An Improved Double Compression Detection Method for JPEG Image Forensics

Vrizlynn L. L. Thing
Digital Forensics Lab
Cryptography and Security Department
Institute for Infocomm Research
Singapore
vriz@i2r.a-star.edu.sg

Yu Chen
Digital Forensics Lab
Cryptography and Security Department
Institute for Infocomm Research
Singapore
ychen@i2r.a-star.edu.sg

Carmen Cheh
Department of Computer Science
School of Computing
National University of Singapore
Singapore
u0807228@nus.edu.sg

***Abstract*—Double JPEG image compression detection, or more specifically, double quantization detection, is an important digital image forensic method to detect the presence of image forgery or tampering. In this paper, we introduce an improved double quantization detection method to improve the accuracy of JPEG image tampering detection. We evaluate our detection method using the publicly available CASIA authentic and tampered image data set of 9501 JPEG images. We carry out 20 rounds of experiments with stringent parameter setting placed on our detection method to demonstrate its robustness. Each round of classifier is generated from a unique, non-overlapping and small subset composing of $1/20$ of the tampered and $1/72$ of the authentic images, to obtain a training data set of about 100 images per class, with the rest of the $19/20$ of the tampered and $71/72$ of the authentic images used for testing. Through the experiments, we show an average improvement of 40.31% and 44.85% in the true negative (TN) rate and true positive (TP) rate, respectively, when compared with the current state-of-the-art method. The average TN and TP rates obtained from 20 rounds of experiments carried out using our detection method, are 90.81% and 76.95%, respectively. The experimental results show that our JPEG image forensics method can support a reliable large-scale digital image evidence authenticity verification with consistent good accuracy. The low training to testing data ratio also indicates that our method is robust in practical applications even with a relatively limited or small training data set available.**

***Keywords*-JPEG image; DCT coefficient; double compression; tampering detection; digital image forensic;**

I. INTRODUCTION

Digital images have become a very important information carrier in our daily lives. However, due to the ease of use and availability of image editing tools [1][2], it brings significant concern over the integrity of digital images, especially in the field of digital forensics. Therefore, it is very important that forensics investigators possess the appropriate technology to accurately and reliably verify the integrity of digital image evidence. In this paper, we focus on the research of Joint Photographic Experts Group (JPEG) image forensic to detect the evidentiary presence of digital image forgery and tampering. JPEG is chosen due to its widespread popularity as the de facto image format used by most electronic devices.

Double compression based image tampering detection is a common form of forged/tampered JPEG image detection method. The term "double compression" refers to the decompression of an already compressed JPEG image and the application of a subsequent recompression action to the image contents to store/save it back into the JPEG format. This process is a natural and mandatory part of the procedure that is carried out when JPEG images are tampered with. For example, to forge an existing JPEG image, the image needs to be decompressed, the manipulation methods such as splicing can then be applied on to the image, and the modified image is then recompressed back into a JPEG image. Such a JPEG double compression action has been observed to cause the presence of the periodic effects on the recompressed DCT coefficients. Thus, the existence of these coefficient effects for a given JPEG image can be used to verify if the image has undergone tampering. Several methods [6], [7], [8], [9], [10] have been proposed in this research direction. The major limitations of these existing methods are their robustness issue due to the need for a large training data set, their main purpose which is to study the double quantization effect instead of providing a full-fledged solution to detect image tampering, and/or the lack of the feature to automatically identify and localize the tampered regions. The experimental evaluation on these existing methods may also be inadequate due to the use of self-generated (and sometimes, a very small set of) training and test data. We discuss them in details in Section II.

Our proposed JPEG forensic tampering detection method is based on detecting the double compression effect. In essence, the double compression effects occur due to the non-tampered region. Therefore, the tampered region can be localized precisely in a detected forged JPEG image [3]. We focus on the research of a reliable detection approach that is more suitable for the practical applications of supporting large-scale digital image evidence authenticity verification. These requirements are essential due to the extremely massive quantity of JPEG images available as potential evidentiary data in computer systems, electronic devices and in the Web. Thus, an automatic image forensics approach, requiring no human involvement or assumption of prior knowledge of the test data, is necessary for a stable and non-subjective processing.

978-0-7695-4875-3/12 $26.00 © 2012 IEEE
DOI 10.1109/ISM.2012.61

We have tested our implementation of the existing automatic approach [3], which to the best of our knowledge, is the only fully automatic method with the capability to identify and localize the tampered regions. We observe that there is significant room for improvements in the robustness and detection accuracy of this existing approach to reach the desired performance in real-world applications.

