Performance Evaluation of Distance Metric for Copy Move Forgery Detection

Sudhakar K
Research Scholar, E.C.E Department
J.N.T.U.Hyderabad
Hyderabad – 500085, Telangana State, India
sudhakar.kallur@gmail.com

Dr.Subhash Kulkarni
Professor and Principal
PESIT – Bangalore South Campus
Bengaluru 560100, Karnataka State, India
sskul@pes.edu

***Abstract*— This paper presents the performance evaluation of various distance metric in copy move forger detection algorithms. The choice of distance metric affects the detection speed. The proposed approach is tested over 9 different distance metrics. The experimental results found indicate the choice of distance metric has a considerable impact on forgery detection speed**

Keywords- Image forgery; Distance metric; DCT; CMFD; Overlapping; Splicing.

I. INTRODUCTION

As the technology evolves day by day it is helping the mankind to develop humans in all dimensions and making the human species most talented animal on this planet. This is one side of the coin, On the controary the same technology pushes humans to the depth of ocean as in image forgery. When digital camera was introduced in the market everyone enjoyed the technology with obvious advantages of these digital cameras over traditional film based cameras. But the same digital images are becoming victim for image manipulation. There is need to test the legitimacy of images before using for applications.

The digital image forgeries are classified in two categories: a) Copy Move Forgery (CMF) ii) Image splicing

The CMF is a method in which the some region of image is copied and pasted with or without modifications on the same image. The fig.1 shows the example of copy move forgery

a) Original Image b) Forged Image

Fig 1: Copy move forgery Example

The forged version of fig.1a is created by copying the 'lady' (image object) and pasted on the same image as shown in fig 1b. Unlike CMF, in image splicing the forged image is shaped by pasting the image region which is copied from other image convey the misinformation to the user [4]. Fig. 2 shows the example for splice forgery [1]. In July 2010, a Malaysian politician Jeffrey Wong Su En claimed that he had been presented Knighthood by the Queen Elizabeth II, in recognition to his contribution to the international aid organization Médecins Sans Frontières. He even circulated a picture in the local media (fig. 2.a) along with his statement, that he had been knighted. When enquired with the British High Commission in Kuala Lumpur, it made clear that the name of Mr. Wong was not part of the official knighthood recipients lists. The commission even had stated that the picture was inconsistent with the normal protocol adopted for knighthood ceremonies. The image was finally shown to be a splicing between an original ceremony photo (fig. 2b) and Mr. Wong's face, built to increase his popularity.

Fig. 2 a) Spliced Image b) Original Image

Many researchers have proposed the different types of forgery detection algorithms, the following two steps are most of the algorithms associate with two major steps

a) Extraction of Features.
b) Feature Similarity Matching.

a) Extraction of Features: In this stage the unique features of given image is extracted. Many approaches are used for extraction of features such as Moments based approaches, Intensity based approaches, Frequency based approaches, Keypoints based approaches and Dimensionality reduction approaches [2]

b) Feature Matching: After extraction of the features, feature matching is performed for detection of forgery. The degree of similarity between the features vectors, confirms the image forgery.

The algorithms in copy move forgery detection (CMFD) use distance metric for features similarity matching. The similarity is calculated by calculating the distance between two sets of features vectors. The set of feature vectors corresponds to forged regions if they are adequately similar i.e. the distance between the feature vectors is below a specified threshold. The threshold value depends on the type of image. Many CMFD algorithms use the Euclidian distance as distance metric for calculation of distance between feature vectors [4].

Here in this work we have experimented for suitable distance metric that improves the detection speed. The effect of distance metric over CMFD algorithms is analyzed by evaluating the DCT approach of copy move forgery detection over 9 different distance metric.

The paper is arranged as follows. Section II presents literature survey. In Section III we discuss different distance metrics commonly preferred and forgery detection using DCT approach. Section IV presents the results and observations of proposed method tested on various images. And finally conclusion is presented in section V.

II LITERATURE SURVEY

During the feature vector matching process the algorithm searches nearest or approximate nearest neighbor [4]. This suggests proper selection of distance metric that greatly affects the detection speed of CMFD algorithm.

