Electromagnetismlike Mechanism Descriptor with Fourier Transform for a Passive Copy-move Forgery Detection in Digital Image Forensics

Sajjad Dadkhah[1], Mario Köppen[1], Hamid A. Jalab[2], Somayeh Sadeghi[2], Azizah Abdul Manaf[3] and Diaa Uliyan[4]

[1]*Kyushu Institute of Technology, 680-4 Kawazu, Iizuka, 820-8502, Fukuoka, Japan*

[2]*Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia*

[3]*Advanced Informatics School, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia*

[4]*Faculty of Information Technology, Middle East University, Amman, Jordan*

dsajjad2@liveutm.onmicrosoft.com, mkoeppen@ieee.org, hamidjalab@um.edu.my,
{ssomayeh, diaa_uliyan}@siswa.um.edu.my, azizaham.kl@utm.my

Keywords: Authentication, Digital Forensics, Forgery Detection, Image Analysis, Image Processing.

Abstract: Copy-move forgery is a special type of forgery that involves duplicating one region of an image by covering it with a copy of another region from the same image. This study develops a simple and powerful descriptor called Electromagnetismlike mechanism descriptor (EMag), for locating tampered areas in copy-move forgery on the basis of Fourier transform within a reasonable amount of time. EMag is based on the collective attraction-repulsion mechanism, which considers each images pixel as an electrical charge. The main component of EMag is the degree of the attraction-repulsion force between the current pixel and its neighbours. In the proposed algorithm, the image is divided into similar non-overlapping blocks, and then the final force for each block is evaluated and used to construct the tampered image features vector. The experimental results demonstrate the efficiency of the proposed algorithm in terms of detection time and detection accuracy. The detection rate of the proposed algorithm is improved by reduction of false positive rate (FPR) and increment of true positive rate (TPR).

1 INTRODUCTION

Over the recent years, the improvement of the computer knowledge and digital imagery equipment expanded the use of digital images into numerous areas, such as TV, journalism, medical imaging and etc (Fridrich, 1999). Moreover, the professional image processing tools such as Photoshop, which enable the easy manipulation of the digital images, have become widely available for free. The existence of such powerful tools raise suspicions on the integrity of the digital images (Jing and Shao, 2012; Dadkhah et al., 2014; Ardizzone et al., 2015).

Digital image forgery is accordingly defined as a tool that mainly solve the integrity problem of the digital images. Image forgery is the science of changing parts of an image to create a fake image for illegal purposes. Image forgery is divided into three groups: (i) *Image splicing* creates a fake image by cutting a part of the image and pasting it to another image (Chen et al., 2007). (ii) *Image retouching* is common in magazine photo editing and does not visibly change the image which is the least corrupting type of digital image forgery (Li and Wang, 2012). (iii) *Copy-move* forgery which is the most significant digital forgery, involves duplicating one region of an image by covering it with a copy of another region from the same image (Piva, 2013).

Copy-move forgery is widely utilized for illegal purposes, in order to conceal or emphasize certain image details by cloning an area of an image to a different area. This type of forgery has become notorious, as its detection requires greater technical skills. It is because the source and destination of the forged image are same (Fridrich et al., 2003; Kirchner et al., 2015). This paper focuses on this category of forgery. Furthermore, various detection methods have been proposed to detect copy-move forgery attacks. Different digital image forgery methods are investigated in this study. The proposed algorithm in this research develops a simple and powerful descriptor for locating tampered regions in copy-move forgery

Dadkhah, S., Köppen, M., Jalab, H., Sadeghi, S., Manaf, A. and Uliyan, D.
Electromagnetismlike Mechanism Descriptor with Fourier Transform for a Passive Copy-move Forgery Detection in Digital Image Forensics.
DOI: 10.5220/0006232206120619
In *Proceedings of the 6th International Conference on Pattern Recognition Applications and Methods (ICPRAM 2017)*, pages 612-619
ISBN: 978-989-758-222-6

on the basis of Fourier transform within a reasonable amount of time.

The proposed *EMag* descriptors utilizes an attraction-repulsion mechanism to move the sample points towards the optimality. *EMag* has both been successfully applied to the solution of different sorts of engineering problems such as resource constraint project scheduling problems (Turabieh and Abdullah, 2011), image processing (Jalab and Abdullah, 2013),(Cuevas et al., 2012) and neural network training (Jalab and Shaker, 2014).

