DOI : https://doi.org/10.56452/7-5-208

ISSN: 0974-5823 Vol. 7 No. 5 May, 2022

International Journal of Mechanical Engineering

Empirical Comparison of Classical and Cognitive Image Forensics

Bhupesha Rawat

Associate Professor, School of Computing, Graphic Era Hill University,

Dehradun, Uttarakhand India 248002

Abstract: Due to the proliferation of image-processing programmes, digital photos are increasingly at risk. There is a growing field of study called Digital Image Forensics (DIF) that aims to solve the open challenge of verifying the origin and information content of digital photographs in the multimedia environment. Without a digital watermark or signature, the passive DIF can uncover an image's veracity and track its history. In order to make a fake seem authentic, it is standard practise to use an enhancement technique like contrast enhancement. Discovering the reality behind a digital picture sometimes involves exposing the effects of contrast augmentation. The goal of this study is to identify global contrast enhancement in both original and JPEG-compressed photos, whether parametric or non-parametric. To identify various kind of global contrast improvements, we propose four feature sets that use block statistics (block variance, block mean, AC discrete cosine transform (DCT) coefficients, and DC DCT coefficients). Machine learning methods that can accurately distinguish between original and global contrast-enhanced images are trained using the suggested characteristics. Both uncompressed and JPEG compressed images may be analysed for the existence of global contrast enhancement using any of the aforementioned machine learning technologies. Post-processing applications such as resampling, picture rotation, noise addition, and histogram-based anti-forensics assaults have no effect on any of the suggested feature sets.

Keywords: Digital Image Forensics, Discrete cosine transform, JPEG, histogram

Introduction

These days, cameras and camcorders are loaded with a plethora of high-tech features and programmes designed to improve and refine your images. The proliferation of multimedia on digital devices is changing the way we live but also making our digital material more vulnerable to theft. This has led to a rise in the amount of content manipulations on the internet, which poses problems for both individuals and society as a whole. These manipulations may range from harmless improvements to the distribution of false information that claims thousands of lives or the swaying of a court's decision. Consequently, it is crucial to verify the data before drawing any conclusions. The primary focus of this thesis is to reveal the authenticity of digital photographs. Digital image forensics (DIF) is the study of verifying the authenticity and integrity of digital pictures. Discovering changes made to digital photos (also known as tamper detection) is DIF's primary goal. The forgeries may be categorised according to the amount of photographs they use. Depending on how the detection is done,

image authentication systems may be classified as active or passive. Active approaches include digital watermarks and signatures, as well as implanting data into a picture before it is archived. For the purposes of image forgeries, this implanted information is often altered or removed throughout the tampering process. The lack of a module for digital watermarking or signatures in most current devices is the main drawback of the active method. In [1]-[7], we see a collection of statistical techniques for detecting the telltale signs of digital picture forgeries in the lack of a signature or watermark. These methods take use of the fact that, despite appearances, any manipulation of a picture will result in a change to the image's underlying statistics. Oftentimes, in order to make visually convincing pictures, it is necessary to

- Adjust the image's brightness (by means such as contrast enhancement) to work with the available light.
- resize, flip, and rotate photos or their components.
- Add noise in a controlled manner to conceal marks of image tampering, for example, the addition of Gaussian noise.
- The resulting picture should be re-saved using a lossy compression format, such as JPEG. Digital picture manipulation or forgery is generally undetectable to the naked eye. However, it may cause new correlations to appear in the image, which can be used to spot digital forgeries.
- The techniques based on pixels of the image that can reveal the statistical signatures hidden in the pixels.
- The techniques based on image format that can find the statistical signatures of lossy compression standards.
- The techniques based on the camera that can detect the signatures left by the camera hardware and processing pipeline.
- The techniques based on physics that can detect the ambiguities in image formation model and the three-dimensional interaction between the objects, camera, and source of light.
- Geometric methods for identifying size and position discrepancies in the real world and in relation to the camera. By manipulating or concealing statistical signatures, forgers may influence forensics decisions. Counter-forensics, sometimes known as anti-forensics, is a subfield of DIF concerned with exposing the weaknesses of current approaches and investigating ways to defend against assaults on forensic judgements.