Many researchers use Euclidian distance for similarity matching. Wang et al [5], utilizes element by element comparison method for similarity matching of feature vectors. Moussa proposed the use of sum of absolute difference for similarity matching process. Malviya and Ladhake [6], [7], [8] proposed the usage of Manhattan distance as a substitute to Euclidean distance for similarity matching between pair feature vectors. Bi and Pun [9] had shown the usage of squared Euclidian distance instead of normal Euclidian distance. The shift frequency threshold based similarity matching was used by the Harjito and Prasetyo[10]. Muzaffer and Ulutas[11] performed the similarly matching by using hashing, hamming distance between hashed features. Sharma and Ghanekar [12] combined the threshold of shift frequency and Euclidian distance for comparison and matching between pairs of descriptors [4].

III FEATURE EXTRACTION AND DISTANCE METRICS

The selection of distance metric is evaluated over the Discrete Cosine Transform (DCT) approach of CMFD algorithm. The DCT approach is frequency depend approach [5][3]. Some of the advantages of the DCT over other methods of detection are as follows.

- DCT shows a high recall, in large noise environment.
- For small variations in the image, the DCT achieves best recall.
- DCT performs better compared to other block based approaches with respect to precision[5] [3] .

The DCT approach of forgery detection is very simple for implementation. The algorithmic steps in DCT method of forgery detection as follows

- The image is pre-processed.
- The image is divided into overlapping blocks. The size of each block is b x b
- Apply DCT to each block and sort the features in lexicographic order
- Search for similar pairs of blocks using feature vectors
- Output the duplicated regions if any

The first step, the color input image of size $U \times V$ is converted into gray scale image using the following equation

$$S = 0.229R + 0.587G + 0.114B \qquad (1)$$

where R, G, and B are the red, green, and blue components of image S, respectively. After conversion of image S into a grayscale image, a window of size $u \times v$ is slided from the top left corner to the bottom lower right corner. This results into overlapping blocks. Each block is represented as K_{pq}, where p and q are the starting points of the block's row and column, respectively

$$K_{pq} = f(x + q, y + p) \qquad (2)$$

where $x,y \in \{0, \dots, K_{pq} - 1\}$, $p \in \{1, \dots, U - v + 1\}$, and $q \in \{1, \dots, V - v + 1\}$.

In pre processing stage the image (U X V) is arranged into overlapping blocks of size $u \times v$. the division results into total 'N' number of blocks. Where 'N' is given by

$$N = (U - u + 1) \times (V - v + 1) \qquad (3)$$

After dividing image in the blocks $K_{pq}(x, y)$ of size $u \times v$, where x, y are 0, 1, 2, . . . , $N - 1$, we decompose the block $K_{pq}(x, y)$ in terms of 2D DCT basis function.

The result occurs in the form of a coefficients matrix $\overline{T}(a,b)$ of size $u \times v$ that contains the DCT coefficients as shown below

$$\overline{T}(a,b) = \alpha_a \alpha_b \sum_{x=0}^{u-1} \sum_{h=0}^{v-1} A_{uv} \cos\frac{\pi(2x+1)a}{2u} \cos\frac{\pi(2y+1)}{2v} \qquad (4)$$

$$0 \le a \le u-1, \; 0 \le b \le v-1$$

$$\text{where } \alpha_a = \begin{cases} 1/\sqrt{u}, a = 0 \\ \sqrt{2/u}, 1 \le a \le u-1 \end{cases} \qquad \alpha_q = \begin{cases} 1/\sqrt{v}, b = 0 \\ \sqrt{2/v}, 1 \le b \le v-1 \end{cases}$$

The DCT coefficients are sorted in lexicographical order and the similarity matching is done with the use of Euclidian distance metric. If any two blocks shows the minimum distance, those two blocks are forged blocks.

The success of such algorithms mainly depends on the accuracy of feature extraction and matching process. In the literature many efficient feature extraction methods have been proposed over the time. Unlike the feature extraction methods the feature matching methods are not evolved over the time. In this paper the effect of distance metric selection in copy mover forgery detection is analyzed over 9 different distance metrics. These distance metrics are Braycurtis, Canberra, Chebyshev, Cityblock, Euclidian, Square Euclidian, , minkowski (p=1), minkowski (p=2), minkowski (p=3).

