Secure Digital Camera

Paul Blythe and Jessica Fridrich
Department of Electrical and Computer Engineering
SUNY Binghamton, Binghamton, NY 13902-6000
{pblythe, fridrich}@binghamton.edu

ABSTRACT

In this paper, we propose a new concept for digital cameras to solve some of the significant problems associated with the use of digital images as evidence in a court of law. The integrity of digital images as evidence rests on the accurate answering of a simple question: *Who did what when?* We show how to use lossless data embedding to combine biometric data with cryptographic hashes and other forensic data to identify from the digital image the photographer, the camera, the time when the image was taken, and verify the image integrity. We call a camera with this capability "Secure Digital Camera". The proposed concept will provide forensic investigators with a tool that will help them establish the integrity of a digital camera image presented to the court and prove that it is a true and accurate representation of reality.

1. INTRODUCTION

According to Blond's Evidence[i] (Blond et al. 1994), photographic evidence can be authenticated by two methods, depending on the type of imagery. The traditional method is to consider images as "illustrative of a witness' testimony." Given the advances in imaging technology, many jurisdictions have adopted an alternative method on the basis of the silent witness theory, which states that photographic evidence "speaks for itself" and is thus admissible through testimony that establishes how it was produced.

In today's world, not only is the general public rapidly replacing classical analog cameras (film) with digital cameras, law enforcement agencies are doing so as well. Increasingly, agencies are relying on digital photography to preserve a visual record of crime scenes, physical evidence, and victim's injuries. This is quite understandable because a digital camera image gives the photographer immediate visual feedback of each picture taken. Digital images can be readily shared via computer networks and conveniently processed for queries in databases. Also, properly stored digital images do not age or degrade with usage. On the other hand, thanks to powerful editing programs, it is very easy even for an amateur to maliciously modify digital media and create realistically looking forgeries. It is also easy to modify an image to make it look as if it came from a different camera. Moreover, at present no cameras allow undisputable identification of the person who took the image. One example of an illegitimate forensic application[ii] is the "burning in" used to darken an African-American's skin in a photo, in a deliberate effort to appeal to a

viewer's prejudice. Forensic tools that help establish the origin, authenticity, and the chain of custody of digital images are thus very essential to the forensic examiner. These forensic tools can prove to be vital whenever questions of digital image integrity are raised. Chain of custody can be one of the most difficult issues faced by the forensic professional trying to introduce a digital image as evidence in a criminal case.

2. PRIOR ART

Both Kodak and Epson have manufactured cameras with digital watermarking capabilities that are relevant to the problems formulated in the introduction. The following is a description of the two manufacturers' cameras:

Epson offered several cameras with watermarking capabilities. They are also all discontinued camera models:

- Epson PhotoPC 700/750Z (1.2Mp)
- Epson PhotoPC 800/800Z (2.1Mp)
- Epson PhotoPC 3000Z (3.1Mp)

Epson uses a software system called the Image Authentication System (IAS). The user must purchase the software as an option and then upload it to the camera from a personal computer. Once the IAS is installed in the camera, it will transparently add a digital watermark (encrypted fingerprint) to each image captured. This allows viewing the images using any software that can read JPEG files. The user must use the IAS software to verify the authenticity of images. The software can also detect any tampering, even if a single pixel has been changed. While not likely to be an essential feature for most users, it has clear forensic benefits in many applications. If the camera is opened, the IAS system must be installed again. The offline software allows one to verify the image integrity as well as show on your personal computer the areas that have been modified.

The following are cameras with watermarking capabilities that were offered by Kodak. They are also all discontinued camera models:

- Kodak DC-200 (0.9Mp)
- Kodak DC-260 (1.3Mp)
- Kodak DC-290 (2.1Mp)

The Kodak DC-290 was the only camera Kodak manufactured with digital watermarking capabilities built in (Fig. 1). The Kodak DC-290 watermark settings allow one to place any or all of the following watermarking options: date, time, text, or logo, visibly into the pictures. One can also select the watermark characteristics, such as left and top offset in the picture, transparency level, text color, and background color. Kodak has developed a robust invisible watermarking system, but it is still part of their Research and Development department, and not yet available in any consumer cameras.

