

Image Tamper Detection using Location Decision Embedding Technique

Shilpa Ravindra Muley¹, Shailesh Kumar²

¹Research Scholar, JJTU

²Research Guide, JJTU

How to cite this article: Shilpa Ravindra Muley, Shailesh Kumar (2024) Image Tamper Detection using Location Decision Embedding Technique. *Library Progress International*, 44(6), 1225-1236

Abstract: The fast and dynamic growth in technology erodes the trust in the integrity of imagery. With the wide availability of digital technology and tools a few affected areas with respect to cyber world are sophisticated photo hoaxes in media, political campaigns, armed forces, fashion and entertainment industry. The rapid rate at which the digital crimes are increasing has become a major concern, especially in the court of law. To cater these needs digital signatures were used, but they are no longer considered as a proof of authenticity or integrity, as there are tools which generate a valid digital signature of tampered images that pass through the validation of image authentication software of reputed digital cameras. To verify the integrity of an image, an authentication mechanism is introduced in this paper by improvising the image acquisition model as a possible solution to cater the needs of legal vindications. In this approach a Verification code of the image is generated using Gödelization technique and embedded in the image using LDET which acts as in-camera finger prints (watermark) of the image to detect tampering if any. The tampered area is localised by detecting and extracting invariant features of the image using SURF, a key point descriptor and matching these features with Euclidean distance. The results prove that the Improvised Image Acquisition Model detects Image tampering and Tamper Localization method locates copy move tampered regions which is robust to scaling and rotation transformations.

Keywords: Copy-move forgery, Tamper Detection, Verification Code, Gödelization, SURF

I. INTRODUCTION

As the world advances into more modern times, vast amount of information is produced and used on a global scale every day. With computers and other smart devices becoming ubiquitous in our daily lives, one of the most basic forms of information that can be interpreted by humans are images and they can be easily sent across the seas in no time. With this advancement however, comes a tall red flag. Images can be easily doctored, morphed or forged in no time. Surveys have shown that one out of every ten images have been altered or digitally rejigged [19].

While there are techniques that tell us if an image has been digitally altered by using prior information about the image that is available with us using strategies that make up what is known as Active forgery detection, it has becoming seemingly more important to be able to do this without any prior information available, called Passive forgery detection. Amongst the most popular and simplest forgery techniques is copy-move forgery, a technique that involves copying a part of the image and pasting it over another similar part to conceal any details. While it is practically undetectable by the human eye, these actions

can be identified by looking through the inconsistencies in the image's statistical properties. They are accomplished in one of two popular methods, Block based and Key point based which can detect even after some processing.

This paper is organized as follows. It starts with the state-of-the-art block based and key point-based feature detection and extraction algorithms. Then follows Problem Statement, the methods used for implementing the proposed model, proposed methodology, experimental results and is finally concluded with future work.

II. LITERATURE REVIEW

Digital Watermarking is a non-blind image tamper detection technique. To detect image tampering Saiyyad [3] embeds a unique identification code at the 2nd level DWT of the host image and its hash code is used as a secondary watermark which needs to be extended to resist various attacks. Sawiya Kiatpapan and Toshiaki Kondo [20] use the down sampled image as a dual watermark embedded into LSB plane. If the watermark is damaged the tamper cannot be detected and recovered. Pongsomboon et al. [1] uses a self-embedding watermarking technique which embeds 2 watermarks of higher resolution in LSB plane and 8 watermarks of lower resolution in 2nd LSB plane to detect the tampered region and recover the original image. This method is more complex to implement and is unable to detect images of various file formats. Another limitation is that the position and size of the tampered area affects the quality of the recovered image.

A simple approach for Copy Move Image Tamper Detection is an exhaustive comparison of the image with every possible transformation of itself. It is computationally slow, and so many approaches were proposed. Local Binary Patterns are popular for texture classification. Zhenhua et al. [10] proposed CLBP to define the operators CLBP_C, CLBP_S, CLBP_M to extract grey level, sign and magnitude features. In [11] the authors propose LBP based fragile watermarking scheme for forgery detection and recovery. A review analysis of LBP variants [14] expresses the need of rotation invariant and noise insensitive texture classification method. Salam Abdul-Nabi Alnesarawi, et.al. uses CRLBP in [9] where features are extracted from overlapping blocks. But this increases the computational cost for high resolution images because of large number of overlapping blocks.