Before proceeding further, let ‘e’ and ‘f’ are the 2 one dimensional arrays. The equations of different distance *Z(e,f)* metrics is as shown below[15].

i) Braycurtis Distance

Braycurtis is defined as follows

$$Z(e,f) = \sum |e_i - f_i| \Big/ \sum |e_i + f_i| \quad (5)$$

ii) Canberra Distance

The Canberra distance is defined as

$$Z(e,f) = \sum_i \frac{|e_i - f_i|}{|e_i| + |f_i|} \quad (6)$$

iii) Chebyshev Distance

Computes the Chebyshev distance between two 1-D arrays *e* and *f*, which is defined as

$$Z(e,f) = \max_i |e_i - f_i| \quad (7)$$

iv) Cityblock Distance:

It is the popular distance metric in computer vision applications after Euclidian distance. The distance between two 1d arrays e and f is defined as below

$$Z(e,f) = \sum_i |e_i - f_i| \quad (8)$$

v) Euclidian Distance

It is defined as follows

$$Z(e,f) = (\sum (w_i |(e_i - f_i)|^2))^{1/2} \quad (9)$$

vi) Square Euclidian Distance

It is defined as follows

$$Z(e,f) = (\sum (w_i |(e_i - f_i)|^2)) \quad (6)$$

vii) Minkowski Distance

The Minkowski distance between 1-D arrays *e* and *f*, is defined as

$$\|e - f\|_p = (\sum |e_i - f_i|^p)^{1/p} \quad (10)$$

IV RESULTS AND DISCUSSION

For evaluation purpose the CoMoFoD data set is used. It includes 260 forged image sets in two categories [13](small 512x512, and large (3000x2000). Images are categorized in 5 categories as per applied manipulation such as translation, rotation, scaling, combination and distortion. Other post processing methods, such as JPEG compression, blurring, noise adding, color reduction etc., are applied to all forged and original images. This data set is hosted on https://www.vcl.fer.hr/comofod/. The hardware system used for the computational purpose has the following specifications: HP computer with Processor Intel core i3 with 2.00 GHZ and 4GB RAM and Windows 10 64 bit as operating system. MATLAB version used is 2018a for programming and experimentation. Google Colab with tensor flow version 2.3.1 is also used in our experimentation.

The fig 3 shows the sample of images of CoMoFoD dataset[13]. The sample of image consists both intensity oriented images and patter oriented images.

Image a Image b Image c
Image d Image e Image f
Image g Image h Image i
Image j Image k Image l

Fig 3: sample images of CoMoFoD dataset

The CMFD was performed for the above image dataset over different distance metrics. The results are tabulated in Table 1. The table 1 shows the time required for detection phase over different distance metrics. After careful analysis of Table 1 it shows that the chebyshev distance requires minimum time for similarity checking as compared with the other distance metrics. It is proven with the fig. 4 which shows the time required for similarity matching over different distance metrics for the set of 12 images. The chebyshev distance metric indicates minimum time used amongst other distance metrics.

The accuracy of forgery detection algorithm is governed by feature extraction algorithm and it is found that choice of distance metric has no major impact on detection accuracy. It can infer that the distance metric influences the detection speed and a proper choice influences the feature matching time

Table1; Detection time for different images over different distance metrics (time in seconds)

