IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13131

A depth analysis of Image Splicing forgery detection

Dr. Jaynesh H Desai

Assistant Professor, Bhagwan Mahavir College of Computer Application, Surat, India[1]

Abstract: This research proposes a novel image splicing detection and localization approach based on the deep convolutional neural network (CNN) learned local feature descriptor. Presented and used to automatically learn hierarchical representations from the input RGB colour or grayscale test images is a two-branch CNN that functions as an expressive local descriptor. The suggested CNN model's first layer, which is specifically made for picture splicing detection applications, is used to extract expressive and varied residual features while also suppressing the impacts of the image contents. Specifically, an optimised combination of the 30 linear high-pass filters employed in the computation of residual maps in the spatial rich model (SRM) is utilised to initialise and fine-tune the kernels of the first convolutional layer.The advancement of digital splicing technology has significantly impacted the progress of digital photo manipulation. This is particularly evident in industries such as newspaper and magazine publication, as well as companies that rely on the verification of photograph authenticity for their publications. Previously, these businesses faced substantial challenges in pre-publication due to the complexities of digital forensics in image processing. However, with the latest developments, the authentication process can now be swiftly addressed with just a few keystrokes. This review is intended to familiarize the reader with various types of digital image splicing forgeries, focusing on the current trend of passive techniques employed to confirm the authenticity of images before they are published

Keywords: Digital image forensics, image forgery detection, Image authentication, , Image Splicing, Passive techniques. Image splicing detection.

I. INTRODUCTION

Growing technological advancements have made digital picture alteration easier, which has affected how much people worry about the image splicing process. The lack of sufficient and necessary verification systems has resulted in a deterioration in the feasibility of automated content due to poor acceptance and existence of image verification processes. Furthermore, the evolution of automated algorithms affects the extent of manipulation that can be done, so limiting the scope of human inspection and increasing the amount of image manipulation that occurs as a result of inadequate verification methods [1].

Many methods are used on text in addition to images to identify scripts; this is accomplished by segmentation, which is essential to the script identification process [2]. An actual documented case was given at the beginning of the 1840s. Being Hippolyta Bayard the first to use picture manipulation techniques such as forgeries. He created a fake image, as seen in figure 1 below, in which he looked to be taking his own life. This technique was merely an answer to Louis Daguerre, creator of the Daguerreotype, much to Bayard's annoyance, obtained a copyright for a photographic development before Bayard made any attempts [2].

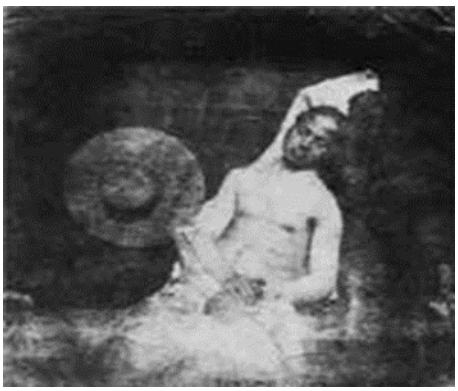


Figure 1: First photographic forger [2]

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13131

II. CLASSIFICATION OF IMAGE FORGERY DETECTION TECHNIQUES

methods have been suggested to achieve outstanding authenticity in photographs. These methods are divided into two categories in this paper: active authentication and passive authentication. This classification is based on whether the original image is truly available; if it is, the fake is categorised as hierarchical, as seen in figure 2.

