Novel framework for optimized digital forensic for mitigating complex image attacks

Shashidhar T. M.[1], K. B. Ramesh[2]
[1]Department of Electronics and Communication Engineering, AMC Engineering College, India
[2]Department of Electronics and Instrumentation Engineering, RV College of Engineering, India

Article Info

Article history:

Received Oct 9, 2019
Revised Apr 7, 2020
Accepted Apr 19, 2020

Keywords:

Image attacks
Image Forensic
Image forgery
Optimization
Tampering

ABSTRACT

Digital Image Forensic is significantly becoming popular owing to the increasing usage of the images as a media of information propagation. However, owing to the presence of various image editing tools and software, there is also an increasing threat to image content security. Reviewing the existing approaches to identify the traces or artifacts states that there is a large scope of optimization to be implemented to enhance the processing further. Therefore, this paper presents a novel framework that performs cost-effective optimization of digital forensic technique with an idea of accurately localizing the area of tampering as well as offers a capability to mitigate the attacks of various forms. The study outcome shows that the proposed system offers better outcomes in contrast to the existing system to a significant scale to prove that minor novelty in design attributes could induce better improvement with respect to accuracy as well as resilience toward all potential image threats.

Corresponding Author:

Shashidhar T M,
Department of Electronics and Communication Engineering,
AMC Engineering College,
Bengaluru, India.
Email: shashidhartm2014@gmail.com

1. INTRODUCTION

It is now well known that different forms of images, as well as video contents, are frequently utilized for information dissipation as the image files are highly expressive over its visual contents of information as well as they are quite simpler to be used. However, the utilization of various tools that is cost-effective as well as highly friendly user tools it gives rise to different image tampering application. It is also seen that the illegitimate amendment for digital images is increasing. There is a variable usage of the term image forensics based on multiple contexts while they are all used for investigating the genuinity of the digital image content [1]. It is also used for assessing the presence of any form of image tampering practices as well as determining the location of the image corruption [2]. The forensic tools utilized for this purpose targets to facilitate blind assessment. This approach can be considered as an improvement of the existing multimedia security approach with more effectiveness to carry forward the embedded data [3]. Some of the examples of this approach are steganography and image watermarking [4]. This approach uses the concept of digital image processing and uses various degrees of analysis tools in order to extract historical data about the digital image [5]. At present, the conventional implementation of digital image processing is carried out in two significant processes. The first form of image forensics targets to implement a certain type of intrusive technique in order to capture the information related to the image capturing device that encapsulates the digital image as well as to determine all the possibilities of the occupied by the devices. Such a mechanism will be aggregated under the uniform study of devices that performs identification methods [6]. The second mechanism of the forensic image targets to investigate all forms of non-uniformities associated with the statistical information of the natural images irrespective of attempting to perform disclosure of any artifacts resulting from image attacks. In the case of image forensics, the mechanism connected to acquisition as well as tampering methods that could leave traces [7]. The prime target of digital image forensics is to perform exposure to such artifacts by extracting the current information associated with digital image processing. The cumulative outcomes of multimedia security are also supporting this mechanism. In order to offer a better form of the process of image forensic, it is necessary to perform an investigation of the possibility of all connectivity between various approaches of image security practices. The process of digital image processing associated with the forensic practices encounters multiple possibilities of the challenges related to steganography and digital watermarking [8]. The role of digital image forensic offers better supportability of the security policies. The authentication of the digital images is quite a challenging practice to be ascertained as well as is potentially challenging task to offer data integrity too.

Therefore, such an approach is called a passive process, and sometimes it is also called a blind image forensic problem. At present, various approaches are being carried out towards digital image forensic with various forms of schemes and strategies [9]. However, existing approaches do not facilitate better optimization in its process of performing identification of the area that has been subjected to illegitimate corruption by the attacker. The idea of the proposed system is to perform the development of a novel optimized framework that can leverage the performance of the image forensic, thereby facilitating resistivity against potential threats against attacks over the image. The organization of the proposed manuscript is as follows: Section 1 discusses the existing literature where different techniques are discussed for detection schemes used in power transmission lines followed by a discussion of research problems and the proposed solution. Section 2 discusses algorithm implementation towards identifying the location of image tampering, and it is further followed by a discussion of result analysis in section 3. Finally, the conclusive remarks are provided in section 4.

