Secure Digital Camera

By

Paul Blythe and Jessica Fridrich

Presented At

The Digital Forensic Research Conference

DFRWS 2004 USA Baltimore, MD (Aug 11th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Secure Digital Camera

DFRWS 2004

Paul Blythe and Jessica Fridrich

BINGHAMTON UNIVERSITY

Research sponsored by the Air Force Research Laboratory

Presentation Outline

- Scenario
- Secure Digital Camera
- Biometrics
- Lossless Embedding for JPEG (Demo)
- Experimental Setup
- Conclusions

Scenario

Problem: Digital images are not easily acceptable in a court because it is difficult to establish their integrity, origin, and authorship

Solution: Construct a (secure) digital camera for which one can prove that a given digital image

- Was not tampered with
- Was taken by a this particular camera
- Was taken by a specific person

Anticipated use: Establishing the chain of custody for forensic photographers

Prior Art

Watermarking Cameras:

Epson

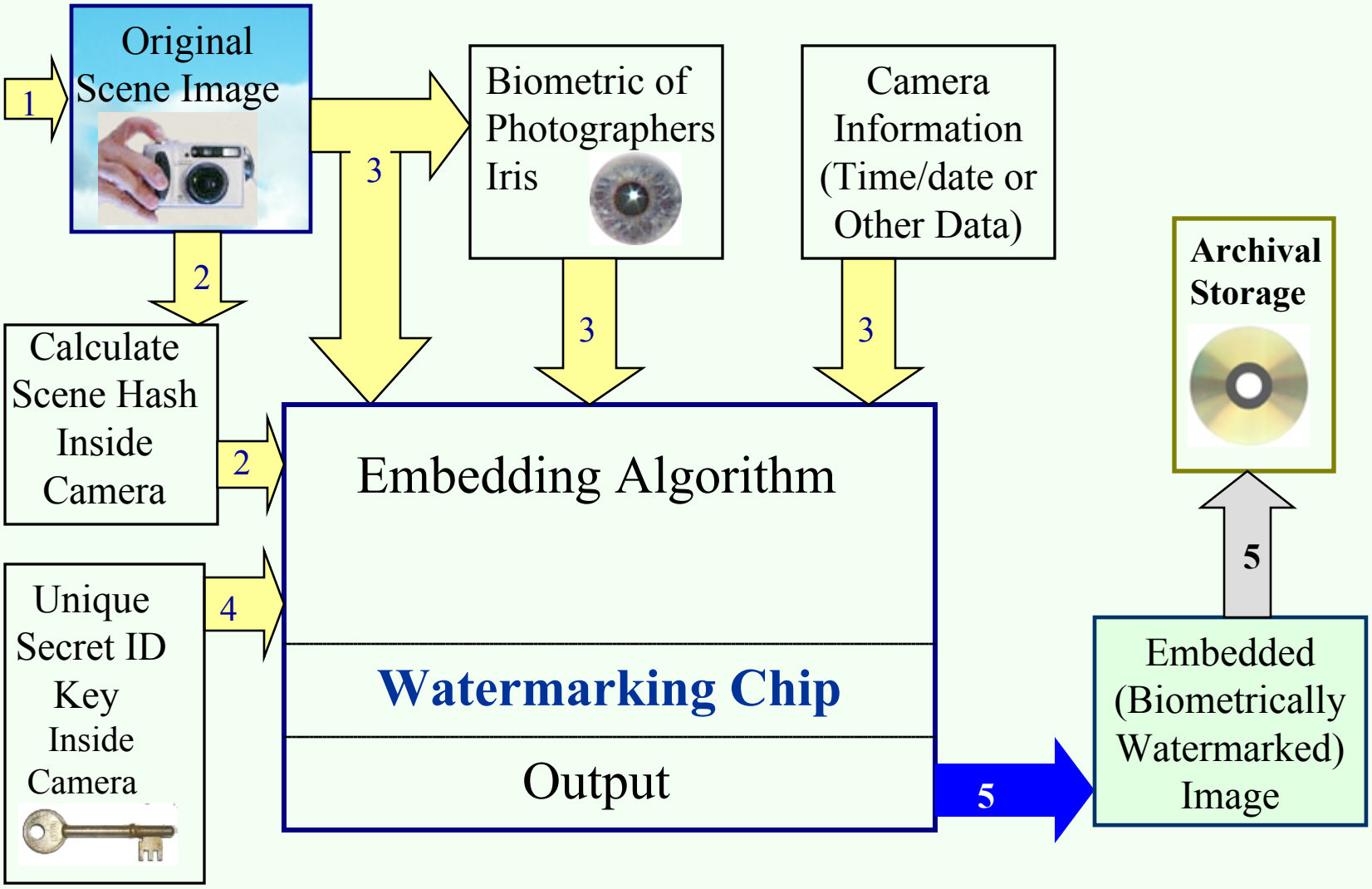
- Requires optional watermarking software for embedding and viewing of watermark
- Detect tampering even if a single pixel has been changed
- Watermark is invisible