Since the Electromagnetism-like Mechanism is a new heuristic algorithm for global optimization and there are fewer investigations about this algorithm until now, the authors of this research are motivated to utilize the *EMag* algorithm as an image feature descriptor to be used for image copy-move detection. The remainder of this paper is organized as follows: Section 2 presents related work on copy-move forgery detection. Section 3 explains the details of the proposed method. Section 4 presents the Performance analysis and experimental results. The research conclusions are presented in Section 5.

2 RELATED WORK

As mentioned in previous section, the source and destination of the forged image in copy-move forgery is same, such that detecting the forgery by using the naked eye is almost impossible (Fridrich et al., 2003). Some operations (e.g., rotation, JPEG compression, resizing, and noise) are usually applied to the original part before pasting. These post- processing transformations make the detection process more difficult, for instance JPEG compression transmitted digital images to compressed format. A forgery detector should be robust to all manipulations and applicable to compressed images (Wu and Chang, 2002). Thus, the detection of forgery using methods that search for incompatibilities inside the digital image is impossible (Farid and Lyu, 2003). Several copy-move forgery detection techniques have been proposed to solve this issue.

A copy-move detection method is proposed by (Ardizzone and Mazzola, 2009) that utilize bit-plane analysis. In this method, the image is analyzed in the bit-plane domain. Blocks of bits are encrypted using the ASCII code for each bit-plane, and the direction of the strings is examined instead of the original bit-plane. The cycle is classified, and similar groups of bits are removed as doubtful areas, which are then passed on to the next plane for processing. The output of the previous planes shows where the image is changed. The execution time in this method is reasonable, which is an advantage. However, bit-plane analysis does not work with JPEG images because JPEG compression and bit-plane representation are not related. Bit-plane analysis is also ineffective when the pasted area is rotated or scaled.

Authors in (Lin et al., 2009) proposed a method that uses a radix sort. This approach works in a manner that is similar to other block generation methods. Radix sorting is utilized instead of lexicographic sorting to improve time complexity and to enhance the resistance to various noises and compressions (e.g., JPEG compression and Gaussian noise). However, radix sorting does not deal with rotation arbitrary angles and cannot successfully detect small copied regions.

Ryu (Ryu et al., 2010) proposed a detection system based on Zernike moments. Zernike moments are used to extract the feature vectors of an image block. Then, the features are sorted lexicographically and adjacent vectors are located. This method works well in terms of robustness to noise and rotation because Zernike moments are algebraically invariant against rotation, noise, and information content. However, it is weak against other transformations, such as scaling or JPEG compression.

Hu (Hu et al., 2011) proposed a detection method based on the discrete cosine transform (DCT). His method is the improved version of Fridrich algorithm, which is based on DCT. In this method, features of each image block are compressed together and determine whether the number of matched blocks in a certain area is more than a specific threshold. For improving matching accuracy, lexicographical sorting algorithm based on distance is proposed. This method is not robust to rotation but it is robust to noise and blurring.

Liu (Liu et al., 2011) proposed a passive image authentication method that can detect duplicated areas under rotation, which uses round blocks and Hu moments to determine forged areas. The image is decomposed using a Gaussian pyramid to create sub-images. Low frequency sub-images are chosen to overcome possible distortion caused by noise contamination and JPEG compression. Subsequently, each sub-image is divided into several non-overlapping round blocks. Hu moment features are extracted from these blocks and used to match features. Finally, the forged regions are located by comparing the shift vectors and copy-region areas. The method mainly is not robust to resizing or cropping images before the image is pasted to another area.

Hou (Hou et al., 2012) proposed a copy-move detection algorithm by using phase correlation within an image. The advantage of this method is its low com-

putational complexity. It is also able to detect small tampered areas because it uses a larger overlap ratio. Although, phase-correlation based methods are able to detect small areas. However, if the image contains multiple forged regions, it cannot detect copy-move areas.

Mishra (Mishra et al., 2013) presented a tamper detection method based on speeded up robust features (SURF) and hierarchical agglomerative clustering (HAC). SURF is used to speed up the process of keypoint extraction while using HAC to group up keypoints. Authors used Haar wavelets to compute descriptors which are robust to illumination changes. This method is robust to noise and JPEG compression but the result of their proposed algorithm is not satisfactory in terms of the true positive detection rate.

