iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4073

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 IV, April 2018- Available at www.ijraset.com

Forensic Technique for Social Network Provenance Classification of Images

Dhanyaja P[1], Reshma V K[2]
[1, 2] *Computer Science and Engineering, Jawaharlal College of Engineering and Technology, Lakkidi, Palakkad, Kerala*

Abstract: ***The unprecedented popularity of various online social networks (OSNs) makes a rapid development to share digital contents online. However, misusing and dissemination of online contents widely happens. Under this circumstance, the identification of the origin and the propagation path of an online image are crucial for many forensic applications. It is a tough task to trace out background details and pre processing of digital image by forensic scientists. Strategic way to address a problem is to simply find image's history: knowing acquisition device and model of camera etc. This paper enlightens image classification based on originating social network. Since image has distinctive traces by social network. Manipulation process will be unique for each social network. Social network provenance based image classification is done through resorting at a trained multi-SVM classifier. Experimental results administrated are distinction attainable on numerous image datasets and in varied operative conditions. Additionally, technique is to go back to the initial JPEG quality image had before being uploaded on a social network.***

Keywords**: *Image classification; Social networks; JPEG; Quality factor; Provenance identification.***

I. INTRODUCTION

Multimedia contents are widely created and spread through various web applications. These digital assets are variably transferred through internet are prone to be misused. Social Networks (SN) are constituted as a real-time source of information used by criminals and attackers as well. Transparent nature of social networking sites are way for criminals to interrogate into. Recent studies are showing almost 500 million people are using social networking sites every day and that much of information is being transferred through it.

Phenomenal increase in the use of Internet and Smartphone owe to take a picture and transferred through one or more social networks at the same time. Day today life is easier so that, on the other side, illegal activities like misusing such digital contents making issues. As multimedia forensics security deals with both the identification of digital content origin and the reconstruction of its history. Find whether the image is authentic or has been manipulated to change its initial representation and meaning is the aim. Recovering all the featured details of image could be satisfactorily help in investigation. Retracing history of image or a video, by resorting at its EXIF metadata is fundamental but low reliability due to easily modifiable or even erasable prevent it from using. On the other hand, reliability can be achieved by analyzing traces on image pixels due to certain manipulations. Many methodologies to assess on the image/video manipulations are literature. They are for differentiating originating devices but the idea, behind this work, is to discern image based on transformed social network (*provenance*) by analyzing some traces on it by that platform.

All the image related issues can be addressed by analyzing this like a forensic technique. In addition to this, technique will enlarge the solution domain regarding image authentication and forgery issues. A better strategic movement can be done with comments, share and like features of social media to advertize based on users behavior. That couldn't make much more sense while provenance classification is not concerned here.

The paper is organized as follows: Section II presents some previous works inherent to the problem of recovering information about the origin and the history of a digital image while Section III introduces the proposed methodology; in Section IV some characteristics of the social networks taken into consideration within this work are reviewed and in Section V various experimental results are discussed to evaluate the performances of the presented technique. Section VI draws conclusions and Appendix A provides some implementation details to interact with APIs made available by the different social networks.

II. RELATED WORK

Image forensic scientific community has to find image history to classify an image based on through which social network it has been uploaded [1], [2] and [3]. Understanding information about the image could be beneficial for the classification, it includes knowing the acquisition device [4], [5], [6], [7], the device model [8], [9], [10], [11], [12]. All these works are based on the concept of having some fingerprint traces in the digital contents of image due to the acquisition process and pre-processing.

The image creation processes varies with various devices. In case of pre-processing that is depends on the device as well as social network platform. Since all these are image manipulations that are giving characteristic changes to images. For example, digital camera identification of image is done based on PRNU (Photo Response Non-Uniformity) noise characteristic [12]. Reduce computational time and maintaining accuracy, with the number of cameras and images are increased digest-based descriptor is taken into account [13], [14]. Open set scenario is depicted in [15], [16] using enhanced version of PRNU to distinguish among images taken by unknown digital cameras.

