Detection of Scaled Region Duplication Image Forgery using Color based Segmentation with LSB Signature

Dr. Diaa Mohammed Uliyan
Department of Computer Science
Faculty of Information Technology, Middle East University
Amman, Jordan

Dr. Mohammed A. F. Al-Husainy
Department of Computer Science
Faculty of Information Technology, Middle East University
Amman, Jordan

***Abstract*—Due to the availability of powerful image editing softwares, forgers can tamper the image content easily. There are various types of image forgery, such as image splicing and region duplication forgery. Region duplication is one of the most common manipulations used for tampering digital images. It is vital in image forensics to authenticate the digital image. In this paper, a novel region duplication forgery detection approach is proposed. By segmenting the input image based on the colour features, sufficient number of centroids are produced, that exist even in small or smooth regions. Then, the Least Significant Bit (LSB) of all the colours of pixels in each segment are extracted to build the signature vector. Finally, the hamming distance is calculated through exploiting the signature vector of image to find the dissimilarity. Various experimental results are provided to demonstrate the superior performance of the proposed scheme under some post processing operations such as scaling attack.**

Keywords*—Digital image forensics; Region duplication; Forgery detection; Image authentication

I. Introduction

The trustworthiness of images is a vital role in many scopes, including court image forensics, medical imaging, criminal investigations, news media, etc. However, with a rapid development in digital cameras, accompanied by sophisticated image editing tools such as Photoshop, has allowed the content of the image to be changed simply and without leaving any perceptible signs of forgery. The fact that "seeing believes" is no longer true. For example, the malicious forged images may carry false information, published over the network and mislead the public. Some criminals create fake evidence of tampering with images, which has a certain impact on social stability. This brings a new challenge toward implementing digital image forensic methods to answer the question: If a digital image has been retouched, what regions have been forged in the image?

Digital image forensic is employed to analyse the integrity and authenticity of the images. The digital image forensics methods can be divided into two categories: (1) active forensics and (2) passive forensics, respectively. The main goal of active methods is to embed watermark or digital signature in the protected digital image. Tampering attack simply destroys these signals. However, there are many imaging devices that do not have the function of embedding the digital watermark or signature.

Active image forensics methods focused on two methods: (1) data hiding (digital fingerprinting and digital watermarking) and (2) image signature (robust image hash). The major drawback of the data hiding is the necessity of inserting hidden information into the image, which destroys the original content of the image.

Passive forensics examine whether an image has been affected by any form of modifications, after it was initially produced. Investigating the processing history of any image and then localising forged regions from the image is the principal research objectives in image authentication. Furthermore, passive forensics can examine whether a received image has undergone by certain tampering operations without relying on any prior information about the original image. It accomplished by analysing intrinsic traces, which left by imaging devices. Then, identifying inconsistencies in signal characteristics [1]. Two main functions of passive methods are image forgery detection [2] and image source identification [3]. They are based on the fact that forgeries could bring the image into specific detectable changes.

II. Related Works

When a digital image is regarded as a piece of occurrence of depicted event, there is a demand to verify the trustworthiness of image. This means that the image has to be authentic to ensure that the image content has not been modified and the depicted scene is a valid representation of the real world. For instance, suppose that a photograph is published in a reputable digital newspaper. The responsible editor cannot make a decision whether the image has been tampered with or not. This decision depends on the type of authentication methods for digital image forensic [4]. Two main types of authentication methods in digital image forensic have been explored in the literature: (1) active methods [5-10], and (2) passive methods [2, 11-14].

In active methods, the image formation process is purposely modified where; digital authentication information is embedded into original image at the acquisition step. This information is extracted during the authentication step for comparison with reference authentication data. The authentication information may be used to verify whether an image has been forged in forensic investigations. There are two

types of techniques in active approach: (1) image signature and (2) imperceptible watermarking.

a) ***Image signature*** is a non-invasive analysis approach for image authentication. It consists of extracting robust features from the image at the sender side and encoding these features to produce an image signature. It has a strong distinguish ability of detecting secret messages from the image. The former emphasise both robustness and sensitivity in image signature. The robustness of signature could be against non-malicious attacks such as JPEG compression, adding noise and image filtering. Sensitivity of image signature could resist the changes caused by malicious attacks such as region duplication forgery with rotation, scaling or blurring. It aims to select features from the image to generate imperceptible signature, by assuming that those features are secured from passive or active attacks [6].

b) ***Digital watermarking*** aims to protect the copyright of digital image. Many watermarks for image are sensitive to forgery attacks. Slight malicious distortion will destroy the watermark and prevent the detection of tampered regions. However, the distortion of the digital image could be a malicious attacks like rotation, scaling and blurring [15].