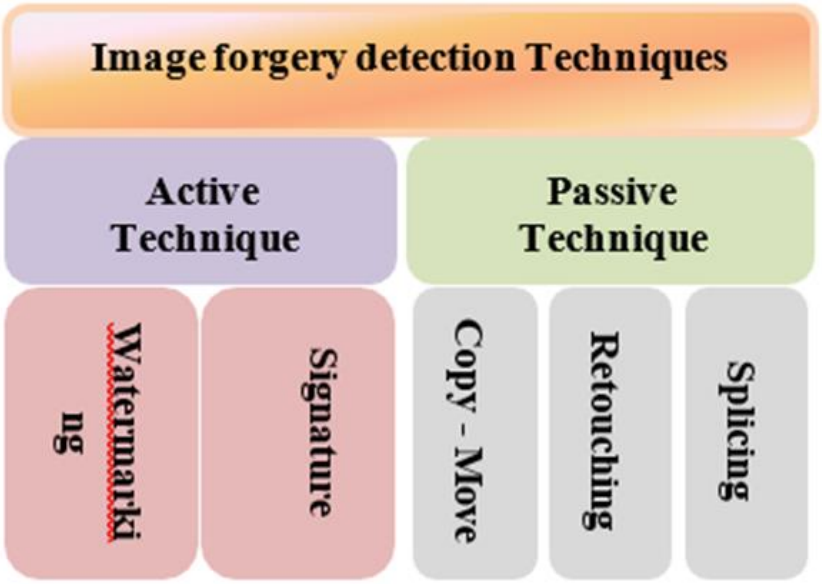


Figure 2: Authentication Techniques of Image

Active Techniques

In the era of false news, pictures of events, situations, and persons can also be altered and presented to the public in addition to verbal information. To lend the article an air of credibility, these artificial depictions of the real person are presented alongside phoney material. To put it simply, an active technique-spliced image is one that has been altered. A number of these active techniques rely on the first passive identification of falsification, which is based on the beliefs that the active techniques present. ([4], [2]).

This practice, though practiced actively in the past, had limited applications types:

Watermark – A digital watermark is integrated into an image being captured, supported by an integrity authentication on the recipient side.

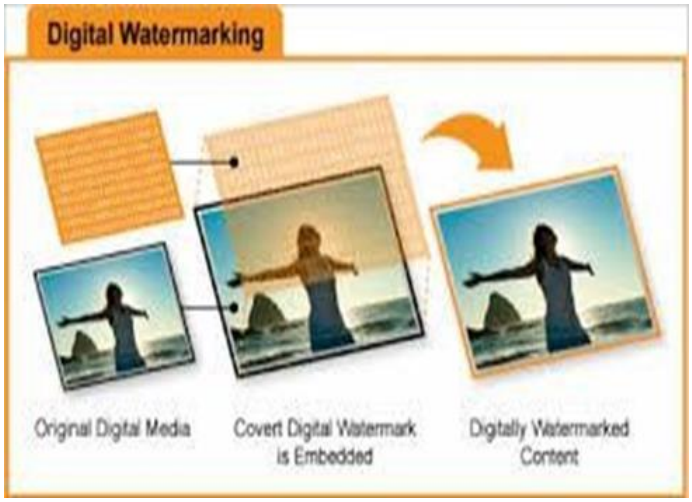


Figure 3: The conversion process from original media to digital watermarked content.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13131

Signature – A camera's image will be extracted of its distinct aspects and then data encoded using a signature.

Passive Techniques

Another name for this method is image forensics. The lead of leaving traces throughout steps provided in various stages while obtaining and storing digitally acquired images is utilised by blind (passive) approaches, as opposed to active approaches, in the detection of counterfeit photos [5].

These traces can be thought of as the fingerprint of the image source. Protective criteria are not present while using passive approaches. They don't make use of any digital picture pre-image informational allocation. Furthermore, these methods only use the picture function and the supposition that specific image modifications may be realised if the image had been altered.

Their process include analysing the binary data in the image to look for any indications of fabrication. [6].

Passive authentication is further divided into:

1- Forgery dependent Approach - Techniques for identifying forgeries that rely on the sort of fraud applied to a picture, such as splicing and copy-move, are called forgery-dependent identification approaches.

2- forgery independent approach - counterfeit-independent methods identify interferences based on lighting mistakes and artefact traces left over from the resampling process, rather than the sort of counterfeit. [7]

Copy-move Forgery Detection

Because it is so simple to use, this is the most well-known and widely used method of image modification [8].

It involves cutting and pasting certain portions of an original image to a different area of a new image. The dynamic colour and range maintain their compatibility mode with the remaining portion of the image because the merged portion is a component of the same image [9].

A superb example of copy-move forgery is shown in Figure 4.

