Secure Digital Camera

Saraju P. Mohanty

VLSI Design and CAD Laboratory (VDCL)

Dept of Computer Science and Engineering

University of North Texas.

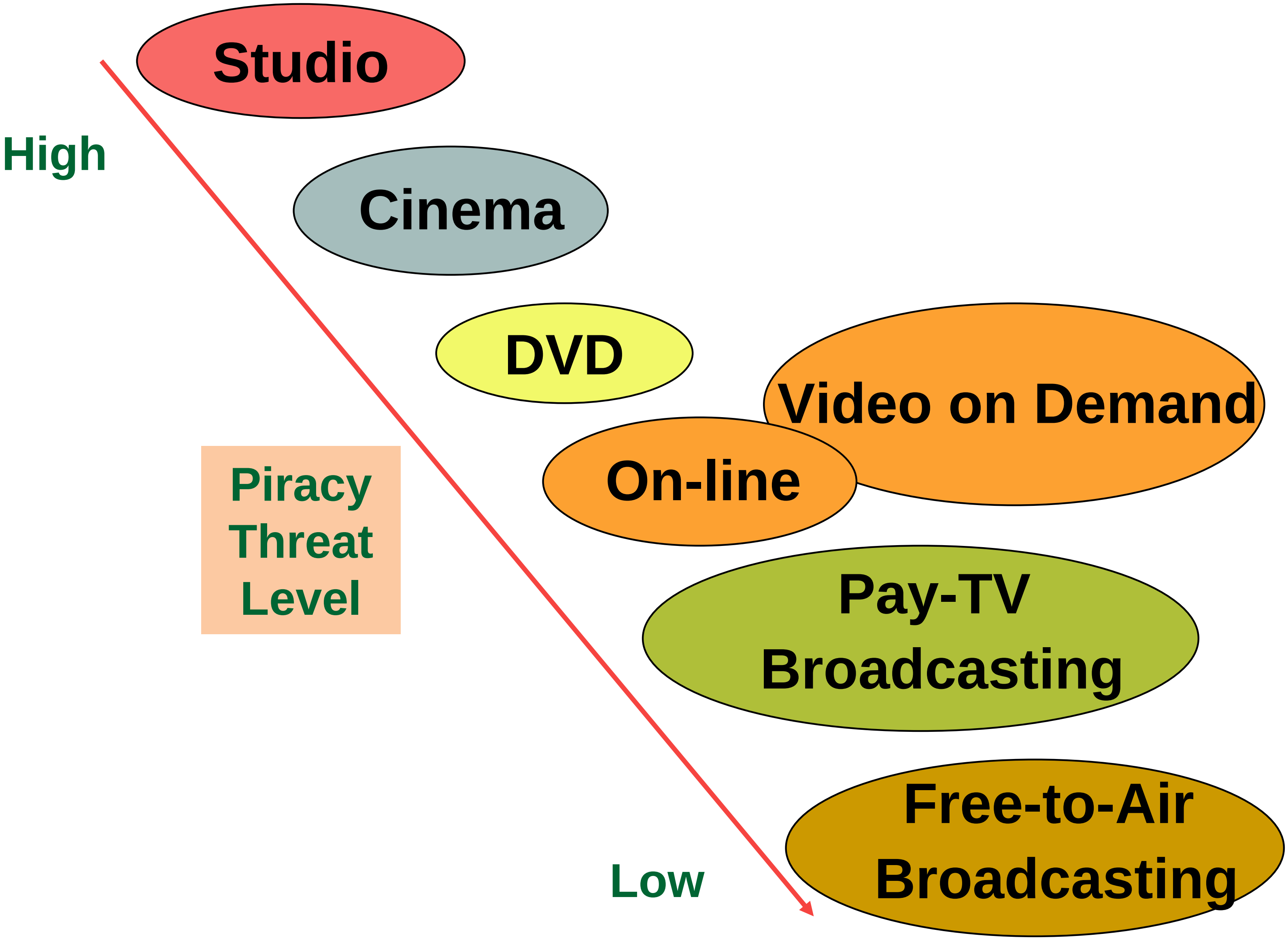
Email: smohanty@cse.unt.edu

Outline of the Talk

- Digital Rights Management (DRM)
- Secure Digital Camera (SDC)
- One of our Digital Integrated Circuit solutions
  - Invisible-Robust / Visible-Transparent Watermarking Low-Power Chip
- Design Challanges
- Application Scenario

What is
Digital Rights Management (DRM)

Multimedia Data



High

Studio

Cinema

DVD

Video on Demand

On-line

Piracy Threat Level

Pay-TV Broadcasting

Free-to-Air Broadcasting

Low

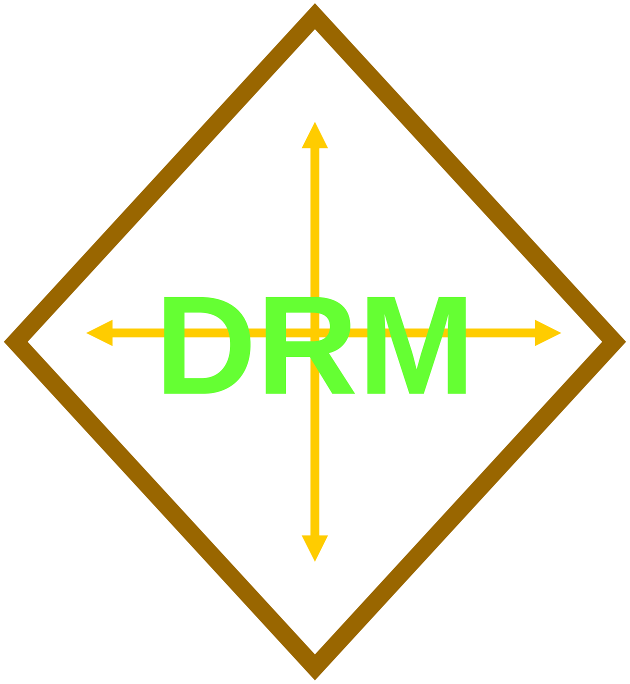
UNIVERSITY OF NORTH★TEXAS™

DRM: Definition

- Broader definition
  - "Digital Rights Management (DRM) involves the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of Rights Holders relationships".

- Typically a DRM system
  - protects intellectual property by either encrypting the data so that it can only be accessed by authorized users and/or
  - marking the content with a digital watermark, so that the content can not be freely distributed

DRM: Perspectives



Business

Governed by Accounting Practices

Transfer of $$

Social

Governed by Social norms

Give a Gift

Technical

Governed by Technical Standards

Legal

Governed by the Laws of the Jurisdiction

DRM Framework: 3 Areas

- **Intellectual Property (IP) Asset Creation and Capture**: process of managing and creation of content in order to simplify its trading.
- **IP Asset Management**: process of managing and enablement the trade of content.
- **IP Asset Usage**: process of usage of content after it has been traded.

