ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 7, July 2017

Performance Enhancement for Copy move Image Forgery Detection using Artificial Bee colony based- BPCS Technique in Image Processing

Samiksha prasad[1] (M.tech scholar)

Email id- erprasadsami92@gmail.com

Dr.Amit Asthana[2] (Assistant Professor)

Computer science engineering

Swami Vivekanand Subharti University

ABSTRACT

As one of the most successful applications of image analysis and understanding, digital image forgery detection has recently received significant attention, Even though there are many systems to detect the digital image forgery, their success is limited by the conditions imposed by many applications. For example, detecting duplicated region that have been rotated in different angles remains largely unsolved problem. In our proposed approach, an attempt to assist these efforts development in the field of Copy-Move digital image forgery detection using bit plane cosine similarity based bee colony optimization technique which split image pixel in three factor bit plane such as onlooker, scout and employee bee key point descriptor of sift, key point using MATLAB 2014Ra.

Keyword-Image forgeries, Digital forensics, Copy-Move forgery detection, block matching, bee colony optimization, BPCS, SIFT key points etc.

I.INTRODUCTION

1.1. IMAGE FORGERY BACKGROUND

Digital image forgery detection system can be ordered into active and passive (blind) approach [11]. The activemethodologies requires earlier data about the unique image. The image close by is accepted to be manufactured and the strategies attempt to recognize the forged bits inside. The greater part of the active approach requires some pre-handling, for example, watermarks installing or mark era amid picture securing, which would confine their application [12, 13]. Thus, there is a requirement for blind forgery detection method, where no earlier data about source picture is required. The blind image

forgery detectionstrategies can be assembled into various classes [14]: pixel-based, organize based, camera based, physical condition based, geometry based.

a. Pixel Based Image forgery detection detects irregularities at the pixel level of the computerized picture. These strategies are classified as; cloning, resampling, measurable and slicing.
b. Format Based Image forgery detection depends on picture designs, particularly in the JPEG organize. It is sorted into JPEG Quantization, Double JPEG, and JPEG blocking. It can distinguish forgery even in compacted picture.
c. Camera based methods Image forgery detection incorporates chromatic distortion, shading channel cluster, camera reaction and sensor commotion to distinguish hints of altering presented at different phases of imaging process.
d. Physical condition constructs Image forgery detection works in light of the premise of lightning condition under which the protest or picture is caught. These strategies are partitioned into three: Light Direction 2D, Light Direction 3D, and Light condition.
e. Geometry Based Image forgery detection is isolated into two, Principal focuses and Metric estimations, which makes estimation of articles on the planet and their position in respect to the camera, to detectforgery.

All Rights Reserved © 2017 IJARECE

1.2. **Artificial Bee Colony Algorithm for copy move position finding**

Throughthe procedure of comparability score combination, a key issue is the manner by which to allot the weights of similitude score. It influences straightforwardly the recovery execution of the framework. To determine the issue of getting the ideal weight an incentive for shading and surface element similitude score and to execute a quick and vigorous CIR plot, Artificial Bee Colony algorithm is utilized. In ABC algorithm,the position of a nourishment source speaks to a conceivable answer for the streamlining issue and the measure of nectar of a sustenance source compares to the nature of the related arrangement.

The quantity of employed bees or the onlooker bees is equivalent to the quantity of arrangements in the populace. At the initial step, the ABC creates a arbitrarily appropriatedoriginal population (*P*) of *SN* arrangements where SN means the extent of utilizedemployedbees or onlooker bees. Every solution *xi* is a *D*-dimensional vector where *D* is the number of optimization parameters and *i* = 1, 2, 3, . . . *SN*. After introduction, the number of inhabitants in the positions is liable to rehash Maximum Number of Iterations (MNIs) of the pursuit procedures of the utilized employed bees, the onlooker bees, and the scout bees. An employedbee delivers an adjustment on the position in honey bee's memory relying upon the nearby data and tests the measure of nectar at the source.The digital image forgeryis arranged into five classifications [14, 15]: Copy-move (cloning) imitation, Image Splicing, Image Retouching, Morphing, and Enhanced.

1.3. Copy-move forgery

It is a particular kind of picture control, where a piece of the picture itself is replicated and glued into another piece of a similar picture. In a duplicate move assault where left side shows unique picture which contains three rockets and right side shows produced imaged with four rockets.

