iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: I Month of publication: January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1236

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Copy-Move Forgery Detection Using Moment Invariants

T. Sudheer Kumar[1]
[1]ECE Department, JNTUH University

Abstract*: Digital Forensics is a branch of forensic science which is related to cybercrime. It basically involves the detection, recovery and investigation of material found in digital devices. Digital images and videos plays most important role in digital forensics. They are the prime evidences of any crime scene. So the fidelity of the image is important. Digital images can be easily manipulated and edited with the help of image processing tools. Copy-move Forgery is the most primitive form of cyber-attack on digital images. Integration of color perception and object representation generates a powerful feature vector of reasonable size which ensures detection against different types of challenges. Experiments on benchmark dataset demonstrate the efficiency and robustness of the proposed approach on different image post processing methods.
***Keywords*: Forgery, forensics, dataset, Moment Invariants, Colour space**

I. INTRODUCTION

Digital Forensics is a branch of forensic science which is related to cyber-crime. It basically involves the detection, recovery and investigation of material found in digital devices. The digital forensic is commonly known as Computer forensic. In nowadays it is not just related with the computer device because the forensic has expended to cover investigation of all the devices which are able to store the digital data. Digital forensics is the process of uncovering and interpreting electronic data for use in a court of law. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.
Digital data like image and video plays most significant role in digital forensics. The authenticity of an image is the major issue in digital image forensic they are the most powerful form of evidences in media-broadcast industry as well as in the courtroom. The improvement and advancement of technology raises questions about the reliability of the digital images or videos, because of the cheap availability of the software and powerful image processing tools.

A. Digital Image Forgery

Image forgery is basically divided into broad approaches: Active approach and Passive Approach. The active approach involves digital watermarking and digital signature while passive approach involves tempering in images. The area of work is focused on Passive part of the forgery. In nowadays many digital forgeries are developed like Image splicing, retouching And copy-move Forgery. Image splicing makes composite image by joining two or more images[14]. Image retouching is a process of enhancing image features such as sharpness, color adjustment, white balance etc.

B. Copy-Move Forgery

Copy-move forgery is the most primitive form of cyber-attack on digital images. In copy-move forgery a part of image (region) itself is copied and pasted into another part of the same image. The intention of the attacker behind this is to “add” or “disappear” some objects from the image. Hence to break the fidelity of the image and fool the viewer[5]. Copy-move attack is more prevalent in images having uniform texture or patterns, for e.g. sand, grass, water etc.
In the copy-move forgery detection the exact block matching gives appropriate results only when the copied region is directly pasted i.e. duplication is performed without any transformations. If in case the copied region being transformed geometrically then blocks matching and correlation methods are fail to detect the forgery[1]. So that we need some technique which gives correct matching in this situation the overall idea of proposed approach is depicted in the figure at first, the input RGB image is converted to both Gray scale and Lab color space images. From both converted images, overlapping square blocks are extracted and targeted feature vectors are generated.
Finally, the forged block is detected by close matching from the sorted feature vectors. Moment invariants-based features: features based on Moment Invariants representing any small gray level region with respect to translation, rotation and scale changes.

©IJRASET (UGC Approved Journal): All Rights are Reserved

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Fig: 1: Example of copy-move forgery

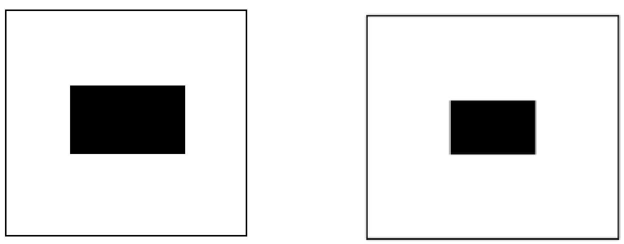
II. MOMENT INVARIANTS

An essential issue in the field of pattern analysis is the recognition of objects and characters regardless of their position, size and orientation as illustrated in figure 2. The idea of using moments in shape recognition gained prominence when Hu (1962), derived a set of invariants using algebraic invariants[15]. Two-dimensional moments of a digitally sampled M X M image that has gray function f *(x, y)*, (*x y*=0, 1, 2…M- 1) is given as

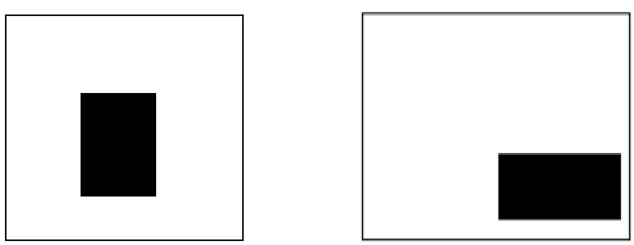
$$m_{pq} = \sum_{x=0}^{x=M-1} \sum_{y=0}^{y=M-1} x^p . y^q f(x,y) \qquad (1)$$