Features like corners, edges, texture, and histogram are characteristics of an image. There are some features which remain invariant to scaling, rotation and other transformations in spite of applying post processing operations on the tampered image. The points which are invariant to transformations and scaling are called as Key Points or Interest Points, the features at these points are detected and extracted. SURF, SIFT, PCA-SIFT, ASIFT, FSIFT, Moment-

Invariants are some of the invariant features. Babak [12] uses Blur moment Invariants feature extraction method, k-d tree representation for feature matching for detecting blurred forged areas which is invariant to contrast changes, but the computation time is high. Forged images with Gaussian Blurring were detected in [13] which failed to detect post-processed forgery. CT and kernel PCA based feature extraction was proposed to identify similar objects in [15]. Zhang [16] proposed a method of tamper detection in flat regions using SURF. Codreanu et al. [17] presents affine-invariant feature detector using a powerful graphics hardware which is computationally very expensive. It can be observed that Image tamper detection using Non-Blind watermarking methods had implementation complexities and unable to withstand even minor attacks, as they need the original and embedded watermark images for

comparison to prove tampering. In this paper, a Verification Code is generated using Gödelization and embedded using Location Decision Embedding Technique for image tamper detection. The Verification Code is also stored in the EXIF data of the image for later verification making this as a blind method, which does not require the original image for comparison. The generation of Verification Code does not use image information and so it is not affected even if the image is modified from small to a large extent and is able to detect tamper of any kind.

The block-based methods are computationally cost and takes much time for images of high resolution, where as key point feature detection methods extract the features within minimum time. SURF is a fast scale and rotation invariant feature detector and descriptor in the state of art which is accurate and sufficiently distinctive with low dimensionality reducing the size of the descriptor, low computational cost, without compromising the performance. This paper uses SURF for feature detection and extraction, Euclidean distance to match the features and locate Copy Move Tampered regions.