The main difference between the Epson and the Kodak cameras is that the Epson is better suited for image integrity verification because it has an invisible watermark and can detect a change in a single pixel. Both cameras add non-removable distortion to the original image. This could be a significant problem in getting the court to accept this watermarked image is an accurate representation of the original scene image.

The Kodak camera has a visible watermark logo. The watermark logo can be added after the picture is taken with Kodak software. This has limited forensic use.

Neither camera can provide an undisputable proof of the image origin or its author.

Figure 1. *Kodak DC-290 watermarked camera image with text and date stamp.*

3. SECURE DIGITAL CAMERA SOLUTION

To address the problems formulated in Section 1, we propose a new concept of a secure digital camera that will embed in each image it takes the following data:

- Biometric identifier (iris image) of the photographer (the iris image is taken through the viewfinder)
- Cryptographic hash of the image data for verifying image integrity
- Time, date, and other relevant data

The embedding will be performed using a lossless embedding algorithm[xii] to avoid issues associated with adding distortion due to embedding. A secret key (unique for each camera) will govern the embedding process. This key can later be used to prove that the image was indeed taken by this camera. The hash of image data will guarantee image integrity since essentially every modification to the image will change this hash (matching the hash after tampering is as difficult as finding a collision for a hash). The time, date, and other metadata from the EXIF header is also embedded to prevent its

replacement. Because all the data is embedded in the image rather than appended to it in the header or visibly in the image and because the embedding is a function of the secret camera key, it is impossible to replace the data or forge a different image to make it look as if it was taken by some other camera or a person.

We now have a system by which we can authenticate the photographer, camera information, and image integrity. These features make maintaining and establishing the chain of custody of this digital image much easier for the courts to accept.

Next, we describe in more detail the individual elements of the proposed secure camera.

3.1 Biometrics identifier

The term '*Biometric*' is derived from the Greek words *bio* (life) and *metric* (the measure of). 'Biometrics' can be defined as: *"A pattern recognition system that recognizes a person by determining the authenticity of a specific physiological and/or behavioral characteristic possessed by that person."* The most commonly used form of biometrics in use today are fingerprints. Fingerprints are a good choice for biometric identification because they feature two very important characteristics required for biometric identification. The first characteristic is that fingerprints are unique for each individual. The second characteristic is that fingerprints are permanent, since they do not change over time. It is for these two reasons that fingerprints have become a readily accepted form of biometric identification in the US court system.

We have considered several possible forms of person identification for our project, such as a simple keypad entry pass-code system or a thumbprint scanner, facial recognition, and the iris. We decided that the iris image was the best fit for our application. The keypad system did not offer the unique user identification feature. A person's face does change over time. The fingerprint identification systems currently under testing are proving to be difficult to use due to moisture problems.

The first iris recognition algorithms were introduced by Daugman in 1994[iii]. He also investigated the randomness and uniqueness of human iris patterns by comparing 2.3 million different pairs of eye images. The amount of statistical variability corresponded to an information density of around 3.2bits per mm^2 over the iris, which (roughly translated) suggests that the probability of two irises agreeing by chance (in more than 70 per cent of their phase sequence) is about one in 7 billion. The probability surprisingly does not even increase in the irises of identical twins[iv].

Iris recognition techniques are currently being used in numerous security applications including access for cash points, mobile phones, hospitals, and airports. The company pioneering the latter is US based EyeTicket [v].

According to Iridian Technologies[vi], the iris is the plainly visible, colored ring that surrounds the pupil (Figs. 2 and 3). The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The iris is a muscular structure that controls the amount of light entering the eye, with intricate details that can

be measured, such as striations, pits, and furrows. The iris is not to be confused with the retina, which lines the inside of the back of the eye.

No two irises are alike. There is no detailed correlation between the iris patterns of even identical twins, or the right and left eye of an individual. The amount of information that can be measured in a single iris is much greater than fingerprints, and the accuracy is greater than DNA. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect artificial irises (e.g., designer contact lenses).

