Engineering Sciences International Research Journal
ISSN (Print) : 2330 – 4338 ; Volume 1 Issue 1 ǁ February. 2013 ǁ

Passive-Blind Technique for Detecting Digital Image Tampering and Steganography

Paranjay R Menaria[1], B. R. Kapuriya[2], S.V.S.S.N.V.G. Krishna Murthy[3]

Abstract: There has been rapid growth of image editing softwares nowadays because of which we can see large amount of tampered images circulating in our daily lives, which creates a demand for automatic forgery detection algorithms to detect whether an image is tampered or not. Doctored image could either be tampered or could have hidden message in it ,called steganography. A good forgery detection algorithm should be passive and blind, requiring no extra prior knowledge of the image content or any embedded watermarks. The goal of this paper is to construct a new classifier which can classify an image into four classes i.e. authentic, spliced , steganographed or spliced and steganographed both applied in the same image.

Keywords: Digital Watermarking, Steganography, Steganalysis, Pattern Recognition

1. INTRODUCTION

In the current digital age, creating and manipulating digital images are easy and simple by using digital processing tools which are widely available from the Internet. However, some people take this opportunity to do something wrong. Many tampered images emerge in news coverage, scientific experiments and even legal evidences. Therefore, we can no longer take the authenticity of images for granted. The need for image tampering detection makes image forensics a very important research issue. Digital Image Tampering could be of any type. Either the image can be tampered to change its meaning or changing the image visually. The other way is to embed a secret message in the image without changing it visually such that the other person who knows the key to get the message can only get it , also known as steganography. Splicing detection, another important area in the field of digital forensics has attracted increasing attention. Is there any relationship between steganalysis and splicing detection? Is it possible to detect splicing and steganography applied in a single image? We address these intact and yet interesting questions.Efforts have been made to detect images with tampering done virtually or for images which are steganographed.But no work has been done in the area if the image the image is visually changed as well as it has been steganographed.

Generally speaking, there are two approaches of image forgery detection: active [5] and passive [3] detection. Active approach requires pre-processing (e.g. watermark embedding) when generate image or before distribute image. However, many of the image capture devices are lack of this functionality, which makes the active approach not universal. The passive approach does not need this operation, however, and could make analysis on various images based on supervised learning. Hence, it gains more attention and becomes a hot research topic. In this paper we focus on passive image splicing detection,steganographed image detection and also images with steganography and splicing both in single image based on machine learning. The rest of the paper is organized as follows.Diffrence and similarity between image splicing and steganography is shown in Section 2.The merged feature set for the proposed classifier is introduced in Section 3. In Section 4 experimental rsults are reported and Conclusion is drawn in Section 5.

2. IMAGE SPLICING AND STEGANOGRAPHY

Steganalysis is to deter the secret communication, while splicing detection is to authenticate a given image by determining if it has been spliced.

Steganography encodes information bits (possibly encrypted) and then embeds the bits into the cover image.Splicing is to replace one or more parts of a host image with fragment(s) from the same host image or other source images.Therefore,the statistical artifacts left with steganography are likely different from those caused by splicing..

So here we design a classifier, which can separate stego images(with hidden data and therefore tampered), spliced images(with inconsistent image fragment(s) and therefore tampered) and spliced and steganographed both images(with hidden data and as well as inconsistent image fragments and therefore tampered)from authentic images.

3. MERGED FEATURE SET

Here two types of feature set is used:First we use the GLCM(gray level co-occurence matrix)of the edge images in image croma as defined in section and second we use the

Markov and DCT feature set as discussed in section . In [9] GLCM(Gray Level Co-occurence Matrix) of the edge image of Cb(or Cr) component is used for splicing detection. A predefined threshold value is used to threshold the edge image to reduce its size as almost all of gray values in the edge image of Cb(or Cr) component are not big (about 95% of them are below 10). After thresholding edge images, we can get four gray level co-occurrence matrices (the size of each matrix is $(T+1)\times(T+1))$ of edge images in the following way:

- The element of GLCM of thresholed E_h denoted by CM_h is $P(E_h(i,j),E_h(i,j+1))$.
- The element of GLCM of thresholed E_v denoted by CM_v is $P(E_v(i,j),E_v(i+1,j))$.
- The element of GLCM of thresholed E_d denoted by CM_d is $P(E_d(i,j),E_d(i+1,j+1))$.
- The element of GLCM of thresholed E_{-d} denoted by CM_{-d} is $P(E\_d(i,j),E\_d(i+1,j-1))$.

These four matrices (CM_h,CM_v,CM_d,CM_{-d}) are used to generate features by the way that each matrix is first transformed to a vector, and then cascaded them to form one feature vector. Therefore, the length of feature vector is $4\times(T+1)\times(T+1)$ .We have used value of T = 8.

