International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Blind Image Forgery Detection by using DCT and SURF Based Algorithm

Kavita Rathi, Parvinder Singh

Abstract*: A remarkable array of visual images surrounds us. Image forgery by using digital technology has eroded confidence in the integrity of imagery. Image forensics is an aid to re-establish the trust and originality of imagery. It is important to identify the type of forgery for application of relevant image forensic technique for optimal output. Based on the availability of the original image, image forensic algorithms are classified in the blind and non-blind algorithms. But the availability of original imagery is not always necessary for all the cases of image tampering. The blind forgery detection is particularly difficult. Key point scheme is introduced instead of block based Discrete Cosine Transformation (DCT) and after the validation, the state of the art blind image forgery techniques, i.e., DCT and proposed Speeded-Up Robust-Features (SURF) algorithms are evaluated. Average Accuracy, True Positive Rate (TPR), and True Negative Rate (TNR) are used as parameters for performance evaluation on various images. Experimental results concluded the efficiency of SURF scheme in dealing with region rotation manipulations. The paper concluded with the efficiency of the key-point based scheme.

Keywords* : Blind Image Forgery, DCT quantization, Image Forensics, Key-point, SURF

I. INTRODUCTION

Image forensics aims at the detection of image tampering detection and authentication of its originality [1]. Passive (Blind) forgery detection techniques assess the authenticity and integrity of an image without the presence of any watermark/signature of originality from the sender [2]. Blind forgery detection techniques primarily work on assumption that even though virtual forgeries may have no visual clues of having been tampered with, the forgeries actually disturb the underlying records; and the forgeries disturb the assets and consistency of a pure image and introduce new artefacts ensuing in various inconsistencies. These inconsistencies become the lead to detect the forgery. This approach is popular known as blind forgery detection as it doesn't need any prior data of images. Existing strategies and knowledge of identification of diverse strains of tampering is used to locate tempering one by one with localization of tampered vicinity.

There exist a large number of tempered images. One such famous example of image tampering, which was published in Egyptian news daily, is presented in Figure 1 (a) showing the tampered image, however, the originally clicked photograph is presented in Figure 1 (b).

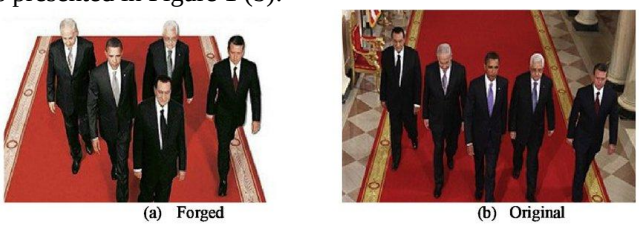

Figure 1 A Famous example of image forgery [3]

There are many image forgery detection algorithms, but the efficiency of such algorithms is very low and high False Positives (FP) ratios. A high of FP ratios can affect tampering detection based decisions. The main algorithms for blind forgery detection use Joint Photographic Experts Group (JPEG) quantization under Discrete Cosine Transformation (DCT) schemes and Key-point based algorithms, for example, Speeded-Up Robust-Features (SURF) algorithms. The introduction of key point scheme with Discrete Cosine Transformation (DCT) is yet to be tested. The present paper is the introduction of the key point scheme with DCT and SURF algorithms, which are two state of the art blind image forgery techniques.

II. RELATED WORKS

A neighbourhood-based approach using quantized DCT vectors as attributes is proposed in [4]. Its improved version is proposed in [5] by using only low energy DCT vectors computed for every part. In these algorithms, similar regions are made on the brink of one another by coefficients of DCT parts and the shift coefficients for matching. The DCT vectors are capable of handling compression, noise and retouching but could not detect copied parts with rotated and scaled attributes. The Discrete Wavelet Transformations (DWT) algorithm is also useful in the detection of copy-move forgery. The DWT vectors by using wavelet transformations are extracted in [6] while the Fourier transformations have been used to calculate attributes and are proved to be scale-invariant [7]. However, features aren't fully rotation invariant also and led to high computational time. The counting bloom filter, which uses approximation bands of DWT, is efficient in comparison to lexicographical sorting for reduction of matching time [8].

Manuscript published on January 30, 2020.
* Correspondence Author
Kavita Rathi*, Department of Computer Science & Engineering, Deenbandhu Chhotu Ram University of Science and Technology Murthal, Sonipat, India. Email:kavita1217@gmail.com
Parvinder Singh, Department of Computer Science & Engineering, Deenbandhu Chhotu Ram University of Science and Technology Murthal, Sonipat, India.