Machine Learning Tools

Machine learning is the study of how computers learn, specifically how to mimic human learning. Let's say you have a task T that has multiple classes, and you want to build a computer programme that can learn through experience or training in accordance with those classes. A computer's ability to learn from E is quantified by the performance metric P. In this study, T is used to identify digital photographs that have been altered from their original state by applying a contrast enhancement filter. The E is the level of detection accuracy as assessed by the ROC curve or the confusion matrix, and the F is the training set constructed from the original and the globally contrast-enhanced pictures. Area under the curve, true positive rate, false positive rate, true negative rate, false negative rate, and cross-validation accuracy are the several P's that may be considered. The statistical properties of the original versus global contrast-enhanced pictures are used to propose feature sets that are used to train machine learning systems to distinguish between the two types of images..

DOI : https://doi.org/10.56452/7-5-208

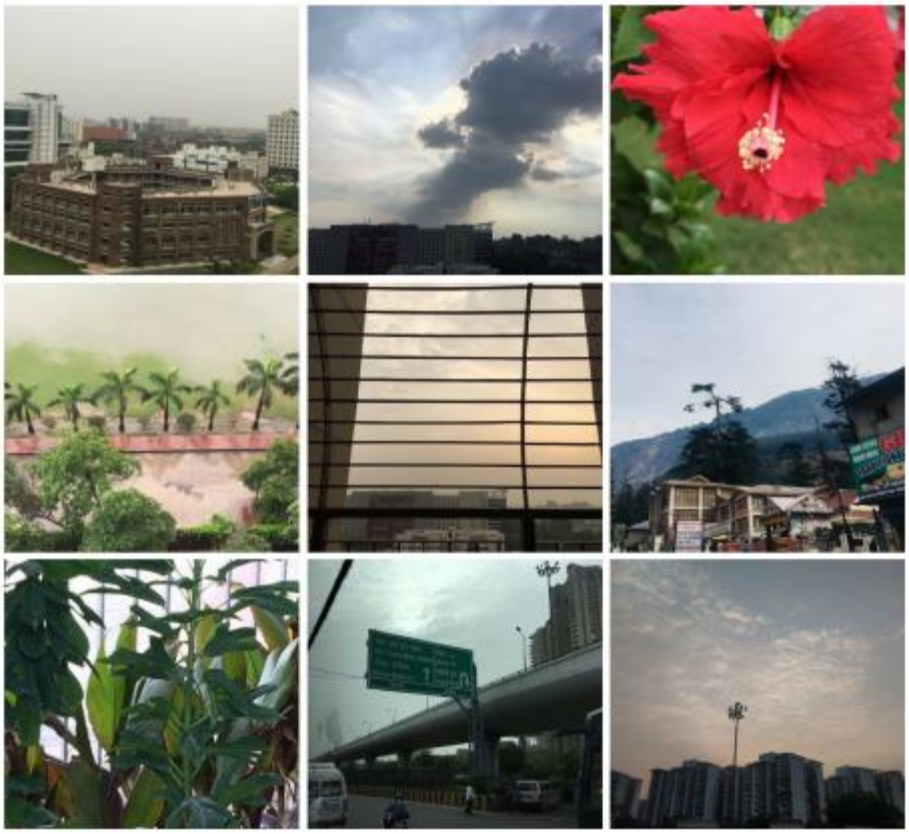

Figure 1: Sample images from the Random Images dataset.

Support Vector Machine (SVM)

In the realm of machine learning, SVMs are the norm. A support vector machine (SVM) builds a hyperplane that optimally partitions the available area of the training matrix. For each value in the training matrix, it determines whether it belongs to class 1 or class 1.**Decision Tree**

One of the most well-known, simple, and effective prediction machine learning algorithms is the decision tree. The training matrix is greedily subdivided into two halves using a binary decision tree. In this procedure, we compare the costs of various combinations of binary splits to see which ones work best. The most cost-effective division is chosen. In this study, we use Gini's diversity index with a split threshold of 100. The input training matrix is represented by the root node, while the predicted output is represented by the leaf nodes.