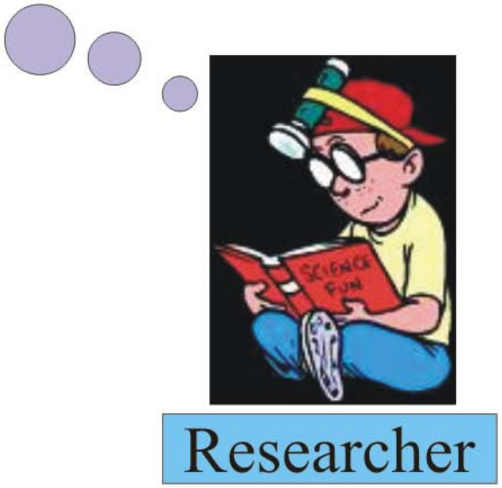
DRM: Techniques

- Encryption
- Watermarking
- Scrambling
- Digital certificates
- Secure communications protocols
- Fingerprinting
- Hashing
- …… and more

DRM: Techniques

It is mine!
Hacker
Multimedia Object
It is mine!!
Owner

- Whose is it?
- How to prove?
- Is it tampered with?
- Where was it created?
- Who had created it?
- What is solution of this ownership problem?

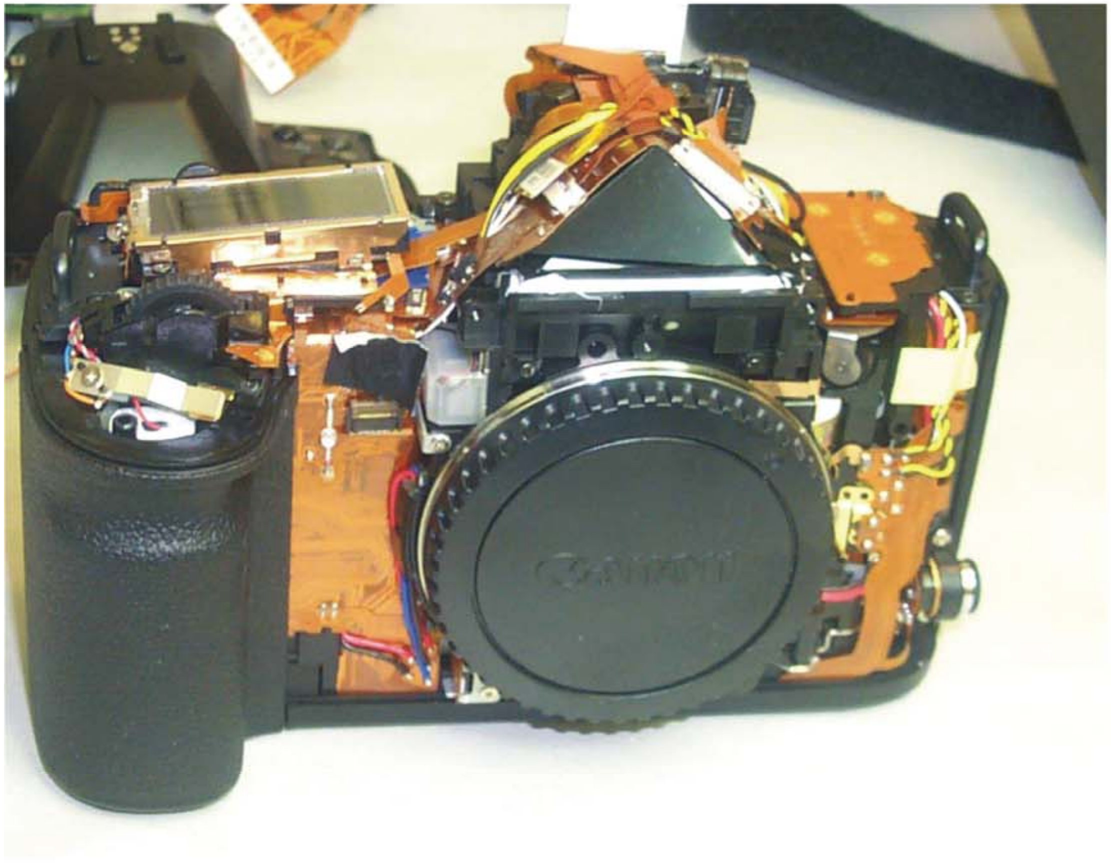


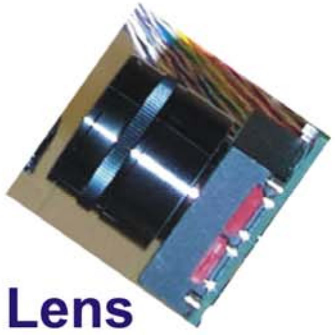
Our Solution for DRM:
Secure Digital Camera (SDC)

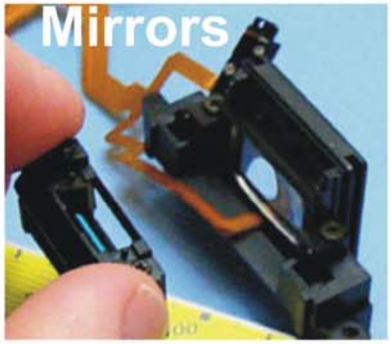
Secure Digital Camera

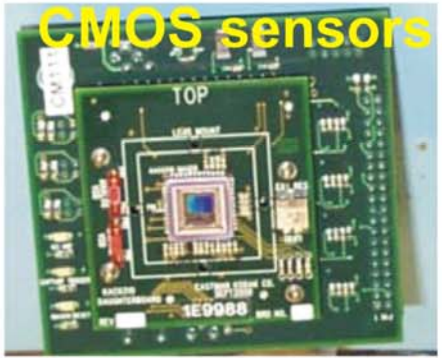
- An apparatus (system-on-a-chip, SoC) with standards features of digital camera and built in facility for live, real-time, low-cost, low-power DRM.
- SDC needs to prove for a given image:
  - Copyright (visible-transparent)
  - Extent of tampering (invisible-fragile)
  - Source of image i.e. camera
  - Cameraman's information
  - ……..

