

Vol. 8, Issue 3, March 2019

Image Resampling Detection: A Review

Rachna Mehta¹, Navneet Agarwal²

PhD Scholar, Department of ECE, CTAE, MPUAT, Udaipur, India¹ Assistant Professor, Department of ECE, CTAE, MPUAT, Udaipur, India²

Abstract: Image resampling detection is a key strategy in the blind image forgery detection and has been developed a lot in a previous couple of years. This paper surveys the picture resampling detection techniques proposed in the latest years, give comprehensive differences in their performance and uncovers the principle difficulties brought up in a few significant issues, for example, detection of rotating image, reducing noise in the resampled image and improving productivity. Moreover, this paper examines the current expariments and brings up potential hotspots in this field. We accept this review can give some direction for researchers from significant research zones, offering them a general and novel view.

Keywords: Image Resampling, Interpolation, Bicubic, Bilinear, Nearest Neighbor.

I. INTRODUCTION

We are living in the age where we are uncovered from time to time to an assortment of magnificent digital pictures which are difficult to accept. Evidently, conventional saying, — seeing is believingl, do not remain constant. Nowadays, due to the progress of mechanized picture dealing with programming and modifying gadgets, an image can be easily controlled and changed [1]. It is amazingly inconvenient for individuals to perceive ostensibly whether the image is original or forged. There is a quick addition in carefully controlled adulterations in standard media and on the Internet [2]. This example demonstrates certifiable vulnerabilities and decreases the believability of computerized pictures. As such, making methods to check the trustworthiness and realness of the propelled pictures is basic, especially taking into account that the photos are presented as proof in an official courtroom, as news things, as a piece of helpful records, or as cash related reports. In this sense, picture resampling detection is one of the basic destinations of Image forensics [3]. The fundamental target of this paper is: To display a different part of Image forgery detection; To audit some late and existing methodology in Image resampling detection; To give a similar investigation of existing techniques with their focal points and detriments. The remainder of the paper is sorted out as pursues. A review of picture forgery detection has exhibited in the principal segment. In the second area, we examine the distinctive kind of Image Interpolation. In the third section, we present and examine various existing procedures of Image resampling detection and the last segment gives the finish of this paper with a conclusion.

II. TYPES OF IMAGE FORGERY

Picture adjusting is described as "including, changing, or erasing some significant highlights from a picture without leaving any conspicuous traces [2]. There have been various methods used for producing a picture. Considering the strategies used to make fashioned pictures, Digital Image forgery can be confined into four essential orders: Image resampling detection, Image splicing and Copy-move forgery.

A. Image Resampling

To make readable forged pictures, a falsifier needs to utilize some geometric activities which require a resampling of pixels. Resampling is a post-camera processing procedure. generally, it is proposed not to compare resampling among the picture tampering methods. In any case, resampling of pixels is the premise of numerous phonies since it is associated with all geometric change (rotation, resize, etc. ...)[3]. While the confirmation of resampling task inside a picture does not fundamentally infer that the picture has been tempered it is a vital piece of information. Accordingly, resampling indicators assume a vital part as an additional forensic tool Furthermore, resampling distortion regularly happens together with another tampering methods, for example, copy-move or splicing detection. For example, to upgrade the visual authenticity, splicing and copy move tampering regularly require scaling or rotation activities which require pixels resampling. A common case is shown in Fig.1.1. The original picture appeared in fig.1.1a is first resized, through a broadening of 120%, and after that edited to acquire a picture of an indistinguishable size from the original; the outcome is appeared in fig.1.9b

IJARCCE



International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 3, March 2019



(a) Original Image

(b) Forged Image Fig.1.1 Image Resampling Example

B. Image Splicing

Diverse components from different pictures are posted in a solitary picture to pass on a thought that doesn't reflect reality. Such splicing can usually be detected by splicing edges [3,4], or the impact of splicing on picture insights, or by considering the directions of the light occurrence on the picture surfaces (Granty, et al., 2010). An example of picture splicing is shown in Fig.1.2.