1.4. Image Retouching

Diverse components from different pictures are superimposed into a solitary composite picture. Fig. 2b indicates image splicing where distinctive components from numerous pictures (right) are compare in a solitary picture (left) to make forgery.

Fig. 2b: Image Splicing

Image retouching –Includes slight change in the picture for different tasteful and business purposes. Retouching is utilized to upgrade or lessen certain elements in the picture. Fig. 2c demonstrates a case of imageretouching,where genuine face is on the privilege and left demonstrates the corrected adaptation of it.

Fig. 2 c: Image Retouching

1.5. Morphing:

It is an image forgery where one protest on picture is transformed into another question in the other picture. Morphing is appeared in Fig.2d, where left and right pictures are the main picture and center one is the morphed image.

All Rights Reserved © 2017 IJARECE

Fig. 2d Morphing

1.6.Enhanced Technique

The novel imageindicated is upper left corner of Fig. 2 e, trailed by different improvements, for example, shading change, obscuring of foundation lastly the upgraded picture on the lower right corner.

Fig. 2e: Enhanced after forgery

1.7. COPY-MOVE FORGERY DETECTION

Copy-move strategy is the most famous image forgery. It is altering system in which some district is replicated and stuck to another piece of a similar picture so as to cover certain elements or items. Because of the idea of district duplication, there are no less than two comparable areas in an altered locale. Copy-Move forgery is performed with the goal of either making a question "covered up" from the picture by covering it with a little square of foundation, replicated from another piece of a similar picture [16] or makes extra duplicate of a protest effectively existing in the picture by replicating it to the coveted area. Since the replicated portions are a piece of a similar picture, the shading palette, commotion segments, dynamic range and alternate properties will be reliable with whatever remains of the picture, and in this way making it is extremely troublesome for a stripped human eye to detect the forgery.

Copy-move forgery detection can be either square based or key-point based strategies. In piece based techniques [17], the picture is isolated into covering/non-covering squares and highlight vector is figured for each pieces. Comparable element vectors are recognized and coordinated to discover forged regions.

II. RELATED WORK

D. Karaboga and B. Akay[1],In this paper, the component extraction organize determines the shading and surface elements from the picture. Shading highlights are extricated utilizing shading histogram technique and the surface components are gotten from co-event grid of the picture. Distinctive elements mirror the diverse qualities of the picture; if those elements are incorporate sensibly, the recovery procedure will be an entire one. In creator proposed framework, the likeness between inquiry picture and each of the pictures from target database are inferred and they are standardized. The standardized likeness estimations of shading and surface are consolidated utilizing combination calculation and combination weights are doled out adaptively by Artificial Bee Colony optimization algorithm [4] to enhance the image recovery execution.

Harpreet Kaur, Jyoti Saxena and Sukhjinder Singh [2]This paper depicts copy-move image forgery detection techniques, for example, SURF, PCA consolidated with SIFT (PCA+SIFT) and DWT joined with SIFT (DWT+SIFT). They are looked at as far as affectability, precision, specificity, FPR (False Positive Rate) and FNR (False Negative Rate). Investigation comes about demonstrate that PCA joined with SIFT technique is prevalent in affectability, precision and lower estimation of FNR contrast with SURF and DWT consolidated with SIFT strategies.

Pameli Mukherjee, Saurabh Mitra [3]This paper indicates examination between two surely understood strategies in light of DWT and DCT. These both techniques went over issues like setting edge, diminishment in execution time, diminishing number of covering pieces and lessening highlight vector measurement.

Harpreet Kaur, Kamaljit Kaur [4]This paper depicts the 2 sorts of Digital image Forgery detection methods i.e. active and passive approach. It portrays the favorable circumstances and detriments of both these methodologies. It likewise looks at the current strategies for 11 both piece based technique and point

All Rights Reserved © 2017 IJARECE

based strategies that are utilized to discover the copy-move forgeryon the bases of their strategy, favorable circumstances and impediments.