There have been various works that have been carried out towards studying the effectiveness of image forensics [10]. These section further upgrades more research work towards a similar topic. Most recently, the adoption of a slicing-based approach towards the bit planes has been carried out by Rhee [11]. The authors have also used the method for the identification of median filtering. Xiao et al. [12] have developed a machine learning approach of histogram equalization towards improving the captures of surveillance system aiming forensic application. Ma et al. [13] have used a convolution neural network for assisting in image retrieval. Study towards the identification of representation learning can be used for searching a specific form of an image that can be used in image forensic using a convolution neural network, as seen in the work of Han et al. [14]. Reillo et al. [15] have used attribute-based identification of varied signatures of humans by extracting the geometric attributes. The work of Neubert et al. [16] has presented a solution towards resisting forging face shape based attack using a morphing based approach for better biometric security. Guo et al. [17] have carried out an identification of the image based on forged color information using histogram-based as well as an attribute-based encoding mechanism. Bayar and Stamm [18] have facilitated image forensic by developing a model using deep learning and enhanced convolution neural networks. Hao et al. [19] have presented a forensic analysis of the palmprint using a supervised learning algorithm using a dual feature in order to assess the quality of the image. Shan et al. [20] have used a deblocking filtering mechanism for the identification of the traces caused by the usage of median filtering. Singh and Singh [21] have carried out the experiment with respect to the statistically-based approach of the second order for resisting JPEG-based attacks over an image using supervised classifiers. The work of Zeinstra et al. [22] has carried out an anti-forensic based approach for safeguarding facial image. Chen et al. [23] have discussed blind forensic method associated with the image forensics. Kim et al. [24] have presented anti-forensic methods using deep neural networks integrated with convolution neural networks to eliminate the artifacts of filters being used. Dam et al. [25] have developed a three-dimensional mechanism for reconstructing the facial structure based on the standard reflectance model for better comparison scores with a forensic sample. Pun et al. [26] have presented an image hashing approach for aligning images in order to identify any form of object detection. Korus and Huang [27] have carried out localization of the tampering event over the image using a multi-scale analysis where the authors have used Markov fields. Conotter et al. [28] have used a linear filtering approach for identifying the series of various functions that lead to attacks on the image over JPEG compression. Sarreshtedari and Akhaee [29] have used a channel coding approach for protecting any possibility of image tampering. Fan et al. [30] have presented work towards the removal of traces against digital filters, also focusing on enhancing the quality of the image. Therefore, there are various approaches to promoting the performance of image forensic. The next section outlines about problems associated with it.

The identified problems associated with the existing studies are as follows:

- Adoption of machine learning (especially neural network) offers good accuracy but at the cost of immense computational complexity.
- Majority of the existing approach are carried out on the basis of pixel-based approach which is not only time consuming but also memory dependent.
- At present, no significant optimization work has been carried out towards the performance of image forensics.
- Existing solutions are quite specific to particular form of image attack and hence they fail to address potential solution towards complex image-attacks.

Hence, the statement of problem can be represented as "Developing a cost effective computational framework that leverages more performance optimization targeting to resist maximum potential threats over image forensics". The next part of the study highlights a solution to address this problem.

The current work is an extension of our prior framework towards artifacts removal [31], while this part of the study introduces a novel analytical framework that is capable of optimizing the performance of the framework towards resisting potential threats over images. The plan for the adoption of the proposed methodology is discussed in Figure 1. The implementation of the proposed study is carried out considering the fact those regions within an image that have been subjected to corruption are accurately identified. The study considers a case study of image-based attack in such a way that irrespective of any form of attack, the performance towards capturing the location of temperament. The underlying concept of the proposed system is that it attacker always leaves its traces of attack in the form of artifacts that are required to be identified as a part of the mitigation process.

According to Figure 1, the proposed system takes the input of the image, which has already been tampered in its location called a forged image. The next part of the algorithm is associated with the process of block partitioning, which is about representing the complete image with blocks of different dimensions followed by partitioning it. The third block is meant for performing extraction of significant attributes so that various forms of artifacts owing to the process of the image capturing or tampering are considered. The extracted attribute is finally subjected to a binary classification process to speed up the process of identifying the region of attack and typical area. Interestingly, the proposed system is capable of identifying any form of artifacts that are illegitimatey incorporated by an adversary while launching an attack. The proposed system performs the extraction of the attributes based on statistically descriptive parameters for higher accuracy and speeding up the process. This process offers a further better representation of the attributes for the better classification process. Finally, the artifacts associated with the complex attack over the image are identified in the proposed system, which further leads to the process of performance analysis. The next part of the discussion is about algorithm implementation.