Fig.1.2.Image splicing example

C. Cloning

Copy-move forgery, also called Cloning when just a single picture is considered for the forging procedure, is pretty much like picture Splicing in perspective of the way that both methods alter a specific picture district with another picture. One area is replicated from a picture and pasted onto another region of a similar picture. In any case, rather than utilizing an outside picture as a source, copy-move forgery [3,4] utilizes segments of the original picture as a source which implies that a similar picture is both the source and the altered picture. Since the replicated parts originate from a similar picture, its imperative properties, for example, noise, texture, and brightness will be perfect with whatever remains of the picture making it more troublesome for specialists to recognize and distinguish the adjustment. The example of cloning is shown in fig.1.8. In this Iran additionally discharged a changed photo on July 9, 2008, demonstrating four rockets ascending into the air rather than three amid a test terminating at an undisclosed area in the Iranian abandon. Unexpectedly, a few western media, including New York Times and Los-Angeles Time distributed that falsified picture as though it was a genuine picture.



a) (b) (c)
Fig.1.8. Example of a copy-move forgery
(a) is the original image, (b) is manipulated, and (c) the duplicated regions





Vol. 8, Issue 3, March 2019

III. TYPES OF IMAGE INTERPOLATION

There are 4 interpolation techniques used in resampling namely,

- 1. Nearest neighbor
- 2. Bilinear interpolation
- 3. Bicubic interpolation

1. Nearest Neighbor:

It is basic and requires less computational time contrasted with other strategies [2,3]. This is likewise called point – shift algorithm. It chooses the values of the pixel which is extremely close by encompassing directions of the planned interpolation point. By utilizing of this, it will finds closest practically identical pixel in the source picture for every pixel in the last picture [12,10,8]. The spots or pixels of shading are indistinguishable to create another pixels as the size of the picture grows. It makes edges that separate bends into rough edges or steps. This type of interpolation impacts for both decrease and expanding of pictures. The addition part for the nearest neighbour algorithm is defined as

$$f(x) = \begin{cases} 0, & x < 0\\ 1, & x > 0 \end{cases}$$

The distance between grid point and interpolated point is denoted by x.

2. Bilinear Interpolation:

It will acknowledge the weighted mean value of the 4 nearby pixels to compute its final value. This will be utilized to discover esteems at the arbitrary situation from the weighted normal of the four closest pixels to calculate the input coordinates and allocate that value to the output coordinate. This method [2] performs interpolation in the two directions, vertical and horizontal. The interpolation Kernel for Bilinear insertion is [14].

$$u(x) = \begin{cases} 0, & |x| > 1\\ 1 - |x|, & |x| < 1 \end{cases}$$

The distance between grid point and interpolated point is denoted by x.

3. Bicubic Interpolation:

This method is improved version over the cubic interpolation in 2 dimensional regular grid. [3,4] The interpolated surface is smoother than equivalent surfaces gained by an above mentioned methods, Bilinear interpolation and Nearest neighbor [12,10,8]. Bicubic goes one step outside the limitations of bilinear by taking into consideration of the closest 4x4 surrounding pixels for a total of 16 pixels. For this cause it became a standard in almost all image editing software or tools such as printer drivers, in-camera interpolations and Adobe Photoshop, The interpolation for Bicubic interpolation is

$$U(x) = \begin{cases} \frac{3}{2}|x|^3 - \frac{5}{2}|x|^2 + 1, & 0 \le |x| < 1\\ -\frac{1}{2}|x|^3 + \frac{5}{2}|x|^2 - 4|x| + 2, & 1 \le |x| < 2\\ 0 & 2 < |x| \end{cases}$$

IV. EXISTING IMAGE RESAMPLING TECHNIQUES

Popescue (2004) studied that [5], A carefully modified picture, frequently leaving no visual hints of having been altered, can be indistinct from a real picture. The tampering, although, may aggravate some basic measurable properties of the picture. Under this supposition, they propose five strategies that evaluate and recognize factual disturbance found in various types of altered pictures: (1) re-sampled pictures (e.g., scaled or rotated); (2) controlled colour filter array inserted pictures; (3) doubled JPEG compressed pictures; (4) pictures with copied regions; and (5) pictures with conflicting noise designs.