Parametric Global Contrast Enhancement Detection

Some parameters, such as in gamma correction, can be used to set the level of parametric contrast enhancement. The block variance from the spatial domain and the AC DCT coefficients form the frequency range of an image are used in the suggested method to disclose the traces or presence of various sorts of contrast enhancements. However, post-enhancement JPEG compression is a major concern, despite the high detection accuracy of state-of-the-art methods for identifying tampering in images by detecting the presence of parametric contrast enhancement. Due to its low memory requirements, JPEG is the most common image format, and since most methods fail or become random guesses when an image is JPEG compressed, methods robust to post-enhancement JPEG compression are necessary. Even in the situation of the composite functioning of contrast improvement and post-processing activities like JPEG compression, it is crucial to design systems or tools that

can distinguish contrast-enhanced photos from original images. DCT is a basic and important mathematical operation in the most widely used JPEG standard for digital pictures, and the study of DCT coefficients has found value in several fields of image processing. As a result, we begin analysing the DCT coefficients of powerlaw-transformed or improved pictures. The discrete cosine transform (DCT) in JPEG pictures is the transition from the domain of space to the frequency domain. Quantization is used as a method that helps with data compression after the DCT step. DCT is an obvious candidate for research given that it plays no role on compression and is reversible.

Extensive analysis of the AC DCT coefficient distributions is performed for the many digital imaging applications, such as picture forensics. AC DCT coefficients have previously been characterised using a variety of unimodal distributions, including the Laplacian, Gaussian, Cauchy, generalised Gaussian, and generalised Gamma. Using tests and statistics such the Chi-square (2), Kolmogorov-Smirnov (KS), and Jensen-Shannon (JS) divergence, it has been shown that the Laplacian distribution is simpler at the expense of universality. Document and text pictures have been characterised using the generalised Gamma and generalised Gaussian distributions. It has been shown in that the distribution of AC DCT coefficients follows the same pattern as the distribution of block variance in a picture. The block variance is the dispersion of a picture into non-overlapping 8x8-pixel chunks. The constant block variance of the DCT coefficients is well-fit by the Gaussian distribution, as shown . Since block variance was found to be stochastic for real-world images, the distribution of AC DCT coefficients is doubly random. Distributions of AC DCT coefficients, which rely on the parameters of the block variance distributions, have been obtained using the methods described in. Two passive image forensic methods for detecting contrast improvements have been developed using the image block variance and AC DCT coefficients and their statistical properties. A linear link between the original and power-law altered pictures is established in the logarithmic domain. It has been calculated that the rate parameter differs considerably between the original and power-law converted pictures if an exponential distribution is fitted to the block variance of the natural log (ln) of the original and power-law transformed images. Parameters from single-parameter exponential and half-Gaussian distributions, however, are unaffected by shifts in the degree to which contrast is boosted. To better characterise the block variance of original and power-law processed pictures in the logarithmic domain, the Gamma (two-parameter), Weibull (two-parameter), and distribution from the exponential family (three-parameter) [36]-[39] have been shown to be superior solutions. For image forensics based on parametric contrast enhancement, the Gamma distribution has been shown to be the optimal compromise between accuracy and complexity. Therefore, the AC DCT coefficients are characterised by a Gaussian-Gamma distribution that is derived analytically. Then, the block variance and AC DCT are proposed as two machine learning tools for identifying contrast enhancement. Logarithmic domain image coefficients.

Literature Review

Saurabh Agarwal et.al.,(2021) These days, digital photographs are the lifeblood of every social media site. The widespread use of these photographs in people's daily lives has led some to question whether or not they are genuine. Forensic analysis of images is required to verify their legitimacy. In this work, we present a new approach to digital picture forensics. Images that have been median-averaged or filtered using a Gaussian distribution may be identified using the suggested method. The first picture is normalised with optimum range in the suggested approach to improve the statistical data. The normalised array is then subjected to a suggested thresholding and difference arrays are computed. Finally, threshold difference

arrays are parsed for co-occurrence features. There is a noticeable performance boost in experimental evaluation. The suggested approach maintains its detection capabilities on low-quality JPEG-compressed small-sized photos.