Digital Camera: Internals

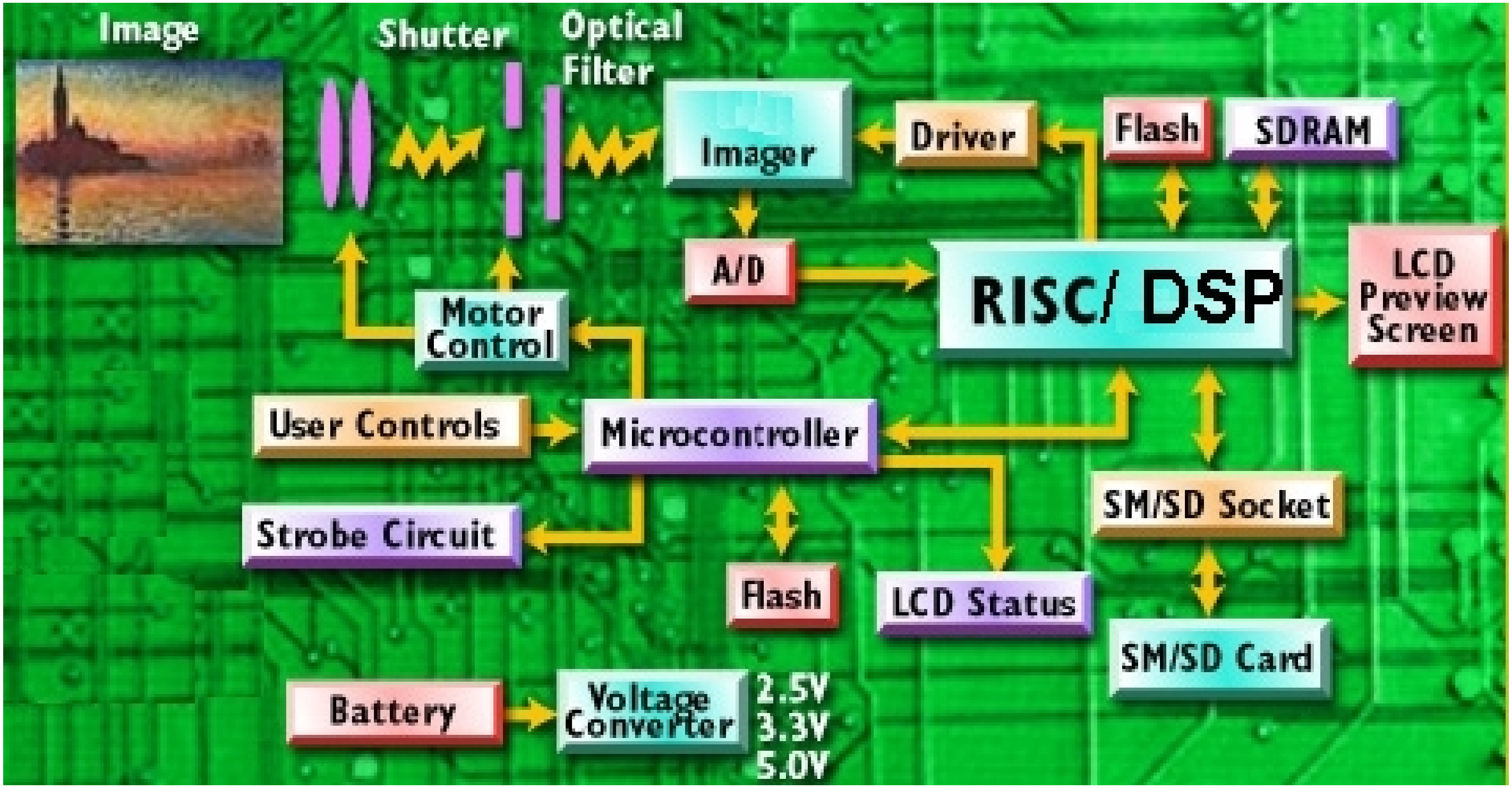




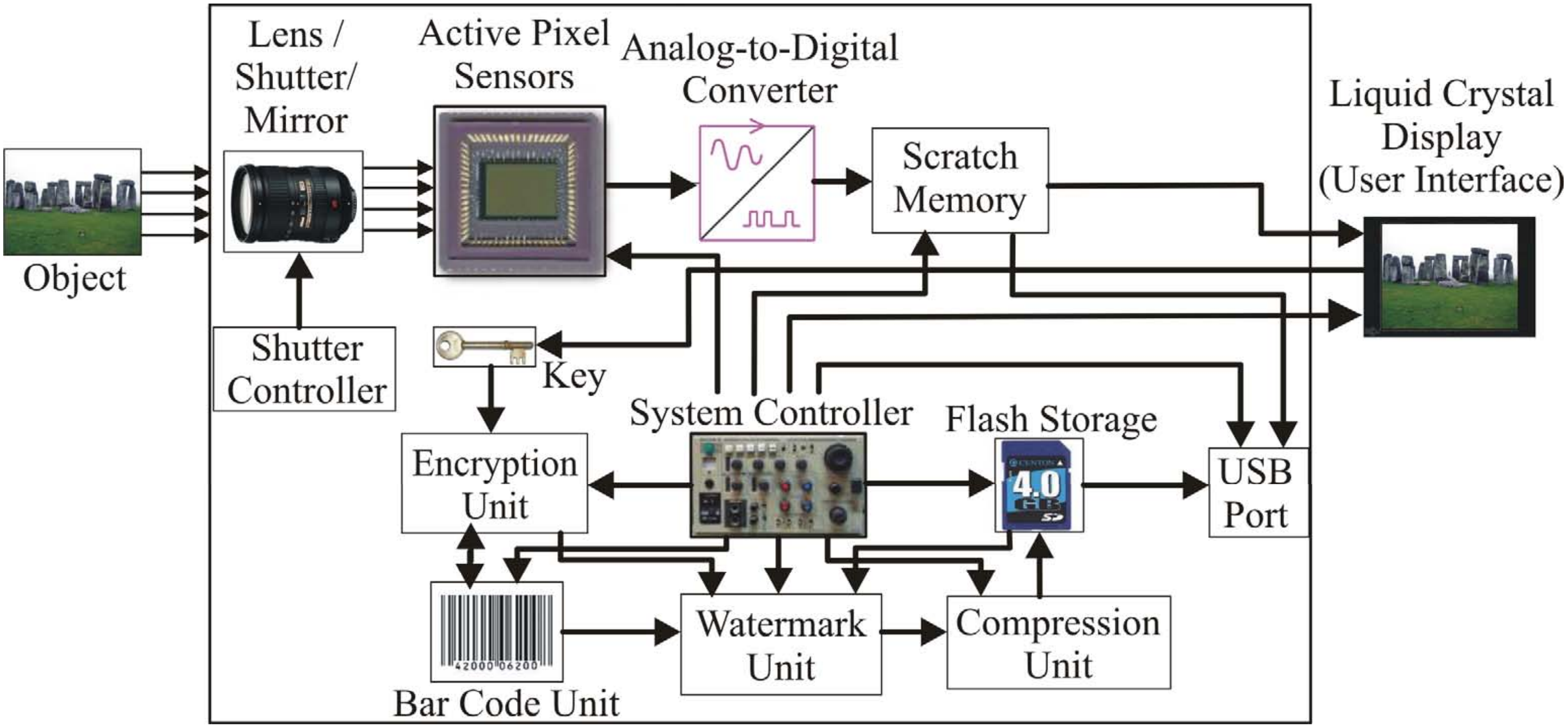




Digital Camera: Typical Circuit



Secure Digital Camera (System-on-a-Chip: SoC)



UNIVERSITY OF NORTH TEXAS™

Hardware Assisted DRM: Advantages

- Easy integration with multimedia hardware, such as digital camera, camcorder, etc.
- Low-power consumption
- High-performance
- Higher reliability and availability compared to software
- More useful for real-time applications like digital video broadcasting
- Low-cost compared to having explicit software

Existing Digital Cameras with Watermarking Capability

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:

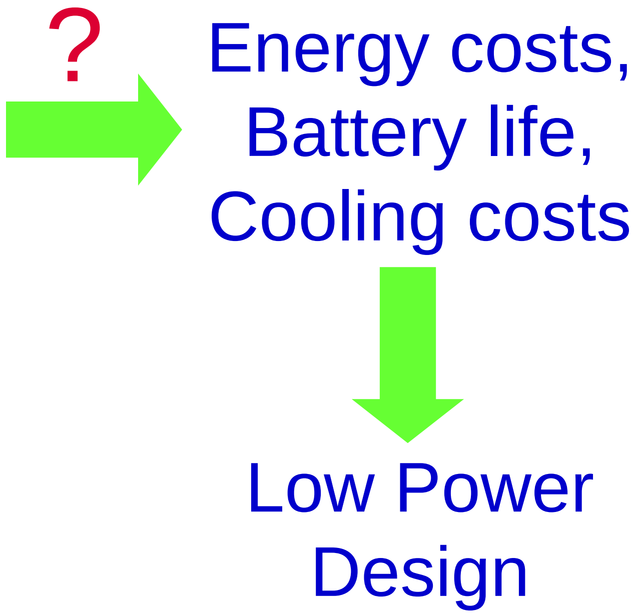
- Watermarking capabilities built into camera
- Visible watermarking only
- Watermark logo can be added after picture is taken

A Invisible-Robust / Visible-Transparent Watermarking Low-Power Chip

Highlights of our Designed Chip

- DCT domain Implementation.
- First to insert both visible and / or invisible watermark.
- First Low Power Design for watermarking using dual voltage and dual frequency.
- Uses Pipelined and Parallelization for better performance.
- Decentralized controller scheme.

