International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:7, No:11, 2013

Copy-Move Image Forgery Detection in Virtual Electrostatic Field

Michael Zimba, Darlison Nyirenda

***Abstract*—**A novel copy-move image forgery, CMIF, detection method is proposed. The proposed method presents a new approach which relies on electrostatic field theory, EFT. Solely for the purpose of reducing the dimension of a suspicious image, the proposed algorithm firstly performs discrete wavelet transform, DWT, of the suspicious image and extracts only the approximation subband. The extracted subband is then bijectively mapped onto a virtual electrostatic field where concepts of EFT are utilized to extract robust features. The extracted features are invariant to additive noise, JPEG compression, and affine transformation. Finally, same affine transformation selection, SATS, a duplication verification method, is applied to detect duplicated regions. SATS is a better option than the common shift vector method because SATS is insensitive to affine transformation. Consequently, the proposed CMIF algorithm is not only fast but also more robust to attacks compared to the existing related CMIF algorithms. The experimental results show high detection rates, as high as 100% in some cases.

***Keywords*—**Affine transformation, Radix sort, SATS, Virtual electrostatic field.

I. Introduction

A Copy-Move Image Forgery, CMIF, is a specific kind of image tampering. In a CMIF, a part of an image is copied and then pasted on a different location within the same image. Usually, such an image tampering is done with the aim of either hiding some image details, in which case a background is duplicated, or adding more details in which case at least an object is cloned. Fig. 1 depicts examples of CMIF attacks.

Fig. 1 Examples of CMIF Forged images are in left column and original images are in right column. Rows depict object removal (above) and object duplication (below)

The forged images are shown in the left column and the original images are shown in the right column. The top row depicts object removal and the bottom row shows object duplication in an image attacked by CMIF.

CMIF attacks are often imperceptible because of the fact that the copied regions come from the same image as the segments where the regions are pasted thereby making the color palettes, noise components, dynamic ranges and other properties compatible with the rest of the image [1], [2]. Furthermore, an attacker can geometrically manipulate, compress or add noise to the copied regions thereby mating and blending the pasted regions into their targeted surroundings [3], [4].

The primary task of a CMIF detection algorithm is to determine if a given image contains cloned regions without prior knowledge of their shape and location. Various transforms, analogies and techniques have been presented in an attempt to detect CMIF. In their proposed block matching based method for detecting CMIF, Fridrich et al. [5] use quantized discrete cosine transform (DCT) coefficients to represent feature vectors. The DCT coefficients are lexicographically sorted and adjacent vectors are checked for similarity. Apart from retouching test, the authors, however, do not employ robustness tests. Most recently, Bayram et al. [6] apply Fourier Mellin Transform (FMT) and 1-D projection of log-polar values in their robust scheme of detecting image forgeries. Experimental results show that their technique is robust to rotation with 10 degrees, scaling with 10% and compression up to quality level 20. Li et al. [7] initially reduce the dimension of the image by considering only the low frequency sub-band of DWT output and then reduce the length of the feature vector using singular value decomposition, SVD. DWT is widely used in image processing.

However, so far, no CMIF detection algorithm which presents a direct EFT analogy has been proposed. The algorithm proposed in this paper therefore presents a novel approach to CMIF detection. It is envisaged that the proposed approach will be of useful practical applications, not only in CMIF detection but also in digital image forensics in general.

In Section II, a focused and comprehensive background towards the design of the proposed algorithm is presented. The proposed CMIF detection algorithm is presented in Section III. Its advantages over existing related CMIF algorithms are stipulated. Section IV presents the detection results by the proposed algorithm and Section V concludes the paper.

II. Background

A. Image to Virtual Electric Field Bijection

Inspired by the work on corner detection in images in an electric field by Abdel-Hamid and Yang [8], we

M. Zimba is with the Department of Physics, Mzuzu University, Private Bag 201, Luwinga, Mzuzu 2, Malawi (Phone: +265 1320 575; fax: +265 1320 568; e-mail: mgmzimba@gmail.com).

D. Nyirenda is with the School of mathematics, University of Witwatersrand, Private Bag X3, Wits 2050, Johannesburg, South Africa (e-mail: Darlison@aims.ac.za).

mathematically map an $M \times N$ image $F(x, y)$ into a virtual $M \times N$ electric field $Q(u, v)$. The mapping is necessary so that we can adopt physics concepts and utilise them to detect CMIF attacks in an image. It should be stated, right at the beginning, that the mapping and the existence of the virtual electric field are purely for mathematical modeling purposes. Therefore the units of all quantities involved, the coordinates of origin of the electric field are all arbitrary.