Therefore, our main objective is to improve the existing JPEG double compression detection [3][4] by introducing a more robust and precise detection method. Our first contribution is the implementation of the work in [3][4] to carry out experiments to evaluate the performance using a publicly available data set [15]. The use of the publicly available data set is to ensure an objective evaluation of this existing work. We then carry out an analysis of the existing approach in an attempt to identify any weakness or limitation that can be overcome to strengthen the approach. Next, we propose a period detection method to improve the tampering detection performance in terms of robustness and accuracy. Lastly, compared with previous works on the double compression detection image forensics methods, our approach is shown to be more practical and accurate for applications which need to automatically detect forged/tampered JPEG images.

Other than JPEG images, the double compression detection method is also applicable to solving other digital forensic problems such as digital audio and video tampering detection. The double compression detection method can also be used to detect the utilization of steganographic algorithms (e.g. Outguess and F5 [5]) on JPEG images.

The rest of the paper is structured as follow. In Section II, we give a brief review of the existing works in JPEG image double compression detection. In Section III, we evaluate the current state-of-the-art method, identify its problem, and describe our proposed period detection method. In Section IV, we describe our implementation of both methods, carry out the experiments to evaluate the performance and discuss the results and findings. We conclude the paper in Section V and propose future work in Section VI.

II. Related Work

Several double JPEG compression detection methods to detect image forgery and tampering have been proposed. We discuss these existing works in this section.

In [6], the characteristic features (i.e. the periodic peaks and gaps) in the DCT histogram of recompressed JPEG images were discussed and pointed out. Three methods were proposed to detect JPEG double compression and the primary quantization matrix estimation was presented. Among their methods, the authors have proven that the Neural Network classifier is the best in terms of performance. In their work, the authors selected the lower frequency DCT coefficients to undergo processing of a two-layer Neural Network. They generated 900 double compressed images from the images they captured. Their primary quantization steps estimation error rate using the Neural Network approach was reported to be below 8%.

In [7], the authors presented a detailed proof and analysis of the double quantization effects detection approach. The author explained that the double compression effects, in the form of periodic peaks or gaps, would be more obvious after undergoing the Fourier transformation process. In their experiment, the authors presented an example using a double compressed JPEG image. They applied the Fourier transform on the histogram of the DCT coefficients and proved that the results indicated much clearer and prominent double compression effects.

In [8], the authors explained that the double compression effects can be better detected by analysing the differences between the DCT element/coefficient and its connected elements. The Markov random process was then used to model the difference map to a "transition probability matrix". A vector of 324 features was obtained and a support vector machine (SVM) was used to generate the model. For their experiments, the authors generated 4005 single and double compressed images from the uncompressed source images from the UCID (Uncompressed Colour Image Database) dataset [11], the Sun Yat-Sen University dataset [12] and the NRCS (National Resources Conservation Service) photo gallery [13]. $5/6$ of the generated images were used for training and the rest were then used for testing. The authors reported an average detection rate of between 81% and 100% for various combinations of quantization steps (i.e. factors).

In [9], the authors proposed applying a "random perturbation strategy" to the JPEG image to examine the double compression artefacts. In their approach, a portion (using a selected ratio) of JPEG coefficients was modified and encoded to form an image M_1. M_1 was then decompressed and recompressed to obtain an image N_1. D_1 can then be obtained as the number of non-matching DCT coefficients between M_1 and N_1. This process was repeated for a determined number of times to obtain a vector of D=D_1, D_2, ..., D_m, the authors explained that the average of D can be used to classify the single and double compressed images. For their experiments, the authors generated single and double compressed images from the source images from the UCID dataset, the NRCS dataset and their own data. By varying the selected modification ratio and quantization factor in the experiments, the maximum detection accuracy was reported to be between 66.40$\%$ to 100$\%$.

In [10], a shift-recompression based approach was proposed to detect misaligned cropping and recompression. The authors explained that during image tampering, there is a high probability that misalignment occurs during copy and paste forgery. Therefore, such "reshuffling" of image regions will leave behind clues of manipulation behaviour. The authors proposed obtaining the shift-recompression reshuffle characteristic features from the images to aid in double compression detection. The authors generated 2000 single compressed JPEG images and 4000 tampered images. They extracted the features from the images, and used 60% of the features for training, and 40% for testing. They reported an average detection rate of between 99.4% to 99.6% for both the linear LibSVM and Logistic regression classifiers.

