Image Forgery Detection using Hash Functions

Sruthi S Menon, Mary Saana N J, Deepa G

Abstract: ***Digital images are widely spread in today's world and morphing of these images are also increased. Morphing of the images is the process of changing original image into another image using different tools. In social media the invasion of these morphed images are rapidly increasing and traditionally, the tampered images were found by the pixel comparison method. This way of detection leads to complexity and space consumption. pHash is used in this system as hashing algorithm.We effectively proposing a new and sophisticated technique to find morphed images using the features of pHash algorithm.***

Index Terms: Image Forging, p(Perceptual Hash)Hash, Retouching, Splicing, Cloning, Hexalisation, Comparison, Grayscale Conversion.

I. INTRODUCTION

Forging of the image is eliminating the essence of an image by adding substantial elements to the same. So we need to study the types of image forging before we go to the proposed algorithm.

- Image Retouching
- Image splicing
- Image cloning

Image Retouching

It is used to increase or decrease the digital image features.

Fig 1. Indication of Image Retouching

Revised Manuscript Received on May 22, 2019

Sruthi S Menon, Department of computer Science and IT, AmritaVishwaVidyapeethamUniversity/ Amrita School of Arts and Sciences Kochi ,India.

Mary Saana N J, Department of computer Science and IT, AmritaVishwaVidyapeethamUniversity/ Amrita School of Arts and Sciences Kochi ,India.

Deepa Gopinath, Department of computer Science and IT, AmritaVishwaUniversity/ AmritaSchoolofArtsandSciencesKochi ,India.

Image Splicing

It is the portions of two or more images are combined to form an individual image.

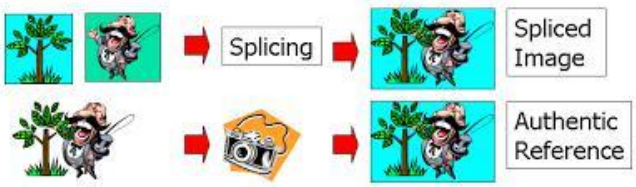

Fig 2. Indication of Image Splicing

Image Cloning

Replicating the constituents in the image to another image or duplicating in thesame figure.

Fig 3. Indication of Image Cloning

These are the basic image forging types. Usually, we use active & passive techniques for forging detection, but now we are introducing a new method for the same. Hash functions are using to find out the image whether it is morphed or not. In traditional methods like pixel comparison technique, we use pixels to detect the forged images, but this leads to system complexity and space issues. Traditional methods are really time-consuming so we can't rely this because of the technology changes day by day. Therefore, with the help of hash functions, we introduce a new type of detection mechanism.

II. PROPOSED SYSTEM

We found some disadvantages in the traditional pixel comparison method, so we proposed a new system in order to detect a forged image. Thepicture estimate in our framework is decreased and

afterward extracted the pixels from RGB components. In our proposed system we are extracting hash values from pixel components and comparisons are based on these hash values.

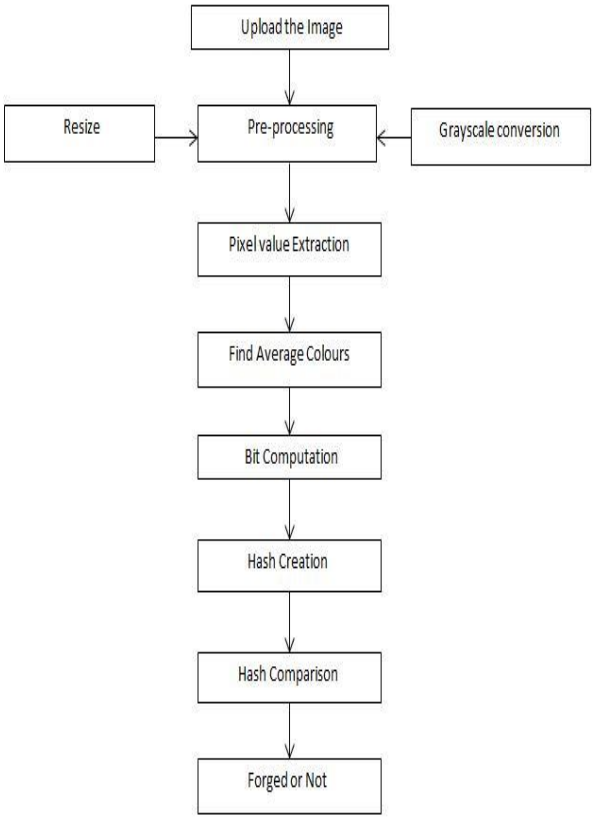

Fig 4. Proposed System

SL No	Method/Algorithm	Time in sec
1	Detection by fusion	12 sec
2	3 LSB detection	30 sec
3	2D wavelet Transform	21 sec
4	JPEG-Compression Model	55 sec
5	pHashing	6 sec