The moments f(x, y) translated by an amount (a, b) are defined as,

$$\mu_{pq} = \sum_x \sum_y (x+a)^p (y+b)^q . f(x,y) \qquad (2)$$



(a) (b)



(c) (d)

Fig.2 (a) 2-d object (b) change of size (c) change of orientation (d) change of position

III.BASIC TERMS AND MATHEMATICAL FOUNDATION

First we define the basic terms which will be then used in construction of the invariants

A. Definition 3.1

By image function (or image) we understand any real function f(x, y) having a bounded support and a finite nonzero integral

B. Definition 3.2

Fourier transform (or spectrum) F (u, v) of the image f(x, y) is defined as

©IJRASET (UGC Approved Journal): All Rights are Reserved

$$F(u,v) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-2\pi i(ux+vy)} f(x,y)dxdy \qquad (3)$$

Where i is the complex unit

C. Definition3.3

Geometric moment "m_{pq} "of image f(x; y), "m_{pq} " where p,q are non-negative Integers and (p + q) is called the order of the moment, is defined as

$$m_{pq}^{(f)} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x^p\, y^q\, f(x,y)dxdy \qquad (4)$$

Corresponding central moment μ_{pq} of order (p+q) of this image f(x, y) is defined as

$$\mu_{pq}^{(f)} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}(x - x_t^{(f)})^p\,(y - y_t^{(f)})^q\, f(x,y)dxdy \qquad (5)$$

Where the coordinates

$$x_t^{(f)} = \frac{m_{10}^{(f)}}{m_{00}^{(f)}}$$

$$y_t^{(f)} = \frac{m_{01}^{(f)}}{m_{00}^{(f)}}$$

Where the coordinates $\left(x_t^{(f)}, y_t^{(f)}\right)$ denotes the Centroid

D. Definition3.4

Complex moment "C (f) $_{pq}$" of order (p + q) of the image f(x; y) is defined as

$$c_{pq}^{(f)} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}(x+iy)^p\,(x-iy)^q\, f(x,y)dxdy \qquad (6)$$

Where i is the complex unit

E. Definition3.5

h(x, y) is Central symmetry image function and the imaging system is energy preserving that is

$$h(x,y) = h(-x,-y) \qquad (7)$$

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} h(x,y)\, dxdy = 1 \qquad (8)$$

Most real sensors and imaging systems have PSF s with certain degrees of symmetry. In many cases they have even higher symmetry than central, such as axial or radial symmetry[10]. Thus, the Central symmetry assumption is general enough to describe almost all practical situations.

F. Definition3. 6

The Centroid the blurred image "g(x, y)" is related to Centroid of the original image "f(x, y)" and that of PSF "h(x,y)" as

$$x_t^{(g)} = x_0^{(f)} + x_0^{(h)} \qquad (9)$$

$$y_t^{(g)} = y_0^{(f)} + y_0^{(h)} \qquad (10)$$

In particular if h(x, y) is centrally symmetric then $x_0^h = y_0^h$ =0 and in such case we have $x_0^g = x_0^f, y_0^g = y_0^f$

IV. ORTHOGONAL MOMENTS

Cartesian moments, are formed using a monomial basis set $x^p\, y^q$ this basis set is non-orthogonal and this Property is passed onto the Cartesian moments. These monomials increase rapidly in range as the order Increases, producing highly correlated descriptions[9]. This can result in important descriptive information being contained within small differences between moments, which lead to the need for high computational precision.

However, moments produced using orthogonal basis sets exist. These orthogonal moments have the advantage of needing lower precision to represent differences to the same accuracy as the monomials. The Orthogonallity condition simplifies the reconstruction of the original function from the generated moments. Orthogonallity means mutually perpendicular, expressed mathematically two functions y^m and y^n are orthogonal over an interval $a<x<b$ if and only if:

$$\int_a^b y_m(x) y_n(x)\, dx = 0; \qquad m \neq n \tag{11}$$

Here we are primarily interested in discrete images, so the integrals within the moment descriptors are replaced by summations. It is noted that a sequence of polynomials which are orthogonal with respect to integration, are also orthogonal

V. EXPERMIENTS AND RESULTS

This section contains outputs of detection of geometric distortions in copy-move forgery. The forgeries are rotation, re-scaling, direct copy-move and both rotation and re-scaling. Figure 3 is our test image. We have taken standard 512 × 512 Gray scale Lena image. All the geometric transformations are performed on this image. If the image is color image then first we have to convert it into gray image by using rgb2gray (image).