For merged feature set features from [4] are also added to the feature vector. Features are calculated for original image as well as for its calibrated image. A detailed description about calibrated image can be found in [2]. The original DCT features are constructed by use of 23 functionals F that produce a scalar, vector, or a matrix when applied to the stego image. Each functional F is evaluated for the stego image J_1 and its calibrated version J_2. The calibrated feature f is obtained as the difference $F(J_1)-F(J_2)$, if F is a scalar, or as an L1 norm $\| F(J_1)-F(J_2)\|_{L1}$ if F is a vector or a matrix.

Let the luminance of a stego JPEG file be represented with a DCT coefficient array $d_{ij}(k),i,j=1,...,8,k=1,...,n_B$, where $d_{ij}(k)$ denotes the (i,j)-th quantized DCT coefficient in the k-th block (there are total of n_B blocks).The first functional is the histogram H of all $64\times n_B$ luminance DCT coefficients.

$$H=(H_L,.....,H_R) \quad (1)$$

where $L=min_{i,j,k}d_{ij}(k),R=max_{i,j,k}d_{ij}(k)$.

The next 5 functionals are the histograms

$$h^{ij}=(h_L^{ij},.....,h_R^{ij}) \quad (2)$$

of coefficients of 5 individual DCT modes $(i,j)\in(1,2),(2,1),(3,1),(2,2),(1,3)$

The next 11 functionals are dual histograms represented with 8 X 8 matrices $g_{ij}^d,i,j=1,...,8,d=-5,...,5$

$$g_{ij}^d=\sum_{k=1}^{n_B}\delta(d,d_{ij}(k)) \quad (3)$$

where $\delta(x,y)=1$ if $x=y$ and 0 otherwise.

The next 6 functionals capture inter-block dependency among DCT coefficients. The first functional is the variation V

$$V=\frac{\sum_{i,j=1}^{8}\sum_{k=1}^{|I_r|-1}|d_{ij}(I_r(k))-d_{ij}(I_r(k+1))|+\sum_{i,j=1}^{8}\sum_{k=1}^{|I_c|-1}|d_{ij}(I_c(k))-d_{ij}(I_c(k+1))|}{|I\_r|+|I\_c|} \quad (4)$$

where I_r and I_c denote the vectors of block indices $1,...,n_B$ while scanning the image by rows and by columns respectively.

Two next two blockiness functionals are scalars calculated from the decompressed JPEG image representing an integral measure of inter-block dependency over all DCT modes over the whole image:

$$B_\alpha=\frac{\sum_{i=1}^{\lfloor(M-1)/8\rfloor}\sum_{j=1}^{N}|c_{8i,j}-c_{8i+1,j}|^\alpha+\sum_{i=1}^{\lfloor(N-1)/8\rfloor}\sum_{j=1}^{M}|c_{i,8j}-c_{i,8j+1}|^\alpha}{} \quad (5)$$

N (M-1)/8 + M (N-1)/8

In equation 3, M and N are image height and width in pixels and $c_{i,j}$ are grayscale values of the decompressed JPEG image, $\alpha = 1,2$.

The remaining three functionals are calculated from the co-occurrence matrix of neighboring DCT coefficients

$$N_{00} = C_{0,0}(J_1) - C_{0,0}(J_2)$$
$$N_{01} = C_{0,1}(J_1) - C_{0,1}(J_2) + C_{1,0}(J_1) - C_{1,0}(J_2) + C_{-1,0}(J_1) - C_{-1,0}(J_2) + C_{0,-1}(J_1) - C_{0,-1}(J_2)$$

$$N_{11} = C_{1,1}(J_1) - C_{1,1}(J_2) + C_{1,-1}(J_1) - C_{1,-1}(J_2) + C_{-1,1}(J_1) - C_{-1,1}(J_2) + C_{-1,-1}(J_1) - C_{-1,-1}(J_2)$$

where

$$C_{st} = \frac{\left(\sum_{i,j=1}^{8}\sum_{k=1}^{|I_r|-1}\delta(s, d_{ij}(I_r(k)))\,\delta(t, d_{ij}(I_r(k+1)))\right) + \sum_{i,j=1}^{8}\sum_{k=1}^{|I_c|-1}\delta(s, d_{ij}(I_c(k)))\,\delta(t, d_{ij}(I_c(k+1)))}{|I\_r| + |I\_c|} \quad (7)$$

In order to alleviate the information loss due to using the L_1 norm and to keep the dimensionality of features "reasonable," we replaced the L_1 norm by the following differences.