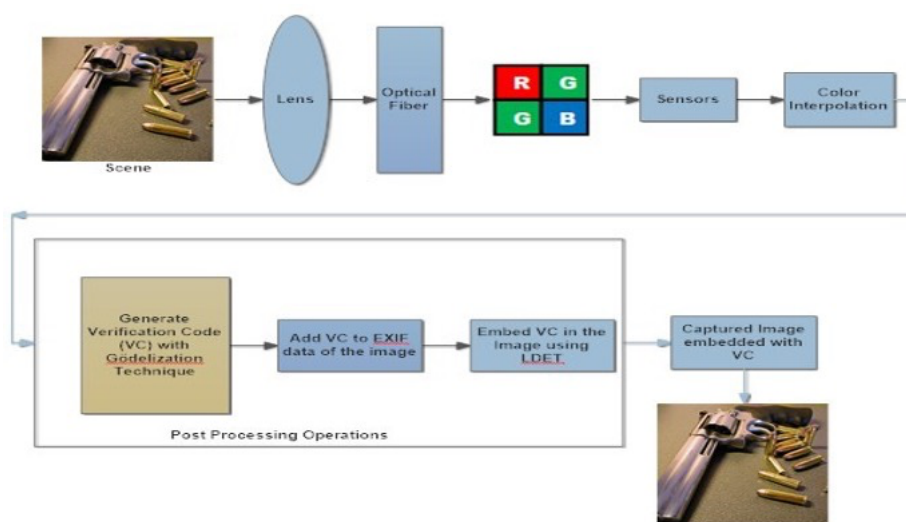


Figure 1: Improved Image Acquisition Model

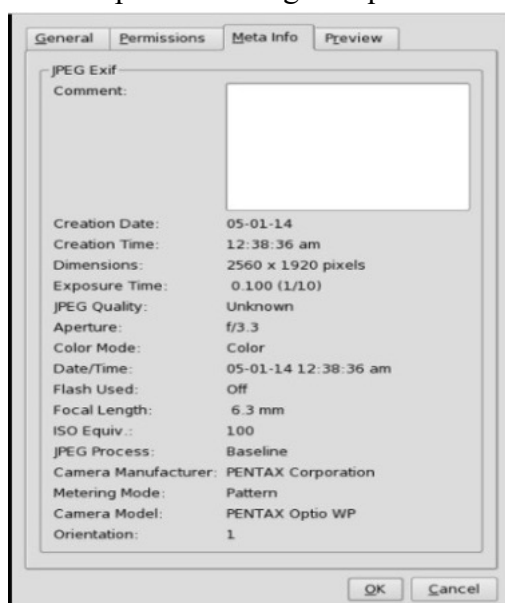


Figure 2: EXIF data of an image

III. PROBLEM STATEMENT

The major concern related to digital images with respect to Security is to find whether the image has been tampered since its time of capture. Highly sophisticated Digital Cameras like Nikon and Canon digitally sign on their images to ensure authenticity. When any of these images are forged, the digital signature should no longer authenticate. But, there exist tools to generate a valid digital signature on forged images that pass through the validation of Image Authentication Software of Nikon or Canon. Hence, digital signatures cannot be considered as a proof of authenticity. As a solution to this problem, Tamper Detection was addressed in our previous paper [2] by introducing a self-generated Verification Code using Gödelization technique in the image acquisition process. This paper improvises the image acquisition model for Tamper Detection and localizes the tampered area. The improvised image acquisition model is shown in Figure 1 and the framework for Copy Move Tamper Detection and Localization is shown in Figure 3.

Related Work

Gödelization Technique and Alphabetic Coding Gödelization converts a positive integer into Gödel Number Sequence (GNS), the product of primes. According to Gödelization [5], GNS of 30 is GNS (1,1,1) encoded as 21x 31 x 51. So now, 30 is encoded as 111. When a digit appears continuously it is Alpha coded i.e 3B. In this paper, the image captured time and digital camera manufacturer's name are encrypted with Gödelization technique to generate Verification Code. This Verification code is embedded in the image using Location Decision Embedding Technique and also stored in the EXIF data of the image file for comparison.

Location Decision Embedding Technique (LDET)

The Verification Code generated using Gödelization technique is embedded in the image using LDET [7]. In this technique embedding starts from the seed pixel and the image captured date encrypted using Gödelization acts as the seed pixel. The embedding sequence of the verification code is random, based on the MSB of the pixels and its parity. This technique protects the integrity of the image and is perceptually invisible to the human eye. The improvised image acquisition model generates the verification code of the image and embeds it into the image during the post processing operations of image acquisition. This verification code acts as in-camera finger prints of the image and helps to detect tampering if any.

Overview of SURF Algorithm

SURF is a novel multi-scale and rotation invariant key point detector and descriptor. SURF used Fast-Hessian detector for Interest Point detection for its repeatability which finds the same interest points under different viewing conditions, while being robust to noise. Even for scale selection, SURF depends on the Hessian Matrix determinant [8]. Sign of Laplacian, used for Indexing, increases the speed of feature matching and accuracy with good performance. In an image I , given a point $x=(x,y)$, Hessian Matrix in x at scale σ represented $H(x, \sigma)$, is defined as

$$H(x, \sigma) = \begin{bmatrix} L_{xx}(x, \sigma) & L_{xy}(x, \sigma) \\ L_{xy}(x, \sigma) & L_{yy}(x, \sigma) \end{bmatrix} \quad (1)$$

Euclidean Distance

Feature matching is based on distance between the feature vectors eliminating outliers. Euclidean Distance is used as a measure of identifying feature vectors with less distance indicating similarity of the features. Given points $p=(p_1,p_2)$ $q=(q_1,q_2)$ distance is given by

$$d(p, q) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2} \quad (2)$$

Proposed Method







This paper works out with two outcomes. Firstly, Improved Image Tamper Acquisition model for Tamper Detection. Secondly, locating the copy-move tampered regions in the image.




Improved Image Acquisition Model for Tamper Detection

There are two concerns in our previous paper of Image Tamper Detection which are improvised in this paper as shown in Figure 1.

- i) Storing Verification codes in the device and using it later for comparison in case of issue is not so practical, as image captured device has to be identified for finding the original verification code for comparison.

Table 1: Performance comparison of Embedded Images using proposed and Pongsomboon et al. [1] methods

Images embedded with Verification Code using proposed method	PSNR	MSE	Mean SSI M value	Embedded Images using Pongsomboon et al..[1] method	PSNR	MSE	Mean SSI M value
	53.7082	0.4388	0.9579		46.1342	0.9698	0.9449
	51.0292	0.6459	0.9465		42.5682	0.9721	0.9354
	49.1976	0.9205	0.9312		39.9126	0.9880	0.9026

	52.2368	0.4891	0.9563		42.6128	0.9719	0.9338
	54.6521	0.4010	0.9655		40.4811	0.9801	0.9125

