ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 6, No.18 , November 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Practical implementation of a methodology for digital images authentication using forensics techniques

Francisco Rodríguez-Santos[1], Guillermo Delgado-Gutierréz[1], Leonardo Palacios-Luengas[1] and Rubén Vazquéz-Medina[1,2]

[1] ESIME Culhuacan, Instituto Politécnico Nacional, Coyoacán, D. F. 04430, México
frodriguezs0901@alumno.ipn.mx

[2] CMP+L, Instituto Politécnico Nacional, Ticoman, D.F. 07340, México
ruvazquez@ipn.mx

Abstract

This work presents a forensics analysis methodology implemented to detect modifications in JPEG digital images by analyzing the image's metadata, thumbnail, camera traces and compression signatures. Best practices related with digital evidence and forensics analysis are considered to determine if the technical attributes and the qualities of an image are consistent with each other. This methodology is defined according to the recommendations of the Good Practice Guide for Computer-Based Electronic Evidence defined by Association of Chief Police Officers of UK; the methodology certainty level is verified by an efficiency coefficient, calculated by the quotient of the number of correct resolutions and the total number of analyzed images. This methodology can help to determine if a specific digital image can be used as evidence, and thereby, help to clarify events or incidents with legal, civil, administrative or criminal implications. Another advantage of the methodology is that it can be applied with open source software tools.

Keywords: *Forensic Science, Digital Evidence, Image Authenticity, Forensic Analysis Methodology, Digital Image Processing, Image Technical Attributes.*

1. Introduction

Today it is very common to find digital images due to the high availability of digital cameras in mobile phones. For some people, a picture may be irrelevant, but for some others, it may represent evidence which could be used to clarify facts with legal, civil, administrative or criminal implications. Therefore, a digital image could have a really high impact in our life and it could be much more representative than the oral or written description of an event, especially if it is considered that the description of that event could be distorted by a person, since time causes human memory deficiencies. With the technological advancement in mobile devices, the digital images have become ubiquitous today. However, modifying a digital image without any obvious traces is not a difficult task with the image editing software available these days. Grabler et al. [1] proposed a demonstration-based system for a visual step-by-step succinct generation tutorials of photo manipulations, which include changing the color of the eyes, teeth bleaching and enhancement of the sun setting, among others. Specialized software tools for digital images edition have potentiated the techniques of image manipulation. These tools allow almost everyone being able to improve the visual quality of an image in an effortless way according to their preferences, needs or interests. Also, these tools allow changing the perception of an event captured in a digital image. The motivations for these changes in digital images could be diverse. Some persons might edit a picture to have fun or to sell something. However, some others may try to involve someone in a wrongful act, or to obtain an illegal benefit.

Garry and Gerrie [2] showed that changing an image or improving its quality, may cause distortion of the reality perception, creating false records and affecting the memory of the people who watch it. Considering digital images that contain sensitive information that could be used as evidence, it is necessary to ensure the images' authenticity, in order to prevent that they are used in a malicious way to damage others. Farid and collaborators in different works showed techniques to determine if an image has been modified or not. Johnson and Farid in 2007 [3] described how such composites can be detected by estimating a camera's intrinsic parameters from the image of a person's eyes; Farid in 2009 [4] presented an overview of the passive techniques for detecting images forgery considering an image forensics context; Farid and Bravo in 2010 [5] showed that the visual system is remarkably inept at detecting simple geometric inconsistencies in shadows, reflections and perspective distortions, and they showed computational methods that can be applied to detect the inconsistencies that seem to elude the human visual system; Kee and Farid in 2010 [6] described a technique for measuring lighting conditions in an image, and described its use for detecting photographic composites; and finally, O´Brien and Farid in 2012 [7] described the existence of forensic techniques to detect geometric or statistical inconsistencies that result from specific forms of photo manipulation. Particularly, they

described a technique based on basic rules of image reflection and perspective projection.