V. S. Kulkarni, Y. V. Chavan [5]This paper expresses the best approach to distinguish Digital image forgeryfor a picture utilizing point based technique. The outcomes are checked for SURF and SIFT technique for forgery detectionon various arrangement of pictures i.e. JPEG, PNG, TIFF and BMP. Both SIFT and SURF has roughly same precision. Be that as it may, the time required to prepare SURF is not as much as SIFT and along these lines SURF strategy is better for still pictures as well as for the pictures continuously mold.

Li, Jian et. al. (2014) [6]has proposed the division based Image Copy-move Forgery Detection Scheme. In this paper, the creators have proposed a plan to distinguish the copy-move forgery in an image, for the most part by extricating the keypoints for examination. The fundamental distinction to the conventional techniques is that the proposed conspire first portions the test picture into semantically free fixes before keypoint extraction. Accordingly, the copy-move regions can be distinguished by coordinating between these patches. The coordinating procedure comprises of two phases. In the principal arrange, they have discovered the suspicious sets of patches that may contain copy-move forgery regions, and generally evaluated a relative change framework. In the second stage, an Expectation-Maximization-based calculation is intended to refine the assessed framework and to affirm the presence of copy-move forgery.

Hashmi, Mohammad Farukh (2014) [7]has dealt with the copy-move image forgery detectionin light of speeded up hearty component change and Wavelet Transforms. In this paper, the creators have proposed d a progression of calculations which are mix of speeded-up hearty element changes and Wavelet Transforms. In doing as such creators have first examined the Speeded-Up Robust Feature (SURF), SURF in blend with Discrete Wavelet Transform (DWT), SURF in mix with Dyadic Wavelet Transform (DyWT). These calculations are not quite the same as the beforehand proposed calculation in the way that they are connected on the whole picture to extricate highlights as opposed to partitioning the picture into the pieces. From the outcomes acquired they can finish up the proposed calculations are superior to their partners both as far as computational intricacy and invariance to scale and revolution and furthermore for the mix of assaults.

Hussain, Muhammad (2014) [8]has played out an execution assessment overview on WLD and LBP descriptors for non-intrusive image forgery detection. The creators have researched the identification of copy-move and splicing, the two destructive sorts of image forgery, utilizing textural properties of pictures. Altering contorts the surface miniaturized scale designs in a picture and surface descriptors can be utilized to identify altering. They did near examination to look at the impact of two best in class best surface descriptors: Multiscale Local Binary Pattern (Multi-LBP) and Multiscale Weber Law Descriptor (Multi-WLD). Multiscale surface descriptors separated from the chrominance segments of a picture are passed to Support Vector Machine (SVM) to recognize it as real or forged.

Jaberi, Maryam et. al. (2014) [9]has worked with precise and hearty limitation of copied locale in copy–move image forgery. In addition, they have likewise proposed refining the relative change utilizing an iterative plan which enhances the estimation of the relative change parameters by incrementally finding extra keypoint matches. To lessen false positives and negatives while extricating the replicated and glued districts, they propose utilizing "thick" MIFT highlights, rather than standard pixel relationship, alongside hystereresis thresholding and morphological operations.

Muhammad, Ghulam (2014) [10]have built up a image forgery detection method utilizing steerable pyramid change and neighborhood parallel example. In this paper, a novel image forgery detection strategy is proposed in view of the steerable pyramid transform (SPT) and local binary pattern (LBP).Initially, given a shading picture, the creators change it in the YCbCr shading space and apply the SPT change on chrominance channels Cb and Cr, yielding various multi-scale and multi-situated subbands. At that point, they portray the surface in each SPT sub band utilizing LBP histograms.

Bit-Plane Complexity Segmentation (BPCS)

Bit-Plane Complexity Segmentation (BPCS) steganography is another basic sort of data hiding methods where a n-bit have picture is disintegrated into n twofold pictures (n bit-planes) before inserting process happens as appeared in Fig. 3 The many-sided quality of each piece plane is computed by finding the whole of shading changes between pixels in the planes. For instance, a white-shading pixel encompassed by four dark shading pixels has a many-sided quality of 4 square of pixels, the maximum complexity is ( ) and the minimum

All Rights Reserved © 2017 IJARECE

complexity is 0.A checkerboard picture of size 4 × 4 where the upper-left pixel is dark. The aggregate number of shading changes in this piece is 2 × (4 – 1) = 24. Bhattacharyya et al. [18] proposed a steganographic strategy for 8-bit pictures in view of finding the entirety of shading changes between pixels in the planes. Bit-planes with unpredictability higher than a limit is then sectioned into 8x8 disjoint squares and 2 mystery bits are inserted in each piece by a mapping plan. As appeared from tests, the downside of this strategy originates from its low implanting limit (1.6% in best cases) with PSNR esteem under 38dB.