A more sophisticated and automatic image forensic approach using double compression detection was proposed in [3][4]. In the approach, all the DCT blocks in a JPEG image are processed to form coefficient histograms (one for each of the 192 (64*3) DCT components). A period detection method was then used to detect and identify the periodic peaks in each histogram. With the estimated period, the probability of each block contributing to the periodic peaks can be obtained to form a probability bit map for each image. The authors extracted four features from the generated probability and used a SVM to train the model. The trained model and detector was then used to generate the decision and localize the tampered region. The authors used 50 images as the source images to generate 5000 single and 5000 double compressed images. 40% of the images were used to train the classifier while the rest were used for testing. They reported an average detection accuracy of around 60%.

III. Evaluation of The Existing Automatic JPEG Image Tampering Detection Method

The period detection method applied to the 192 histograms forms an important and essential module in its double compression detection mechanism. The performance of the image forensic tool relies on the accuracy of the period detection. We observed that the performance of the existing method, which we implemented as described by the authors in [3][4], does not give good detection results when applied to the publicly available tampered image data set [15]. The average detection accuracy is consistent with the one obtained by the authors when their method was applied to the test images that they have generated themselves. Therefore, it indicates the correctness of our implementation and their experimental evaluation (albeit on a different set of test images). Through our analysis, we found out that the main problem lies within the existing period detection method. We describe the problem in the following subsection and propose a better suited method to improve the detection accuracy.

A. The Existing Detection Method

The existing period detection method in [3] is formulated in Equation (1).

$$H(p) = \frac{1}{i_{max} - i_{min} + 1} \sum_{i=i_{min}}^{i_{max}} h(i \times p + s_0) \tag{1}$$

The estimated period p for each histogram is the p given by $Max(H(p))$. Here, $h(x)$ denotes the value of the x-th bin of the histogram, p is the period, s_0 is the index of the bin with the largest value, $i_{max} = \lfloor (s_{max} - s_0)/p \rfloor$, $i_{min} = \lceil (s_{min} - s_0)/p \rceil$, and s_{max} and s_{min} are the maximum and minimum index of the bins in the histogram, respectively.

This method estimates how well the period gathers the high value bins by using the average of the sum of the bins in each period. However, the major flaw in this method is that it tends to favour larger periods. The larger periods have fewer bins involved in the summation $\sum_{i=i_{min}}^{i_{max}}$ and could run into the risk of resulting in a higher $H(p)$ most of the time. Smaller periods, on the other hand, include more bins and despite the fact that the sum is high, the $H(p)$ is smaller than those large periods due to the averaging effect. Due to the random distribution of the bins with high votes/values for complex and realistically tampered images, there is a high risk that the $H(p)$ for larger periods is higher than the smaller but correct one, and wrongly detected. We provide examples and elaborate on this point in Section III.C.

B. Our Proposed Detection Method

To achieve a more accurate and robust period detection, we propose to detect the local maximum within each period. We calculate the local maximum by applying Equation (2).

$$f(i,p) = \frac{h(i) - Max\{N(z,p)\}}{Mean\{N(z,p)\}} \tag{2}$$

Where, $h(i)$ refers to the value of the i-th bin of the DCT coefficient histogram. $N(z,p)$ denotes the neighbouring bins of the i-th bin within the period p, $N(z,p) = \{h(i) | z - p < i < z + p, i \neq z\}$. The numerator $h(i) - Max\{N(z,p)\}$ is not reflective of the amount of deviation of the i-th bin from its neighbouring bins. Therefore, it needs to be weighted by the mean of the neighbouring bins $Mean\{N(z,p)\}$, in order to obtain a better detection.

Thus, $f(i,p)$ represents the difference between the i-th bin and its neighbours (defined by period p). As illustrated in Equation (3), for each bin, f is calculated and the median of f of all the bins involved in the period is calculated to obtain $H(p)$. The median is used instead of the mean as it is more robust to extreme values.

$$H(p) = Median\{f(i,p) | i = x \times p + s_0, i_{min} \leq x \leq i_{max}\} \tag{3}$$

Where, $i_{max} = \lfloor (s_{max} - s_0)/p \rfloor$, $i_{min} = \lceil (s_{min} - s_0)/p \rceil$, and s_{max} and s_{min} are the maximum and minimum index of the bins in the histogram, respectively. The period can be estimated as the value that gives the maximum "average difference" among all the bins and its neighbours, where the possible values of p range from 1 to $(s_{max} - s_{min})/5$. This restriction can further eliminate errors caused by the calculation for the unnecessary, large periods.