There are several studies about image forensics methods that could help to determine the images' authenticity. Luo et al. [8] presented a survey and the implementation challenges about forensics passive technology. Hwang and Har in 2013 [9] proposed a re-interpolation algorithm which uses the characteristics of interpolation to detect forged images. Peng and Li in 2014 [10] proposed a method to identify among natural images, which represents a real fact, and which is a computer-generated graphics based on statistical and textural features. Hwang and Har in 2014 [11] showed that interpolation is an effective way to analyze digital images and define an identification method for digital image forgery and filtering region. On the other hand, Cao et al. [12] proposed an algorithm capable of concealing the quantization artifacts that are left in a single JPEG compressed image to hide the JPEG compression traces, which could make harder to find modifications in a digital image.

When an image is presented as evidence to clarify a sensitive case, it must be verified in order to determine if the fact that represents is real. Therefore, the process defined to verify the image authenticity must be robust, and it is based on international guides and best practices about evidence management.

This work proposes a methodology to determine if a JPEG image is authentic or not, and it is based on the features analysis of digital images using forensics techniques. The analyzed image features are the metadata, the image thumbnail, the camera traces derived from the demosaicing process and the signatures of software used to edit digital images. The demosaicing process allows reconstructing a full color image from the incomplete color samples output from an image sensor overlaid with a color filter array (CFA). The proposed methodology includes a set of methods that are applied independently, each one defines different evaluation metrics; which are used to define a technical resolution (verdict) that indicates if the analyzed digital image is authentic, post produced or modified. Finally, with this information, a technical dictum is generated in accordance to the NIST SP800-86 [13] guide.

2. Proposed methodology

The proposed methodology is a passive technique for image forensics that operates in the absence of any watermark or signature. The used techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying features of a digital image. The proposed methodology is not intended to detect specific changes in JPEG format images, it only determines if the analyzed images were modified or not, without specifying the used procedure and the image region that was modified. In addition, the performed analysis does not require the original image without any modifications or some extra attributes associated with it. The proposed methodology was basically defined according to the *Good Practice Guide for Computer-Based Electronic Evidence* defined by Association of Chief Police Officers of UK [14], although it also considers other international guidelines related with the digital forensic analysis and evidence management [15-20]. The proposed methodology considers that the analyzed images can be computer-based electronic evidence subjected to the same rules and laws that apply to documentary evidence.

The proposed methodology consists of 4 steps: 1) Collection, 2) Extraction of the image's technical features, 3) Analysis of the image's technical features, and 4) Issuance of the dictum.

2.1 Step 1: Collection.

This step includes two activities:

i) **Documentation.** The context of the incident, the device that generated the image, and the container device, in which the image is presented to be analyzed, must be documented. This is the first registration of the chain of custody on the methodology.
ii) **Saving and integrity verification.** The hash value (SHA 256) of the original image, and subsequently two identical copies of the original image must be obtained. It must be verified that the copies have the same hash value than the original image. One of these copies will be used for the analysis, and the other copy must be safely stored with the original image in order to support future comparisons. The registration of the validation that the three hash values are identical must be included in the custody chain of the process.

2.2 Step 2: Extraction of the image's technical features.

This step involves three activities:

i) **Format Verification.** The image format must be verified. It must be confirmed that the header of the image corresponds to a JPEG format. If the header does not match, the analysis process must be concluded and a register of this condition must be specified in the chain of custody of the process.
ii) **Features extraction.** If the image format matches the kind of image, then, the following information from the digital image must be extracted:

a. Image metadata.
b. Image thumbnail. It is the reduced version of the image to be analyzed, and it is at the header of the image file.
c. Camera traces. Footprints of the demosaicing, which is used to complete the pixels of the image when is created.
d. Compression signatures. Evidences in the image file of some image editing software.

iii) **Registration.** Image's technical features must be registered according with the chain of custody of the process. This registration must contain date, time and responsible of the extraction, as well as a brief description of the found technical features.

2.3 Step 3: Analysis of the image's technical features.

In this step the four technical features extracted from the digital image are analyzed in order to authenticate the digital image. For this purpose, the following premises must be considered as the analysis objects:

i) **Analysis of image metadata.** It is considered that when a digital image is modified, it may lose some metadata generated at the time of its capture. Thus, it is important to verify if the digital image preserves the metadata generated at the time of its capture. The image metadata considered are: brand and model of the camera, compression by software, orientation, date/time of capture and orientation of the image thumbnail.

ii) **Analysis of image thumbnail.** There are many software programs for image processing which are used to modify digital images, but these programs do not necessarily modify the image thumbnail. In this way, a thumbnail should be generated from the analyzed image, and then it must be compared pixel by pixel with thumbnail in the metadata file. Both must have the same dimensions. If the difference among the image thumbnails pixels is not significant (when at least the 90 percent of the thumbnails pixels are equals), it is defined that the image was not modified, but if the difference among them is significant, it is defined that the image was modified.

iii) **Analysis of camera traces.** This activity intends to verify the integrity of digital images and to detect the traces of tampering without using any protecting pre-extracted or pre-embedded information at the analyzed image [20]. When a digital image is captured, the camera makes an interpolation processing denominated demosaicing in order to complete the intensity values (pixels) of the digital image. This process affects the resolution and quality of the digital image. Thus, if the image has been modified, it is possible to find inconsistencies at the plane Y on the digital image, assuming that the color space is YCrCb. Plane Y suffers less loss of information when the JPEG compression is applied and the affectation by modification can be detected.

iv) **Searching compression signatures.** This activity intends to detect when an image editing software was used to make some change in a digital image. Regularly editing software leaves a compression signature in the header of that digital image.

At all time, the chain of custody must be considered in the step 3, and the registration of the hash values calculated when each action taken is performed.

Subsequently, it must be issued a technical resolution of each technical image's feature analyzed. In this resolution, it must be indicated whether the image approves or disapproves the testing. Finally a global technical resolution must be emitted to determine the image authenticity.

2.4 Step 4: Issuance of the dictum.

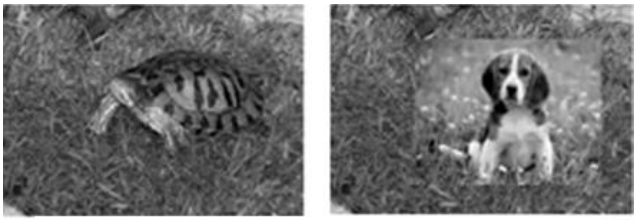
A dictum (verdict) that summarizes the conclusions of the analysis must be issued. This dictum must contain the image name, analysis date, image format, make and model of the camera used to capture the digital image, hash value of the image, brief description of the analysis performed, name of the analyst, results obtained at each step, and final technical resolution which indicates if the analyzed digital image is authentic, post produced or modified.

3. Technical application of the proposed methodology

In order to show the results of the application of this methodology, the following tools are going to be used: *Exiftool* to extract metadata, *Jhead* to extract the thumbnail image associated with the digital image, *JForensicsPG 1.0* an own software developed in Java 1.6 to generate a new thumbnail of the digital image and compare both thumbnails (extracted and generated); *JForensicsPG 1.0* is used for the camera traces analysis too, and *JPEGSnoop* that allows extracting the information of the header of the image, in order to verify the presence of any compression signature. Is important to mention that the software developed has intellectual property registration to the INDAUTOR, which is the organization that regulates the registration of software in Mexico. *JForensicsPG 1.0* has

the registration number 03-2012-022810521500-01 dated March 15, 2012.

For the example of the analysis of the image's technical features, two images are used. The first one image is named ORIGINAL.jpg, which is an image in the same state as it was generated at the time of its capture (with no modifications) with a device SAMSUNG GT-S5670L. The second one image is named MODIFICADA.jpg, which is an image modified with *Picasa 3* software; for generate MODIFICADA.jpg there was included in ORIGINAL.jpg a cut of another image. Fig. 1 shows the images used for the example.



a) *b)*

Fig. 1 Images used for the application analysis example; *a)* Image *ORIGINAL.jpg*, b) Image *MODIFICADA.jpg*.