In the past few years, digital watermarking has been applied to authenticate and localise tampered regions within images [9, 10, 16, 17]. Fragile and semi-fragile digital watermarking techniques are often utilised for image authentication. Fragile watermarking is appropriately named because of its sensitivity to any form of attack even slight modification. In contrast, semi-fragile watermarking is more robust against various editing attacks. It can be used to verify tampered content within images for both malicious and non-malicious attacks. In addition, semi-fragile schemes verify the integrity of the original image, as well as permitting alterations caused by non-malicious modifications such as image formation processes. Moreover, semi-fragile watermarking focused on detecting intentional attacks than validating the originality of the image [8, 10, 18].

In passive methods, the key idea is detecting forged regions in the suspected image. The forgery detection is done by analysing pixel level correlations based on the operation used to create a tampered image. Forgery detection techniques can be categorised into three groups: (1) image splicing [19, 20], (2) image retouching and (3) region duplication forgery.

1) ***Image splicing*** adds a part of an image into another image in order to hide or change the content of the second image [21].

2) ***Image retouching*** modifies an image by improving or reducing features without changing the image content significantly [22].

3) ***Region duplication forgery*** is defined as copying a region of an image and moving it into different area of the image. The duplicated regions could be post-processed with some transformations such as blurring, rotation and scaling. This leads it more difficult to detect [4, 23-25].

According to these types of forgery, a different type of image retouch might be performed through hiding an external information into the image in what is known as steganography. The traditional types of steganography techniques are used; the LSB of the image's colours to hide the external information [26, 27]. These changes in the LSBs of the image's colours will certainly cause a distortion in the image quality and may lead to change some details of objects in the image [27].

In the literature, there are two types of region duplication forgery detection algorithms: block-based method and keypoint based method. In block-based method, the process of detection method starts by dividing the image into overlapping blocks and extracting the features of each block. For instance, (Bayram et al., 2009) [28] used Fourier Mellin Transform to generate feature vectors for locating forged regions. (Lin et al., 2011) [29] proposed a forgery detection technique based on Hessian features and Discrete Cosine Transform (DCT) to locate forged regions. Ryu et al., 2013 [30] 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.

When block-based methods divide image into blocks to extract features, keypoint-based methods extract features from local interest points in the image. These features are computed only on the image itself, without any division, and the extracted features vectors per keypoint are compared with each other to find similar keypoints. Two well-known keypoint-based methods are: Scale Invariant Transform Methods (SIFT) [31, 32] and Speeded Up Robust Features (SURF) [33, 34]. One of the state of art of keypoint based methods is (Amerini et al., 2011) [32] that proposed a novel method based on SIFT, which is able to examine region duplication forgery and image splicing. It has high reliability when detecting forged images under some post processing operations such as scaling.

The main goal of this paper is to authenticate the image with localising the forged region by extracting image signature from colour features. The proposed method is a block-based method, where the image is divided into segments and each segment is retained by square block to extract features later. The specific contributions are: Firstly, the image is divided into segments based on the colour palette and combined with signature vector of LSB for each segment to obtain more robust clues. Secondly, in order to detect forged regions, an improved detection step is applied, which tries to retain all the potential irregularities in signatures between tampered image and the original signature received from the sender. Finally, based on the Hamming distance obtained between signature vectors of LSBs, the localisation of the forged regions step is performed.

The outlines of the paper are organised as: Section 3 shows the framework of region duplication forgery detection method and then explains each phase in details. In Section 4, experimental results are conducted. Finally, the conclusions are shown in Section 5.

III. PROPOSED MODEL

A novel method for image authentication has been proposed. The main objective of the proposed method is detecting forged regions under scaling and blurring. These

regions can be uniform regions and non-uniform regions. Uniform regions are used to hide contents in the image by forgers, while non-uniform regions are used to clone regions.

The poroposed method consists of two phases: Phase 1 that is creating a signature for the coloured bitmap image (.bmp) from the Least Significant Bit (LSB) of the pixels' colours in the pre-selected segments. And Phase 2 that is detecting the forged regions in the image that was sent by the sender using the signature created in Phase 1. Figure 1 depicts the general diagram of the two phases of the proposed model.

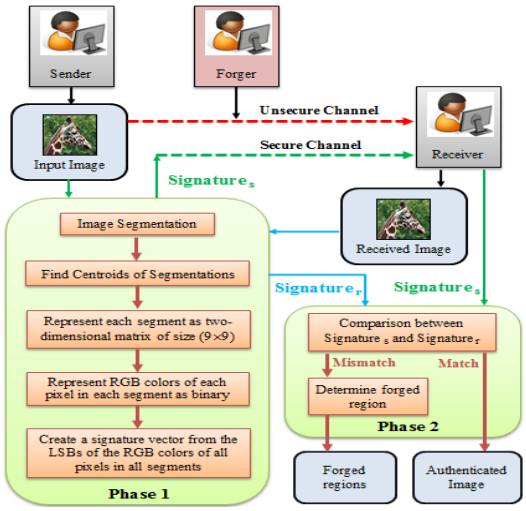


Fig. 1. General diagram of the two phases of the proposed model

To give a deep look in the two phases of the proposed model and the operations that are implemented in each phase, a detailed explanation will be stated later with an experimental example for each operation.