Kodak

- Watermarking capabilities built into camera
- Visible watermarking only
- Watermark logo can be added after picture is taken

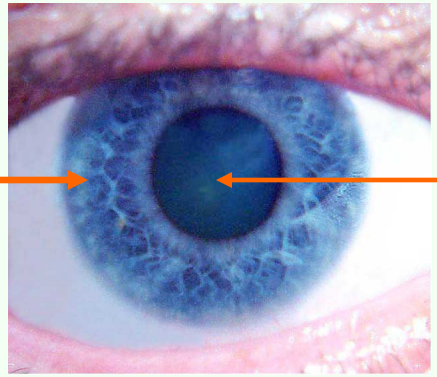
Both cameras add non removable distortion to the image

Secure Digital Camera



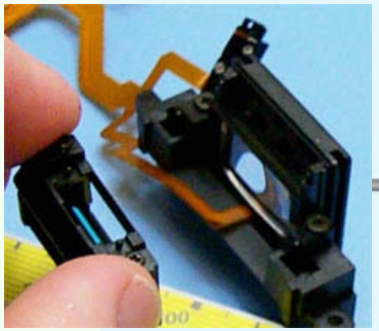
Embedding Scenario

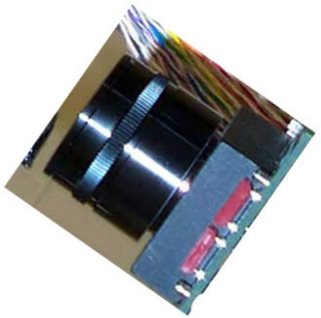
Iris Biometric

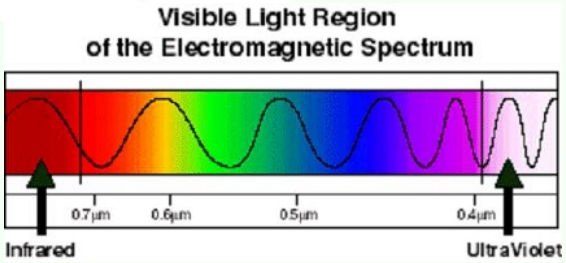


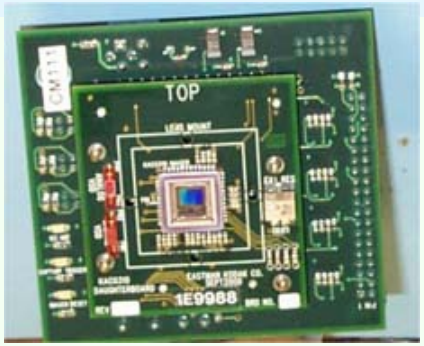
- Iris recognition is based on visible features, i.e. rings, furrows, freckles and corona.
- Iris patterns possess a high degree of randomness.
- The Iris is essentially formed by 8 months, and remains stable through life.
- Statistically more accurate than even DNA matching since the probability of 2 irises being identical is 1 in 10 to the power of 78 (1^{7}).

