I J C T A, 10(9), 2017, pp. 361-370 ISSN: 0974-5572
© International Science Press

Image Authentication Based on Salient Regions of Image

Thottempudi Pardhu* and R. Karthik**

ABSTRACT

Image authentication is always a key issue in this era of multimedia technology. As we are very much familiar with all numerous hacking techniques along with the availability of image editing tools such as Photoshop,Stir Marketc., Image security becomes a major issue, so this provides us with a lot of Research scope in the field of Image Authentication. Our paper presents a model to authenticate images transmitted across a non-secure channel. Therefore we propose the technique of image authentication based on the detection of Saliency Regions in the image and then forming a feature vector for the input image. Saliency regions are totally based upon the region of interest present in an image and it provides an accurate representation of texture features of the image.

Keywords: Multimedia Security; Saliency Detection;Hash Code; Image Authentication; Forgery Detection; Robustness

1. INTRODUCTION

Image Authentication is one of the key issue of this digital era and to this work we use Image hash, Image hash is a fixed length output from an input image. Hash is generated using the features of an image. As, the hash is shorter in length so, it is much faster to use. Image hash is used for many applications like image retrieval [1], image copy detection [2], digital water marking [3], image indexing [4], image authentication [5], image quality assessment [6], multimedia forensics [7]. Image hashing must satisfy two basic criterions which are: anti-collision capability [8], [9] and perceptual robustness. Perceptual robustness means that the hash for two visually same image must be same and along with this condition must be there that if any changes are made to the image then the hash must change drastically. Now to check the perceptual robustness property of our image authentication algorithm we have a total number of 60 operations over a single image , which includes brightness adjustments, contrast adjustments, salt and pepper noise addition etc. and to check the efficiency of this algorithm toward image forgery we have done experiments over sets of 250 images and their tampered versions Many hashing techniques have been developed in past years but most of them are sensitive toward the rotation property. As we know that the rotation is one of the content preserving operation which is not easy to model. So, in order to solve this problem we are proposing our algorithm which is almost independent toward the rotation of images. We have done the experiments with a total of 1900 images and their visually similar versions as well as their tampered versions.

The rest of paper is organisedas : Section II reviews the previous related work done in the field of image authentication then in Section III we will introduce you about the proposed method of image authentication then in Section IV we will discuss the results and after all in Section V we will conclude our work.

* Department of Electronics & Communication Engineering MLR Institute of Technology Hyderabad, India, *Email: pthottempudi2020@gmail.com*

** Department of Electronics & Communication Engineering MLR Institute of Technology Hyderabad, India, *Email: karthik.r@mlrinstitutions.ac.in*

2. RELATED WORK

Till date a lot of work has been done by many experts in field of image hashing .Several earlier methods have developed the image hash based on both local [10-15] and global [16-19] features of the Image. In [20], the author proposed that image hashing technique which was based upon the global features extracted using Zernike moments and local features using shape texture information of the image. In [21], Tang *et al* proposed an image hashing method by using the ring partition and NMF to obtain rotation robustness. Author has incorporated a secondary image by partitioning the original image in several rings and then applies NMF to it to get a lower dimensional hash representation of the image. Major drawback is leaving 21% information of an image, which is the corner of the image. If any changes are made in corers then the algorithm is not able to detect the forgery.

3. PROPOSED METHOD

The proposed method is a four stage method in the first step we will do the pre-processing over the image, in second step we will detect the Region of interest and then make a saliency map after all these steps, now we will apply blob analysis over the saliency map in order to find the characteristics of the detected saliency region.We will find the major axis and the minor axis of the detected blobs and then we will form a hash vector by using these characteristics, we will also use a secret key in order to make our hash more secure and key dependent.

3.1. Pre Processing

In order for the formation of hash vector we will first do the pre-processing on the input image, In this process we will first convert our image into M × M image by using bi-linear interpolation After this step, in