For the sake of mathematical modeling, consider the image $F(x, y)$ as a domain consisting of $k = M \times N$ pixels, $p_i, \quad i = 1,2,\cdots k$. Assume that an electric field $Q(u, v)$ exists which can be considered as a domain consisting of $k = M \times N$ positive point charges $q_j, \quad j = 1,2,\cdots k$. Then we define a bijection g that maps the image domain to the electric field domain as follows:

$$g : F(x, y) \to Q(u, v) \tag{1}$$

Furthermore, the following conditions are imposed on the function g. The mapping $q_j = g(p_i)$ holds if and only if both the following conditions are satisfied:

1) A pixel p_i located at (x, y) in the image domain $F(x, y)$ can be mapped to a positive point charge q_j which is located at (u, v) in the virtual electric field domain $Q(u, v)$ if and only if $(x, y) = (u, v)$. For example, a pixel at $(3,7)$ in the image $F(x, y)$ can only be mapped to a positive point charge at $(3,7)$ in the electric field $Q(u, v)$.
2) The magnitude of the charge of the point charge q_j in $Q(u, v)$ is equal to the intensity of the pixel p_i in $F(x, y)$. For example, a charge whose magnitude is 37 units could only have been mapped from a pixel of intensity 37.

If the map g satisfies both the above conditions, then it is coherent that the codomain $Q(u, v)$ inherits the pixel distribution of the domain $F(x, y)$. In that case, a region duplication in the image $F(x, y)$ is a region duplication in the electrostatic field $Q(u, v)$. Consequently we can operate in $Q(u, v)$ to detect duplicated regions in $F(x, y)$. We can also refer to a positive point charge q_j as a pixel q_j in the virtue electric field and talk of pixels generating spherically symmetric electrostatic force fields, and having electric potential.

With such a bijection defined, we invoke the concepts of electrostatic field theory, EFT. For more detailed description of the concepts of EFT consult Halliday [9], Silvester [10] and Grant [11].

1) Assuming that Coulomb's Law holds in the virtual electrostatic field, then the electrostatic force acting along the line between any two pixels q_j and q_i which are separated by the distance r_{ji} is given by the following vector equation:

$$\vec{F}_{ji} = C \frac{q_j q_i}{r_{ji}^{\,2}} \vec{r}_{ji} \tag{2}$$

where the vector $\vec{F}_{ji}$ is the force between the two pixels with charge magnitudes q_j and q_i respectively, $\vec{r}_{ji}$ is a unit vector along the $q_j - q_i$ axis, and C is a constant which for the sake of simplicity is set to 1 in the virtual electrostatic field because the units are arbitrary.

2) If the pixel q_j exists in a neighborhood of k pixels, then the net force exerted on the pixel by all its neighboring pixels can be computed by the superposition principle as follows:

$$\vec{F}_j = \sum_{i \in 1,k | i \neq j} \vec{F}_{ji} = q_j \sum_{i \in 1,k | i \neq j} \frac{q_i}{r_{ji}^{\,2}} \vec{r}_{ji} \tag{3}$$

Both the magnitude and direction of the net force are functions of the magnitudes and directions of all the contributing pixels. The direction of the net force may not even point towards any pixel. However, (2) and (3) give intuitive concept of the pixel interactions in the virtual electrostatic field. The only disadvantage with the force analogy of (2) and (3) is the fact that they involve vectors and vector computation is relatively complex. The immediate associated scalar quantity, electric potential, would be a better option.

1) The pixel q_j has an electric potential V_{ji} as a result of interacting with the pixel q_i which is at the distance r_{ji} from q_j. The electric potential V_{ji} can be computed by the following scalar equation:

$$V_{ji} = q_j \frac{q_i}{r_{ji}} \tag{4}$$

2) By the superposition principle, the net electric potential of the pixel q_j due to interaction with k pixels can be computed by the following summation:

$$V_j = \sum_{i \in 1,k | i \neq j} V_{ji} = q_j \sum_{i \in 1,k | i \neq j} \frac{q_i}{r_{ji}} \tag{5}$$

Since electric potential is a scalar quantity, its computation is less complex. The CMIF detection algorithm proposed in this paper extracts feature vectors whose components consist of functions of electric potential. The electric potential of a pixel existing in isolation in a uv plane of the virtual electrostatic field is unique by direct analogy [9]. Fig. 2 shows

a 3D plot of the electric potential of a pixel q_j located at the origin of a uv plane. Similarly, the electric potential of a pixel existing in an isolated block of k pixels with fixed intensities and locations is unique. We exploit this property of pixel electric potential to trace similar blocks in a CMIF attacked image.