Silva (Silva et al., 2015) proposed a digital image tamper detection algorithm based on multi-scale analysis and voting processes of the image. In their method, interest points are extracted from the image based on geometric constraints, then a multi-scale representation are created, and formed the groups tested by utilizing a robust descriptor. Their proposed method is robust to rotation and scale but it is not good enough for JPEG compression attack. Robust copy-move forgery detection is essential; the detector should be robust to post-processing operations and some types of transformation. Most existing methods cannot deal with all these manipulations and are often computationally expensive.

3 PROPOSED METHOD

In this paper an efficient approach for detecting copy-move forgery in digital images by proposing a new *EMag* descriptor for locating copy-move tampered regions is presented. The proposed Electromagnetism Mechanism Descriptor with Fourier Transform is described in the following stages: *EMag* Block feature extraction, Block feature matching and tamper localization.

3.1 *EMag* Block Feature Extraction

The proposed *EMag* algorithm for Copy-move detection is illustrated in Figure 1 . As illustrated in Figure 1, the general procedure of the proposed algorithm are as follows:

1. Dividing the digital image into blocks of pixels with appropriate size.
2. Extraction of certain feature of each block by proposed *EMag* algorithm and Fourier transformation.
3. Block feature matching and tamper localization. The similar blocks are connected to localize the copied region when tampering is detected.

The proposed algorithm in this paper has explored a special feature inside digital images which is influenced by Fourier transformation. The proposed *EMag* algorithm extract the Electromagnetism descriptors within each blocks. Finally, the final force for each block is calculated and used to construct the tampered image features vector. However, the details of the proposed *EMag* Block feature extraction are described in the following steps:

Step 1. Preprocessing. The original image I is converted into grayscale by equation (1).

$$I = 0.299R + 0.587G + 0.114B \quad (1)$$

where R, G, and B are three channels of the input color image and I is its luminance component (Lin et al., 2009).

The grayscale image is then divided into similar-sized non-overlapping blocks *($B \times B$ pixels)*, which are smaller than the sizes of the detected duplicated regions. The default block size is 21×21 pixels.

The proposed method is analysed to determine the best block size value for attaining the highest *TPR* and lowest *FPR* scores. Specifically, the block size value affects the number of matched points. A proper block size

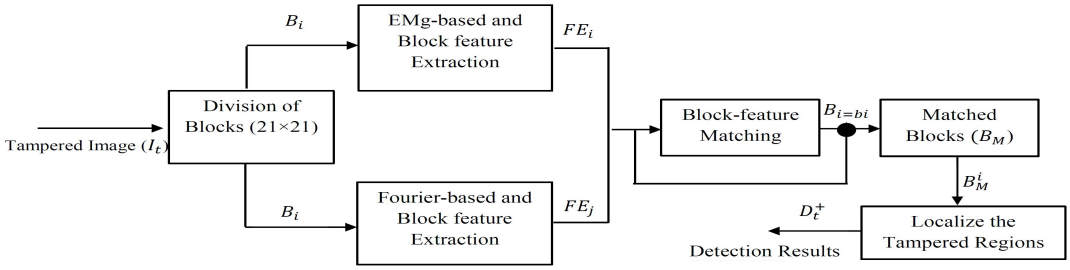


Figure 1: The general procedure of the proposed copy-move forgery detection.

value is therefore required to reduce the number of false matches. The goal is to maximise the *TPR* value while suppressing *FPR*. The best *FPR* is the lowest value which means only a few percentage of the original images are incorrectly recognized as forged ones, while the best *TPR* is the highest value which means all the forged images are correctly recognized as forged.

Several block size values are tested to gauge their influences on the identification of the forged and original images, the best block size value is empirically found to be 21×21, and the best *FPR* is 6.2% and the best *TPR* is 95.4%. The number of blocks in the image is calculated by *[M/B]×[N/B]* where *M*, *N* are the image pixels.

Step 2. Dividing into sub-blocks for *EMag* Process. Each block size $B \times B$ is divided into non-overlapping sub-blocks of size 3×3.

Step 3. Electromagnetism descriptors. For each block size $B \times B$ pixels, the total electrical force *Fi* is calculated. The total electrical force *Fi* is calculated for each 3×3 sub-block.