For the global histogram functional H and for 5 histograms of individual DCT modes h_{ij} , we take the differences of elements in the range $[-5,+5]$. Thus, the histogram features are

$$H_l(J_1) - H_l(J_2), l \in -5,....,+5$$

$$h_l^{ij}(J_1) - h_l^{ij}(J_2), l \in -5,....,+5$$

For the dual histogram functionals $g^d, d \in -5,...,+5$, we take the difference of the 9 lowest AC modes

$$g_{ij}^{d}(J_1) - g_{ij}^{d}(J_2), (i,j) \in (2,1),(3,1),(4,1),(1,2),(2,2),(3,2),(1,3),(2,3),(1,4)$$

For the co-occurrence matrix functionals, we use the central elements in the range [-2,+2]× [-2,+2]. This yields 25 features

$$C_{st}(J_1) - C_{st}(J_2), (s,t) \in [-2,+2]\times[-2,+2]$$

The rationale behind restricting the range of the differences between functionals to a small interval around zero is that DCT coefficients follow a generalized Gaussian distribution centered around zero. Thus, the central part of the functionals holds the most useful information for steganalysis.

Another feature set which we use in merged feature set is the markov feature set as used in [4]. The Markov feature set models the differences between absolute values of neighboring DCT coefficients as a Markov process. The DCT coefficients in $F(u,v)$ are arranged in the same way as pixels in the image by replacing each 8×8 block of pixels with the corresponding block of DCT coefficients. Next, four difference arrays are calculated along four directions: horizontal, vertical, diagonal, and minor diagonal (further denoted as $F_h(u,v), F_v(u,v), F_d(u,v)$ and $F_m(u,v)$ respectively).

$$F_h(u,v) = F(u,v) - F(u+1,v)$$

$$F_v(u,v) = F(u,v) - F(u,v+1)$$

$$F_d(u,v) = F(u,v) - F(u+1,v+1)$$

$$F_m(u,v) = F(u+1,v) - F(u,v+1)$$

From these difference arrays, four transition probability matrices M_h, M_v, M_d, M_m areconstructed as

$$M_h = \frac{\sum_{v=1}^{S_v-1}\sum_{u=1}^{S_u-1}\delta(F(u,v) = m, F(u+1,v) = n)}{\sum_{v=1}^{S_v-1}\sum_{u=1}^{S_u-1}\delta(F(u,v) = m)}$$

$$M_v = \frac{\sum_{v=1}^{S_v-1}\sum_{u=1}^{S_u-1}\delta(F(u,v) = m, F(u,v+1) = n)}{\sum_{v=1}^{S_v-1}\sum_{u=1}^{S_u-1}\delta(F(u,v) = m)}$$

$$M_d = \frac{\sum_{v=1}^{S_v-1}\sum_{u=1}^{S_u-1}\delta(F(u,v)=m, F(u+1,v+1)=n)}{\sum_{v=1}^{S_v-1}\sum_{u=1}^{S_u-1}\delta(F(u,v)=m)}$$

$$M_m = \frac{\sum_{v=1}^{S_v-1}\sum_{u=1}^{S_u-1}\delta(F(u+1,v)=m, F(u,v+1)=n)}{\sum_{v=1}^{S_v-1}\sum_{u=1}^{S_u-1}\delta(F(u+1,v)=m)}$$

where $m \in [-T,T], n \in [-T,T]$ and

$$\delta(F(u,v)=m, F(u,v+1)=n) = \begin{cases} 1 & if F(u,v)=m, F(u,v+1)=n \\ 0 & otherwise \end{cases}$$

The calibrated Markov features are formed by differences as $M^c = M(J_1) - M(J_2)$.To reduce the resulting dimensionality, we used the average $\overline{M} = (M_h^{(c)} + M_v^{(c)} + M_d^{(c)} + M_m^{(c)})/4$ of all four calibrated matrices, instead. This feature vector has dimensionality 81. The Merged feature set of total 274+324 = 598 features.

4. EXPERIMENTAL RESULTS

1. Image Dataset

Randomly 1000 authentic and 1000 spliced images were taken from CASIA image dataset [10].1000 images from ucid image dataset[7] were taken and message was embedded into it using MBS and perturbed quantization (PQ) steganography technique.Another 1000 images were taken from CASIA dataset[10] and then they too were steganographed.This created a image dataset of 1000 authentic,1000spliced,1000 steganographed and 1000 spliced and steganographed both.These images were used for training and the remaining images in the dataset were used for testing and validation.

2. Detection Performance

Five runs (by randomly selecting training samples each run) were performed on neural network.The performance of the proposed techniques is better than the techniques discussed in the above sections.This can be seen from Tables .It not only increses the performance of detecting splicing and steganography but it also detects if an image is steganographed as well as spliced.The comparison between the existing techniques implemented and the proposed technique is put up here in the tabular form.We have tested our algorithm for model based steganography [6] and perturbed quantization steganography [1].As different images may have different embedding capacity, the embedding strength for each image is measured in units of BPC (bits per non-zero DCT AC coefficients). In our experiments, five embedding rates (0.05, 0.1, 0.2, 0.3, and 0.4 BPC) were tested for both the MBS and the PQ methods.