Tampered Original

Figure 4: Copy- move Forgery. [10]

Image Retouching

This tool, which is widely used for both commercial and artistic purposes, is an extra criterion in image forgery. Retouching techniques are specifically used to enhance or lessen the image's characteristics and quality. Retouching is also done to create a more realistic composite image from the merged photos; this may involve stretching, rotating, or scaling one of the merged images. Figure 5 provides an example of this method. The Iranian military published the contentious photo.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

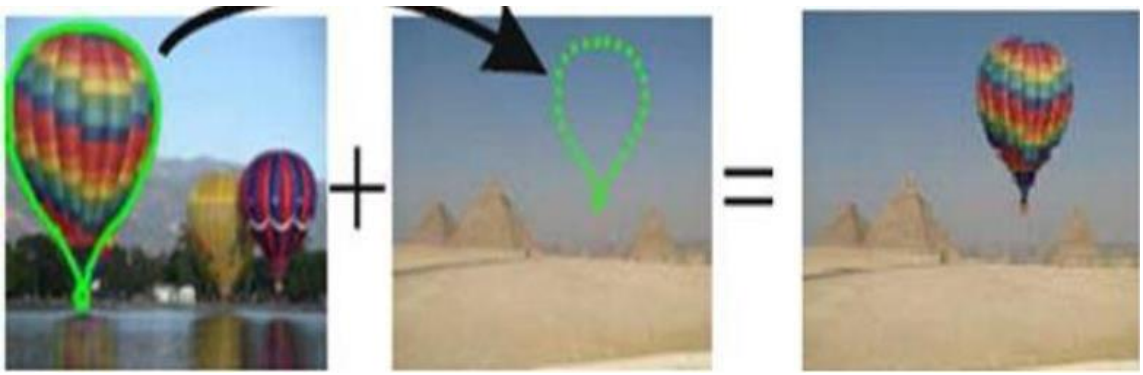
DOI: 10.17148/IJARCCE.2024.13131

Figure 5: Re-sampled image: Launching of Missile weapon by Iranian military

Image Splicing

Image splicing is the process of manipulating one image by merging or compositionally modifying it. When two distinct images are attempted to be combined, the result is typically a fabricated image with a contradicting background.

The process of making a spliced image utilising a source image that is copied and pasted into a target image is illustrated in the image below (Figure 6).



a. Source image b. Target image c. Composite image

Figure 6: Image splicing equation

With widely accessible photo editing software, even an amateur photographer may produce convincing image forgeries of this kind. All that has to be done is manipulate the image by transferring a portion of the source image (a) to the destination image (b). [11] Even novices in the field can perform these kinds of splicing with the least amount of difficulty.

Since most image forgers appear to employ image splicing as their preferred method, it is critical to comprehend how this process is carried out. These kinds of modifications do exhibit visible evidence of manipulation, just like a real print photo would. The photograph is transformed into a virtually authentic replica that may be used for the intended purpose by combining several images into one an article or report.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13131

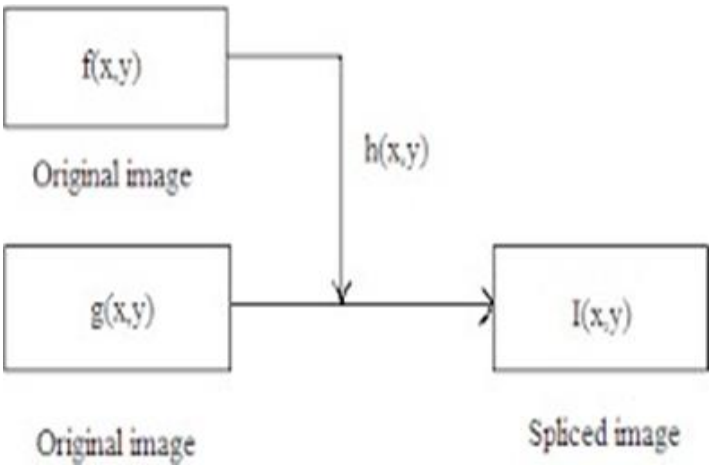


Figure 7 shows an illustration of picture splicing along with the steps needed to finish the procedure. [11]

Figure.7: The steps of image splicing, f(x,y) and g(x,y) are original images, h(x,y) these are a part of f(x,y) which is inserted into g(x,y) that then generates a spliced image I(x,y).

