International Journal of Grid and Distributed Computing
Vol. 10, No. 12 (2017), pp.21-30
http://dx.doi.org/10.14257/ijgdc.2017.10.12.03

Studies on the Performance of Image Matching Techniques for IFD Model

K. Asish Vardhan[1], N. Thirupathi Rao[2], J. Anitha[2],
Debnath Bhattacharyya[2] and Tai-hoon Kim[3*]

[1]Department of CS&SE, Andhra University, Visakhapatnam, AP-530 003, India
[2]Department of CSE, Vignan's Institute of Information Technology (A), Visakhapatnam, AP-530 049, India
[3]Department of Convergence Security, Sungshin Women's University, 249-1, Dongseon-dong 3-ga, Seoul 136-742, South Korea
*ashi.mintu@gmail.com {nakkathiru, debnathb, anithanv28}@gmail.com, *taihoonn@daum.net*

Abstract

Advanced pictures are difficult to control and alter since the convenience of capable picture management and changing programming. These days, it is believable to contain or push out very important highlights from a picture without leaving any conspicuous hints of altering. As computerized cameras and camcorders supplant their simple partners, the requirement for verifying advanced pictures, approving their substance, and distinguishing frauds will just increment. Most existing systems to identify such altering are for the most part at the cost of higher computational multifaceted nature. Specifically, the attention was given on recognition of an uncommon kind of computerized phony – the Copy-Move assault in which a piece of the picture is reordered on another part for the most part to cover undesirable bits of the picture. Consequently, the fundamental objective of Copy-Move Forgery Detection (CMFD) is to distinguish duplicate move phonies territories that are same or to a great degree comparative. In CMFD a productive and strong way to deal with recognizes such particular sort of phonies is actualized. This takes after piece based coordinating strategy to recognize frauds in an advanced picture. In the first place, the first picture is separated into settled size squares, clustering the pieces by crossing point region among squares and removing comparable bunches. This strategy may effectively distinguish the fashioned part notwithstanding when the replicated region is improved/modified to blend it with the foundation and when the manufactured picture is spared in a noteworthy realistic document organize, for example, JPEG or PNG.

Keywords*: Images. Image matching, IFD, Forgery Detection*

1. Introduction

Picture processing is a method to improve crude pictures got from cameras/sensors put on satellites, space tests and air ships or pictures taken in typical everyday life for different applications. Different procedures have been produced in Image Processing amid the last four to five decades. A large portion of the strategies are produced for improving pictures got from unmanned shuttles, space tests and military observation flights. Picture Processing frameworks are getting to be noticeably well known because of simple

Received (August 20, 2017), Review Result (November 8, 2017), Accepted (November 14, 2017)
* Corresponding Author

ISSN: 2005-4262 IJGDC

accessibility of capable staff PCs, extensive size memory gadgets, illustrations programming's and so on.

1.1. Image Processing Techniques

The different Image Processing strategies are:

a. **Image representation**- Image portrayal Image characterized in genuine is considered as a capacity f(x,y) where x is number of lines and y is number of segments of the picture. The crossing point of line and section is a pixel.

b. **Image pre-processing**- Image pre-handling Image pre-preparing system is utilized to set up the picture appropriate for the specific application. Picture pre-preparing strategy incorporates scaling, extending, smoothing and so on.

c. **Image enhancement** – Image upgrade – Image upgrade system is utilized to enhance the nature of the picture as pictures got from the different sources like satellites and computerized cameras will contain parcel of commotion. A portion of the upgrade methods are Histogram adjustment, Noise Filtering and so forth.

d. **Image rebuilding** - Image reclamation alludes to evacuation or minimization of debasements in a picture. This incorporates de-obscuring of pictures corrupted by the impediments of a sensor or its condition, commotion sifting, and amendment of geometric contortion or non-linearity because of sensors.