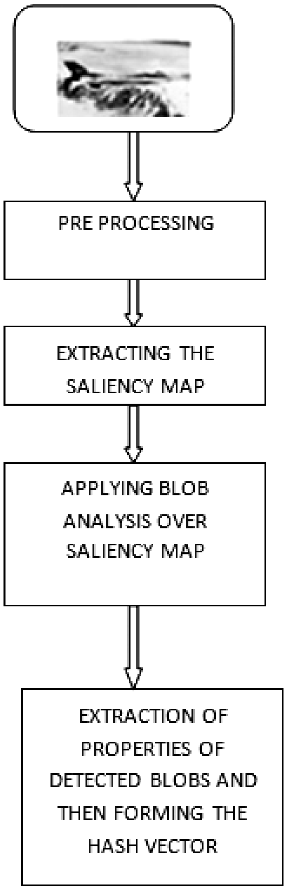

PRE PROCESSING
EXTRACTING THE SALIENCY MAP
APPLYING BLOB ANALYSIS OVER SALIENCY MAP
EXTRACTION OF PROPERTIES OF DETECTED BLOBS AND THEN FORMING THE HASH VECTOR

Figure 1: Flow chart of the Proposed method

order to remove the noise from the input image we will then pass our image from a Gaussian low pass filter with pre-defined characteristics. After removing the contamination of nose from the image , our image is ready for the next step, which is the saliency region detection.

3.2. Saliency Region Detection

Now, the main part of the algorithm comes into the scope, here we will detect the saliency map of the input image. The ability of the human for the detection of visual saliency is extraordinary and many algorithms are proposed in the past to do the computational modelling of this property of human beings, in order to make the field of image processing much and more successful. So, we will use the Saliency detection using a spectral residual approach [22]. Salient region of an image is defined as the region which attracts the visual. As per the authors of [22], the information stored in the image can be taken as the sum of two parts in which one consist of the innovation and the other is the prior knowledge. The first oneis the new and the second oneis redundant.

3.2.1. Log Spectrum

Scale invariance is one of the most famous and most widely used property [23, 24] of the invariant factors of the natural image statistics. This property is also famous with the 1/*f* law. The law states that the amplitude *P*(*f*) of the averaged Fourier spectrum of a natural image's ensemble obeys a distribution as follows:

$$E\left(P\left(f\right)\right) \propto \frac{1}{f} \tag{1}$$

When plotted on a log-log scale the amplitude of the ensemble of the images with averaged over the orientations, lies almost over a straight line, Instead of using the log-log spectrum we will use only log spectrum for the evaluation of the saliency region of the input image. Which is obtained as:-

$$S(f) = \log(P(f)) \tag{2}$$

3.2.2. Saliency Map

Now, we will do the process of detecting the saliency map, A system which is aiming at the minimization of the redundant visual data must be aware about the statistical similarities of the input stimuli. We must pay attention towards the information which is jumping out of the smooth curve. It is believed thatbecause of the regions of interest in the image there in the spectrum, statistical singularity exists.

The information regarding the saliency region is obtained when the redundant part is removed. To represent the general information of the image Log spectrum *S*(*f*) of an image is used. The reason behind is that the log spectra of different images similar and they contains the redundant information in them.

Let us denote the redundant information as the convolution between the log spectrum and an low pass kernel *k of l* × *l dimensions* as:

$$Q(f) = k * S(f) \tag{3}$$

Here, *k* is an *l* × *l* matrix defined as:

$$k = \frac{1}{l^2}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$$

Spectral residual which represents the novelty of the image, *P*(*f*) can be obtained by subtracting *Q*(*f*) from *S*(*f*). Then we will do the inverse Fourier transform of *P*(*f*) in order to get the Saliency map as:

$$M(x) = F^{-1}(Q(f) - S(f))$$

Now, we will take a threshold which will be equal to three times of the mean value of $M(x)$ to determine the salient regions in the input image. Salient regions for one of the benchmark images is shown in Fig. 2