Popescu and Farid (2005), portrayed that [6], how resampling (e.g., scaling or turning) presents particular factual correlation, and depict how these relationships can be consequently recognized in any part of a picture. Their system works without any computerized watermark or mark. They demonstrate the viability of this approach on uncompressed TIFF pictures, and JPEG and GIF pictures with insignificant compression. The author anticipates that this system will be among the first of numerous devices that will be expected to uncover computerized imitations

Gallaghar. A (2005), proposed the novel interpolation [8] detection algorithm is a fast and efficient algorithm for determining if an image has undergone interpolation with a low-order interpolator and the rate of that interpolation. The



Vol. 8, Issue 3, March 2019

algorithm operates by exploiting the property that the second derivative signal of the interpolated images contains a periodicity. The algorithm produced reliable results on test images from a Kodak EasyShare CX7300 digital camera where interpolation occurs prior to compression with the digital zoom feature. The performance of the algorithm degrades for highorder interpolation filters such as a windowed sinc interpolation filter.

Prasad and Ramakrishanan (2006), found that the resampling task [7] changes certain attributes of the pasted segment, which when distinguished fills in as a piece of information of tampering. In their work, they introduce deterministic procedures to recognize resampling and confine the segment of the picture that has been messed with. They utilized Two procedures for identification, one is a pixel domain and other is frequency domain. In the pixel domain, they found the periodicity of the resampled and non-resampled pictures by zero crossing property of second difference and found that the resampled samples have distinct magnitude peaks by utilizing DFT in the examination of non-resampled samples

Wang and Moullin (2007), represented [10] that Supervised learning is a powerful and universal approach to deal with the twin challenges of unknown picture statistics and unknown steganographic codes. A pivotal piece of the learning procedure is the determination of low-dimensional instructive features.

Mahdian and Saic (2008), examined [11] particular periodic properties exhibit in the covariance structure of interpolated signals and their derivatives. Besides, they have presented a concise two– dimensional extension of the depicted hypothesis. Likewise, they have investigated a use of Taylor series to the added signals. The fundamental commitment of their work is a technique prepared to do effortlessly identifying hints of scaling, rotation, skewing changes and any of their self-assertive blends. The strategy is quick, blind and effective. It works for wide assortment of resampling factors. Another favourable position of the technique is it can be extremely useful in the estimation of scaling factors or rotation angles.

Kirchner (2008), Inspired by these ongoing discoveries [12], in their work, the author returned to Popescu and Farid's work and investigate the inception of periodic artifacts in the p-map of a resampled picture, which is the principle yield of the detector. A simplified show in light of the variance of the prediction residue will fill in as a tool to clarify the real appearance of the p-map and its spectral representation for arbitrary geometric changes. This goes past the original work of Popescu and Farid, as they didn't give an unequivocal connection on how a specific change will impact the detector output in the spatial and in the frequency domain.

Kichner and Gloe (2009), have researched [13] the discovery of resampling in re-compressed pictures. While lossy compression so far has for the most part been talked about as far as negative consequences for the perceptibility of geometric changes, they have demonstrated how blocking artefacts in re-compressed pictures can really expand identification execution. In view of linear predictor residue resampling discovery, the principle commitments of their work lie in a depiction of how affine transformation of pre-compressed pictures influence the identifier yield (I. e. the pmap's Fourier spectrum) and the introduction of a reasonable recognition variation. experiment results come about affirm that resampling discovery in JPEG pictures isn't by definition an act of futility.

Liu and Sung (2009), , focused [16] on the relationship of neighboring Discrete Cosine Transform (DCT) coefficients and they proposed a technique to identify resized JPEG pictures and spliced pictures, which are generally utilized as a part of picture forgery. In detail, the neighbouring joint density features of the DCT coefficients are extracted; at that point, Support Vector Machines (SVM) are applied to the features for detection. To enhance the assessment of JPEG resized discovery, we use the shape parameter of generalized Gaussian distribution (GGD) of DCT coefficients to quantify the picture complexity..

Kichner (2010), investigated [14] how the characteristic structure of resized (and therefore interpolated) pictures can be abused to show the particular linear relationships between's neighboring pixels more unequivocally. While existing strategies measure addition curios in some kind of residue signal, acquired by linear filtering with a global kernel, they have demonstrated that the particular periodicities can likewise be recognized in a progression of custom fitted row and column predictors.

Dalgaard et. al.(2010), found [18] that identification of resampling traces for computerized picture blind authentication has been communicate to as of late by A. C. Gallagher and later stretched out by B. Mahdian and S. Saic. On the opposite side, it is notable from the synchronization region in communication that prefiltering is a proper tool to enhance the execution of those plans misusing the basic cyclostationarity of correspondence signals. In this manner, the discovery of resampling traces enhances essentially when the derivative of the interpolated signals is utilized for covariance calculation. This work focuses on the part of prefiltering as a method for boosting resampling traces and, specifically, on the utilization of derivation.

Ucheddu (2010) et al. found [20], in actuality, a large portion of the published works do not have an unmistakable clarification of the conditions under which an examination between proposed strategies and contending procedures is done; generally research results of resampling detection comes about are given on little dataset; the data about the experiment setups (like freely accessible informational collections, usage of the proposed calculation and picked



Vol. 8, Issue 3, March 2019

parameters, steps followed in the analyses) is normally insufficient point by point to warrant a simple reproducibility of the prior work. Every one of these impediments don't permit a reasonable and simple approval and examination with recently proposed strategies. Their work goes for beginning to fill this research gap by concentrate a strategy for the execution investigation of picture scientific methods ; specifically they concentrated on the class of criminological algorithm i.e i.e Kirchner and Gloe's method and Mahdian & Saic method intended for the discovery of resampling activities connected to the computerized pictures and they describe indepth analysis in general of their behavior under different working conditions.

Zhang et. al. (2011, proposed [21] a technique relative to the additive noise steganography model, they proposed a strategy to recognize the least significant bit (LSB) matching steganography in grayscale pictures. Pictures are disintegrated into detail sub-bands with local linear transform (LLT) masks which are sensitive to embedding. Novel normalized characteristic function features weighted by a bank of band-pass filter are produce from the detail sub-bands. A minimal feature set is sought by utilizing a thresholding algorithm.

Feng et. al (2012), proposed [19] the contemporary technique to distinguish resampling traces. The strategy depends on analyzing the normalized energy density present inside windows of shifting size in the second derivative of the picture in the frequency domain and utilizes this characteristic to determine a 19-D feature vector that is utilized to train an SVM classifier. Exploratory outcomes are accounted for on 7500 raw pictures from the BOSS database. Correlation with earlier work uncovers that the proposed algorithm performs likewise to resampling rates more prominent than 1, and is better than earlier work for resampling rates under 1. Analysis is performed for both bilinear and bicubic interpolation and subjectively homogeneous results are watched for each.

Kodovsky (2013), proposed [22] that the measurable properties of cover source unequivocally influence steganographic security. For example, the Square-Root Law (SRL) [1] states that a steady level of factual perceptibility is acquired when the message length get bigger relative to the square root of the number of pixels in the picture. This law shows when pixels from a similar source are included/expelled, e.g., by sewing together pictures to get a display or by editing. At the point when the quantity of pixels is changed by resizing, the factual properties of the source change and the SRL never again holds in its standard frame. The examination of this wonder is the subject of their work.

Li et. al. (2013), proposed [16] a moment feature based technique to distinguish resample pictures. Instead of focusing on the places of resampling peaks, we use a moment feature to utilize the periodic interpolation qualities in the frequency domain. Not just the places of resampling peaks yet, in addition, the amplitude distribution are contemplated. With the extricated moment feature, trained SVM classifier is utilized to recognize resampled pictures

Birajdar and Mankar (2014), proposed [23] an algorithm which introduces the blindly recognize worldwide rescaling activity and evaluate the rescaling factor in view of the auto covariance sequence of zero-crossing of the second derivative of the altered picture. The analysis outcomes utilize UCID and USC-SIPI database demonstrate the legitimacy of the algorithm under various interpolation schemes. The method is vigorous and effectively identifies rescaling task for pictures that have been subjected to different types of assaults like JPEG compression and self-assertive editing. Of course, some debasement in detection accuracy is seen as the JPEG quality factor diminished.

Hou et. al. (2014), examination [24] introduces a technique for resampling detection on textured images. To begin with, the local linear transform is utilized to get textural detail sub-bands. A 36-D feature vector is then extricated from the normalized characteristic function moments of textural detail subbands to train a support vector machine classifier. At last, exploratory outcomes are accounted for on three databases, with each having very nearly 10,000 pictures. Examination with the past investigation uncovers that the proposed technique is powerful to resampling detection.

Padin et. al. (2015) proposed a straightforward methodology for resampling detection. In their proposed identifier they just need to calculate the SVD of a given picture block and a measure of its level of saturated pixels per row/column, for perceiving upsampled pictures from original ones. The accomplished execution is promising and when contrasted with Kirchner's technique, their indicator beats it. As their future work, they are wanting to apply a similar thought for distinguishing resampling activities by factors smaller than one, however together producing the traces left by the demosaicing procedure and the downsampling in the three color parts of an advanced picture.

Bayar and stemm (2016), proposed [25] a universal criminological way to deal with alteration detection by using deep learning. In particular, they propose another convolutional network design able to do naturally detection of altering features straightforwardly from training information. They build up a convolutional layer that is particularly intended to smother a picture's content and adaptively learn alteration detection features. The outcomes of these examinations demonstrate that our proposed approach can naturally recognize a few distinctive changes with an average accuracy of 99.10%.

Peng and Wu (2017), proposed [26] a successful and secure detector, which can at the same time recognize resampling and its manufactured resampling. They find that the interjection activity utilized in the resampling and manufactured resampling makes these two sorts of picture demonstrate distinctive measurable practices from the unaltered pictures, particularly in the high-frequency domain.



Vol. 8, Issue 3, March 2019

TABLE I

Summary for Image Resampling Detection Techniques

Sr. No.	Author	Year	Contribution
1	Popescue [5]	2004	They propose five strategies that evaluate and recognize factual disturbance found in various types of altered pictures: (1) re-sampled pictures (e.g., scaled or rotated); (2) controlled colour filter array inserted pictures; (3) doubled JPEG compressed pictures; (4) pictures with copied regions; and (5) pictures with conflicting noise designs. These strategies work without any inserted watermarks or signatures.
2	Popescu and Farid [6]	2005	The author portray that, how resampling (e.g., scaling or turning) presents particular factual correlation, and depict how these relationships can be consequently recognized in any part of a picture. Their system works without any computerized watermark or mark.
3	Gallaghar. A [8]	2005	They proposed the novel interpolation detection algorithm by exploiting the property that the second derivative signal of the interpolated images contains a periodicity.
4	Prasad and Ramakrishanan [7]	2006	They utilized two procedures for resampling detection, one is a pixel domain and other is frequency domain. In the pixel domain, they found the periodicity of the resampled and non-resampled pictures by zero crossing property of second difference and in frequency domain they use Block DCT has been utilized for a careful highpass filtering which draws out the contrasts amongst resampled and non-resampled pictures.
5	Wang et. al. [10]	2007	They introduces Supervised learning is a powerful and universal approach to deal with the twin challenges of unknown picture statistics and unknown steganographic codes. By using two kinds of features—empirical moments of probability density functions (PDFs) and empirical moments of the characteristic function of the PDFs.
6	Mahdian et. al. [11]	2008	The authors have examined particular periodic properties exhibit in the covariance structure of interpolated signals and their derivatives. Besides, they have presented a concise two– dimensional extension of the depicted hypothesis.
7	Kirchner et. al. [12]	2008	The authors returned to Popescu and Farid's work and investigate the inception of periodic artifacts in the p-map of a resampled picture, which is the principle yield of the detector.
8	Kichner et. al. [13]	2009	They have demonstrated how blocking artifacts in re-compressed pictures can really expand identification execution by using affine transformation.
9	Liu and Sung [16]	2009	In their work, they in light of the relationship of neighbouring Discrete Cosine Transform (DCT) coefficients, they propose a technique e to identify resized JPEG pictures and spliced pictures, which are generally utilized as a part of picture forgery
10	Kichner [14]	2010	The author have investigated how the characteristic structure of resized (and therefore interpolated) pictures can be abused to show the particular linear relationships between's neighboring pixels more unequivocally
11	Dalgaard et. al [18]	2010	This work focuses on the part of prefiltering as a method for boosting resampling traces and, specifically, on the utilization of derivation
12	Ucheddu [20]	2010	Specifically they concentrated on the class of criminological algorithm i.e i.e Kirchner and Gloe's method and Mahdian & Saic method intended for the discovery of resampling activities connected to the computerized pictures and they describe indepth analysis in general of their behavior under different working conditions.
13	Zhang et. al. [21]	2011	They propose a strategy to recognize the least significant bit (LSB) matching steganography in grayscale pictures.
14	Feng et. al [19]	2012	Their strategy depends on analyzing the normalized energy density present inside windows of shifting size in the second derivative of the picture in the frequency domain and utilizes this characteristic to determine a 19-D feature vector that is utilized to train an SVM classifier
16	Li et. al. [16]	2013	They use a moment feature to utilize the periodic interpolation qualities in the



