital Images," in *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 3, pp. 515-525, March 2014. doi:10.1109/TIFS.2014.2300937.

[21] S. Dehnie, T. Sencar and N. Memon, "Digital Image Forensics for Identifying Computer Generated and Digital Camera Images," *2006 International Conference on Image Processing*, Atlanta, GA, 2006, pp. 2313-2316.

[22] Hany Farid, "Image Forgery Detection–A survey", 2009, www.citeseerx.ist.psu.edu,doi=10.1.1.151.8970.