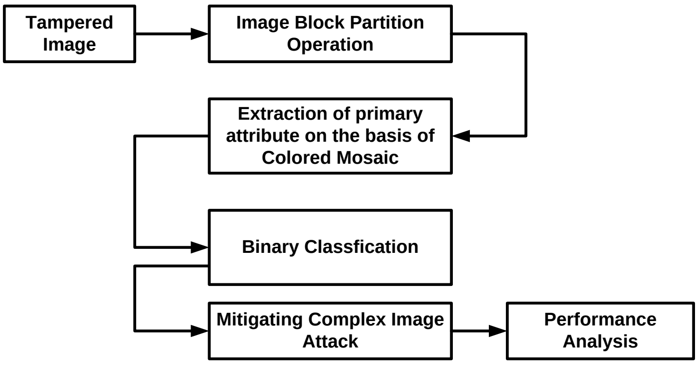

Tampered Image
Image Block Partition Operation
Extraction of primary attribute on the basis of Colored Mosaic
Binary Classfication
Mitigating Complex Image Attack
Performance Analysis

Figure 1. Proposed analytical framework

2. ALGORITHM IMPLEMENTATION

The core purpose of the proposed algorithm design is to ensure that the processing is carried out in such a way that there is a better solution toward resisting the form of the attack over the image, especially when the attack is quite of complex nature. The complete assessment and investigation of the image are carried out considering 2000 models that are characterized by colored high definition quality and is captured from high definition image capturing device. The complete process of implementation is carried out considering 4 stages of implementation in order to mitigate complex image attack. The discussion of the algorithms used in this part of the proposed system is briefed below:

2.1. Algorihm for image block partition operation

This is the first algorithm of implementation where the logic is to extract all essential information that will assist in formulating essential attributes for the given image on the basis of the constructed blocks. This attributes are used for identifying the core region of image intrusion over the tampered image. The algorithm takes the input of original image, convert them in matrix, and consider all the row fields (h_f) and column fields (v_f) which after processing yields an outcome of B_p (block partitioned image). The steps of the algorithm are as follows:

```
Algorithm for Imeg Block Partition
Input: $h_f/v_f$ (horizontal and vertical field)
Output: $B_p$ (block partitioned image)
Start
1. For i=1:$x_{max}$,              where $x_{max}$=[$h_f$ $v_f$]
2.     Read elem ($x_{max}$)
3.     $B_p$→obtain block_elem
4. End
End
```

The discussions of the algorithmic steps are as follows: The algorithm targets to exract significant attribute so that essential source identificational traits of the given image are analyzed more closely. This step will assist in later part of operation in order to act as a baseline attributes to distinguise the original region and tampred region of the given image. For effective analysis, the proposed study considers multiple dimension of the block size in order to create a test-case. The algorithm reads all the elements in each field (Line-1) and stores the cell-based information and not pixel-based informaion (Line-2). All the cell-based information are then grouped in the form of blocks that are now partitioned and now stored in another matrix called as B_p or partitioned block elements. The advantage of this algoritm is that identification time of the corrupted region will be faster as the identification process is carried out not on the basis of the pixels but on the basis of the blocks, which is the first step towards optimization.

2.2. Algorithm for extraction of primary attribute on the basis of colored mosaic

This is the second part of implementation that focuses on extracting the final attributes based on which the final differentiation for original and tampered region will be carried out. The algorithm takes the input of actual scope of the blocks obtained form the prior algorithm and yields an outcome of final attributes after performing processing on the top of it. The target is to finalize the attributes. The significant steps of the algorithm implementation are as follows:

```
Algorithm for Extraction of primary attribute on the basis of Colored Mosaic
Input: $b_1/b_2$ (lower and higher number of blocks)
Output: $F_{att}$ (Final Attributes)
Start
1. For i: $b_1$:$b_2$
2.     extract $g_c$
3.     Apply bilear kernel
4.     $P_{att}$→[$E_{prob}$, β, d], $F_{att}$→($P_{att}$, β, card(b))      //final feauture
5.     α→f($F_{att}$, c)
6.     Compute α, $F_{att}$, c
7.     Compute γ and E
8.     Extract $F_{att}$($B_m$, c)
End
```

The discussions of the algorithmic steps are as follows: The complete algorithm is cdesigned on the basis of possibilities of artifacts as the result of any form of extrinsic problem while capturing the image from image capturing device e.g. camera. In order to execute this algorithm, there are various parameters that plays a significant role in processing e.g. cardinality of the attributes being extracted in the form of block card(b), filters used in mosaic form *β*, probability of error E_{prob}, primary attribute Patt in the form of variance value of obtained along with the pixels that are interpolated. The proposed study considers the complete scope of the block obtained from prior algorithm where b_1 and b_2 represents minimum and maximum size of block (Line-1). The next step is to apply bilinear kernel in order to construct a predictor (Line-2). The next step of the algorithm will be to construct a matrix for primary attribute P_{att} and final attribute F_{att} (Line-3). The formulation of the primary attribute is carried out using probability of error Eprob, filters used in mosaic *β*, and dimensions *d* (Line-4) while the final attribute F_{att} is computed using obtained primary attribute in prior step, filters of mosaic *β*, and cardinality of dimension of blocks (Lme-4). The next step is about obtaining maximum a posteriori *α* by applying a function *f*(x) with an input arguments of final attributed obtained Fatt and statistical constant *c* (Line-5). Basically, the statistical constant c is calculated with respect to mean and standard deviation. The study finally stores the obtained value *α* in discrete matrix and other associated parameters (Line-6). Finally, the algorithm computes transition state γ and cumulative error E (Line-7) followed by updating of the final attributes F_{att} (Line-8). Basically, this step of the algorithm processing is carried out on the basis that maximum likelihood function that generates two states of transition. The algorithm is capable of assessing various form sof errors and artifacts that are explored in different levels and obtains its statistical attributes in order to perform computation of any possibility of tamperment of the image and it can do it without any predefined information of forgery. The implementation of this algorithm also exhibits that a better form of optimizing charecteristics are obtained that could have even the slightest possibility of tamepering the image. The positional information of the forged region for a given image is not so much challenging to find owing to the adoption of descriptive statistical approach which offered increasing accuracy in its performance.

2.3. Algorithm for binary classfication

This prime purpose of this algorithm is to assists in discretizing the regions using binary classification approach for speeding up the process of identification of the tampered region. The algorithm takes the input of scope of blocks and final attributes that after processing results in formation of a binary classified image. The steps of the algorthms are as follows:

```
Algorithm for Binary Classification
Input: $b_1/b_2$ (scope of blocks), $f_{att}$ (final attributes)
Output: a (binarized classified image)
Start
1. For i=$b_1$:$b_2$
2.     h→$f_1$($F_{att}$) and $c_o$=0
3.     For i=1: length (h)
4.         If h(i)>co
5.           a(i)=1
6.     End
7. End
End
```

The discussions of the steps of the algorithm are as follows: the implementation of the algorithm is carried out in such a way that it can perform classification on binary basis for identifiying all the tampered regions as well as non-tampered regions for the given image. For the entire minimum and maximum scope of block (b_1 b_2), the algorithm applies a function f_1(x) where the statistical information about the final attributes F_{att} is computed with respective to all the blocks corresponding to an image (Line-2). This step also considers cut-off value c_o initialized to zero. For all the size of the matrix h that holds all the statistical attributes of the blocks corresponding with the transition state. For all the size of h (Line-3), if the elements size is found to be more than cut-off value c_o than they are assigned 1 where 0 and 1 represents for black and white respectively. By doing this step, it will mean that size of the matrix h with its respective elements can have various value, but shortlisting will be done as per the logic specified in Line-4 and Line-5. This process is quite faster and significantly assists in optiminizing the processing time for classification of the regions which is subjected to assessment for tamperment. Using lesser number of resources, the adoption of binary classification assists in further steps of operation which is about correct identification and mitigation of the sophisticated image attacks.

2.4. Algorithm for mitigating complex image attack

The core purpose of this algorithm is to ensure offer the solution towards the regions inflicted with the image attacks. While the main contribution of the proposed algorithm will be to rectify the ultimate mechanism for facilitating in yielding the regions tampered. The algorithm takes the input of scope of the image block as well as regions that are obtained from prior algorithm and that after processing yields an outcome of image that is corrected one I. The steps involved in the proposed algorithm are as follows:

```
Algorithm for Mitigating Complex Image Attack
Input: b1/b2 (scope of image blocks), reg (identified regions of attack)
Output: I ()
Start
1. For i=$b_1$:$b_2$
2.    apply $f_2$($reg_1$)
3.    Extract ($reg_2$)→$f_2$($reg_1$)→Img(bin)
4.    If region($reg_2$)>region(~$reg_2$)
5.        $reg_2$=~$reg_2$
6.    End
7.    I=$f_3$($reg_2$)
8. End
End
```