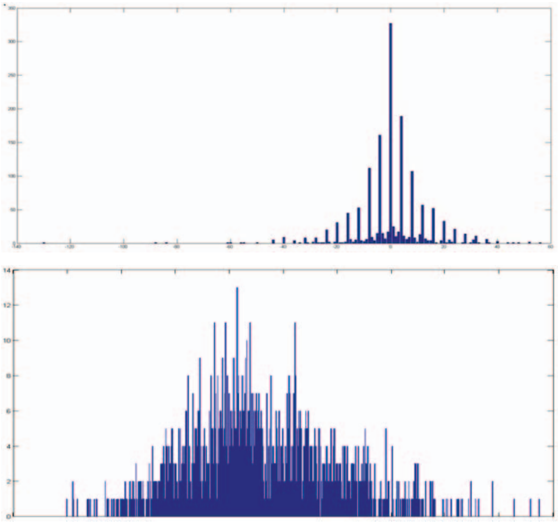

Figure 1. Histogram examples for comparisons between both methods

C. Analysis

Our proposed period detection method is superior to the original method in determining the period of the DCT histogram, when dealing with more challenging tampered cases. The method proposed in [3] aims to identify the peaks in the DCT histogram by summing up s_0 with a number of its assumed periodic occurrences at the two tails of the distribution. Thus, the averaging of the large (in fact, largest) s_0 with a small number of its periodic occurrences (due to the large period), may lead the decision to a period value that is biased. Our proposed method, on the other hand, discovers the peaks of the DCT histogram by checking whether the bins are local maxima within the period. The difference between the histogram bin value and the maximum bin value of its neighbours ensures that the bin included in the analysis is always the maximum among its neighbours. It also decreases the influence of randomly distributed bins which have very high values or in turn, votes. Weighing $h(i) - Max\{N(i,p)\}$ by the mean of the neighbours $Mean\{N(i,p)\}$ ensures that a larger value of $f(i,p)$ is obtained for a local maximum even if the $Max\{N(i,p)\}$ is close to the bin value. To better illustrate the merits of our method, we present two case studies based on real images' histograms to provide an insight through comparisons between both methods. The two histogram examples are shown in Figure 1.

The histogram at the top in Figure 1 is observed to have a period of 4. The original method detects the period to be 44 whereas our method detects the period to be the accurate value of 4. In the original method:

$$\sum_i h(i \times 4 + s_0) = 1285 \quad and \quad \sum_i h(i \times 44 + s_0) = 334$$

$$H(4) = \frac{1}{47} \sum_i h(i \times 4 + s_0) = \frac{1}{47} \times 1285 \approx 27.3$$

$$H(44) = \frac{1}{4} \sum_i h(i \times 44 + s_0) = \frac{1}{4} \times 334 = 83.5$$

Here, the number of occurrences of the analysed periods at 4 and 44 are 47 and 4, respectively. Therefore, the averaging values ($H(x)$) can not reflect the actual period, as $H(44) > H(4)$. Real-world images usually have complex contents, which leads to their DCT coefficient histograms having non-periodic random bins with very high values or votes. In the original method, the large period with the corresponding few occurrences may affect the detection accuracy. For the same histogram, our method returns $H(4) = 12.895$ and $H(44) = -18.3$. Since $12.895 > -18.3$, our proposed method is able to obtain the correct result.

Besides the inaccuracy in detecting the correct period, the existing method may also return a period which is non-existent in some cases. This error may lead to false positive detections in the tampering detection results. The histogram shown as the bottom illustration in Figure 1 does not have any obvious period. Thus, the correct period should be 1. In the original method,

$$\sum_i h(i \times 1 + s_0) = 1536 \quad and \quad \sum_i h(i \times 66 + s_0) = 74$$

$$H(1) = \frac{1}{875} \sum_i h(i \times 1 + s_0) = \frac{1}{875} \times 1536 \approx 1.755$$

$$H(66) = \frac{1}{22} \sum_i h(i \times 66 + s_0) = \frac{1}{22} \times 74 \approx 3.384$$

From the original method, $H(66) > H(1)$. Therefore, this example shows that once again, the original method suffers from the randomly distributed high value bins. It results in detecting a large period with fewer occurrences. On the other hand, based on our proposed method, $H(66) = -2.36$ and since all the other period values (with the exception of period 1) return negative values, the detected period is concluded to be 1. Thus, the false positive result can be eliminated.

In the next section, we carry out an objective experimental evaluation of both methods using the publicly available authentic and tampered image data sets in [15].

IV. Experiments

A. Outlines of Implementation

First, we present a brief introduction to our implementation of both the detection methods. The implementation steps are listed below.