Extracting robust and characterizing features to distinguish among various classes of originating devices like scanned images, photos, and computer. Distinctive digital content fingerprints created during the image acquisition process are examined here. A set of provenance known images used to train a classifier (e.g. SVM, KNN and Multi-SVM) to extract features; then the trained classifier can analyze digital content to establish which category it belongs to among scanned images, photos or computer generated. Table I gives comparison between the existing random forest classifier and the proposed multi-SVM classifier, from this it is clear that proposed one is much effective in all the ways.

TABLE I. Comparison Table

Comparison parameters	Existing random forest classifier	Proposed multi-SVM classifier
Accuracy	0.6033	0.6460
Error	0.3967	0.3540
Sensitivity	0.6033	0.6460
Specificity	0.9863	0.9878
Precision	0.6037	0.6564
False positive rate	0.0137	0.0122
F1 score	0.5979	NaN
Kappa	0.8375	0.8180
Elapsed time	249.145 sec.	204.012 sec.

In [17] a method without any previous knowledge to blind clustering and identify photos created by different sources devices. Revealing the determined image post-processing such as an interpolation, resampling, double JPEG compression or filtering operation will help to go back to its provenance [18], [19], [20], [21] with reconstruction of history of an image or a video. In particular, some approaches [22], [23], [24], [25], [26] analyzing the statistical distribution of the values by DCT coefficients.

In [27], [28], [29] methods for the detection of double JPEG compression feature vectors derived from histogram of DCT coefficients are proposed with classifiers; for steganography applications and image forgery detection. Furthermore, the authors in [30], [31], [32] has proposed phylogenetic analysis that is reconstructing image history based on image phylogeny tree reconstruction using image dissimilarity computation on near-duplicate images.

The peak use of social media contents are really deals with a huge amount of data and with lots of issues related to the data. In [33] to conform facebook image's authenticity various algorithms used for image processing are exploited and traces are found with it.

A study on social network services to detect JPEG images on *Facebook* is done in [34], [35]. In particular, the authors define a metric to measure the distance between JPEG image and its compressed version [34] and in [35] a technique to detect *Facebook* images tampering is proposed. In [36] an analysis on how the social networks like *Facebook*, *Badoo* and *Google+* process the uploaded images and what changes are made to its characteristics, such as JPEG quantization table, pixel resolution and related metadata is performed. Exif data contain some extra data concerning the image, such as camera features and settings, date, time and general information. Facebook utterly removes Exif data.

III. PROPOSED METHOD

Here we propose a novel method to effectively identify the original social network platform through which it is been transferred. The schematic diagram of the proposed method is depicted in Fig. 1. For the classifier training a large volume of images from these three OSN platforms is used. From those training images extract feature vectors using the method to be explained in Section III-A.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

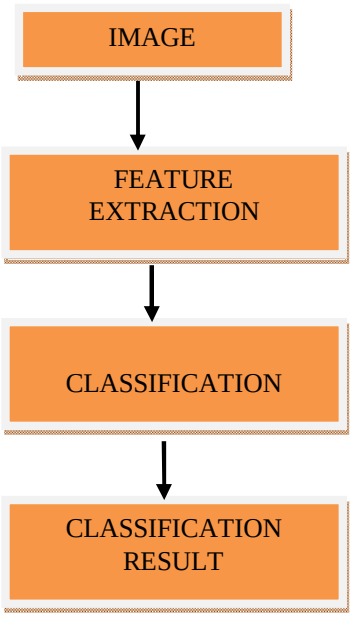


Fig. 5: Proposed system

Multi-class SVM classifier for identifying the image origin undergone training using extracted feature vector as will be presented in Section III-B. For the testing phase images feature is extracted and using trained classifier to get the social network origin of the image. The proposed method has two main phases: the distinctive features extraction and, the testing with already trained ad-hoc classifier step. The following two subsections describes in detail.

A. Features Extraction

Images created using camera and smartphone are undergone through some unknown and peculiar preprocessing this could leave fingerprints on image so that its basic JPEG compression is deformed; this is more specific in case of social networks, to resize the image for transmission. The small footprints are effectively traced out to classify an image based on its provenance social network platform, considering the DCT (Discrete Cosine Transform) domain to look for such distinctive traces. DCT coefficients are useful to track distortions introduced by JPEG compressions [27] is already proven.