In the *EMag* implementation, the charge of pixels q represents the value of image pixel. However, F_i is calculated based on the electromagnetism theory which states that the force exerted on a point charge via other charges is inversely proportional to the distance between the charges and directly proportional to the product of their charges. The overall resultant attraction-repulsion force for each image block determines the actual feature of forgery image. The final force vector for each image block is evaluated under the Coulombs law by equation (2).

$$F_i = \sum_{j \neq i}^{n} \left\{ \begin{array}{l} \left(\frac{(x_i \times x_j)}{\|x_i - x_j{}^2\|} \; if \quad f(x_j) < f(x_i) \right) \\ \left(\frac{(x_i \times x_j)}{\|x_j - x_i{}^2\|} \; if \quad f(x_j) \geq f(x_i) \right) \end{array} \right\} \quad (2)$$

where *i=1,2,..,n (n=9)*, $\times$ is multiplication, and x_j , x_i are the value of the center pixel in the image sub-block and its surrounding pixels, respectively. In this formula, $f(x_j) < f(x_i)$ represents attraction and $f(x_j) > f(x_i)$ corresponds to repulsion.

Step 4. Feature extraction by Fourier transform. A two-dimensional discrete Fourier transform is applied to the extracted *EMag* features, which are translation invariant. Fourier transform is utilized to formulate a function with an intensity signal across the image. This function is disjointed into a sum of orthogonal functions. The two-dimensional discrete Fourier transform of *f(m, n)* is given by equation (3).

$$F(k,l) = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} f(m,n) e^{-jkm} e^{-jln} \quad (3)$$

where *f(m,n)* is the image in the spatial domain, and the exponential term is the basis function corresponding to each point *F(k,l)* in the Fourier space. k and l are the frequency variables. *F(k,l)* is frequency domain representation of *f(m, n)*. *F(k,l)* is a complex valued function that is periodic both in k and l with a period of 2π and period range of $-\pi \leq k, l \leq \pi$ (Rosenfeld and Kak, 2014).

Fourier transform is applied to each block of the image B_i to perform a correlation, which can help in identifying similar correlation values in an image and locate the location of the matched blocks.

3.2 Block Feature Matching and Tamper Localization

The procedure of the proposed Block feature matching and tamper localization algorithm is described in the following steps:

Step 1. Correlation computation for each blocks. Correlation C_i is computed between every two blocks which is defined as the convolution of the individual blocks to locate the features within the image.

Step 2. Sorting correlation values. For faster tamper localization procedure all correlation values C_Bi has to be sorted. All correlations are sorted with a *k-d* tree (Bentley, 1975) and saved in a matrix.

Step 3. Block matching. All blocks are compared after the sorting to determine their similarity on the basis of the block-matching threshold. The matching process works by computing where the maximum correlation value exceeds the threshold and then determining whether the two blocks are similar.

Step 4. Eliminating False Blocks. When two blocks are identified as similar, they are not necessarily matched blocks. In some images (e.g., sky or nature), several blocks are similar to each other. Numerous similar blocks should be present at a specific distance to ensure that

similar blocks are copied and pasted. Thus, the Euclidean distance is used to calculate between two similar blocks and identify the duplicated blocks. the Euclidean distance is calculated by equation (4).

$$Pdist(p_1, p_2) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \tag{4}$$

where x_1, x_2, y_1 and y_2 are the coordinates of the matched points.

Step 5. Tamper localization. The inverse of a procedure is conducted on the transformed image to retrieve the original image with a tampered region map. The inverse of a two-dimensional Fourier transform is computed by equations (5)-(7). Figure 2 demonstrates the procedure of proposed block matching and tamper localization.

```
1:  Dist^Ratio ⇒ i ∈ {0.1 < i < 0.9}
2:  j = 2
3:  [vals, indx] ⇒ Sort^A+(Inverse^cos(Dprdo^des))
4:  while vals(j) < Dist^Ratio × vals(j + 1)
5:      do Process
6:  end while
7:  Process
8:  j ⇒ j + 1
9:  for all i ∈ {keypoint^des}
10:   for all k ∈ [2, ..., j − 1]
11:       match(i) → ∀x ∈ {0, ..., inx(k)}
12:     if pdist(loc_i, match(i)) > 10 then
13:         match_1^cord ⇒ [loc_{i+1}, loc_i]
14:         match_2^cord ⇒ [loc_{i+1}(match(i)), loc_i(match(i))]
15:
16:     end if
17:  end for
18: end for
```

Figure 2: Block matching procedure.