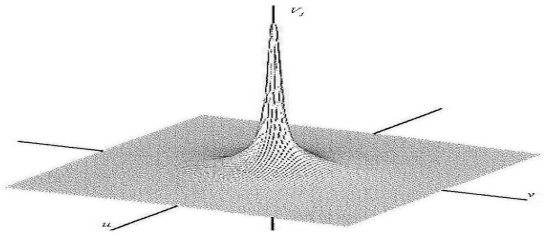

Fig. 2 3D plot of electric potential of a pixel in the uv plane

B. Electric Potential Based Feature Extraction

Inspired by the work on block characteristic based feature extraction by Zimba and Xingming [12], we extract electric potential based features to represent blocks of pixels. In this section the block based approach to electric potential feature extraction is presented. Then the robustness of the extracted feature to various attacks is established.

Suppose a $b \times b$ block, which for modeling purposes only is considered as a complete image existing in isolation, is divided into three concentric squares $sq_i,\ 1 \le i \le 3$ of distinct sides $s_i,\ 1 \le i \le 3$ respectively as shown in Fig. 3. Both b and $s_i,\ 1 \le i \le 3$ should be odd in order to have a pixel at the centroid. Each concentric square should in turn be considered as a complete image existing in isolation.

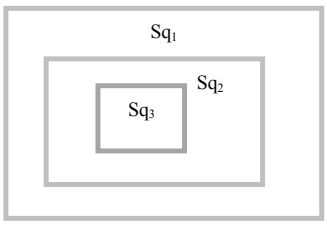

Fig. 3 Block division into three concentric squares.

We define a feature vector, $\vec{h} = h_1 h_2$, in which the individual components $h_i, i = 1,2$ are computed as follows:

1) Each concentric square is represented by the net electric potential of the pixel which is located at the centroid of the square. The centroid pixel's electric potential is as a result of interacting with all the pixels within the square. Because the squares are concentric, their centroids coincide.
2) Let $V_i,\ 1 \le i \le 3$ be the electric potentials of the centroid pixels of the squares $sq_i,\ 1 \le i \le 3$, then $h_i = \left\lfloor \Gamma \frac{V_{i+1}}{V_i} \right\rfloor,\ 1 \le i \le 2$ for some positive integer Γ and $\lfloor\ \rfloor$ is the floor operator.
3) Normalize the components $h_i, i = 1,2$ to unsigned integers in the range [0-255].

By definition the complete expression for the component h_1 of the extracted feature vector $\vec{h} = h_1 h_2$ is given by the following equation:

$$h_1 = \left\lfloor \Gamma \frac{V_2}{V_1} \right\rfloor = \left\lfloor \Gamma \frac{\sum_{i \in 1, k_2 | i \ne j} \frac{q_i}{r_{ji}}}{\sum_{i \in 1, k_1 | i \ne j} \frac{q_i}{r_{ji}}} \right\rfloor \tag{6}$$

where $k_i,\ 1 \le i \le 2$ are the pixel populations within the concentric squares $sq_i,\ 1 \le i \le 2$ respectively.

For any features to be of practical use there is need to establish the invariance of the features to various attacks, such as scaling, translation, rotation, noise addition, lossy compression. In case of the defined features, it suffices to show the invariance of only the component h_1 to the various attacks. The argument can easily be extended to the other component. It should be stated that the overall robustness of the CMIF detection algorithm proposed in this paper to various attacks is a two-fold defense. First, we extract robust features. Secondly a robust duplication verification method is employed during the duplication verification stage. The two arsenals complement each other against various attacks.

To model a scaling attack, we suppose the block is scaled by a factor β. Consequently the component h_1 defined in (6) is modified as shown in (7).

From (7), it is clear that the component h_1 is invariant to scaling. By extension, it follows that the defined feature $\vec{h} = h_1 h_2$ is robust to scaling attacks.

$$h_1 = \left\lfloor \Gamma \frac{\sum_{i \in 1, k_2 | i \ne j} \frac{q_i}{\beta r_{ji}}}{\sum_{i \in 1, k_1 | i \ne j} \frac{q_i}{\beta r_{ji}}} \right\rfloor = \left\lfloor \Gamma \frac{\frac{1}{\beta} \sum_{i \in 1, k_2 | i \ne j} \frac{q_i}{r_{ji}}}{\frac{1}{\beta} \sum_{i \in 1, k_1 | i \ne j} \frac{q_i}{r_{ji}}} \right\rfloor = \left\lfloor \Gamma \frac{\sum_{i \in 1, k_2 | i \ne j} \frac{q_i}{r_{ji}}}{\sum_{i \in 1, k_1 | i \ne j} \frac{q_i}{r_{ji}}} \right\rfloor \tag{7}$$

The robustness of the feature vector $\vec{h} = h_1 h_2$ to translation attacks is obvious because the ratio and floor operations have some quantizing effect on the components of the feature vector [12].