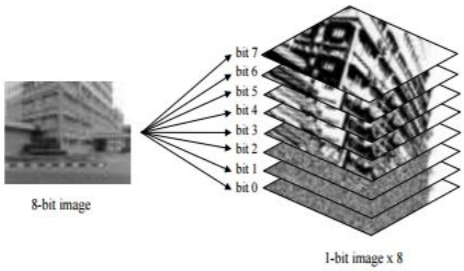

Figure 3: bit plane slicing approach 8x8

III.PROBLEM STATEMENT

The location of fake cash notes and human action pictures is a standout amongst the most basic undertakings performed by the machines, where a powerful, dependable, and high handling system is required to naturally perceive fake from valid money. As specified in the past area, some security includes in money notes are obvious and might be distinguished effectively by the essential human detects, for example, shading and size of the notes. In any case, this strategy is restricted by the way that the nature of banknotes is falls apart after some time, and such components may not be perceivable by then Other than wearing out and getting harmed, some cash notes have exceptionally complex plans that force some level of trouble when handled with programmed currency recognition

V. PROPOSED ALGORITHM

In the BPCS-ABC algorithm, while onlookers and employed bees carry out the LSB plane corrupt process, the scouts control the exploration process for outer plane. Detailed pseudo-code of the BPCS-ABC algorithm is given below are as:

1: Initialize the population of solutions for 4 bit plane xi; i ¼ 1; SN
2: Evaluate the populationfor eight bit-planes of the image
3: cycle = 1
4: repeat
5: Produce new solutions ti for the employed bees by 4 bit plane and evaluate them
6: Apply the greedy selection process for all planes for the employed bees
7: Calculate the probability values Pi for the solutions xi
8.Check whether there are some abandoned solutions or not.
9.If true,
10.Replace them with some new randomly-generated solutions by 1), where ϕ is a random real number in [-1, 1],
11.min and max stand for lower and upper bounds of possible solution.
12.Produce the new solutions ti for the onlookers from the solutions xi selected depending on Pi
13.Apply the 4x4 cross sectional process for the onlookers
14.Perform size-estimation i.e. calculate the places where we can store the secrete image.
15.Perform bit plane complexity segmentation on image i.e. embed secrete blocks into carrier image.
16.Find the abandoned solution for the scout, if exists, and replace it with a new randomly produced solution xi
17.Group the bytes of the secret file into a series of secret blocks.
18.If a block is less complex than the threshold (α0),
19.Then conjugate it to make it a more complex block.
20.Memorize the best solution achieved so far
21.cycle = cycle + 1
22. until cycle = MCN

