Methods for identification of images acquired with Digital cameras

Zeno J Geradts(a), Jurrien Bijhold(a), Martijn Kieft(a), Kenji Kurosawa(b), Kenro Kuroki(b), Naoki Saitoh(b)
(a) Netherlands Forensic Institute, Volmerlaan 17, 2288 GD Rijswijk, Netherlands
(b) National Research Institute of Police Science, 6-3-1 Kashiwanoha, Kashiwa, Chiba 277-0882, Japan

ABSTRACT

From the court we are asked whether it is possible to determine if an image has been made with a specific digital camera. This question has to be answered in child pornography cases, where evidence is needed that a certain picture has been made with a specific camera. We have looked into different methods of examining the cameras to determine if a specific image has been made with a camera: defects in CCDs, file formats that are used, noise introduced by the pixel arrays and watermarking in images used by the camera manufacturer.
In the cheaper ranges of cameras, it appeared that there are visible errors in the pixel arrays. The more expensive cameras have better CCDs with fewer errors. The errors can be visualized by averaging the images multiple times. This was visualized with Trust brand cameras. Depending on the amount of compression that has been used, these errors remain visible. We have not recovered any identification method for the Mavica Camera of Sony. Information exists about the settings in the files; however, we could not find a serial number or watermarking in the images. A different noise level has been measured between two Sony Mavica cameras.

Keywords: Pixel defects, forensic science, compression, digital cameras, CCDs, watermarking, pixel arrays, image comparison

1. INTRODUCTION

Many new digital cameras are available on the market. From the court we receive questions if an image has been acquired with a specific camera. Often these images have become available on the Internet or other distribution channels. In cases with child pornography this is a relevant question if a camera has been found with a suspect.
For this project we evaluated different methods of examining the cameras:
(1) Defects in pixel arrays and compensation for these errors in the cameras
(2) Noise introduced by the pixel array
(3) File formats that are used
(4) Watermarking in images used by the camera manufacturer
The first method with defects of the CCD is investigated and tested for actual cameras. It is known that this method can be used for analogue and digital video cameras;[1] however, we have not found any references for still cameras. In this research the work is focused on still cameras and the method for identification of images that are acquired by these cameras.

2. PIXEL DEFECTS

2.1 Technical Defects of CCDs

For understanding pixel defects, it is important to have some background information on the way that a CCD (Charge Coupled Device) operates. The CCD refers to a semiconductor architecture in which the charge is transferred through storage areas. Three basic functions are distinguished in a CCD:

- Charge collection
- Charge transfer

Enabling Technologies for Law Enforcement and Security, Simon K. Bramble, Edward M. Carapezza, Leonid I. Rudin, Editors, Proceedings of SPIE Vol. 4232 (2001) © 2001 SPIE · 0277-786X/01/$15.00

- Conversion of charge to voltages

With these CCDs an absorbed photon will create an electron hole pair. Depending on the CCD, the holes or the electrons can be transferred. There is considerable literature and patents on the manufacturing, physics and operations of a CCD[2].

If a positive voltage is applied to the CCD gate, this causes the mobile positive holes in p-type silicon to migrate downwards since charges will repel. This region, which is void of positive holes, is called the depletion zone. If the depletion zone absorbs a photon whose energy is greater than the energy gap, it will produce an electron-hole pair. The electron stays in the depletion zone, whereas the hole moves to the ground electrode. The amount of electrons that can be collected is proportional to the applied voltage, oxide thickness and gate electrode area. The total number of electrons that can be stored is called the well capacity.

The CCD register consists of series of gates. Manipulation of the gate voltage in a systematic and sequential manner transfers the electrons from one gate to the next in a conveyor belt manner. For charge transfer, the depletion zones should overlap. Each gate has its own control voltage that can be varied in time. The voltage is called the clocking signal. When the gate voltage is low, it will act as a barrier. This works as an electronic shutter. The charge is transferred by column. This will result in a serial data stream for the two dimensional image. Figure 1 shows the operation in a graphical way.