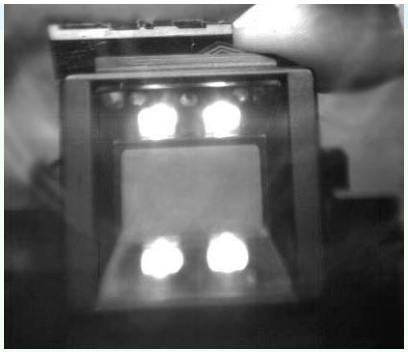
Iris Capture





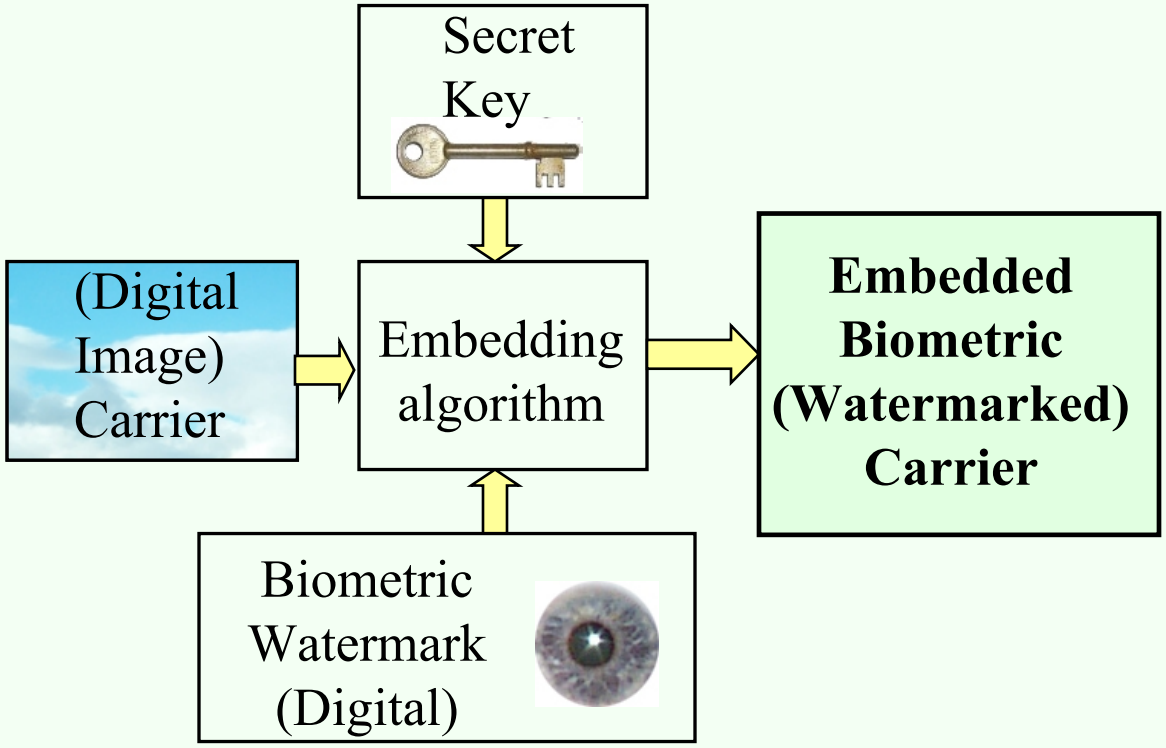






Biometric Watermarking

– Creates a link between a human subject and the digital media by embedding biometric information into the digital object

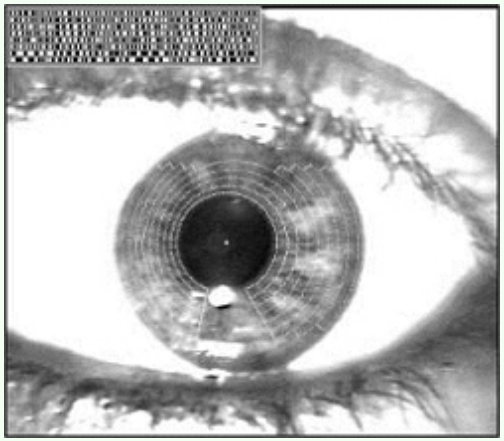


Iris Representation

Iris Code (Daughman 1994)