VI.RESULT

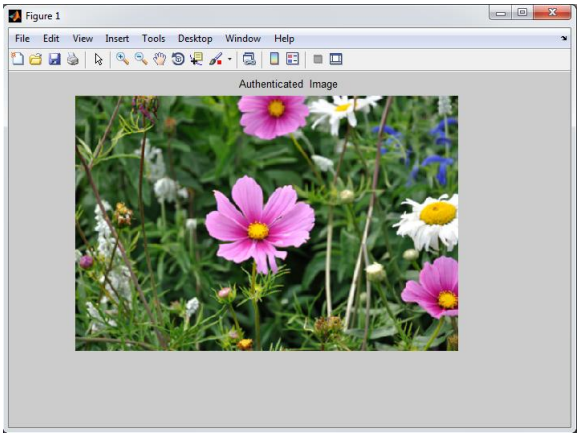

Figure6.1. Input image

All Rights Reserved © 2017 IJARECE

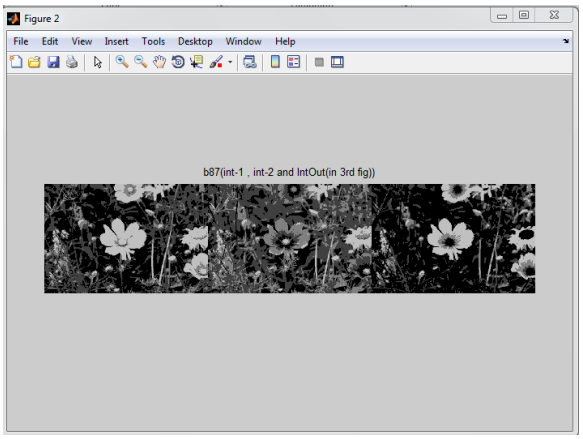

Figure6.2. Bit 8 Slicing Pattern for Forged Image

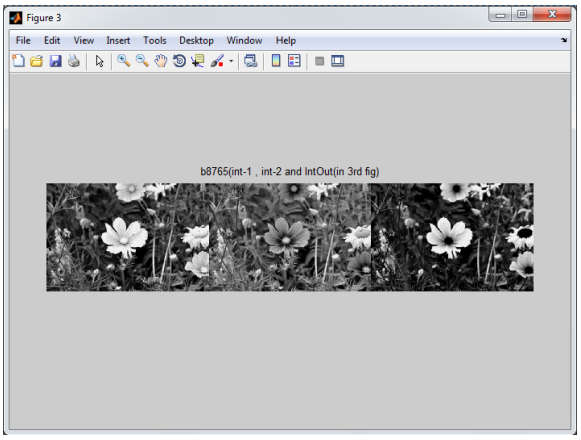

Figure6.3. On Looker Bit Plane Slicing for Forged Image

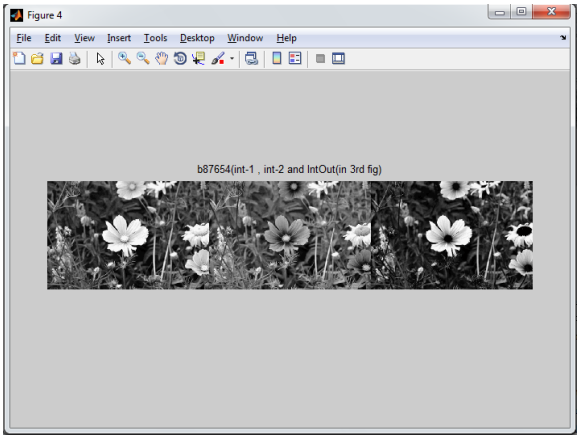

Figure6.4. Bit Plane Slicing using Bee Colony

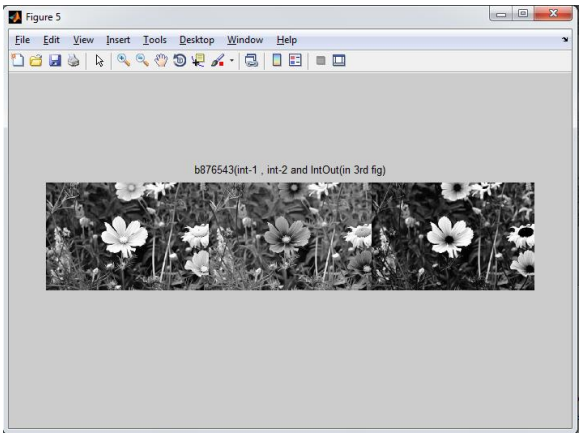

Figure6.5. Bit Plane Slicing for scout

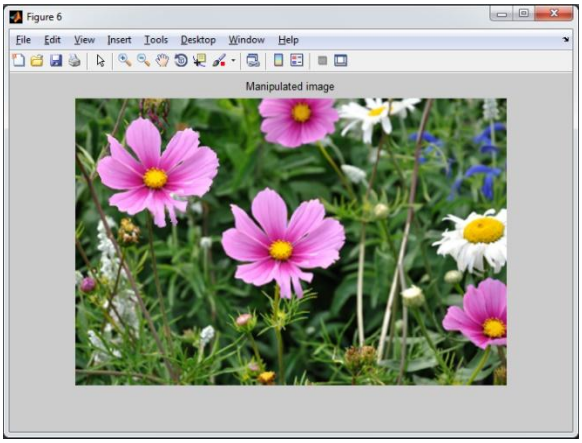

Figure6.6. Manipulated Image

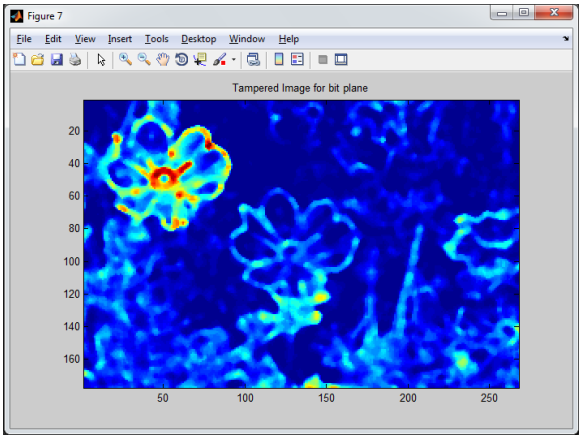

Figure6.7. Tempered Image for Bit Plane

All Rights Reserved © 2017 IJARECE

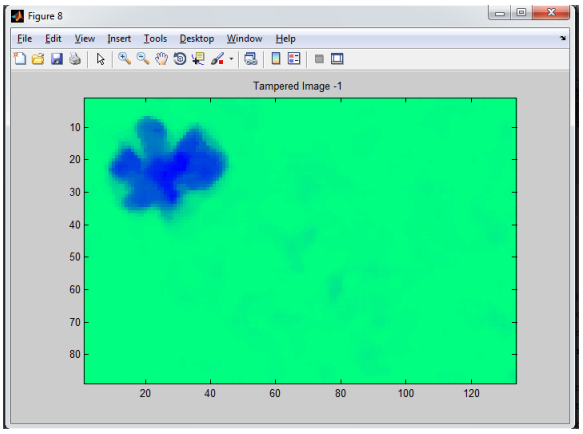

Figure6.8. Tempered Image-1

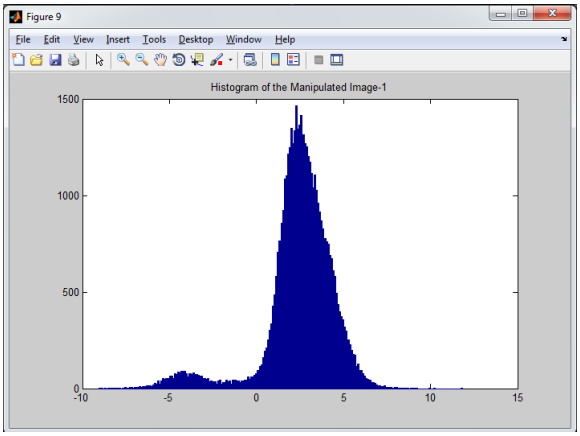

Figure6.9. Histogram of the Manipulated Image-1

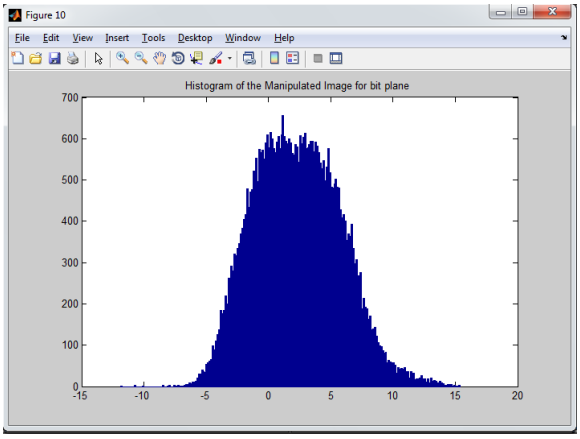

Figure6.10. Histogram of the Manipulated Image for Bit Plane

VII.CONCLUSION

We concluded that the major problem with copy move forgery is the detection of duplicated image regions affected by common image processing operations, e.g. compression, noise addition, rotation, scaling, flipping etc.Bee colony based BPCS technique outperform detecting copy-move blocks even for the flat regions but these are not good in detecting scaled copied blocks. Block matching methods using square blocks are not suitable for detection of rotated or scaled duplicated blocks for bit plance. However, using circular blocks instead of rectangular blocks can significantly make the detection invariant against rotation. So, there is the requirement of the some advanced techniques that can work naturally.

