ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.9

Salient Point Based Steganography

Renuka Mathapati[1], Dr. Jagadeesh Pujari[2], Dr V.V.Subrahmanyam[3]
Assistant Professor[1], HOD[2], Associate Professor[3]
Department of computer science[1, 3], Department of Information Science[2]
JSS SMI UG & PG Studies, Dharwad, India[1]
SDMCET College of Engineering, Dharwad, India[2]
IGNOU, New Delhi, India[3]

Abstract:
This paper discusses on about the Harris laplace affine detector which can identify similar regions between images that are related through affine transformations and have different illuminations. These affine-invariant detectors should be capable of identifying similar regions in images taken from different viewpoints that are related by a simple geometric transformation: scaling, rotation and shearing. These detected regions have been called both invariant and covariant. On one hand, the regions are detected invariant of the image transformation but the regions covariant change with image transformation.

Keywords: Harris Laplace, Interest points, salient points, Encryption, Decryption

I.INTRODUCTION

Most of computer vision applications employ interest points of the scene (images or frames) to understand it. Therefore an accurate detection of the interest points is essential for many computer vision applications. The interest points must be invariant to rotation, zoom, and blur, illumination and point of view changes [1]. In this paper we propose a novel approach for detecting interest points invariant to scale and affine transformations. Our scale and affine invariant detectors are based on the following recent results:
(1) Interest points [2] extracted with the Harris detector can be adapted to affine transformations and give repeatable results (geometrically stable).
(2) The characteristic scale of a local structure is indicated by a local extremum over scale of normalized derivatives (the Laplacian) [3].
(3) The affine shape of a point neighborhood is estimated based on the second moment matrix. Our scale invariant detector computes a multi-scale representation for the Harris interest point detector and then selects points at which a local measure (the Laplacian) is maximal over scales. This provides a set of distinctive points which are invariant to scale, rotation and translation as well as robust to illumination changes and limited changes of viewpoint. The characteristic scale determines a scale invariant region for each point. We extend the scale invariant detector to affine invariance by estimating the affine shape of a point neighborhood. An iterative algorithm modifies location, scale and neighborhood of each point and converges to affine invariant points. This method can deal with significant affine transformations including large scale changes. The characteristic scale and the affine shape of neighborhood determine an affine invariant region for each point [4] In the area of communication, security plays an important role to prevent from unauthorized access. The work proposed here represents a way for securing the text. The algorithm, that we have proposed here, will secure the text message Here, we have used the concept of steganography using harris laplace detector algorithm where interest points are found and checked for the neighbourhood bits and then text gets embedded into it An interest point [5] is a point in an image which has a well-defined position and can be robustly detected. This means that an interest point can be a corner but it can also be, for example, an isolated point of local intensity maximum or minimum, line endings, or a point on a curve where the curvature is locally maximal[6][7][8].

II. PROPOSED WORK

This work involves encryption and decryption of secret message which is been embedded in the image by extracting the interest point using harris laplace algorithm then determining the local maximum of the given value and then embedding in column wise, in the 8 neighbours of a pixel. If we have reached end of rows in image (bottom of Image), reset the row, increment column by selecting neighbouring 8 pixel values starting clockwise from 12 o clock pixel then check neighbours selecting candidate pixel and Storing RGB values of 8 neighbouring pixels in 'pix' and then embedding the corresponding text in that pixel value. Each neighbour contains only one bit of the text clearing last bit R Plane and B plane are indicators (Signature)(1 0 1 0 values) Only G Plane is used to store data in ODD number that ends with 1 else end with 0 by default (after clearing) then add nth bit and find difference between encoded and original. Following are the images i.e FIG (A) which shows image without text and FIG (B) which shows image with text or hidden text under image.

Figure.1. (a): image without text

Figure.2. (b): image with text

III. ALGORITHM

Encoding:

1. Input a bmp image file
2. Input Text file
3. Extract key points using Harris-Laplace algorithm
4. Convert into gray level image
5. Extract interest points
6. Find the scale (standard deviation)
7. Find the integration scale
8. Interest point response
9. Alison Noble measure
10. Original Harris measure
11. Find local maxima on neighborgood
12. Set threshold 1% of the maximum value
13. Find local maxima greater than threshold
14. Build interest points
15. Compute scale-normalized laplacian operator
16. Verify for each of the initial points whether the LoG attains a maximum at the scale of the point
17. SET SCALE TO 3*SIGMA FOR DISPLAY
18. String to array of ASCII values
19. Storing 8 bits in bit_array by shifting and ANDing
20. Embedding text in the image Column wise, in the 8 neighbours of a pixel
21. If we have reached end of rows in image (bottom of Image), reset the row, increment column
22. Selecting neighbouring 8 pixel values
23. Starting Clockwise from 12 o clock pixel
24. Check Neighbours (neighbours, points2, row_ max, col_max)
25. Selecting candidate pixel
26. Storing RGB values of 8 neighbouring pixels in 'pix'
27. Embedding the corresponding text in that pixel value
28. EACH NEIGHBOUR CONTAINS ONLY ONE BIT OF THE TEXT
29. Clearing last bit R Plane and B plane are indicators (Signature)(1 0 1 0 values) Only G Plane is used to store data
30. Difference between encoded and original