– Would require a real-time iris image signal-processing chip inside the camera

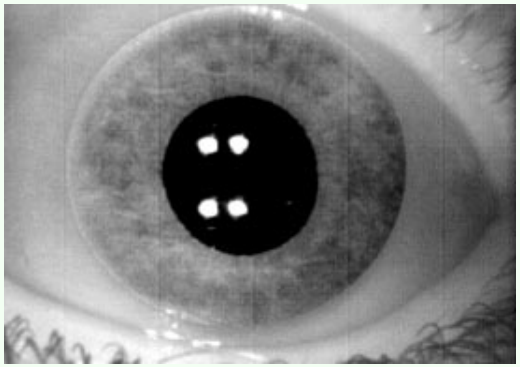
– Can be represented with only 512 bytes



Compressed iris image

– JPEG compression is already supported by the hardware inside the camera

– Requires more embedding capacity



Authentication Watermarks

Can be classified into two groups:

Fragile

– The purpose of fragile watermarks is to detect every possible modification of the image with high certainty.

Semi-fragile

– Semi-fragile watermarks are supposed to be insensitive to “allowed” manipulations, such as lossy compression, but react sensitively to malicious content-changing manipulations

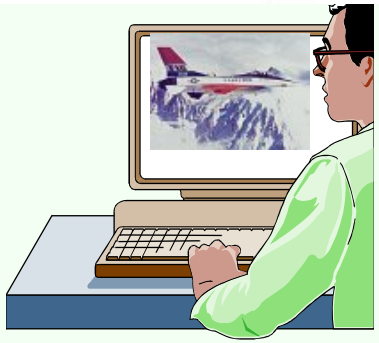
Lossless Embedding

Most watermarks introduce non-reversible distortion due to quantization, truncation, or rounding

<u>This leads to an irreversible loss of information</u>

Unacceptable for forensics
- Difficult legal issues

Unacceptable for medical imagery
- Artifacts are potentially dangerous



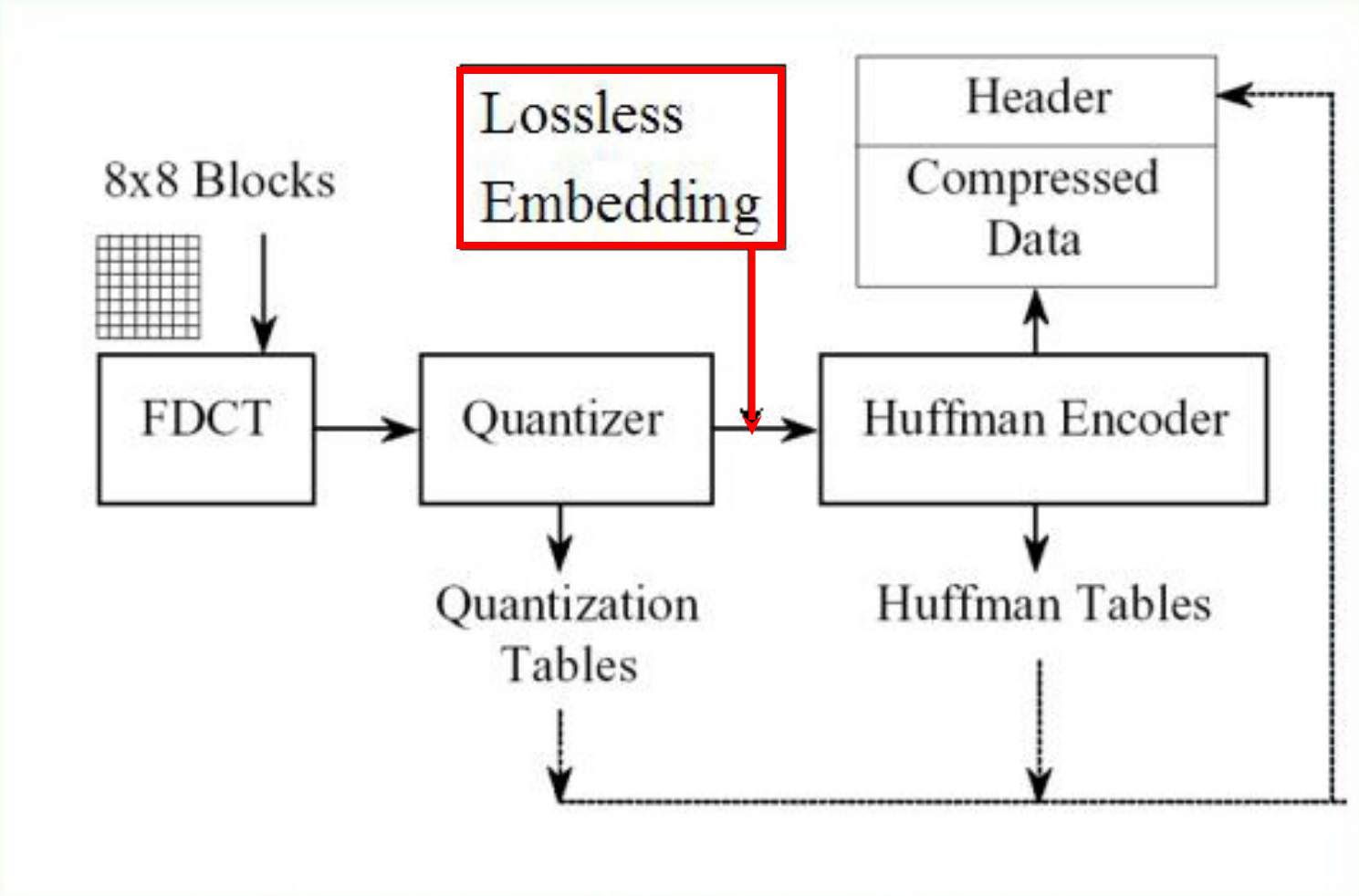
Unacceptable for high-importance military imagery
- Special viewing conditions (zoom)
- Sensitive preprocessing (filters, enhancement)