Kaijun Wu et.al.,(2021) Median filtering is a non-linear digital filtering method that may maintain edges and smooth sections inside a picture, making it a popular tool among forgers as image processing technology has advanced. As a result, everyone is interested in how to employ middle-of-the-road forensics tools to verify an image's legitimacy and safeguard its associated data. However, in median filter forensics, it is still a challenge to successfully identify the median filter out of high JPEG compressed small-size images. on this research, we present a methodology for dealing with this problem that is grounded on deep residual learning. To be more precise, a brand-new kind of convolutional neural network known as MFFNet was developed. In the first stage, we ingeniously created a preprocessing layer with varied residuals to record different median filter artefacts and retrieve the features left behind by the median filter. Then, we painstakingly developed an MFFNet to auto-learn the complex hierarchical features that survived the rigorous JPEG compression. To combat the deep network's tendency towards over-fitting, we implemented a number of diversity-boosting enhancements during training in order to produce a median filter detector that is both more easily trainable and less prone to instability. The proposed framework greatly outperforms state-of-the-art approaches for recognising very low-resolution JPEG-compressed images, as shown by a large number of experiments conducted on the composite database.

Yuan Wang et.al.,(2021) The widespread availability of digital material on today's Internet has far-reaching consequences for society as a whole. Images in digital media have data properties that make them susceptible to manipulation for a variety of reasons. This study employs CNN algorithm technology to investigate image data tampering forensics practises in digital media, builds an information theory model to account for the chain of events that occurs when tampering occurs, and employs a limited convolution CNN network algorithm to detect the tampering behaviour of images of varying sizes. CNN algorithm provides superior identification accuracy and recognition efficiency in digital media picture data manipulation forensics, as shown by a simulation study comparing CNN and SVM algorithms.

Ge Xu et.al.,(2020) The number of Internet of Things cameras used in smart cities has increased rapidly in recent years. This paper proposes a prediction model for picture forensics using IoT cameras that is based on ensemble learning. In this case, we're interested in extracting human body dimensions from two-dimensional (2D) photos. To begin, the DensePose algorithm takes the two images and extracts 24 features representing different parts of the body. Second, upper body characteristics are combined with dimensions such as height and weight. After that, a regression prediction model is built using an ensemble learning technique called LightGBM. Non-contact image prediction is presented, and it is easy to implement. On an experimental dataset, its viability and validity are confirmed. The experimental findings show that the suggested technique is quite accurate in predicting the size of various human body parts. In particular, the average absolute errors for the predicted chest, waist, and hip measurements are about 2.5 centimetres, whereas the average absolute errors for the other measurements are around 1 centimetre.

Methodology

Here, we provide a passive DIF technique that detects GHE operations and attests to an image's validity using its block mean statistical properties. The image's block mean is calculated by adding together the means of the image's nonoverlapping chunks. The lossy image compression technique known as block truncation coding and its variants have given

the block mean of a picture a central role. Using block mean statistics, the suggested technique trains a support vector machine with 10-fold cross-validation. The trained SVM classifier is capable of distinguishing between uncompressed (RAW) and compressed (JPEG) versions of a picture. Images that have been compressed twice with JPEG but at different quality settings will also reveal the presence of GHE. Both uncompressed and JPEG compressed photos benefit from the high cross-validation accuracies attained in the identification of GHE operation. A second SVM is taught to distinguish between pictures that have been globally equalised using the histogram and those that have not (parametric global contrast-enhanced images). Among several contrast enhancement techniques, the suggested approach is very accurate in detecting GHE.