In future reference, we want to suggest the nature inspired techniques to check the image forgery by making use of natural experience of nature.

REFERANCES

[1] D. Karaboga and B. Akay, "A comparative study of Artificial
Bee Colony algorithm," *Applied Mathematics and Computation,*
vol. 214, no. 1, pp. 108–132, 2009.

[2] Harpreet Kaur, Jyoti Saxena and Sukhjinder Singh,"Simulative Comparison of Copy- Move Forgery Detection Methods for Digital Images," International Journal of Electronics, Electrical and Computational System IJEECS ISSN 2348-117X Volume 4, Special Issue September 2015.

[3] Pameli Mukherjee and Saurabh Mitra, "Comparative Analysis of Techniques for Detecting Copy-Move Image Forgery," International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 11, November 2015.

[4] Harpreet Kaur and Kamaljit Kaur, "A Brief Survey of Different Techniques for Detecting Copy Move Forgery," International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4,2015.

[5] V. S. Kulkarni and Y. V. Chavan, "Comparison of methods for detection of Copy-Move Forgery in Digital Images," International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6, June,2014.

All Rights Reserved © 2017 IJARECE

[6] Li, Jian, Xiaolong Li, Bin Yang, and Xingming Sun. "Segmentation-based Image Copy-move Forgery Detection Scheme.", Information Forensics and Security, IEEE Journals, 2014.

[7] Hashmi, Mohammad Farukh, Vijay Anand, and Avinash G. Keskar. "A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms." In Computer and Communication Technology (ICCCT), 2014 International Conference on, pp. 147-152. IEEE, 2014.

[8] Hussain, Muhammad, Sahar Q. Saleh, Hatim Aboalsamh, Ghulam Muhammad, and George Bebis. "Comparison between WLD and LBP descriptors for non-intrusive image forgery detection." In Innovations in Intelligent Systems and Applications (INISTA) Proceedings, 2014 IEEE International Symposium on, pp. 197-204. IEEE, 2014.

[9] Jaberi, Maryam, George Bebis, Muhammad Hussain, and Ghulam Muhammad. "Accurate and robust localization of duplicated region in copy–move image forgery." Machine vision and applications 25, no. 2 (2014): 451-475.

[10] Muhammad, Ghulam, Munner H. Al-Hammadi, Muhammad Hussain, and George Bebis. "Image forgery detection using steerable pyramid transform and local binary pattern." Machine Vision and Applications 25, no. 4 (2014): 985-995.

[11] B.L.Shivakumar, Lt. Dr. S.Santhosh Baboo, "Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods," Global Journal of Computer Science and Technology, 2010, Vol. 10, Issue 7, pp. 61-65.

[12] D. Kundur, D. Hatzinakos, "Digital watermarking for tell-tale tamper proofing and authentication," Proc. IEEE, vol 8, no. 7, 1999, pp. 1167-1180.

[13] J. Fridich, "Methods For Tamper Detection In digital Image," Proc ACM Workshop on Multimedia and Security, Orlando,, FL, October 30- 31, 1999, pp. 19-23.

[14] M. D. Ansari, S. P. Ghrera, V. Tyagi, "Pixel-Based Image Forgery Detection: A Review,"IETE Journal of Education, 55:1, 40-46.

[15] S. A.Thajeel, G. Sulong, "A survey of copy-move forgery detection Techniques," Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645.

[16] S. Sharmila, S. Prajakta, S. Hiral, "Image Forgery Detection Techniques for Forensic Sciences,"ijournals, ISSN-No: 2347-4890,vol 2, issue 8, August 2014.

[17] Resmi S, Chithra A S, "Recent Block-based Methods of Copy-Move Forgery Detection in Digital Images," International Journal of Computer Applications (0975 – 8887) Volume 89 – No 8, March 2014.

[18] S. Bhattacharyya, A. Khan, A. Nandi, A. Dasmalakar, S. Roy, and G. Sanyal, "Pixel mapping method (PMM) based bit plane complexity segmentation (BPCS) steganography," in World Congress on Information and Communication Technologies (WICT), Mumbai, 2011, pp. 36-41.

All Rights Reserved © 2017 IJARECE