NSF Workshop on Big Data Security and Privacy
University of Texas, Dallas, September 16th-17th, 2014
Authenticity of Images in Social Media

Balkirat Kaur, Malcolm Blow, Justin Zhan, North Carolina A&T State University
Greensboro, NC, USA
bkaur1@aggies.ncat.edu, mablow@aggies.ncat.edu, zzhan@ncat.edu
Agenda

• Introduction
• Problem definition
• Related Work
• Our Approach
• Method and explanation
• Conclusion
Images and Privacy

Privacy of images in big data
• Smart phones made clicking and posting easier.
• One image clicked per day = Numerous amounts of Data

Facebook Results by [www.Web-strategist.com/blog](http://www.Web-strategist.com/blog/)
• More than 60 million active users.
• More than 14 million images uploaded everyday.

MySpace Results by [www.Web-strategist.com/blog](http://www.Web-strategist.com/blog/)
• On average, 300,000 people join everyday.
• 8 Million images uploaded everyday.

Originality of images ...???
Importance of our work

- Flickr … image database
- Pinterest… visual discovery tool
- Difficulty to identify the originality
- Enlarge and amplified social data
- Security related issue, copyright issues.
- My approach is one step towards the privacy of images; originality will incur privacy
Importance of our work

- Large Big data social networks
- Analyzing security of images in social media to discover important facts, e.g., Copyright issues

Leads to a secure & trustworthy data
Security concerns..?

- Development of image processing softwares e.g. Avid, Vegas etc.
- Distinction between original and modified is difficult.
- Unexpected exposure of one’s social environment and personal information.
- Images can be posted on social media without confirmation of originality.
- Tagging is allowed without consent of individuals leading to unwanted disclosure and privacy violations.
Related Work

- Reversible Watermarking techniques in medical images.
- Image interpolation by computing the interpolation coefficient for forged and original image using expectation-maximization.
- Hybrid image authentication watermarking techniques using a combination of fragile and robust watermark.
- Digital Watermarking techniques using least significant bit and discrete cosine transformation for the digital watermarking of images.
- Watermarking/encryption algorithms for the verification and reliability of the medical images.
- Using semantic annotations, face recognition and user-defined privacy rules.
Behind the Camera..???

TURNING LIGHT INTO A DIGITAL FILE
How your digital camera converts captured light into image pixels

The colour filter array
The 'photosites' on the sensor only measure the brightness of the light, not its colour. So that colour information is gathered, each photosite has a red, green or blue filter. These are arranged in a mosaic known as a Bayer pattern, after the boffin that came up with it. He found that by using twice as many green filters as blue or red, you got a sharper image. A demosaicing process turns this raw data into the full-colour grid of pixels in the recorded images.
Digital Image in a camera

- Defacto Image format of most digital cameras is Jpeg.
- 3-channel image into luminance/chrominance channel YCbCr.
- Each channel partitioned into 8*8 pixel blocks.
- Sampling and Quantization using 2-d Discrete cosine Transform(DCT).
- DCT coefficients subjected to Huffman Coding.

Varied bits/Pixel values

A. 1-bit (Bitmap)
B. 8-bit (Grayscale)
C. 8-bit (Indexed color)
D. 24-bit (RGB)

Image Courtesy: pirate.shu.edu/
Each block $f_c(.)$ in an image is converted to Frequency space $F_c(.)$ using a 2-d Discrete Cosine Transform.

$$F_c(u, v) = \alpha_{u,v} \sum_{x=0}^{16} \sum_{y=0}^{16} f_c(x, y) \cos \left( \frac{(2x + 1)u\pi}{16} \right) \cos \left( \frac{(2y + 1)v\pi}{16} \right)$$

Each DCT coefficient $F_c(.)$ is quantized by $q_c(.)$.

$$\hat{F}_c(u, v) = \text{round} \left( \frac{F_c(u, v)}{q_c(u, v)} \right)$$

Here,

- $c$ denotes a specific channel
- $\alpha_{u,v}$ is a normalizing scale factor
- $f_c(.)$ is the underlying pixel values

