DWT and SIFT based Passive Copy-Move Forgery Detection

Lakhwinder Kaur Bhullar
M.E. (ECE)
UIET, Panjab University
Chandigarh

Sumit Budhiraja
Assistant Professor, ECE
UIET, Panjab University
Chandigarh

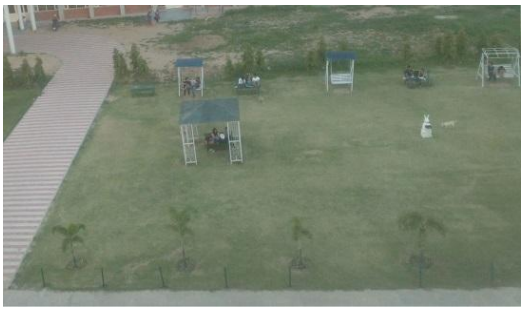
Anaahat Dhindsa
Assistant Professor, ECE
UIET, Panjab University
Chandigarh

ABSTRACT
With the use of powerful image modifying softwares, image authenticity is a big question for image forensics. One can no longer believe what they see. When a section of image is copied, geometrically transformed and pasted at different spot onto the same image with the intention of concealing or hiding some important information, it is copy move forgery. In the past few years several techniques for copy-move forgery detection have been proposed. In this paper Discrete Wavelet Transform (DWT) have been used with Scale Invariant Feature transform (SIFT) for copy move image forgery detection. SIFT keypoint descriptors are extracted from the low frequency subband of the discrete wavelet transformed image. The extracted keypoints are grouped into clusters using either of the linkage methods (median, centroid or ward) and are matched to detect the forgery. Different wavelet bases with SIFT have been compared using True Positive Rate (TPR) and False Positive Rate (FPR) as the performance evaluation parameter along with the computation time on a wide range of forged and original image database.

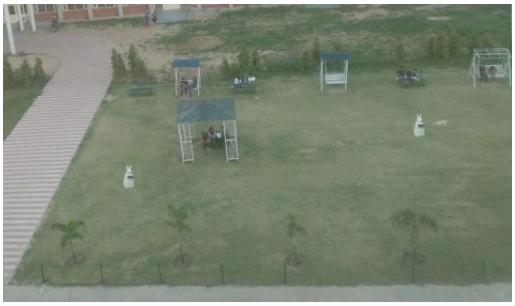
Keywords
SIFT, Copy-move forgery, invariant keypoint

1. INTRODUCTION
In today's digital age, digital images have very important and crucial role in our day-to-day lives, from official documents, in daily newspapers, magazines, scientific journals, medical diagnosis to proof at court. With the use of highly advanced, user friendly and easily available image modifying tools such as Photoshop, it has become effortless even for the non professional to alter and manipulate digital images, thus putting a question mark on their authenticity. The main objective of image forensics is to check the authenticity of images. With the aim to create misleading images, the attackers generally apply certain image processing operations to conceal visible traces of forgery. Basic image properties such as noise, color contrast and appearance remains same as both the copied and pasted sections are from the same image, which makes the detection difficult.

Copy-move image forgery is a special type of forgery where a section or part of the image is copied, subjected to some image processing operations and pasted on the same image with the aim to hide or conceal some important information in the image. Techniques present in literature are classified as either Active or Passive Authentication Techniques [1].



(a) Original unforged image



(b) Forged image

Fig 1: An example for copy move image forgery

Active techniques like Digital Signature and Digital Watermarking require pre-embedded data at the capturing end which is regenerated at the authentication end. Unlike Active techniques, Passive techniques do not require any prior embedded information. (Fig. 2)

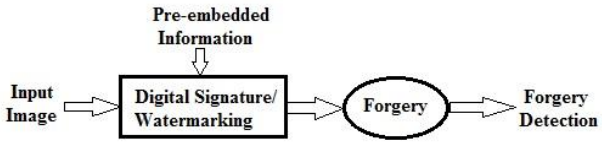


Fig 2(a): Active Forgery Detection Technique

Fig 2(b): Passive Forgery Detection Technique.