Vol. 8, Issue 3, March 2019

			frequency domain. They also work on the amplitude distribution. The moment extracted features are applied on SVM classifier for detection
17	Kodovsky [22]	2013	Proposed that the measurable properties of cover source unequivocally influence steganographic security.
18	Birajdar et. al. [23]	2014	The author proposed an algorithm which introduces the blindly recognize worldwide rescaling activity and evaluate the rescaling factor in view of the auto covariance sequence of zero-crossing of the second derivative of the altered picture
19	Hou et. al. [24]	2014	They consider the task of resampling detection as a texture classification issue. A 36-D feature vector is then extricated from the normalized characteristic function moments of textural detail sub bands to train a support vector machine classifier.
20	Padin et. al.	2015	In their proposed detector they just need to calculate the SVD of a given picture block and a measure of its level of saturated pixels per row/column, for perceiving upsampled pictures from original ones
21	Bayar et. al. [25]	2016	They propose another convolutional network design able to do naturally detection of altering features straightforwardly from training information.
22	Peng and Wu [26]	2017	They propose a novel resampling and forged resampling detection approach to deal with high pass filter and autoregressive model.

V. COMAPARATIVE RESULTS

We have examined different strategies that are proposed by numerous authors to identify image resampling detection. The point of view of the significant number of techniques is to perceive the forgery in the image yet the strategies are assorted. Table 1 demonstrates the examination of different Image resampling detection techniques, which have talked about in this paper.

VI. CONCLUSIONS

In this paper various strategies of image resampling detection have been studied and talked about. Every one of the methodologies and procedures discussed in this paper has the ability to perceive forgery. Regardless, a couple of algorithms are not feasible with respect to recognizing the forged region Then again, a few algorithms have a time unpredictability issue. Along these lines, there is a need to build up a viable furthermore, exact picture detection algorithm.