Lossless Watermarking

– To overcome the problem of authentication watermarks, "**Lossless Watermarking**" was proposed.

– With "**Lossless Watermarking"**, the embedding distortion can be completely removed from the watermarked image and thus one can obtain the original image.

Lossless Watermark Embedding for JPEG



Simplified Block Diagram – JPEG

Lossless Watermark Embedding for JPEG

Original Image (partitioned in 8⌈ 8 blocks) 640 ⌈ 480=307,200 blocks

Step 1) Select one or more Quantization Steps from the Quantization Table (i.e. (5,2) = 30) and Change its value by ½ = **15**

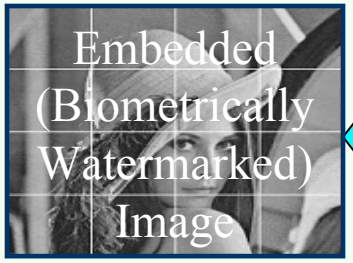
10	10	15	20	25	30	35	40
10	15	20	25	30	35	40	50
15	20	25	30	35	40	50	60
20	25	30	35	40	50	60	70
25	30	35	40	50	60	70	80
30	35	40	50	60	70	80	90
35	40	50	60	70	80	90	100
40	50	60	70	80	90	100	110

Quantization table

Step 2) All corresponding DCT coefficients in all blocks of the image are multiplied by 2 (2⌈ 4= **8**)

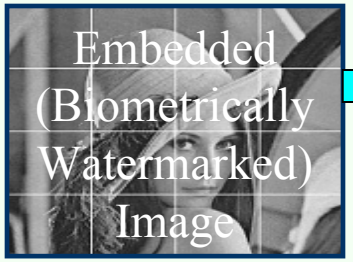
DCT coefficients

120	60	40	30	4	3	0	0
70	48	32	3	4	1	0	0
50	36	4	4	2	0	0	0
40	4	5	1	1	0	0	0
5	4	0	0	0	0	0	0
3	2	0	0	0	0	0	0
1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0



Step 3) Lossless & Invertable (LSB) embedding is used to keep the image appearance unchanged.