The paper organization is as follows: Related work for copy move forgery detection is presented in section II. Section III presents DWT and SIFT based technique with its main steps and tools used. Section IV contains the simulation results and section V contains the conclusion.

2. RELATED WORK

A large number of passive copy move forgery detection techniques have been proposed in literature which can be grouped as: block-based and keypoint based methods. A comparative analysis in terms of characteristics among Discrete Cosine Transform (DCT), Log Polar Transform, Texture and Intensity, Invariant moments, Invariant key-points and Principal Component Analysis (PCA) is presented by Al.-Qershi et al. [2]. It was shown in the paper that invariant key-point features are robust against most of the intermediate and post-processing operations such as reflection, rotation, scaling, compression, noise, etc.

Discrete Cosine Transform (DCT) alone or combined with either Discrete Wavelet Transform (DWT) or Quantization Coefficient Decomposition (QCD) to reduce the feature vector dimension is used for feature extraction from the subdivided image blocks [3-6]. Polar Harmonic Transform (PHT), 2D-FT, Krawtchouk Moments and Gabor Features are also used for block based feature extraction [7-10]. Lexicographical sorting, which presents the most similar feature vectors in the consecutive rows is used for feature matching in most of the block based methods [3,4,7,8,9].

Using SIFT keypoint decriptors for copy move forgery detection was initially proposed by Huang et al. [11]. Extracted SIFT keypoint descriptors are matched using nearest neighbour algorithm or cluster matching to detect the forgery [11,12]. Another detection technique based on SIFT that could even estimate the geometric transformation in the forgery was presented by Amerini et al. [13]. Features extracted using Speeded Up Robust Features (SURF), followed by matching and verification showed good detection results [14].

Evaluation of popular detection approaches of both block based (DCT, DWT, KPCA, PCA, Zernike, etc.) and key-point based (SIFT & SURF) methods is presented by Christlein [15]. The experimental results showed that almost all techniques perform equally well for robustness towards noise & JPEG compression. Zernike is well suited for rotation. However, if a copied area has large amounts of scaling or rotation or any other kind of distortion key-point based (SIFT & SURF) are best choices.

3. DWT and SIFT based Algorithm for Copy-Move Forgery Detection

For reliable copy move forgery detection in digital images, combination of DWT and SIFT is used. SIFT feature descriptors have strong stability against rotation, JPEG compression, Gaussian noise addition, scaling and other distortions. The workflow for DWT and SIFT based copy move forgery detection is given in Fig. 3.

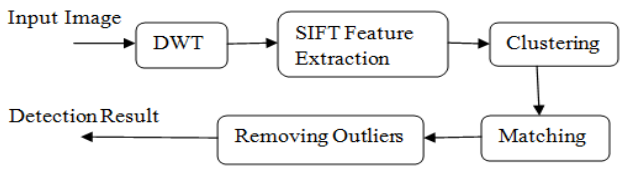


Fig 3: Proposed Algorithm Workflow

The input image is first decomposed using one of the DWT bases function from which SIFT features are extracted. Matching is done among the clusters and then the outliners are removed to give the final detection result.

3.1 Decomposition Using DWT

2D-DWT is applied in the initial stage of forgery detection process as it helps to extract more number of SIFT features which will help in better detection performance. Approximate subimage is more stable as most of the image energy is concentrated in it. Therefore approximate subimage using different wavelet bases such as Haar, Biorthogonal, Daubechies, coiflets and symlets is used to extract SIFT features and descriptors. Application of 2D-DWT acts as a preprocessing step of the algorithm.