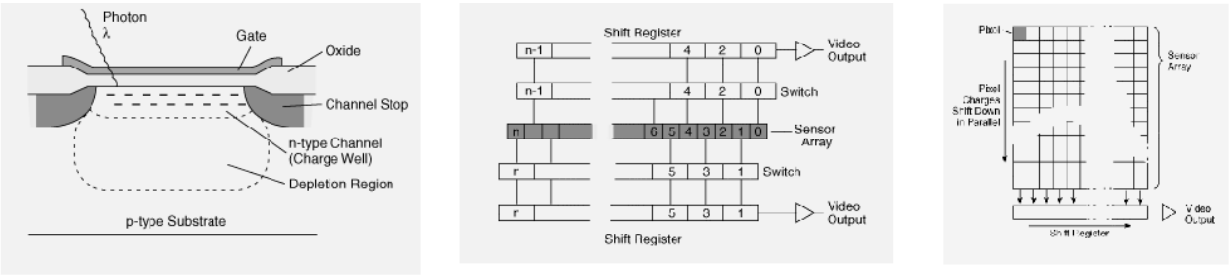

Figure 1: *Operation of a CCD*

When manufacturing large arrays, they sometimes contain defects. The defects are often given in the datasheets of manufacturers. The definitions of these artifacts differ for each manufacturer. Arrays with a large number of defects are less expensive than arrays with a few defects.

Manufacturers give the next definitions:

- Point defects: if a CCD is illuminated to seventy percent of its saturation, the pixel deviates more than six percent
- Hot point defects: pixels with very high output voltages (the dark current is ten times higher than average)
- Dead pixels: pixels with a poor responsitivity
- Pixel traps: problem with the charge transfer process, and results in partial or complete bad columns
- Cluster defects: a cluster of point defects

In most commercial cameras there exists hardware for compensating the errors in the cameras.[3] Four classes of defects with four specific origins are dark current sources [4]:

(1) Dislocations from device stresses, from process stresses, and from the unfaulting of stacking faults;
(2) Stacking faults nucleated from front side damage;
(3) A defect located at the Si/SiO2 interface;
(4) A defect of dimensions that causes banding in the dark current pattern. The position of the defect can be random.

2.2 Experiments

We examined different CCD-cameras (from the 640x480 to the over 2-million pixel cameras). The cheap cameras were the Trust brand, and the more expensive cameras were the Sony brand.

Trust Photocam

The Trust brand cameras appeared to actually be of the TECO brand Dimera 3500-cameras with 350 Kpixel CCD and 2 MB Flash Memory (this information was given by the importer of these cameras). It was possible to determine the pixel defects in these cameras when there is a black background (Figure 2) and when using a contrast enhancement. We have tested the

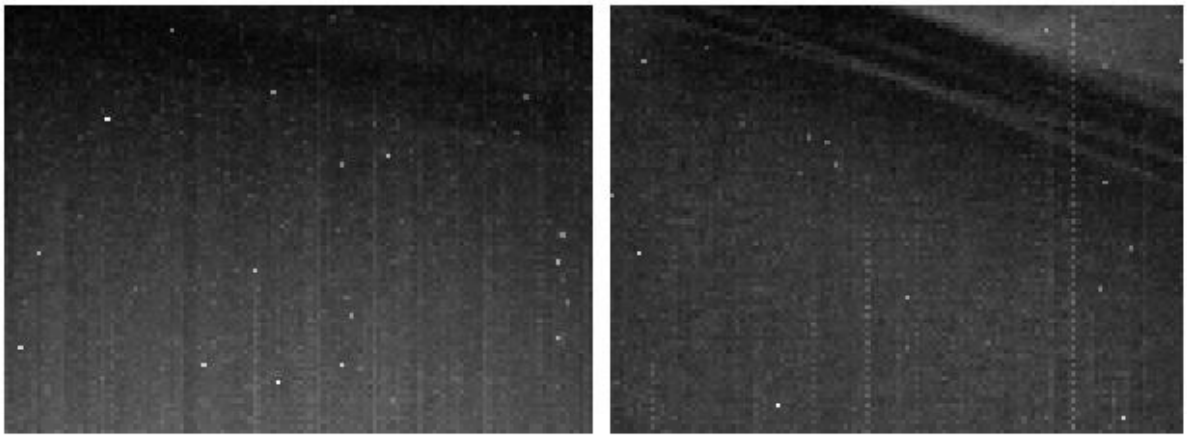

Figure 2: *Ten blank images are averages in a movie. The white spots are the pixel defects. They appear on different places for two different Trust cameras*

errors in 12 different Trust brand cameras. In each camera, there were at least 5 pixels that had pixel defects, and each CCD had pixel defects on another place. For each camera we could distinguish the next numbers of pixel defects: 8, 10, 12, 6, 13, 5, 7, 12, 9, 11, 8, 15 and 25. We counted these pixel defects by comparing five images acquired by the same camera and finding the pixel defects that were reproducible in these images.