This paper improvises it by encrypting the image captured time along with the camera manufacturer's name instead of diagonal pixel values of the image with Gödelization technique to generate Verification Code. This Verification code is stored in the EXIF data of the image file as shown in Figure 2. This eliminates the need of storing the verification code in the device, making this a passive method. This technique is applied at the time of image creation along with the manufacturer's name to produce its Gödel Number Sequence. This Gödel String acts as a unique Verification Code for the image. Once the image is captured the verification code is generated and is embedded using LDET during post-processing operation. It is also stored in the EXIF data of the image after capturing and before generating the image as in-camera finger print of the image. Table 1 shows the results of the images embedded with the Verification Code.

ii) The Verification Code embedded using LSB+1 column plane is easy to predict and extraction is straightforward. LDET method [7] generates a unique random sequence of embedding positions based on the seed pixel. This paper employs LDET as it cannot be predicted easily. The image captured date is encrypted using Gödelization technique and this is treated as the Seed pixel.

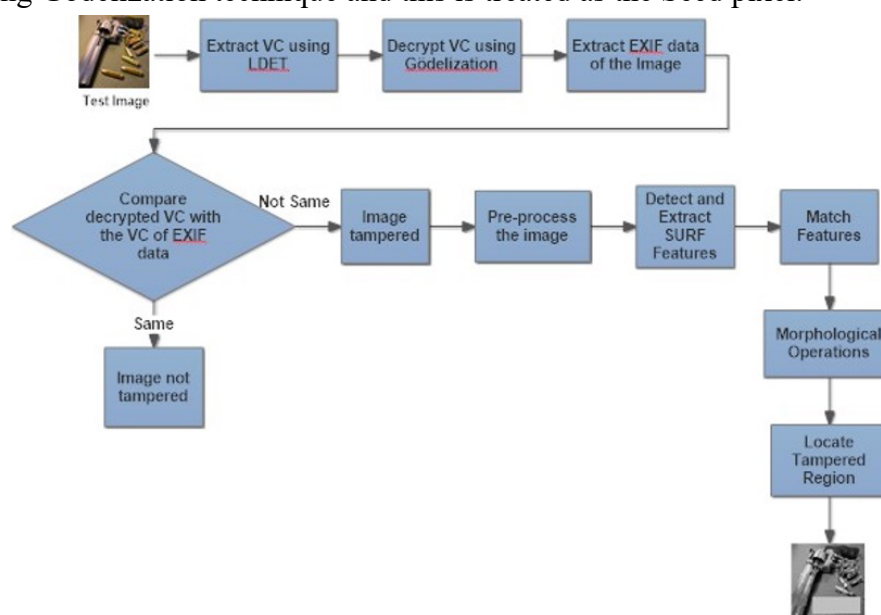


Figure 3: Framework for Copy Move Tamper Detection and Localization

Embedding Self-Generated Verification Code

Step 1: Compute the Verification Code of the Image by encrypting the image captured time and camera manufacturer's name using Gödelization technique.

Step2: Store this Verification Code in the EXIF data of the image after the Basic Post Processing Operations.

Step 3: Compute the Seed pixel by encrypting the image captured date using Gödelization technique

Step 4: Embed the Verification Code in the image using Location Decision Embedding Technique starting from the Seed pixel.

Extracting Verification Code and Tamper Detection

Step 1: Open the EXIF data of the test image.

Step 2: Compute the Seed pixel by encrypting the image captured date using Gödelization technique.

Step 3: Extract the Verification Code from the image using Location Decision Embedding Technique with Seed pixel.

Step 4: Compare the extracted Verification Code with the one in the EXIF data of the image to identify Tamper Detection.

Once the image is identified as tampered, the tampered area has to be located. Locating the Copy Move Tampered region of an image is described stepwise in 4.2. Figure 4 shows the flow diagram of the algorithm.

Procedure for Copy Move Tamper Localization

Step 1: Pre-processing – The test image is converted from RGB to greyscale. In this process, same amount of colour has to be emitted in each of the red, green and blue channels. But brightness of green component is dominating, so a weighted sum method is taken. This is computed using the standard formula

$$Y=0.229R+0.587G+0.114B \quad (3)$$

Step 2: Feature Detection and Extraction - A robust, low dimensionality feature detector and descriptor SURF is used for detecting features as shown in Figure (5).

Step 3: Feature Matching – Feature vectors are lexicographically sorted to group similar features. The original and tampered areas have the minimum distance. So, Euclidean distance is calculated on matched features based on threshold to obtain the matching points.

Step 4: Post processing – There are chances of small areas left inside the detected region. Morphological operations are applied to cover them.