By using equations (5)-(7), the spatial domain image is first transformed into an intermediate image using the N one-dimensional Fourier transform, which is then transformed into the final image. The final image reveals the tampered region on the basis of the location of copied and pasted regions.

$$f(m,n) = \frac{1}{4\pi^2} \int_{w_1=-\pi}^{\pi} \int_{w_2=-\pi}^{\pi} F(w_1, w_2) \, e^{j} w_1 m e^{j} w_2 n dw_1 dw_2 \tag{5}$$

where

$$F(k,l) = \frac{1}{m} \sum_{j=0}^{m-1} p(k,j) e^{-i2\pi \frac{ij}{m}} \tag{6}$$

and

$$p(k,j) = \frac{1}{m} \sum_{i=0}^{m-1} f(i,j) e^{-i2\pi \frac{kj}{m}} \tag{7}$$

Where w_1 and w_2 are frequency variables, and $F(w_1, w_2)$is frequency-domain representation of $f(m, n)$ (Rosenfeld and Kak, 2014).

4 EXPERIMENTAL RESULTS

The proposed method is evaluated with a 2.0 GHz Intel Pentium processor and 4 GB of RAM and Matlab 2013a. The performance of the proposed forgery detection method is evaluated on a dataset that consists of 100 images with different contents from the Columbia photographic image repository (Ng et al., 2005) and our personal collection. The images varied in size, format, and shape of the duplicated areas.

To evaluate the robustness and sensitivity of the proposed method, detection performance is measured in terms of *TPR* equation (7) and *FPR* equation (8). *TPR* is the fraction of forged images correctly recognized as forged, and *FPR* is the fraction of original images that are not correctly recognized as original (Mishra et al., 2013). The value of *FPR*, *TPR*, and time is calculated, and an evaluation is performed with other existing methods.

$$TPR = \frac{\text{\# forged images detected as forged}}{\text{\# forged images}} \tag{8}$$

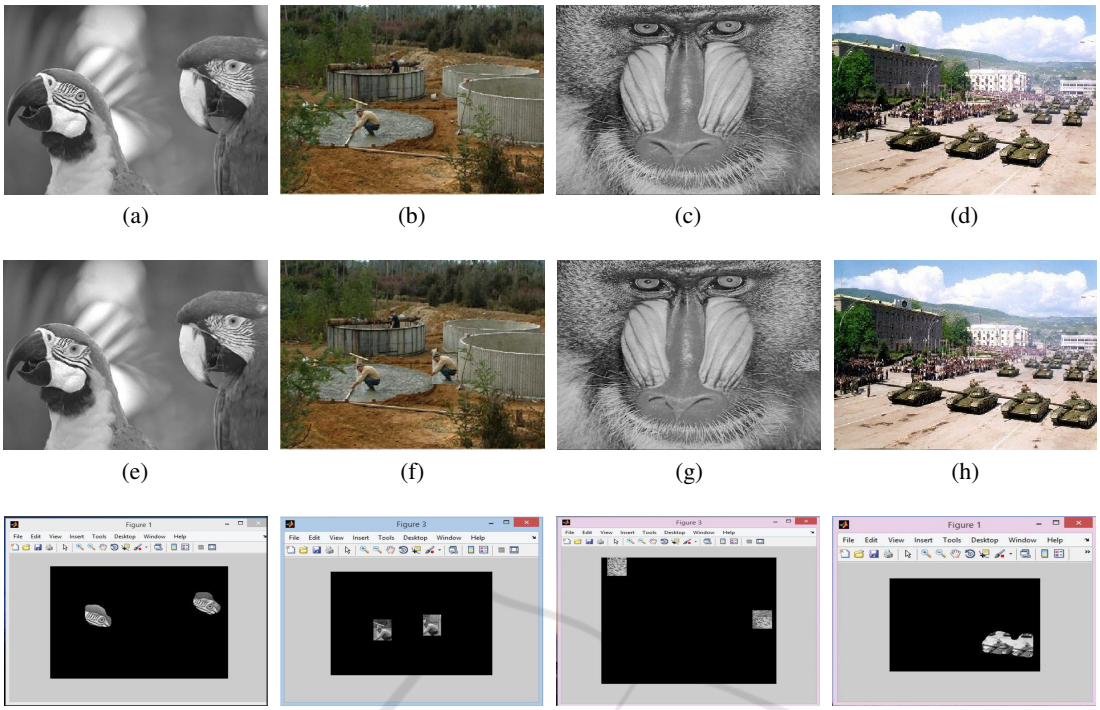
$$FPR = \frac{\text{\# original images detected as forged}}{\text{\# original images}} \tag{9}$$

Table 1 shows the processing time on average (in seconds) for an image. The results indicate that the proposed method performs better with respect to the others methods; in fact the processing time of Kangs method is 60 seconds for a grayscale image with a dimension of 256×256.