Nano-CMOS Based Systems

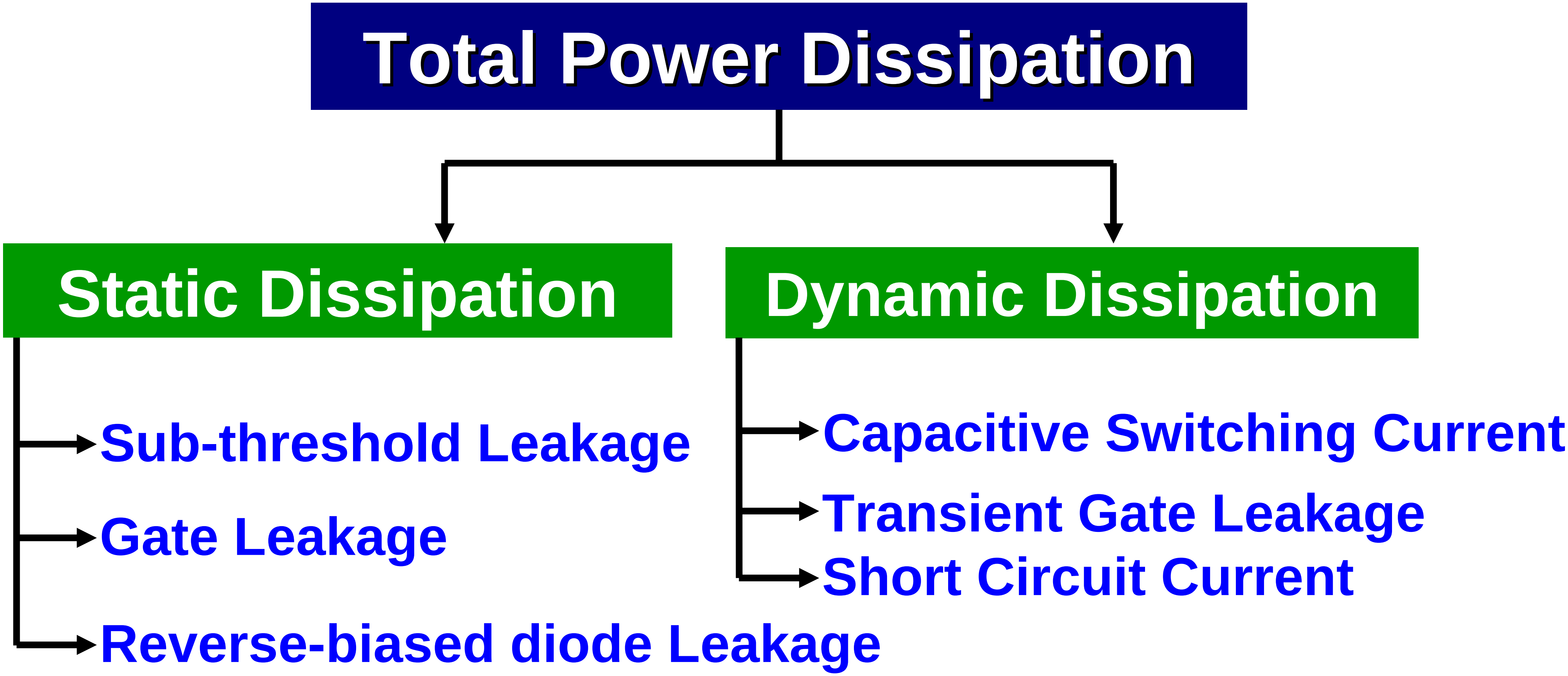

?

Energy costs, Battery life, Cooling costs

Low Power Design

Almost the entire electronic appliance industry today is driven by CMOS technology.

Power Dissipation in Nano-CMOS Based Systems



Total Power Dissipation

Static Dissipation

- Sub-threshold Leakage
- Gate Leakage
- Reverse-biased diode Leakage

Dynamic Dissipation

- Capacitive Switching Current
- Transient Gate Leakage
- Short Circuit Current

Our Low-Power Design Approach

Adjust the frequency and supply voltage in a co-coordinated manner to reduce dynamic power while maintaining performance.

Algorithms Selected for the Chip

- Visible watermarking algorithm:
  - →S. P. Mohanty, K. R. Ramakrishnan and M. S. Kankanhalli, "A DCT Domain Visible Watermarking Technique for Images", in *Proceedings of the IEEE International Conference on Multimedia and Expo*, 2000, pp. 1029-1032.
- Invisible watermarking algorithm:
  - →I. J. Cox, J. Kilian, T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, Vol. 6, No. 12, 1997, pp. 1673-1687.

Invisible Watermarking Algorithm: Original Version

- DCT of the entire original image is computed assuming as on block.
- The perceptually significant regions of the image are found out. The authors have used 1000 largest coefficients.
- The watermark X = $\{x_1, x_2, \ldots, x_n\}$ is computed where each x_i is chosen according to N(0, 1), where N(0, 1) denotes a normal distribution with mean 0 and variance 1.
- The watermark is inserted in the DCT domain of the image by setting the frequency components v_i in the original image to v^*_i using the following for scalar factor α:

$$\boxed{v_i^* = v_i(1 + \alpha x_i)}$$

Invisible Watermarking Algorithm: Modified Version

1. Divide the original image into blocks.
2. Calculate the DCT coefficients of all the image blocks.
3. Generate random numbers to use as watermark.
4. Consider the three largest AC-DCT coefficients of an image block for watermark insertion.

Visible Watermarking Algorithm

1. Divide original and watermark image into blocks.
2. Calculate DCT coefficients of all the blocks.
3. Find the edge blocks in the original image.
4. Find the local and global statistics of original image using DC-DCT and AC-DCT coefficients.
5. The mean of DC-DCT coefficients and mean and the variance of AC-DCT coefficients are useful.
6. Calculate the scaling and embedding factors.
7. Add the original image DCT coefficients and the watermark DCT coefficients block by block.