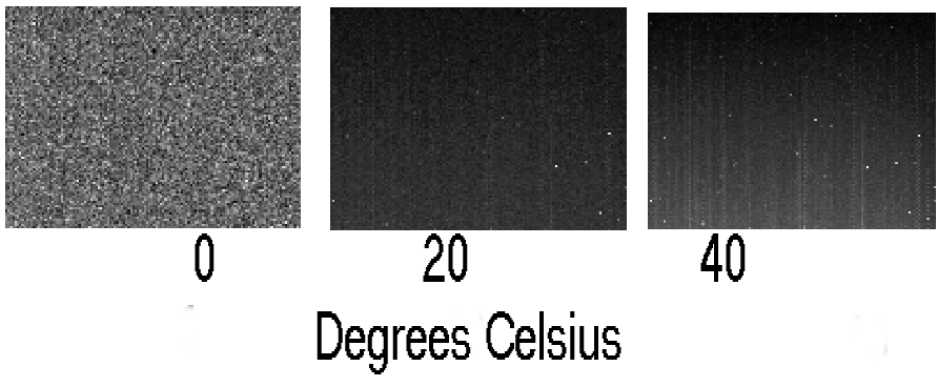

Figure 3: *Pixel defects at different temperatures for the same Trust camera*

For determining what kind of quality the manufacturer delivers for the CCD-chip, we dismounted the camera and took out the CCD-chip. It appeared to be a Sharp LZ23BP2-chip. The data-sheets are available on line [5]. In the data sheet a Photo Sensitivity non-uniformity of ten percent is allowed. This is defined by (Vmax-Vmin)/Vo, where Vmax and Vmin are the maximum and minimum values of each segment's voltage respectively. Vo is defined as the standard condition when Vo = 150 mV.

Since the datasheets stated that defects also depend on temperature, we cooled the cameras to zero degrees Celsius, and it appeared that less pixel defects were visible. When increasing the temperature to 40 degrees Celsius, it appeared that more pixel defects could be seen. After cooling down, the pixel defects were visible at the same position. In Figure 3 the images in different temperatures are visualized. The pixel defects are visible if there is an image taken of a dark object or a grey surface. Furthermore, there should be several images available. For this reason the visibility of the defects depends on the contents of the actual image.
In Figure 4 an example is shown of a real image. We could visualize a number of pixel defects in this image. In this camera we could distinguish 15 pixel defects, and when compared with the real image, six pixel defects were visible as is

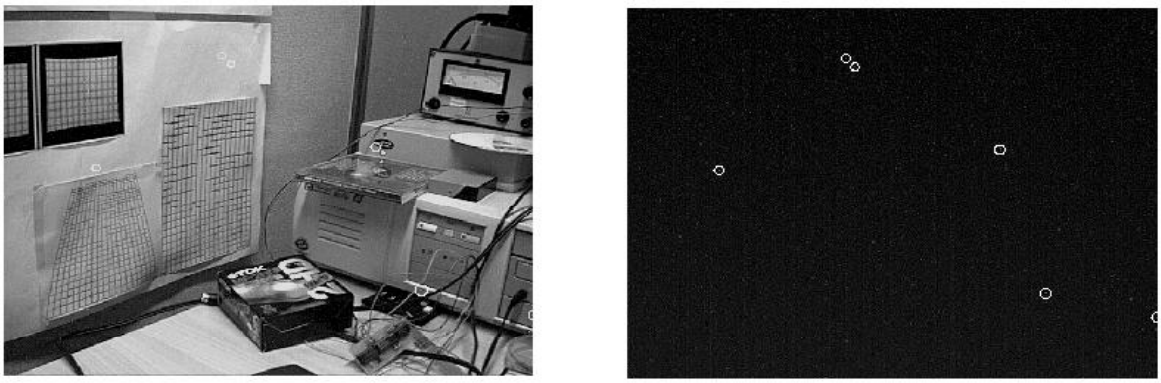

Figure 4: *Pixel defects in a real image (left) on the right the pixel defects are pointed out*

shown in this image. The pixel defects were visible in the regions that were darker and in the lighter areas if a surface with the same intensity lighting was visible. Furthermore, we could make more pixel defects visible in other images that we took with this camera.
Since we were interested in the cause of the pixel defects, we have taken out the CCD. The color filter was on top of the CCD, and we had to remove the color filter with a chemical (Hydrogen Fluoride for 10 seconds). We could see spots on the CCD as is shown in Figure 5. We could match some of these defects with the pixel defects in the CCD; however, more experiments are needed to determine if the pixel defects can be visualized on the CCD itself. From these experiments it is still not clear which kind of pixel defects (as mentioned in the previous sections) are visible; however, they appear to be random.