Phase 1: Create Signature

At the sender side, five necessary steps are applied in this phase to create a signature (signature$_s$) from the input image. First, do a segmentation operation to determine the distinct segments in the input image. Second, determine the centroid of each segment. Third, represent each segment as a two-dimensional matrix of size (9×9) pixels. Forth, extract the LSBs of the colours of pixels in each segment. Fifth, use these bits to construct the desired signature. The implementation details of each step are given below:

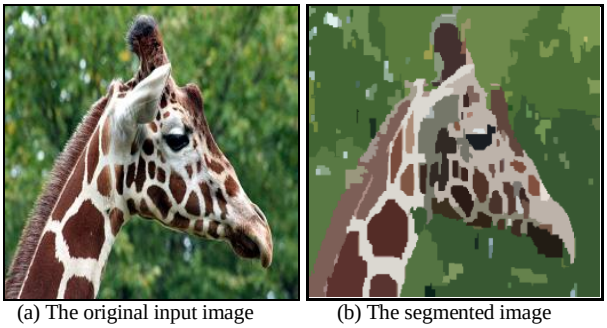
Step 1: The input image is passed through the segmentation operation to determine all the segments in the image. To achieve good segmentation results, a technique for selection of primitive colour features will be of great idea to extract objects from images. Particularly, the forgery could be applied in existing objects in the image. Based on this issue, a region growing segmentation based on colour features is applied as described in [35]. First, the image is transformed from RGB into YC_bC_r colour space using the following equation:

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 65.481 & 128.553 & 24.966 \\ -39.797 & -74.203 & 112 \\ 112 & -93.786 & -18.214 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} \quad (1)$$

Second, region growing for each pixel with its neighbouring pixels is generated based on similarity criteria. The similarity of a pixel to its (3×3) neighbourhoods are calculated as follows:

$$\sigma_x = \sqrt{\frac{1}{9}\sum_{i=1}^{9}(x_i - \bar{x})^2} \quad (2)$$

where, x is the intensity value of Y, C_b, C_r, and $\bar{x}$ is the mean value of x. The total standard deviation is $\sigma = \sigma_Y + \sigma_{C_b} + \sigma_{C_r}$, then the standard deviation is normalised to [0, 1] by $\sigma_N = \frac{\sigma}{\max(\sigma)}$, where $\max(\sigma)$ is the maximum of the standard deviation in the image. Finally, the similarity of a pixel to its neighbours is computed as $S = 1 - \sigma_N$. Figure 2 shows the original input image and the corresponding segmented image.



(a) The original input image (b) The segmented image

Fig. 2. Implementation of segmentation operation: (a) The original input image and (b) The corresponding segmented image.

Step 2: Find the centroid for each one of the segments that have been determined in the segmentation operation. The centroid of each segmented region in the image has coordinates $(\bar{x}, \bar{y})$, it can be located as follows:

$$\bar{x} = \frac{1}{A}\int_A x\, dA \quad and \quad \bar{y} = \frac{1}{A}\int_A y\, dA \quad (3)$$

Here, $(\bar{x}, \bar{y})$ is the coordinates of the centroid of the differential pixel of region dA in the image. Figure 3 shows the centroid of each segment that is determined in the segmentation operation.

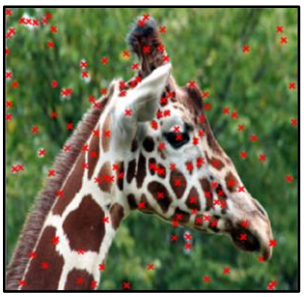


Fig. 3. Centroid of each segment that is determined in Fig. 2 (b)

Step 3: Represent each segment as a two-dimensional matrix of size (9×9) of pixels. Figure 4 shows an example of the representation of the image segment in Figure 2(a). Where each cell of the (9×9) matrix represents three numeric values of the Red, Green and Blue colors of the corresponding pixel in the cell.