Visible Watermarking Algorithm

- The α_k and β_k for edge blocks are taken to be α_{max} and β_{min} respectively.
- For non-edge blocks α_k and β_k are computed as:

$$\alpha_k = \sigma^*_{AC_{Ik}} \left[\exp\left\{ -(\mu^*_{DC_{Ik}} - \mu^*_{DC\,I})^2 \right\} \right]$$

$$\beta_k = \frac{1}{\sigma^*_{AC_{Ik}}} \left[1 - \exp\left\{ -(\mu^*_{DC_{Ik}} - \mu^*_{DC\,I})^2 \right\} \right]$$

- α_k and β_k are then scaled to the ranges (α_{min}, α_{max}) and (β_{min} , β_{max}) respectively, where α_{min} and α_{max} are the minimum and maximum values of the scaling factor, and β_{min} and β_{max} are the minimum and maximum values of the embedding factor.

Visible Watermarking Algorithm: Modifications

- Use $c_{Iwhite}(0,0)$ for normalization instead of $c_{Imax}(0,0)$
- Rewrite α_k and β_k equations:

$$\alpha_k = \frac{\sigma_{AC_{Ik}}}{\sigma_{AC_{\mathrm{Im}ax}}}\left[\exp\left\{-(\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^2\right\}\right]$$

$$\beta_k = \frac{\sigma_{AC_{\mathrm{Im}ax}}}{\sigma_{AC_{Ik}}}\left[1 - \exp\left\{-(\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^2\right\}\right]$$

- Removing σ_{ACImax}:

$$\alpha^c{}_k = \sigma_{AC_{Ik}}\left[\exp\left\{-(\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^2\right\}\right]$$

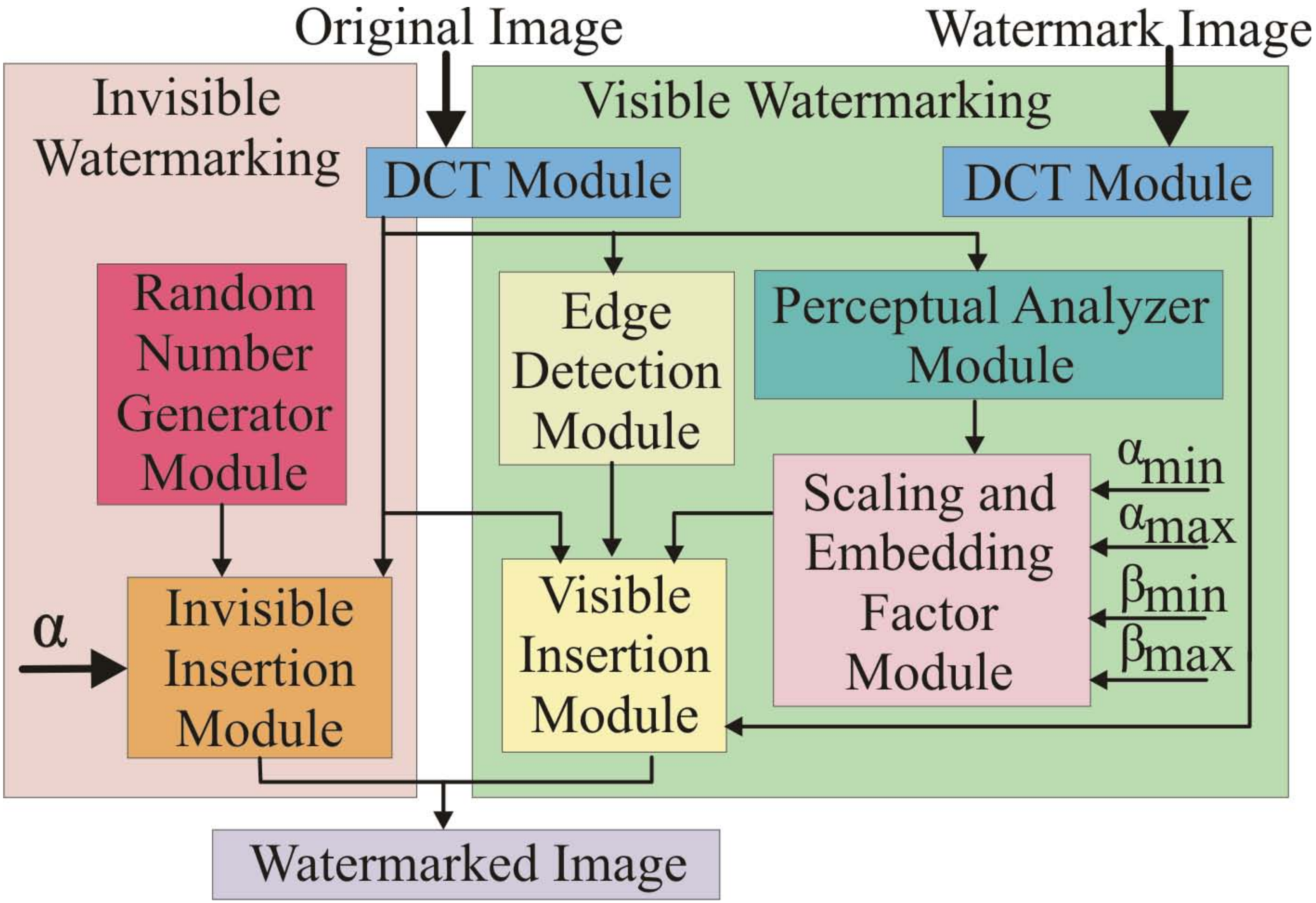
$$\beta^c{}_k = \frac{1}{\sigma_{AC_{Ik}}}\left[1 - \exp\left\{-(\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^2\right\}\right]$$

- Using Taylor series exponential is removed:

$$\alpha^c{}_k = \sigma_{AC_{Ik}}\left\{1 - (\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^2 + (\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^4\right\}$$

$$\beta^c{}_k = \frac{1}{\sigma_{AC_{Ik}}}\left\{(\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^2 - (\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^4\right\}$$

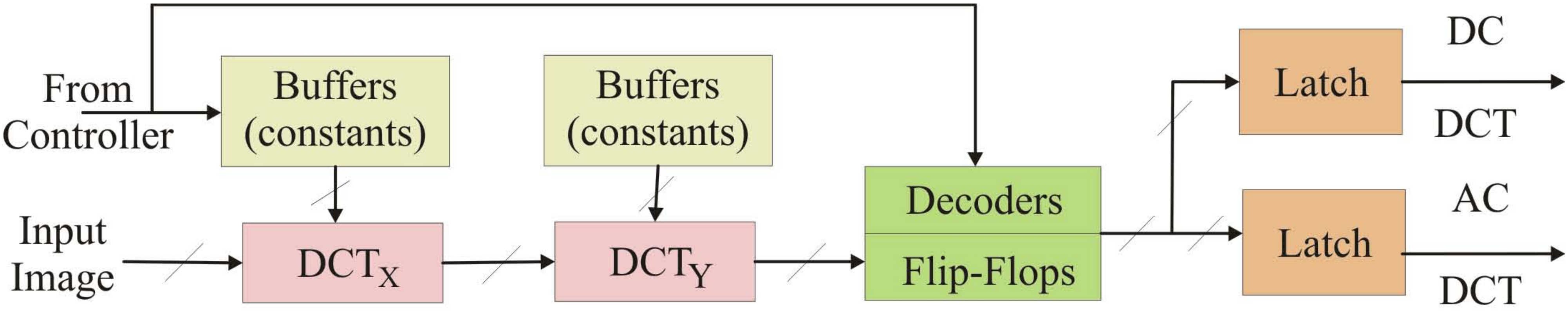
The Proposed Architecture



The Proposed Architecture (Different Modules)

- **DCT Module**: Calculates the DCT coefficients.
- **Edge Detection Module**: Determines edge blocks.
- **Perceptual Analyzer Module**: Determines perceptually significant regions using original image statistics.
- **Scaling and Embedding Factor Module**: Determines the scaling and embedding factors for visible watermark insertion.
- **Watermark Insertion Module**: Inserts the watermark
- **Random Number Generator Module**: Generates random numbers.