Image I has to be dequantized first with its quantization table. For that first images coefficient array is extracted. A nine indexed location selected for each image to select DCT coefficients. Since image has to be processed for extracting unique traces in it we have to consider the whole image. For this purpose image is divided with 8X8 mask matrix. So that we will get a number of blocks in that image, each block is extracted with nine values. Nine locations are selected based on the zigzag scanning through 8X8 blocks of images. The DC coefficient ($k = 0$) first location matrix is skipped.

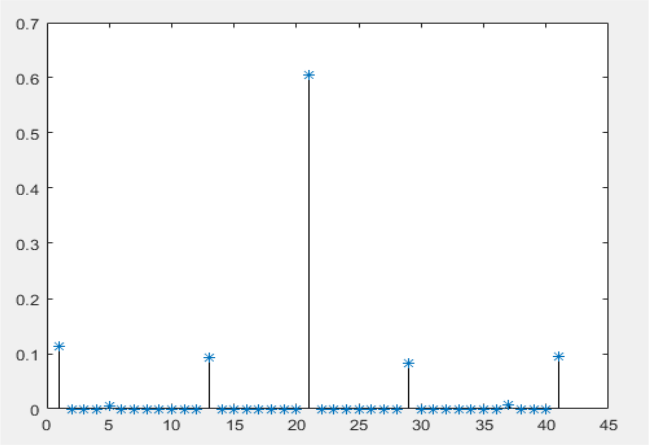


Fig.2.a. Histogram representation of DCT values

All features are normalized in the range between 0 and 1. Find any possible distinctiveness, each histogram represents positive and negative values; from -20 to +20 to avoid having a complicated representation as well to cover all features. In Figures 2.a, b. represents the sample histogram of DCT-coefficients.

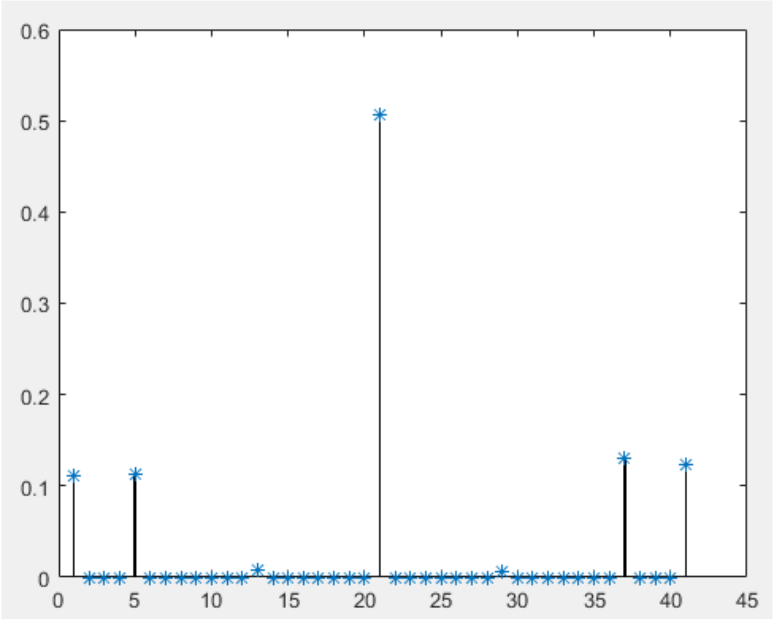


Fig.2.b. Histogram representation of DCT values

B. Training and Classification

The social network provenance image classification has been performed by resorting at a trained multi- SVM classifier. Known labeled images are used to train classifier with the features vector Vimm composed by $NV = [(2\ X\ B\ +1)N]$ elements computed as described in subsection III-A. The classifier training is done by providing a number of images from all the categories to analyze each class category well.

The adopted classifier is a *multi SVM* which is based on a general technique of SVM [37] that is an ensemble learning method for classification and other tasks. It is designed as one-against-one mode and is achieved by considering all multi class problems as binary classification problems $N(N-1)/2$ binary classifiers are constructed for each two OSN platforms, and $N = 4$ in our case. A voting scheme is for final decision making regarding the selection of origin social network.