Perhaps f(x,y) and g(x,y) are the same image.

FRAMEWORK OF THE PROPOSED SPLICING DETECTION APPROACH

The framework of the proposed splicing detection approach is illustrated in Fig. 1, which consists of the following four major steps.

1) CNN-BASED LOCAL DESCRIPTOR CONSTRUCTION

The labelled patch samples (spliced or pristine) taken from the training set of images are used to pre-train the proposed CNN model (Fig. 8) in the first phase. In order to create a potent local feature descriptor for splicing detection, the pre-trained CNN focuses on the local statistical artefacts caused by image tampering procedures and develops a hierarchical representation for spliced picture patches (see Sections III-B, III-C, and III-D for more information).

FIGURE 8. The architecture of the proposed two-branch CNN and its sub-network (in black dotted boxes). For the sub-network (CNN-128), ReLU and BN layers are not included for brevity. The size of kernels in each convolutional layer is specified as: (number of output feature maps)×height×width×(number of input feature maps). Note that, either of the two sub-networks can be used to validate the performance of pre-trained CNN model due to the parameters sharing.

2) CNN-BASED FEATURE EXTRACTION

First, the image under examination is divided into blocks the size of patches in this phase. The final convolutional layer's feature maps are then used as an expressive feature for an image block using the pre-trained CNN-based local descriptor (sub-network of the proposed CNN model) to extract features for each block (see Section III-E for details).

3) FEATURE FUSION

To depict the test image, the CNN-based local descriptors for each block are combined into a global one. To be more precise, the recovered local features are combined with the block pooling technique—the suggested feature fusion strategy—to create the final discriminative feature for SVM classification (see Section III-E for details).

4) SVM CLASSIFICATION

The final stage involves training an SVM classifier to perform binary classification, or splicing or authentication, depending on the discriminative feature vector that was created via the feature fusion technique.

III. LITERATURE SURVEY

This comprehensive literature review delves into the analysis of techniques employed in image splicing forgery and explores various methods for detecting such forgeries. The study highlights the importance of checking for consistency in camera characteristics across inconspicuous parts of an image to unveil spliced content. Automatic detection methods utilizing geometric invariants from locally planar irradiance points (LPIPs) for estimating the camera response function

DOI: 10.17148/IJARCCE.2024.13131

(CRF) are discussed, with a focus on distinguishing between authentic and spliced areas [12].Additionally, the review emphasizes the use of Support Vector Machine (SVM)-based classifiers for analyzing image data, resulting in 70% precision and 70% recall [12]. A human visual model proposed by [13] incorporates visual saliency and fixation for automatic detection, although a learning curve is acknowledged for accurate implementation.

Another approach, suggested by [14], involves modeling edge information to detect tampered images. The finite-state Markov chain of the image's Chroma near the edge is considered, and low-dimensional feature vectors extracted from the stationary distribution are utilized for tampering detection. The effectiveness of this algorithm is evaluated using Support Vector Machines.

The paper introduces an algorithm based on Quaternion discrete cosine transform (QDCT) for image splicing detection [15]. SVM classification is applied to images based on the proposed algorithm, which incorporates color information, leading to high classification accuracy.The use of the Barrel and Pincushion based on Polaroid parameter is proposed to identify picture grafting [16].

The paper suggests employing an indifferent system for quantitative measurement of lens spiral twisting in different areas of a photo through line-based alignment. It highlights the potential misinterpretation of lens spiral twisting, especially at various zoom levels, as spliced images due to Picture Joining.Class dependences based on three successive classes and transition probabilities are considered for image splicing detection [17].

Transition probabilities are determined by the progression of the current class to the next two classes, and conditional co-occurrence probabilities are analyzed with a matrix fed into SVM for proper classification. Dimensionality reduction using Principal Component Analysis (PCA) is recommended to address computational complexity and overfitting issues.Motion blur estimation based on image gradients is proposed for detecting irregularities in spliced regions [18].