An image's pixel histogram may be produced with the use of methods like GHE, AHE, etc., and this is what we mean when we talk about non-parametric contrast enhancement. The GHE may be thought of as a separate picture enhancing process. Even though detecting GHE operation does not always mean malicious image tampering, the presence of GHE operation triggers the process of investigating an image in greater depth. Gray-level histograms are the focus of GHE's operation, which takes the histogram of an input picture and returns a uniformly distributed histogram for the output image. Since [60] is a continuous mathematical operation, applying it to a discrete image results in a non-ideal "uniform" distribution of the histogram. This technique, in which the brightness of individual pixels are spread out throughout the full grayscale, is occasionally used to hide evidence of photo editing. The current state of the art methods for detecting tampered images have their own shortcomings when it comes to determining whether or not a picture is genuine based on its attributes, footprints, digital signature, or digital watermark. This is a significant obstacle in the development of a framework for picture tamper detection based on the suggested authentication method, which checks the image's integrity and decides whether or not it has been tampered with. There are two stages to the suggested procedure. Initially, we work on creating an image authentication mechanism that could be incorporated into our current method of acquiring images. This method includes extra procedures that introduce a verification code into the picture, allowing for its validity to be established. The suggested Location Decision Embedding Technique is used to construct a genuine digital picture by embedding a verification code that was developed by the user and added to the image's metadata. During this stage, an authenticating image generation process is made available. In the second stage, we provide a system that can identify and pinpoint instances of picture tampering and copy-move tampering. When a picture is presented as evidence in court, it passes through the phases of the proposed detection process indicated in Figure 2 and is verified using the verification code to establish its credibility. When a tampered picture is detected, the copy-move tamper localization technique pinpoints the offending region.

DOI : https://doi.org/10.56452/7-5-208

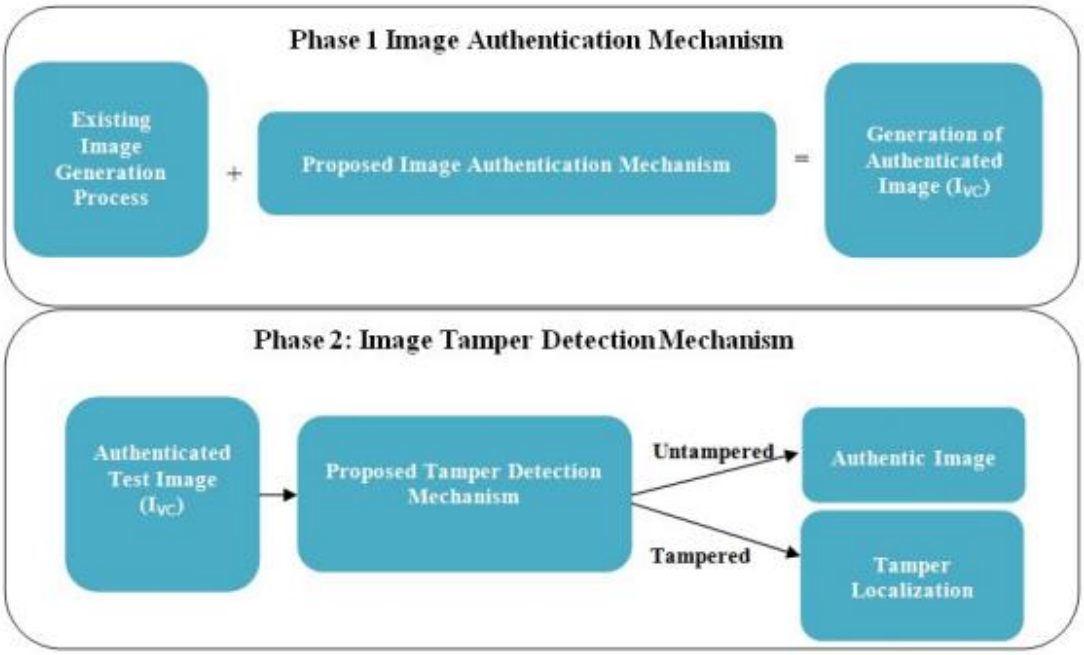

Figure 2. Proposed Methodology

Figure 3(a) Original Frames

Figure 3(b) Forged Frames

Figure 3(a) and (b) above depict an example of this video fraud method in action. Here, the real video frames (as shown in Fig. 3(a)) are on top, while the false video frames (as shown in Fig. 3(b)) are below. Dummy frames 4 and 5 are shown to be carbon copies of the actual frames 1 and 2, as seen above.