The wavelet transformation sub-bands are partitioned into overlapping parts with and therefore the vectors from sub-band parts are used as attributes. The approach of tempering detection by using the similarity and dissimilarity function on vectors from approximation parts and vectors from detailed parts is robust for compression and rotation based forgeries [8]. Harmonic Transform is useful for extracting attributes with round features [9], however, the Cosine Transform extract attributes from rectangular parts [10]. Furthermore, the Harmonic Transform and Cosine Transform have are numerical stable. The Polar Transform, which is invariant to rotation and scale, is proposed in [11]. The geometric property, which is invariant to scaling and rotation, is shown through translations in log-polar images. The posh transformation is used for mapping the translations within the log-polar domain. Low computational complexity is attributed to the usage of transformations.

III. DCT ALGORITHM

JPEG is most famous and usually used compression which is used in the type of packages. To perceive if an image that was JPEG compressed and now it recompressed after tampering plays a very vital function in photo tampering detection. The DCT method uses the probability estimation devised to estimate which quantization table was used. DCT algorithm exploits the reality that double compression quantities to particular double quantization DCT coefficients. The new and unique artefacts introduced by tempering remain visible in the histogram of DCT coefficient by using Fourier transforms. The algorithm of DCT based image forgery detection is presented in Figure 2.

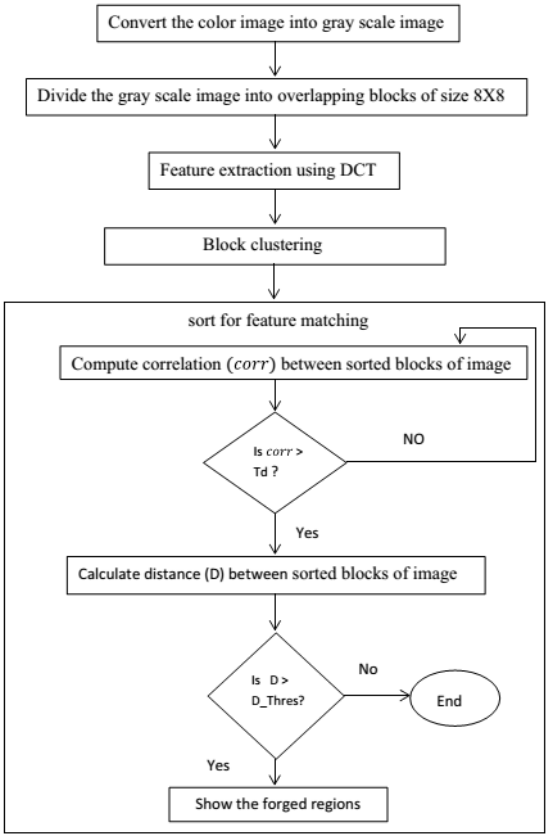

Figure 2 Block diagram of DCT based Image Forgery detection

The flowchart of DCT algorithm for the detection of the image forgery includes

1. The transformation of the RGB image to gray scale image;
2. Divide the image into blocks (overlapping) 8 × 8 blocks;
3. Quantization Based Features extraction using DCT;
4. Apply Block clustering;
5. Apply sorting for matching quantization features;
6. Compute Correlation between sorted blocks; if correlation is greater than the threshold;
7. Mark as forged region, else 6;
8. Calculate distance (D) between sorted blocks of image
9. If distance (D) is greater than threshold distance
10. Show the forged regions, else end.

Segmentation process is used to divide image into 8x8 blocks, image of size MxN the blocks can be calculated using

$$B = (M - b + 1) \times (N - b + 1)$$

the feature extraction for each block B is estimated using

$$X_k = w(k) \sum_{n-0}^{N-1} x_n \cos\left[\frac{(2n+1)\pi k}{2N} \quad k = 0, \ldots\ldots, N-1\right]$$

Where scaling factor w(k) is given as:

$$w(k) = \begin{cases} \sqrt{\frac{1}{N}} & k = 0 \\ \sqrt{\frac{1}{2N}} & 1 \leq k \leq N-1 \end{cases}$$