The motion blur is measured through inconsistent region segmentation in images with a small amount of blur.Detection methods based on Markov features acquired using Discrete Cosine Transform (DCT) domain and Discrete Wavelet Transform (DWT) are suggested [19]. SVM-RFE is used for feature selection, and Local Binary Pattern (LBP) is computed for each pixel, with the resulting LBPed image and partitioned LBPed image based on Slantlet transform used to create a feature vector for SVM classification.

The pioneers of the multi-resolution Weber Law Descriptors (WLD) suggest a forgery detection method using WLD to extract chrominance components [20]. A support vector machine is employed to determine image forgery using a database containing forgery information.A technique proposed by [21] involves using double examples (LBP) along with Discrete Cosine Transform (DCT) to address the increased risk of image manipulation. Chrominance information is isolated under covering squares, and SVM classification is applied, resulting in an increased identification accuracy of up to 97%.Partial Blur Type Consistency, as suggested by [22], involves block-based image partitioning to extract local blur types. Out-of-focus image blocks generate invariant blur regions, and fine splicing localization is utilized to increase region boundary precision for detecting inconsistencies in spliced images.

In summary, the literature survey provides a thorough exploration of various techniques for detecting image splicing forgeries, encompassing methods such as camera characteristics consistency, edge information modeling, quaternion discrete cosine transform, motion blur estimation, and others. The review highlights the importance of applying advanced technologies, including machine learning algorithms such as SVM, for accurate and efficient detection of image splicing forgeries.

TABLE I COMPARISON TABLE

Authors	Year	Method	Dataset	Detection Accuracy (%)
Hsu and Chang.[12], (2007)	2007	CRF& LPIP	own dataset	Precision-70 Recall 70
Qu, Qiu and Huang.[13] ,(2009)	2009	human visual system (HVS)	Columbia	96.33

DOI: 10.17148/IJARCCE.2024.13131

Kong and Box. [14],(2010)	2010	modeling the edge image of chroma component as a finite- state Markov chain & extract low dimensional feature vector from its stationary distribution .	Columbia	93.55
Wei, Gulla and Fu.[15], (2010)	2010	QDCT	DVMM	93.42
Chennamma and Rangarajan.[16], (2011)	2011	consistency of lens radial distortion	Columbia	86
Zhao *et al.*. [17], (2011)	2011	conditional co-occurrence probability matrix (CCPM)	Columbia	Markov 86.8 - CCPM 88.5
Kakar, Sudha and Ser. [18], (2011)	2011	spectral analysis of image gradients	own dataset	93.43
He *et al.*. [19], (2012)	2012	Markov features generated, DCT, DWT, feature selection method SVM-RFE	CASIA 2	95.50
Hussain *et al.*. [20], (2013)	2013	multi-resolution Weber law descriptors (WLD) based image forgery detection	CASIA 1	93.33
Alahmadi *et al.*[21], (2013)	2013	LBP, DCT	CASIA 1	97.7
Bahrami and Kot. [22], (2015)	2015	partial blur type inconsistency	Own dataset	96.3

IV. CONCLUSION

These days, some who are antisocial have moved to creating settings that they can manipulate in whatever way they like by using manipulated or phoney photographs. Because of this dishonest behaviour, photos used in all media platforms (such as newspapers and magazines) must be verified. Even though image splicing has been the subject of many research, identifying image modifications remains a challenging task. Before a precise digital picture authentication procedure is developed, a lot of issues still need to be taken care of, even if image splicing can currently be identified. These concerns include finding the original image to show evidence of manipulation, limitations with image resolution, and the persistence of certain image forms known as (shallow depth of field) the review methods were unable to determine whether these photos were manipulated or real. The literature study offers a number of techniques for detecting picture slicing and expresses optimism for the development of a more intricate yet precise discipline of digital forensic analysis in the future.