DOI : https://doi.org/10.56452/7-5-208

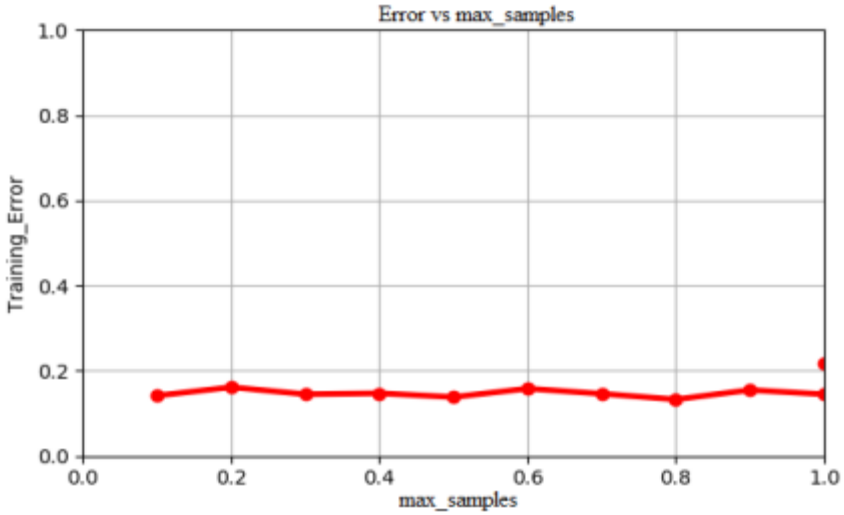

Figure 4 Performance Analysis - Error vs. Max_samples

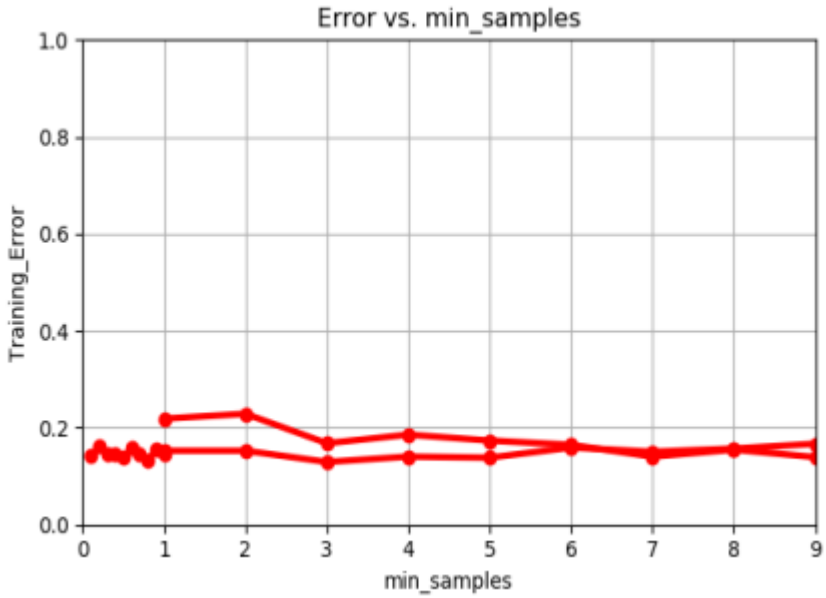

Figure 5. Performance Analysis - Error vs. Min_samples

Conclusion

It is commonly agreed that one of the best techniques to validate the authenticity and integrity of digital images is via image source forensics. Motivated by the fantastic results produced with data-driven approaches on computer vision challenges, numerous academics have applied these methods to this job in recent years. The most significant data-driven techniques for solving the forensics of picture sources are presented in this survey. To help organise this large subject, we've broken it down into the following five categories: images taken from different sources, forensics for computer graphics (CG) images, detecting GAN-generated images, identifying cameras used to capture the images, and identifying cameras used to capture images from social networks.