Lossless Watermark Extraction



Step 1) The randomly embedded LSBs are identified

Step 2) Extract the LSBs of the DCT coefficients along the path

Authentication Data

DCT coefficients

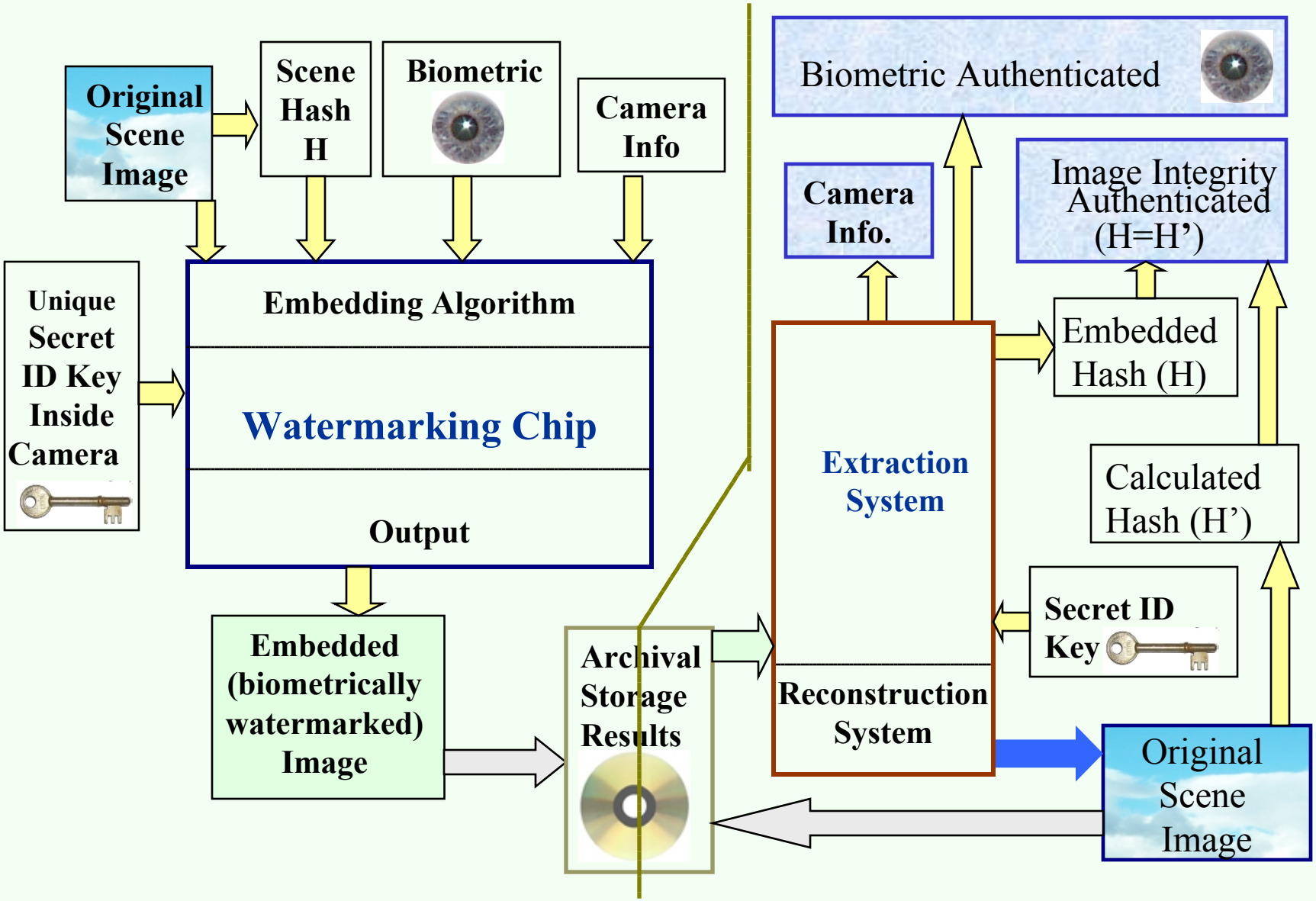
120	60	40	30	4	3	0	0
70	48	32	3	4	1	0	0
50	36	4	4	2	0	0	0
40	4	5	1	1	0	0	0
5	4	0	0	0	0	0	0
3	2	0	0	0	0	0	0
1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0

10	10	15	20	25	30	35	40
10	15	20	25	30	35	40	50
15	20	25	30	35	40	50	60
20	25	30	35	40	50	60	70
25	30	35	40	50	60	70	80
30	35	40	50	60	70	80	90
35	40	50	60	70	80	90	100
40	50	60	70	80	90	100	110