REFERENCES

- [1]. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, 2007, Digital watermarking and steganography. Science Direct, pp. 425-467,
- [2]. Johnson.M.K and Farid.H, 2007, Exposing Digital Forgeries Through Specular Highlights on the Eye, In: Proceeding of the 9th International conference on Information Hiding, held at Saint Malo, France during June 11-13, 2007, pp. 311-325.
- [3]. Judith, A. Wiem, T. Jean-Luc, D. 2010, Digital image forensics: a booklet for beginners, *Multimedia Tools and Applications*, 51: 133-162.
- [4]. Kakar. P, Sudha.N, and Ser.W, 2011, Exposing Digital Image Forgeries by Detecting Discrepancies in Motion Blur, *IEEE Transactions on Multimedia*, 13: 443–452
- [5]. Popescu.A.C and Farid.H, 2004, Statistical tools for digital forensics, In: Proceedings of the International workshop on Information Hiding held at Toronto, Canada during May 23-25, 2004, pp. 128–147.
- [6]. Popescu.A.C and Farid.H,2005, Exposing digital forgeries by detecting traces of re-sampling, *IEEE Transactions on Signal Processing*, 53: 758-767.
- [7]. Prasad, S.; Ramakrishnan, K.R., 2006, On resampling detection and its application to image tampering. *In: Proceedings of the IEEE International Conference on Multimedia and* Exposition held at Toronto, Canada during July 9-12, 2006, pp. 1325–1328
- [8]. Gallagher. A, 2005, Detection of linear and cubic interpolation in JPEG compressed images, In: Proceedings of the 2nd Canadian Conference on Computer and Robot Vision held at Victoria, BC, Canada during May 9-11, 2005, pp. 65–72
- [9]. Prasad, S.; Ramakrishnan, K.R., 2006, On resampling detection and its application to image tampering. *In: Proceedings of the IEEE International Conference on Multimedia and* Exposition held at Toronto, Canada during July 9-12, 2006, pp. 1325–1328.
- [10]. Wang Y, Moulin P, 2007, Optimized feature extraction for learning-based image steganalysis. IEEE Transactions on Information Forensics and Security 2: 31–45.
- [11]. Mahdian. B and Saic. S, 2008, Blind authentication using periodic properties of interpolation, *IEEE Transactions on Information Forensics and Security*, 3: 529–538.
- [12]. Kirchner.M, 2008, Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue, In: *Proceedings of the 10th ACM Workshop on Multimedia Security*, held at oxford, United Kingdom during September 22-23, 2008, pp. 11–20.
- [13]. Kirchner.M and Gloe.T, 2009, On resampling detection in recompressed images, In: Proceedings of the 1st IEEE International Workshop on Information Forensics and Security held at London, United kingdom during December 6 – 9, 2009, pp. 21–25.
- [14]. Kirchner.M, 2010, Linear row and column predictors for the analysis of resized images, In: *Proceedings of the12th ACM Workshop Multimedia* and Security held at Roma, Italy during September 9 – 10, 2010, pp. 13–18.
- [15]. Kodovský J, Fridrich J, and Holub V, 2012, Ensemble classifiers for steganalysis of digital media, *IEEE Trans. Information Forensics and Security*, 7:, 432–444.
- [16]. Liu. Q and Sung. A, 2009, A new approach for JPEG resize and image splicing detection, In: Proceedings of the First ACM Workshop Multimedia Forensics held at Beijing, China during October 23, 2009, pp. 43–48



Vol. 8, Issue 3, March 2019

- [17]. Kirchner.M, 2010, Linear row and column predictors for the analysis of resized images, In: *Proceedings of the12th ACM Workshop Multimedia* and Security held at Roma, Italy during September 9 – 10, 2010, pp. 13–18.
- [18] Dalgaard. N, Mosquera. C, and Pérez-González. F, 2010, On the role of differentiation for resampling detection, In: Proceedings IEEE International Conference on Image Processing held at Hong Kong, China during September 26-29, 2010, pp. 1753–1756
- [19]. Feng XY, Cox IJ, Doërr G, 2012, Normalized energy density-based forensic detection of resampled images, *IEEE Transactions on Multimedia* 14: 536–545.
- [20]. Uccheddu. F, Rosa. A. D., Piva. A, and Barni. M, 2010, Detection of resampled images: Performance analysis and practical challenges," In: Proceedings of 18th European. Signal Processing Conference held at Aalborg, Denmark during August 24–27, 2010, pp. 1675-1679.
- [21]. Zheng EG, Ping XJ, Zhang T, 2011, Local linear transform and new features of histogram characteristic functions for steganalysis of least significant bit matching steganography. *KSII Transactions on Internet and Information System* 5: 840–855
- [22]. Kodovský.J and Fridrich.J, 2013, Steganalysis in resized images, In: Proceedings of the IEEE International Conference on Acoustic, Speech, Signal Processing held at ., Vancouver, BC, Canada during May 26 31, 2013, pp. 2857–2861
- [23]. Birajdar, G, Mankar, V, 2014, Blind method for rescaling detection and rescale factor estimation in digital images using periodic properties of interpolation. *AEU International Journal of Electronics and Communication* 68: 644–652
- [24]. Hou.X, Zhang T, Xiong G, Zhang Y, and Ping X, 2014, Image resampling detection based on texture classification, *Multimedia Tools and Applications*, 72: 1681–1708.
- [25]. Bayar. B and Stamm.C.M, 2016, A Deep Learning Approach To Universal Image Manipulation Detection Using A New Convolutional Layer, In: Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, June 20-22, 2016 held at Vigo, Galicia, Spain, pp. 5-10,
- [26]. Peng.A, Wu.Y, Kang.X, 2017, Revealing traces of image resampling and resampling antiforensics, Hindawi Journal of Advances in Multimedia, 2017: pp. 1-13.