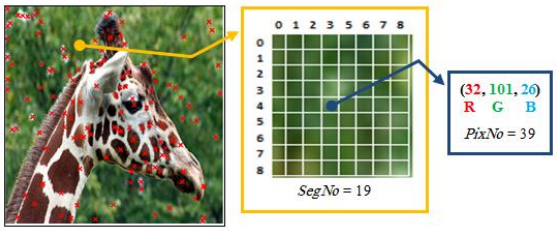


Fig. 4. Representation of the image segment as two-dimensional matrix of size (9×9)

Step 4: Extract the LSB of each using the mathematic formula (4). Where each colour of the pixel represents 1-byte=8 bits. Hence, LSB technique [7] is the most common method for embedding messages in images. The LSB of each pixel of an image may be replaced with some bits.

$$LSB_{Color} = Color \ \textbf{mod} \ 2 \quad (4)$$

In Figure 4 the LSB of each of the three colours (32, 101, 26) is as follows:

$$LSB_{Red} = 32 \ \textbf{mod} \ 2 = \mathbf{0}$$

$$LSB_{Green} = 101 \ \textbf{mod} \ 2 = \mathbf{1}$$

$$LSB_{Blue} = 26 \ \textbf{mod} \ 2 = \mathbf{0}$$

Step 5: Create a signature (***Signature***$_s$ for the sender) as a chain of LSBs that are extracted from the colours of pixels in all segments of the image. The LSBs of the pixel colours are extracted by passing through the image's segments and the segment's pixels sequentially (row by row) from the top-left to the bottom-right. The index of the extracted LSB of each of the three colours of the pixel is calculated using the three mathematical formulas (5), (6) and (7) respectively:

$$LSBIndex_{Red} = (SegNo \times SegSize) + (PixNo \times 3) \quad (5)$$

$$LSBIndex_{Green} = (SegNo \times SegSize) + (PixNo \times 3) + 1 \quad (6)$$

$$LSBIndex_{Blue} = (SegNo \times SegSize) + (PixNo \times 3) + 2 \quad (7)$$

where, *SegNo* is the segment number in the image: 0…(*NoOfSeg* -1), *NoOfSeg* is the number of segments in the image. *SegSize* is the number of colours in each segment, which is equal ((9×9)×3). *PixNo* is the pixel number in each segment: 0…80.

The indices of the three colours showed in Figure 4 are calculated using the above mathematical formulas (2), (3) and (4), where *SegNo* = 19 and *PixNo* = 39:

$$LSBIndex_{Red} = (19\times(9\times9)\times3) + (39\times3) = 4734$$

$$LSBIndex_{Green} = (19\times(9\times9)\times3) + (39\times3) + 1 = 4735$$

$$LSBIndex_{Blue} = (19\times(9\times9)\times3) + (39\times3) + 2 = 4736$$

The indices of the LSBs of the above three calculated colours in the chain of LSBs of the signature *Signature*$_s$:

Signature$_s$:	**Indices:**			4734	4735	4736		
	LSBs:		**…**		**0**	**1**	**0**	**…**	

The total number of bits in the signature is calculated using the mathematical formula (8) and the size of the signature (in byte) is calculated using the mathematical formula (9):

$$TotalNoOfBits = NoOfSeg \times SegSize \quad (8)$$

$$SizeOfSignature \approx \text{round}\ (TotalNoOfBits / 8) \quad (9)$$

Phase 2: Check Image Authentication

The same five steps in Phase 1 are applied at the receiver site to create a signature (*signature*$_r$) from the received image. And to check the authentication of the received image, the following additional steps should be implemented after that:

Step 1: Make a comparison between the two vectors of signatures (*signature*$_s$ and *signature*$_r$). If *signature*$_s$ and *signature*$_r$ have different *TotalNoOfBits*, this means that there are different number of segments that have been found in the received image through the segmentation operation in Step 1 of Phase 1. Therefore, the received image was certainly changed by such a forger. The type of effect that made by the forger is one of the following two situations:

a) If TotalNoOfBits(Signature$_s$*) > TotalNoOfBits(Signature*$_r$*),* this means that some distinct details (objects) in the image sent have been disappeared in the received image.

b) If TotalNoOfBits(Signature$_s$*) < TotalNoOfBits(Signature*$_r$*),* this means that some distinct details (objects) appeared in the received image which did not exist in the sent image.

But, if signature$_s$ and signature$_r$ have equal *TotalNoOfBits*, still there is a probability of changes that might be existing at the level of LSBs in each segment.

Step 2: Using the Hamming distance metric ($H_{distance}$) to calculate the number of bits that changed in the *signature*$_r$ with corresponding bits in signature$_s$. The Hamming distance metric ($H_{distance}$) is calculated using the formula (10).

$$\boldsymbol{H_{distance} = \sum_{k=0}^{TotalNoOfBits-1} [Signature_s(k) \ XOR \ Signature_r(k)]} \quad (10)$$

Now, based on the $H_{distance}$ value, if $H_{distance} = 0$ then go to Step 3. Otherwise, go to Step 4.

Step 3: No forgery found and the received image is authenticated.