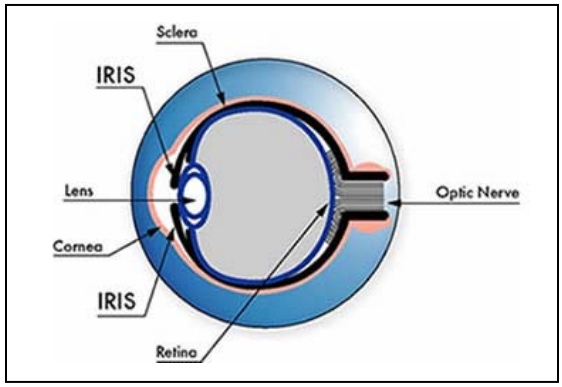

Figure 2. *Diagram of the human iris.*

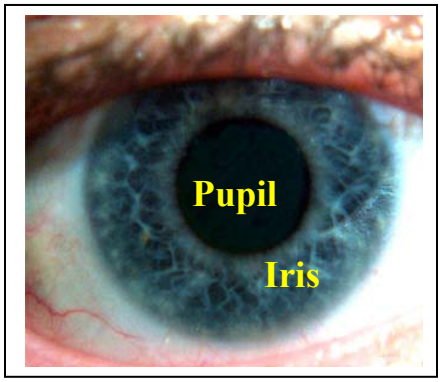

Figure 3. *Color photograph of iris*.

The following are advantages and disadvantages of the iris for identification

- Highly protected, internal organ of the eye
- Iris patterns possess a high degree of randomness
- Limited genetic penetrance of iris patterns
- The iris is essentially formed by 8 months, and remains stable through life
- Embedding and identification are tractable

- Located behind a curved, wet, reflecting surface
- Obscured by eyelashes, lenses, reflections
- Partially occluded by eyelids, often drooping
- Deforms non-elastically as pupil changes size
- Illumination should not be visible or bright
- Some negative (Orwellian) connotations

3.2 Lossless watermarking

In the past, invisible digital watermarks have been proposed as a means to verify image integrity and authenticity[vii]. Authentication watermarks can be classified into fragile and semi-fragile. The purpose of fragile watermarks is to detect every possible modification of the image with high certainty. Fragile watermarks are usually realized by embedding a cryptographic hash in the image.[viii,ix,x,xi,xii] Semi-fragile watermarks are supposed to be insensitive to "allowed" manipulations, such as lossy compression or small amount of

common processing, but react sensitively to malicious content-changing manipulations, such as adding or removing objects. Robust (visual) hashes[xvi] and robust watermarks[xi] can be employed to facilitate content authentication of digital images. Authentication using digital watermarks provides certain advantages that cannot be achieved using classical authentication tools. Because the image digest (the hash) is embedded in the image rather than attached to it or embedded in the header, the authentication data is inconspicuous, it cannot be easily removed or replaced, and cannot be preserved after any image manipulation. Since the watermark is embedded in the image data itself, it stays inside even after losslessly resaving the image in a different format.

The majority of the early authentication watermarking designs introduced some small amount of non-removable distortion into the digital image. Models of the human visual system are usually used to "prove" the invisibility of the watermark. In some applications, such as watermarking of medical images or sensitive military imagery, no distortion is allowed due to legal and other reasons. Forensic imagery also belongs to the category of sensitive images. Consequently, the distortion due to embedding of an authentication watermark will violate evidence integrity.

Authentication watermarks embedded by a watermarking chip inside the digital camera have been proposed in the past (e.g., the Epson camera). However, because the authentication process invariably modifies the image, the legal problems associated with watermarking prevented the spread of watermarking technology for sensitive images. To overcome this problem of authentication watermarks, "lossless watermarking" was proposed[xiii,xiv]. In lossless watermarking, the embedding distortion can be completely removed from the watermarked image and thus one can obtain the authentic original image[xii,xiii]. In this paper, we only describe the main idea in a simplified manner.

Lossless watermark embedding

1. One or more selected quantization steps from the JPEG quantization table are changed to half their values.
2. To keep the image appearance unchanged, all corresponding DCT coefficients in all blocks of the image are multiplied by 2.
3. The payload is then embedded using the Least Significant Bit (LSB) embedding in the modified DCT coefficients (they are all even).
4. The secret camera key is used to generate a pseudo-random embedding path. This path determines the location of the payload bits among all DCT coefficients.