Decoding:

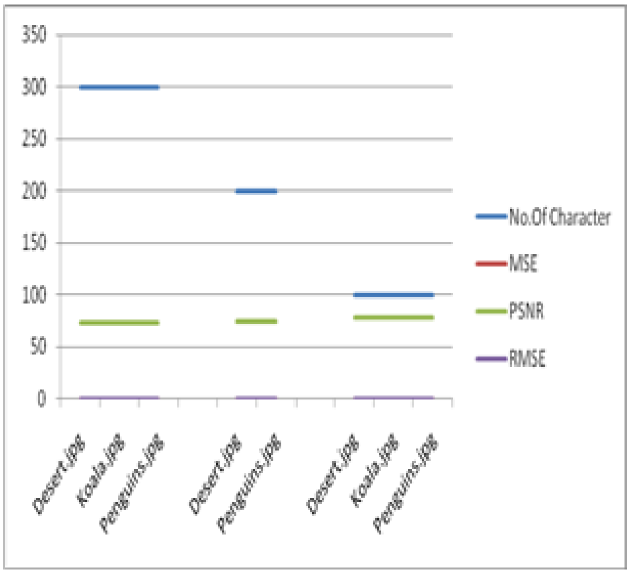
1. Input encoded image file
2. Final variable to hold the decoded character
3. Bit shift value
4. Selecting neighbouring 8 pixel values
5. Starting Clockwise from 12 o clock pixel
6. Selecting candidate pixel
7. Storing RGB values of 8 neighbouring pixels in 'pix'
8. Embedding the corresponding text in that pixel value
9. EACH NEIGHBOUR CONTAINS ONLY ONE BIT OF THE TEXT
10. Obtaining last bit
11. R Plane and B plane are indicators (1 0 1 0 values)
12. Only G Plane is used to store data
13. ODD number, end with 1
14. Else end with 0 by default (after clearing) end
15. If all conditions are true, obtain the embedded bit
16. Retrieve the text from the file

IV. RESULTS

During our implementation phase, we have tested our algorithm for different sets of images as well as text messages. For each and every normal bitmap images the proposed technique is working fine. Different parameters are been applied to test the quality of the image like Mean Square Error (MSE),Peak Signal to Noise Ratio (PSNR) and Root Mean Square Error (RMSE) with their results when applied to the image. As the length of the text increases the results of these parameters also varies. Thus more number of characters can be embedded into the image depending upon its size.

IV. A. TABULAR REPRESENTATION OF DIFFERENT PARAMETERS APPLIED TO IMAGE USING HARRIS LAPLACE DETECTOR:

Image format	No.Of Character	MSE	PSNR	RMSE
Desert.jpg	300	0.003628	72.56839	0.060231
Koala.jpg	300	0.003352	72.91196	0.057895
Penguins.jpg	300	0.003446	72.79172	0.058702
Desert.jpg	200	0.002385	74.38908	0.048841
Penguins.jpg	200	0.002385	74.38908	0.048841
Desert.jpg	100	0.001136	77.6129	0.033697
Koala.jpg	100	0.001167	77.49298	0.034166
Penguins.jpg	100	0.001106	77.72622	0.033261



V. CONCLUSION

This paper concludes that harris laplace algorithm is used to extract interest points and embed the text within the neighbour 8 bits which cannot be detected by any unauthorized users.

VI. REFERENCES:

[1].Presentation slides from Mikolajczyk et al. on their 2005 paper.

[2].Code, test Images, bibliography of Affine Covariant Features maintained by Krystian Mikolajczyk

[3].Bibliography of feature (and blob) detectors maintained by USC Institute for Robotics and Intelligent Systems

[4].Digital implementation of Laplacian of Gaussian

[5].Andrew Willis and Yunfeng Sui (2009). "An Algebraic Model for fast Corner Detection". 2009 IEEE 12th International Conference on Computer Vision. IEEE. pp. 2296–2302. doi:10.1109/ICCV.2009.5459443. ISBN 978-1-4244-4420-5.

[6].Shapiro, Linda and George C. Stockman (2001). Computer Vision, p. 257. Prentice Books, Upper Saddle River. ISBN 0-13-030796-3.

[7].Witkin, A. P. "Scale-space filtering", Proc. 8th Int. Joint Conf. Art. Intell., Karlsruhe, Germany,1019–1022, 1983.

[8].T. Lindeberg (2014) "Scale selection", Computer Vision: A Reference Guide, (K. Ikeuchi, Editor), Springer, pages 701-713.