IV. EXPERIMENTAL RESULTS

During experimental tests, the trained classifier is decides on the features vector Vimm to select and do classification based on it. two modes of classes can be chosen as a number of classes which depended on the JPEG quality factors and the second one which was determined only by the number of social networks (no categorization for *QF* was required). The experimental set-up first of all, the two parameters have been fixed $Bin = 20$ to compromise with all feature extraction and length of feature vector and $N = 9$ by a previous work [25] involved within the proposed methodology (see subsection III-A); resulting in an effective representation of the most significant DCT coefficients. The features vector Vimm characterizing each image has a dimension of 369 elements in total ($NV = [(2X(Bin = 20)+1)\ X\ (N = 9)]$).

UCID (Uncompressed Color Image Database) used for digital images for the experiments [38] which is composed by 1338 images (512 X 384 pixels) in TIFF format. These have been used as a basis to generate JPEG compressed images at different wanted quality factors. JPEG compression has been performed by resorting at MATLAB R2015b (*jpegtooolbox 1.4* library). The quality factors have been considered within the range [$QF = 50$ to 95] with a step of 5, so this leads to 10 different values. For each of these quality factors 1000 images of the UCID database have 30000 pictures in total. Support vector machine (SVM) was initially designed for binary classification. To extend SVM to the multi-class scenario, a number of classification models were proposed. Multi SVM set up kernel function is linear by default. Fig. 3 represents a ROC for multi SVM classifier.

Images are selected with a wide variety of characteristic range in our daily life including portrait, landscape, animal and building. The off-line trained multi-class SVM classifier will be used to distinguish the origin platform of the download images.

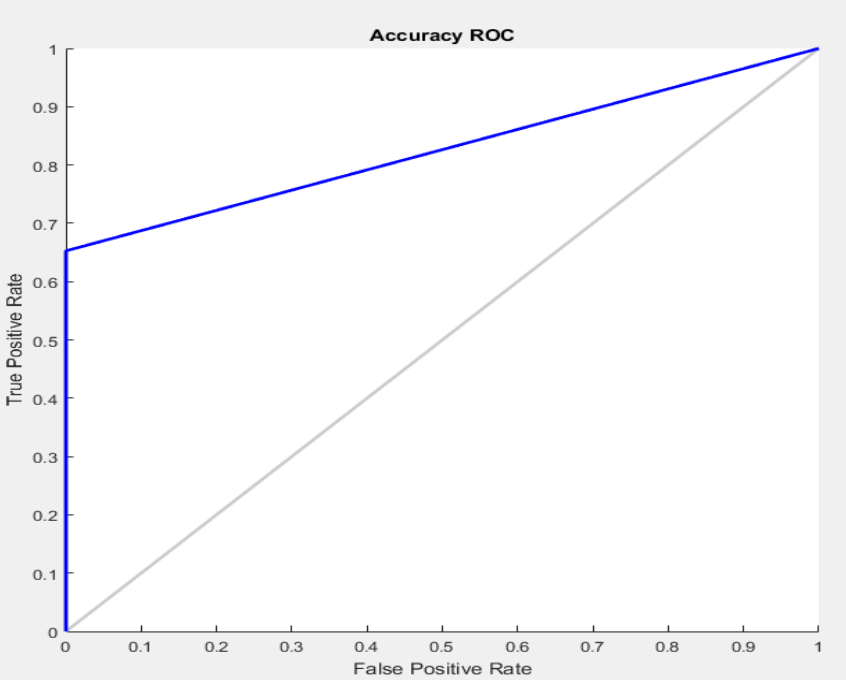


Fig.3 ROC for multi SVM classifier

V. CONCLUSION

The paper is more effective in way to classify an image based on its originating social network. The classification and feature extraction procedures complement each other, and get good results. Of course, classification with multi-SVM is grateful compared to existing methods. The future work will be implementation of various classifiers.