1) Construct the histograms, one for each DCT coefficient in each colour channel. The lower frequency region is selected for processing.
2) Calculate the period of each histogram using the original method and our proposed method.

3) For each DCT coefficient element in each 8x8 block, calculate the posterior probability of it being not tampered with (i.e. authentic). The DCT elements in the non-tampered block would tend to result in more probable votes for the periodic bins.
4) Sum up the posterior probabilities for each block in the image, and form a bit map where each point in the map corresponds to a DCT block and the intensity of the point refers to the sum of the posterior probabilities.
5) Extract the features T_{opt}, ρ, $\rho_0+\rho_1$ and C_0, which are the optimal threshold, the squared difference between the mean probabilities of the two classes, the variance of the posterior probabilities of two classes and the connectivity factor, respectively, from the probability bit map.
6) For both methods, train the final classifier using a linear SVM.

B. Experiment Setting

The purpose of this experiment is to evaluate our double compression detection method in the application of image forensics. Since double compression detection can detect the recompressed JPEG images and also localize the tampered content (if any) in the recompressed images, it can be used to detect forged JPEG images that have undergone a variety of image tampering processes, as long as double compression is involved. Since double compression is the natural procedure to commit the changes and store the image back into the JPEG format, this assumption is reasonable.

To train and test the SVM classifiers for each method, we used the images provided in CASIA Tampered Image Detection Evaluation Database Version 2 [15]. The database is the latest data set released by the National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science. Compared to CASIA Version 1, this data set is a “more challenging image tampering evaluation database”, with a larger number of authentic and tampered images, and with “more realistic and challenging fake images by using post-processing across tampered regions”. The data set consists of 7437 authentic and 2064 tampered color JPEG images. Among the tampered color images, the tampered region(s) in 968 images is from the same authentic image (we refer to this set of tampered images as Set “S”), while the tampered region(s) in 1096 images is from a different authentic image (we refer to this set of tampered images as Set “D”). We randomly split the tampered color images into 20 sets, where each set consists of 102 images with no overlap among the different sets (i.e. $968/20$=48 tampered images from Set “S” and $1096/20$=54 tampered images from Set “D”). We also randomly split the authentic images into 72 sets (i.e. $7437/72$=103) so as to obtain a total of 103 images per set (close to the number of 102 images per tampered image set). Again, there is no overlap among the different authentic sets. We carried out 20 rounds of experiments. During each round of the experiments, we used one set of the data (i.e. 103 authentic images, 48 tampered images from Set “S” and 54 tampered images from Set “D”) to train our classifiers and the rest of the data (i.e. 7334 authentic images, 920 tampered images from Set “S” and 1042 tampered images from Set “D” in each round of experiments) to obtain the test results. Therefore, there is no overlap between the training and testing data set. By using only 5% (i.e. $1/20$) of the tampered images for training, we are also testing the robustness of our detection method at the same time. The test results for each round of the experiments are shown in Table I and II. The average accuracy of the authentic image detection for the original and proposed method is 64.72% and 90.81%, respectively. The average accuracy of the tampered image detection for the original and proposed method is 53.12% and 76.95%, respectively. The accuracy of detecting tampered images in the case where the tampered region(s) is from the same or different authentic image is distributed almost equally. Therefore, the detection methods are not biased in performance between these two different “forms” of tampering. From the experimental results, we also observe that the results are consistent among all rounds of evaluations and that the proposed method outperforms the original method significantly.

An important point to note is that the double compression detection methods belong to the class of passive blind image forgery or tampering detection approaches. Therefore, prior knowledge of the original images is assumed to be absent. As the CASIA image data set does not provide the information on the groundtruth information with regard to the precise regions of tampering[1], it is difficult to carry out further evaluations based on the tampered regions identified. However, CASIA does provide the original and tampered images for Set “S” (i.e. tampered region(s) is from within the same image), and the two original images and tampered images for Set “D” (i.e. tampered region(s) is extracted from one original image and applied to another original image). Therefore, from the above experiments we have carried out, we extract a few sets of test images together with the original images provided by CASIA, and show the final output based on the block-based posterior probability bit maps generated by both detection methods. In Figure 2, the images in the first column from the left are the original images provided by CASIA, the images in the second column are the forged or tampered images where the tampered region(s) is from within the same image (i.e. by tampering within the original image), the images in the third column are the result maps generated by the original method, and the images in the fourth and final column are the result maps generated by

[1] We have verified this with Ms Jing Dong and Mr Wei Wang who are managing the CASIA data set. We were also informed that CASIA Version 3, which has not yet been released, will be taking into consideration the release of explicit localization information.