Fig: 3: Test image size of size 512x512

Figure.4 depicts all the SIFT key-points extracted from different scales. All the key-points are invariant. Similarly we are extracting the SIFT key-points for the forged image also. Each SIFT key-points have 128 dimension feature vectors. These 128 dimensional vectors are comes from orientations an magnitudes of the key-points

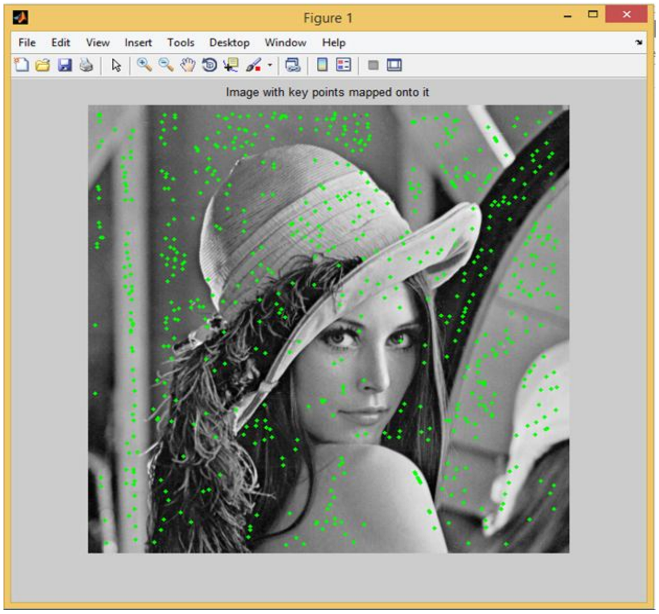


Fig.4:Key points mapped in to image

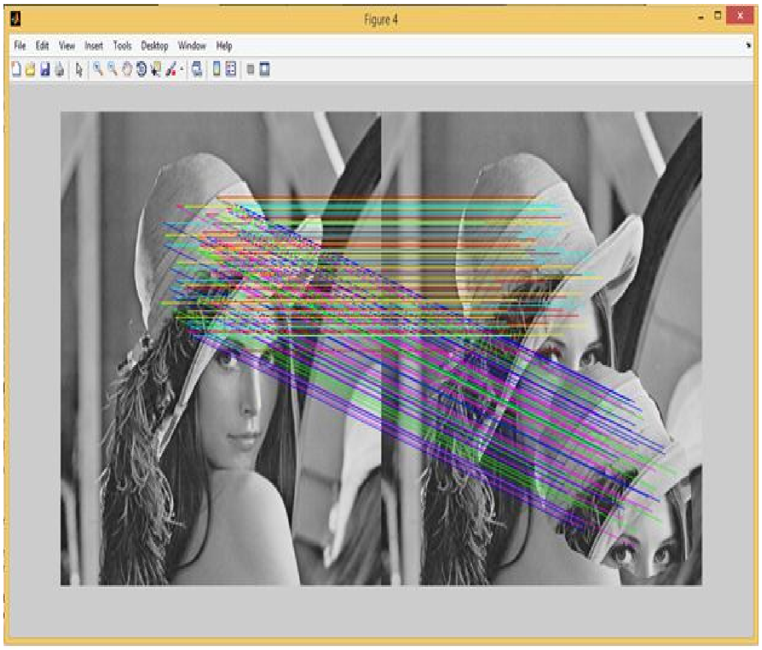


Fig: 5: Detection of copy-move image using moment invariants

In this image we have copied a region and pasted into another location. The colourful line shows the matched original region and forged region in the image. The 128 feature vectors of the SIFT key-points in both regions must be same. In direct copy-move attack the duplicated region is directly pasted into another location without any distortions. When we are comparing the key-points according to their 128 dimensional feature vector, all key-points at both the regions having same 128 dimensional feature values