VI. ACKNOWLEDGMENT

The authors would like to thank HOD in charge of Computer Science and Engineering department Mr. Sarath V Sankaran, and M-tech coordinator, Mr. Shyjith M.B for providing me constant guidance, encouragement and interesting discussions.

REFERENCES

[1] Roberto Caldelli, Member, IEEE, Rudy Becarelli, and Irene Amerini, Member, IEEE , Image origin classification based on social network provenance in ieee transactions on information forensics and security, 2016.

[2] M. Stamm, M. W., and K. Liu, “Information forensics: An overview of the first decade,” Access, IEEE, vol. 1, pp. 167–200, 2013.

[3] M. Barni, “A game theoretic approach to source identification with known statistics,” in 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1745–1748, March 2012.

[4] N. Khanna, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, “Forensic techniques for classifying scanner, computer generated and digital camera images,” in Proc. of IEEE ICASSP, Las Vegas, USA, 2008.

[5] C. McKay, A. Swaminathan, G. Hongmei, and M. Wu, “Image acquisition forensics: Forensic analysis to identify imaging source,” in Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on,, pp. 1657–1660, 2008.

[6] S. Lyu and H. Farid, “How realistic is photorealistic?” IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 845–850, 2005.

[7] R. Caldelli, I. Amerini, and F. Picchioni, “A DFT-based analysis to discern between camera and scanned images,” International Journal of Digital Crime and Forensics, vol. 2, no. 1, pp. 21–29, 2010.

[8] S. Bayram, H. Sencar, N. Memon, and I. Avcibas, “Source camera identification based on cfa interpolation,” in Image Processing, 2005. ICIP 2005. IEEE International Conference on, vol. 3, pp. III–69–72, Sept 2005.

[9] N. Khanna, A. K. Mikkilineni, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, “Scanner identification using sensor pattern noise,” in Proc. Of SPIE, 2007.

[10] H. Gou, A. Swaminathan, and M. Wu, “Robust scanner identification based on noise features,” in Proc. of SPIE, vol. 6505, 65050S, 2007.

[11] J. Fridrich, “Digital image forensic using sensor noise,” IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 26–37, 2009.

[12] J. Luk´as, J. Fridrich, and M. Goljan, “Digital camera identification from sensor pattern noise,” IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 205–214, 2006.

[13] M. Goljan, J. Fridrich, and T. Filler, "Managing a large database of camera fingerprints," in Media Forensics and Security, ser. SPIE Proceedings, N. D. Memon, J. Dittmann, A. M. Alattar, and E. J. Delp, Eds., vol. 7541. SPIE, p. 754108,2010.

[14] D. Valsesia, G. Coluccia, T. Bianchi, and E. Magli, "Compressed fingerprint matching and camera identification via random projections," IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1472–1485, July 2015.

[15] C. T. Li, "Unsupervised classification of digital images using enhanced sensor pattern noise," Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS'10), pp. 3429–3432, 2010.

[16] I. Amerini, R. Caldelli, P. Crescenzi, A. Del Mastio, and A. Marino, "Blind image clustering based on the normalized cuts criterion for camera identification," Signal Processing: Image Communication, vol. 29, no. 8, pp. 831 – 843, 2014. [Online] Available: http://www.sciencedirect.com/science/article/pii/S092359651400109X

[17] I. Amerini, R. Becarelli, B. Bertini, and R. Caldelli, "Acquisition source identification through a blind image classification," IET Image Processing, vol. 9, pp. 329–337(8), April 2015. [Online]. Available:http://digitallibrary.theiet.org/content/journals/10.1049/iet-ipr.2014.0316

[18] H. Farid, "Exposing digital forgeries from jpeg ghosts," IEEE Transactions on Information Forensics and Security, vol. 4, no. 1, pp. 154–160, March 2009.

[19] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," IEEE Transactions on Information Forensics and Security, vol. 3, no. 1, pp. 101–117, March 2008.

[20] B. Mahdian and S. Saic, "Blind authentication using periodic properties of interpolation," IEEE Transactions on Information Forensics an Security, vol. 3, no. 3, pp. 529–538, Sept 2008.