Step 4: To determine precisely the segment in the image, a pixel in the segment and even which one of the three colours (Red, Green, and Blue) of the pixel that is changed by the forger. Hamming distance chain ($HC_{distance}$) of bits found using the formula (11), where k=0…*TotalNoOfBits*.

$$HC_{distance}(k) = Signature_s(k) \ \textbf{XOR} \ Signature_r(k) \quad (11)$$

Any bit has value 1, in $HC_{distance}$, means that the bit in this index in the *signature*$_r$ is different from the corresponding bit value in the *signature*$_s$. But if the bit has value 0, in $HC_{distance}$, this means that the values of the bits in both *signature*$_s$ and *signature*$_r$ on this index are equal. Now, to find the segment number, the pixel number in the segment and the colour in the pixel, the following three mathematical formulas (12), (13) and (14) be used:

$$SegNo = (Index(k) \ \textbf{div} \ SegSize) \quad (12)$$

$$PixNo = ((Index(k)\ \boldsymbol{mod}\ SegSize)\ \boldsymbol{div}\ 3 \quad (13)$$

$$Color = \begin{cases} if\ (Index(k)\boldsymbol{mod}\ 3) = 0,\ Color = Red \\ if\ (Index(k)\boldsymbol{mod}\ 3) = 1,\ Color = Green \\ if\ (Index(k)\boldsymbol{mod}\ 3) = 2,\ Color = Blue \end{cases} \quad (14)$$

As a result, forged region is determined based on dissimilarity criteria between two vectors of signatures. Figure 5 shows an example of detecting forged region subjected to add a new object to the original image in Figure 2 (a). It is shown that the desired colors of pixels in the segment have really changed.

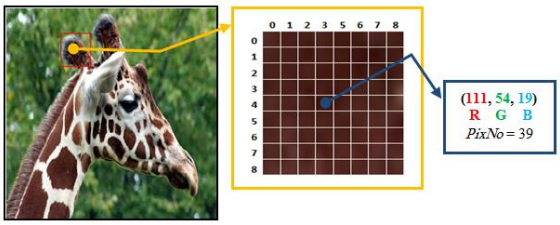


Fig. 5. Example of detecting forged region subjected to add a new copy moved object

IV. Experimental Results and Discussions

The proposed method was evaluated on a computer with a 32-bit CPU 4.0 GHz and 8 GB of RAM. The proposed method was implemented in Matlab 2013b and C sharp programming language. The performance of the proposed forgery detection method was evaluated on dataset named MICC-F220, F600 [32]. It is a well-known benchmark for evaluating existing region duplication forgery methods as mentioned in "related works" section. The dataset consists of 220 images, 110 original images and 110 forged images.

Two types of region duplication forgeries are currently used: the first one is a normal region duplication forgery which is performed by copying and moving the desired region to another region. The main goal for this type of forgery is to: a) add objects or b) hide objects. The second type of this forgery is a more complicated: some part of the image is copied, but before being pasted to another region, a pre-processing operation is applied to the copied part. Some of pre-processing operations are scaled and blurred that make forgery detection more challenging. Figure 6 illustrates some samples of region duplication forgery detection for different types of region duplication forgeries with the proposed algorithm.

Hence, the purpose of image forgery is to add or hide an object in the image content. Based on the colour segmentation method as described in Phase 1, the forged image may have more detected segments related to the new objects as shown in Table 1. For instance, more centroids of segmented regions are detected in the forged Giraffe image. Moreover, hiding any content of the image may hide some important segments in the images. This leads to decrease the number of detected centroids of segments in the forged image as shown in the forged Watch image. In some other complicated forgery cases, when the forged image has forged regions with scaling and blurring, the detection phase in the proposed method is based on the check of the LSBs of the pixels in the detected segments as shown in warrior and Christmas-hedge images. As a result of detection phase the forged region in the suspected image is detected with blue square block as shown in Table 1.

To evaluate the accuracy of the proposed method, the robustness of the proposed technique against scale attack are examined. Different Scale Factor (SF) (SF = 0.4, 0.6, 0.8,-0.4, -0.6 and -0.8) are respectively applied to the original part of the image before moving and pasting it to another region. Figures 7 and 8 indicated the detection results of the proposed method under scale up and down attacks.

In addition to that, the detection rates: False Positive Rate (FPR) and True Positive Rate (TPR) are calculated for all the images in the MICC-F220, F600 dataset. TPR is defined as the ratio of forged image that correctly identified, while FPR is defined as the ratio of original images that are not correctly identified. Table 2 demonstrates that the proposed method gives good results in terms of FPR & TPR even when applying different scaling factors on all the images in the dataset.