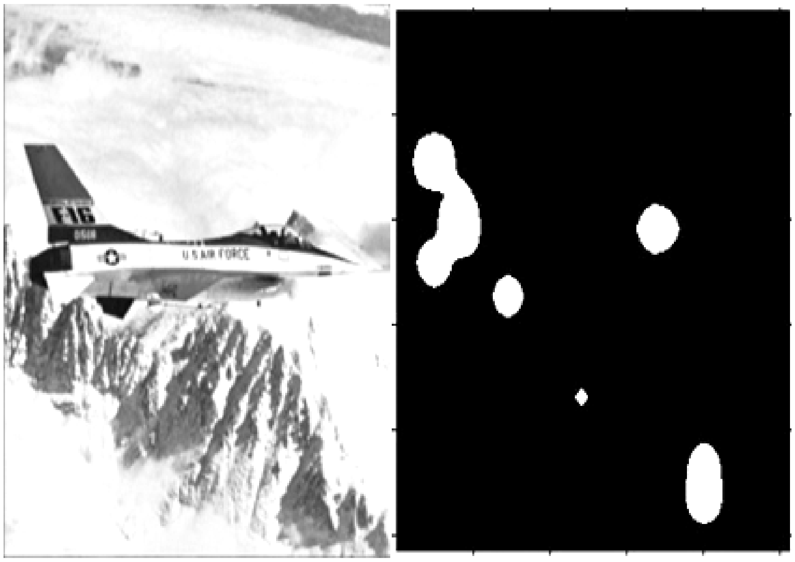


Figure 2: Saliency Region

3.3. Blob Analysis and Hash formation

After the extraction of the saliency map of the input image. Now, we will apply the blob analysis algorithm on the input binary image of saliency map. The Blob Analysis object computes statistics for connected regions in a binary image. In Image Processing, blob detection methods are used to detect regions in an image that differ in properties ascompared to the surrounding regions. In other way we can say that Blob is a region where some properties are almost constant. So we can say that all the points in the image are similar to each other. By using the Blob Analysis algorithm we can get many information regarding the blob which is detected over a connected region or we can say it in an indirect way that we can extract the information regarding the salient region of the image.

We can extract these below mentioned properties by using the blob analysis area, major axis, minor axis, centroid, bounding box coordinates etc. But for the formation of the hash we will take only major axis and minor axis. The reason behind this is that when forgery is done over an original image then we will get one more or one less salience region in the image, so we will get a major difference in the hashes of the forged image and the original image. Here after detecting the salient regions, it is not important that all the images have the same number of salient regions, so in order to solve this problem we will pad zeros in the shorter hash and then by doing so both the hashes will be of equal sizes.

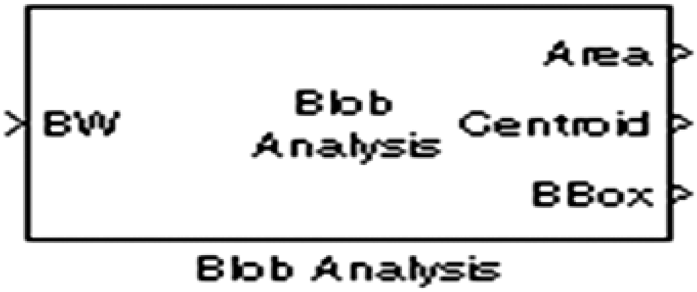


Figure 3: Blob Analysis

4. EXPERIMENTAL RESULTS

In this section we have tested our algorithm over a set of 1900 images to check its efficiency. The parameters used are 512×512 image size. For the comparison between the hashes of the images we have used L2 norm to evaluate the distance between the hashes and in the further paper we will denote it as Hash distance, Now initially we will discuss the results for the perceptual robustness of the image, in which we have done a total of 60 content preserving operations over a single image and we have taken a total of 30 color images from USC-SIPI Image database[24], and we have taken a total of 100 images from CASIA Tampered image deletion evaluation database[25] to check the efficiency of our hashing technique toward the forged images. So, we have taken a set of total $(60 \times 30) + (100) = 1900$ images to check the efficiency of the algorithm. After doing the analysis of the results we have taken our threshold value at the hash distance of 50. Now we will display the results for five benchmark images in fig, 4 in the form of graph in Table I, which are given below:

