Digitized Authentication For Image Forensics

D.S.Sellva Manoj, G.Sujatha

Abstract— It is often desirable to determine whether it has been modified in any way from its original recording. The JPEG format affords the engineers to provide many implementations which gives rise to widely varying JPEG headers which provide image authentication. A camera signature that is extracted from an JPEG image which contains the below stated information about the (1) Quantization tables, (2) Huffman codes, (3) thumbnails, and(4) EXIF format. The signature is highly distinct across 1.3 million images spanning 773 different cameras and cell phones. Specifically, 62% of images have a signature that is unique to a single camera, 80% of images have a signature that is shared by three or fewer cameras, and 99% of images have a signature that is unique to a single manufacturer. The signature of Adobe Photoshop is also shown to be unique relative to all 773 cameras.Using these signature we can be able to find whether the Evidence is in original form or it is being modified. The method of Comparing the Hash values are used to provide the integrity of the image. If the Provided Evidence Contains any Secret message , find whether the Message is in original form or its being tampered .

Index Terms— Digital Forensics, Digital Tamper, JPEG Headers, EXIF .

1 INTRODUCTION

DIGITAL images are now routinely introduced as evidence into courts of law. It has, therefore become critical to verify the integrity of this digital evidence.Digital forensics techniques have been developed to detect various traces of Digital tampering

The traces of Digital Tampering are as stated region duplication [1],[4]; resampling [5],[6];color filter array artifacts [7],[8]. However, relatively benign modifications either cannot be detected by these techniques, or render these techniques ineffective. It is often desirable to determine if a digital image has been altered in any way from the time of its recording, including manipulations as simple as cropping .In contrast, it has been previously shown that exchangeable image file format(EXIF) headers [9] and JPEG quantization tables [10],[13] used by cameras and software manufacturers are somewhat distinct, and can, therefore, be used to determine if an image has been altered from its original recording.

Building on this earlier work, the various aspects of JPEG format can be used for authentication. Unlike previously several features of the JPEG format are not considered, namely properties of the run-length encoding employed by the JPEG standard, and aspects of the EXIF header format. This analysis is validated on over 1.3 million images spanning 33 different camera manufacturers and 773 different camera and cell phone models.

- *D.S.Sellva Manoj is currently pursuing masters degree program in information security and computer forensics in SRM University,INDIA, PH-+91 9940983622. E-mail: reseaux05@gmail.com*
- *G.Sujatha is Asst.Prof Department of information technology in SRM University, Country, E-mail: sujatha.g@ktr.srmuniv.ac.in,*

2 LITERATURE REVIEW

A Common manipulation in tampering with digital images is known as region duplication, were a continuous portion of pixels is copied and pasted to a different location in the same image.

Several general techniques in digital image forensics may be applied to detect duplicated regions. For JPEG images , a double JPEG quantization is usually a telltale sign of tampering operations(include region duplication), and can be detected based on the histograms of quantized DCT coefficients. These duplicated regions are well blended into the surroundings at the target locations , and become very difficult to detect visually.

Copy move image tampering is one of the frequently used technique to hide or manipulate the content of the image.some part of the same image or some other image is pasted on another part of image. To detect the region of some other image statistical methods may work but if the region pasted belongs to the same image then it's quite difficult to detect this forgery.

Resampling detection, meanwhile a standard tool in image forensics, it is helpful to investigate the resampling detection in re-compressed JPEG images. While a reliable detection for almost arbitrary geometric transformations in uncompressed image has been reported, it is well-known that detection performance severely drops already for moderate JPEG compression.

3 PROPOSED MODEL

The existing system tells that an image that is being taken from any Digital media can be given as an Evidence , so that the evidence will be either sent via network where an intermediator may Tamper the Evidence. The Tampering of an image can be found by the receiver by Extracting the Digital Evidence's camera signature using an tool called Exchangeable Image File Format (EXIF) .

Using this tool the receiver can Extract so many Image file Directories (IFD) into which the metadata's of the evidence are hidden, some of the metadata are: (1) Camera Make & Model, (2)Thumbnail, (3)Zooming length, (4) Gps (5) Date and Time

By extracting these metadata we can be able to compare these data's with the original image and check whether the Evidence is Tampered or not. The signature is used for an authentication using the JPEG Headers.