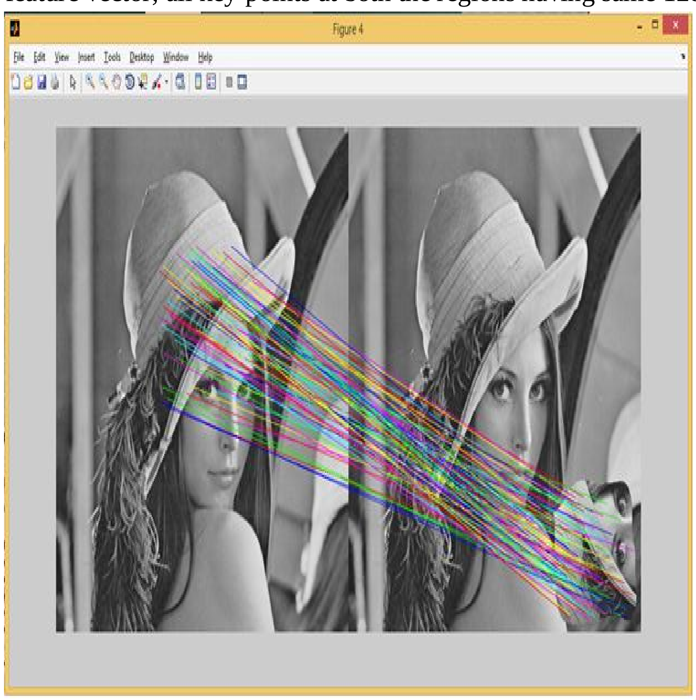


Fig: 6 Detection of copy-move forgery with both rotation and re-scaling operations

In figure 6 we have taken a region and perform rotation and re-scaling on that region and that we have pasted it. The matching lines show the mapping between original region and forged region. The re-scaling is the dominating factor in this forgery. Because rotation does not affect the number of key-points but re-scaling changes the number of key-points extracted

©IJRASET (UGC Approved Journal): All Rights are Reserved

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Moment Invariants	Average F-Measure
DCT	0.90
PCA	0.85
LEGENDRE	0.91
ZERNIKE	0.92
SIFT	0.89

VI. CONCLUSION

In this paper we have proposes an efficient method to detect copy-move forgery in digital images. The proposed method is also capable of detecting geometric transformations applied on the forged region, with the help of SIFT key-points and Moment invariants. Our experimental results prove that the proposed method can detect a region duplication forgery, in which rescaling and rotation attacks are applied together or individually on the duplicated region. The proposed method is more effective and gives better Performance than the exact block matching techniques, in terms of geometric attacks detection in region duplication.

REFERENCES

[1] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra. A sift-based forensic method for copy–move attack detection and transformation recovery. InformationForensics and Security, IEEE Transactions on, 6(3):1099–1110, 2011.

[2] Sevinc Bayram, Husrev T Sencar, and Nasir Memon. An efficient and robust method for detecting copy-move forgery. In Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, pages 1053–1056. IEEE, 2009.

[3] Yanjun Cao, Tiegang Gao, Li Fan, and Qunting Yang. A robust detection algorithm for copymove forgery in digital images. Forensic science international, 214(1):33–43, 2012.

[4] Vincent Christlein, Christian Riess, and Elli Angelopoulou. On rotation invariance in copy move forgery detection. In Information Forensics and Security (WIFS), 2010 IEEE International Workshop on, pages 1–6. IEEE, 2010.

[5] A Jessica Fridrich, B David Soukal, and A Jan Luk´aˇs. Detection of copy-move forgery in digital images. In in Proceedings of Digital Forensic Research Workshop. Citeseer, 2003.

[6] Mohammad Farukh Hashmi, Vijay Anand, and Avinas G Keskar. Copy-move image forgery detection using an efficient and robust method combining un-decimated wavelet transform and scale invariant feature transform. AASRI Procedia, 9:84–91, 2014.

[7] Hao-Chiang Hsu and Min-Shi Wang. Detection of copy-move forgery image using gabor descriptor. In Anti-Counterfeiting, Security and Identification (ASID), 2012 International Conference on, pages 1–4. IEEE, 2012.

[8] Li Jing and Chao Shao. Image copy-move forgery detecting based on local invariant feature. Journal of Multimedia, 7(1):90–97, 2012.

[9]] Li Kang, Xiao-pin Cheng, K Li, and C Xiao-ping. Copy-move forgery detection in digital image. In Proc of the 3rd International Congress on Image and Signal Processing.[S. l.]: IEEE Computer Society, pages 2419–2421, 2010.

[10]] Weihai Li and Nenghai Yu. Rotation robust detection of copy-move forgery. In Image Processing (ICIP), 2010 17th IEEE International Conference on, pages 2113–2116. IEEE, 2010.

[11] David G Lowe. Distinctive image features from scale-invariant keypoints. International journal of computer vision, 60(2):91–110, 2004.