1.2. Introduction to Forgery Detection

Discovery strategy found can be sorted into two ways dynamic technique and inactive strategy. A dynamic location strategy hand-off on the nearness of watermarking or unique mark, which comprises of adding picture points of interest keeping in mind the end goal to portray advanced altering, for example, name, date, signature, and so forth. What's more, requires information about the first picture. While the aloof strategy comprises of distinguishing fabrications or copied questions in pictures without considering the data of the first pictures. The basic Passive falsification systems in computerized pictures can be isolated into three principle gatherings:

- Detect Copy-Paste (*i.e.*, Splicing)
- Detect Image Retouching
- Detect Copy-Move (*i.e.*, Cloning).

Modifying procedure which chips away at controlling the advanced picture by changing its highlights without making detectable adjustments of the substance of the picture. This can be either Technical modifying or Creative correcting. Picture joining then again, make utilization of the first picture with extra pictures to create an altered duplicate, such strategy take a shot at including some piece of different pictures to the first picture so falsifiers cover up or adjust the substance of the picture. Duplicate Move (Image Cloning), which works by replicating an unmistakable piece of a picture and moving it to another piece of a similar picture with the goal that counterfeiter sweep cover up or copy some piece of the picture.

1.3. Copy Move Forgery

One of the particular kind of frauds that should be possible effortlessly by utilizing the devices, for example, Cloning in Photoshop. In this, a piece of the picture itself is reordered into another piece of a similar picture. This is normally performed with the goal to influence a protest “to vanish” from the picture by covering it with a fragment replicated from another piece of the picture. Finished territories, for example, grass,

foliage, rock, or texture with unpredictable examples, are perfect for this reason in light of the fact that the duplicated ranges will probably mix with the foundation and the human eye can't without much of a stretch recognize any suspicious ancient rarities. Since the duplicated parts originate from a similar picture, its commotion segment, shading palette, dynamic range, and most other vital properties will be good with whatever remains of the picture and in this way won't be perceivable utilizing techniques that search for inconsistencies in factual measures in various parts of the picture.

1.4. Copy-Move Forgery Detection (CMFD)

Any Copy-Move falsification presents a relationship between's the first picture section and the stuck one. Duplicate Move Forgery Detection (CMFD) utilizes this sort of connection as a reason for an effective recognition of this kind of phony. Since the phony will probably be spared in the lossy JPEG arrangement and in view of a conceivable utilization of the correct instrument or other confined picture preparing devices, the portions may not coordinate precisely but rather just roughly.

2. Literature Review

Because of the sophisticate altering programming, advanced pictures can be effortlessly controlled and changed without leaving unmistakable pieces of information, accordingly, it represents a genuine social issue in the matter of the amount of their substance can be trusted, regardless of whether it is legitimate or altered particularly as an observer in a court, protection claims and logical misrepresentation. Computerized picture criminology has developed to uncover advanced altering in pictures. There are a few sorts of altering, notwithstanding, covering a few items from regular pictures is a typical type of computerized picture altering, known as duplicate move phony (CMF).It is a particular kind of picture altering, where a piece of the picture is reordered on another piece of a similar picture. With a specific end goal to identify Copy-Move Forgery in a picture we have to comprehend piece based coordinating. To comprehend this, I took the help of paper". A powerful location calculation for duplicate move imitation in computerized images by Yanjun Cao and TiegangGAO".

Since the advanced pictures assume a noteworthy part in rearranging the method for speaking to and exchanging thoughts adaptable with consideration was paid as of late towards examining the appropriate system for investigating and identifying falsification in the computerized pictures. This consideration was because of the most recent malignant exercises in which a solitary protest inside the picture is copied inside a similar picture. Such exercises can be found in the duplicate move imitation that considers a standout amongst the most known action goes for concealing the information. Generally it is conceivable to distinguish the copied protest by registering and contrasting these premises and the entire picture. Be that as it may, new falsification location strategies are as yet missing of avant-garde malignant exercises. The issues and difficulties being tended to in the space of advanced picture falsification are fraud location systems, computerized phonies of social effects, and imitation counteractive action procedures. The advanced frauds have numerous viewpoints and suggestions on social, legitimate, specialized, insight, investigative systems, security, and administrative issues

As needs be it is developing that summed up arrangements and strategies, building institutionalized informational indexes, benchmarks, assessment criteria and so forth are as yet should have been proposed to understand the new systems limiting the odds for advanced imitations. Pictures could be manufactured utilizing diverse systems, and the most well-known fabrication is the duplicate move, in which a district of a picture is copied and put somewhere else in a similar picture. Duplicate Move imitation recognition framework is to recognize such sorts of controls in a computerized picture. Picture legitimacy is essential in numerous social regions. For example, the dependability of

photos has a basic part in courts, where they are utilized as confirmation. In the restorative field, doctors settle on basic choices in light of computerized pictures. It is generally utilized as a part of crime scene investigation for distinguishing altered confirmations in examination. In any case, because of tremendous advancement in innovation one can't just confide in the pictures as confirmation or take choices in view of computerized pictures. By utilizing this, one can without much of a stretch know whether the picture is altered or not and in view of that the picture can be acknowledged as proof.

The primary thought of this paper is to identify duplicate move areas in the given test picture. This can be executed by first choosing the picture and after that the framework utilizes highlight extraction and square coordinating for each piece to identify imitation in the picture.

3. Existing System

The current system uses active techniques such as watermarking or digital signatures to solve the authentication problem in images and to make it free from tampering. Problems with existing system:

The present forgery detection has following failures:

a. This system has limitations because they require human intervention or specially equipped cameras such as Digital cameras with watermarking technology in it.

b. This system also requires the information of the original image to detect forgery in an image.

c. This system depends completely on watermarks and original image information, but by using technically advanced digital photography tools, one can edit, maneuver or tamper the images easily.

3.1. Proposed System

Primarily the system wants details about original image to trace forgery but Copy-Move forgery detection system can detect copy-move type forgery in digital images without any data about the original image and without any watermarks in the image

3.1.1. Improved Copy-Move Forgery Detection

The improved Copy-Move Forgery detection works based on block matching technique which is one of the passive techniques of forgery detection. In this PERFECT Match algorithm is implemented to detect tampering in digital images. In this method First the image as taken as input for the system and the image is then converted into color palette. Then the whole image is decomposed into N BY N blocks. Then these blocks are ordered by their pixel values. From this those blocks with small color difference are extracted. Those are clustered based on the intersection area. Then filter out all the small clusters. Now by checking the distance between the twin clusters we can detect the copy move regions in the image because the tampered image will have same distance between any twin clusters points. So based on this is all the points have same distance then that region can be detected as copy-move region and a box will be drawn covering the copy and moved regions in that image.

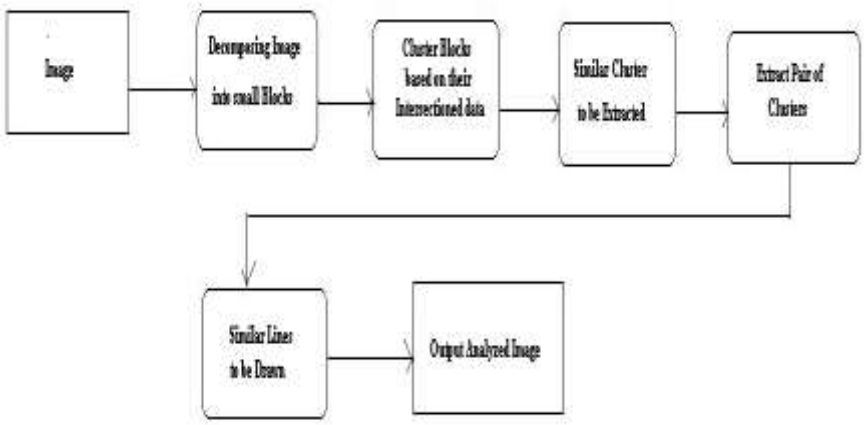

Figure 1. Methodology Adopted

3.1.2. Perfect Match Algorithm

This strategy begins with separating the picture into a few pieces by utilizing a window of specific size and moving it by one pixel along the picture. The pixel esteems for each square and put away them into an exhibit. At that point those qualities are arranged lexicographically to locate the comparative sections in the columns of the framework. At that point, this arranged network is utilized to locate the produced locales.

Perfect Match algorithm is as follows,

1. To eliminate the details of the image the whole image is first blurred. This can be done by applying image Filters. By this all the details about the image can be eliminated which helps in detection of forged regions in the image.

Figure 2. Image to be Given as Input

2. Then the image is converted into degraded palette where the whole picture is converted into small pixels of colors palette.

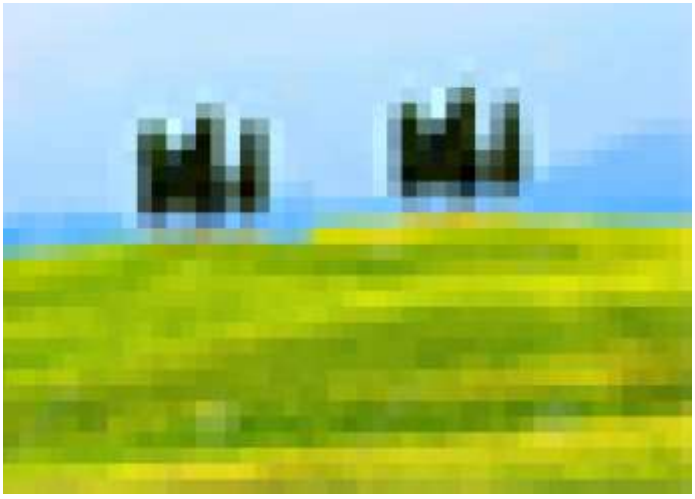

Figure 3. Image Converted to Small Pixels of Data

3. A square of size b x b is slid beginning structure upper left corner of picture w x h to one side and down until the point when it achieves the base right corner on the picture. For each piece slid position in the picture, remove the best column and base line pixel esteems inside the square and store it in a cluster A. The exhibit would have 2b segments and (w – b + 1) x (h – b + 1) rows. Then the every one of the squares which is put away in a cluster are requested in light of the pixel esteems.

4. From the sorted array all the blocks are compared with each other and those adjacent blocks which are having very small absolute color difference between them are extracted. And those are clustered into clusters by computing the intersection area between each block.

5. Thus based in the clusters formed by intersection area twin clusters can be found and by which we can eliminate non identical twin clusters as they have low intersection area between them. Thus by which we can get only twin clusters in the whole image.

6. From the identical twin cluster only similar clusters are extracted by calculating the distance between each point in a twin cluster. There are various ways for calculating the distance. We will use Hausdorff distance to measure the distance between each point. Given two finite points sets $A=\{a_1,a_2,a_3,a_4.....,a_p\}$ and $B=\{b_1,b_2,b_3,b_4.....b_q\}$ then Hausdorff distance can be defined as

$$H(A, B) = \max (h(A, B), h(B,A))$$

Where

$$H(A, B) = \max_{a\in A} \min_{b\in B} \| a- b\|$$

H(A, B) is called directed Hausdorff distance from A to B. It identifies the point that is farthest from any point in B and measures the distance from A to its nearest neighbor in B using || ||. Intuitively, if h (A,B) = d, then each point of A must be within distance d of some point of B and vice versa. So based on this if distance between all points in a twin clusters are same then those clusters are extracted for set of all identical twin clusters.

7. After extracting all exact identical clusters mark them on the image to show them as output, and tampered areas in the image. This can be done by coloring each pixel with a color and drawing a box surrounding the identical regions in the image.

4. System Design and Results

Design Guide:

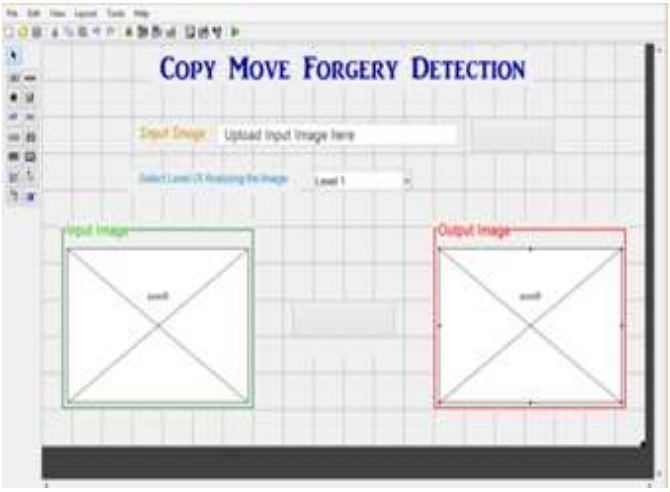

Figure 4. GUI Interface

The above diagram is the model picture of the designed model for the identification of the forged regions in the set of images or individual images to be loaded in to the proposed model system. The user interface for the users who ever using the current system, there is an interface should be required for the further processing of the images. Hence, the above model can be taken or treated as the user interface for the proposed model system.

After Design

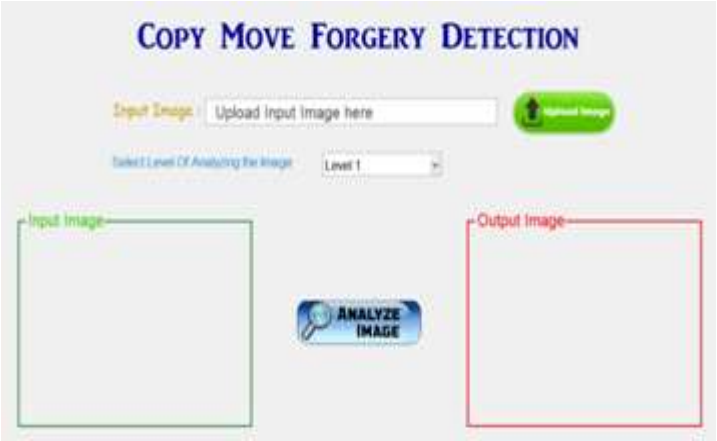

Figure 5. After Design

The above diagram is the model picture of the designed model for the identification of the forged regions in the set of images or individual images to be loaded in to the proposed model system. In the current above image, the users will get an option to upload the images which he would like to verify the regions where were being forged by intentionally or by mistake. Also, the system model is having various levels from level 1 to level 4 for the seriousness and the types of the images that we are going to upload to the proposed system for verification. The output image for the further verification and processing can be viewed in the above screenshot of the proposed model.

Welcome screen:

This screen allows the user to start his/her interaction with the CMFD (Copy Move Forgery Detection) system. This screen has an option to upload an image which will be the input image for the system.

Figure 6. Starting Page of the Proposed Model

After Clicking On the Upload Button:

After clicking on the upload button in the welcome screen a dialog box will appear where the user has to browse and select the input image.

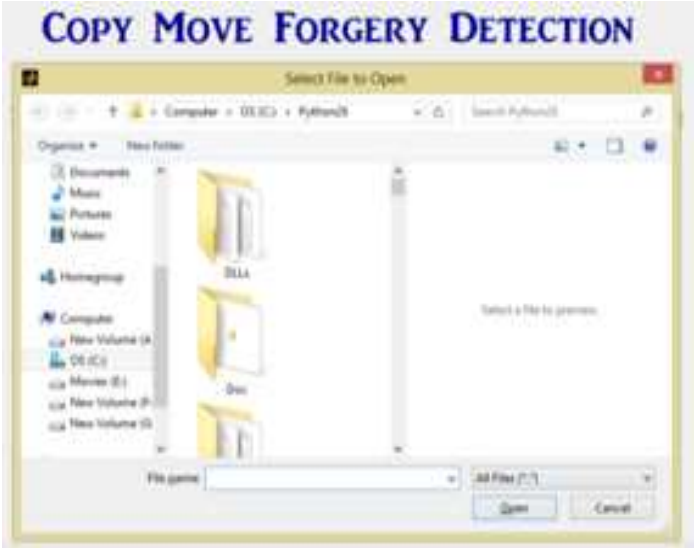

Figure 7. Selection of Files from the Computer for Uploading Images

Selecting level of Analyzing:

There are three levels of analyzing the input image which are Level 1, Level 2 and Level 3 from which the user has to select one and based on that, the process of analyzing the image will be carried out to find the tampering in image,

Figure 8. Selection of Levels for Images

After analyzing the image:

Once if analyzing of input image is finished an output image is displayed under output image label, which shows the detected copy move regions in the given image. This is result screen and if the user wants to analyze the image again he/she can change the Level of analyzing and can analyze the image again or can simply upload an image again using upload button.

Figure 9. Output Results Page after Analyzing the Input Images

Table 1. Comparison Analysis

S.No	Test Cases	Robust Match	Perfect Match
1	Case-1	75%	78%
2	Case-2	85%	91%
3	Case-3	75%	81%
4	Case-4	75%	82%

In the analysis and testing of the proposed method, we had considered the four test cases and the results were observed with the percentage of the match. The first case that we had considered was the “whether working for textured areas such as sky”. The second case for testing the proposed system was considered was “whether image was in the given or accepted format or not”. The third case for testing the proposed system considered was the “whether proposed model was working for the Big areas or not”. And the fourth case considered was the “whether proposed model was working for the small regions on the image or not”.

5. Conclusion

The technique proposed in the current article by which the client can recognize duplicate move sort falsifications finished with the expectation to hide certain subtle elements or to copy certain parts of a picture. The proposed technique can recognize duplicate move areas in a picture with no learning about the first picture and with no watermarks in the picture. Essentially, the undertaking is separated into four phases; each relates to the indentified venture goals. These stages were successively executed since the consequence of the past stage is utilized as a part of the following stages. The proposed strategy depends on square coordinating idea where the picture is isolated into pieces. Subsequently, this proposed conspire is successful and productive in distinguishing the cloned areas in a picture.

References

[1] J. Fridrich, "Methods for Methods for Tamper Detection in Digital Images", in proceedings of the ACM Workshop on Multimedia and Security, Orlando, FL, **(2009)**, pp. 19−23.
[2] N. Memon, "An efficient and robust method for detecting copy-move forgery", In Proceedings of the ICASSP09; **(2009)**.
[3] A. Swaminathan and M. Wu, "Robust scanner identification based on noise features", in Proceedings of the Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, CA, USA, vol. 6505, **(2007)**, pp. 65050S.
[4] N. Khanna and E. Delp, "Source Scanner Identification for Scanned Documents", IEEE International Workshop on Information Forensics and Security - WIFS, **(2009)**.
[5] P. Chiang, N. Khanna, A. Mikkilineni, M. Segovia, J. Allebach, G. Chiu and E. Delp , "Printer and Scanner Forensics: Models and Methods", Intelligent Multimedia Analysis for Security Applications, Studies in Computational Intelligence, vol.282, **(2010)**, pp 145-187.
[6] A. Mikkilineni, "Scanner identification using sensor pattern noise", in Proceedings of the Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, CA, USA, vol. 6505, **(2007)**, p. 65051K.
[7] N. Khanna, "Scanner Identification Using Feature-Based Processing and Analysis", IEEE Transactions on Information Forensics and Security, vol. 4, no. 1, **(2009)**, pp.123-139.
[8] N. Khann, "Scanner Identification with Extension to Forgery Detection", Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, vol. 6819, **(2008)**, pp. 68190G-68190G-10.
[9] N. Khanna, "Forensic techniques for classifying scanner, computer generated and digital camera images", In Proceedings of the IEEE international conference on acoustics, speech and signal processing, Las Vegas, NV, **(2008)** , pp 1653–1656.