Distance	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Image 7	Image 8	Image 9	Image 10	Image 11	Image 12
Braycurtis	35.8	38.99	37.48	38.55	34.58	39.41	37.53	36.76	35.42	38.31	37.25	34.29
Canberra	78.66	74.28	64.63	65.25	66.18	78.02	80.1	63.03	63.2	64.22	63.49	64.27
Chebyshev	22.78	18.19	17.85	18.23	17.77	18.29	17.95	17.5	18.89	19.28	18.07	18.25
Cityblock	24.62	19.34	19.29	18.87	18.73	19.29	19.16	18.7	19.15	18.82	19.23	18.66
Eucledian	32.05	24.22	28.15	29.39	29.91	25.73	24.84	29.69	27.9	28.36	29.1	30.33
Sqeucledian	28.73	25.53	26.06	26.41	28.41	27.04	25.97	24.88	24.97	26.01	25.42	27.65
Minkowski(p=1)	49.37	44.87	40.71	41.15	41.24	40.62	41.06	40.28	41.11	43.11	42.01	40.95
Minkowski(p=2)	29.09	28.42	28.26	30.55	31.22	29.35	28	30.51	30.53	27.66	27.96	26.8
Minkowski(p=3)	57.28	53.13	56.58	59.07	52.28	58.76	53.11	53.25	59	57.32	56.86	55.28

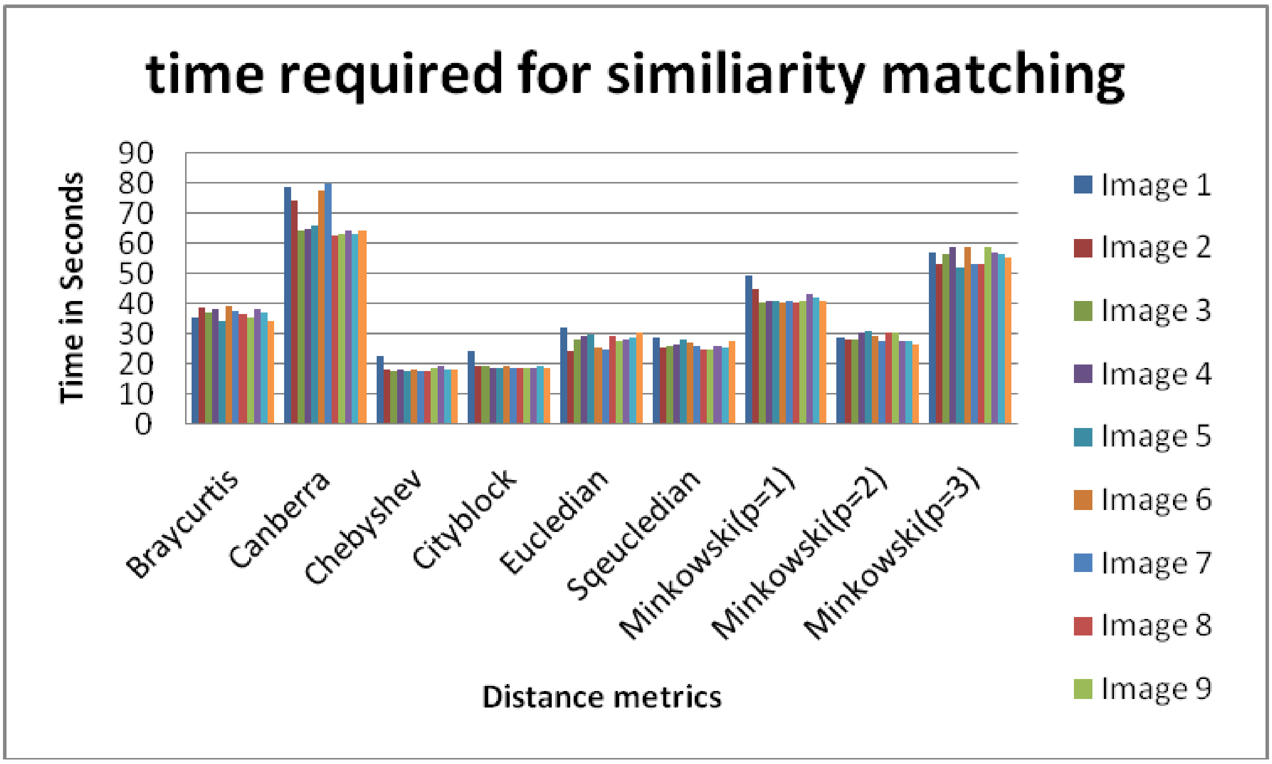

Fig. 4. Plot of time required for similarity matching over different distance metric

V CONCLUSION

The success of CMFD algorithms mainly depends on the Feature extraction stage and feature matching stage. The selection of distance metric greatly affects the detection time. With the proper selection distance metric the detection is improved. Future work will be optimization of color space for improvement of accuracy.