Fig 5. Comparison

III. ALGORITHM OVERVIEW

1) Upload the image
2) Pre-processing: Resizing the images into predefined size using normalisation technique
3) Pixel value extraction: Grayscale conversion can be done using the RGP Components and it is converted into black and white components.
4) From the black and white components, we are extracting white components because it is visible and black is invisible.
5) Hash conversion: White components are converted to hash functions using pHash algorithm. It has a c+ function in their p hash lib.
6) Hexalisation conversion. Hash values of white components are huge decimal values, so we convert it into hexadecimal values which have 10 to 20 numeric values.
7) Store these Hash values into Database.
8) Upload the forged image.
9) Repeat from step 2
10) Comparison: Hash value of the forged image will compare hash values in the database using the sequence matching technique.
11) Set Limit: Convert the output into a value between 0 and 1. Then sets 0.65 as a limit. So we can identify the similarity of images when the value rises from the limit. Hence we can detect the forgery in images. Pseudo code for this algorithm
1.Obtain Image
2.Reduce size 8x8 image.resize(8*8)
The fastest way to remove high frequencies and detail is to shrink the image. In this case, shorten it to 8x8 so that there are 64 total pixels.
3. Reduce color. Gray scale conversion mage.convert("L1"). The image dimensions 8x8 is converted to a gray scale. This

It is then changed over to gray scale by utilizing gray scale conversion. Using pHash algorithm, We can compute hash value from the extracted white components. This p Hash value will be higher. However, our main goal is to reduce space consumption, we are using hex alisation process in order to convert the huge hash values, so we get numeric values of length ranging between 10 to 20.Our system avails us reduce the system's intricacy and storage quandaries. At present we are using the pHash algorithm in order to convert it into hash values.It is a more convenient way to detect fraudulent images. It is comparatively easier and increases our storage capacity as well.

changes the hash from 64 pixels (Which means 64 red, 64 green, and 64 blue) to 64 total colors.

4. Average the colors.

l=getpixel(i,j)

r=getpixel(i+1,j)

if l>r append to a difference list compute the mean value of the 64 colors.

5. Optimize bits and Formulate hash.

decimal_value = 0

hex_string = list

iterate the difference list:

if true decimal_value += 2 ** (index % 8)

elsedecimal_value += 2 ** (index % 8)

This is the fun part.The value of the colour 0 or 1,which depends upon each and every bit.

6. Comparison

ratio= Sequencemater(i,j) where i and j are two hashes. If(ratio>0.6)

forged

Else

normal

IV. METHODS USED IN PROPOSED

SYSTEM A. Preprocessing

Preprocessing is defined as advancement of images that conquer the unwanted fragments or improvement of image features.

B. Grayscale Conversion

Grayscale conversion is defined as the conversion of RGB components(values 24bits) into grayscale components(value 8 bits).

C. Hashing

Hashing in image processing is developing a value from the components/pixels of images using mathematical functions. In our proposed system we use pHash algorithm or perceptual hash algorithm in order to find the hash values to corresponding pixel values.

V. PHASH ALGORITHM

1.Size reduction –reduce the size of image in order to start the process.

2. Colour reduction – grayscale conversion for colour reduction.

3. DCT (discrete cosine transform) computation – uses 32*32 DCT.

4.DCT reduction – converts 32*32 into 8*8 DCT.

5. Average value computation.

6. DCT reduction

7. Hash Construction

D. Hexalisation

Hexadecimal to binary is a conversion process involving the two mentioned number systems. The original number mentioned in base 16 is the hexadecimal and it is converted to binary format in base 2.

E. Comparison

Compare the hash values inorder to identify morphed or not. For Comparison we introduce a threshold of 0.6 value.

VI. RESULT

As part of this research, we uploaded random images to our system and stored it the system after extracting the P Hash Values. Then we tried to input Morphed images of the previous uploads, our system compared the Hash functions of both images and found both have same Hash Values and the result was positive as system found the Morphed Image and rejected it.

VII. CONCLUSION AND FUTURE WORK

Our research is paving a new path in the forged Image detection

system. We identified that the old Active and passive method consumes so much of the system space and complex to use. Our new method proves that forged Image detection is easier and system space consumption is much lesser. We succeeded in using P Hash method for the functioning through this research. We extracted the pixels and calculated Hash value and stored it. We used Hexalisation to lower the storage consumption. In this paperwe introduce an effective algorithm for check an image is forged or not. This algorithm works effectively than different algorithm. Be that as it may, the proposed framework can't accept more than one picture at any given moment. So future study is needed to accept more images simultaneously to improve the efficiency of algorithms.

REFERENCES

1. Zernike, Beugungstheorie des schneidenverfahres und seiner verbesserten form, der phasenkontrastmethode, Physica, 1934, 1, pp.689-704.
2. Z. Tang, S. Wang, X. Zhang, W. Wei and S. Su, Robust image hashing for tamper detection using non-negative matrix factorization. Journal of Ubiquitous Convergence and Technology, 2008, 2(\): 18-26.
3. Z. Tang, Perceptual Image Hashing: Framework, Methods, and Performance Evaluation, PhD dissertation, Shanghai University, 2009, pp.59-60.
4. M. Tagliasacchi, G. Valenzise and S. Tubaro.Hash-based identification of sparse image tampering.IEEE Transactions on Image Process. 2009, 18(\ 1):2491-504.
5. A. Swaminathan, Y. Mao and M. Wu, Robust and secure image hashing, IEEE Transactions on Information Forensics and Security, 2006, 1 (2): 215-230.
6. S. Bayram, I. Avcibas, B. Sankur, N. Memon, "Image manipulation detection with binary similarity measures", Proc. European SignalProcessing Conf., 2005.
7. H. Farid, Detecting digital forgeries using bispectral analysis, 1999.
8. J. Liao, R.S. Lima, D. Nehab, H. Hoppe, P.V. Sander, Yu J.**Automatingimage morphing using structural similarity on a halfway domain**
9. ACM TOG, 33 (5) (2014) 168:1–168:129.S. Xiang, H. J. Kim and J. Huang, Histogram-based image hashing scheme robust against geometric deformations, Proc. of the ACM Multimedia and Security Workshop, ACM Press, 2007, pp. 121-128.
10. F. Ahmed, M.Y. Siyal and V. U. Abbas, A secure and robust hash-based scheme for image authentication, Signal Processing, 2010, 90(5): 14561470
11. D. Wu, X. Zhou and X. Niu. A novel image hash algorithm resistant to print-scan, Signal Processing, 2009,89(\2): 2415-2424.
12. E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," IEEE Trans. Antennas Propagat., to be published.
13. J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," IEEE J. Quantum *Electron.*, submitted for publication.
14. C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
15. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy
studies on magneto-optical media and plastic substrate interfaces(Translation Journals style)," *IEEE Transl. J. Magn.Jpn.*, vol. 2, Aug. 1987, pp. 740–741 [*Dig. 9th Annu. Conf. Magnetics* Japan, 1982, p. 301].
16. M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science, 1989.
17. (Basic Book/Monograph Online Sources) J. K. Author. (year, month, day). *Title* (edition) [Type of medium]. Volume(issue). Available: http://www.(URL)
18. J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com
19. (Journal Online Sources style) K. Author. (year, month). Title. *Journal*
[Type of medium]. Volume(issue), paging if given. Available : http://www.(URL)
20. R. J. Vidmar. (1992, August). On the use of atmospheric plasmas as electromagnetic reflectors. *IEEE Trans. Plasma Sci.* [Online]. *21(3).* pp. 876—880. Available: http://www.halcyon.com/pub/journals/21ps03-vidmar.

AUTHORS PROFILE

Sruthi S Menon MCA Scholar at Amrita University, Amrita School of Arts & Sciences, Kochi, Kerala, India.

Mary Saana N J MCA Scholar at Amrita University, Amrita School of Arts & Sciences, Kochi, Kerala, India..

Deepa G Assistant Professor at Amrita University, Amrita School of Arts & Sciences, Kochi, Kerala, India.