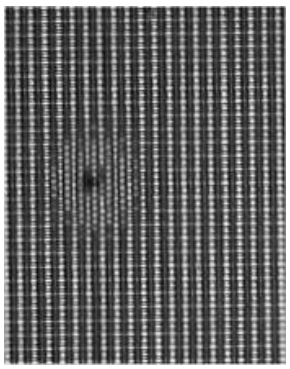

Figure 5: *magnification of a part of a CCD array of Trust camera with damage*

Other cameras

We could make the pixel defects visible with the Camera Photocam LCD Pro of Trust with the CCD-chip of Sony 008 XDYK ICX204AKA. The more expensive cameras have better CCDs with fewer errors. We investigated these errors by averaging multiple images; however, we could not make these errors visible in the Sony Cybershot, Sony Mavica, Sony FD83 and Sony Handycam. It appeared, however, that the noise levels between the same cameras are different.

2.3 Compression

Compression might influence the visibility of pixel defects. For this reason, we tested an uncompressed image of pixel defects of the Trust camera with different compression levels of standard JPEG-compression. In these experiments it appeared that the position of the pixel did not change until a compression of 50 was used. In the highest compression modes we could see the DCT-matrices very well. Some of the pixels were spread out, depending on the position of the matrix and the pixel defects. Figures 6 and 7 show the results.

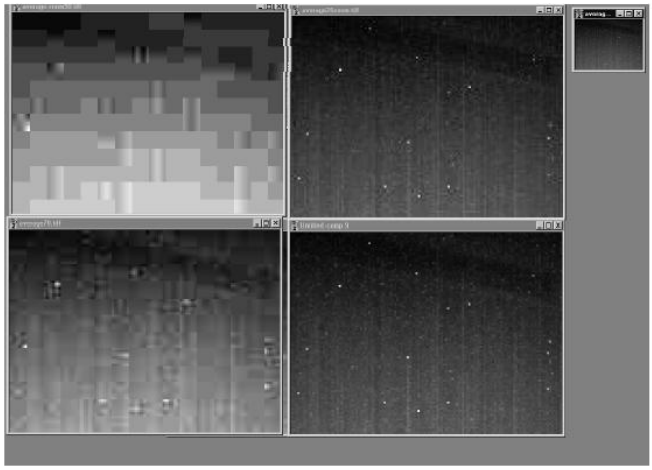

Figure 6: *Pixel defects for Trust camera. The influence of standard JPEG-compression if tested at the position of the pixels (image up, left: factor 90 compression; up right compression of 50; down left: 70; down right: uncompressed)*

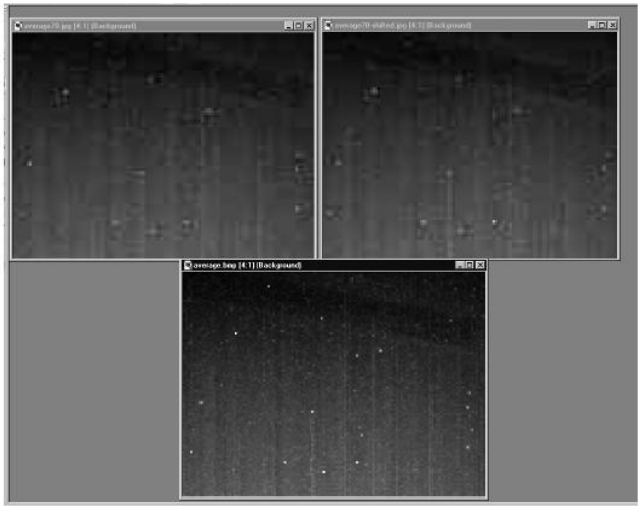

Figure 7: *Influence of shifting of an image at high compression level (70) s of JPEG. The pixels spread out, depending on the position of the DCT-matrix.*

2.4 Evidence Interpretation

We suggest using the Bayesian framework[6 7] to interpret the evidence from pixel defects comparisons (see e.g., Robertson and Vignaux 1995, Aitken 1995). Suppose that in a legal case an image with child pornography (the crime image) is compared with a camera from a suspect. Several reference images are made with the camera and the pixel defects in them are compared with those in the crime image. Each comparison between a reference image and the crime image will yield some similarities and some differences, which we will call the results. Suppose that the following two hypotheses are considered to be of interest in the case:

(A) The crime image was made by the camera of the suspect, and
(B) The crime image was made by an unknown other digital camera.

The questions that have to be answered in order to find the evidential strength in this case are:

(1) How probable are the results if the crime image was made by the camera of the suspect (hypothesis A is true),
(2) How probable are the results if the crime image was made by an unknown other digital camera (hypothesis B is true).

The evidential strength is defined by the ratio of the probabilities (1) and (2), the so-called likelihood ratio (LR). In order to estimate the probability (1), we need to have information about the variation of pixel defects in images made by the suspect's camera. This information can be obtained from the reference images, and from research about the behavior of pixel defects when a camera is being used over time. In general, probability (1) will be large when the pixel defects in the crime and reference images are very similar, and will be small if they show many dissimilarities which are hard to explain e.g., by wear.

In order to estimate the probability (2), we need to have information about the pixel defect patterns found in other cameras, not necessarily from the same brand or type as the suspect's camera. This requires knowledge of how the defects are produced and data about pixel defect patterns from different camera types and brands.

As a highly simplified example: suppose that the pixel defects are due to a pure random process, which yields a fixed probability *p* for each pixel to be a defect, independent of all other pixels. Furthermore, suppose that two images of the same camera always contain exactly the same pixel defects. Under these conditions, the crime image can only be produced by the suspect's camera if the pixel defect pattern is exactly the same, say a vector *V* of zeros and ones describing the positions of *x* pixel defects in a total of *N* pixels. The probability (1) is the probability that both the suspect's camera and the crime image show pixel defect pattern V if the suspect's camera made the image. This simplifies to the probability that the suspect's camera shows pixel defect pattern V, denoted as Pr[suspect's camera = V]. The probability (2) is the probability that both the suspect's camera and the crime image show pixel defect pattern V if an unknown camera made the image. Under the assumption that the unknown camera and the suspect's camera have independent pixel defect patterns, probability (2) simplifies to:

$$\Pr[\text{suspect's camera} = V] \times \Pr[\text{unknown camera} = V] \quad \textbf{(1)}$$

Hence,

$$LR = 1/\Pr[\text{unknown camera} = V] \quad \textbf{(2)}$$

It is easy to derive from our assumptions that:

$$\Pr[\text{unknown camera} = V] = p^x (1-p)^{N-x}. \quad \textbf{(3)}$$

Hence, the evidential strength is given by :

$$LR = 1/\, p^x (1-p)^{N-x}. \quad \textbf{(4)}$$

For realistic values of *p*, *x* and *N* this can yield quite large LR values, meaning strong evidence that the suspect's camera made the image. We emphasize, however, that this example is very much simplified and is given for illustration purposes only.

3. OTHER METHODS

For finding information that is relevant for the identification, the files have to be compared. For finding a serial number in headers, a hex editor can be used. Images of different cameras can be compared, and the differences between the image headers might give information on a serial number. We have examined this for our cameras; however, we could not find any difference for the file headers.
For the Sony Mavica, the evaluation of the file format can be useful for getting an indication on what kind of file has been used. Furthermore, the settings of the camera are also stored in the headers. We could not find any serial number in the file itself, except for a counter in the filename. This information is stored in a separate file.
The comparisons of noise levels are possible by making an image of the same object and comparing the images with each other. For comparison we have used a white surface and made a black image by shutting the lens, since this is most reproducible. We have seen a difference of the noise level between two Sony Mavica cameras.
The investigation of watermarking and steganography[8] is possible if it is known what kind of algorithm has been used. If this is not known, there is an option by trial and error method of contrast enhancement. This is most optimal on a black image and a gray or white image, since the object in the image will not disturb the watermark. We have not seen any watermark in the examined cameras. Steganography is also an option for hiding data in an image by the manufacturer; however, we also could not find evidence that this is used yet.