[21] M. Kirchner, "On the detectability of local resampling in digital images," pp. 68 190F–68 190F–11, 2008. [Online]. Available: http: //dx.doi.org/10.1117/12.766902

[22] L. Zhouchen, H. Junfeng, T. Xiaoou, and T. Chi-Keung, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis," Pattern Recognition, vol. 42, no. 11, pp. 2492–2501,2009.[Online]Available: http://www.sciencedirect.com/science/article/pii/S0031320309001198

[23] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," Information Forensics and Security, IEEE Transactions on, vol. 7, no. 3, pp. 1003–1017, 2012.

[24] S. Milani, M. Tagliasacchi, and S. Tubaro, "Discriminating multiple JPEG compression using first digit features," in 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2253–2256, March 2012.

[25] I. Amerini, R. Becarelli, R. Caldelli, and A. Del Mastio, "Splicing forgeries localization through the use of first digit features," in Information Forensics and Security (WIFS), 2014 IEEE International Workshop on, Dec 2014, pp. 143–148.

[26] T. Bianchi and A. Piva, "Detection of nonaligned double jpeg compression based on integer periodicity maps," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 842–848, April 2012.

[27] T. Pevny and J. Fridrich, "Detection of double-compression in jpeg images for applications in steganography," IEEE Transactions on Information Forensics and Security, vol. 3, no. 2, pp. 247–258, June 2008.

[28] J. He, Z. Lin, L. Wang, and X. Tang, Detecting Doctored JPEG Images Via DCT Coefficient Analysis. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 423–435.

[29] Q. Liu, A. H. Sung, and M. Qiao, A Method to Detect JPEG-Based Double Compression. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 466–476.

[30] A. A. de Oliveira, P. Ferrara, A. De Rosa, A. Piva, M. Barni, S. Goldenstein, Z. Dias, and A. Rocha, "Multiple parenting phylogeny relationships in digital images," IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 328–343, Feb 2016.

[31] A. Melloni, P. Bestagini, S. Milani, M. Tagliasacchi, A. Rocha, and S. Tubaro, "Image phylogeny through dissimilarity metrics fusion," in Visual Information Processing (EUVIP), 2014 5th European Workshop on, Dec 2014, pp. 1–6.

[32] I. Amerini, R. Becarelli, R. Caldelli, and M. Casini, "A featurebased forensic procedure for splicing forgeries detection," Mathematical Problems in Engineering, p. 9, 2015.

[33] M. Moltisanti, A. Paratore, S. Battiato, and L. Saravo, Image Analysis and Processing — ICIAP 2015: 18th International Conference, Genoa Italy, September 7-11, 2015, Proceedings, Part II. Cham: Springer International Publishing, 2015, ch. Image Manipulation on Facebook for Forensics Evidence, pp. 506–517.

[34] A. NG, L. Pan, and Y. Xiang, Applications and Techniques in Information Security: 5th International Conference, ATIS 2014, Melbourne, VIC, Australia, November 26-28, 2014. Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, ch. A Novel Method for Detecting Double Compressed Facebook JPEG Images, pp. 191–198.

[35] A. V. Mire, S. B. Dhok, N. J. Mistry, and P. D. Porey, "Localization of tampering created with facebook images by analyzing block factor histogram voting," Int. J. Digit. Crime For., vol. 7, no. 4, pp. 33–54, Oct. 2015.

[36] A. Castiglione, G. Cattaneo, and A. De Santis, "A forensic analysis of images on online social networks," in Intelligent Networking and Collaborative Systems (INCoS), 2011 Third International Conference on, Nov 2011, pp. 679–684.