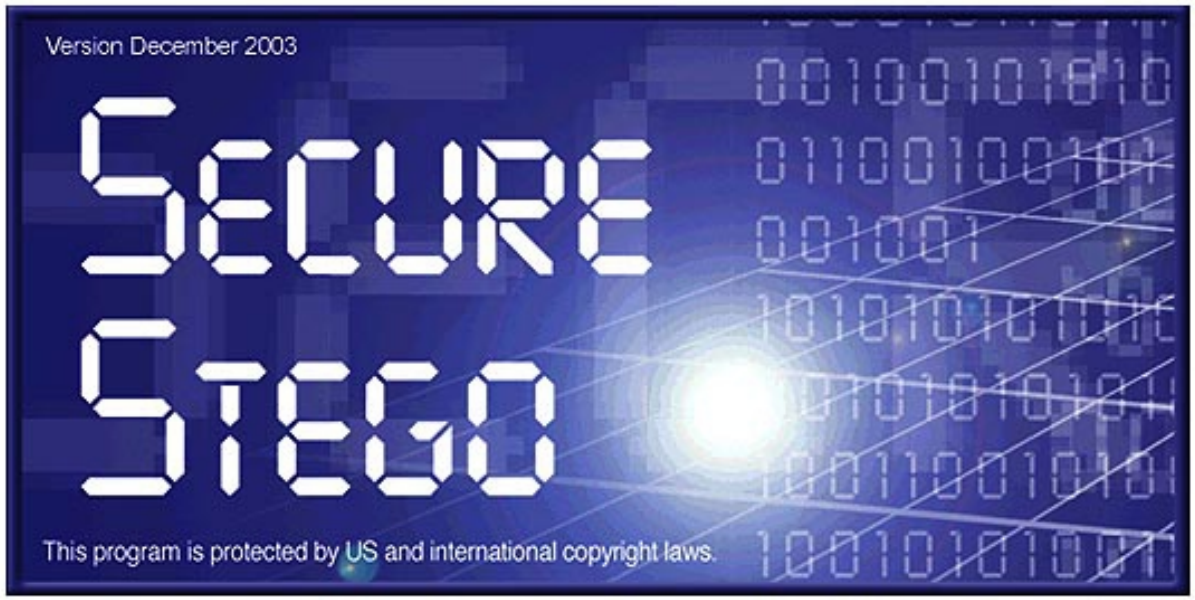
Quantization table

Step 3) All LSBs are set back to zero & DCTs are divided by 2, and the corresponding DCT quantization step is multiplied by 2