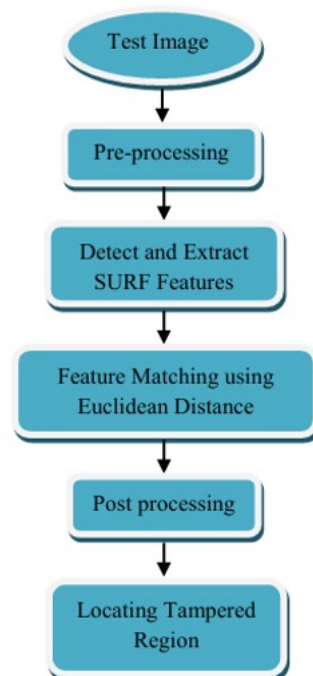


Figure 4: Flow chart of Copy Move Tamper Localization

Table2: Performance Comparison of Copy Move Tamper Detection and Localization using Salam et al [9] and Proposed approach

Features	Accuracy	Precision	Recall	False Positive Rate
Salam et al.[9]	96.72	94.54	96.89	2.35
Proposed approach	98.52	97.95	100	0.5

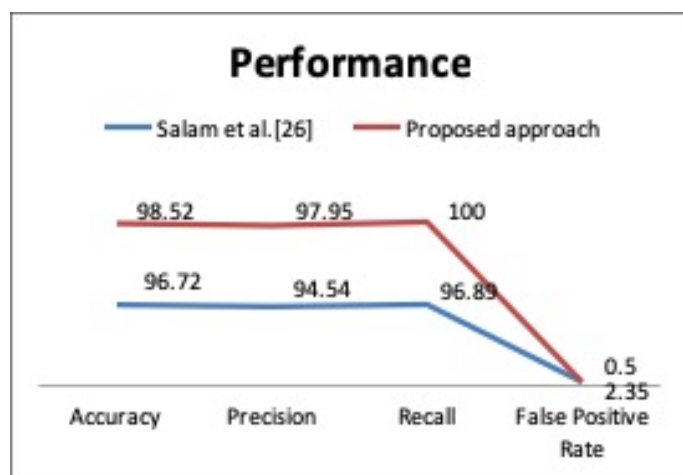


Figure 6: Performance Comparison of Image Tamper Localisation using proposed approach and Salam et al.[9] method



Figure 7: (a)(d)(g)(j)(m)(p) original images (b)(e)(h)(k)(n)(q) are tampered images (c)(f)(i)(l) tampered areas (o) scaled (u) rotated

Experimental Results and Analysis

MICC-F220 copy move tampered image dataset is used to evaluate the performance of Tamper Detection and Copy Move Tamper Localization consisting of 220 images.15 forged images of size 512

x 512 were created manually. 50 images were tested by generating Verification Code using Gödelization technique and embedded with Location Decision Embedding Technique. PSNR, MSE and SSIM are calculated as a measure of performance and compared with method [1]. The results prove that the proposed method gives a better PSNR and SSIM values. 30 images from MICC-F220 and 15 manually forged images were tested which consists of untampered and tampered with various post processing operations. The performance of evaluation is calculated using the standard Accuracy, Precision, Recall, and False Positive Rate measures [18] as follows.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

$$Precision = \frac{TP}{TP + FP} \quad (5)$$

$$Recall = \frac{TP}{TP + FN} \quad (6)$$

$$FPR = \frac{FP}{FP + TN} \quad (7)$$

Where

TP is True Positive - Tampered image identified as tampered

TN is True Negative – Untampered image identified as untampered

FP is False Positive – Untampered image identified as tampered

FN is False Negative – Tampered image identified as untampered

Performance of the proposed method on different types of post processing operations is shown in Table 2 with precise evaluation in Figure 6. Some of the results of images in the datasets are shown in Figure 7.

IV. CONCLUSION & FUTURE WORK

We presented a framework for a highly effective Copy Move Tamper Detection and Localization. The improvised image acquisition model generates and embeds Verification Code while capturing the image. The generation of Verification Code does not use image information and so it is not affected even if the image is modified from small to a large extent. This verification code acts as in-camera finger prints of the image and helps to detect tamper of any kind and the Localization method locates the region of copy move tamper. The experimental results and performance analysis show that the proposed framework detects tampers of any kind based on the Verification Code and locates copy move tampered region with scaling and rotation post processing operations. The Verification Code embedded in the EXIF data makes this a passive Image Tamper Detection model eliminating the need of the image capturing device in case of disputes to prove whether it is tampered or not. This approach is simple and easy to implement. SURF is a fast feature descriptor of the key points and is robust to scaling and rotation transformations. Tampered Images of small portions are detected as tampered, but

the tampered region is not completely located without morphological operations. As a future work, we have to locate very small tampered regions without morphological operations.