3.2 SIFT Feature Extraction

SIFT descriptors that are invariant to scaling, rotation and affine transformations are computed using the following four major steps [16]

3.2.1 Scale Space Extrema Detection

A function, *L(x, y, σ)* is defined as the scale-space of an image which is generated by the convolution of Gaussian function, *G(x, y, σ),* and an input image, *I(x,y)*:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y)$$

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2}$$

Where $*$ is the convolution operation, *(x, y)* is the pixel coordinates and σ is the scale space factor or the variance of the Gaussian normal distribution. For efficient detection of stable and reliable keypoints, DOG (Difference Of Gaussian) function, $D(x, y, \sigma)$, which is computed by convolving the difference of two nearby scales separated by a constant scaling factor 'k' with an input image.

$$D(x, y, \sigma) = \big(G(x, y, k\sigma) - G(x, y, \sigma)\big) * I(x, y)$$

$$= L(x, y, \sigma) - L(x, y, \sigma) \quad (1)$$

3.2.2 Keypoint Localization

Selection of keypoints from extrema is done by rejecting the points along image edges or those with low contrast as they are unstable over image variations. Taylor expansion of scale-space function,$D(x, y, \sigma)$ shifted such that the sample point is origin:

$$D(\mathbf{x}) = D + \frac{\partial D^T}{\partial \mathbf{x}}\mathbf{x} + \frac{1}{2}\mathbf{x}^{\mathbf{T}}\frac{\partial^2 D}{\partial \mathbf{x}^2}\mathbf{x} \quad (\mathbf{2})$$

To determine the extremum location,$\hat{\mathbf{x}}$ derivative of $D(\mathbf{x})$ w.r.t. $\mathbf{x}$ is taken and set to zero**.**

$$\hat{\mathbf{x}} = -\frac{\partial^2 D^{-1}}{\partial \mathbf{x}^2}\frac{\partial D}{\partial \mathbf{x}} \quad (3)$$

For rejecting the low contrast unstable extrema, function value at the extrema is obtained by substituting eqn. (3) in (2).

$$D(\hat{\mathbf{x}}) = D + \frac{\partial D^T}{\partial \mathbf{x}}\hat{\mathbf{x}}$$

To remove the edge response of DOG operator, Hessian matrix, **H**, of second order is used. Let α the maximum eigen value, β be the smaller one and the ratio of two eigen values be $r = \alpha/\beta$.

$$\mathbf{H} = \begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix} \quad (4)$$

The trace and determinant for Hessian matrix is given as:

$$Tr(\mathbf{H}) = D_{xx} + D_{yy} = \alpha + \beta$$
$$Det(\mathbf{H}) = D_{xx}D_{yy} - (D_{xy})^2 = \alpha\beta$$

$$\frac{Tr(\mathbf{H})^2}{Det(\mathbf{H})} = \frac{(\alpha+\beta)^2}{\alpha\beta} = \frac{(r+1)^2}{r} \quad (5)$$

The feature points need to meet the below equation otherwise it is eliminated.

$$\frac{Tr(\boldsymbol{H})^2}{Det(\boldsymbol{H})} < \frac{(r+1)^2}{r}$$

3.2.3 Orientation Assignment

To achieve rotation invariance, each keypoint is assigned an orientation. For each Gaussian smoothed image sample,$L(x,y)$, the magnitude of gradient, $m(x,y)$, and orientation, $\theta(x,y)$, is computed using difference of pixels:

$$m(x,y) =$$

$$\sqrt{(L(x+1,y) - L(x-1,y))^2 + (L(x,y+1) - L(x,y-1))^2}$$

$$\theta(x,y) = \tan^{-1}\frac{L(x,y+1) - L(x,y-1)}{L(x+1,y) - L(x-1,y)}$$

Gradient direction of feature points is calculated using histogram of oriented gradients. Orientation histogram peaks represents the dominant direction of the local gradients.

3.2.4 Keypoint Descriptor Generation

The values of orientation histogram, in both image plane and scale space form the descriptor. With 4×4 array of histograms and 8 orientation bins in each, results in $4 \times 4 \times 8 = 128$ element feature vector.

3.3 Clustering

Extracted SIFT keypoint descriptors from the approximate sub image of the DWT decomposed original image are grouped using agglomerative hierarchical clustering. The clustering is completed by using one of the many linkage methods such as median, centroid or ward. For any cluster *C* formed from clusters A and B, having n_C number of points. If x_{Ci} represents the *i*th point in the cluster, then the various linkage methods operate as follow:

1. Median:

Euclidean distance between the centroids of the two clusters is used

$$dist(C,D) = \|\tilde{\mathrm{x}}_C - \tilde{\mathrm{x}}_D\|_2$$

where $\tilde{\mathrm{x}}_C$ and $\tilde{\mathrm{x}}_D$ represents the weighted centroids of the clusters *C* and *D*, which are recursively calculated as below:

$$\tilde{\mathrm{x}}_C = \frac{1}{2}(\tilde{\mathrm{x}}_A + \tilde{\mathrm{x}}_B)$$

2. Centroid:

Euclidean distance between the cluster centroids is used

$$dist(C,D) = \|\bar{\mathrm{x}}_C - \bar{\mathrm{x}}_D\|_2$$

where $\bar{\mathrm{x}}_C = \frac{1}{n_C}\sum_{i=1}^{n_C} \mathrm{x}_{Ci}$

3. Ward:

Increment in the sum of squares of the distances between all the points in the cluster and the centroid of the cluster is used

$$dist(C,D) = \sqrt{\frac{2n_C n_D}{(n_C + n_D)}}\,\|\bar{\mathrm{x}}_C - \bar{\mathrm{x}}_D\|_2$$

3.4 Matching

For matching among any two clusters say C_A and C_B, for each point, $i \in C_A$ vector descriptor $\bar{d}_i$ is compared with the vector descriptor $\bar{d}_j$for all $j \in C_B$. To improve the matching efficiency, angle between the vectors of two clusters is computed.

$$\gamma_{ij} = \cos^{-1}(\bar{d}_i \cdot \bar{d}_j)$$

and $\gamma_1 = \min_{\mathrm{j}\in C_\mathrm{j}} \gamma_{ij}$, $\gamma_2 = \min_{\mathrm{j}\in C_{\mathrm{j}-\mathrm{j}_1}} \gamma_{ij}$

where j_1 is a point with descriptor vector d_j in cluster C_B having minimum angle with the descriptor vector $\bar{d}_i$ in C_A. If the ratio of two minimum angles, γ_1 and γ_2 is less than a threshold value (say 0.5), then only the matches are accepted.

3.5 Removing False Matches

After the matching process, a set of inliers is selected and outliers are discarded by applying Random Sample Consensus (RANSAC). To apply RANSAC, atleast four matches must be there between the clusters. This algorithm randomly selects any four points from the matched points and then estimates the homography, *H*. All the remaining matched points are transformed according to *H* and compared in terms of distance with respect to their corresponding matches. Distance metric used for RANSAC is as follow:

$$d = \sum_{i=1}^{Num} min\big(D\big(P_{ib}, \Psi(P_{ia}{:}H)\big), t\big)$$

where P_{ia} and P_{ib} are the points in cluster a and b respectively, $\Psi(P_{ia}{:}H)$ represents the projection of point P_{ia} of cluster a based on transformation matrix H, t is the threshold value (0.01) and Num represents the number of points.The points with distance greater than t are termed as inliers while others as outliers and are discarded.

4. SIMULATION RESULTS

For performance evaluation of the copy move image forgery detection algorithm, simulation results are performed on a set of 300 images out of which 150 images are original i.e. unforged and 150 have been forged using copy move forgery. These images are randomly selected from MICC-F220 and MICC-F2000 [29]. The image resolution lies in the range of 501×335 pixels to 800×600 pixels. The forged images contain either square or rectangular forged regions which have been copied and pasted after applying different attacks of either rotation, translation, scaling (symmetric or asymmetric) or even combination of these.

Performance of the forgery detection algorithm for copy move is measured by True Positive Rate (TPR) and False Positive Rate (FPR). TPR is the percentage of correctly identified forged images while FPR is the percentage of original images falsely identified as forged.

$$TPR(\%) = \frac{no.of\ forged\ images\ detected\ as\ forged}{total\ no.of\ forged\ images} \times 100$$

$$FPR(\%) = \frac{no.of\ original\ images\ detected\ as\ forged}{total\ no.of\ original\ images} \times 100$$

In this detection algorithm, an image is considered to be detected as forged by copy-move forgery if the algorithm identifies two or more clusters having atleast four pairs of matched points.

Table 1. TPR and FPR (in %) for three linkage methods (median, centroid and ward) with DWT and SIFT

	Median		Centroid		Ward	
	TPR	**FPR**	**TPR**	**FPR**	**TPR**	**FPR**
SIFT	94.6	12.0	97.3	9.3	96.7	8.7
Db9	96.7	9.3	97.3	4.7	96.7	5.3
Haar	78.0	6.7	90.7	4.0	82.7	6.0
Sym 2	92.7	7.3	90.0	6.0	92.0	6.0
Coif 1	90.0	12.0	92.7	4.7	93.3	6.7
Bior 3.5	94.0	11.3	98.7	5.3	96.0	9.3

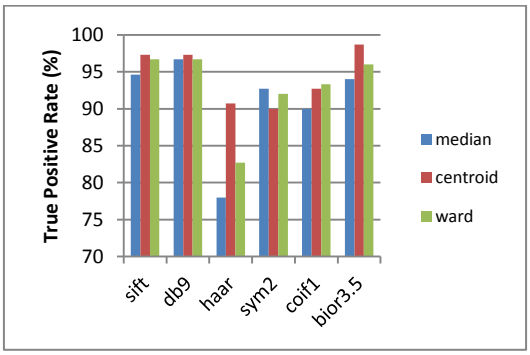


Fig 4: TPR (%) for different wavelet bases in cases of different linkage methods

Different wavelet bases namely Daubechies, Haar, Symlets, Coiflets and Biorthogonal have been employed. Detection performance of these wavelet bases with SIFT for copy move forgery is given in Table 1.

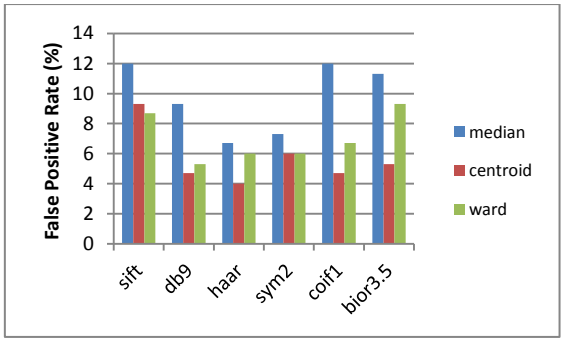


Fig 5: FPR (%) for different wavelet bases in cases of different linkage methods

From Fig. 4 and Fig. 5 it is observed that centroid linkage gives better results than median or ward in almost all the cases. When SIFT combined with Bior3.5 DWT is applied, TPR increases and FPR decreases simultaneously, which indicates better performance rather than using SIFT alone for copy move forgery detection.

Simulation time solely depends on the type of wavelet bases function applied and not on the type of linkage method used. The average simulation time for an image for different wavelet bases with SIFT is shown in Fig. 6. The average simulation time values have been computed by randomly selecting same 40 images for each case.

Table 2. Average computational time in seconds for an image for different wavelet bases

	Average computational time for an image(seconds)
SIFT	18.2
SIFT+Sym2	18.2
SIFT+Db9	25.2
SIFT+Bior3.5	60.7
SIFT+Coif1	18.0
SIFT+Haar	8.6

It is observed from Table 2 that SIFT combined with haar wavelet transform showing least detection results takes the least amount of computation time. Also SIFT combined with Bior 3.5 showing best detection results takes the maximum time of approximately 1 minute. This is because image decomposed using different wavelet bases functions have variation in the number of keypoints extracted.