The discussions of the steps involved in the algorithm are as follows: the algorithm considers the average of transition state s_1 with a condition that its value should be more than the cut-off value of c_o=0. The input towards this function is basically a corrupted image by adversary that yields a rectified image after processing as well as identification of the tampered region *I*. The precision of the image is increased initially and is classified with respect to highest value of 255. Because of this operation, the proposed system permits identification of multiple positions within an input image where the determination of the blocks of the boundary. For all the scope of image blocks (Line-1), the proposed system applies an explicit function f_2(x) which is responsible for filling the insignificant white portion of an image after the binary classification is over (Line-2). This step is carried out in order to prevent a form of outliers and its possibilities. The algorithm extracts filled regions and further subtracts the filled regions with a reference matrix while a logic of binary approach is filled using concatenation operation. The implementation also constructs a concatenated matrix in the form of repositing all the false positives value found in tampered regions that are subjected for rectification that is carried out using morphological operation. The outcome matrix is re-checked for presence of any holes (Line-3) as further optimizing the process of identification and solution together. Therefore, if any holes are found, it will be instantly filled up and the information is stored in the form of explicit region reg_2 (Line-4). The proposed study than formulation a conditional statement to assess if the amount of the region under reg_2 is more than that of $\sim reg_2$ (Line-4/5) and in such case, the simpler substitution operation will be carried out. This matrix will will represent a rectified image and hence it can be treated as an error free image without any possibilities of false positive within that binary version of an image (Line-5). The next operation is linked with further mechanizing for the purpose of obtaining the original tampered regions as the ultimate yield. In order to work in this direction, the proposed system constructs a binary mask by performing concatenation operation of the binary objects present in the stored matrix file. The proposed system obtains the image with double precision and subjects it to an unsigned integer in order to generate the mask and the determination of the original tampered region. One of the interesting facts of this algorithm is that it is capable of performing decision towards rectifying the regions intruded by adversary and this operation is completely automated and is independent of any interactive operation of human. In order to perform a validation of this part of the proposed system, the algorithm makes use of the ground truth information. This operation will permit the users for choosing the tampered regions with an aid of manual selection and then it follows the operation of re-computing the average values for both the matrixes respectively. This form of assessment is carried out in order to evaluate the uniformity of the numerical values. Finally, a concatenation operation is carried out using an explicit function f_3(x) which leads to generation of the final rectified image I (Line-7). The proposed system has identified these non-uniformities with respect to static as well as dynamic objects for better purpose. One of the interesting part of implementation of proposed algorithm is that it offers similar performance if the intrusion with the shape of tamperment is carried out over any regions. However, this operation is carried out in more spontaneous manner and is independent of much number of computational dependencies towards exploring the artifacts owing to the multiple form of malicious activities over any form of images.

3. RESULT ANALYSIS

The assessment of the proposed system is carried out in experimental approach where multiple forms of images and different variants of the images are used for analysis. The discussion of the outcomes obtained is presented with respect to (a) visual representation and (b) numerical representation. The analysis has been carried out by constructing more than 2000 high definition images in the form of image dataset while these dataset has been constructed on the basis of captures carried out by DSLR camera. The resolution of the image is 24 megapixel with smaller and bigger dimension of the image dataset. In order to obtain better evidential feature of the analysis, the proposed dataset consist of two directories viz. (a) tampered image and (b) ground truth image.

From the display of Figure 2, it can be seen that the orginal image has been tampered with the different image thereby generating a forged image. During the analysis, it has been seen that forged area could be possibly symmetrical or non-symmetrical with possibilities of different regional spaces. The analysis has been carried out with different dimension of the regions of the forged image in order to investigate various possibilities of image forensic. Once the forged image is considered as an input, the proposed system performs multiple scale of blocking operation exhibited in Figure 2. The user is also facilitied with varied options for using value of partitioning process. The concept derived here is that detection process is improved via blocking operation and it also increases the possibility of exploring the significant regions too. The selection of the values of the block partitioning process is selected on the basis of imperceptibility of the forged image. Hence, smaller values of blocking are deployed only in the cases that demands better imperceptibility while increased value of the blocking is demanded when there is a need of higher level of difficulty for the input forged image see Figure 3.

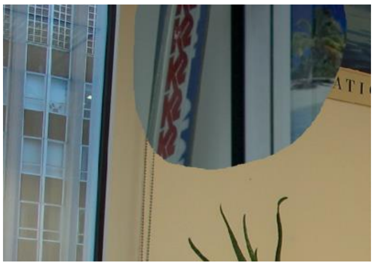
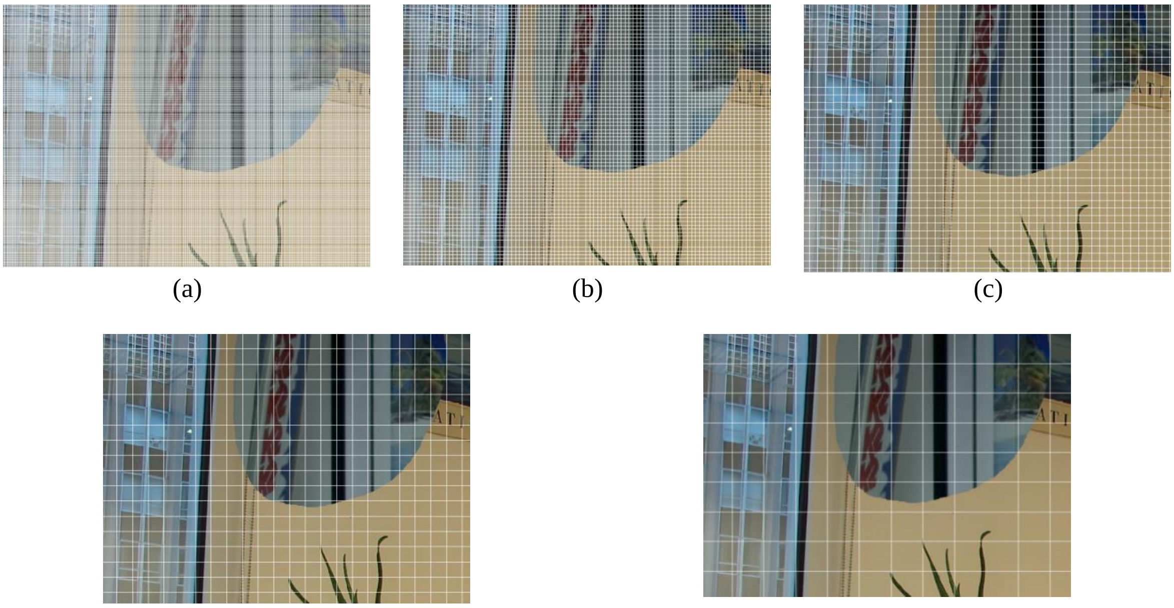