3.1 Analysis of image metadata

In this analysis the following metadata are extracted: i) camera's make, ii) camera's model, iii) software compression, iv) image's orientation, v) date/time of image capture and vi) thumbnail's orientation. If it is possible to obtain at least four of these six metadata, this step is going to be approved; otherwise the result is going to be disapproved. Fig. 2 shows an example of the metadata extracted from an image without any change (ORIGINAL.jpg) using *ExifTool*.

```
ExifTool Version Number         : 7.38
File Name                       : ORIGINAL.jpg
Directory                       : C:\Users\Frank_07\Desktop
File Size                       : 1411 kB
File Modification Date/Time     : 2012:01:19 12:32:46
File Type                       : JPEG
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Make                            : SAMSUNG
Camera Model Name               : GT-S5670L
Orientation                     : Horizontal (normal)
Software                        : Imagen Digital ACD Systems
Modify Date                     : 2012:01:19 11:32:44
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/40
F Number                        : 2.6
Exposure Program                : Aperture-priority AE
ISO                             : 100
Exif Version                    : 0220
Date/Time Original              : 2011:10:29 18:10:53
Create Date                     : 2011:10:29 18:10:53
Max Aperture Value              : 2.6
Metering Mode                   : Center-weighted average
Flash                           : No Flash
Focal Length                    : 3.8 mm
User Comment                    : User comments
```

Fig. 2 Metadata of the image *ORIGINAL.jpg*.

Figure 3 shows the metadata obtained of MODIFICADA.jpg using *ExifTool*. The only change made was pasting a cut of another image with *Picasa 3* software. There is observed that make, model, orientation, software and date/time of capture are not found any more when the change was made in ORIGINAL.jpg. Therefore, for MODIFICADA.jpg result of this point is disapproved.

```
ExifTool Version Number         : 7.38
File Name                       : MODIFICADA.jpg
Directory                       : C:\Users\Frank_07\Desktop
File Size                       : 24 kB
File Modification Date/Time     : 2011:10:29 19:14:04
File Type                       : JPEG
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Exif Byte Order                 : Little-endian (Intel, II)
Image Width                     : 240
Image Height                    : 320
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 240x320
-- press any key --
```

Fig. 3 Metadata of the image *MODIFICADA.jpg*.

3.2 Analysis of image thumbnails

For this action, it is necessary to extract the thumbnail associated to the image which is being analyzed and then a new thumbnail from this image must be generated. Both thumbnails must have the same dimensions. Then, the thumbnails (extracted and generated) must be compared pixel by pixel (considering the same position pixels comparison). For each pair of pixels compared, the difference should not exceed the absolute value of 8. This value was chosen as a maximum difference because it does not represent a significant change in the color perception of the human eye (considering this premise for 8-bit images). If more than ten percent (10%) of pixel differences vary for more than the absolute value of eight, the result of this phase is disapproved, otherwise it is approved. Fig. 4 shows graphically this comparison process:

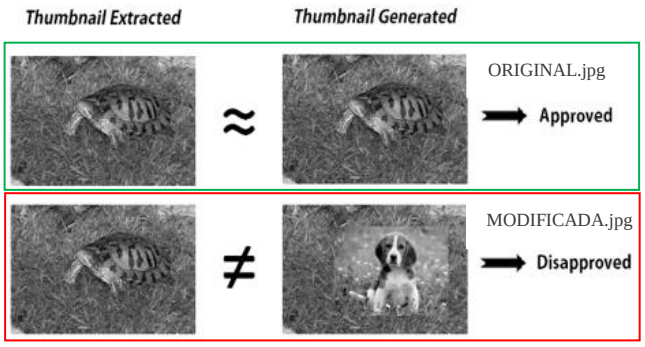


Fig. 4 Graphical thumbnails comparison example.