References

- [1] P. Pongsomboon, T. Kondo and Y. Kamakura, 2016, "An image tamper detection and recovery method using multiple watermarks," 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, 2016, pp. 1-6.
- [2] P. Raja Mani, D. Lalitha Bhaskari, 2017, "A Prototype for Image Tamper Detection with Self-generated Verification Code Using Gödelization"© Springer, Smart Computing and Informatics, Smart Innovation, pp. 219-226
- [3] M. A. M. Saiyyad and N. N. Patil, 2014, "Authentication and tamper detection in images using dual watermarking approach", Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization, Noida, pp. 1-5.
- [4] https://en.wikipedia.org/wiki/Exif#/media/File:Konqueror_Exif_data.jpg
- [5] D. Lalitha Bhaskari, P. S. Avadhani, A. Damodaram, 2009, "A Combinatorial Approach for Information Hiding Using Steganography And Gödelization Techniques" in the Journal of IJSCI(International Journal of Systemics, Cybernetics and Informatics), pp. 21–24, ISSN 0973-4864.
- [6] P. Raja Mani, D. Lalitha Bhaskari, 2013, "Gödelization and SVD Based Image Watermarking under Wavelet Domain", Proc. of Int. Conf. on Front. of Intell. Comput., AISC 199, pp. 675–681, Springer-Verlag Berlin Heidelberg 2013.
- [7] P. Raja Mani, D. Lalitha Bhaskari, 2014, "A Secured Approach for Watermark Embedding using Keybased Gödelization Technique under Spatial and Frequency Domains", IJCA (0975–8887)Volume 95–No. 19 pp:32-36, June 2014
- [8] Herbert Bay, Andreas Ess, Tinne Tuytelaars, and Luc Van Gool, June 2008, "Speeded Up Robust Features", ETH Zurich, Katholieke Universiteit Leuven Journal of Computer Vision and Image Understanding, Volume 110, Issue 3 pp. 346-359.
- [9] Salam Abdul-Nabi Alnesarawi, Ghazali Sulong, March 2015, "A Novel Approach for Detection of Copy Move A Novel Approach for Detection of Copy Move Forgery using Completed Robust Local Binary Pattern, JIHMS, Vol. 6, Issue No. 2, pp:351-364.
- [10] Zhenhua Guo, Lei Zhang, David Zhang*, March 2010, "A Completed Modeling of Local Binary Pattern Operator for Texture Classification" IEEE Transactions on Image Processing 19(6):1657-63.
- [11] Jun-Dong Chang, Bo-Hung Chen, Chwei-Shyong Tsai, Feb 2013 "LBP-based Fragile Watermarking Scheme for Image Tamper Detection and Recovery", ISNE, IEEE pp:173 - 176
- [12] Babak Mahdian, Stanislav Saic, Sep.2007, "Detection of copy–move forgery using a method based on blur moment invariants", Forensic Science International, Vol.171 No.2-3, pp. 181-189.
- [13] Guzin Ulutas, Mustafa Ulutas, Nov. 2013, "Image forgery detection using Colour Coherence Vector", Electronics, Computer and Computation (ICECCO), pp. 107 – 110.

- [14] Classification Ch. Sudha Sree1, M. V. P Chandra Sekhara Rao, May 2017, "Performance Analysis of Local Binary Pattern Variants in Texture", IJARCET, Volume 06, Issue 05, ISSN: 2278 – 1323 pp. 677 to 684.
- [15] S. Kiatpapan and T. Kondo, 2015, "An image tamper detection and recovery method based on self- embedding dual watermarking," 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Hua Hin, pp. 1-6.
- [16] <http://www.technospot.net/blogs/uploading-your- photos-online-beware/>
- [17] https://en.wikipedia.org/wiki/Precision_and_recall
- [18] Valeriu Codreanu, Feng Dongy, et al., 2013, "GPU- ASIFT: A Fast Fully Affine-Invariant Feature Extraction Algorithm" 978-1-4799-0838-7/13©2013 IEEE pp. 474-481
- [19] Zhang, Guang-qun, and Hang-jun Wang, September 2012, "SURF-based Detection of Copy-Move Forgery in Flat Region." International Journal of Advancements in Computing Technology (IJACT), vol. 4, no. 17, pp.521-529.