	Authentic Images (of 7334)	**Tampered Images in Set “S” (of 920)**	**Tampered Images in Set “D” (of 1042)**	**Tampered Images (of 1962)**
Round 1	4473	522	579	1101
Round 2	5056	461	505	966
Round 3	4382	545	587	1132
Round 4	5495	415	457	872
Round 5	4807	481	535	1016
Round 6	4753	489	541	1030
Round 7	4905	509	520	1029
Round 8	5261	460	501	961
Round 9	5071	459	506	965
Round 10	4935	458	512	970
Round 11	4696	486	553	1039
Round 12	4788	484	546	1030
Round 13	4235	550	594	1144
Round 14	4903	490	525	1015
Round 15	4610	533	570	1103
Round 16	4186	540	588	1128
Round 17	4542	500	553	1053
Round 18	4538	508	568	1076
Round 19	4928	496	542	1038
Round 20	4266	540	637	1177
Overall Average	94930/146680=64.72%	9926/18400=53.95%	10919/20840=52.39%	20845/39240=53.12%

Table I
CORRECTLY DETECTED RESULTS BASED ON ORIGINAL METHOD

	Authentic Images (of 7334)	**Tampered Images in Set “S” (of 920)**	**Tampered Images in Set “D” (of 1042)**	**Tampered Images (of 1962)**
Round 1	6390	740	836	1576
Round 2	6781	679	779	1458
Round 3	6604	708	791	1499
Round 4	6362	753	842	1595
Round 5	6759	710	806	1516
Round 6	6837	681	790	1471
Round 7	6513	738	828	1566
Round 8	6484	722	820	1542
Round 9	6915	656	766	1422
Round 10	6952	679	761	1440
Round 11	6572	729	822	1551
Round 12	6829	694	790	1484
Round 13	6616	717	809	1526
Round 14	6674	715	812	1527
Round 15	6468	723	834	1557
Round 16	6675	698	788	1486
Round 17	6780	681	779	1460
Round 18	6764	692	792	1484
Round 19	6659	696	797	1493
Round 20	6567	720	822	1542
Overall Average	133201/146680=90.81%	14131/18400=76.80%	16064/20840=77.08%	30195/39240=76.95%

Table II
CORRECTLY DETECTED RESULTS BASED ON PROPOSED METHOD

our proposed method. In Figure 3, the images in the first and second columns (from the left) are the original images provided by CASIA, the images in the third column are the forged or tampered images which were generated based on each set of the two orginal images, the images in the fourth column are the result maps generated by the original method, and the images in the fifth and final column are the result maps generated by our proposed method. Based on Figure 2 and 3, we can observe that our proposed method is potentially stronger in localizing and determining the tampered regions too.

V. CONCLUSION

In this paper, we introduce an improved double compression detection based JPEG image forgery and tampering detection method. We present a new period detection method, designed to take into consideration the characteristics of the random distribution of high value bins in the DCT histograms of real-world images caused by their complex