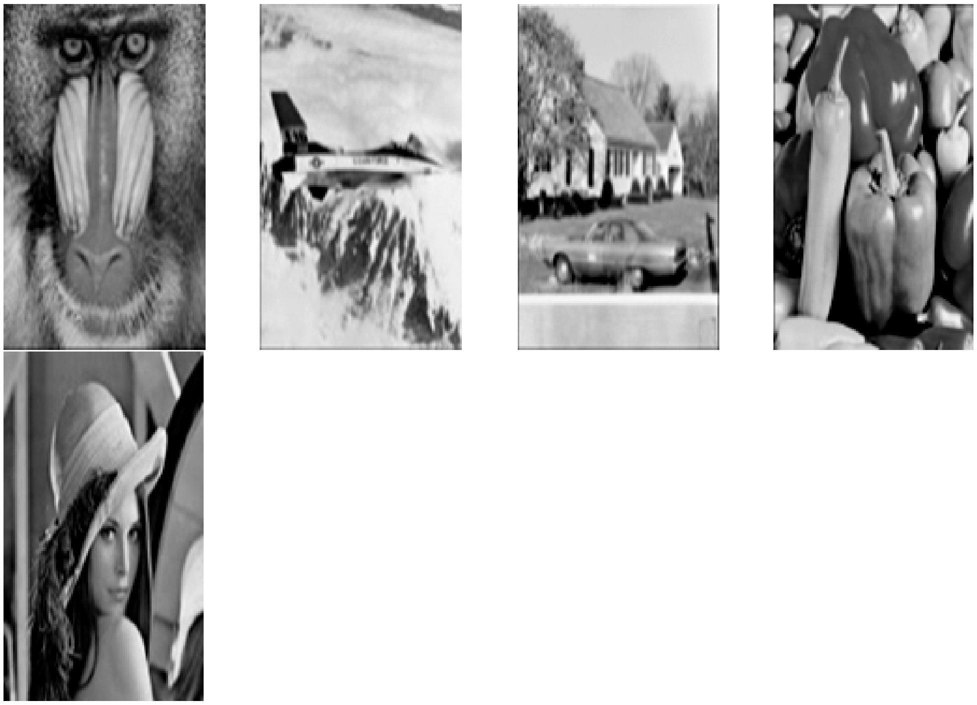
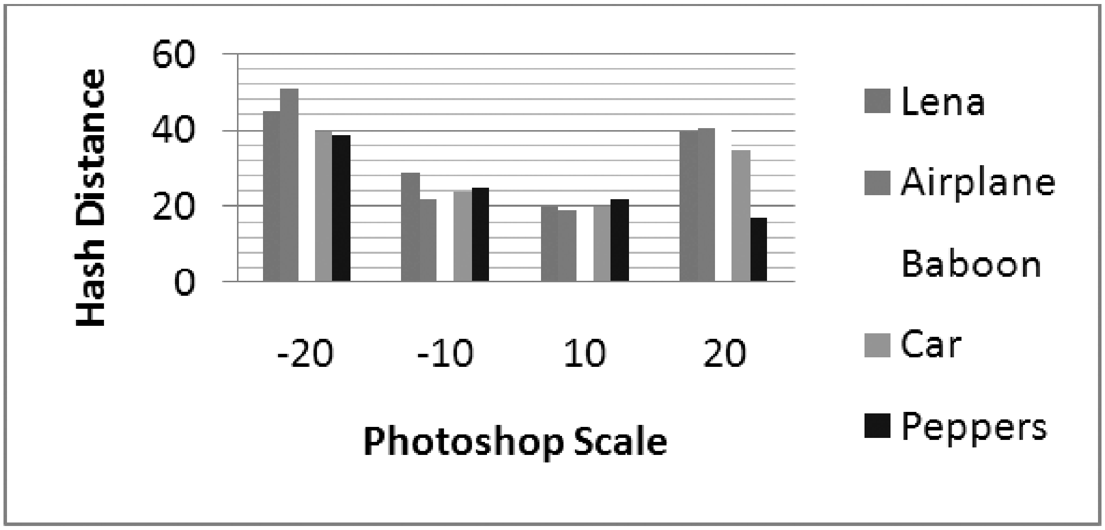
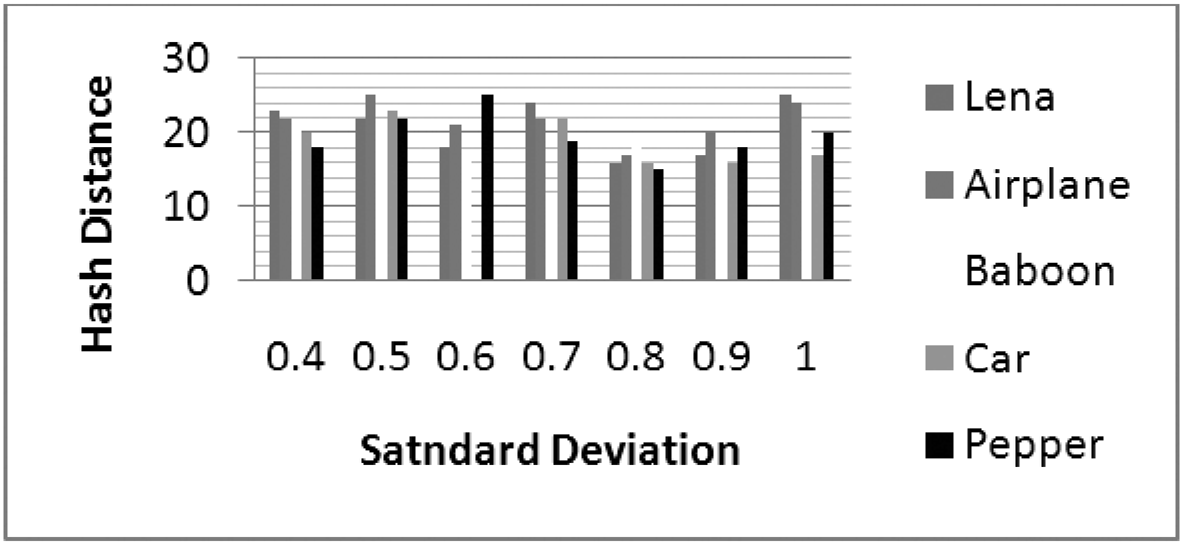


