Paper Title* (use style: *paper title*)

*Note: Sub-titles are not captured in Xplore and should not be used

line 1: 1st Given Name Surname
line 2: *dept. name of organization (of Affiliation)*
line 3: *name of organization (of Affiliation)*
line 4: City, Country
line 5: email address or ORCID

line 1: 2nd Given Name Surname
line 2: *dept. name of organization (of Affiliation)*
line 3: *name of organization (of Affiliation)*
line 4: City, Country
line 5: email address or ORCID

line 1: 3rd Given Name Surname
line 2: *dept. name of organization (of Affiliation)*
line 3: *name of organization (of Affiliation)*
line 4: City, Country
line 5: email address or ORCID

Abstract— With the rise in social media and internet users there is a raise in the images data around the globe. Many images are edited and are represented in a different meaning for own benefits of a user, this is called as Image Forgery. The detection of such images is important as it can create fake news or false information. This paper intends to propose the solutions for the former problem through hashing method.

Keywords—component, formatting, style, styling, insert (*key words****)***

I. Introduction

Image Forgery is a method where a image is taken and edited and presented in such a way that the information or the meaning is changed. This method is widely used in create false information or misleading news and can be spread through digital media. The changes introduced in a image in this method are done in such a way that a normal user cannot be able to understand if the image is manipulated or is a original image. But with the use of hashing on a block of pixel values it can be decided that if the image is being manipulated or not.

This paper offers method to implement the use of hashing algorithm on top of an image and compare the hash values for the pixel blocks to decide if the image is forged. Hash functions always generate a unique value for a distinct data, and this can be beneficial when it comes to images as there are many pixel combinations. So, this problem can be covered through hashing functions.

The hashing is better compared to a machine learning method as hashing does not require additional data gathering and training. Also compared to a conventional machine learning there are less compute power required to run and deploy the method.

II. Image Forgery Detection Algorithm

A. *MD5 Algorithm*

For this method the MD5 algorithm is selected as I provide check sum for data integrity. MD5 will take a series of integers in our scenario it will be a series of pixels values and will generate a hexcode as a hash value of a particular image block.
The hash function will take one input an Image I to generate hash value h=H(I).

B. *Image Preperation:*

Both original image and tampered image are compressed, and the length and height are reduced as per equation:

C = (B / W)
height = (H* C)
So, the dimension of the adjusted image will be (B x height).

C. *Image tiling:*

The adjusted image is taken and divided into 25 sub images called as tiles.

D. *Calculate Image hash value of each tile.*

Each tile will have a Hash value generated using MD5 algorithm. As shown in below image the hash value of each 25 tiles is calculated.

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

E. Compare image and highlight tampered image tile.

If the hash value of a tile is not equal to the respected original tile hash value than that tile is taken, and a border is made in order to highlight the image. As shown in blow image.

F. Forgery Detection Algorithm

Step1: Adjust the images and compress the pixels of the image.

Step2: Divide both original and forged compressed image into 25 parts.

Step3: Calculate the Hash value of every tile for both the images.

Step4: Compare the Hash value with the respected tile.

Step5: Draw borders in the tile if the Hash value is different.

Step6: Merge the image with highlighted forgery edits in the image.

G. Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

III. Experimnetal Results

Image Forgery can be classified into a categories like copy move, splicing and rotation.

Attacks and its handling:

A. Copy Move:

This attack includes of a duplication of an object from insides of an image or from an external image. In below figures it can be shown that in tempered figures there are more coins than of the original image.

(a)Original

(b)Tampered

B. Splicing Move:

This attack contains a part of image which is taken from another image and included in the images. In the below figure you can see that the part of the images is being copied and edited in the images as per the tampered image.

C. Rotation:

In this attack the image presented is rotated around any of its axis(horizontally or vertically) as shown in below image.

IV. Related Work

The template is designed for, but not limited to, six authors. A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This

is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity "Magnetization", or "Magnetization, M", not just "M". If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write "Magnetization (A/m)" or "Magnetization {A[m(1)]}", not just "A/m". Do not label axes with a ratio of quantities and units. For example, write "Temperature (K)", not "Temperature/K".

ACKNOWLEDGMENT *(Heading 5)*

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression "one of us (R. B. G.) thanks ...". Instead, try "R. B. G. thanks...". Put sponsor acknowledgments in the unnumbered footnote on the first page.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.