Figure 2. Tampered image

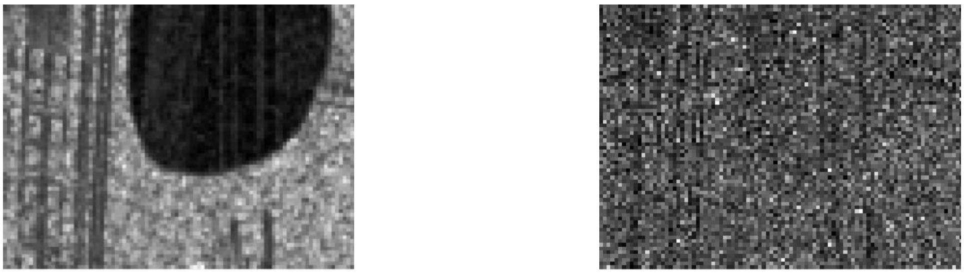


(a) (b) (c)

(d) (e)

Figure 3. Variants of partitioning image block:
(a) 4x4, (b) 8x8, (c) 16X16, (d) 32x32, and (e) 64x64

Once the selected block is finalized, than the next process will be to perform extraction of all the significant attributes. Adoption of the statistical approach further improves the accuracy factor only in less value of iteration as well as it also positively affect the computational efficiency. The adoption of such statistical process results in faster processing too. Figure 4 highlights the mean value of the image while standard deviation as an outcome of the statistical operation. The study outcome of the proposed system shows that after the colored mosiaic is extracted then the identification of the traces can be carried out in simpler fashion shown in Figure 5.



(a) (b)

Figure 4. Process of extracting significant attributes (a) Mu image and (b) Sigma image

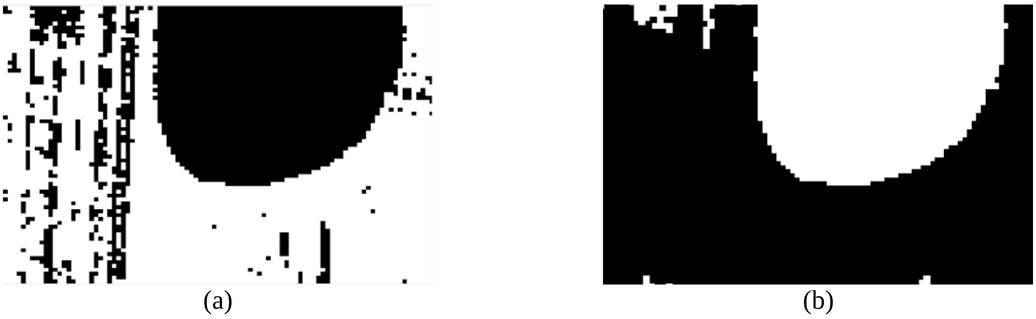


Figure 5. Analysis of (a) classification and (b) rectification

Therefore, from the visual outcome highlighted in Figure 6, it can be seen that proposed system offers significantly better display of the region that are actually tampered. Apart from this process of extracting the image blocks that is equivalent to the transition state is finally used for statistical information associated with the tampered image. Hence, a better imperceptibilty factor is decoded in the proposed system where the correct and reliable identification is carried out using simple techniques. Apart from this, the outcome of the proposed study is compared with the existing approaches related to localization-based [32] and feature-extraction based [33]. Using the same dataset, the comparative analysis is carried out. The outcome of comparative analysis is shown in Figure 7.