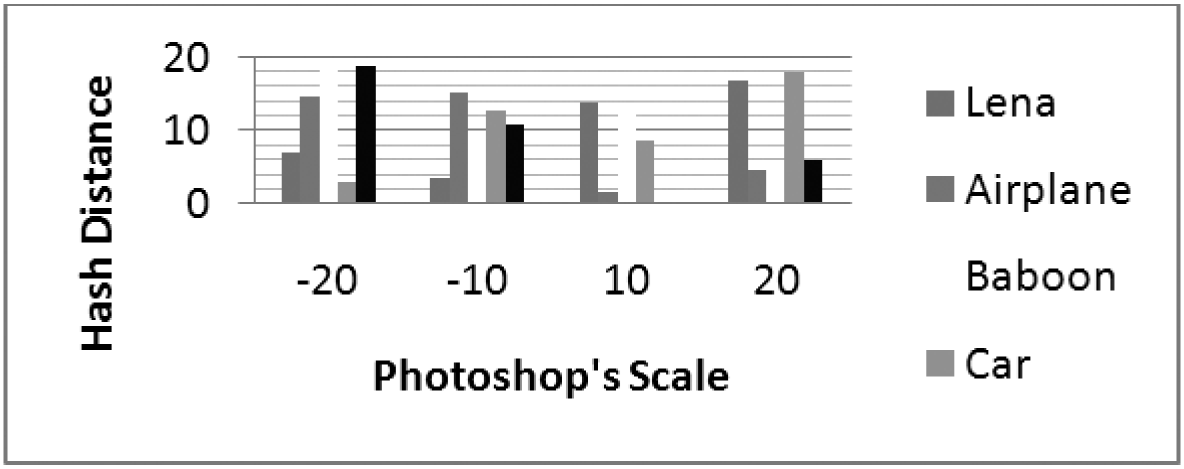
Figure 4: Benchmark Images



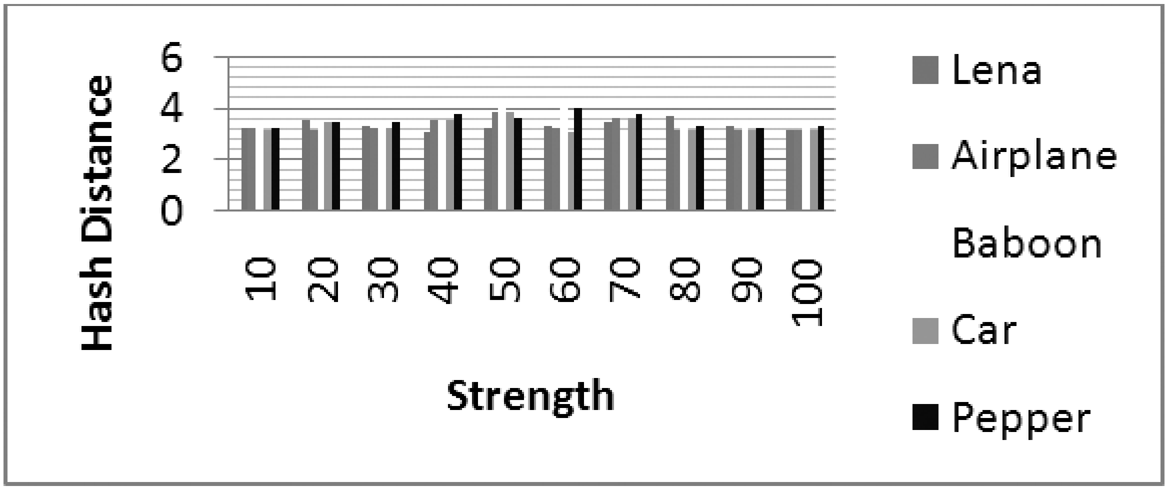
(a) Brightness



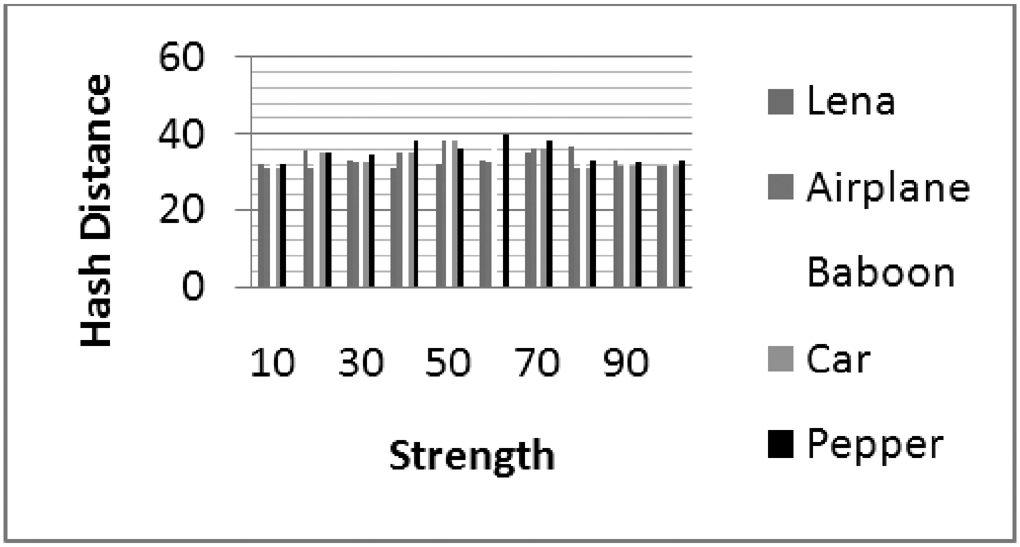
(b) Gaussian Filtering



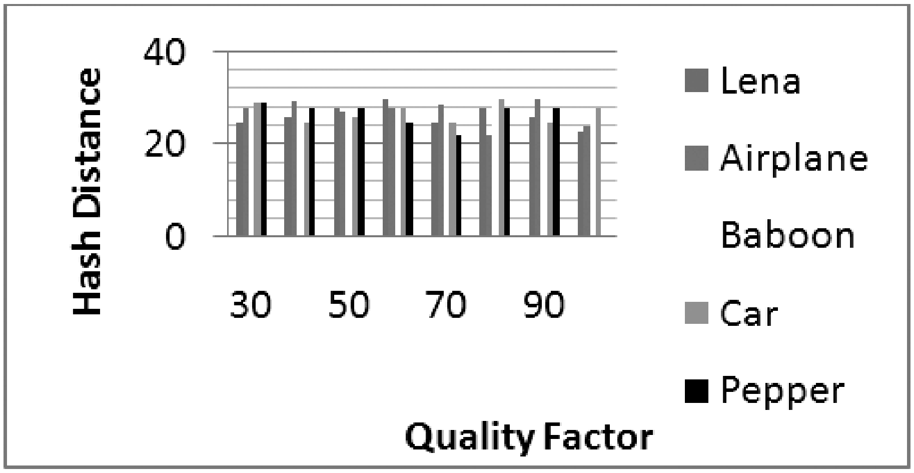
(c) Contrast



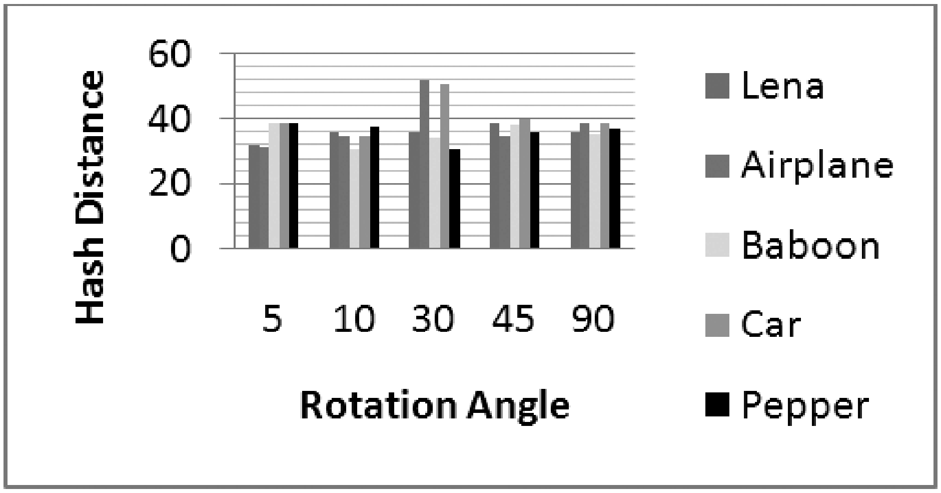
(d) Salt and Pepper Noise



(e) Watermarking



(f) JPEG Compression

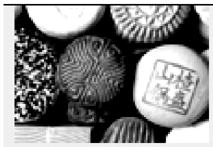
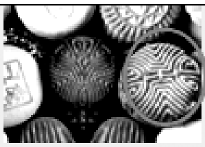
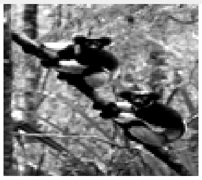
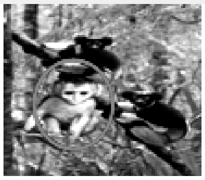
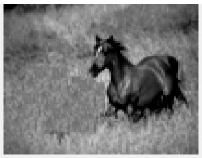
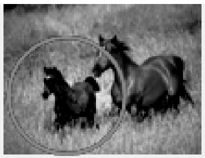
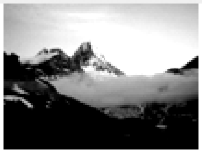
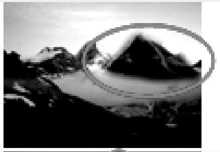
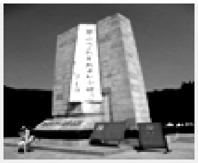
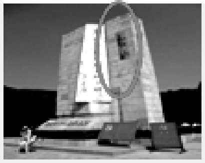


(g) Rotation

As from the above results we can see that all the values of hash distance are below the threshold value which is taken at 50 but the value of hash distance for the rotation with an angle of 30^o is greater than our threshold value and for the brightness adjustment or contrast adjustments with +20 & -20 are also near about to the value of threshold , the reason behind this is , when the brightness or contrast of an image is changed drastically then the texture of the image is also changed drastically and due to this the salient region