3.3 Analysis of the camera traces

This process analyzes 3×3 blocks of pixels of the Y plane of the digital image as proposed in [21]. This process calculates the values that must be generated in the demosaicing process for each 3×3 block, starting from left upper corner, up to the right bottom corner. The way to find the corner values of 3×3 blocks must be performed by increments of 2. For example, the position of the upper right corner of the first block is (0, 0), for the first horizontal offset, the position of the upper right corner of the second block would be (2, 0), the upper right corner of the third block would be (4, 0), and subsequently up to the end of horizontal blocks. Then, vertical position will be increased in 2 and horizontal position is reset (0, 2) to begin with horizontal offsets in the same way, up to up to go entirely through the Y plane in horizontal and vertical way. If the plane Y is not a multiple of 3, only must be gone up to the last position in which it is possible to extract an entire 3×3 block of pixels, i.e., it may not be scrolled maximum the last 2 lines of pixels, either horizontally or vertically.
Through this process, the four values at the corners of each block are extracted and then the remaining five values of the block are calculated. Notice in Fig. 5 that the black numbers correspond to the values of the corners of each block and numbers in gray are the values calculated.

Example:

(32 + 54) / 2 = 43

(32 + 48) / 2 = 40

(48 + 47) / 2 = 47.5

(47 + 54) / 2 = 50.5

(32 + 48 + 47 + 54) / 4 = 45.25

32	43	**54**	59	**63**			
40	45	51	56	61			
48	48	**47**	53	**58**			
41	42	44					
33	37	**40**		**52**			

Fig. 5 Example of how a digital camera makes the interpolation process (demosaicing).

Then, the calculated values are compared with the values of the same position in the plane Y of the image. As in the thumbnail comparison, the difference among same position pixels of both planes does not have to be greater than the absolute value of 8. The reason for establishing this difference is because this is a non-significant difference in the color perception of the human eye. Subsequently, the following metric must be applied: If more than ten percent (10%) of pixel differences vary for more than the absolute value of eight, the result of this phase is disapproved, otherwise it is approved.

3.4 Searching Compression Signatures

In this action, the header of the image is reviewed in order to find a compression signature using an image editing software. If it is found a signature, the result of this searching is going to be disapproved; and in the final technical resolution the name of the software used for image processing must be printed. If it is not found a signature, the result is going to be approved. An example of the application of this point using the open source tool *JPEGSnoop* is shown in Fig. 6, where a signature of Adobe Photoshop software was found in the header of the image.

```
*** Searching Compression Signatures ***

  Signature:           01180AF3DE63318828A86409EF4013DD
  Signature (Rotated): 01180AF3DE63318828A86409EF4013DD
  File Offset:         0 bytes
  Chroma subsampling:  1x1
  EXIF Make/Model:     OK   [00000000000000] [00000]
  EXIF Makernotes:     NONE
  EXIF Software:       OK   [Adobe Photoshop CS5.1 Windows]

  Searching Compression Signatures: (3327 built-in, 2 user(*) )

          EXIF.Make / Software        EXIF.Model
          ------------------------    ----------------------------------
     SW :[Adobe Photoshop          ]
```

Fig. 6 Compression signature found using JPEGSnoop tool.

Therefore, the process applied to the image must be written in the chain of custody; it is important to obtain one more time the hash value (SHA 256) of the image used for the analysis. Then, this hash value must be compared with the hash value obtained before starting the analysis process. If the hash values compared are exactly equals, the process concludes successfully, otherwise, the process failed because of the management of the image during the process, and it cannot be used as evidence. Both cases (the one that applies) must be registered in custody chain.

4. Final dictum

The guide [13] indicates that in order to accept digital media as evidence, this media has to maintain the properties that authenticate it. Therefore, according to the process of analysis performed with the four technical features described above, the final technical resolution (verdict or dictum) that determines the image's authenticity is defined as follows:

i) If the fours kinds of analysis are approved, the final technical resolution is: ***Authentic***.
ii) If the first three kinds of analysis are approved and a compression signature of any image editing software is found, the final technical resolution is: ***Post Produced Image***. In this case, the image maintains the properties

that authenticate it, and the presence of that signature only indicates that the image has a quality improvement.

iii) Any other combination than the mentioned above, the final technical resolution is: ***Modified***.