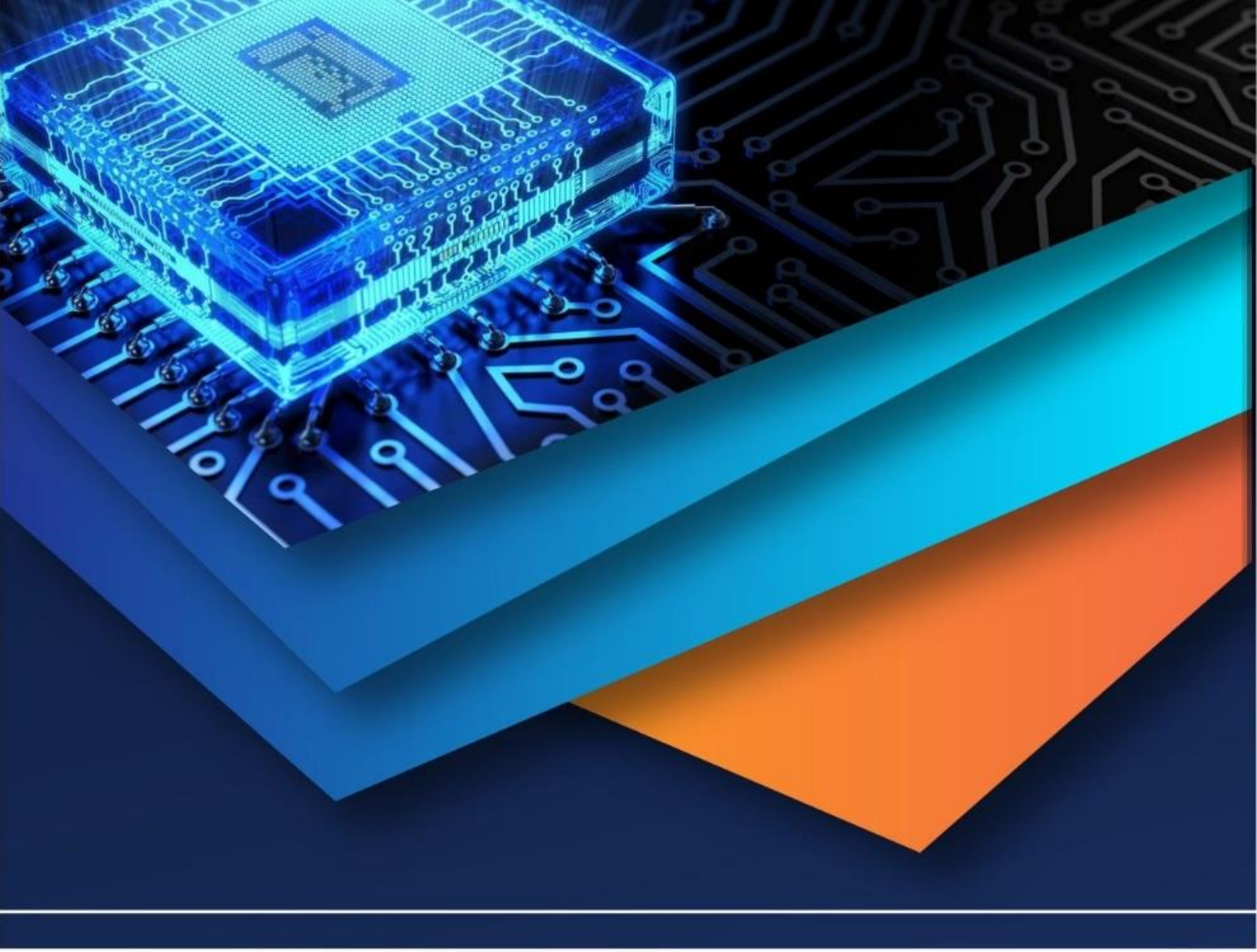
[37] Yoshlnaga Kato. Ridetoshi Saito and Toshiaki Ejima, "An Application Of SVM: Alphanumeric Character Recognition" Nagaoka University of Technology. Nagaoka-shi, JAPAN. 940-21.

[38] G. Schaefer and M. Stich, "UCID - an uncompressed colour image database," in Storage and Retrieval Methods and Applications for Multimedia 2004, ser. Proceedings of SPIE, vol. 5307, 2004, pp. 472-

480.

DHANYAJA P is a PG scholar in the department of computer science and technology, JCET, PALAKKAD, under KTU, KERALA, INDIA. Her current research area includes image processing.

RESHMA V K is a Ph.D. candidate in NOORUL ISLAM UNIVERSITY working as assistant professor in JCET, PALAKKAD, KERALA, INDIA. Her current research area include image processing and stegnography.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY