Secure Digital Camera

By

Paul Blythe and Jessica Fridrich

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2004 USA

Baltimore, MD (Aug 11th - 13th)

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 biometric solution to solve some of the significant problems associated with use of digital camera images as evidence in a court of law. We present a lossless watermarking solution to the problems associated with digital image integrity and the relationship to its chain of custody. 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 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.

INTRODUCTION

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 "perfect" forgeries. This is not only true for the general public, 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, is one example of an illegitimate forensic application[i]. Forensic tools that help establish the origin, authenticity, and the chain of custody of digital images are 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.

1. SECURE DIGITAL CAMERA SOLUTION

Biometrics

The term '*Biometric*' is derived from the Greek words *bio* (life) and *metric* (the measure of). 'Biometrics' can been 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 possess 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 were the first legally accepted biometric technique used for identification.

In this paper, we use a different form of biometrics that uses the human iris to identify or verify a person's identity. The first iris recognition algorithms were introduced by Daugman in 1994.[ii] 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.[iii]

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 [iv].

Watermarking

In the past, invisible digital watermarks have been proposed as a means to verify image integrity and authenticity[v]. 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.[vi,vii,viii,ix,x] 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-invertible 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. However, because the authentication process invariably modifies the image, the legal problems associated with watermarking prevented the spread of watermarking technology. To overcome this problem of authentication watermarks, "lossless watermarking" was proposed.[xi,xii] 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]

Solution to Digital Image Integrity
Our Secure Digital Camera will solve three problems associated with digital image integrity and their relationship to its chain of custody:

1. To verify exactly *Who* the photographer was.
2. To identify exactly *What* camera was used.
3. To verify image *integrity*.

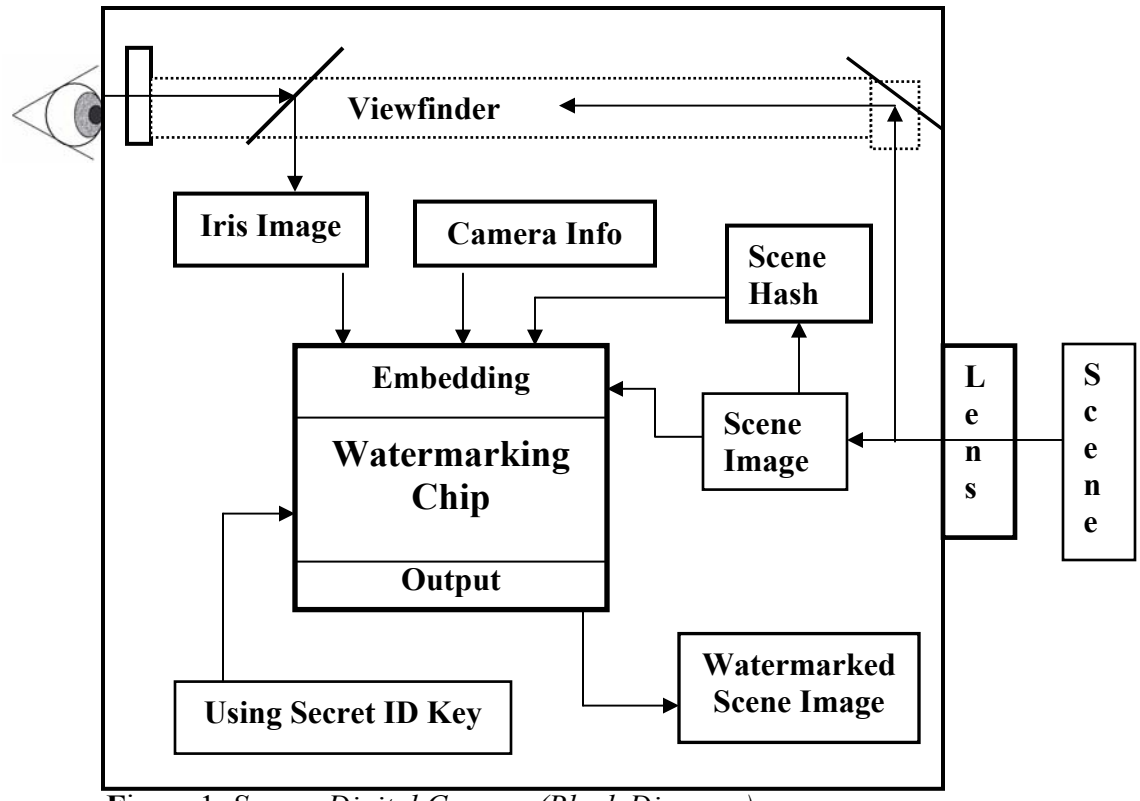

Figure 1. *Secure Digital Camera (Block Diagram).*

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. 1).

Brief Explanation of Embedding Steps:

1. Press shutter release to capture scene image.
2. Calculate hash of scene image.
3. Simultaneously obtain iris image from viewfinder and form the bioforensic signature.
4. Inside the watermarking chip using a secret ID key uniquely associated with the camera, embed the bioforensic authentication signature into the scene image.
5. Produce the authenticated (watermarked) scene image for archival storage.

Brief Explanation of Extraction Steps:

1. Extract off-line from the watermarked scene image the bioforensic authentication signature using the secret ID key.
2. Reconstruct the original scene image and calculate its hash H.
3. Extract the compressed iris image from the bioforensic signature and verify the extracted iris image with iris image database for personnel identification.
4. Extract the hash H' from the bioforensic signature and compare this hash with H for digital image integrity (H=H' implies verified integrity, H≠H' indicates tampering).
5. Store results on an archival storage system.

The Iris

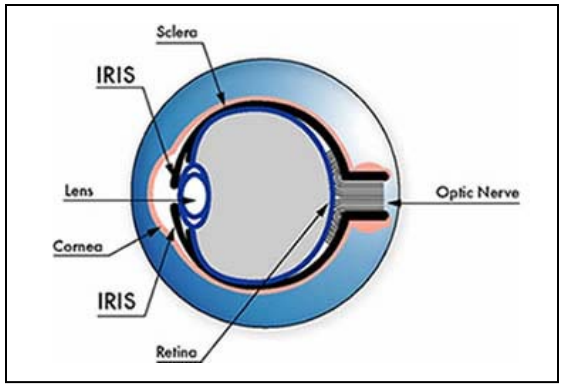

Figure 2. Diagram *of the human iris.*

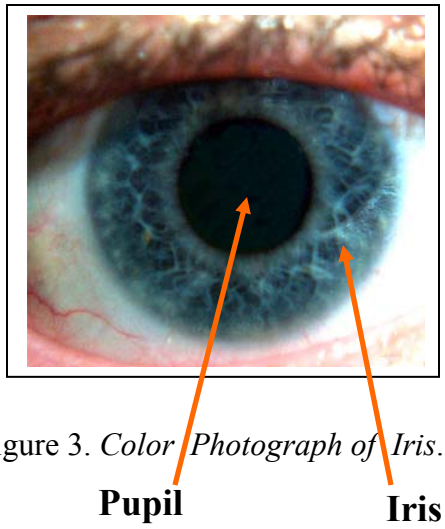

Figure 3. *Color Photograph of Iris.*

According to Iridian Technologies[xiii], the iris is the plainly visible, colored ring that surrounds the pupil (Figs. 2, 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).

Advantages of the Iris for Identification:

- Highly protected, internal organ of the eye
- Iris patterns possess a high degree of randomness
- Pre-natal morphogenesis (7th month of gestation)
- Limited genetic penetrance of iris patterns
- Patterns apparently stable throughout life
- Embedding and identification are tractable

Disadvantages of the Iris for Identification:

- 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

Lossless embedding method for JPEG images

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 for JPEG images described in.[xii] A brief explanation of the lossless watermarking scheme follows.

One selected quantization step from the quantization table is either changed to half its value and all corresponding DCT coefficients in all blocks of the image are multiplied by 2 to keep the image appearance unchanged. Simple Least Significant Bit (LSB) embedding in those modified coefficients is then used to invertibly embed the authentication signature. The placement of embedding changes is a pseudo-randomly generated path through the DCT coefficients obtained from the Secret ID Key. The verification proceeds by extracting the bioforensic signature from the LSBs of DCT coefficients in the same pseudo-random order. After extraction, all LSBs are set back to

zero, divided by 2, and the corresponding DCT quantization step is multiplied by 2. This step brings the watermarked image back to its original state.

For JPEG images with sampling $4:c_1:c_2$, the capacity of this lossless embedding scheme is $L \times MN/64 + C \times MN/256 \times c_1 \times c_2$, where L is the number of luminance DCT coefficients and C the number of chrominance coefficients used for embedding in each block. As an example, for a 4 megapixel 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.

2. EXPERIMENTAL SETUP

There were several options we had to choose for the biometric part of our watermarking scheme. We considered a simple keypad entry pass-code system. We also considered several biometric approaches such as, thumbprint scanner, facial recognition, and iris recognition.

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. A glove would hamper its use as well.

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 decided to use the iris image and lossy compress it 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.

In the below table 1, we show the lossless capacity for different Scene Image sizes. The lossless embedding capacity shown in the last three columns was obtained using $L = 13$ and $C = 0$.

Camera Sensor	Image Size In Pixels		Grey Scale	Color Capacity Kb		
Size (M Pixels)	N	M	Capacity Kb	(4:4:4)	(4:2:2)	(4:2:0)
2.1 MP	1200	1792	53.32	106.64	53.32	26.66
3.1 MP	2048	1536	78.00	156.00	78.00	39.00
3.9 MP	2272	1704	96.00	191.99	96.00	48.00
5.0 MP	2592	1944	124.94	249.88	124.94	62.47
6.29 MP	3072	2048	156.00	312.00	156.00	78.00
11.0 MP	4064	2704	272.48	544.96	272.48	136.24

Table 1 *Lossless embedding capacity*

Obtaining the Iris Image

Our next step was to decide how we would obtain a usable Iris Image. For that task we modified a viewfinder (Fig. 8) from a Canon EOS camera (Fig.9).

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.10). We modified the viewfinder and replaced the auto-focus CCD sensor with a 640×480 pixel CMOS image sensor from Kodak (Fig. 12).

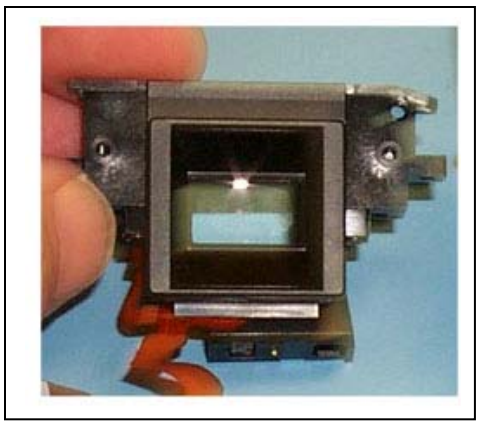

Figure 8. *Canon Viewfinder assembly.*

Figure 9. *Canon EOS Camera.*

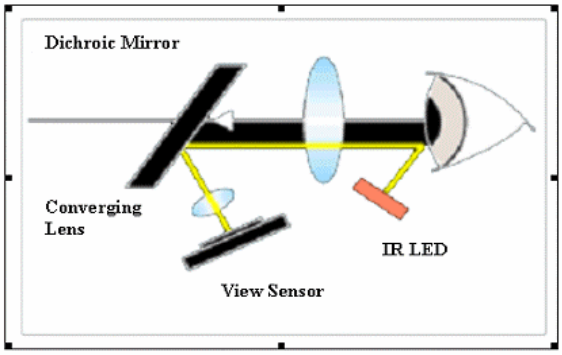

Figure 10. *Canon eye controlled focus.*

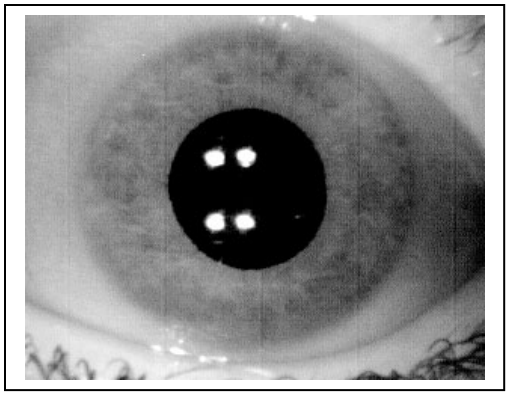

Figure 11. *Actual Captured Iris Image.*

Final Iris Capture Experiments

The final Iris Image capture experiments were to determine which combination of Lenses would give us an Iris Image with enough detail for our application (70–100 pixels in radius minimum), and the best depth of focus (Fig.11). We were able to achieve our goals (Fig.13).

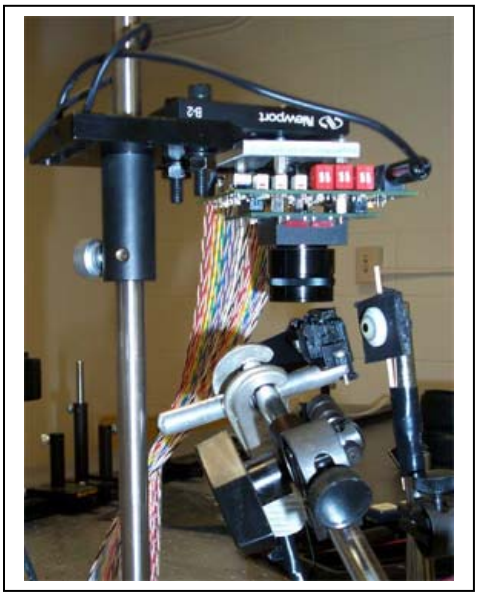

Figure 12. *CMOS image sensor system.*

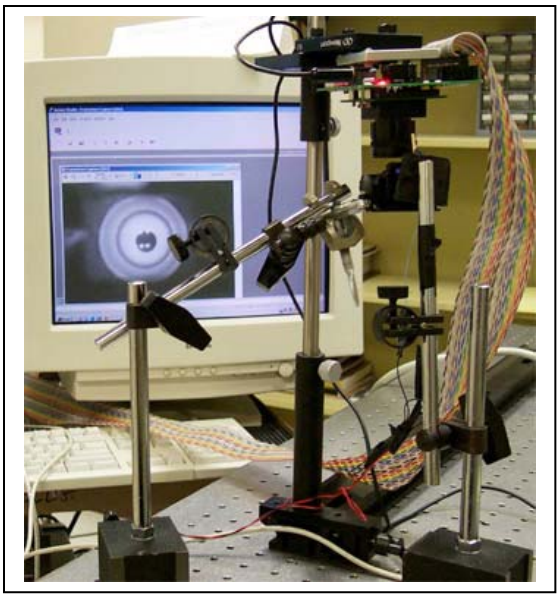

Figure 13. *Iris Image Capture Test Setup.*

The current iris capture system (Fig. 14) consists of the following hardware components:

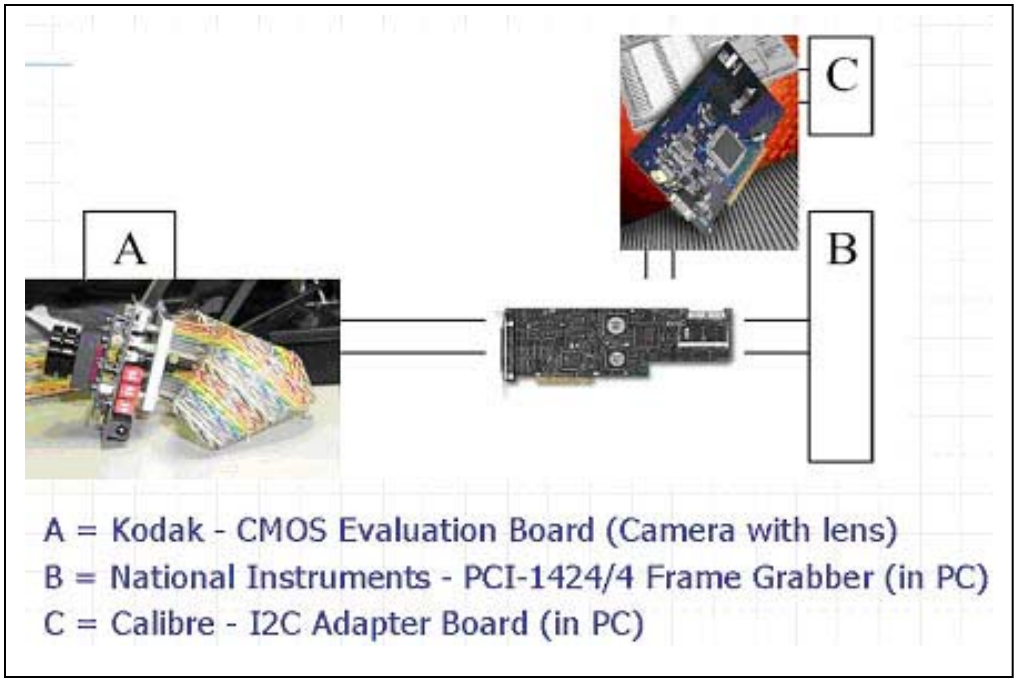

Figure 14. *Current iris capture system block diagram.*

3. CONCLUSIONS

According to Blond's Evidence[xiv] (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.

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.

The authentication process consists of the following steps:

1.) A person looks through the viewfinder and while taking the scene image, an image of the person's iris is taken through the viewfinder.
2.) This iris image is then JPEG compressed to fit within available lossless capacity.
3.) The bioforensic data is appended to the compressed iris image
4.) This combined payload is then losslessly embedded into the scene image.

The verification process consists of the following steps:

1) The iris image and bioforensic data is extracted from the watermarked scene image.
2) The original scene image is reconstructed from the watermarked image.
3) The reconstructed image is hashed and the hashes compared to the hash extracted from the bioforensic data (match indicates integrity of the watermarked image, mismatch indicates tampering).
4) The iris matching is done off-line.

Prior art

Kodak and Epson both have manufactured camera with digital watermarking capabilities.

Epson: The following are the Epson cameras that have watermarking capabilities. They are all discontinued camera models, as is the corresponding IAS software:

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

Epson uses a 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 still allows viewing of images using any software that can read JPEGs, but the IAS software can verify the authenticity of images. It 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 the areas that have been modified on your personal computer.

Kodak: The following are the Kodak cameras that have watermarking capabilities. They are all discontinued camera models:

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

Figure 15. *Kodak DC-290 watermarked camera image with text and time/date stamp.*

The Kodak DC-290 was the only camera Kodak made with digital watermarking capabilities built in. It is also discontinued from manufacturing. The 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 watermarks characteristics, such as left and top offset in picture, transparency level, text color, and background color (Fig.15).

The main difference between the Epson and the Kodak cameras is that the Epson is better suited to camera image verification. It has an invisible watermark and can detect a change in a single pixel.

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

Our Secure Digital Camera offers significant advantages over the two previous methods of digital watermarking. Our watermark would not only be invisible, it would be a biometric identifier of the photographer. By losslessly embedding together, all camera information, the iris image, and the hash of the original image, we now have a system by which we can establish the origin, authenticity, and the chain of custody of this digital image.

ACKNOWLEDGEMENTS

Special thanks belong to Rebecca Bussjager, from the AFRL/SNDP (Air Force Research Lab) at Rome, NY. She was very helpful in designing the different lens combinations necessary to achieve the correct image size and depth of field. The main factors we had to consider were the viewfinder to eye distance, and the viewfinder to CMOS sensor distance. Rebecca spent much of her after work hours helping us with solutions to these and other optical design challenges. The support she provides is a significant asset to this project and it is greatly appreciated.

REFERENCES

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

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

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

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

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

[vi] 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

[vii] 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

[viii] 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

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

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

[xi] 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

[xii] 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

[xiii] 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/

[xiv] 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