which were not detected in the original image will now get detected very clearly. So, due to this we are getting a high value of hash distance. Now, the reason for the low values for other operations is very clear , as we know that the saliency map of an image is not going to change else any drastic forgery is made in the image. We have taken a total set of 30×60 = 1800 images for the efficiency test of our algorithm towards content preserving operation and we have found 12 images with the hash distance value greater than 60 So, finally the efficiency of our hashing technique for content preserving operations is $\frac{\left(60\times30-12\right)}{60\times30}\times100=99.33\%$. Now we will show the results for the tampered images in Table 1.

As from the results displayed above we can see that the values of hash distance for all the forged images are above the threshold except the threshold value of one image i.e. last image with the hash distance value of 48.9. This image is tested intentionally by us, aswe can see that the changes made in the image are very less so because of this the value of hash distance is less than threshold. We have tested our algorithm over 100 images and we have found that all the sets of images were having the value greater than the threshold value, or we can say that the values are far apart from the threshold value. So, our algorithm is having the efficiency of nearly about 100% for tampered or forged images. As we can see that if our algorithm is lacking behind in the case of Brightness adjustment then it is also gaining in the gamma correction. So, overall we can say that the proposed hashing technique is having agood anti-collision capability and perceptual robustness.

TABLE I

Original Image	Forged Image	Hash Distance
		85.8354
		106. 9698
		77.2895
		83.9754
		48.8998

5. CONCLUSION

We have proposed an image authentication technique by using saliency detection, which has a good robustness against most of the content preserving operation and it also have the good discriminative property for the tampered or forged images. As we have shown the comparison of our hashing technique with previous hashing algorithms and it shows a better discriminative as well as perceptual robustness proper as compared to the previous algorithms, It lacks somewhere when the rotation attack is considered or brightness or contrast adjustment is considered as compared to previous algorithms but it is also leading in the other properties. Now, after studying all the hashing techniques we can conclude that if one or more hashing techniques are merged together than we can achieve a good image hashing technique.