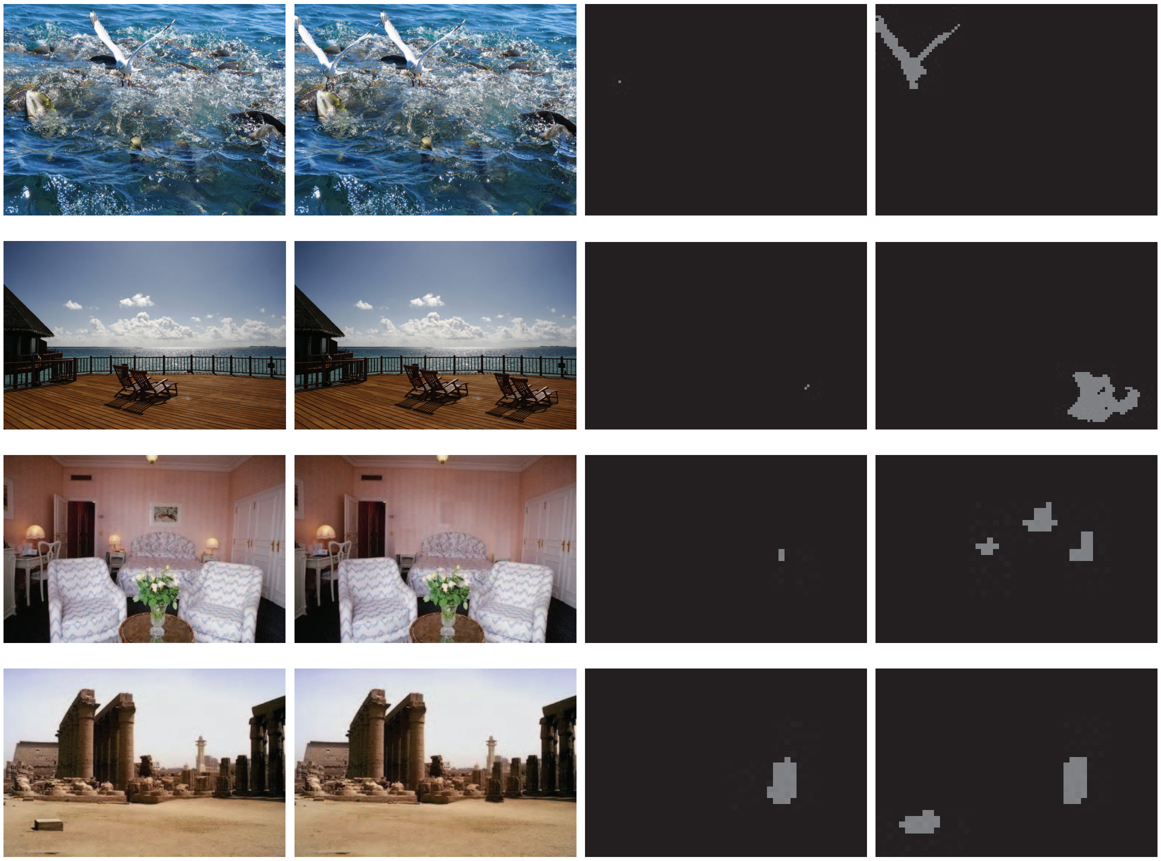

Figure 2. Set "S" result map examples for visual comparisons between the original method (third column from left) and our proposed method (fourth and final column) where images in the first column are the orginal images used to generate the tampered images in the second column

contents. We evaluated our detection method using the publicly available CASIA authentic and tampered image data set of 9501 JPEG images by carrying out 20 rounds of experiments with the stringent constraint of using a small set of images (i.e. 5% or ∼100 images) for training while leaving a higher number of (non-overlapping) images in each round for testing purpose, to demonstrate the robustness and accuracy of our detection method. Each round of classifier in the experiments was generated from a unique, non-overlapping and small subset of the tampered and authentic images. Through the experiments, we showed an average improvement of 40.31% and 44.85% in the true negative (TN) rate and true positive (TP) rate, respectively, when compared with the current state-of-the-art method. The average TN and TP rates obtained from 20 rounds of experiments carried out using our detection method, were 90.81% and 76.95%, respectively. The experimental results show that our JPEG image forensics method can support an automated and reliable large-scale digital image evidence authenticity verification. Through visual comparisons of both methods based on the automated tampered regions localization, we showed that our method has a potentially stronger performance. In addition to double compression detection approaches, other approaches rely on explicit discriminating tampered or non-tampered features extracted from image contents such as the JPEG coefficients, camera response functions, and frequency distribution statistics near detected edges. Such features may be dependent on other factors such as the target cameras or the environment conditions during image capture. These detection approaches require training using images taken with a wide variety of external factors, which may be impractical to achieve. On the other hand, approaches that require a very small training data set are more risk-averse from being overly trained and specifically optimized for certain data sets only.

VI. Future Work

Based on the analysis conducted on the failed cases of tampered images detection by our method in the experiments, we discovered that the reason is due to the less obvious presence of periodic effects in the DCT coefficient histograms. As the obviousness of the periodic effects varies for different combinations of quantization steps in the primary and secondary compressions [8], these factors should

