International Journal of Engineering Innovation & Research
Volume 2, Issue 6, ISSN: 2277 – 5668

Retouching Detection and Steganalysis

Hiral Shah
V.E.S. Institute of Technology,
University of Mumbai, Mumbai, India.
Email: hiral.shah.06@gmail.com

Prajakta Shinde
V.E.S. Institute of Technology,
University of Mumbai, Mumbai, India
Email: prajaktashinde.7@gmail.com

Jaya Kukreja
V.E.S. Institute of Technology,
University of Mumbai, Mumbai, India
Email: jayakukreja18@gmail.com

***Abstract* — Images play an important role in forensics laboratory. Due to easy availability of image editing and processing tools it is simple to manipulate and modify digital images without leaving any obvious traces of tampering. For digital image used as evidence, image authentication is necessary. In this paper, first, different image tampering techniques are discussed. Retouched image forgery technique is discussed. Steganography is discussed and its difference with image tampering. A method for Steganalysis is discussed. Finally conclusion and future work is discussed.**

***Keywords* – Forgery Detection, Image Authentication, Image Forensics, Image retouching, Image Tampering, Steganography, Steganalysis.**

I. INTRODUCTION

Digital images have wide applications in medical diagnosis, forensics, commercial photography, journalism, entertainment, education etc. Most of the applications that use digital images are sensitive applications; like a medical diagnosis made based on an image, a judgment made in a courtroom based on an image produced as evidence, etc. From the tabloid magazines to the fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our e-mail in-boxes, doctored photographs are appearing with a growing frequency and sophistication.

Digital image forensics is used for authenticating information available in images, authenticating images captured form CCD cameras, authenticating of images as evidence, document authenticating, and fingerprint recognition. When images are produced in courtrooms as evidence, integrity of these images is very important.

Digital image forgery detection methods are classified into, active methods and passive methods. Active methods depend on watermarking and digital signature to authenticate an image. Active methods work only when we have some prior information about the image. Hence such a method does not work when handling images from unknown or unreliable sources.

Unlike active methods, a passive method is capable of detecting image forgery without any prior information about the image or its source and it detects tampering by identifying changes in the image properties like inconsistencies in lighting and changes in the mathematical properties of a raw digital image. These techniques work on the assumption as digital forgeries may leave no visual clues that indicate tampering but they may alter the underlying statistics of an image.

II. IMAGE TAMPERING TECHNIQUES

Some of the image manipulation techniques are[5]:

A. Splicing

It is a method of tampering images by combining two sources to produce a new image which retains the majority of one image for detail. Fig.1 is an example of a spliced image.

Fig.1.(a) Source image

Fig.1.(b)Target image

Fig.1.(c)Spliced image

B. Retouching

Retouching is used for photo enhancement i.e. enhancing the appeal of the image by adjusting colors / contrast / white balance (i.e. gradational retouching), sharpness, removing elements or visible flaws on skin or materials, etc. Retouching is mostly done for magazine covers, photo shoots to give a better feel to the photo. Fig.2 is an example of Retouched image.

Fig.2. Before and after retouching image

International Journal of Engineering Innovation & Research
Volume 2, Issue 6, ISSN: 2277 – 5668

Copy-Move Attack

A copy move attack is commonly used to conceal parts of an image or to remove unwanted portions in an image. A portion from the picture is copied and pasted over any unwanted portion in the same image. It is also called as cloning Fig.3 is an example for copy move forgery.

Fig.3. After and before copy move attack

C. Morphing

Morphing is a special effect in motion pictures and animations that changes (or morphs) one image into another through a seamless transition. Most often it is used to depict one person turning into another through technological means or as part of a fantasy or surreal sequence. Traditionally such a depiction would be achieved through cross-fading techniques on film. Since the early 1990s, this has been replaced by computer software to create more realistic transitions.Fig.4 shows morphed image example.