With reference to the work by Zimba and Xingming [12]

the defined feature vector $\vec{h} = h_1 h_2$ is robust to rotation. For example, let the block $B^{'}$ be the result of rotating the block of Fig. 3 through 90^0 clockwise and let $sq_1^{'}$, $sq_2^{'}$, and $sq_3^{'}$ be the concentric squares of $B^{'}$, then it is clear that $sq_i^{'} = sq_i$, $1 \le i \le 3$. It follows that the feature vector $\vec{h} = h_1 h_2$ is robust to such a rotation. The argument also holds, for practical purposes, for rotation through arbitrary angles because the majority of each square's populace will still be within the square at any rotation.

Next we establish the tolerance of the defined features to noise addition attacks as follows. Assuming that the per pixel additive white Gaussian noise (AWGN) is a zero-mean independent and identically distributed random variable with a variance n, then the component h_1 is modified as follows:

$$\begin{aligned} h_1 &= \left\lfloor \Gamma \frac{\sum_{i\in 1,k_2 | i\neq j} \frac{q_i + n_i}{r_{ji}}}{\sum_{i\in 1,k_1 | i\neq j} \frac{q_i + n_i}{r_{ji}}} \right\rfloor \\ &= \left\lfloor \Gamma \frac{\sum_{i\in 1,k_2 | i\neq j} \frac{q_i}{r_{ji}} + \left(\left(\sum_{i\in 1,k_2 | i\neq j} \frac{n_i}{r_{ji}} \right) \approx 0 \right)}{\sum_{i\in 1,k_1 | i\neq j} \frac{q_i}{r_{ji}} + \left(\left(\sum_{i\in 1,k_1 | i\neq j} \frac{n_i}{r_{ji}} \right) \approx 0 \right)} \right\rfloor \\ &= \left\lfloor \Gamma \frac{\sum_{i\in 1,k_2 | i\neq j} \frac{q_i}{r_{ji}}}{\sum_{i\in 1,k_1 | i\neq j} \frac{q_i}{r_{ji}}} \right\rfloor \end{aligned} \tag{8}$$

Equation (8) shows that the component h_1 is robust to noise addition. Besides, the floor operation has the quantizing effect on the component h_1. Consequently, the feature vector $\vec{h} = h_1 h_2$ is robust to noise.

At the same time, JPEG compression and Gaussian blurring attacks only slightly change the low frequency components of the image signal and discard high frequency components. Hence due to ratio and floor operations, the defined feature vector $\vec{h} = h_1 h_2$ is also robust to these operations.

C. Affine Transformation

The need for geometric manipulation of images is ubiquitous in 2D image processing. The intentions may be as innocent as removing optical distortions introduced by a camera or as malicious as removing traces of duplication attacks. The treatment of such manipulations within the framework of geometric concepts requires sufficient mathematical description of an object or shape in an image. The simplest and most direct approach in mathematically describing a shape is to locate a finite number N of points along its boundary and concatenate them into a point distribution matrix, PDM, [13]. Consider the PDM, P, described in terms of N Euclidean coordinate pairs as follows

$$P = \begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_N \\ y_1 & y_2 & y_3 & \cdots & y_N \end{bmatrix} \tag{9}$$

The 2D affine transformation of the PDM, P, into a new PDM, $P^{'}$, can be achieved mathematically by simply multiplying each column of P by a 2×2 transforming matrix T as follows

$$\begin{bmatrix} x^{'} \\ y^{'} \end{bmatrix} = T \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \tag{10}$$

It must be stated that we are interested in those affine transformations that change only the PDM of a given shape but do not necessarily change the essential shape itself. These shape-invariant operations such as translation, rotation and scaling are often applied in malicious geometric image attacks. Note that the simple affine transformation of (10) does not include translation operation. The basic translation operation is defined at individual coordinate level by the following vector addition.

$$\begin{bmatrix} x^{'} \\ y^{'} \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} \alpha_x \\ \alpha_y \end{bmatrix} \tag{11}$$

The translation operation can be incorporated into matrix multiplication by mapping the 2D Euclidean coordinate pair into homogenous coordinates [14] of higher dimension. In the homogenous system, affine transformation takes the following general form

$$\begin{bmatrix} x^{'} \\ y^{'} \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} \tag{12}$$

Whether one is using 2D Cartesian coordinates or homogenous coordinates, the tracing of the affine transformation depends on knowing the affine transformation parameters α_{ij}.