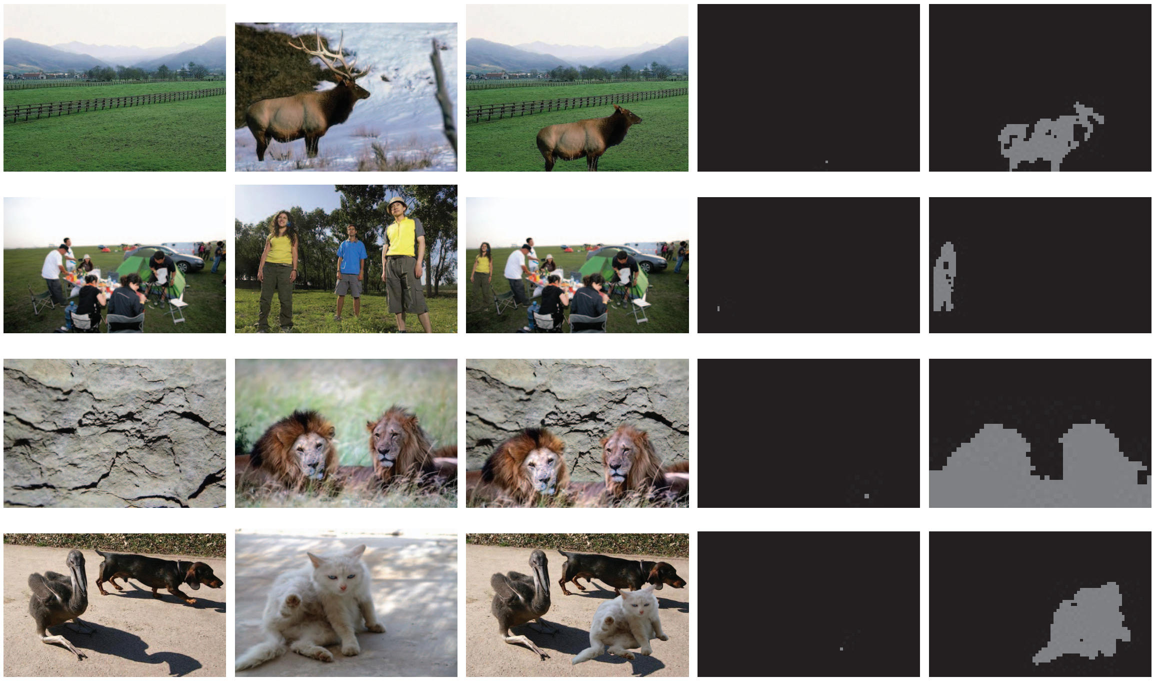

Figure 3. Set “D” result map examples for visual comparisons between the original method (fourth column from left) and our proposed method (fifth and final column) where images in the first and second columns are the orginal images used to generate the tampered images in the third column

be taken into consideration to improve the detection performance further. Therefore, the research directions proposed in [9][10] could be studied further to incorporate enhancements of our current method.

REFERENCES

[1] H. Farid, A Survey of Image Forgery Detection, IEEE Signal Processing Magazine, Vol. 26, No. 2, pp. 16-25, 2009.

[2] Y. Chen and V. L. L. Thing, A Study on the Photo Response Non-Uniformity Noise Pattern Based Image Forensics in Real-World Applications, International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV), 2012.

[3] Z. Lin, J. He, X. Tang, and C. Tang, Fast, Automatic and Fine-Grained Tampered JPEG Image Detection via DCT Coefficient Analysis, Pattern Recognition, Vol. 42, No. 11, pp. 2492-2501, 2009.

[4] J. He, Z. Lin, L. Wang, and X. Tang, Detecting Doctored JPEG Images via DCT Coefficient Analysis, European Conference on Computer Vision, Lecture Notes on Computer Science, Vol. 3953, pp. 423-435, 2006.

[5] J. Fridrich J., M. Goljan, and D. Hogea, Attacking the Out-Guess, ACM Workshop on Multimedia and Security, December 2002.

[6] J. Lukas and J. Fridrich, Estimation of Primary Quantization Matrix in Double Compressed JPEG Images, Digital Forensics Research Conference (DFRWS), August 2003.

[7] A. Popescu and H. Farid, Statistical Tools for Digital Forensics, International Workshop on Information Hiding, 2004.

[8] C. Chen, Y. Q. Shi, and W. Su, A Machine Learning Based Scheme for Double JPEG Compression Detection, IEEE International Conference on Pattern Recognition, December 2008.

[9] F. Huang , J. Huang and Y. Q. Shi, Detecting Double JPEG Compression with the Same Quantization Matrix, IEEE Transactions on Information Forensics and Security, Vol. 5, No. 4, pp. 848-856, 2010.

[10] Q. Liu, Detection of Misaligned Cropping and Recompression with the Same Quantization Matrix and Relevant Forgery, ACM International Workshop on Multimedia in Forensics and Intelligence, November, 2011.

[11] G. Schaefer, and M. Stich, UCID - An Uncompressed Colour Image Database, SPIE Storage and Retrieval Methods and Applications for Multimedia, Vol. 5307, pp. 472-480, 2004.

[12] http://ist.sysu.edu.cn

[13] http://photogallery.nrcs.usda.gov

[14] http://www.pdphoto.org

[15] CASIA Image Tempering Detection Evaluation Database Version 2.0, http://forensics.idealtest.org