IV. PROPOSED KEY-POINT BASED SURF ALGORITHM

The SURF based image forgery detection approach uses key-point detector. Key-points are detected by Hessian operator which is based upon Hessian matrix. Instead of DCT, HAAR wavelet transformation is used. The Hessian matrix H(x, s) for x at scale s for a given image point $x = (x, y)$ in the image is defined as

$$H(x, \sigma) = \begin{bmatrix} L_{xx}(x, \sigma) & L_{xy}(x, \sigma) \\ L_{xy}(x, \sigma) & L_{yy}(x, \sigma) \end{bmatrix}$$

where $L_{xx}(x, \sigma)$ is the convolution of the Gaussian second order derivative $\frac{\partial^2}{\partial x^2} g(\sigma)$ with the image I in point x, and similarly for $L_{xy}(x, \sigma)$ and $L_{yy}(x, \sigma)$. Block diagram of proposed SURF based forgery detection algorithm is presented in Figure 3.

The flowchart of the proposed SURF algorithm for the detection of the image forgery includes:

1. Transformation of the RGB image to gray scale image;
2. Calculate Hessian Matrix of gray scale image;
3. Key-point based Feature extraction using SURF;
4. Apply Block clustering;
5. Select strongest matching key-points for matching forgery features;
6. Compute Correlation between key-points;
7. If correlation is greater than the threshold mark as forged region, else 6;
8. Calculate distance (D) between sorted blocks of image
9. If distance (D) is greater than threshold distance

10. Show the forged regions, else end.

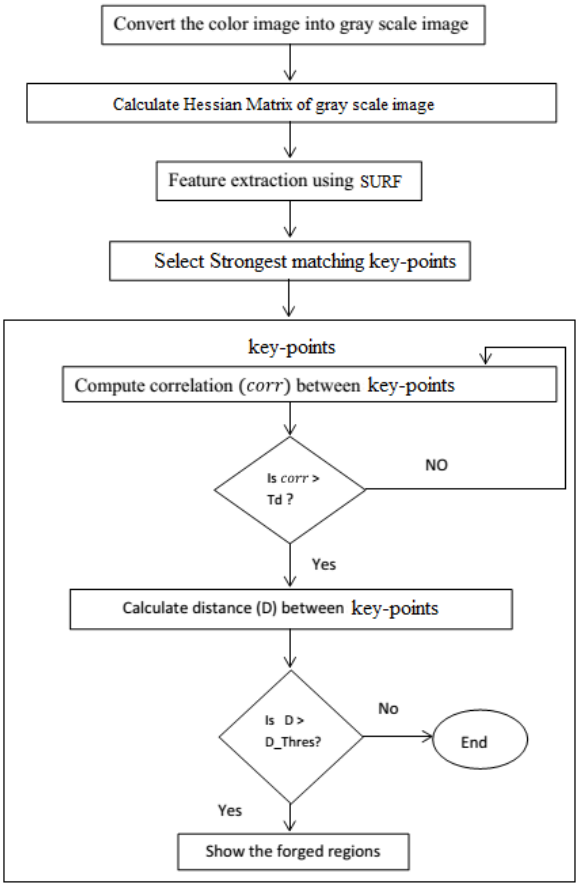

Figure 3: Block diagram of Proposed SURF based forgery detection algorithm

V. EXPERIMENTAL ANALYSIS

An Intel Core i3 Central Processing Unit having 8 Giga Bite Random Access Memory and operating system raring at 2.4 Giga Hertz by using Windows 7 and 64 bit Operating System is used for executing the proposed methodology. The proposed methodology is implemented in MATLAB. Average Accuracy, True Positive Rate (TPR), and True Negative Rate (TNR) are used as parameters for performance evaluation on various images. For experimental analysis a large number of images were considered for the evaluation. Afterwards average of each examining parameter was calculated and presented in Table 1 and in Figure 4, which present the Average Accuracy, TPR and TNR rates for block based DCT and SURF algorithms, and clearly indicated improvement by using key-point based method in the existing algorithms.

Table 1 Average Accuracy, TPR and TNR Measures of Accuracy of key point based DCT and SURF algorithms

Metric	SURF	DCT
Accuracy	96.45	91.86
TPR	97.83	89.94
TNR	94.87	89.57

The average accuracy, TPR and TNR for key point based SURF algorithm are 96.45 per cent, 97.83 per cent, and 94.87 per cent, however, the average accuracy, TPR and TNR for key point based DCT algorithm are 91.86 per cent, 89.94 per cent, and 89.57 per cent. It is clear from the results that the SURF method performs better than DCT as it achieved average accuracy which is approximately 5 per cent more than DCT at 91.86 per cent. For True Positive Rate (TPR) key-point based SURF algorithm outperformed block based DCT algorithm, which is also about 8 per cent higher than DCT at 89.94 per cent, and for False Positive Rate (FPR) SURF algorithm achieved about 5 per cent more than DCT at 89.57 per cent.