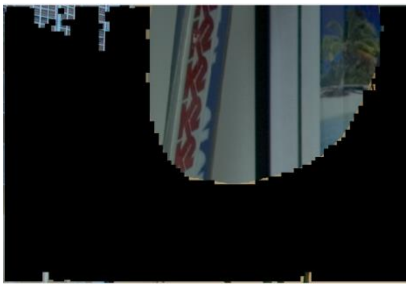


Figure 6. Identification of tampered region

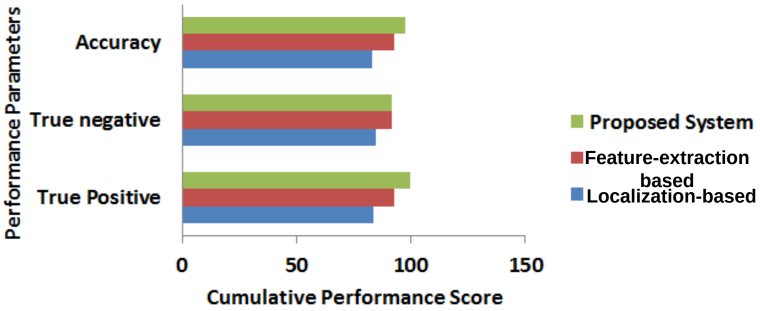


Figure 7. Comparative analysis

The outcome shows that proposed system does not take more than 0.75 seconds to carry out the extraction of the significant features that contributes towards higher accuracy of 99% with lower outlier rate of 16.45%, which is comparatively better than existing system. The prime reason behind this is that localization-based approach [32] performs identification of the traces equivalent to the proposed system but it does so with more number of the attributes associated with it and hence proposed system offers better optimization performance. The feature-extraction based approach [33] make use of random theory along with usage of thresholding however that do it recursively that significantly degrades the accuracy level in contrast to proposed system.

4. CONCLUSION

This paper has presented a mechanism for promoting image forensic performance where the idea is two-fold viz. (a) capture information about the location of tampering and (b) improving the performing using optimization. The contribution of the proposed system is as follows: (a) the proposed model is developed without using any sophisticated security (conventional) technique, nor any recursive approaches are used, (b) a significant level of faster processing time is obtained along with performance (accuracy) improvement.

REFERENCES

[1] G. Cao, et al., "Forensic detection of median filtering in digital images," in *2010 IEEE International Conference on Multimedia and Expo*, pp. 89-94, 2010.

[2] X. Feng, I. J. Cox, and G. Doerr, "Normalized energy density-based forensic detection of resampled images," *IEEE Transactions on Multimedia*, vol. 14, no. 3, pp. 536-545, 2012.

[3] M. F. Breeuwsma, "Forensic imaging of embedded systems using JTAG (boundary-scan)," *Digital investigation* 3, no. 1, pp. 32-42, 2006.

[4] A. Cheddad, et al., "Digital image steganography: Survey and analysis of current methods," *Signal processing*, vol. 90, no. 3, pp. 727-752, 2010.

[5] T. Gloe and R. Böhme, "The Dresden Image Database for benchmarking digital image forensics," in *Proceedings of the 2010 ACM Symposium on Applied Computing*, no. 2-4, pp. 1584-1590, 2010.

[6] T. Van Lanh, et al., "A Survey on Digital Camera Image Forensic Methods," in *2007 IEEE International Conference on Multimedia and Expo*, Beijing, pp. 16-19, 2007.

[7] D. T. Dang-Nguyen, C et al., "Raise: A raw images dataset for digital image forensics," in *Proceedings of the 6th ACM Multimedia Systems Conference*, pp. 219-224. ACM, 2015.

[8] F. Y. Shih, *Digital watermarking and steganography: fundamentals and techniques*. CRC press, 2017.

[9] A. Swaminathan, M. Wu, and K. J. Ray Liu, "Digital image forensics via intrinsic fingerprints," *IEEE transactions on information forensics and security*, vol. 3, no. 1, pp. 101-117, 2008.

[10] T. M. Shashidhar and K. B. Ramesh, "Reviewing the effectivity factor in existing techniques of image forensics," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 6, pp. 3558-3569, 2017.

[11] K. H. Rhee, "Forensic Detection Using Bit-Planes Slicing of Median Filtering Image," *IEEE Access*, vol. 7, pp. 92586-92597, 2019.

[12] J. Xiao, S. Li and Q. Xu, "Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation," *IEEE Access*, vol. 7, pp. 55432-55442, 2019.

[13] Z. Ma, et al., "Shoe-Print Image Retrieval with Multi-Part Weighted CNN," *IEEE Access*, vol. 7, pp. 59728-59736, 2019.

[14] H. Han, J. Li, A. K. Jain, S. Shan and X. Chen, "Tattoo Image Search at Scale: Joint Detection and Compact Representation Learning," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 41, no. 10, pp. 2333-2348, 2019.

[15] R. Sanchez-Reillo, J. Liu-Jimenez and R. Blanco-Gonzalo, "Forensic Validation of Biometrics Using Dynamic Handwritten Signatures," *IEEE Access*, vol. 6, pp. 34149-34157, 2018.

[16] T. Neubert, A. Makrushin, M. Hildebrandt, C. Kraetzer and J. Dittmann, "Extended StirTrace benchmarking of biometric and forensic qualities of morphed face images," *IET Biometrics*, vol. 7, no. 4, pp. 325-332, 7 2018.