D. Same Affine Transformation Selection

The idea of recovering parameters of affine transformation of a region in an image was once presented by Amerini et al. [15]. In their work [15], the authors use Maximum Likelihood estimation of homography [14] to estimate the parameters of the affine transformation in homogenous coordinates.

However, a simple and straightforward approach to recovering the parameters of the affine transformation of a

region in an image in 2D Cartesian coordinates, named the same affine transformation selection, SATS, is proposed by Christlein et al. [16]. SATS is an alternative selection and verification method to the common shift vector method. Like shift vector, SATS has an outlier filtering property. However, SATS is insensitive to affine transformation in that it recovers the affine transformation parameters of a geometrically manipulated region at a cost of only a slightly increased computational time. Hence SATS is a better option for the verification of the duplicated regions which have been affected by translation, rotation or scaling. The detailed SATS method is as follows:

Let B_{i1} and B_{i2} be $b \times b$ matching blocks whose centers, in row vector form, are $\vec{c}_{i1}$ and $\vec{c}_{i2}$ respectively. If B_{i2} is a result of an affine transformation of B_{i1} then

$$\vec{c}_{i2} = \vec{c}_{i1}.A + \vec{s}, \tag{13}$$

The 2×2 matrix A in (13) consists of the two rotation and two scaling parameters and the vector $\vec{s}$ consists of the two translation parameters. Let $\vec{h}_i = (\vec{h}_{i1}, \vec{h}_{i2})$ be a vector of the feature vectors $\vec{h}_{i1}, \vec{h}_{i2}$ extracted from the matching blocks B_{i1} and B_{i2} respectively, then a set of three such vectors as $\vec{h}_i$ is enough to initially approximate all the six parameters of the affine transformation. The concise presentation of the SATS algorithm is shown in Table I.

The run time complexity of the SATS algorithm is clearly determined by the number of the overlapping blocks tiled over the image.

TABLE I
SATS ALGORITHM

for every matched pair $\vec{h}_1 = (\vec{h}_{11}, \vec{h}_{12})$ **do**
  Let the hypothesis-set $H = \{\vec{h}_1\}$
  for matches $\vec{h}_i$ **do**
    if $d(\vec{c}_{11}, \vec{c}_{i1}) < t_1$ and $d(\vec{c}_{12}, \vec{c}_{i2}) < t_1$ **then**
      $H = H \bigcup \vec{h}_i$;
    end if
  end for
  if $|H| < 3$ **then**
    continue;
  end if
  From H compute A and $\vec{s}$.
  for every $\vec{h}_i$ where $\vec{c}_{i1}$ is close to matched blocks in H **do**
    Compute $\vec{c}_{i2} = \vec{c}_{i1}.A + \vec{s}$, as in (13)
    if $d(\vec{c}_{i2}, \vec{c}_{i2}) < t_1$ **then**
      $H = H \bigcup \vec{h}_i$;
      if $|H| \bmod 10 \equiv 0$ **then**
        re-compute A and $\vec{s}$ to stabilize the estimate
      end if
    end if
  end for
  if $|H| > t_2$ **then**
    store A, $\vec{s}$ and mark the blocks in H as copy-moved
  end if
end for

III. The Proposed Algorithm

The proposed CMIF detection algorithm firstly performs the DWT of a suspicious image and extracts only the low frequency subband. The extracted subband is then mapped to the virtue electrostatic field where robust feature vectors are computed according to Section II (B)

1) Let $F(x, y)$ be a suspicious image with $k_3 = M \times N$ pixels per channel.
2) Initialize the following parameters:
(i) $b \times b$, the block size.
(ii) l, the level of orientation.
(iii) t_1, separation threshold.
(iv) t_2, connectivity threshold.
3) Perform an $l-$level DWT on the $F(x, y)$ to obtain subbands $F_\alpha^l(u, v)$ where $\alpha \in \{LL, LH, HL, HH\}$ represents orientation and a positive integer l is the level of the orientation. Each $F_\alpha^l(u, v)$ has a reduced image space of $k_2 = r \times c \approx \frac{k_3}{4^l}$ pixels. The pixels are actually DWT coefficients normalised to unsigned integers in the range [0-255].
4) Extract only $F_{LL}^l(u, v)$ to reduce image space to $k_2 = r \times c \approx \frac{k_1}{4^l}$ pixels.
5) Perform the bijection $g : F_{LL}^l(x, y) \to Q(u, v)$ according to Section II *A*.
6) Slide a fixed $b \times b$ window on $Q(u, v)$ pixel by pixel from top-left corner to bottom-right corner, in a raster scan order, resulting in $k = (r - b + 1)(c - b + 1)$ overlapping blocks.
7) Each of the k $b \times b$ block considered as a complete image existing in isolation is divided into four concentric squares sq_i, $1 \le i \le 4$ of distinct sides s_i, $1 \le i \le 4$ respectively similar to the division shown in Fig. 3. Each concentric square is considered as a complete image

existing in isolation. Compute a feature vector, $\vec{h} = h_1 h_2 \ldots h_6$, as follows:

(i) Each concentric square is represented by the electric potential of the centroid pixel due to interaction with all the pixels within the square.