Table 1: Comparison result of proposed method with other methods.

Method	Time(S)/ Grayscale	Time (S)/ Colour
(Kang and Wei, 2008)	60	120
(Li and Yu, 2010)	N/A	44
Proposed Method	7	15
Proposed Method	5.44	8.19

By contrast, the detection time for the same image is 5 seconds for the proposed algorithm. The average



(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

Figure 3: The original images are in the top row (a-d). The forged images are in the middle (e-h) and the last row shows the detected region(i-l).

runtime of the Kangs algorithm (Kang and Wei, 2008) for a 256×256 color image is approximately 120 seconds; compare with the proposed algorithm for the same size of color image, it takes 8 seconds to identify the duplicated areas. Several different images are used in the experiment, which are challenging for copy-move forgery detection with different sizes of copied regions.

Figure 3 illustrates the detection results of the proposed method. Figure 3i to Figure 3l show the duplication detection map of the proposed method applied to the tempered images in Figure 3e to Figure 3h. As Figure 3i to Figure 3l illustrated, the proposed method can accurately detect the duplicated regions.

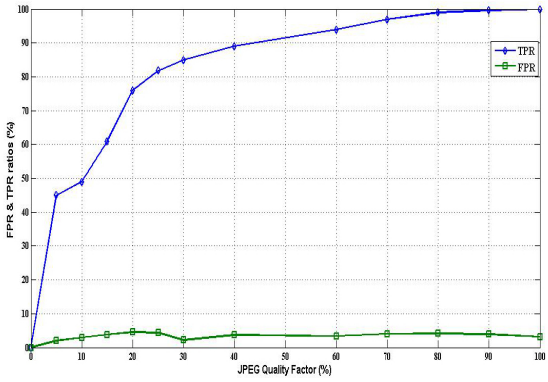


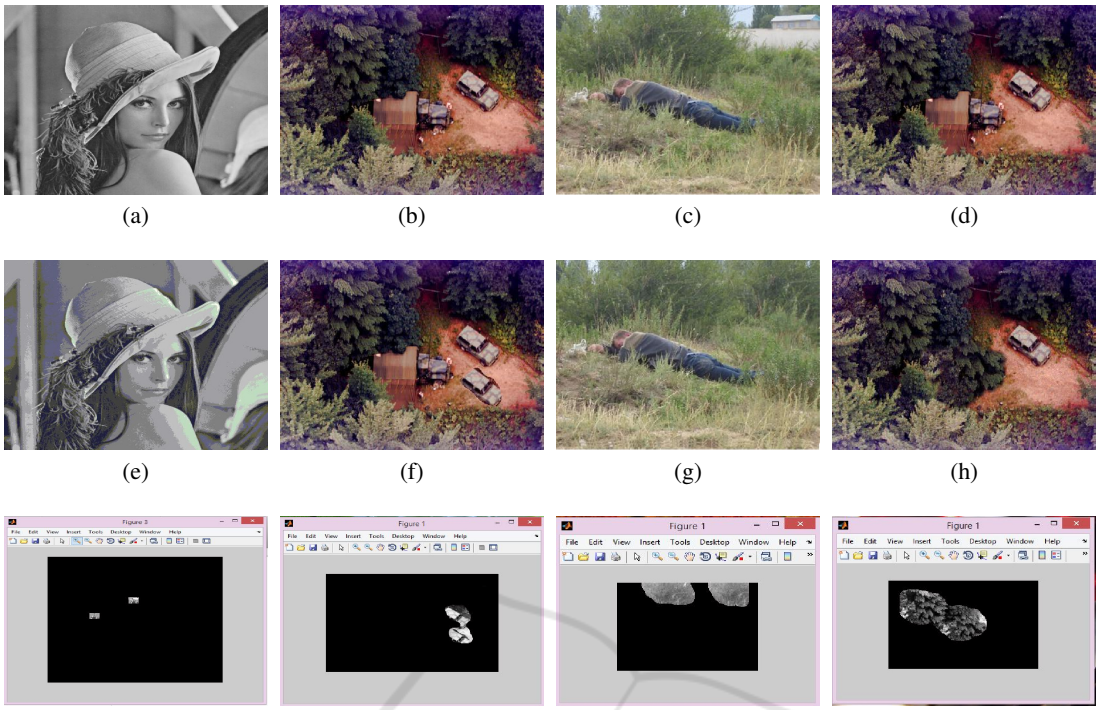
Figure 4: FPR and TPR for different JPEG quality factors.