Secure Camera Scenario

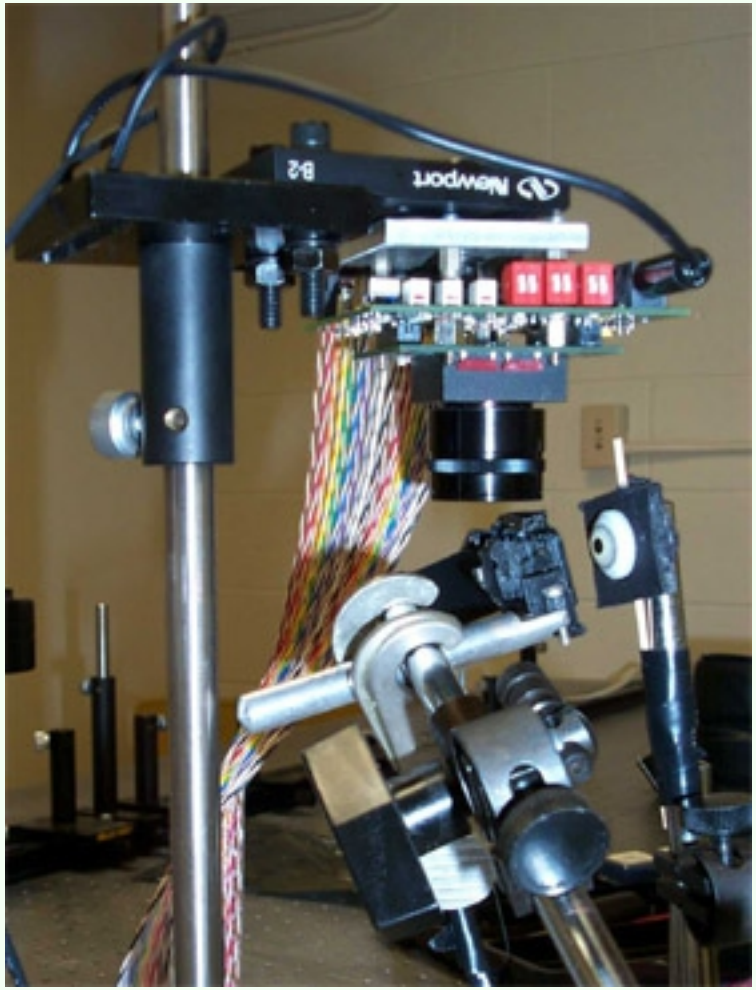


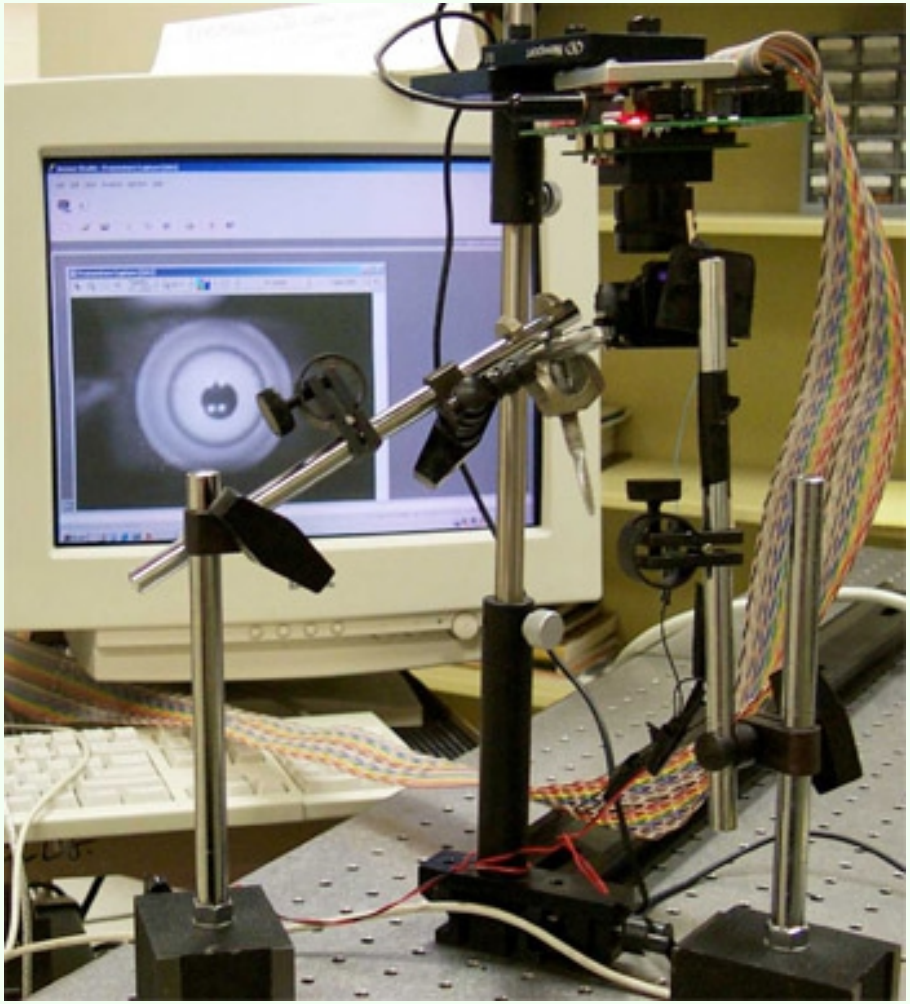
Secure Stego



I will now demonstrate the software we used to simulate the Watermarking Chip. Secure Stego contains a software implementation of our lossless data embedding technique.

Experimental Setup





Conclusion

The Secure Digital Camera offers a solution to the problems associated with the chain of custody for digital images presented to the court.

The solution involves losslessly embedding the compressed photographer's iris (taken through the viewfinder), hash of the scene image, date, time, and other data in the scene image itself

The embedded data

- verifies digital image integrity (secure cryptographic hash)
- establishes image origin (camera information)
- verifies the image authenticity (photographers biometric)