The Proposed system shows that we can be able to find whether the image is being tampered using the Jpeg Headers and EXIF tool, and also we can be able to find whether the evidence is having any hidden message using the LSB Steganography technique.

If the Evidence is having any hidden message & if the evidence is tampered , then we cannot be able to retrieve the original image that is being hidden inside the given evidence. Because the evidence values may differ before and after the attack is generated in the image. Here We are generating Three kinds of attack on the evidence a) Crop Attack, b) Pixel Attack, c)Tamper Attack . These attack's are generated by the intermediator and finally the receiver receives the attacked image and thinks that the received one is the original image from the intended sender.

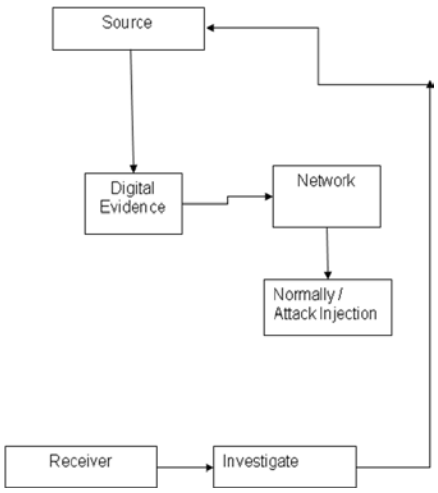

fig 1.Solution Architecture

Fig 1 presents how Evidence is being send form the source to the destination and in the middle how an attack is being injected and how the receiver is going investigates the Tampered evidence is shown. Initially Source sends the evidence to the appropriate receiver via the network, the receiver receives the evidence and find's whether the received evidence is being tampered or not.

3.1 EVIDENCE SELECTION

The Evidence selected should be in the digital form , so that the JPEG Headers & EXIF (Exchangeable Image File Format) can be used later to find whether the received evidence is tampered or not .If the Evidence is not an Digital media the tool will not be able to find whether the produced one is being tampered or it is original form.

Initially the sender selects the Evidence and sends to the intended recipient using the Destination key. The receiver can enter the key and can receive the evidence. The evidence is an JPEG image where we can easily extract the Headers and the signature of the image using EXIF. The images that are not JPEG are eliminated , and if the image is not an three channel colour image, it's also eliminated.

3.2 ATTACK INJECTION

The Evidence that is being send to the receiver can be tampered in the middle by three way's as mentioned below (a) Crop Attack , (b) Pixel Attack , (c)Tamper Attack.

3.2.1 CROP ATTACK

Basically the attacker receives the original image and keeps it and crop's some of the image region based on the width and height of the produced image and send's the cropped image to the receiver , the receiver doesn't know that the image is cropped in the middle and he thinks that the he received the original image form the intended receiver. The following figure shows you the Exact result of the Attack:

(a) Original image

(b) Received image

fig 2. Cropp Attack

3.2.2 PIXEL ATTACK

This type of attack cannot be visually identified in the initial state by the receiver because he thinks that the image is of originally like this , but the attacker adds some values to the RGB of the given image and sends the image to the receiver. The below fig shows the exact attack generation:

(a) Original image (b) Received image

fig 3.Pixel Attack

3.2.3 TAMPER ATTACK

The attacker Receives the image from the sender and edits the image using the Photoshop or any other editing tool and sends that image to the intended recipient like an sender. The below show figure shows you the way of attack will be generated.

(a) Original image (b) Received image

fig 4. Tamper Attack

4 EVIDENCE SELECTION

After the Attack Injection the Attacker sends the attacked image the intended recipient, initially the receiver doesn't know that the received evidence is an original one or an tampered .

For this verification , in this application we use JPEG Header tool which includes the EXIF metadata's which will be easy to identify whether the image is original or an modified one.

For Example in the above tampered figure 4.3 you can see that both of the images are of same and it seems like both are original but while using this tool we can find that the image is an edited one using the Photoshop tool.