As illustrated in Figure 4, when the different quality factors of JPEG compression is applied, there is only a slight change in the value of *FPR* and *TPR* . To evaluate the accuracy of the proposed algorithm, detection rates (*FPR* and *TPR*) are computed for different quality factors applied to all the images in the Columbia dataset. Figure 4 demonstrates the acceptable results of the proposed algorithm in terms of *FPR* and *TPR*.

In table 2, the performances of the proposed algorithm in terms of authenticity detection (*FPR* and *TPR*) is reported. The experimental results have il-

Table 2: Comparison of proposed method based on TPR and FPR.

Method	FPR(%)	TPR(%)
(Fridrich et al., 2003)	84	89
(Popescu and Farid, 2004)	86	87
(Bashar et al., 2010)	0.12	32.1
(Mishra et al., 2013)	3.64	73.64
(Silva et al., 2015)	0.12	71.92
Proposed Method	6.2	95.4



(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

Figure 5: Detection results (i-l) of our method on a set of forgery images with duplicated regions undergone different types of distortion (e-h), and (a-d) shows the original images.

lustrated the superiority of the proposed algorithm in comparison to other schemes in terms of efficiency.

Figure 5 shows the detection results of the proposed method on some realistic forgeries. The forgery images in the second row are generated with Photoshop and Gimp. The results show the robustness of the proposed method against JPEG compression and Gaussian noise. The duplicated regions in Figure 5e are small, and the forged image is under JPEG compression. Figure 5f is a tampered image with Gaussian noise. Figure 5h shows that the proposed method can detect forgery; even when the copied and pasted regions are similar to each other.

5 CONCLUSIONS

In this paper, an efficient copy-move forgery detection algorithm based on Electromagnetism Mechanism is proposed. The proposed *EMag* descriptors are utilized for locating the copy-move tampered regions. The degree of the attraction-repulsion force between each pixel and its neighbour is calculated, and an accurate description of the electrical forces between two objects are utilized to distinguish between forged and original pixels. The proposed false block elimination, eliminates the incorrect identified blocks with similar structures which greatly influence on the result of *TPR* and *FPR*. The proposed block size of 21×21 pixels and sub-blocks of 3×3 pixels creates a high efficiency in locating small tampered regions. However, the performance analyse and experimental result clearly demonstrate the efficiency of the proposed algorithm in terms of scaling, detection time, robustness against different noises ratio, JPEG compression and rotation. Future research include capability of detecting image splicing and image retouching.

ACKNOWLEDGEMENTS

The author of this article would like to thank Kyushu Institute of Technology, University of Malaya and Universiti Teknologi Malaysia for thier educational support.

REFERENCES

Ardizzone, E., Bruno, A., and Mazzola, G. (2015). Copy–move forgery detection by matching triangles of

keypoints. *IEEE Transactions on Information Forensics and Security*, 10(10):2084–2094.

Ardizzone, E. and Mazzola, G. (2009). Detection of duplicated regions in tampered digital images by bit-plane analysis. In *Image Analysis and Processing–ICIAP 2009*, pages 893–901. Springer.

Bashar, M., Noda, K., Ohnishi, N., and Mori, K. (2010). Exploring duplicated regions in natural images.

Bentley, J. L. (1975). Multidimensional binary search trees used for associative searching. *Communications of the ACM*, 18(9):509–517.

Chen, W., Shi, Y. Q., and Su, W. (2007). Image splicing detection using 2-d phase congruency and statistical moments of characteristic function. In *Society of photo-optical instrumentation engineers (SPIE) conference series*, volume 6505, page 26. Citeseer.

Cuevas, E., Oliva, D., Zaldivar, D., Pérez-Cisneros, M., and Sossa, H. (2012). Circle detection using electro-magnetism optimization. *Information Sciences*, 182(1):40–55.

Dadkhah, S., Manaf, A. A., and Sadeghi, S. (2014). An effective svd-based image tampering detection and self-recovery using active watermarking. *Signal Processing: Image Communication*.

Farid, H. and Lyu, S. (2003). Higher-order wavelet statistics and their application to digital forensics. In *IEEE workshop on statistical analysis in computer vision*, volume 8, page 94. Citeseer.

