Block and Fuzzy Techniques Based Forensic Tool for Detection and Classification of Image Forgery

Mohammad Farukh Hashmi† and Avinash G. Keskar*

Abstract – In today’s era of advanced technological developments, the threats to the authenticity and integrity of digital images, in a nutshell, the threats to the Image Forensics Research communities have also increased proportionately. This happened as even for the ‘non-expert’ forgers, the availability of image processing tools has become a cakewalk. This image forgery poses a great problem for judicial authorities in any context of trade and commerce. Block matching based image cloning detection system is widely researched over the last 2-3 decades but this was discouraged by higher computational complexity and more time requirement at the algorithm level. Thus, for reducing time need, various dimension reduction techniques have been employed. Since a single technique cannot cope up with all the transformations like addition of noise, blurring, intensity variation, etc. we employ multiple techniques to a single image. In this paper, we have used Fuzzy logic approach for decision making and getting a global response of all the techniques, since their individual outputs depend on various parameters. Experimental results have given enthusiastic elicitations as regards various transformations to the digital image. Hence this paper proposes Fuzzy based cloning detection and classification system. Experimental results have shown that our detection system achieves classification accuracy of 94.12%. Detection accuracy (DAR) while in case of 81×81 sized copied portion the maximum accuracy achieved is 99.17% as regards subjection to transformations like Blurring, Intensity Variation and Gaussian Noise Addition.

Keywords: Image forensics, Cloning detection, Fuzzy logic, Blurring, Intensity variation, Gaussian noise addition

1. Introduction

With the technological advancements digital cameras and high resolution providing mobile phone have become necessities of today’s generation. All the events are made evident by means of photographs and hence authenticity of these digital images is of great importance as several legislative, technical as well as newscast organizations are dependent on these evidences, proofs and digital testimonies. The ease of availability of image editing software has made the situation much more challenging as manipulation of images has become a very novice task for an imitator. Identification and verification of alterations performed on images is essential to keep a check on mortification, legal implications, falsification of documents and other undesirable transformations. [1]

Digital image tampering can be classified into two sections: Cloning and composition. In cloning based image tampering, a small copied portion of image is pasted on the same image at some other location. This type of attack is also known as “copy-cover forgery” because the intention of the forger incorporating this technique is to hide some information of image with the content available in same image. Composition based image tampering comprises of utilizing two or more images to tamper a third image. These types of alterations are also known as “image creation based forgery” [2].

Digital Image forgery detection techniques can be classified into two categories: First one is active forgery detection technique which involves watermarking and digital signature based approach to detect possible forgery in the given image. The main disadvantage of this scheme is that it requires additional information to be added in the image at the time of capturing. Since the camera, we posses, does not own this property, hence this technique is not applicable in general.

Second is blind detection technique which falls under passive forgery detection, this technique is based on the characteristics available in the image to find the alteration performed. Though blind detection technique is complex but due to its versatility it has found much interest of researchers in the last decade. An example of copy-move forgery is shown in Fig. 1.

Generally, the image forensic research has put up all its strength in detecting footprints by a single image forgery detection tool. As already mentioned, whenever an image forgery is done, it is done with more than one image processing tool and thus, our task of detection of forgery is
obtained, along with its uncertainties, and helps in prolific gives accurate results by assimilating all the responses which generally deals with such real-time scenarios and significance. This problem is solved by Fuzzy Theory, enthusiastic results, both in terms of accuracy and mere OR-ing of the individual outputs does not give upon the complexity of the image under investigation, a image processing techniques to detect forgery depends individual answers obtained. Since the working of these image processing techniques to detect forgery depends upon the complexity of the image under investigation, a mere OR-ing of the individual outputs does not give enthusiastic results, both in terms of accuracy and significance. This problem is solved by Fuzzy Theory, which generally deals with such real-time scenarios and gives accurate results by assimilating all the responses obtained, along with its uncertainties, and helps in prolific detection of image forgery cases. For understanding the proposed methodology, one is ought to know the elementary fuzzy theory and its entities.

The rest of the paper is organized as follows:-Section 2 gives a brief outline of the related works in association with the researches in this field. Section 3 explains the basic guidelines to be understood for appreciating the methodologies of functioning of Fuzzy logic. Section 4 explains the proposed methodology and algorithm flow. This also explains the working mechanism of the Fuzzy based Classifier. Section 5 concludes the paper by displaying the results and corresponding illustrations.

2. Related Work

Many researchers have found interest in detection of digital image forgery through blind detection technique. Considering the recent related works in this area, we will firstly, have a brief outlook on the survey papers. Qazi, Tanzeela et al. [3] presented in the survey of basic blind image detection techniques, in which they discussed techniques regarding the exposure of image forgeries and concept like splicing and retouching. Al-Qershi et al. [4] discussed the similar scenario of image forgery detection techniques. He has also explained various types of forgery detection techniques in his survey. Mahdian, Babak et al. [5] elaborated concordant with bibliography of blind image detection techniques in image forensics. They tried, using the image function plainly, strived to detect image tampering.

Regarding the idea of the crux of our algorithm, i.e., the fuzzy logic and classifier based techniques; we got motivation from Cozzolino, Davide et al. [6], in which he tested several combining rules working at measurement as well as abstract levels, detecting the type of forgery. Barni, Mauro et al. [7] explained the intricate issues regarding the applicability of fuzzy logic for prolific and tenable detection and classification of forgery.

Christlein, Vincent et al. [8] explained in an Evaluation of popular copy move forgery detection approaches, tried to undergo a rigidified analysis dependent on per-image and per-pixel basis to detect copy-move forgery. Similar attempts were made by Ketenci, Seniha et al. [9] with imparting more resistance to attacks like Gaussian blurring and jpeg compression. Li, Guohui et al. [10] presented in a sorted neighborhood approach for detecting duplicated regions in image forensics based on DWT and SVD. On the same lines, Wang, Yang et al. [11] presented a cloning task using DWT in the Wavelet based image duplication forgery detection.

Detection of image tempering was first analyzed by Fridrich et al. [12], they have proposed DCT based block matching algorithm which is proven to improve the computational efficiency of exhaustive search algorithm. Later Popescu et al. [13] explained similar method which utilizes PCA based dimension reduction method instead of DCT to reduce the dimensionality of the feature vector and hence to reduce the computational complexity as well as computational time. His method has been proven to be better than the prior DCT based algorithm experimentally. Wu Qiong et al. [14] proposed DCT-SVD based method in which the image given is first undergone through two-level DWT. The resulting image is of ¼ dimension of the raw image, which is then passed through SVD based dimension reduction and lexicographic sorting to find the possible match. The aforementioned techniques were aimed at reduction of the computational complexity but the authors have not considered the post-forgery alteration on the image. The easy availability of the editing software has made it quite easy for a forger to conceal the alteration performed through several post processing algorithms including intensity variation, blurring, rotation and noise addition.

In this regard Huang et al. [15] has proposed improved DCT based image forgery detection system which is capable of to cope up with distortions like blurring, JPEG compression and additive white Gaussian noise.

Cao et al. [16] presented circular block based multiple copy-move forgery detection system, their technique is robust to blurring and noise addition as well as it can detect multiple copied portions in the same image.

To enhance the efficiency of DWT based approach, Muhammad et al. [17] proposed undecimated dyadic wavelet transform (DyWT) based blind copy move forgery
detection system. DyWT is scale invariant and hence it is robust to attack like scaling. Many other researchers have also worked on copy move forgery detection techniques to improve the computational efficiency, flexibility and robustness of the algorithm including Akbarpour et al. [18], Lynch et al. [19], Zhao et al. [20], Li et al. [21] and Ketenci et al [22]. Hashmi et al. [30] has been presented comprehensive technique for detection of any type of image forgery. Various feature extraction techniques like DCT, LBP, Curvelet transform, Gabor filter etc. are used to represent the image in transformed domain and HMM and SVM are the machine learning methods used to classify the image to identify the authenticity and classify of images.

The above mentioned schemes are useful in improving efficiency and robustness of the system but due to the uncertainty of the field a single method cannot confront all the aforementioned distortions. Additionally, in real time a tampered image may be outcome of more than one image processing tool, As a result, a robust tamper detection technique necessitates that a number of detection techniques should be applied on the image to handle different alterations. The above discussion led to the need of an algorithm which not only manages the instability presented by detection algorithms but also combines the result of different algorithms into a single channel. Hence this paper proposes a “fuzzy logic based approach” to deal with the inaccuracy of different algorithms and to provide a single solution based on the cumulative and cascaded elicitations.

We evaluate the performance forgery detection system with DWT, DCT, PCA, DWT-DCT, DWT-DCT-SVD and DFT based dimension reduction technique and build a fuzzy based classification system to categorize the distortions applied on the image.

3. Elementary Guidelines of Fuzzy Theory

“Fuzzy” theory is not a new concept in our scientific community as far as its foundations are concerned. Its description is found in some notes of Aristotle, as far as 2500 years back, but without any type of concept concretization. It was concretized by Lofti Zadeh in 1960’s. The basic crunch behind Fuzzy logic is that “even if people don’t know the precise numerical data for reasoning in any case, they are capable of controlling their deductions in an adaptable manner.” If such capability is machined, then, first of all, it would be quite easy to implement it, since it is a direct correlation between Mathematics and Linguistics, and can also provide prolific consequences [7].

In order to learn the way how fuzzy logic works, we prologue three concepts, viz. fuzzy sets, fuzzy operations, if-then statements.

1) Fuzzy Sets: In our conventional Set Theory, we know that an element can be either present or not present in a given universal set. This is called ‘crisp’ logic. In fuzzy sets, we introduce a membership function m whose range is [0, 1]. This membership function implies the extent up to which an element is present in a given set. Thus, crisp logic is the extreme case of Fuzzy logic.

2) Fuzzy operators: -Similar to classic sets, Zadeh has defined operations like union, intersection and complement to be applied to fuzzy sets. Let P and Q be two fuzzy sets and m1(x) and m2(x) be their membership functions. The basic set-operators can be generalized as written below:

\[ m(P \cup Q) = \max(m_1(x), m_2(x)) \]  
\[ m(P \cap Q) = \min(m_1(x), m_2(x)) \]  
\[ \overline{m} = 1 - m \]  

3) If - then statements: - These statements are basic instructions which expatiate the demeanor of a system by means of commands which are easily understandable by the machine.

Let us now formalize these concepts in a more serious way.

Let y1, y2, ..., y(n) and z1, z2, ..., z(m) be fuzzy variables and let P1, P2, ..., P(n) and Q1, Q2, ..., Q(m) be fuzzy sets. An if-then rule can be defined as:

IF y1 is P1 AND y2 is P2 AND ... AND y(n) is P(n) (antecedent)  
THEN z1 is Q1 AND z2 is Q2 AND ... AND z(m) is Q(m) (Consequent).

4. Proposed Methodology

Cloning an image with an objective to hide any individual or object in the sight is the most common part of digital image forgery. When this has been done with attention, it may be tough for anyone to diagnose cloning creatively. The variable size of cloned portion makes it computationally unattainable to match all the probable image locations. The threat is even bigger when the forger distorts the image to hide the forgery. Block matching based forgery detection technique [12] is strong forgery detection tool available in the digital image processing literature.

The idea behind the algorithm is to “divide an M×N image into a number of overlapping blocks of size (b×b) which results in [(M-b+1)*(N-b+1)] blocks in total. Feature matrix of size (k*b2) is constructed by reshaping each block into a row vector of size (k* b2). This feature matrix is then sorted lexicographically which assures that similar feature vectors are sorted adjacent to each other”. The difference between the adjacent pair of row is known as “shift vector”.

“Higher the occurrence of shift vector implies that a
portion has been duplicated and the resulting location information of such portions is saved for further processing and decision making.”

It is clear that as the image size increases the computational complexity of the algorithm also increases. A variety of dimension reduction techniques e.g. DWT, DCT, DFT, PCA and SVD are presented in the literature to reduce the computational complexity of the algorithm [12-15].

DCT and PCA methods are robust to small elementary changes in the image after forgery and noise addition but then failed to provide higher accuracy when drastic changes are made by the forger. DWT provides robustness to Gaussian noise addition but does not perform well when image is manipulated with blurring effect. A single technique is not suitable for all kind of post processing performed on an image, hence a novel and tenable forgery detection and classification system has been proposed in this paper.

The proposed technique applies a set of detection algorithms on the given image and comments on the nature of forgery are done with fuzzy based classifier. The architecture of the proposed forgery detection system is shown in Fig. 2 on the adjacent page. The given image is first converted to 256×256 pixel gray scale image, and the resulting image is then divided into b×b sized overlapping blocks generating a total number of \((M-b+1)\times(N-b+1)\) blocks.

\[
B(x, y) = I(x+i, y+i)
\]

\(x, y \in \{0, ..., b-1\}\), \(i \in \{0, ..., M-b\}\), and \(j \in \{0, ..., N-b\}\)

3. Now dimension reduction technique is applied over each b×b block as follows:

\[
C = DWT(B(x, y))
\]

\(x, y \in \{0, ..., b-1\}\), \(i \in \{0, ..., M-b\}\), and \(j \in \{0, ..., N-b\}\)

Where x and y represents the starting points of block’s row and column respectively.

Total no. of blocks \(T = (M-b+1)(N-b+1)\)

4. Then the feature vector is extracted as follows:

\[
Z = C(1 : Nc)
\]

where \(Nc = \{1, ..., n\}\), \(n\) is the length of \(C\).

5. These feature vectors are arranged into a \((M-b+1)\times(N-b+1)\) matrix, represented by \(m\).

6. The resulting feature matrix \(m\) is then sorted lexicographically on order to arrange similar components adjacent to each other. A matching procedure based on calculating offset value between neighbouring elements is applied to find the similarity. A threshold value \(N_d\) set to determine the amount of neighbour. “If the Euclidian distance between the pair is less than the threshold then the pairing neighbour is considered to be part of forgery”. Their location information \((x, y)(x', y')\) and the shift vector between them \([x, -x', y, -y']\) are therefore stored. From these offset values most frequent element is calculated and each pixel in the image is compared with this frequent element and accordingly replaced with black pixel.
7. Similar procedure is employed for the remaining dimension techniques and in similar vein; we get results in different formats, depending upon the intrinsic property of the methodological transform.
8. Now, we are in a dilemma. We have multiple conclusions regarding the authenticity and tampering probability of the digital image. Here, we need a global response which will crisply tell us whether the image is tampered or not.
9. The best way we have here, which we have employed also, is to utilize a Fuzzy Classifier; since fuzzy approach is the best when we have to deal with uncertainties. Thus, when we encapsulate our results in a fuzzy based classifier, we eventually get a global affirmation regarding the integrity of the digital image under test.
10. Functioning Mechanism of Fuzzy Based Classifier
   1) Considering the fuzzy approach paradigm shift, we inchoate by expatiating with perceptual and linguistic terms the goal we would like to accomplish. We are now in a position that we have got enough results regarding tampering by various images transforms.
   2) Here, we have an idea that “if from the techniques we employed for detection, if some technique detects the image as tampered and at the same time the reliability of the response given by that technique is high, then, we can trust its response”.
   3) “On the other hand, if another method (transform) also affirms tampering case, but, its reliability function is not that strong as anticipated, then, we still trust its output, but only to a lesser extent”.
      Let D be a fuzzy variable which implies the detection of tampering of a specific tool having range [0, 1] and at the same time, let us consider R to be also a fuzzy variable depicting the reliability of the response, having same range.
      Let YES and NO be two another variables.
      YES = Detection is HIGH.
      NO = Detection is LOW.
      Here, in fuzzy approach, HIGH and LOW are fuzzy sets.
      Illustration: Let our tools (DFT, DCT, SVD, DWT or hybridization of these tools, etc.) give responses as (YES, YES, NO, YES), then we have the scenario as:
      \[ D1 \text{ high } \land D2 \text{ high } \land D3 \text{ low } \land D4 \text{ high.} \]
      The trustworthiness or the reliability of the tool thus comes into picture and fully impacts the further consequences. If we wholeheartedly trust a tool, then we assign to the response the most intense fuzzy set (extremely strong or extremely weak). If, on the other hand, we don’t trust the reliability of some tool to an expected level, we opt for the less intense fuzzy set (weak, strong).
   4) For sake of conceptual clarity, we now deal with the automatic construction of the fuzzy rules.
      For sake of simplicity, we at this point of time, consider only two tools and case (NO, YES) depicting the anticipated Fuzzy tampering with aligned JPEG grids.
      The squeezed Fuzzy rule is explained as follows:
      \[ \text{IF } (D1 \text{ low } \land D2 \text{ high}) \]
      \[ \text{THEN } \text{IF } (R1 \text{ high } \land R2 \text{ high}) \]
      \[ \text{THEN tampering is EXTREMELY STRONG} \]
      \[ \text{ELSE tampering is STRONG} \]
      Expressing this fuzzy statement in a standard form by decomposing the inside square brackets,
      \[ \text{IF } (D1 \text{ low } \land D2 \text{ high}) \]
      \[ \text{THEN } \text{IF } (R1 \text{ high } \land R2 \text{ HIGH}) \text{ THEN tampering is EXTREMELY STRONG} \]
      \[ \text{IF } (D1 \text{ low } \land D2 \text{ high}) \]
      \[ \text{THEN } \text{IF } (R1 \text{ high } \land R2 \text{ high}) \text{ bar } \]
      \[ \text{THEN tampering is STRONG} \]

11. Weight value for the fuzzy inference system is then calculated based on the difference between the detected and the copied portion.

\[ W = \text{Mean} \left( \text{mean} \left( I(x_1 : x_2, y_1 : y_2) - R(x'_1 : x'_2, y'_1 : y'_2) \right) \right) \]
(8)

Here \((x_1, y_1) \rightarrow (x_2, y_2)\) and \((x'_1, y'_1) \rightarrow (x'_2, y'_2)\) and are the dimensions of copied and detected region respectively.

Finally the performance of the algorithm is evaluated based on True Positive Rate, False Positive Rate and Accuracy given as:

\[ \text{Accuracy(\%)} = \frac{\text{number of detected elements}}{\text{number of copied elements}} \times 100 \]  
(9)

\[ \text{TPR} = \frac{\text{number of images detected as forged being forged}}{\text{number of forged images}} \]  
(10)

\[ \text{FPR} = \frac{\text{number of images detected as forged being original}}{\text{number of original images}} \]  
(11)

4.2 Fuzzy based forgery classification system:

The architecture of proposed fuzzy based forgery classification system is shown in Fig. 2. Based on the difference between the duplicated and detected duplicate region a weight value is calculated. This weight value is given to proposed fuzzy based classifier which then classifies the nature of processing performed on the image as Blurring, Intensity Variation, Noise addition and Normal forgery. The rules are given in Table 1 below:

Here, in our case we have used single threshold fuzzy logic based classifiers. We have used six methodologies precursors and 4 types of attack. This for each method, what you have is a set of 4 inputs. The total combinations will be \(4 \times 4 \times 4 \times 4 \times 4 \times 4 (4^6)\) but since a single threshold logic is used, the no of possible choices dwindles.

For instance, DWT-DCT is prominently implemented for intensity variation is having the highest membership.
Table 1. Rule set for proposed forgery classification system

<table>
<thead>
<tr>
<th>PCA</th>
<th>DWT</th>
<th>DWT-DCT</th>
<th>DWT-DCT-SVD</th>
<th>DFT</th>
<th>DCT</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Blurring</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Gaussian Noise</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Highest</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Intensity Variation</td>
</tr>
<tr>
<td>Highest</td>
<td>Highest</td>
<td>High</td>
<td>Highest</td>
<td>Highest</td>
<td>Highest</td>
<td>Normal Forgery</td>
</tr>
</tbody>
</table>

(fuzzy) function and the other methods have low membership function, so far efficient determination of intensity variation. We need not consider all the possible when we know that the hybridized DWT-DCT is the best for a particular type of attack. Therefore, we have rated out the unprolific poor choices for an sample space. Results are shown in Fig. 5.

The range is started as 0 to 100 in fuzzy inference system (FIS) depicts the accuracy set of proposed methodology. This implies that the accuracy levels in FIS $\in [0,100]$. FIS system are shown in Fig. 3.

The tools, inclusive of fuzzy classifier, given efficient robustness to the algorithm, comparable to that given by the Gaussian membership function. Proposed system has been tested with different membership functions like triangular, Gaussian so that robustness of the system will dominant. Proposed tools gives the results comparable results for different others membership function. Comparable results are obtained with Gaussian membership function for classification of forgery. System is robust for variation of the membership functions. Results for membership functions are shown in Fig. 4.
5. Experimental Results and Discussions

Under this head, we performed our simulations in MATLAB 13 (32GB RAM) i7 processor with MICC-F220 images and CASIA dataset [27, 28]. We exposed the investigated images with various attacks associated with Gaussian blurring, noise addition, intensity variation etc. and then we tried to validate our fuzzy based algorithm in its sequential detection.

As we already know, we have applied 6 different forgery detection techniques in individual as well as hybrid form (which is also a novel approach). The role of the fuzzy-based classifier comes into picture afterwards. The Tables 2 to 3 testimonies that as we increase the block size, as we are already familiar with, the computational complexity for the algorithm ekes out and thus the overall efficiency dwindles.

We also find that the hybridization of the methods has given more enthusiastic results than those given by the other techniques individually.

In this section, we shall deal with the prolific issues of the paper. The result analysis has been divided into 3 main sections, which in turn, have been divided into further subsections. The first section deals with the applicability and validity of the proposed fuzzy logic based algorithm under various types of forgerial modifications. Here, for better understanding of the algorithm, we have used 2 blocks (used for lexicographic sorting) differing in the size. The second section prologues a graphical outlook on the conclusions of the algorithm, with reference to the previous section. The last section compares the related works in this field of forensic sciences and the peculiarity of our algorithm.

Table 2. Accuracy result for forgery detection system (56×56)

<table>
<thead>
<tr>
<th>Method</th>
<th>Without Processing (%)</th>
<th>Gaussian Noise (%)</th>
<th>Motion Blur (%)</th>
<th>Intensity Variation (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Block Size</td>
<td>Block Size</td>
<td>Block Size</td>
<td>Block Size</td>
</tr>
<tr>
<td>DWT</td>
<td>3×3 4×4 8×8 16×16</td>
<td>3×3 4×4 8×8 16×16</td>
<td>3×3 4×4 8×8 16×16</td>
<td>3×3 4×4 8×8 16×16</td>
</tr>
<tr>
<td>DCT</td>
<td>89.57 85.97 76.56 53.60</td>
<td>74.20 72.03 59.78 40.14</td>
<td>49.39 48.40 39.10 23.27</td>
<td>86.47 83.19 70.69 48.76</td>
</tr>
<tr>
<td>PCA</td>
<td>89.57 88.57 76.56 53.60</td>
<td>32.27 41.14 60.33 39.50</td>
<td>29.10 24.68 39.32 23.31</td>
<td>86.51 83.19 70.69 48.78</td>
</tr>
<tr>
<td>DWT-DCT</td>
<td>92.08 89.57 6.56 53.60</td>
<td>75.64 72.68 68.84 50.06</td>
<td>56.06 49.36 45.79 35.33</td>
<td>86.47 84.82 75.19 62.43</td>
</tr>
<tr>
<td>DWT-DCT-SVD</td>
<td>92.76 89.45 76.56 53.60</td>
<td>70.12 71.11 59.75 37.34</td>
<td>49.36 40.54 45.79 35.33</td>
<td>86.47 83.19 70.69 48.75</td>
</tr>
<tr>
<td>DFT</td>
<td>94.35 89.12 85.93 71.91</td>
<td>63.90 61.28 70.50 57.42</td>
<td>40.52 26.44 47.03 36.38</td>
<td>86.13 87.97 76.69 66.16</td>
</tr>
</tbody>
</table>

Table 3. Accuracy result for forgery detection system (81×81)

<table>
<thead>
<tr>
<th>Method</th>
<th>Without Processing (%)</th>
<th>Gaussian Noise (%)</th>
<th>Motion Blur (%)</th>
<th>Intensity Variation (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Block Size</td>
<td>Block Size</td>
<td>Block Size</td>
<td>Block Size</td>
</tr>
<tr>
<td>DWT</td>
<td>3×3 4×4 8×8 16×16</td>
<td>3×3 4×4 8×8 16×16</td>
<td>3×3 4×4 8×8 16×16</td>
<td>3×3 4×4 8×8 16×16</td>
</tr>
<tr>
<td>DCT</td>
<td>97.78 97.52 91.28 82.62</td>
<td>88.45 86.51 80.84 79.49</td>
<td>71.95 71.22 68.24 57.90</td>
<td>94.37 92.46 87.74 79.49</td>
</tr>
<tr>
<td>PCA</td>
<td>98.47 94.36 89.54 82.68</td>
<td>82.89 77.94 72.58 69.72</td>
<td>78.23 76.89 70.64 65.48</td>
<td>94.72 93.25 90.63 82.88</td>
</tr>
<tr>
<td>DWT-DCT</td>
<td>95.74 93.25 89.36 82.46</td>
<td>84.85 83.79 78.52 67.28</td>
<td>67.28 69.70 68.78 65.57 55.40</td>
<td>94.75 93.84 90.75 83.49</td>
</tr>
<tr>
<td>DWT-DCT-SVD</td>
<td>97.45 96.84 90.72 82.69</td>
<td>82.73 77.97 72.84 69.47</td>
<td>71.65 70.46 68.69 57.40</td>
<td>94.48 93.23 90.78 82.64</td>
</tr>
<tr>
<td>DFT</td>
<td>99.17 97.58 95.35 83.45</td>
<td>78.36 75.54 69.12 65.14</td>
<td>65.78 63.52 60.36 55.47</td>
<td>96.78 95.25 93.57 89.74</td>
</tr>
</tbody>
</table>
5.1 Performance analysis for image forgery detection, in concordance with variation in block length and size of copied portion

The proposed fuzzy based forgery detection system is simulated on MATLAB (2013a). A random set of images has been taken from MICC-F220 & CASIA [27, 28] dataset and tested for varying block length and size of copied portion and results have been compared with respect to accuracy. Block size are varied as 3×3, 4×4, 8×8 and 16×16 while the size of duplicated portion is taken as 56×56 and 81×81. Table 1 Shows the comparative accuracy result for 56×56 sized copied part for proposed forgery detection system and the result for 81×81 are given in Table 2. The comparative results are shown in Fig. 6 to Fig. 11.

Table 2 shows the variation of accuracy for different block sizes with 56×56 size copied portion. It is observed that for smaller block size accuracy value is high while it reduces on increasing the block size. DFT performs well with highest accuracy of 94.35% in case of Normal forgery and 88.13% in case of Intensity variation. While in presence of Gaussian noise and Motion blurring DWT based scheme outperforms all other schemes with an accuracy of 80.99% and 51.92% respectively. It should be noted that in our scheme accuracy is not calculated by number of correctly detected image while we have chosen pixel based approach to calculate the accuracy.

Table 3 shows the same for the size of copied portion to be 81×81. With increase in the size of copied portion (number of elements to be copied) improvement in the
performance of detection techniques has been observed. Now the highest achievable accuracy is 99.17% which was achieved with a block size of 3×3 in case of normal forgery and 96.78% in case of intensity variation both by Discrete Fourier Transform scheme. Unlike the prior case DCT based scheme provides the highest accuracy in case of motion blurring and DWT-DCT-SVD cascaded scheme provides 89.78% accuracy in case of Gaussian noise addition.

The Accuracy Vs Block size graph for DWT based forgery detection system is given in above. DWT performs better in case of normal forgery while it is found out to be the worst as far as our research standards are concerned. The performance of PCA based forgery detection system is given in figure above, PCA performs well in case of Intensity variation and normal forgery while it does not perform well when Blurring and Gaussian noise addition is performed over forged image. Fig. 7, Fig. 9, Fig. 9 and Fig. 10 show the performance of DCT, DFT, DWT-DCT and DWT-DCT-SVD algorithms respectively. The overall observation shows that “accuracy of the algorithm is inversely proportional to the block size”. Also the “computational time is inversely proportional to the block size used”. Higher block size provides to lower computational time but it results in diminished accuracies.

5.2 Performance analysis for accuracy of image forgery detection

A. Pixel based accuracy calculation

Performance of proposed detection forensic tools in terms of pixel based accuracy is given in Table 4 below. 220 images were randomly chosen from MICC-F220 [27] and undergone through Gaussian Noise addition, Motion Blurring, Intensity variation and Normal forgery respectively. DFT performs well with highest accuracy of 99.17% in case of Normal forgery and 97.68% in case of Intensity variation. While in presence of Gaussian noise and Motion blurring DWT-DCT-SVD based scheme outperforms all other schemes with an accuracy of 97.68 and 91.83% respectively. It should be noted that in our scheme accuracy is not calculated by number of correctly detected image while we have chosen pixel based approach to calculate the accuracy. All algorithms are able to detect all types of forgery with respect to pixel values. Comparison graph of pixel based accuracy calculation for forgery detection system is shown in Fig. 12 and represented in Table 4.

Table 4. Pixel based accuracy calculation for forgery detection system

<table>
<thead>
<tr>
<th>Data Set type</th>
<th>(DCT) (in %)</th>
<th>(DFT) (in %)</th>
<th>(DWT-DCT-SVD) (in %)</th>
<th>(DWT-DCT) (in %)</th>
<th>(DWT) (in %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Forgery (220 images)</td>
<td>98.47</td>
<td>99.17</td>
<td>97.89</td>
<td>97.45</td>
<td>97.78</td>
</tr>
<tr>
<td>Forgery with Noise addition (220 images)</td>
<td>82.89</td>
<td>78.36</td>
<td>97.68</td>
<td>82.73</td>
<td>88.45</td>
</tr>
<tr>
<td>Forgery with Blurring (220 images)</td>
<td>78.23</td>
<td>65.78</td>
<td>91.83</td>
<td>71.65</td>
<td>71.95</td>
</tr>
<tr>
<td>Forgery with Intensity variation (200 images)</td>
<td>94.72</td>
<td>96.78</td>
<td>81.69</td>
<td>94.48</td>
<td>94.37</td>
</tr>
</tbody>
</table>

5.3 Performance analysis for image forgery classification

The performance of proposed fuzzy based classifier is given in Table 4 below. 100 images were randomly chosen from MICC-F220 and CASIA dataset [27, 28] and undergone through Gaussian Noise addition, Motion Blurring, Intensity variation and Normal forgery respectively. Hence a total number of 1600 images with 4 dataset were experimented by our proposed algorithm. Fuzzy logic was supposed to classify the distortion performed on the image after the detection of forgery. Out of 1600 images, 387 images were successfully classified in as normal forgery, 384 were classified as Noise addition based forgery, 357 as blurring and 378 as were detected to be undergone through intensity variation based attack. The overall accuracy provided by the algorithm was 94.12% in terms of successful classification. Accuracy Result for Fuzzy based forgery classification system tabulated in Table 5 and presents the result of Accuracy Result for proposed fuzzy based classifier including four test scenarios.

Fig. 11. Accuracy graph for DWT-DCT-SVD based forgery detection system (56×56)

Fig. 12. Comparison graph of pixel based accuracy calculation for forgery detection system
5.4 Performance analysis of the proposed algorithm under various attacks on the investigated image:

Here, in this section we will try to have a look at the authenticity of the algorithm under various types of attacks, generally encountered in Image Forensics like Gaussian Blurring, addition of Gaussian white noise to the image, jpeg compression with different quality factors, etc. Forged image with different attacks like Gaussian blurring, addition of Gaussian Noise, Intensity variation, Normal Forgery and their detected image is shown in Fig. 13 to Fig. 16. The images shown below explain the scenario in a crystal clear manner.

A.1 -Effect of gaussian (motion) blurring:-

![Fig. 13. (a) Forged image with motion blurring; (b) detected image](a) ![Fig. 13. (a) Forged image with motion blurring; (b) detected image](b)

A.2 -Effect of addition of gaussian noise:-

![Fig. 14. (a) Forged image with gaussian noise addition; (b) detected image](a) ![Fig. 14. (a) Forged image with gaussian noise addition; (b) detected image](b)

5.5 Comparison study with previous existing methods

Here, in this section, we shall try to develop a comparative outlook, in association with the algorithm designed in this paper with the related algorithms in the same field.

The peculiarity of this paper over the previously developed algorithms is that in addition of applying the basic feature extracting transforms like DCT, DWT, etc., we have designed a Fuzzy based classifier which, in crude words, will strive to refine the results fetched. A more novel approach in this paper is the prolific hybridization of the transforms, which has given a broader perspective regarding the utility and applicability of the feature extraction transforms.

Comparatively, the fuzzy logic proves to fetch us the most authenticate results regarding the tampering of the image (authenticity), which is not discussed by any fellow in Image Forensics.