Depending on the specific frequency $u,v$ and channel $c$, each DCT coefficient $F_c(.)$ is quantized by $q_c(.)$. This is primary stage of information loss, so, DCT coefficients are subjected to Huffman Coding.
Digital image in a Camera

- Compression and quality are the two factors controlled and balanced by camera manufacturers in different make and models.
- JPEG is the primary still image format for most of cameras because, it maximizes the total number of images you can store, allows for a fast write to the memory and above all, it is compatible with email and internet in general.
- Jpeg compression utilize the sensitivity of the human eye to a low frequency area over a high frequency area.
- Color space conversion module transforms the RGB encoding into YCbCr coding using:
  \[ Y = 0.299R + 0.587G + 0.114B \]
  \[ Cb = 0.564B - 0.564Y \]
  \[ Cr = 0.713R - 0.713Y \]
- Downsampling reduces the sampling rate of the converted data and the 2-D DCT transforms the data into frequency domain.
- Quantization eliminates high frequency components and small amplitude elements.
- Entropy encoder (Huffman) decreases the number of bits to represent the image.
Our Approach

Originality of an image is checked by creating our own image signature from the values of features of an image which include:

- Make and model of the camera.
- Date and time of image capture.
- JFIF format of the image
- Huffman and quantization values.

All these values including date and time of image capture etc. can be got from image metadata. This combination of an image signature is used to distinguish between an original image and a modified image. Experiments are done using metadata from the image Hex file using a hex editor.
### Our Approach

<table>
<thead>
<tr>
<th>Name</th>
<th>Hex</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOI</td>
<td>FFD8</td>
<td>Start of Image</td>
</tr>
<tr>
<td>EOI</td>
<td>FFD9</td>
<td>End of Image</td>
</tr>
<tr>
<td>SOF</td>
<td>FFC0</td>
<td>Start of Frame</td>
</tr>
<tr>
<td>SOS</td>
<td>FFDA</td>
<td>Start of Scan</td>
</tr>
<tr>
<td>DHT</td>
<td>FFC4</td>
<td>Define Huffman Table</td>
</tr>
<tr>
<td>DQT</td>
<td>FFDB</td>
<td>Define Quantization Table</td>
</tr>
<tr>
<td>FFE0</td>
<td></td>
<td>Jpeg Marker</td>
</tr>
</tbody>
</table>

**Jpeg Header Markers for a Hex file**

Jpeg header markers are used together to read the hexadecimal file of an image, to differentiate between an original image and a tampered image. Famous example of lena.jpg is used to define the various parameters in the hex file of this image.
FFD8 defines the start of a jpeg image and header starts at FFE0. Similarly, all quantization tables start from FFDB, and FFC4 defines the starting of the Huffman table.
Reading the Hexadecimal file of an Image

Frame Header and Huffman Table in lena.jpg
Datasets

- Images from different makes and models of cameras were used.

- Duplicates from these images is created using various techniques including MS Paint, Adobe Photoshop, and certain open source watermarking and image manipulation softwares.

- Manipulations include but are not limited to:
  - Cropped Images
  - Region Duplication
  - Saturation/Exposure
  - Hidden Data
  - Grayscale
Original vs Tampered Image

(a) Original Image
(b) Manipulated Image

Image tampered by hiding a text file behind the original image.
Original vs Tampered Image

(a) Original Image  
(b) Manipulated Image

Image (b) is the cropped version of original image (a).
Image (b) is a black and white version of original image (a).
Experimental Evaluation

- Original Images from different make and models of cameras
- Modified images using various softwares and techniques.
- About 450 images were tested using this technique.

<table>
<thead>
<tr>
<th>Tampering method</th>
<th>No. of tested images</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cropped images</td>
<td>142</td>
</tr>
<tr>
<td>Region duplication</td>
<td>69</td>
</tr>
<tr>
<td>Saturation/exposure</td>
<td>87</td>
</tr>
<tr>
<td>Hidden data</td>
<td>91</td>
</tr>
</tbody>
</table>
Conclusion & Future work

- Our system will allow social media websites to identify JPEG files that have been altered from their original state.
- Add ability to identify the alterations.
- Identifying an algorithm to implement it in social media.
- Control the tagging in the images.
Thank You!!!