(ii) Let V_i, $1 \le i \le 4$ be the electric potentials of the centroid pixels of the squares $sq_{i,}$ $1 \le i \le 4$, then

$$\vec{h} = \left\lfloor \Gamma \frac{V_2}{V1} \right\rfloor \left\lfloor \Gamma \frac{V_3}{V_1} \right\rfloor \left\lfloor \Gamma \frac{V_3}{V_2} \right\rfloor \left\lfloor \Gamma \frac{V_4}{V_1} \right\rfloor \left\lfloor \Gamma \frac{V_4}{V_2} \right\rfloor \left\lfloor \Gamma \frac{V_4}{V_3} \right\rfloor$$

(iii) Normalize the components $h_i, i = 1,2,\ldots,6$ to unsigned integers in the range [0-255].

(iv) Form a $k_1 \times 6$ matrix H whose rows are the k_1 feature vectors, $\vec{h} = h_1 h_2 \ldots h_6$

8) Sort the rows of the matrix H using Radix Sort.

9) Performed SATS algorithm on the sorted matrix H according to Section II (D) to verify region duplications and to filter out outliers.

10) Finally, filter out isolated matching blocks through morphological opening to obtain the final results.

The following are the credits of the proposed algorithm over existing CMIF detection algorithms. 1) The algorithm introduces a novel and effective approach to CMIF detection, the virtual electrostatic field based approach. 2) Normally, the computational complexity of a CMIF detection algorithm converges to the complexity of the feature sorting method which in turn is a function of the dimensions of the image. Consequently, most CMIF detection methods which operate in the spatial domain are generally more complex [1], [17]. The algorithm reduces the dimension of the image through DWT. This overly reduces the complexity of the algorithm. 3) Another remarkable reduction in the complexity of the proposed algorithm is achieved through sorting the extracted features using the Radix Sort which has the complexity of $O(tk_1)$ instead of the common Lexicographic Sort which would have the complexity of $O(tk_1 \log k_1)$ for the same task. 4) At the same time, the extracted features are robust to additive noise, JPEG compression, Gaussian blurring and affine transformation. 5) Finally, a more robust region duplication verification approach, SATS, which is insensitive to affine transformation, is employed. Therefore, the proposed algorithm is not only non-complex but also two-fold robust to attacks.

IV. Experimental Results

To validate the proposed algorithm, experiments are conducted on a dataset of 300 images sourced mostly from *www.freefoto.com*. Most images have the dimensions of 256×256 pixels. When a $1-$level DWT, Haar, is performed on the images, the dimensions of the images reduce to 128×128 pixels. The level of orientation is restricted to $l = 1$. The size of the block is set to $b \times b = 17 \times 17$ pixels throughout the experiments. The distance of the matching block pairs is set to $t_1 = 17$ and the least frequency of connected matches is set to $t_2 = 50$.

Fig. 4 shows examples of the detection results by the proposed. In the left column are the original images; in the middle column are the forged images in which the duplicated regions are affected by various attacks; the right column shows the results from the proposed algorithm.

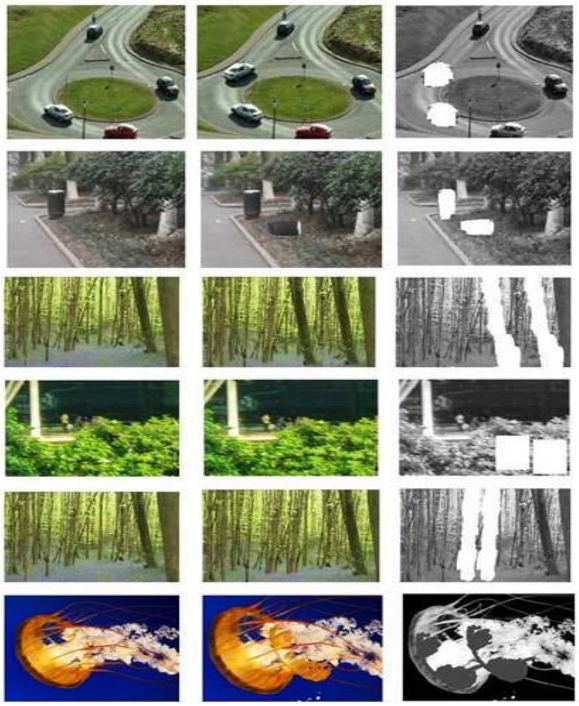

Fig. 4 Detection results by the proposed algorithm

We assess the performance of the proposed CMIF algorithm using the following stricter method. Let D_1 and D_2 be an original region and a duplicated region respectively, R_1 and R_2 be the respective output regions mapped by the proposed algorithm, then the accuracy r and false negative w of the detection are respectively defined in (14) and (15) as follows:

$$r = \frac{|R_1 \cap D_1| + |R_2 \cap D_2|}{|D_1| + |D_2|} \tag{14}$$

$$w = \frac{|R_1 \cup D_1| + |R_2 \cup D_2|}{|D_1| + |D_2|} - r \tag{15}$$

The results by the proposed algorithm for the set of 300 images whose duplicated regions are affected by various forms of attacks are shown in Table III. The results demonstrate that the algorithm has, on average, recommendable accuracy in cases where the duplicated regions are merely translated or reflected. High detection rates are also registered in cases where the duplicated regions are

affected by JPEG compression or additive noise. There is a fairer accuracy where the duplicated regions are affected by rotation, or combined forms of affine transformation. The accuracy of the algorithm is relatively low in cases where duplicated regions are affected by scaling or rotation through arbitrary angles. The lower detection results are due to local pixel exchanges which occur when the duplicated regions attacked by scaling or rotation through arbitrary angles are scanned by the fixed window. In general, however, we note that the accuracy of the algorithm increases with an increase in the size of the duplicated regions.

We take an extra effort to compare the proposed algorithm with the existing CMIF algorithms in terms of feature extraction approach, number of blocks required to cover the whole image, feature vector lengths and run time complexity. The comparison results are shown in Table III. For comparison purposes, consider a 256×256 image tiled with 8×8 overlapping blocks. Recall that $k_1 \approx \frac{k}{4^l}$ where $k = (M - b + 1)(N - b + 1)$. Because the dimensions of the image are reduced through DWT and the feature vectors are sorted using Radix Sort, the run time complexity of the proposed method is lower than those of the existing methods.

TABLE II
RESULTS OF THE PROPOSED ALGORITHM FOR A SET OF 300 IMAGES

Forms of Attacks		Average Detection Rate of Duplicated Regions of Various Sizes (pixels) and Forms of Attacks					
		32×32		48×48		64×64	
		r	*w*	*r*	*w*	*r*	*w*
Translation		1.0000	0.0559	1.0000	0.0523	1.0000	0.0309
JPEG	100	1.0000	0.0398	1.0000	0.0371	1.0000	0.0333
Quality	80	0.9884	0.0867	0.9893	0.0843	0.9997	0.0757
	60	0.9723	0.1341	0.9791	0.1278	0.9826	0.1188
	40	0.9563	0.1273	0.9622	0.1207	0.9678	0.1152
SNR	40	0.9900	0.1107	0.9947	0.1069	0.9990	0.0892
(dB)	32	0.9841	0.1196	0.9880	0.1121	0.9896	0.1013
	24	0.9628	0.1458	0.9691	0.1379	0.9733	0.1301
	20	0.9015	0.1497	0.9229	0.1443	0.9319	0.1305
Scaled		0.7677	0.4872	0.7745	0.4746	0.7841	0.3994
Reflection		1.0000	0.0659	1.0000	0.0611	1.0000	0.0442
Rotation	60˚	0.8240	0.2413	0.8465	0.1883	0.8495	0.1739
	90˚	0.9992	0.1168	1.0000	0.0999	1.0000	0.0935
	120˚	0.8156	0.2174	0.8183	0.2101	0.8273	0.1749
Mixed affine transformation		0.8669	0.2272	0.8723	0.2117	0.8811	0.1792

TABLE III
COMPARISON WITH EXISTING RELATED ALGORITHMS

Algorithm	Feature Approach	Number of 8x8 blocks	Feature vector length.	Run time complexity for a given k
Fridrich	Quantized DCT	62,001	64	$O(64 \log k)$
Popescu	PCA	62,001	32	$O(32 \log k)$
Li	DWT&SVD	14,641	8	$O(8 \log k_1)$
Zimba	Block Characteristic	14641	7	$O(7k_1)$
Proposed	EFT-based	14,641	6	$O(6k_1)$