5 STEGANOGRAPHY

The sender not only sends the evidence simply he embeds some text inside the evidence using the LSB technique and encrypting the message using the ECC (Elliptic Curve Cryptography) where this can be extracted by only the receiver using the encryption key to decrypt the message.

The LSB technique is the one where we are hiding the message inside the neighbour regions where they are in least bit and we use the ECC method to encrypt the text and also to decrypt the text.

If the given evidence is being tampered in the middle by an attacker , we cannot be able to extract the hidden message from the evidence.

6 CONCLUSION

The cameras produce distinct JPEG headers that facilitate both forensic and ballistic analysis. This analysis does not differentiate between benign and nefarious modifications. While this is a stringent criteria, it is useful in certain arenas. This forensic analysis can be useful in a legal setting, for example, where it is important to determine if evidence has been altered in any way.

As with any forensic technique, it is important to consider countermeasures. In our case, a determined forger could conceal their traces of tampering by extracting the signature of a camera, modifying the image, and then resaving the image with the appropriate EXIF format and all of the appropriate parameters: image size, image quantization table, image Huffman code, thumbnail size, thumbnail quantization table, and thumbnail Huffman code. While this is certainly possible, it is currently beyond the scope of popular photo-editing software. Our analysis is also vulnerable to a standard rebroadcast attack in which a digital image is manipulated, printed, and re-photographed.

In this Digital World , the JPEG images play an vital role either as an entertainment or as an Evidence that is being produced in the courts of law . This evidence can easily be Tampered using any of the Products that are available in the market. Thus this Forensic Technique can be useful in a legal setting, for example, where it is important to determine if the evidence is being Tampered or it is in the original form. We can also be able to find whether the given evidence is having any Secret message that is being hidden inside. We can first detect the hidden message then we can proceed for the Evidence Analysis, where we are going to check whether the hidden message is being Tampered in any way.

REFERENCES

[1] J. Fridrich,D. Soukal, and J. Lukáš, "Detection of copy move forgery in digital images," in *Proc. Digital Forensic Re-*

search Workshop, Cleveland, OH, Aug. 2003.

[2] A. Popescu and H. Farid, Exposing Digital Forgeries by Detecting Duplicated Image Regions Department of Computer Science, Dartmouth College, Tech. Rep. TR2004-515, 2004.

[3] S. Bayram, H. T. Sencar, and N. Memon, "A survey of copy-move forgery detection techniques," in *IEEE Western New York Image Processing Workshop*, Rochester, NY, 2008.

[4] X. Pan and S. Lyu, "Region duplication detection using image feature matching," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp.857–867, Dec. 2010.

[5] A. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of re-sampling," *IEEE Trans. Signal Process.*, vol. 53, no. 2, pt.2, pp. 758–767, Feb. 2005.

[6] M. Kirchner and T. Gloe, "On resampling detection in re-compressed images," in *Proc. IEEE Workshop on Information Forensics and Security*,2009, pp. 21–25.

[7] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," *IEEE Trans. Signal Process.*, vol. 53, no.10, pp. 3948–3959, Oct. 2005.

[8] M. Kirchner, "Efficient estimation of CFA pattern configuration in digital camera images," in *Proc. SPIE Conf. Media Forensics and Security*, San Jose, CA, 2010.

[9] P. Alvarez, "Using extended file information (EXIF) file headers in digital evidence analysis," *Int. J. Digital Evidence*, vol. 2, no. 3, pp.1–5, 2004.

[10] H. Farid, Digital Image Ballistics From JPEG Quantization Department of Computer Science, Dartmouth College, Tech. Rep. TR2006-583, 2006.

[11] J. Kornblum, "Using JPEG quantization tables to identify imagery processed by software," *Digital Investigation*, vol. 5, pp. S21–S25, 2008.

[12] H. Farid, Digital Image Ballistics From JPEG Quantization: A Followup Study Department of Computer Science, Dartmouth College,Tech. Rep. TR2008-638, 2008.

[13] E. Kee and H. Farid, "Digital image authentication from thumbnails,"in *Proc. SPIE Symp. Electronic Imaging*, San Jose, CA, 2010.