A comparison of [4] and the proposed technique for detecting steganographed images is shown in table 1. The results shows that the proposed combined classifier is better than the implemented technique.

Table 1 : Comparison of Penvy's Method and Proposed Combined Classifier For Steganalysis

Steganography	BPC	Penvy's Method	Proposed Classifier
MBS	0.05	63.79	66.42
MBS	0.1	69.42	72.13
MBS	0.2	79.57	82.43
MBS	0.3	93.00	94.09
MBS	0.4	94.09	98.56
PQ	0.05	58.22	62.11
PQ	0.1	60.36	64.81
PQ	0.2	63.65	69.78
PQ	0.3	66.5	79.30
PQ	0.4	69.42	89.67

A comparison of [9] and the proposed technique for detecting spliced images is shown in table 2.The results shows that the proposed combined classifier is better than the implemented technique.

Table 2 : Comparison of and Proposed Combined Classifier For Detecting Splicing

Wie Wang Splicing Detection	Proposed Classifier
.90	95.67

The Proposed CLassifier can also detect images which are spliced and steganographed both. The Results for detecting spliced and steganographed images is given in the table 4

Table 3 : Results of Proposed Combined Classifier For Detecting Spliced and Steganographed both Images

Steganography	BPC	Proposed Classifier
MBS	0.05	64.21
MBS	0.1	70.68
MBS	0.2	84.24
MBS	0.3	92.21

MBS	0.4	97.00
PQ	0.05	63.20
PQ	0.1	66.28
PQ	0.2	72.34
PQ	0.3	78.89
PQ	0.4	94.36

Table 4 : Overall results of proposed combined classifier

Steganography	BPC	Proposed Classifier
MBS	0.05	62.44
MBS	0.1	72.45
MBS	0.2	86.23
MBS	0.3	91.78
MBS	0.4	98.63
PQ	0.05	65.20
PQ	0.1	67.21
PQ	0.2	75.32
PQ	0.3	79.71
PQ	0.4	96.87

5. CONCLUSION

In this paper we have proposed a classifier which can classify an image into any one of the four classes. The four classes are authentic, spliced, steganographed and spliced and steganographed both. DCT and Markov features and the GLCM features are used in this classifier.The detection rate of the proposed classifier is high. The results are compared with the results of the individual feature set. In future work we plan to include more types of forgeries in the classifier and make a classifier which can detect all types of image forgeries.

6. REFERENCES

[1] J. Fridrich, M. Goljan, and D. Soukal. Perturbed quantization steganography. *Multimedia Systems*, 11(2):98–107, 2005.

[2] J. Fridrich. Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes. In *Information Hiding*, pages 67–81. Springer, 2005.

[3] T.T. Ng, S.F. Chang, C.Y. Lin, and Q. Sun. Passive-blind image forensics. *Multimedia Security Technologies for Digital Rights*, pages 383–412, 2006.

[4] T. Pevn`y and J. Fridrich. Merging markov and dct features for multi-class jpeg steganalysis. *Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX*, 6505:3, 2007.

[5] V.M. Potdar, S. Han, and E. Chang. A survey of digital image watermarking techniques. In *Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on*, pages 709–716. IEEE, 2005.

[6] P. Sallee. Model-based steganography. *Digital Watermarking*, pages 254–260, 2004.

[7] G. Schaefer and M. Stich. Ucid-an uncompressed colour image database. *Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia*, 5307:472–480, 2004.

[8] Yun Shi, Chunhua Chen, Guorong Xuan, and Wei Su. Steganalysis versus splicing detection. In *Digital Watermarking*, volume 5041 of *Lecture Notes in Computer Science*, pages 158–172. Springer Berlin / Heidelberg, 2008.

[9] W. Wang, J. Dong, and T. Tan. Effective image splicing detection based on image chroma. In *Image Processing (ICIP), 2009 16th IEEE International Conference on*, pages 1257–1260. IEEE, 2009.

[10] Credits for the use of the casia image tempering detection evaluation database (caisa tide) v2.0 are given to the national laboratory of pattern recognition, institute of automation, chinese academy of science, corel image database and the photographers.

* * *

[1]Paranjay R Menaria
Department of Applied Mathematics DIAT(DU) , Pune-411025 , pmenaria@gmail.com
[2]Mr. B.R. Kapuriya
Research And Development Establishment , Pune-411015 , Email: brkapuriya@gmail.com
Dr. S.V.S.S.N.V.G. Krishna Murthy ,Department Of Applied Mathematics DIAT(DU),Pune-411025
email : sgkmurthy@gmail.com