The performance parameters of this technique were compared with those of previously known techniques. As seen from Table 6 and Fig. 17. The proposed technique provides acceptable values for all parameters. It achieves an accuracy of 94.12%. It also provides TPR and Precision are 97.18 and 96.12. Hence the proposed technique has a greater ability to detect a forged image as forged and an authentic image as authentic.

There are also tampered test images with post processing operation, such as normal Forgery, Gaussian blurring and Gaussian noise Addition. We have tempered the image

<table>
<thead>
<tr>
<th>Data Set type</th>
<th>Number of images</th>
<th>Correctly classified</th>
<th>Incorrectly classified</th>
<th>Accuracy (in %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Forgery (100 images)</td>
<td>400</td>
<td>387</td>
<td>13</td>
<td>96.75</td>
</tr>
<tr>
<td>Forgery with Noise addition (100 images)</td>
<td>400</td>
<td>384</td>
<td>16</td>
<td>96.0</td>
</tr>
<tr>
<td>Forgery with Blurring (100 images)</td>
<td>400</td>
<td>357</td>
<td>43</td>
<td>89.25</td>
</tr>
<tr>
<td>Forgery with Intensity variation (100 images)</td>
<td>400</td>
<td>378</td>
<td>22</td>
<td>94.5</td>
</tr>
<tr>
<td>Total</td>
<td>1600</td>
<td>1506</td>
<td>94</td>
<td>94.12 (overall)</td>
</tr>
</tbody>
</table>

A.3 -Effect of intensity variation:-

![Fig. 15. (a) Forged image with effect of intensity variation; (b) Detected image](a) ![Fig. 15. (a) Forged image with effect of intensity variation; (b) Detected image](b)

A.4 -Effect of copy-move forgery:

![Fig. 16. (a) Forged first image; (b) Detected first image](a) ![Fig. 16. (a) Forged first image; (b) Detected first image](b)

Table 5. Accuracy result for fuzzy based forgery classification system

Table 5. Accuracy result for fuzzy based forgery classification system

<table>
<thead>
<tr>
<th>Data Set type</th>
<th>Number of images</th>
<th>Correctly classified</th>
<th>Incorrectly classified</th>
<th>Accuracy (in %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Forgery (100 images)</td>
<td>400</td>
<td>387</td>
<td>13</td>
<td>96.75</td>
</tr>
<tr>
<td>Forgery with Noise addition (100 images)</td>
<td>400</td>
<td>384</td>
<td>16</td>
<td>96.0</td>
</tr>
<tr>
<td>Forgery with Blurring (100 images)</td>
<td>400</td>
<td>357</td>
<td>43</td>
<td>89.25</td>
</tr>
<tr>
<td>Forgery with Intensity variation (100 images)</td>
<td>400</td>
<td>378</td>
<td>22</td>
<td>94.5</td>
</tr>
<tr>
<td>Total</td>
<td>1600</td>
<td>1506</td>
<td>94</td>
<td>94.12 (overall)</td>
</tr>
</tbody>
</table>
through addition of noise and Gaussian blurring. The following above tables shows the detection accuracy of our methods which gives better results than other exiting methods with less computational time. Table 7, Table 8 and Table 9 shows accuracy of detection accuracy under various attacks on test images which is also good than other methods. Presented DAR curves prove that detection accuracy of our method is also increased as compare with other exiting methods.

Table 6. Comparison of forgery classification with existing techniques

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Recall(TPR)</th>
<th>Precision</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Farid-2009[23]</td>
<td>37.70</td>
<td>90.02</td>
<td>87.80</td>
</tr>
<tr>
<td>Li-2009[24]</td>
<td>91.59</td>
<td>45.24</td>
<td>47.21</td>
</tr>
<tr>
<td>Bianchi-2011[25]</td>
<td>59.29</td>
<td>95.17</td>
<td>93.65</td>
</tr>
<tr>
<td>Mahdian-2008[26]</td>
<td>37.84</td>
<td>82.09</td>
<td>80.21</td>
</tr>
<tr>
<td>Mohammad-2014[30]</td>
<td>90.00</td>
<td>88.00</td>
<td>89.00</td>
</tr>
<tr>
<td>Proposed Algorithm</td>
<td>97.18</td>
<td>96.12</td>
<td>94.12</td>
</tr>
</tbody>
</table>

Table 7. Comparison of detection accuracy with normal forgery on test images

<table>
<thead>
<tr>
<th>Images</th>
<th>Our method (Hybridized) (DWT-DCT-SVD)</th>
<th>Improved DCT [29]</th>
<th>PCA [12]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deer</td>
<td>84.15</td>
<td>67.17</td>
<td>68.58</td>
</tr>
<tr>
<td>Disconnected_shift</td>
<td>69.15</td>
<td>46.91</td>
<td>40.52</td>
</tr>
<tr>
<td>Dscf</td>
<td>82.45</td>
<td>39.33</td>
<td>-</td>
</tr>
<tr>
<td>Extension</td>
<td>72.15</td>
<td>25.54</td>
<td>40.25</td>
</tr>
<tr>
<td>Red_tower</td>
<td>91.75</td>
<td>55.49</td>
<td>70.16</td>
</tr>
<tr>
<td>Tree</td>
<td>77.13</td>
<td>61.02</td>
<td>57.91</td>
</tr>
<tr>
<td>Truck</td>
<td>74.06</td>
<td>57.64</td>
<td>55.53</td>
</tr>
<tr>
<td>CRW</td>
<td>62.45</td>
<td>20.81</td>
<td>24.00</td>
</tr>
</tbody>
</table>