REFERENCES

[1] Judith A Redi, Wiem Taktak, Jean-Luc Dugelay, Digital image forensics: a booklet for begineers, Multimedia Tools Applications., vol. 51, no. 1, pp.133162, Jan. 2011.

[2] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess,and Elli Angelopoulou, An Evaluation of Popular Copy-Move Forgery Detection Approaches,IEEE Transactions on Information Forensics And Security, 7(6), pp 1841-1854 Dec 2012.

[3]H. Farid, Asurvey of image forgery detection, Signal Process. Mag.,26(2), pp. 16-25, Mar. 2009.

[4] S. Teerakanok and T. Uehara, "Copy-Move Forgery Detection: A State-of-the-Art Technical Review and Analysis," in *IEEE Access*, vol. 7, pp. 40550-40568, 2019, doi: 10.1109/ACCESS.2019.2907316.

[5] Y. Wang, L. Tian, and C. Li, “LBP-SVD Based Copy Move Forgery Detection Algorithm,” in Proc. ISM, Taichung, Taiwan, pp. 553–556, 2017.

[6] A. V. Malviya and S. A. Ladhake, “Copy move forgery detection using low complexity feature extraction,” in Proc. UPCON, Allahabad, pp. 1–5, India, 2015.

[7] A. V. Malviya and S. A. Ladhake, “Pixel Based Image Forensic Technique for Copy-move Forgery Detection Using Auto Color Correlogram,” Procedia Comput. Sci., vol. 79, pp. 383–390, 2016.

[8] M. Barile, "Taxicab Metric," [Online]. Available: https://home - pages.inf.ed.ac.uk/rbf/HIPR2/hough.html, Accessed on: Dec. 17, 2020.

[9] X. Bi and C. M. Pun, “Fast reflective offset-guided searching method for copy-move forgery detection,” Inf. Sci. (Ny)., vol. 418–419, pp. 531–545, 2017.

[10] B. Harjito and H. Prasetyo, “Passive Copy-Move Forgery Detection Using Halftoning-based Block Truncation Coding Feature,” J. Phys. Conf. Ser.,vol. 855, p. 012016, Jun. 2017.

[11] G. Muzaffer and G. Ulutas, “A fast and effective digital image copy move forgery detection with binarized SIFT,” in Proc. TSP, Barcelona, Spain, pp. 595–598, 2017.

[12] S. Sharma and U. Ghanekar, “A Rotationally Invariant Texture Descriptor to Detect Copy Move Forgery in Medical Images,” in Proc. CICT, Ghaziabad, India, pp. 795–798, 2015.

[13] Tralic D., Zupancic I., Grgic S., Grgic M., "CoMoFoD - New Database for Copy-Move Forgery Detection", in Proc. 55th International Symposium ELMAR-2013, pp. 49-54, September 2013.

[14] Sudhakar. K, Sandeep V M, Subhash Kulkarni “Shape Based Copy Move Forgery Detection Using Level Set Approach”, Proc. Fifth International Conference on Signal and Image Processing, pp 213-217, 2014.

[15] The SciPy community, “Distance Computations (scipy.spatial.distance)”, [Online]. Available: https://scipy.github.io/devdocs/spatial.distance.html, accessed on Dec 18, 2020.

[16] K. Sudhakar, V. M. Sandeep and S. Kulkarni, "Speeding-up SIFT based copy move forgery detection using level set approach," 2014 International Conference on Advances in Electronics Computers and Communications, Bangalore, pp. 1-6, 2014, doi: 10.1109/ICAECC.2014.7002407.

[17] K. Sudhakar, V. M. Sandeep and S. Kulkarni, "Redundant sift features via level sets for fast copy move forgery detection," 2016 International Conference on Signal and Information Processing (IConSIP), Vishnupuri, pp. 1-4, 2016, doi: 10.1109/ICONSIP.2016.7857475.