Lossless watermark extraction

1. The camera key is used to identify the pseudo-random extraction path. This path determines the location of the payload bits in LSBs of DCT coefficients. The payload is extracted.
2. After extraction, all LSBs of DCT coefficients (from Step 2 above) are set back to zero and the DCT values are divided by 2.
3. All of the corresponding DCT quantization steps are multiplied by 2. The watermarked image is now returned to its original state.

For JPEG images with sampling 4:c_1:c_2, the capacity of this lossless embedding scheme is $L \times MN/64 + C \times MN/256 \times c_1 \times c_2 - L - C$ where L is the number of luminance DCT coefficients and C the number of chrominance coefficients used for embedding in each 8×8 block. As an example, for a 4 Mega-pixel grayscale image if two luminance DCT coefficients are used and no chrominance is used, the available capacity is $4 \times 10^6/64/8$kB = 15.6 kilobytes. Other examples are shown in Table 1.

Camera Sensor Size (M Pixels)	Image Size In Pixels		Grey Scale Capacity KB
	N	M	
2.1 MP	1200	1792	53.32
3.1 MP	2048	1536	78.00
3.9 MP	2272	1704	96.00
5.0 MP	2592	1944	124.94
6.29 MP	3072	2048	156.00
11.0 MP	4064	2704	272.48

Table 1. *Lossless embedding capacity*

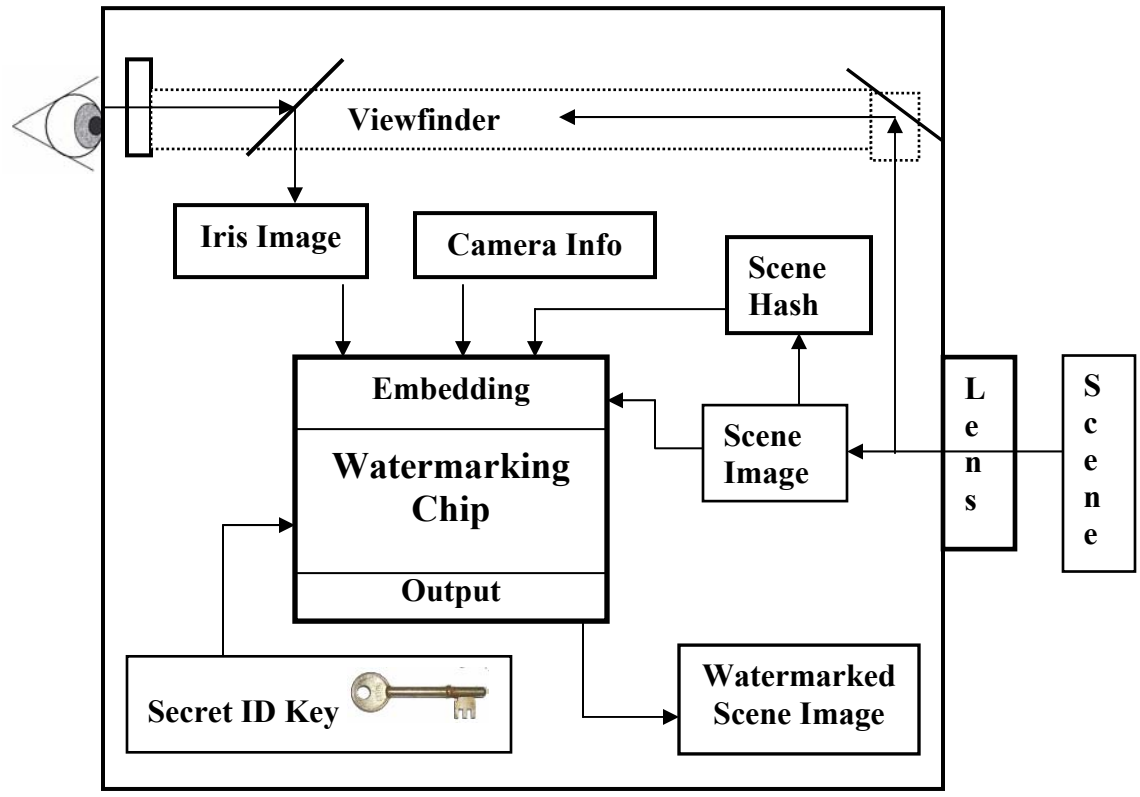

Figure 4. *Secure Digital Camera (block diagram).*

3.3 Secure digital camera

The proposed Secure Digital Camera automatically captures an image of the human iris through the viewfinder each time a digital photograph is taken. This iris image is then compressed and combined with a hard-wired secret camera identification key, the hash of the original scene being photographed, and additional digital camera specifics, e.g. a time stamp. The end result is a digital bioforensic authentication signature that is losslessly embedded by the Watermarking Chip inside the Secure Digital Camera (Fig. 4).