Table 8. Comparison of detection accuracy with blurring attacks on test images

<table>
<thead>
<tr>
<th>Images</th>
<th>Our method (Hybridized) (DWT-DCT-SVD)</th>
<th>Improved DCT [29]</th>
<th>PCA [12]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deer</td>
<td>81.14</td>
<td>44.02</td>
<td>69.51</td>
</tr>
<tr>
<td>Disconnected_shift</td>
<td>76.18</td>
<td>43.02</td>
<td>42.42</td>
</tr>
<tr>
<td>Dscf</td>
<td>90.15</td>
<td>70.50</td>
<td>-</td>
</tr>
<tr>
<td>Extension</td>
<td>70.02</td>
<td>35.50</td>
<td>34.68</td>
</tr>
<tr>
<td>Red_tower</td>
<td>76.78</td>
<td>52.82</td>
<td>50.23</td>
</tr>
<tr>
<td>Tree</td>
<td>69.45</td>
<td>46.87</td>
<td>48.03</td>
</tr>
<tr>
<td>Truck</td>
<td>72.03</td>
<td>13.95</td>
<td>23.43</td>
</tr>
<tr>
<td>CRW</td>
<td>68.86</td>
<td>59.02</td>
<td>53.14</td>
</tr>
</tbody>
</table>

Table 9. Comparison of detection accuracy with Gaussian noise addition attacks on test images

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Deer</td>
<td>80.18</td>
<td>44.02</td>
<td>69.51</td>
</tr>
<tr>
<td>Disconnected_shift</td>
<td>75.49</td>
<td>43.02</td>
<td>42.42</td>
</tr>
<tr>
<td>Dscf</td>
<td>91.82</td>
<td>70.50</td>
<td>-</td>
</tr>
<tr>
<td>Extension</td>
<td>71.66</td>
<td>35.50</td>
<td>34.68</td>
</tr>
<tr>
<td>Red_tower</td>
<td>77.89</td>
<td>52.82</td>
<td>50.23</td>
</tr>
<tr>
<td>Tree</td>
<td>73.86</td>
<td>46.87</td>
<td>48.03</td>
</tr>
<tr>
<td>Truck</td>
<td>78.76</td>
<td>13.95</td>
<td>23.43</td>
</tr>
<tr>
<td>CRW</td>
<td>69.87</td>
<td>59.02</td>
<td>53.14</td>
</tr>
</tbody>
</table>
algorithms. In Fig. 18 we can observe that DAR of forged image with under normal forgery increases as compare to exiting methods. In Fig. 19 we can observe that DAR of forged image with Gaussian Blurring increases as compare to exiting methods. Fig. 20 shows that DAR of forged image which tampered by addition of noise also increase as compare with other methods.

As we visualized, given above is a comparison made among some of the performance parameters in among our proposed algorithm and the other relevant papers. From the table, we see that our proposed algorithm, if analyzed, proves to be a much better option when the activities of the image forensics are on a running platform. Our method has better and zealous recall rate, precision and accuracy when compared with other papers. So, this methodology proves to be a good choice for the upcoming researchers to the fascinating field of Image Forensics.

6. Conclusion

Block matching based forgery detection and fuzzy based forgery pattern classification system has been presented in this paper. Performance of digital forgery detection system for different dimension reduction approaches including DWT, PCA, DCT, DFT, DWT-DCT, and DWT-DCT-SVD has been evaluated and compared with varying block size and the size of copied portion. Simulation results presented in Table 2 and Table 3 shows that DFT based forgery detection system outperforms all the dimension reduction techniques in case of intensity variation and normal forgery (without any post processing) while DWT based technique is best suitable in case of noise addition and blurring. With the 56×56 sized copied part DFT based technique maximum accuracy of 94% (based on detection of total number of copied and detected elements) while in case of 81×81 sized copied portion the maximum accuracy achieved is 99.17%. The proposed fuzzy based forgery classification system has been evaluated for four cases including images, without any post-processing, with noise addition (Gaussian noise), and with intensity variation and motion blurring. The proposed classifier has achieved 94.12% overall accuracy in classification of all test scenarios.

References


Acknowledgements

We would like to thank our Supervisor and Coordinator of Center of Excellence Dr. Avinash G. Keskar for his constant encouragement and guidance toward this project. This project is funded from Centre of Excellence (CoE), Department of Electronics and Communication Engineering, VNIT Nagpur. Special thanks to Director VNIT Nagpur for providing institutional facilities and needed administrative and authoritative support during the work at VNIT.

Mohammad Farukh Hashmi was born in 1983, India, The author received his B.E in Electronics & Communication Engineering from R.G.P.V Bhopal University. He obtained his M.E in Digital Techniques & Instrumentation in 2010 from R.G.P.V Bhopal University. He is currently pursuing his doctoral studies at VNIT Nagpur under the supervision of Dr.A.G.Keskar. He has published up to 34 papers in international conferences and journals. He has a teaching experience of 3.5 years. His current research interests are Computer Vision, Circuit Design, and Digital IC Design etc. Mr. Mohammad F. Hashmi is a member of IEEE, ISTE, and IAENG.

Avinash G. keskar was born in 1959, India. The author completed his B.E from VNIT, Nagpur in 1979 and received gold medal for the same. He completed his M.E. from IISc, Bangalore in1983, receiving the gold medal again. He has 26 years of teaching experience and 7 years of industrial experience. He is currently a Professor in Department of Electronics and Communication Engineering, VNIT Nagpur. His current research interests include Computer Vision, Soft Computing, and Fuzzy Logic etc. Dr. Keskar is a senior member of IEEE, FIETE, LMISTE, FIE.