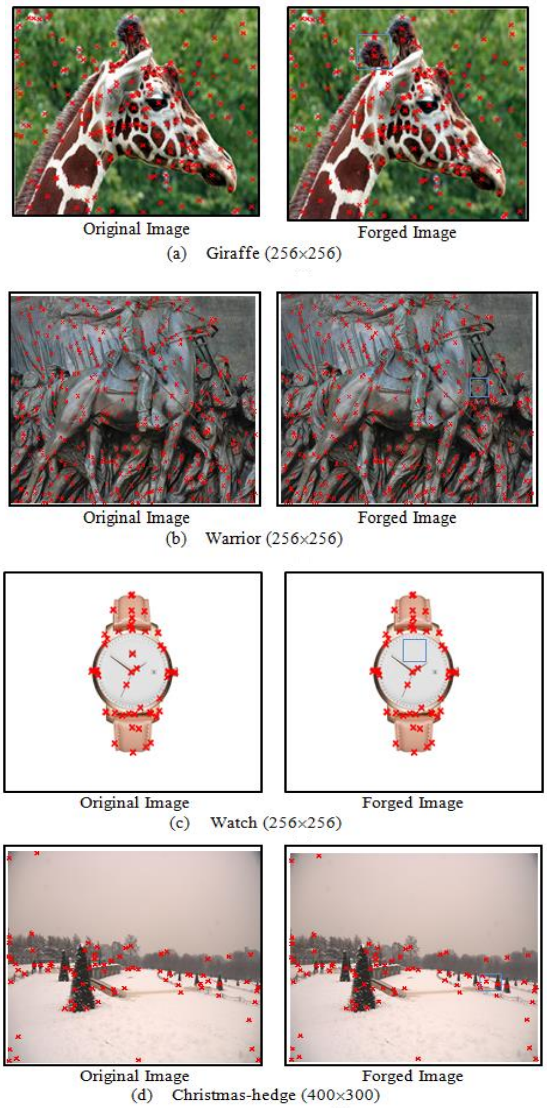
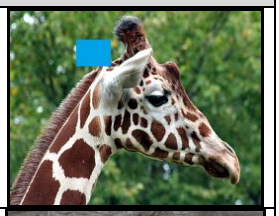
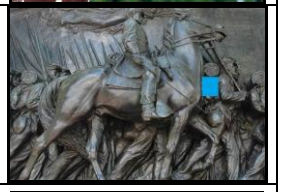


Fig. 6. Images used in the experiments: (a) Add an object in the image, (b) Add an object under scale up attack (with scale factor =0.4), (c) Hide an object under scale down attack (with scale factor=-0.6) and (d) Add a blurred object (with blur radius=0.3)

TABLE I. NUMBER OF DETECTED SEGMENTS IN THE ORIGINAL AND FORGED AGAINST VARIOUS ATTACKS.

Image		Number of centroids	Type of attacks	Detection results
Giraffe	Original	177	Normal add object	
	Forged	182		
Warrior	Original	354	Add object under scaling up	
	Forged	355		
Watch	Original	81	Hide object under scaling down	
	Forged	80		
Christmas-hedge	Original	175	Add object under blurring	
	Forged	176		

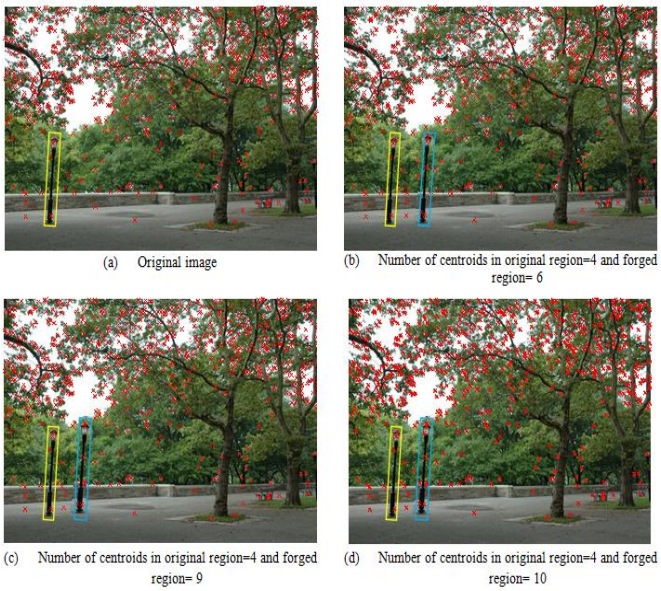


Fig. 7. Detection results of the proposed method for the a) Original image under various Scaling up Factors (SF) attacks: b) SF=0.4 c)SF=0.6 d)SF=0.8