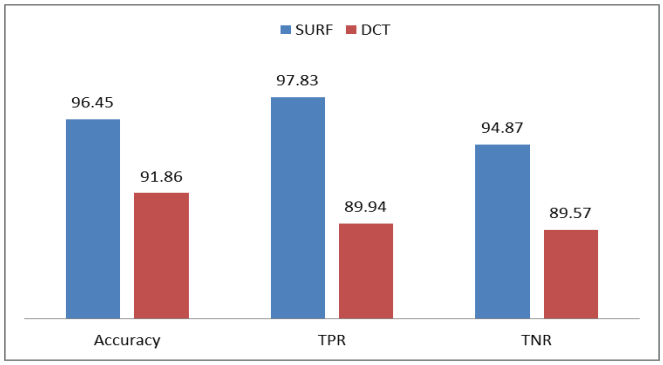

Figure 4: Results of image forgery detection using SURF and DCT, clearly showing improvement by using key-point based method

VI. CONCLUSION AND FUTURE SCOPE

Passive or Blind image forgery is most common method of image forgery in which many portions of image are tampered. This type of forgery is most difficult to detect. In this work we validated two state of the art blind image forgery techniques DCT and proposed key-point based SURF algorithms. Average Accuracy, True Positive Rate (TPR), and True Negative Rate (TNR) are used as parameters for performance evaluation on various images. Experimental results concluded the efficiency of SURF scheme in dealing with region rotation manipulations. This shows the efficiency of the key-point based scheme. The future work will see more efficient key-point based schemes in which clustering portion is modified with better key-point identification methods.

REFERENCES

1. Farid, H. (2009). Image forgery detection. IEEE Signal processing magazine, 26(2), 16-25.
2. Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. Digital Investigation, 10(3), 226-245.
3. Siddique, H., & Shenker, J. (2010). Hosni Mubarak left red faced over doctored red carpet photo. the Guardian. Retrieved 4 January 2020, from https://www.theguardian.com/world/2010/sep/16/mubarak-doctored-red-carpet-picture
4. Fridrich, A. J., Soukal, B. D., & Lukáš, A. J. (2003). Detection of copy-move forgery in digital images. In in Proceedings of Digital Forensic Research Workshop.
5. Huang, Y., Lu, W., Sun, W., & Long, D. (2011). Improved DCT-based detection of copy-move forgery in images. Forensic science international, 206(1-3), 178-184.
6. Khan, S., & Kulkarni, A. (2010). Reduced time complexity for detection of copy-move forgery using discrete wavelet transform. International Journal of Computer Applications, 6(7), 31-36.

7. Bashar, M. K., Noda, K., Ohnishi, N., Kudo, H., Matsumoto, T., & Takeuchi, Y. (2007, May). Wavelet-Based Multiresolution Features for Detecting Duplications in Images. In MVA (pp. 264-267).
8. Bayram, S., Sencar, H. T., & Memon, N. (2009, April). An efficient and robust method for detecting copy-move forgery. In 2009 IEEE International Conference on Acoustics, Speech and Signal Processing (pp. 1053-1056). IEEE.
9. Muhammad, G., Hussain, M., & Bebis, G. (2012). Passive copy move image forgery detection using undecimated dyadic wavelet transform. Digital investigation, 9(1), 49-57.
10. Li, L., Li, S., & Wang, J. (2012, November). Copy-move forgery detection based on PHT. In 2012 World Congress on Information and Communication Technologies (pp. 1061-1065). IEEE.
11. Li, Y. (2013). Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic science international, 224(1-3), 59-67.
12. Li, W., & Yu, N. (2010, September). Rotation robust detection of copy-move forgery. In 2010 IEEE International Conference on Image Processing (pp. 2113-2116). IEEE.
13. Wu, Q., Wang, S., & Zhang, X. (2010, November). Detection of image region-duplication with rotation and scaling tolerance. In International Conference on Computational Collective Intelligence (pp. 100-108). Springer, Berlin, Heidelberg.