References

1. S. Agarwal and K. -H. Jung, "Image Forensics using Optimal Normalization in Challenging Environment," *2021 International Conference on Electronics, Information, and Communication (ICEIC)*, Jeju, Korea (South), 2021, pp. 1-4, doi: 10.1109/ICEIC51217.2021.9369794.
2. K. Wu, W. Dong, Y. Cao, X. Wang and Q. Zhao, "An Improved Method of Median Filtering Forensics for Enhanced Image Security Detection," *2021 International Conference on Networking and Network Applications (NaNA)*, Lijiang City, China, 2021, pp. 308-312, doi: 10.1109/NaNA53684.2021.00060.
3. G. Xu *et al.*, "An Ensemble Learning-Based Prediction Model for Image Forensics From IoT Camera in Smart Cities," in *IEEE Access*, vol. 8, pp. 222117-222125, 2020, doi: 10.1109/ACCESS.2020.3043765.
4. Y. Wang and Y. Li, "Research on Digital Media Image Data Tampering Forensics Technology Based on Improved CNN Algorithm," *2021 5th Asian Conference on Artificial Intelligence Technology (ACAIT)*, Haikou, China, 2021, pp. 393-397, doi: 10.1109/ACAIT53529.2021.9731182.
5. Ingole, K. . A review on secure image sharing using diverse media using Matlab. Research and Applications: Embedded System Vol 4, No 2 (2021) http://hbrppublication.com/OJS/index.php/RAES/article/view/1892
6. F. Ahmed, F. Khelifi, A. Lawgaly and A. Bouridane, "The 'Northumbria Temporal Image Forensics' Database: Description and Analysis," 2020 7th International Conference on Control, Decision and Information Technologies (CoDIT), Prague, Czech Republic, 2020, pp. 982-987, doi: 10.1109/CoDIT49905.2020.9263888.
7. Y. Quan, C. -T. Li, Y. Zhou and L. Li, "Warwick Image Forensics Dataset for Device Fingerprinting in Multimedia Forensics," *2020 IEEE International Conference on Multimedia and Expo (ICME)*, London, UK, 2020, pp. 1-6, doi: 10.1109/ICME46284.2020.9102783.
8. G. U. Reddy, M. Madhu Bala and B. Padmaja, "An Overview on Digital Forensics Tools used in Crime Investigation for Forgery Detection," *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, Gunupur, India, 2020, pp. 1-5, doi: 10.1109/ICCSEA49143.2020.9132965.
9. R. S. Khalaf and A. Varol, "Digital Forensics: Focusing on Image Forensics," *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Barcelos, Portugal, 2019, pp. 1-5, doi: 10.1109/ISDFS.2019.8757557.
10. S. Qu, "An approach based on object detection for image forensics," *2019 1st International Conference on Industrial Artificial Intelligence (IAI)*, Shenyang, China, 2019, pp. 1-6, doi: 10.1109/ICIAI.2019.8850791.
11. S. K. Yarlagadda *et al.*, "Shadow Removal Detection and Localization for Forensics Analysis," *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brighton, UK, 2019, pp. 2677-2681, doi: 10.1109/ICASSP.2019.8683695.
12. S. Cha, U. Kang and E. Choi, "The Image Forensics Analysis of JPEG Image Manipulation (Lightning Talk)," *2018 International Conference on Software Security and Assurance (ICSSA)*, Seoul, Korea (South), 2018, pp. 82-85, doi: 10.1109/ICSSA45270.2018.00029.
13. Y. Chen, Z. X. Lyu, X. Kang and Z. J. Wang, "A Rotation-Invariant Convolutional Neural Network for Image Enhancement Forensics," *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Calgary, AB, Canada, 2018, pp. 2111-2115, doi: 10.1109/ICASSP.2018.8462057.

DOI : https://doi.org/10.56452/7-5-208

14. C. Maigrot, E. Kijak and V. Claveau, "Context-Aware Forgery Localization in Social-Media Images: A Feature-Based Approach Evaluation," *2018 25th IEEE International Conference on Image Processing (ICIP)*, Athens, Greece, 2018, pp. 545-549, doi: 10.1109/ICIP.2018.8451726.
15. S. Agarwal and H. Farid, "Photo forensics from JPEG dimples," 2017 IEEE Workshop on Information Forensics and Security (WIFS), Rennes, France, 2017, pp. 1-6, doi: 10.1109/WIFS.2017.8267641.