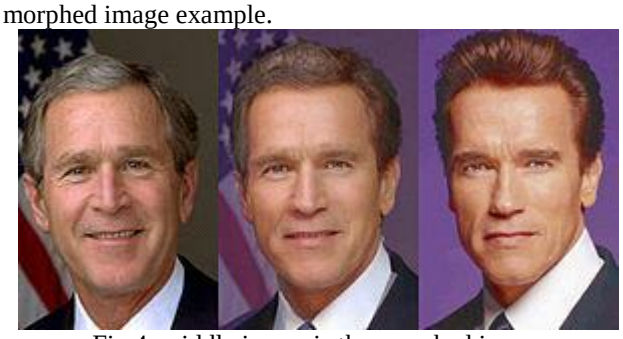

Fig.4. middle image is the morphed image

D. Geometrical transformation

Some images have a portion of the picture altered by some common geometric transformations such as translation, scaling and rotation. Forgers make a copy of the portion of the picture; make changes to it by geometrically modifying that portion of the image. This is shown in Fig.5.

Fig.5. (a) Original Image of evidence showing a cartridge

Fig.5. (b) Fake Image of evidence showing two cartridges; Second, scaled and transformed

III. STEGANOGRAPHY

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data.

Fig.6. (a) Original image

Fig.6. (b) Image to be hidden

Fig.6. (c) Output image

Tampering and Steganography, though both the techniques manipulate a digital image from its original capture but, they differ from each other at their vary purposes. One manipulates an image for the purpose of hidden communication whereas the other manipulates it to fake a fact and mislead the viewer to misbelieve the truth behind a scene.

Image Steganography is the process of secret communication where a piece of information (a secret message or an image, preferably encrypted) is encoded into the bits of an innocent looking cover image, in such a manner that the very existence of the secret information remains concealed without raising any suspicion in the minds of the viewers. Because of its inherent purpose of data hiding, Steganography requires the original and the Stego image to look alike. Steganography is more global in nature and offer vary little or no change to the image content in comparison to tampering which makes dramatic changes to the image content those are more local in nature. Fig.6 is an example of Image Steganography.

IV. RETOUCHING DETECTION TECHNIQUE

Advertisers and fashion and fitness magazines have always been in the business of creating a fantasy of sorts for their readers. Magazine covers and advertisements routinely depict impossibly beautiful and flawless models with perfect physiques. These photos, however, are often the result of digital photo retouching.

Retouched photos are ubiquitous and have created an idealized and unrealistic representation of physical beauty. A significant literature has established a link between these images and men's and women's satisfaction with their physical appearance. Impossibly thin, tall, and wrinkle- and blemish-free models are routinely splashed onto billboards, advertisements, and magazine covers. The ubiquity of these unrealistic and highly idealized images has been linked to eating disorders and body image dissatisfaction in men, women, and children. In response, several countries have considered legislating the labelling of retouched photos.

We propose a method to detect retouching in an image using human perception. Using PCA technique for face recognition [1], [2] or any other existing algorithm used for face recognition in forensics department recognize the model and obtain recent photos to compare it with retouched image. Using human perception to determine if the image is retouched or not.

PCA algorithm used:

1. The 'M' training or gallery images of size N × N pixels are converted to $N^2 \times 1$ size vector. Let these vectors be I_1, I_2, I_M.
2. The mean face vector is calculated using
   $m=1/M \quad \sum_{i}^{M}$
3. Subtract the mean face from the face vectors $\Phi_i=I_i-m$
4. The Eigen vectors and Eigen values of the covariance matrix $C = A^TA$ is calculated, where $A=[\Phi_1, \Phi_2 .... \Phi_M]$
5. The Eigen vectors ordered by sorting Eigen Values and the Eigen space is the matrix V consisting of Eigen vectors as columns. The difference face vectors are projected onto the Eigen space V.

Suppose the images in Fig.7 were taken in few hours of each other. There cannot be much change in skin color due in few hours. Thus we conclude that Fig.7 is a retouched image.