Finally, a final dictum (verdict) must be emitted. This dictum must include the time and date of analysis, the name of the analyst, the name and the hash value (SHA 256) of the image analyzed, and a brief description of analyzed aspect including their respective result and the final technical resolution.

5. Results

For testing this methodology, a set of 450 digital images were used as follows: 150 original (without modifications), 150 modified (changing the fact that the image represents) and 150 post produced, only with quality improvement. The digital images used were generated with 10 different cameras of the following make and models of mobile devices: BlackBerry Curve 8530, Apple iPhone 4, Apple iPhone 5, Huawei Speed U8667, Nokia 3710 fold, Samsung GT-I8190, Samsung GT-I9300, Sony Xperia S LT26i, Sony Xperia U ST25i, Sony Ericsson Xperia Mini Pro HD SK17a. There were captured 45 images of each camera and divided as 15 originals, 15 modified and 15 post produced images. The smaller digital image has a size of 1600×1200 pixels which capture with a BlackBerry 8530 mobile device; and the bigger digital image has a size of 4000×2250 pixels captured with Sony Xperia S mobile device; the size of the images captured with the others 8 cameras are among that range. For modifying and post produce the images, the following software was used: *Picasa 3, Adobe Photoshop* and *Paint* of Windows XP.
Considering the sample of *N=450* digital images, divided in 150 originals images (O), 150 modified images (M) and 150 post produced images (P), three variables were defined, O_A, M_A and P_A in order to find the success verdict and determine the methodology efficiency. These variables indicate the times that the final technical resolution successful correspond to the group of the image analyzed (original, modified or post produced); in other words, these variables represent the number of image in the group minus the quantity of false negative in the technical resolutions obtained. These variables are defined according with Eqs. (1), (2) and (3).

$$O_A = O - F_{NO}\,, \tag{1}$$

$$M_A = M - F_{NM}\,, \tag{2}$$

$$P_A = P - F_{NP}\,, \tag{3}$$

where F_{Ni} is the amount of false negatives; *i* stands for *O* for Original, *M* for Modified or *P* for Post produced images.

In this way, the methodology efficiency is defined by Eq. (4):

$$E = \frac{1}{N}(O_A + M_A + P_A)\,, \tag{4}$$

where *N = 450* is the total number of digital image considered in the analysis.

The results obtained by applying the process described in this work are shown in Table 1, where the efficiency percentage was calculated, having a result of %E = 93.76.

Table 1: Results obtained by applying the proposed methodology

Image	**Detection**			**Total of detected digital images**	**Final resolution per 1/*N***
	O_A	**M_A**	**P_A**		
Original	142	1	12	155	0.3155
Modified	3	145	5	153	0.3222
Post Produced	5	4	133	142	0.2955
	150	**150**	**150**	**450**	***E*=0.9376**

Results in Table 1 show that there are also final technical resolutions with false positive. False positives are defined as the times that an authentic verdict was made when the Modified (*M*) or Post Produced (*P*) images were analyzed. Therefore, it is defined that false positives depend on false negatives of the other two groups of images. With this basis, Eqs. (5), (6) and (7) define the false positives where *i* stands for *O* for Original, *M* for Modified or *P* for Post produced images.

$$F_{PO} = F_{NM}k_3 - F_{NPP}k_1\,, \tag{5}$$

$$F_{PM} = F_{NO}k_2 - F_{NPP}(1-k_1)\,, \tag{6}$$

$$F_{PP} = F_{NO}(1-k_2) + F_{NM}(1-k_3)\,, \tag{7}$$

where F_{Ni} is the amount of false negatives and *i* stands for *O* for Original, *M* for Modified or *P* for Post Produced images.
These results also show that it is possible to calculate the values of false positives and false negatives of each group of images. Table 2 shows these particular calculations:

Table 2: False positives and false negatives found in the results shown in Table 1

Groups of images	False Negatives	False positives
Original	8	13
Modified	5	8
P. Produced	17	9

In Eqs. (5), (6) and (7), it can be observed that there are three factors k_1 , k_2 and k_3 . These factors indicate a specific weight of the false negative results of one group of images, which directly affect the quantity of false positive results of the other groups. Clearing these three factors in Eqs. (5), (6) and (7), are obtained Eqs. (8), (9) and (10).

$$k_3 = \frac{F_{PO} - F_{NPP}k_1}{F_{NM}}, \qquad (8)$$

$$k_1 = 1 + \frac{(-F_{PM} + F_{NO}k_2)}{F_{NPP}}, \qquad (9)$$

$$k_2 = 1 + \frac{(-F_{PP} + F_{NM} - F_{NM}k_3)}{F_{NO}}, \qquad (10)$$

Finally, solving Eqs. 8, 9 and 10 by substituting the results of the false positives and false negatives of Table 2, the values of the weight factors are obtained:

$$k_1 = \frac{9}{17},\ k_2 = 0 \quad \text{and} \quad k_3 = \frac{4}{5}.$$

These factors are useful when it is necessary to calculate the false positive values of other groups of images, where the distribution of the images is unknown.

6. Conclusions

It was feasible to define a methodology which determines if a digital image in JPEG format is authentic, post produced or modified, based on internationally accepted guides and best practices about evidence management. The process applied to metadata, thumbnail, camera traces and compression signatures found in the digital image provides a robust analysis that grants certainty and reliability of the dictum emitted. The efficiency percentage obtained is 93.76% of the proposed methodology; therefore, it can be applied to help in the clarification of facts or events arising from security incidents with legal, civil, administrative or criminal implications. According to laws of each country, this process may help to present a digital image as evidence.

The proposed methodology can be applied using open software tools, like is shown in the technical application example. However, it is possible to develop software that automatizes the four analysis process (metadata, thumbnail, camera traces and compression signatures), because each aspect of analysis is in a digital way and only requires computer processing.

Acknowledgments

R. Vázquez-Medina wishes to thank Instituto Politécnico Nacional (IPN México) for financially support this research through grant SIP/IPN 20150316 and SIP-2015-RE/013. F. Rodríguez-Santos (CVU-377075), G. Delgado-Gutiérrez (CVU-372164) and L. Palacios-Luengas (CVU-373990) thank for the scholarship provided by CONACYT–México. Technical and computational support from J. L. Pichardo- Méndez (CVU-668444) is gratefully acknowledged.

References

[1] GRABLER F, AGRAWALA M, LI W, DONTCHEVA M, IGARASHI T. Generating photo manipulation tutorials by demonstration. ACM Transactions on Graphics (SIGGRAPH) 28, 3, 2009.

[2] GARRY M, GERRIE M. When photographs create false memories. Current Directions in Psychological Science 14, 326–330, 2005.

[3] JOHNSON M, FARID H. Detecting photographic composites of people. In 6th International Workshop on Digital Watermarking. Guangzhou, China, 2007.

[4] FARID H. A survey of image forgery detection. IEEE Signal Processing Magazine 2, 26, 16–25, 2009.

[5] FARID H, BRAVO M. Image forensic analyses that elude the human visual system. In SPIE Symposium on Electronic Imaging. San Jose, CA, 2010.

[6] KEE E, FARID H. Exposing digital forgeries from 3-D lighting environments. In Workshop on Information Forensics and Security, 2010.

[7] O´BRIEN JF, FARID H. Exposing Photo Manipulation with inconsistent reflections. ACM Transactions on Graphics. 31(1):4:1–11, 2012.

[8] LUO WEIQI, QU ZHENHUA, PAN FENG, HUANG JIWU. A survey of passive technology for digital image forensics. Front. Comput. Sci. China, 1(2): 166−179, 2007.