The Proposed Architecture (DCT Module)



DCT Module

- Computes DCT of a 4x4 block
- Both DCTX and DCTY modules have similar architectures

The Proposed Architecture (DCT Module)

DCT module implements the following equations:

$x00=((in00*c00) + (in01*c01) + (in02*c02) + (in03*c03))$

$x10=((in10*c00) + (in11*c01) + (in12*c02) + (in13*c03))$

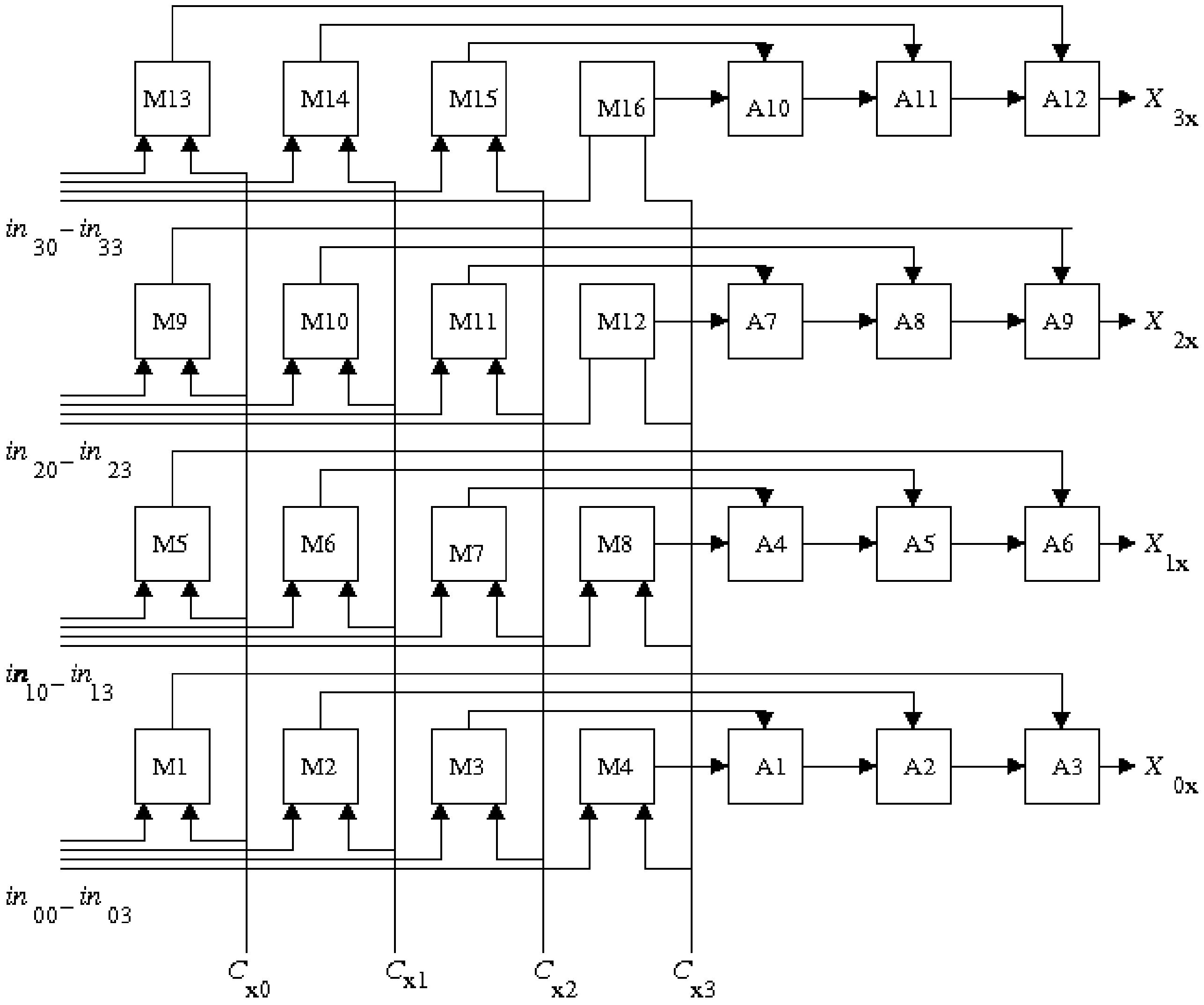
$x20=((in20*c00) + (in21*c01) + (in22*c02) + (in23*c03))$

$x30=((in30*c00) + (in31*c01) + (in32*c02) + (in33*c03))$

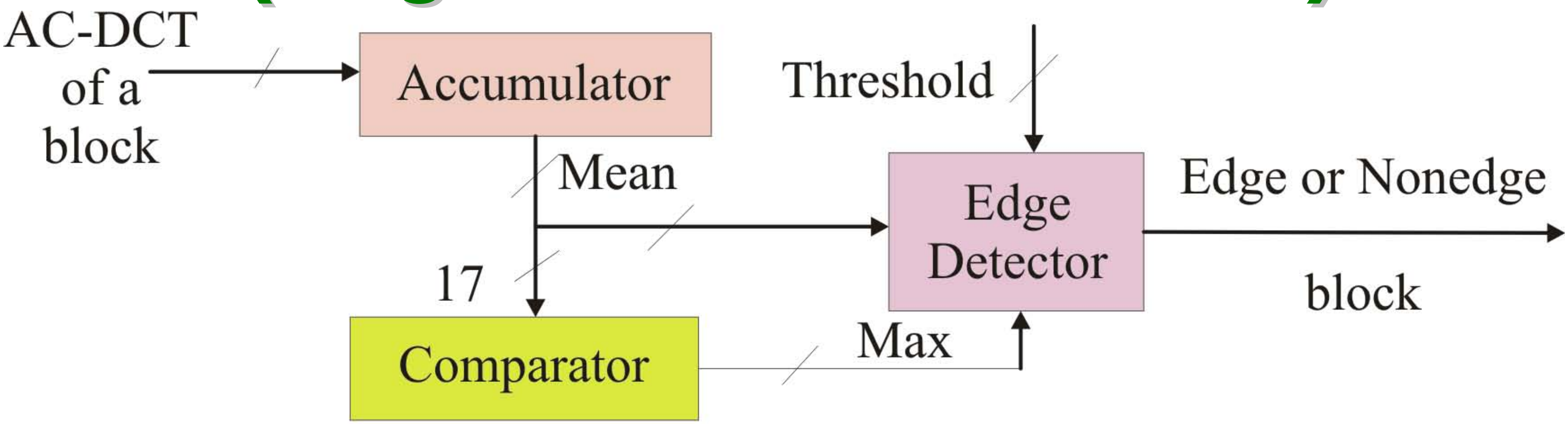
NOTE:

- in_{ij} – input, c_{ij} – constants, x_{ij} – coefficients
- 16 multiplications and 12 additions involved

The Proposed Architecture (DCT Module)



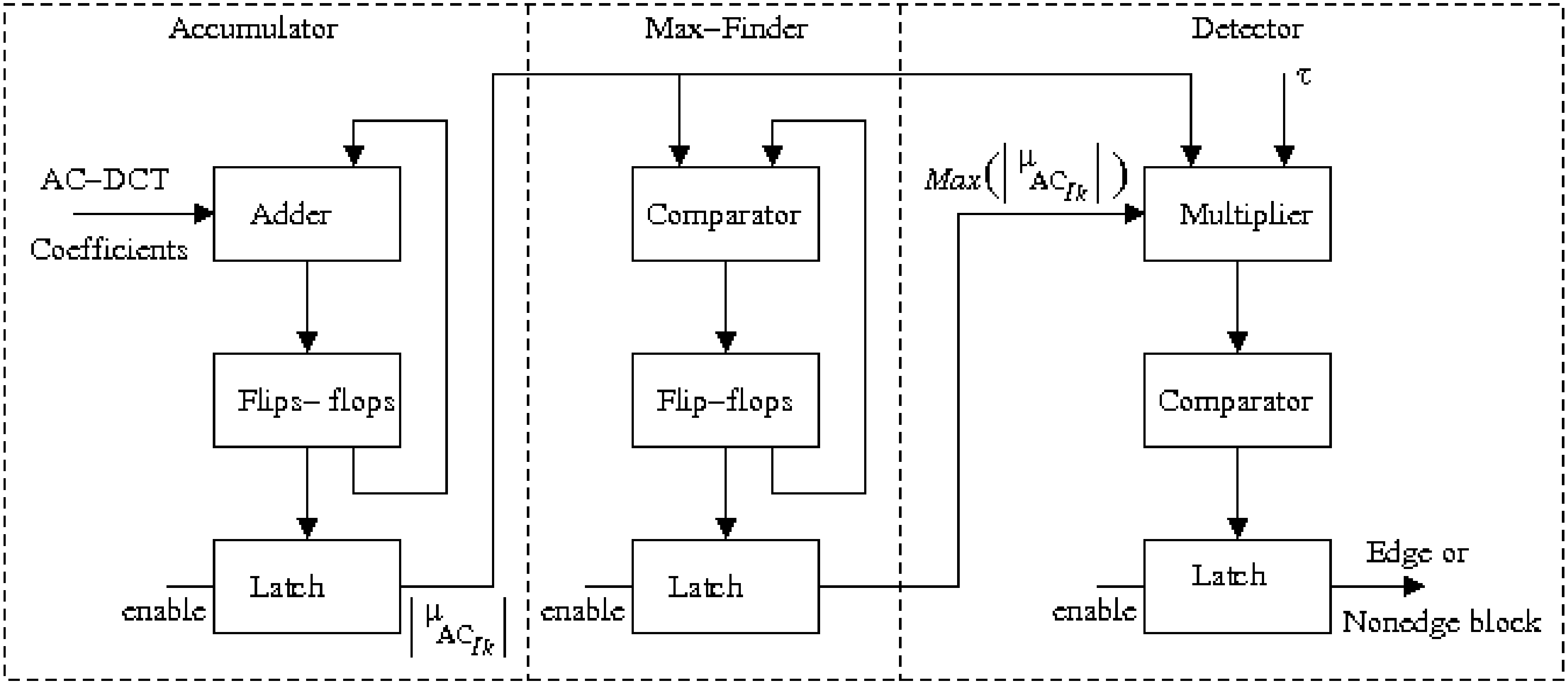
The Proposed Architecture (Edge Detection Module)



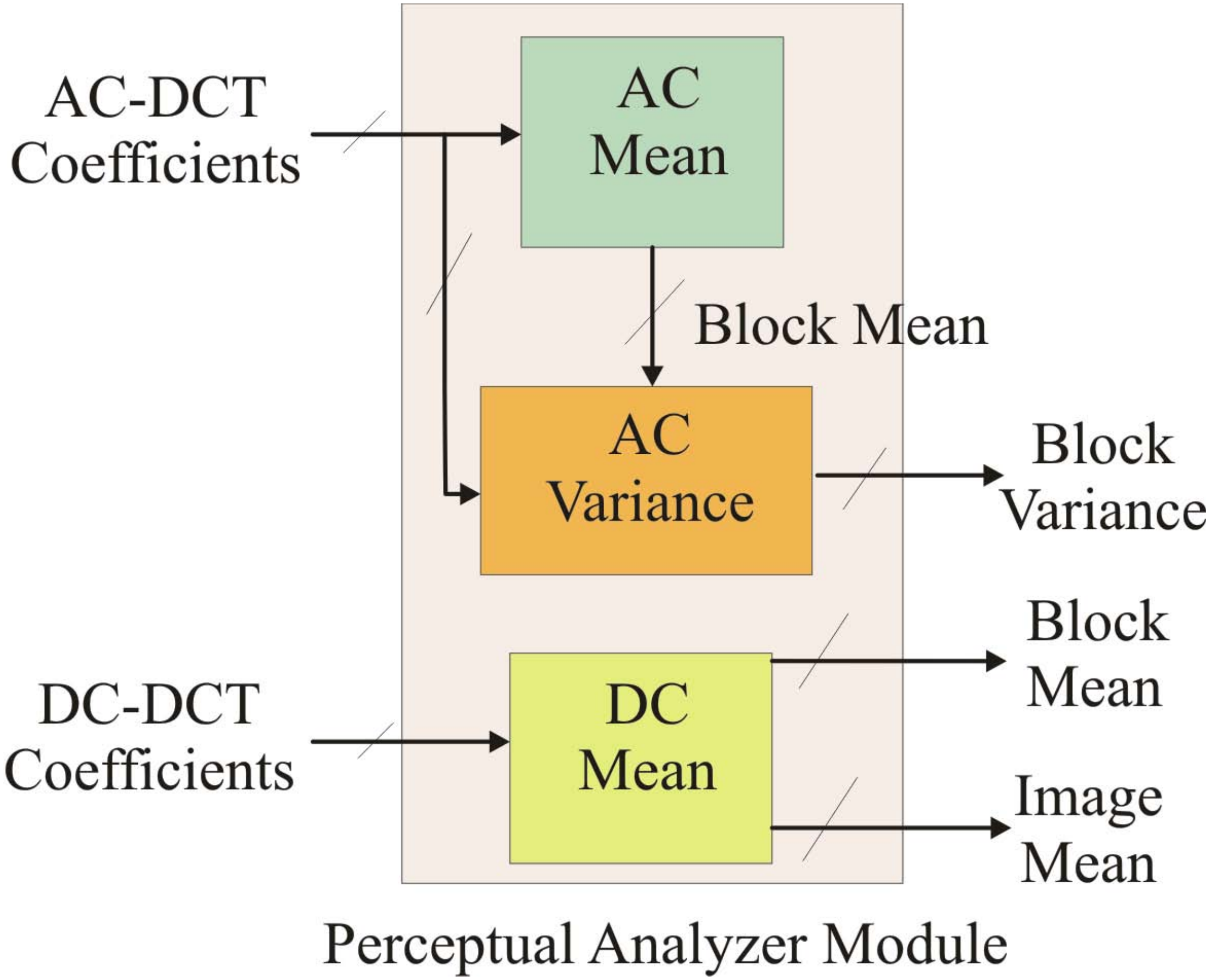
Edge Detection Module

- Compute from AC-DCT: $\mu_{AC_{Ik}} = \frac{1}{N_B * N_B} \sum_m \sum_n | c_{Ik}(m,n) |$
- Find the maximum: $| \mu_{AC_{\mathrm{Im}\ ax}} | = Max\ (| \mu_{AC_{Ik}} |)$
- Declare edge block if: $| \mu_{AC_{Ik}} | > \tau | \mu_{AC_{\mathrm{Im}\,ax}} |$