Fig.7. (a) Comparison image

Fig.7. (b) Retouched image

V. STEGANALYSIS

A practical example of embedding in the 1st LSB and up to the 4th LSB is illustrated in Fig.8. Embedding in the 4th LSB generates more visual distortion to the cover image as the hidden information is seen as "non-natural". Usually only 2 LSB are embedded as it does not create as much image distortion as 4 LSB embedding.

Bit Plane Slicing can be used to detect any anomalies in an image. If there are any anomalies, it means that the image is sending hidden data. In the Fig.8 example bit plane slicing of the Stegno image will show 4 plane of 1st image MSBs and 4 planes of 2nd image MSBs bits.

Bit Plane Slicing is very easy method to detect any anomalies in images. In the example it will even give the hidden data but for some other image steganography techniques we might only see the anomalies actual hidden data might not be retrieved by bit plane slicing.

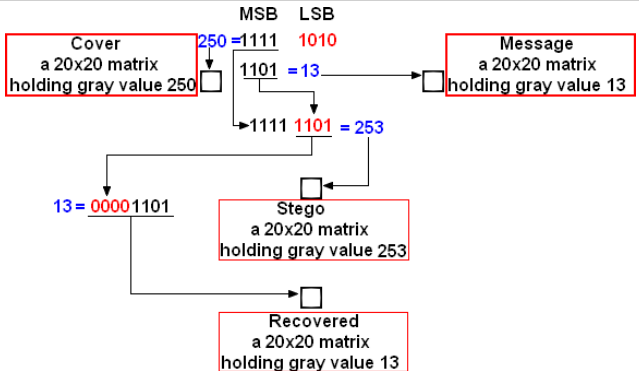

Fig.8. The effect of altering the LSBs up to the 4th bit plane.

For output image in Fig.9 bit plane slicing is as shown in the Fig.10 if the MSB of the middle image in Fig.9 is put in LSB first image of Fig.10.

Fig.9. Stegnography

Fig.10. Bit plane slicing for output image of Fig.9

VI. Conclusion

A lot of research has been done on passive tamper detection techniques and still a lot of work is going on worldwide to successfully detect tampering in digital images. In this paper we have reviewed retouched image detection method .There exits many other techniques for different type of tampering such as detection based on examining the lighting environment, camera feature based detections, studying the statistical and geometric properties. We also reviewed a steganalysis technique.

Future Work

All of the tamper detection techniques are found to be tampering sensitive i.e. they are capable of identifying only a particular type of tampering and not all types of tampering. Thus, future research on detection of Image Tampering should focus on developing a false proof method that is independent of the tampering technique as well as the image format.

References

[1] Nedevschi S, Peter I.R. , Dobos I.-A. , Prodan C.," An improved PCA type algorithm applied in face recognition", IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), 2010, pp. 259-265.

[2] Bozorgtabar B., Noorian, F., Rezai Rad G.A., 5th International Symposium on Telecommunications (IST), 2010,pp. 801-805.

[3] Pradyumna Deshpande , Prashasti Kanikar, "Pixel Based Digital Image Forgery Detection Techniques", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp. 539-54.

[4] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, Volume 90,Issue 3, March 2010, pp. 727-752.

[5] G. R. Elwin J , Aditya T S , M. Shankar S," Survey on Passive Methods of Image Tampering Detection", International Conference on Communication and Computational Intelligence, 2010,pp .431-436.

[6] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi, "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), 2012, Volume (6), Issue (3).pp.168-187.

Author's Profile

Hiral Shah
Student, V.E.S. Institute of Technology, University of Mumbai, India.
Email: hiral.shah.06@gmail.com

Prajakta Shinde
Student, V.E.S. Institute of Technology, University of Mumbai, India.
Email: prajaktashinde.7@gmail.com

Jaya Kukreja
Student, V.E.S. Institute of Technology, University of Mumbai, India.
Email: jayakukreja18@gmail.com