[9] MIN-GU HWANG AND DONG-HWAN HAR. A Novel Forged Image Detection Method Using the Characteristics of Interpolation. J Forensic Sci., Vol. 58, No. 1, January 2013.

[10] FEI PENG, JIAO-TING LI, MIN LONG. Identification of Natural Images and Computer-Generated Graphics Based on Statistical and Textural Features. J Forensic Sci., Vol. 60, No. 2, March 2014.

[11] MIN GU HWANG, DONG HWAN HAR. Identification Method for Digital Image Forgery and Filtering Region through Interpolation. J Forensic Sci., Vol. 59, No. 5, September 2014.
[12] YANJUN CAO, TIEGANG GAO, GUORUI SHENG, LI FAN, LIN GAO. A New Anti-forensic Scheme — Hiding the Single JPEG Compression Trace for Digital Image. J Forensic Sci, Vol. 60, No. 1, January 2015.
[13] KENT K, CHEVALIER S, GRANCE T, DANG H. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology. Special Publication 800-86. August 2006.
[14] Association of Chief Police Officers. Good Practice Guide for Computer-Based Electronic Evidence. Official release version.
[15] A Road Map for Digital Forensic Research. Report from the First Digital Forensic Research Workshop (DFRWS) Technical Report; 2001 Nov. DTR -T001-01 Final.
[16] CICHONSKI P, MILLAR J, GRANCE T, SCARFONE K. Computer Security Incident Handling Guide. National Institute of Standards and Technology. Special Publication 800-61 Revision 2. August 2012.
[17] Scientific Working Group on Digital Evidence. Best Practices for Computer Forensics v.3.1. September 2014.
[18] National Institute of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. NCJ 199408.
[19] National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. NCJ 219941.
[20] BABAK MAHDIAN, STANISLAV SAIC. A bibliography on blind methods for identifying image forgery. Signal Processing: Image Communication, Volume 25, Issue 6, July 2010.
[21] Farid H. 5 ways to spot a fake photo. The Scientific American Magazine; Page 5, June 2, 2008.

Francisco Rodríguez-Santos Obtain the Engineering degree in 2010 and subsequently the master in information security degree in 2012. Nowadays, studies the PhD. in the Section of postgraduated studies and research which belongs to the Superior School of mechanic and electric engineering of Instituto Politécnico Nacional in Mexico City. He is a member of the Forensics workgroup of Mexican Accreditation Entity and his interest areas are the information security, information forensics, pattern recognition and regulatory compliance in information security.

Guillermo Delgado-Gutierrez Master in Microelectronics Engineering graduated in 2013 in the Section of postgraduated studies and research which belongs to the Superior School of mechanic and electric engineering of Instituto Politécnico Nacional in Mexico City. Nowadays, studies the PhD. in the same Section of Studies. He is a member of the Forensics workgroup of Mexican Accreditation Entity and his interest areas are information security, signal processing, digital forensics analysis and regulations.

Leonardo Palacios-Luengas Master in Microelectronics Engineering graduated in 2012 in the Section of postgraduated studies and Rresearch which belongs to the Superior School of mechanic and electric engineering of Instituto Politécnico Nacional in Mexico City. Nowadays, studies the PhD. in the same Section of Studies. His interest areas are cryptography, steganography, embedded systems programming and digital electronics design.

Rubén Vázquez-Medina He obtained the Electronics Engineering degree in 1988, he has a Master in Sciences of Electric Engineering, obtained in 1993. He has the PhD. Degree obtained in 2008 in the Universidad Autónoma Metropolitana. Since 2006 is a guest professor in the Master in Information Security program of the Superior Naval Studies Center of Mexican Navy. Nowadays is the subdirector of the postgraduated section of the Cleaner Production Mexican Center since 2014. He conducts research in the areas of cryptography, steganography, computer forensics and compliance in information security; and modeling diffusion reaction systems for applications in information security.