REFERENCES

[1]. Sridevi M, Mala C, Sanyam S.(2012). Comparative study of image forgery and copy-move techniques. Adv Intell Soft Comput,166 AISC(VOL. 1),715–23.
[2]. Harouni, M., Rahim, M. S. M., Al-Rodhaan, M., Saba, T., Rehman, A., & Al-Dhelaan, A. (2014). Online Persian/Arabic script classification without contextual information. The Imaging Science Journal, 62(8), 437-448.
[3]. Lin C, Chang S.(1998). Generating Robust Digital Signature for Image / Video Authentication. Multimed Secur Work ACM Multimed '98, Bristol, UK.
[4]. Birajdar GK, Mankar VH.(2013). Digital image forgery detection using passive techniques: A survey Digit Investig,10(3),226–45.
[5]. Name L, Name F, Training O, Training P, Darin C, Training RO, et al.(2014). No Title No Title.Igarss, 2014. 1-5 p.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13131

[6]. Zhou Z, Zhang X.(2010). Image splicing detection based on image quality and analysis of variance. In: Education Technology and Computer (ICETC), 2nd International Conference on, p. V4--242.
[7]. Farid H.(2009). Exposing digital forgeries from JPEG ghosts. IEEE Trans Inf Forensics Secur, 4(1),154–60.
[8]. Redi J a., Taktak W, Dugelay JL.(2011). Digital image forensics: A booklet for beginners. Multimed Tools Appl, 51(1),133–62.
[9]. Bruno A, Informatica I.(2010). Copy-Move Forgery Detection via Texture Description. ACM Work Multimed Forensics, Secur Intell Co-located with ACM Multimed, 59–64.
[10]. Bravo-Solorio S, Nandi AK.(2011). Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. Signal Processing, 91(8),1759–70.
[11]. Kang X, Wei S.(2008). Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics. 2008 Int Conf Comput Sci Softw Eng, 926–30.
[12]. Cortes C, Vapnik V.(1995). Support-Vector Networks,297, 273–97.
[13]. Hsu Y-F, Chang S-F.(2007). Image splicing detection using camera response function consistency and automatic segmentation. In: Multimedia and Expo, IEEE International Conference on, p. 28–31.
[14]. Qu Z, Qiu G, Huang J.(2009). Detect digital image splicing with visual cues. In: International workshop on information hiding, p. 247–61.
[15]. Kong H, Box PO.(2010). IMAGE TAMPERING DETECTION BASED ON STATIONARY DISTRIBUTION OF MARKOV CHAIN National Laboratory of Pattern Recognition. Institute of Automation , Chinese Academy of Sciences, 2101– 4.
[16]. Wei W, Gulla JA, Fu Z.(2010). Advanced Intelligent Computing Theories and Applications. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics) [Internet], 6215(2),380–91.
[17]. Chennamma HR, Rangarajan L.(2011). Image Splicing Detection Using Inherent Lens Radial Distortion. Int J Comput Sci Issues [Internet], 7(6),10.
[18]. Zhao X, Wang S, Li S, Li J.(2011). Passive detection of image splicing using conditional co- occurrence probability matrix. APSIPA ASC 2011-Asia-Pacific Signal Inf Process Assoc Annu Summit Conf 2011.
[19]. Kakar P, Sudha N, Ser W.(2011). Exposing digital image forgeries by detecting discrepancies in motion blur. IEEE Trans Multimed,13(3), 443–52.
[20]. He Z, Lu W, Sun W, Huang J.(2012) Digital image splicing detection based on Markov features in DCT and DWT domain. Pattern Recognit [Internet],45(12),4292–9.
[21]. Hussain M, Muhammad G, Saleh SQ, Mirza AM, Bebis G.(2013). Image forgery detection using multi-resolution Weber local descriptors. Eurocon, 1570–7.
[22]. Alahmadi AA, Hussain M, Aboalsamh H, Muhammad G, Bebis G.(2013). Splicing image forgery detection based on DCT and Local Binary Pattern. 2013 IEEE Glob Conf Signal Inf Process Glob 2013 - Proc, 253–6.

BIOGRAPHY

Dr . Jaynesh Desai, an experienced educator with a Masters Computer Application from SRIMCA College, Veer Narmad South Gujarat University as well running PHD from Bhagwan Mahavir University, Surat. With year of academic experience teaching various computer science subject at UG and PG levels, as Jaynesh pursue diverse interpersonal skills and abilities and a passion for upsurging technologies like PHP, Network Security, Image Forensic, Cyber Security, Python, DJango. He has not only achieved certification in Cyber Security from IBM as well as published and presented in different domain. He has showcase has knowledge and understanding of emerging technologies, and experience in academic make him valuable asset and promising author in the field.