[17] Y. Guo, X. Cao, W. Zhang and R. Wang, "Fake Colorized Image Detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 1932-1944, Aug. 2018.

[18] B. Bayar and M. C. Stamm, "Constrained Convolutional Neural Networks: A New Approach towards General Purpose Image Manipulation Detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2691-2706, Nov. 2018.

[19] F. Hao, L. Yang, G. Yang, N. Liu and Z. Liu, "RFPIQM: Ridge-Based Forensic Palmprint Image Quality Measurement," *IEEE Access*, vol. 6, pp. 62076-62088, 2018.

[20] W. Shan, Y. Yi, J. Qiu and A. Yin, "Robust Median Filtering Forensics Using Image Deblocking and Filtered Residual Fusion," *IEEE Access*, vol. 7, pp. 17174-17183, 2019.

[21] G. Singh and K. Singh, "Counter JPEG Anti-Forensic Approach Based on the Second-Order Statistical Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1194-1209, May 2019.

[22] C. G. Zeinstra, R. N. J. Veldhuis, L. J. Spreeuwers, A. C. C. Ruifrok and D. Meuwly, "ForenFace: a unique annotated forensic facial image dataset and toolset," *IET Biometrics*, vol. 6, no. 6, pp. 487-494, 2017.

[23] C. Chen, J. Ni, Z. Shen and Y. Q. Shi, "Blind Forensics of Successive Geometric Transformations in Digital Images Using Spectral Method: Theory and Applications," *IEEE Transactions on Image Processing*, vol. 26, no. 6, pp. 2811-2824, June 2017.

[24] D. Kim, H. Jang, S. Mun, S. Choi and H. Lee, "Median Filtered Image Restoration and Anti-Forensics Using Adversarial Networks," *IEEE Signal Processing Letters*, vol. 25, no. 2, pp. 278-282, Feb. 2018.

[25] C. van Dam, R. Veldhuis and L. Spreeuwers, "Face reconstruction from image sequences for forensic face comparison," in *IET Biometrics*, vol. 5, no. 2, pp. 140-146, 2016.

[26] C. Pun, C. Yan and X. Yuan, "Image Alignment-Based Multi-Region Matching for Object-Level Tampering Detection," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 377-391, Feb. 2017.

[27] P. Korus and J. Huang, “Multi-Scale Fusion for Improved Localization of Malicious Tampering in Digital Images,” *IEEE Transactions on Image Processing*, vol. 25, no. 3, pp. 1312-1326, March 2016.

[28] V. Conotter, P. Comesaña and F. Pérez-González, “Forensic Detection of Processing Operator Chains: Recovering the History of Filtered JPEG Images,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2257-2269, Nov. 2015.

[29] S. Sarreshtedari and M. A. Akhaee, “A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery,” *IEEE Transactions on Image Processing*, vol. 24, no. 7, pp. 2266-2277, July 2015.

[30] W. Fan, K. Wang, F. Cayre and Z. Xiong, “Median Filtered Image Quality Enhancement and Anti-Forensics via Variational Deconvolution,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 1076-1091, May 2015.

[31] T. M. Shashidhar and K. B. Ramesh, “An efficient computational approach to balance the trade-off between image forensics and perceptual image quality,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 3474-3479, 2019.

[32] P. Ferrara, T. Bianchi, A. De Rosa, and A. Piva, “Image Forgery Localization via Fine-Grained Analysis of CFA Artifacts,” *IEEE transactions on information forensics and security*, vol. 7, no. 5, October 2012.

[33] J. G. Han, T. H. Park, Y. H. Moon, K. Eom, “Efficient Markov feature extraction method for image splicing detection using maximization and threshold expansion,” *Journal of Electronic Imaging*, vol. 25, no. 2, 2016.

BIOGRAPHIES OF AUTHORS

Shashidhar T. M. is a research scholar at Visvesvaraya Technological University Belagavi, Karnataka, India. Currently pursuing PhD under RVCE (VTU), Karnataka, India. His teaching experience is around 11 years. Hisresearch area is Signal Processing. He has completed hisM. Tech (Digital electronics and communication system) from PESIT, Bengaluru, Karnataka, India. Alsocompleted B.E. (Electronics and communication), from SJMIT, Chiradurga, Karnataka, India.

Dr. K. B. Ramesh is an associate professor and Head of Department of Electronics and Instrumentation Engg. R V College of Engineering, Bengaluru, Karnataka, India. He has completed PhD in Computer Science and Engineering from Kuvempu University. He has around twenty-threeyears (23) of teaching experience in E&I Engg. His major research area is in Computer Science and Engineering and minorresearch area is in Biomedical Engineering/ Bioinformatics.