Authentication

1. Press shutter release to capture scene and iris image (bioforensic signature).
2. Calculate hash of scene image.
3. Concatenate the camera information, iris image, and the calculated hash of the scene image to produce the final payload to be losslessly embedded.
4. Inside the watermarking chip using the camera key losslessly embed the final payload.
5. Produce the authenticated (watermarked) scene image for archival storage.

Verification

1. Extract off-line from the embedded watermarked scene image the bioforensic authentication signature using the camera key.
2. Reconstruct the original scene image and calculate its hash H'.
3. Extract the embedded payload and read the embedded hash H.
4. Compare this hash with the calculated hash H**'** for digital image integrity (H=H**'** implies verified integrity, H≠H' indicates tampering).
5. Extract the compressed iris image and verify the extracted iris image with photographer's iris or from an iris image database, for personnel identification.
6. Read the remaining camera information and compare to the EXIF header.
7. Interpret the results.

4. EXPERIMENTAL SETUP

The purpose of this paper is to prove the feasibility of the proposed concept. We did not implement in hardware the lossless embedding part. Instead, we simulated the Watermarking Chip using a software implementation of a lossless data embedding technique from Section 3.2.

Once we decided upon the Iris Image as the biometric choice, we had another choice to make. We had to decide whether to use the iris image or a bit stream representation of the iris image.[iii] We opted for the iris image compressed using JPEG to make its size fit within the available lossless capacity. This eliminates the need for a real time iris image signal-processing chip inside the camera. Also, JPEG compression is already supported by the hardware inside the camera.

In Table 1, we show the lossless capacity for different Scene Image sizes. The lossless embedding capacity was obtained using $L = 13$ and $C = 0$.

4.1 Obtaining the iris image

Our next step was to decide how to obtain a usable iris image. For that task we modified a viewfinder (Fig. 5) from a Canon EOS camera (Fig. 6).

We chose the Canon EOS camera because it already had a viewfinder with Near IR (700–900nm, infrared) LED's (Light Emitting Diodes) that illuminated the eye for use in there "eye controlled focusing system" (Fig. 7). We modified the viewfinder and replaced the auto-focus CCD sensor with a 640×480 pixel CMOS image sensor from Kodak (Fig. 9).