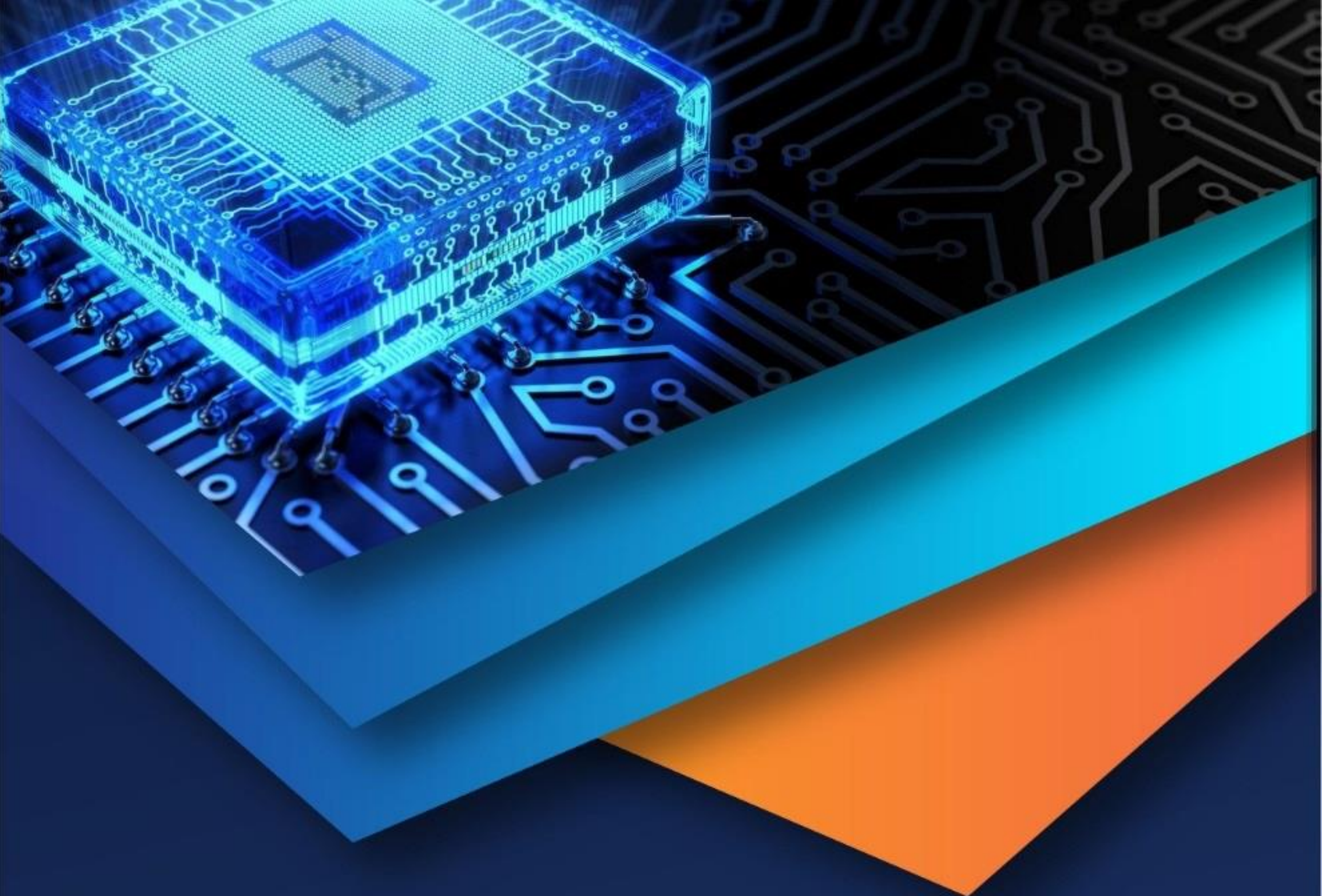
[12] Babak Mahdian and Stanislav Saic. Detection of copy–move forgery using a method based on blur moment invariants. Forensic science international, 171(2):180–189, 2007.

[13] Xunyu Pan and Siwei Lyu. Detecting image region duplication using sift features. In Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on, pages 1706–1709. IEEE, 2010.

[14] Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee. Detection of copy-rotate-move forgery using zernike moments. In Information Hiding, pages 51–65. Springer, 2010.

[15] Resmi Sekhar et al. Recent block-based methods of copy-move forgery detection in digital images. International Journal of Computer Applications, 89(8):28–33,2014

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

INDEX COPERNICUS 45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)