5. CONCLUSION

In this paper wavelet transform has been used with SIFT features for reliable detection of the duplicated region in the copy move tampered images. Simulation performed on original and forged images with different processing operations show that combination of DWT and SIFT improves the detection performance as compared to only SIFT. Bior 3.5 wavelet combined with SIFT using centroid linkage method shows the best detection results in terms of both TPR and FPR while taking maximum time for result computation. It is also observed that as the number keypoints extracted from the DWT decomposed image increases, the computational time also increases. In the future, detection technique can be further improved to detect the

cases of image splicing. The combination of this technique with some other techniques can also be tried to extract features from uniform regions, where the performance of SIFT is not optimum.

6. REFERENCES

[1] Birajdar, Gajanan K., and Vijay H. Mankar. "Digital image forgery detection using passive techniques: A survey." Digital Investigation 10.3 (2013): 226-245.

[2] Al-Qershi, Osamah M., and Bee Ee Khoo. "Passive detection of copy-move forgery in digital images: State-of-the-art." Forensic science international 231.1 (2013): 284-295.

[3] Wang, Xiaofeng, et al. "A DWT-DCT Based Passive Forensics Method for Copy-Move Attacks." Multimedia Information Networking and Security (MINES), 2011 Third International Conference on. IEEE, 2011.

[4] Huang, Yanping, et al. "Improved DCT-based detection of copy-move forgery in images." Forensic science international 206.1 (2011): 178-184.

[5] Ghorbani, Mehdi, Mohammad Firouzmand, and Ahmad Faraahi. "DWT-DCT (QCD) based copy-move image forgery detection." Systems, Signals and Image Processing (IWSSIP), 2011 18th International Conference on. IEEE, 2011.

[6] , Sunil, Jagannath Desai, and Shaktidev Mukherjee. "A fast DCT based method for copy move forgery detection." Image Information Processing (ICIIP), 2013 IEEE Second International Conference on. IEEE, 2013.

[7] Li, Leida, Shushang Li, and Jun Wang. "Copy-move forgery detection based on PHT." Information and Communication Technologies (WICT), 2012 World Congress on. IEEE, 2012.

[8] Ketenci, Seniha, and Guzin Ulutas. "Copy-move forgery detection in images via 2D-Fourier Transform." Telecommunications and Signal Processing (TSP), 2013 36th International Conference on. IEEE, 2013.

[9] Imamoglu, Mustafa Bilgehan, Guzin Ulutas, and Mustafa Ulutas. "Detection of copy-move forgery using Krawtchouk moment." Electrical and Electronics Engineering (ELECO), 2013 8th International Conference on. IEEE, 2013.

[10] Detection of copy-move forgery image using Gabor descriptor." Anti-Counterfeiting, Security and Identification (ASID), 2012 International Conference on. IEEE, 2012.

[11] Huang, Hailing, Weiqiang Guo, and Yu Zhang. "Detection of copy-move forgery in digital images using SIFT algorithm." Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on. Vol. 2. IEEE, 2008.

[12] Ardizzone, Edoardo, Alessandro Bruno, and Giuseppe Mazzola. "Detecting multiple copies in tampered images." Image Processing (ICIP), 2010 17th IEEE International Conference on. IEEE, 2010.

[13] Amerini, Irene, et al. "A SIFT-based forensic method for copy–move attack detection and transformation recovery." Information Forensics and Security, IEEE Transactions on 6.3 (2011): 1099-1110.

[14] Shivakumar, B. L., and S. Santhosh Baboo. "Detection of Region Duplication Forgery in Digital Images Using SURF." International Journal of Computer Science Issues (IJCSI) 8.4 (2011).

[15] Christlein, V., Riess, C., Jordan, J., & Angelopoulou, E. (2012). "An evaluation of popular copy-move forgery detection approaches." Information Forensics and Security, IEEE Transactions on, 7(6), 1841-1854.

[16] Lowe, David G. "Distinctive image features from scale-invariant keypoints." International journal of computer vision 60.2 (2004): 91-110

[17]