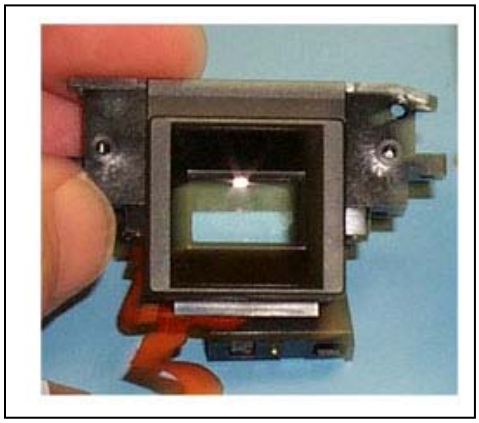

Figure 5. *Canon viewfinder assembly.*

Figure 6. *Canon EOS camera.*

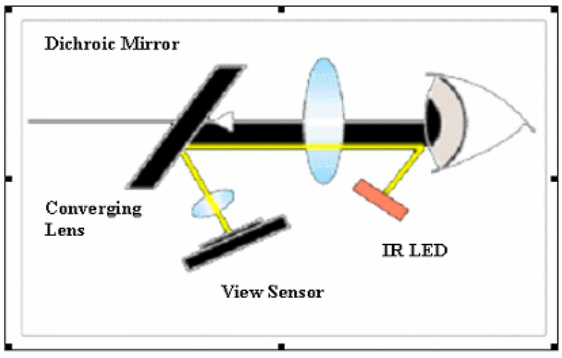

Figure 7. *Canon eye controlled focus.*

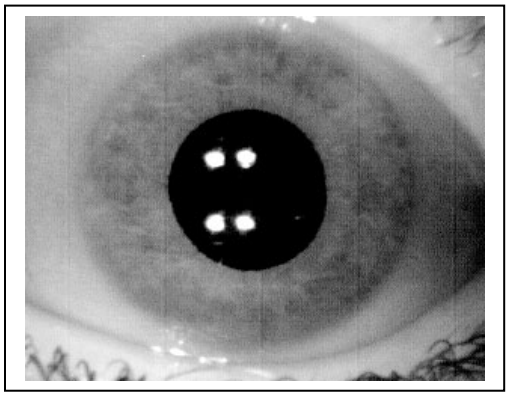

Figure 8. *Actual captured iris image.*

Through experiments and ray-tracing simulations, we determined a combination of lenses that gave us an iris image with enough detail for our application (70–100 pixels in radius minimum) and sufficient depth of focus (Fig. 8). This image was further JPEG compressed to bring it within the capacity of the lossless embedding scheme (see Table 1). The compressed image contains sufficient level of detail to enable iris identification.

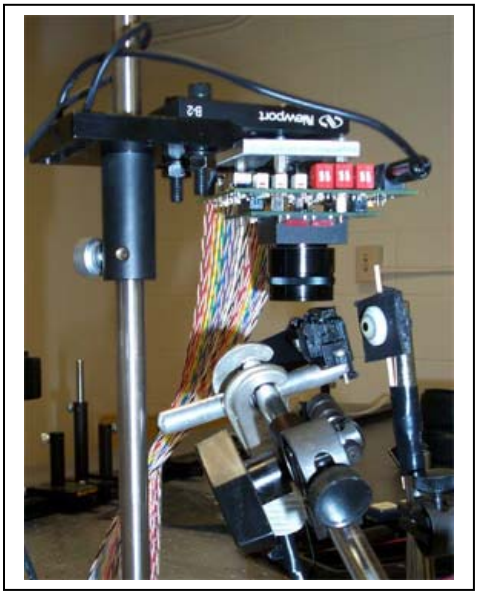

Figure 9. *CMOS image sensor system.*

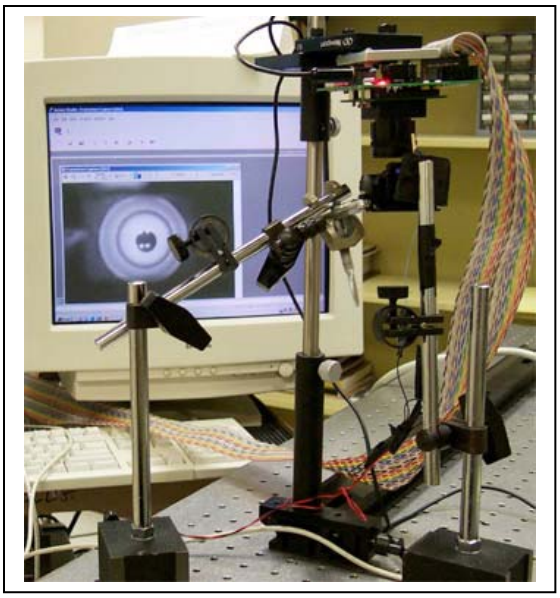

Figure 10. *Iris image capture test setup.*

Figure 9 shows the lens bench setup using an artificial glass eye with 11mm iris radius. The modified viewfinder and the Kodak iris capture system with the dual lens configuration, which was the best configuration for our purposes, is shown in Figure 10.

5. CONCLUSIONS

In this paper, we propose a new concept of a Secure Digital Camera that offers a solution to the problems associated with the chain of custody for digital images presented to the court. The camera losslessly embeds the photographer's iris image, the hash of the scene image, date, time, and other camera/picture information into the image of the scene. The embedding process depends on a secret camera key. The embedded data can be later extracted to verify the image integrity, establish the image origin and verify the image authenticity (identify the camera and the photographer). The watermark is not only invisible but also completely removable (lossless). The use of the iris as a biometric reliably verifies the photographer. Secure cryptographic hashes (e.g., MD5) guarantee that no modifications can be made to the image that cannot be detected.