V. CONCLUSION

In this paper a novel copy-move image forgery, CMIF, detection method has been proposed. The proposed method has presented a new approach which relies on electrostatic field theory, EFT. Solely for the purpose of reducing the dimension of the image, the proposed algorithm initially performs discrete wavelet transform, DWT, of a suspicious image and extracts only the approximation subband. The extracted subband is then bijectively mapped onto a virtual electrostatic field where concepts of EFT are utilized to extract robust features. The extracted features are invariant to additive noise, JPEG compression, and affine transformation. Finally, same affine transformation selection, SATS, a duplication verification method, is applied to detect duplicated regions. SATS is a better option than the common shift vector method because SATS is insensitive to affine transformation. Consequently, the proposed CMIF algorithm is not only fast but also more robust to attacks compared to the existing related CMIF algorithms. The experimental results have shown high detection rates.

REFERENCES

[1] H. Farid, "A Survey of Image Forgery Detection," in *Signal Proc. Magazine*, vol. 26, no. 2, 2009, pp.16-25.
[2] A.C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Resampling", *IEEE Trans. Signal Processing,* vol. 53, pp. 758-767, 2005.
[3] H. Sencar and N. Memon, "Overview of State- of- the- art in Digital Image Forensics," *Algorithms, Architectures and Information Systems Security*, pp. 325-344, 2008.
[4] T. Ng, S. Chang, C. Lin, and Q. Sun, " Passive-Blind Image Forensics," *Multimedia Security Technologies for Digital Rights Management*, Academic Press, pp. 383-412, 2006.
[5] J. Fridrich, D. Soukal and J. Lukas, "Detection of Copy-Move Forgery in Digital Images," in *2003 Proc. Digital Forensic Research Workshop*.
[6] S. Bayram, T. Sencar and N. Memon, "An Efficient and Robust Method for Detecting Copy-move Forgery," *ICASSP*, pp. 1053-1056, 2009.
[7] G. Li, Q. Wu, D. Tu, and S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD," in *Proc. IEEE International Conf. Multimedia and Expo*, Beijing China, 2007, pp. 1750-1753.
[8] G.H. Abdel-Hamid and Y.H. Yang, "Electrostatic Field-based Detection of Corners of Planar Curves," *in Proc. 1993 Canadian Conf. Electrical and Computer Engineering*. Vancouver, 1993.
[9] D. Halliday and R. Resnick, *Physics Part III. Willey International Edition*, Wiley, New York, 1962.
[10] P. Silvester, *Modern Electromagnetic Fields*, Prentice-Hall, 1967.
[11] I.S. Grant and W.R. Phillips, *Electromagnetism*, Wiley, New York, 1990
[12] M. Zimba and S. Xingming, "Fast and Robust Image Cloning Detection Using Block Characteristics of DWT Coefficients," *JDCTA: International Journal of Digital Content Technology and its Application*s, Vol. 5, No. 7, 2011, pp.359-367.
[13] C. Solomon and T. Breckon, *Fundamentals of Digital Image Processing,* Wiley-Blackwell, 2011.
[14] R.I. Hartley and A. Zisserman, *Multiple View Geometry in Computer Vision*, Cambridge University Press, 2nd edition, 2004.
[15] I. Amerini, L. Ballan, R. Caldelli, A.D. Bimbo and G. Serra, "Geometric Tampering Estimation by Means of a Sift-Based Forensic Analysis," *International Conf. Acoustic Speech and Signal Processing*, Dallas TX, USA, March 14-19, 2010.
[16] A.V. Christlein, C. Riess and E. Angelopoulou, "On Rotation Invariance in Copy-Move Forgery Detection," in *Proc. IEEE Workshop, Information Forensics and Security*, Seattle USA, 2010.
[17] C. Riess and E. Angelopoulou, "Scene Illumination as an Indicator of Image Manipulation," *12th International Workshop on Information Hiding*, Springer, Vol. 6387, 2010, pp. 66-80.

Michael Zimba received BSc in Electrical Engineering from University of Malawi in 2005; MSc in Information Theory, Coding and Cryptography from

Mzuzu University, Malawi, in 2009; and PhD in Signal Processing and Analysis from Hunan University, China, in 2012. He is currently a Lecturer with the Department of Physics at Mzuzu University, Malawi.

Darlison Nyirenda received BSc (Ed) Mathematics from Mzuzu University, Malawi, in 2007; MSc in Information Theory, Coding and Cryptography from Mzuzu University, Malawi, in 2011; PGDip in Mathematical Sciences from African Institute for Mathematical Sciences, South Africa in 2011; MSc in Mathematics from Stellenbosch University, South Africa in 2013; He is currently an Associate Lecturer and a PhD Student in the School of Mathematics at University of Witwatersrand, South Africa.