REFERENCES

[1] M. Slaney and M. Casey, "Locality-sensitive hashing for finding nearest neighbors [Lecture Notes]," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 128–131, Mar. 2008.

[2] C.-S. Lu, C. Y. Hsu, S.-W. Sun, and P.-C. Chang, "Robust mesh-based hashing for copy detection and tracing of images," in *Proc. IEEE Int.Conf. Multimedia Expo*, Jun. 2004, pp. 731–734.

[3] C. Qin, C.-C.Chang, and P.-Y. Chen, "Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism," *Signal Process.*, vol. 92, no. 4, pp. 1137–1150, 2012.

[4] E. Hassan, S. Chaudhury, and M. Gopal, "Feature combination in kernel space for distance based image hashing," *IEEE Trans. Multimedia*, vol. 14, no. 4, pp. 1179–1195, Aug. 2012.

[5] F. Ahmed, M. Y. Siyal, and V. U. Abbas, "A secure and robust hashbased scheme for image authentication," *Signal Process.*, vol. 90, no. 5, pp. 1456–1470, 2010.

[6] X. Lv and Z. J. Wang, "Reduced-reference image quality assessment based on perceptual image hashing," in *Proc. IEEE Int. Conf. ImageProcess.*, Nov. 2009, pp. 4361–4364.

[7] W. Lu and M. Wu, "Multimedia forensic hash based on visual words," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2010, pp. 989–992.

[8] R. Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin, "Robust image hashing," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2000,pp. 664–666.

[9] Z. Tang, X. Zhang, and S. Zhang, "Robust perceptual image hashing based on ring partition and NMF," *IEEE Trans. Knowl. Data Eng.*,vol. 26, no. 3, pp. 711–724, Mar. 2014.

[10] F. Ahmed, M.Y. Siyal, and V.U. Abbas (2010) A Secure and Robust Hash-Based Scheme for Image Authentication. Signal Processing 90(5); 1456-1470

[11] Z. Tang, S. Wang, X. Zhang, W. Wei, and Y. Zhao (2011) Lexicographical Framework for Image Hashing with Implementation Based on DCT and NMF. Multimedia Tools and Applications, 52(2); 325-345

[12] V. Monga and M.K. Mihcak (2007) Robust and Secure Image Hashing via Non-Negative Matrix Factorizations. IEEE Trans. Information Forensics and Security 2(3); 376-390

[13] F. Khelifi and J. Jiang (2010) Perceptual image hashing based on virtual watermark detection. IEEE Trans. Image Process 19(4); 981–994

[14] K. Fouad and J. Jianmin (2010) Analysis of the security of perceptual image hashing based on non-negative matrix factorization. IEEE Signal Process.Lett. 17(1); 43–46

[15] X. Lv and Z. J. Wang (2012) Perceptual image hashing based on shape contexts and local feature points. IEEE Trans. Inf. Forensics Security 7(3); 1081–1093

[16] S. Xiang, H. J. Kim, and J. Huang (2007) Histogrambased image hashing scheme robust against geometric deformations. in Proc. ACM Multimedia and Security Workshop pp 121–128.

[17] Z. Tang, S. Wang, X. Zhang, W. Wei, and S. Su (2008) Robust Image Hashing for Tamper Detection Using Non-Negative Matrix Factorization. J. Ubiquitous Convergence and Technology 2(1); 18-26

[18] A. Swaminathan, Y. Mao, and M. Wu (2006) Robust and Secure Image Hashing. IEEE Trans. Information Forensics and Security 1(2); 215-230

[19] Y. Lei, Y. Wang, and J. Huang (2011) Robust Image Hash in Radon Transform Domain for Authentication. Signal Processing: Image Comm. 26(6); 280-288

[20] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao (2013) Robust Hashing for Image Authentication Using Zernike Moments and Local Features. IEEE transactions on information forensics and security 8(1); 55-63

[21] Z. Tang, X. Zhang, and S. Zhang (2014) Robust perceptual hashing Based on Ring partition and NMF. IEEE transactions on knowledge and data engineering 26(3); 711-724

[22] XiaodiHou and Liqing Zhang Saliency Detection : A spectral Residual Approach. 2007 IEEE Conference on Computer Vision and Pattern Recognition P:1-8.

[23] (2007). USC-SIPI Image Database.[Online]. Available: http://sipi.usc.edu/database/

[24] CASIA Tampered image detection evaluation database [Online] Available : http://forensics.idealtest.org/.