Fridrich, A. J., Soukal, B. D., and Lukáš, A. J. (2003). Detection of copy-move forgery in digital images. In *in Proceedings of Digital Forensic Research Workshop*. Citeseer.

Fridrich, J. (1999). Methods for tamper detection in digital images. In *Multimedia and Security, Workshop at ACM Multimedia*, volume 99, pages 29–34.

Hou, D. M., Bai, Z. Y., and Liu, S. C. (2012). A new algorithm for image copy-move forgery detection. In *Advanced Materials Research*, volume 433, pages 5930–5934. Trans Tech Publ.

Hu, J., Zhang, H., Gao, Q., and Huang, H. (2011). An improved lexicographical sort algorithm of copy-move forgery detection. In *Networking and Distributed Computing (ICNDC), 2011 Second International Conference on*, pages 23–27. IEEE.

Jalab, H. A. and Abdullah, N. A. (2013). Content-based image retrieval based on electromagnetism-like mechanism. *Mathematical Problems in Engineering*, 2013.

Jalab, H. A. and Shaker, K. (2014). Training the neural networks by electromagnetism-like mechanism based algorithm. In *INTERNATIONAL CONFERENCE ON QUANTITATIVE SCIENCES AND ITS APPLICATIONS (ICOQSIA 2014): Proceedings of the 3rd International Conference on Quantitative Sciences and Its Applications*, volume 1635, pages 582–586. AIP Publishing.

Jing, L. and Shao, C. (2012). Image copy-move forgery detecting based on local invariant feature. *Journal of Multimedia*, 7(1).

Kang, X. B. and Wei, S. M. (2008). Identifying tampered regions using singular value decomposition in digital image forensics. In *Computer Science and Software Engineering, 2008 International Conference on*, volume 3, pages 926–930. IEEE.

Kirchner, M., Schöttle, P., and Riess, C. (2015). Thinking beyond the block: block matching for copy-move forgery detection revisited. In *SPIE/IS&T Electronic Imaging*, pages 940903–940903. International Society for Optics and Photonics.

Li, W. and Yu, N. (2010). Rotation robust detection of copy-move forgery. In *Image Processing (ICIP), 2010 17th IEEE International Conference on*, pages 2113–2116. IEEE.

Li, Y. and Wang, H. (2012). An efficient and robust method for detecting region duplication forgery based on non-parametric local transforms. In *Image and Signal Processing (CISP), 2012 5th International Congress on*, pages 567–571. IEEE.

Lin, Z., He, J., Tang, X., and Tang, C.-K. (2009). Fast, automatic and fine-grained tampered jpeg image detection via dct coefficient analysis. *Pattern Recognition*, 42(11):2492–2501.

Liu, G., Wang, J., Lian, S., and Wang, Z. (2011). A passive image authentication scheme for detecting region-duplication forgery with rotation. *Journal of Network and Computer Applications*, 34(5):1557–1565.

Mishra, P., Mishra, N., Sharma, S., and Patel, R. (2013). Region duplication forgery detection technique based on surf and hac. *The Scientific World Journal*, 2013.

Ng, T.-T., Chang, S.-F., Hsu, J., and Pepeljugoski, M. (2005). Columbia photographic images and photorealistic computer graphics dataset. *Columbia Univ., New York, ADVENT Tech. Rep*, pages 205–2004.

Piva, A. (2013). An overview on image forensics. *ISRN Signal Processing*, 2013.

Popescu, A. C. and Farid, H. (2004). Exposing digital forgeries by detecting duplicated image regions. *Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515*.

Rosenfeld, A. and Kak, A. C. (2014). *Digital picture processing*, volume 1. Elsevier.

Ryu, S.-J., Lee, M.-J., and Lee, H.-K. (2010). Detection of copy-rotate-move forgery using zernike moments. In *International Workshop on Information Hiding*, pages 51–65. Springer.

Silva, E., Carvalho, T., Ferreira, A., and Rocha, A. (2015). Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. *Journal of Visual Communication and Image Representation*, 29:16–32.

Turabieh, H. and Abdullah, S. (2011). An integrated hybrid approach to the examination timetabling problem. *Omega*, 39(6):598–607.

Wu, H.-C. and Chang, C.-C. (2002). Detection and restoration of tampered jpeg compressed images. *Journal of Systems and Software*, 64(2):151–161.