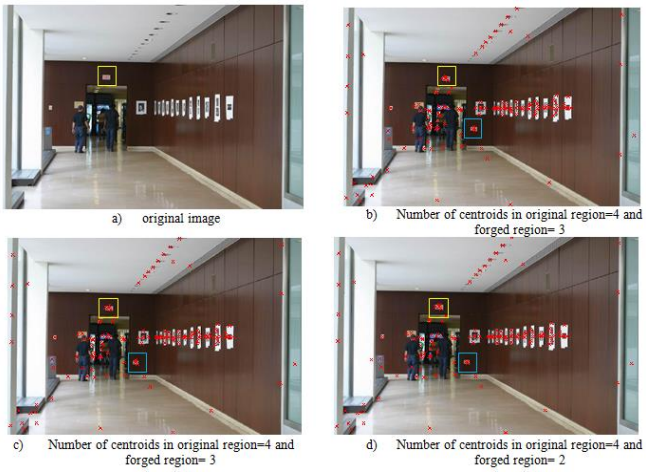


Fig. 8. Detection results of the proposed method for the a) Original image under various Scaling down Factors (SF) attacks: SF=-0.4 c)SF=-0.6 d)SF=-0.8

TABLE II. THE DETECTION PERFORMANCE SCALED REGION DUPLICATION FORGERY FROM 50 SAMPLE IMAGES ON MICC DATASET.

Scale up	Average TPR	Average FPR	Scale down	Average TPR	Average FPR
0.2	0.95	0.03	**-0.2**	0.96	0.02
0.4	0.94	0.035	**-0.4**	0.95	0.03
0.6	0.92	0.05	**-0.6**	0.94	0.035
0.8	0.92	0.06	**-0.8**	0.92	0.05
1	0.90	0.06	**-1**	0.92	0.06

To compare the performance of the proposed method with the state of the art, two key approaches were used as baselines: 1) keypoint based methods: (Amerini et al., 2011) [32], (Mishra et al., 2013) [33] and block-based method: (Li, J. et al, 2015) [36]. As seen from Table 3, the proposed method achieved a good detection rate in terms of TPR=94.5% and FPR= 6 %. In comparison, Amerini et al. method [32] achieves around 100% and of 8%.

The proposed method reduces the false positive rate while still maintaining a high true positive rate, as shown in Table 3. Here, it can be seen that TPR of the proposed method is better than some keypoint based methods: [33] and block-based method: [36]. In case of FPR, the method reduced the false positives 2% less than Amerini et al. method [32] to achieve robustness and reliability of detecting forged images. In Table 3, Mishra et al method [33] gives less FPR than the proposed method due to SURF features.

TABLE III. AVERAGE TPR AND FPR VALUES IN (%) FOR EACH METHOD USING MICC DATASET.

Methods	TPR%	FPR%
(Amerini et al.,2011) [32]	**100**	**8**
(Mishra et al., 2013) [33]	**73.64**	**3.64**
(Li, J. et al, 2015) [36]	**88**	**13.8**
Proposed method	**94.5**	**6**

V. CONCLUSION

In this paper, the image authentication method for detecting different types of image forgery is introduced. In the proposed model, the colour based segmentation and LSB of colour pixels were used to extract the image features, and all the extracted

LSBs are used to generate image signature. Then, forgery detection is developed and tampering localisation method is employed using Hamming distance. Experimental results show that the proposed method is robust against some post processing distortions such as scaling. The proposed method can detect the changes in the image signature caused by malicious attacks such as region duplication forgery or hiding some content in the image.

The proposed method struggles to detect rotated forged regions due to the weakness of LSB features against this type of forgery. The future research will focus on rotation invariant features.

REFERENCES

[1] D. M. Uliyan, H. A. Jalab, and A. W. A. Wahab, "Copy move image forgery detection using Hessian and center symmetric local binary pattern," in Open Systems (ICOS), 2015 IEEE Confernece on, 2015, pp. 7-11.

[2] A. Piva, "An Overview on Image Forensics," ISRN Signal Processing, vol. 2013, 2013.

[3] C.-T. Li, "Source camera identification using enhanced sensor pattern noise," Information Forensics and Security, IEEE Transactions on, vol. 5, pp. 280-287, 2010.

[4] O. M. Al-Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," Forensic science international, vol. 231, pp. 284-295, 2013.

[5] X.-Y. Luo, D.-S. Wang, P. Wang, and F.-L. Liu, "A review on blind detection for image steganography," Signal Processing, vol. 88, pp. 2138-2157, 2008.

[6] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, pp. 727-752, 2010.

[7] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, pp. 142-172, 2011.

[8] Z. Guojuan and L. Dianji, "An overview of digital watermarking in image forensics," in Computational Sciences and Optimization (CSO), 2011 Fourth International Joint Conference on, 2011, pp. 332-335.

[9] C. Singh and S. K. Ranade, "Geometrically invariant and high capacity image watermarking scheme using accurate radial transform," Optics & Laser Technology, vol. 54, pp. 176-184, 2013.

[10] Y. Huo, H. He, and F. Chen, "A semi-fragile image watermarking algorithm with two-stage detection," Multimedia Tools and Applications, pp. 1-27, 2013/01/05 2013.

[11] W. Luo, Z. Qu, J. Huang, and G. Qiu, "A novel method for detecting cropped and recompressed image block," in Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on, 2007, pp. II-217-II-220.

[12] W. Wang, J. Dong, and T. Tan, "A survey of passive image tampering detection," in Digital Watermarking, ed: Springer, 2009, pp. 308-322.

[13] R. Poisel and S. Tjoa, "Forensics investigations of multimedia data: A review of the state-of-the-art," in IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on, 2011, pp. 48-61.

[14] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10, pp. 226-245, 2013.

[15] L. Laouamer, M. AlShaikh, L. Nana, and A. C. Pascu, "Robust watermarking scheme and tamper detection based on threshold versus intensity," Journal of Innovation in Digital Ecosystems, vol. 2, pp. 1-12, 2015.

[16] S. Rawat and B. Raman, "A chaotic system based fragile watermarking scheme for image tamper detection," AEU-International Journal of Electronics and Communications, vol. 65, pp. 840-847, 2011.

[17] L. Zhang and P.-P. Zhou, "Localized affine transform resistant watermarking in region-of-interest," Telecommunication Systems, vol. 44, pp. 205-220, 2010/08/01 2010.

[18] R. Bao, T. Zhang, F. Tan, and Y. E. Wang, "Semi-fragile watermarking algorithm of color image based on slant transform and channel coding," in Image and Signal Processing (CISP), 2011 4th International Congress on, 2011, pp. 1039-1043.

[19] I.-C. Chang and C.-J. Hsieh, "Image Forgery Using An Enhanced Bayesian Matting Algorithm," Intelligent Automation & Soft Computing, vol. 17, pp. 269-281, 2011.

[20] Z. Moghaddasi, H. A. Jalab, R. Md Noor, and S. Aghabozorgi, "Improving RLRN image splicing detection with the use of PCA and kernel PCA," The Scientific World Journal, vol. 2014, 2014.

[21] Z. He, W. Lu, W. Sun, and J. Huang, "Digital image splicing detection based on Markov features in DCT and DWT domain," Pattern Recognition, vol. 45, pp. 4292-4299, 2012.

[22] R. Granty, T. Aditya, and S. Madhu, "Survey on passive methods of image tampering detection," in Communication and Computational Intelligence (INCOCCI), 2010 International Conference on, 2010, pp. 431-436.

[23] V. Christlein, C. Riess, J. Jordan, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," vol. 7, pp. 1841 - 1854 2012.

[24] Y. Sheng, H. Wang, and G. Zhang, "Comparison and Analysis of Copy-Move Forgery Detection Algorithms for Electronic Image Processing," in Advances in Mechanical and Electronic Engineering. vol. 178, ed: Springer, 2013, pp. 343-348.

[25] Diaa M. Uliyan Hamid A. Jalab ,Ainuddin W. Abdul Wahab Palaiahnakote Shivakumara Somayeh Sadeghi, "A novel forged blurred region detection system for image forensic applications," Expert Syst. Appl., vol. 64, pp. 1-10, 2016.

[26] M. A. F. Al-Husainy, "Message Segmentation to Enhance the Security of LSB Image Steganography," International Journal of Advanced Computer Science and Applications, vol. 3, pp. 57-62, 2012.

[27] M. A. F. Al-Husainy, "Image Steganography Method Preserves the Histogram Shape of Image," European Journal of Scientific Research, vol. 130, pp. 101-106, 2015.

[28] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009, pp. 1053-1056.

[29] S. D. Lin and T. Wu, "An integrated technique for splicing and copy-move forgery image detection," in Image and Signal Processing (CISP), 2011 4th International Congress on, 2011, pp. 1086-1090.

[30] S.-J. Ryu, M. Kirchner, M.-J. Lee, and H.-K. Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments," Information Forensics and Security, IEEE Transactions on, vol. 8, pp. 1355-1370, 2013.

[31] X. J. Shen, Y. Zhu, Y. D. Lv, and H. P. Chen, "Image Copy-Move Forgery Detection Based on SIFT and Gray Level," in Applied Mechanics and Materials, 2013, pp. 3021-3024.

[32] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," Information Forensics and Security, IEEE Transactions on, vol. 6, pp. 1099-1110, 2011.

[33] P. Mishra, N. Mishra, S. Sharma, and R. Patel, "Region duplication forgery detection technique based on SURF and HAC," The Scientific World Journal, vol. 2013, 2013.

[34] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in Multimedia Information Networking and Security (MINES), 2010 International Conference on, 2010, pp. 889-892.

[35] F. Y. Shih and S. Cheng, "Automatic seeded region growing for color image segmentation," Image and vision computing, vol. 23, pp. 877-886, 2005.

[36] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," Information Forensics and Security, IEEE Transactions on, vol. 10, pp. 507-518, 2015.