4. CONCLUSION AND DISCUSSION

We examined twelve Trust brand cameras. It appeared that the errors in the CCDs were visible and it might be possible to identify the camera. The pixel defects were on random places of the CCD. More expensive cameras did not have pixel defects that were visible. Image compression algorithms can, however, suppress or move the pixel defects and noise.[9] In a forensic report the final conclusion of such work should be considered carefully, since it is not known if other cameras have the same pixel defects at the same place. Even with the cameras used, we do not know if they were from the same batch. The exact cause of the pixel defects should be investigated before drawing a final conclusion based on this work. For this reason the manufacturing process itself should be studied, and subsequently manufactured CCDs should be investigated and compared.
For cameras where no pixel defects are visible, different methods should be used, such as images that are on the camera or that are in the memory or the raw files that come from the camera when transferring images to the hard disk of a computer. We evaluated the different strategies that can be used to research the file formats. Some cameras can even have the serial numbers in the headers of the files[10] or in a cryptographic way;[11] however, we do not know of a commercial camera where this has been implemented yet. Furthermore, in patents,[12] watermarking is described as a way of identification. There are possibilities that this information is erased as the images are converted to other formats.
For digital video there are also other methods for examination. Since multiple image frames exist in these kinds of video file formats, averaging multiple image frames can be used for these systems. Also the existing noise levels in the video can be determined if a dark image has been recorded. Fixed pattern noise (FPN) refers to pixel-to-pixel variations that occur when an array is in the dark.
In a real court case, we could solve the claim in a different way. The camera of a suspect was submitted to our laboratory and apparently there were no images found on the camera itself. When examining the buffer memories in the camera by the menus, the images appeared to be erased. We had to take the memory chips out of the camera and examine the chip that had been used. It appeared that there was a function in the chip itself to find the erased images. In this case child pornography was found on the erased images. We also found pixel defects in this CCD; however, this is not used in the evidence.
When doing casework for identifying cameras, it is necessary to acquire more cameras of the same model. The cameras should acquire a sample image under the same condition to be compared for differences. Depending on the camera used, noise levels should also be considered for the investigation.

5. ACKNOWLEDGMENTS

The authors would like to thank Marjan Sjerps for the valuable discussion about the statistics in this paper. Furthermore, we would like to thank Kees Kuit for examining the CCD-chips and the flash cards in the cameras.

6. REFERENCES

1. K. Kurosawa, K. Kuroki, N. Saitoh, CCD *Fingerprint method - identification of a video camera from videotaped images*, IEEE International Conference on Image Processing **3**(1), p 537-540, 1999.
2. G. Holst, *CCD arrays, cameras and displays*, SPIE, 1998, ISBN 0-9640000-4-0, 1998.
3. N. Suzuki, Pixel defect removing circuit for solid-state image pickup device, patent US5327246, file date Jan. 23, 1992.
4 H.F. Schaake, C.G. Roberts, A.J. Lewis, *Characterization of electrically active defects in silicon using charge coupled device (CCD) image sensors*, Report (1978), TI-08078-08; Order No. AD-A069536, 181 pp., NTIS From: Gov. Rep. Announce. Index (U. S.), 79(21), 206, 1979.
5. http://www.sharpmeg.com/products/ccd/pdf/LZ23BP2_db.pdf
6. B. Robertson, G. A. Vignaux, *Interpreting Evidence: Evaluating Forensic Science in the Courtroom*, John Wiley & Son Ltd; ISBN: 0471960268, 1995.
7. G.C. Aitken, *Statistics and the Evaluation of Evidence for Forensic Scientists (Statistics in Practice)*, John Wiley & Son Ltd; ISBN: 0471955329, 1995.
8 . S. Katzenbeisser, F.A.P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House; ISBN: 1580530354, 2000.
9. T. Nagasawa, *Imaging, system, video-processing apparatus, encoding apparatus, encoding method, and method of removing random noise*, US5926224, 1997.
10. E. Steinberg , *Method and apparatus for in-camera image marking and authentication*, US5862218, file date April 4, 1996.
11. G. Friedman, *Digital camera with apparatus for authentication of images produced from an image file*, US5499294, 1995.
12. Rhoads; Geoffrey B., *Security system for photographic identification*, US5841886, 1996.