Using digital biometric signatures, hard-wired camera identification, and the image hash concurrent to the acquisition of data, allows the examiner to effectively establish a digital chain of custody. This is because the verification process is integrated inside of the

Secure Digital Camera. This is important because it establishes that the examiner did not corrupt or tamper with the subject evidence at any time in the course of the investigation. This is a particularly important step, as courts will only accept duplicated computer data if the data is demonstrated to be an accurate copy of the "original" computer data. A Secure Digital Camera also helps to minimize the potential for errors in law enforcement procedures and processes, thus enhancing the integrity of digital evidence.

ACKNOWLEDGEMENTS

The work on this paper was supported by Air Force Research Laboratory, Air Force Material Command, USAF, under the research grant number F30602-02-2-0093. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation there on. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of Air Force Research Laboratory, or the U. S. Government. Special thanks belong to Rebecca Bussjager, from the AFRL/SNDP (Air Force Research Lab) at Rome, NY for help with the ray-trace designs of different lens combinations necessary to achieve the correct image size and depth of field.

REFERENCES

[i] Blond, N., Bahn, M., Loring, S., and Meyers, W.: *Blond's Evidence*. Sulzburger and Graham, New York, 1994

[xvi] Fridrich, J.: "Visual Hash for Oblivious Watermarking". In: *Proc. SPIE Photonic West Electronic Imaging 2000, Security and Watermarking of Multimedia Contents*, San Jose, January, 2000, pp. 286–294

[ii] Russ, C. J.: *Forensic Uses of Digital Imaging 125* (CRC Press 2001). O. J. Simpson's skin was darkened in a police photograph

[iii] Daugman, J.: U.S. Patent No. 5,291,560: *Biometric Personal Identification System Based on Iris Analysis.* Issue Date: 1 March 1994

[iv] Daugman, J.: "How Iris Recognition Works". *IEEE Trans. CSVT* **14**(1), 2004, pp. 21–30

[v] Eye-ticket.: *Access control products using iris recognition.* Headquartered in McLean, Virginia, U.S.A, http://www.eyeticket.com/index.html

[vi] Iridian Technologies.: *Holder of John Daugman's patents for iris recognition*, 1245 Church Street, Suite 3, Moorestown, New Jersey, 08057 USA http://www.iridiantech.com/

[vii] Wong, P.: "A Watermark for Image Integrity and Ownership Verification". *Proc. IS&T PIC,* Portland, Oregon, 1998.

[viii] Celik, M., Sharma, G., and Saber, E.: "A Hierarchical Image Authentication Watermark With Improved Localization and Security". In: *Proc. ICIP 2001*(CD ROM version), paper ID 3532, Thessaloniki, Greece, October, 2001

[ix] Coppersmith, D., Mintzer, F., Tresser, C., Wu, C. W., and Yeung, M. M.: "Fragile Imperceptible Digital Watermark with Privacy Control". In: *Proc. SPIE, Security and Watermarking of Multimedia Contents*, San Jose, January, 1999, pp. 79–84

[x] Marvel, L. M., Hartwig, G. W., and Boncelet, C. Jr.: "Compression-Compatible Fragile and Semi-Fragile Tamper Detection". In: *Proc. SPIE, Security and Watermarking of Multimedia Contents*, San Jose, January, 2000, pp. 140–151

[xi] Walton, S.: "Information Authentication for a Slippery New Age". *Dr. Dobbs Journal* **20** (4), 1995, pp. 18–26

[xii] Yeung, M. M. and Mintzer, F.: "An Invisible Watermarking Technique for Image Verification". In: *Proc. ICIP'97*, Santa Barbara, California, 1997

[xiii] Fridrich, J., Goljan M., and Du R.: "Invertible Authentication Watermark for JPEG Images". *ITCC 2001,* Las Vegas, Nevada, April 2–4, 2001, pp. 223–227

[xiv] Fridrich, J., Goljan M., and Du R.: "Lossless Data Embedding for All Image Formats". In: *Proc. SPIE Photonics West*, Vol. 4675, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, San Jose, California, January, 2002, pp. 572–583