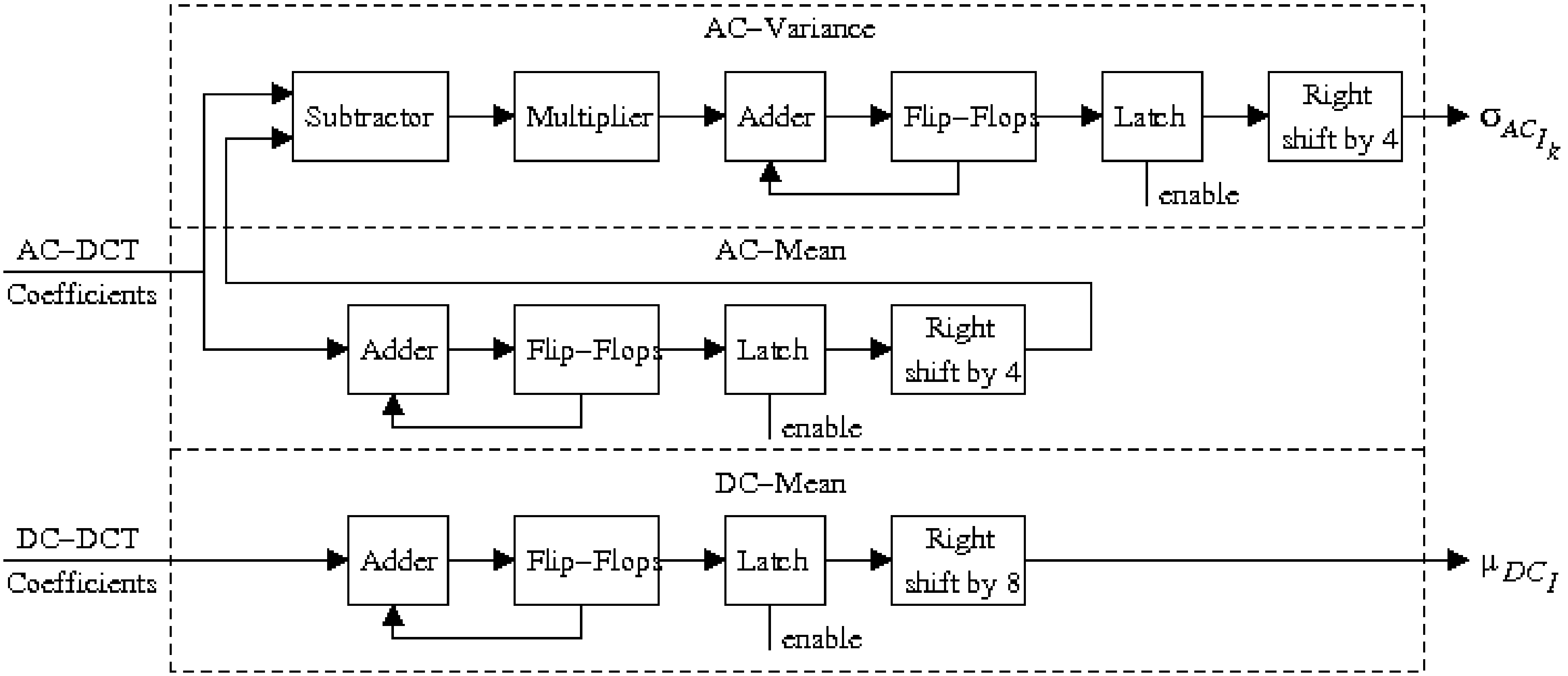
The Proposed Architecture (Edge Detection Module)



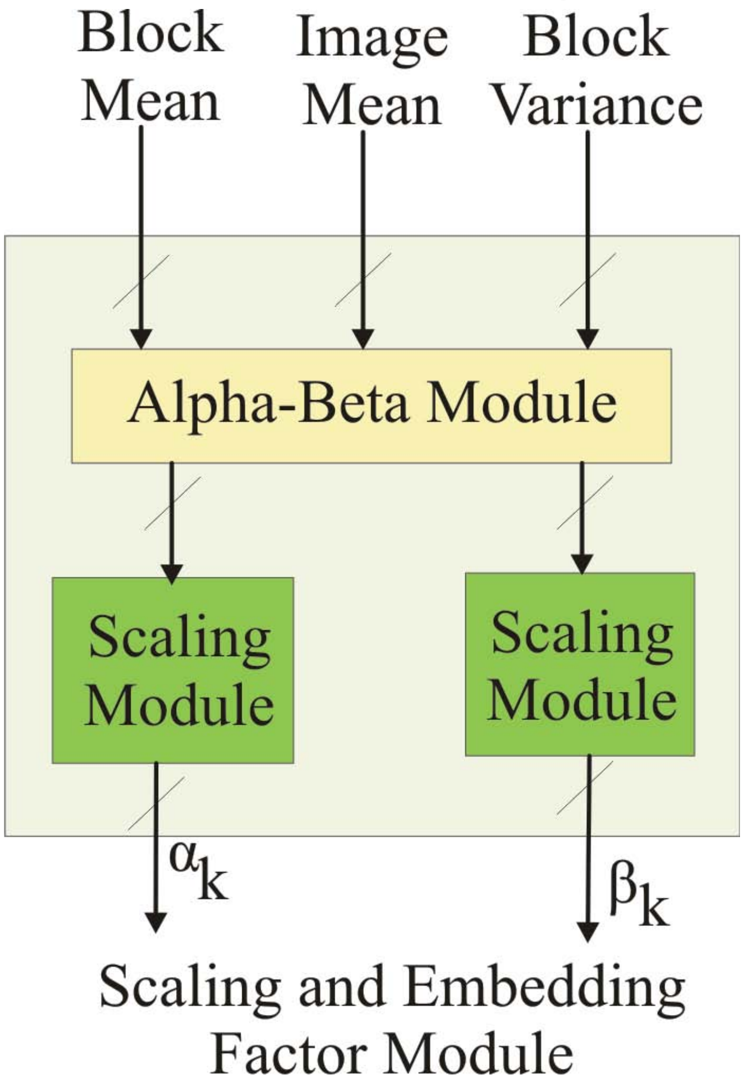
The Proposed Architecture (Perceptual Analyzer Module)



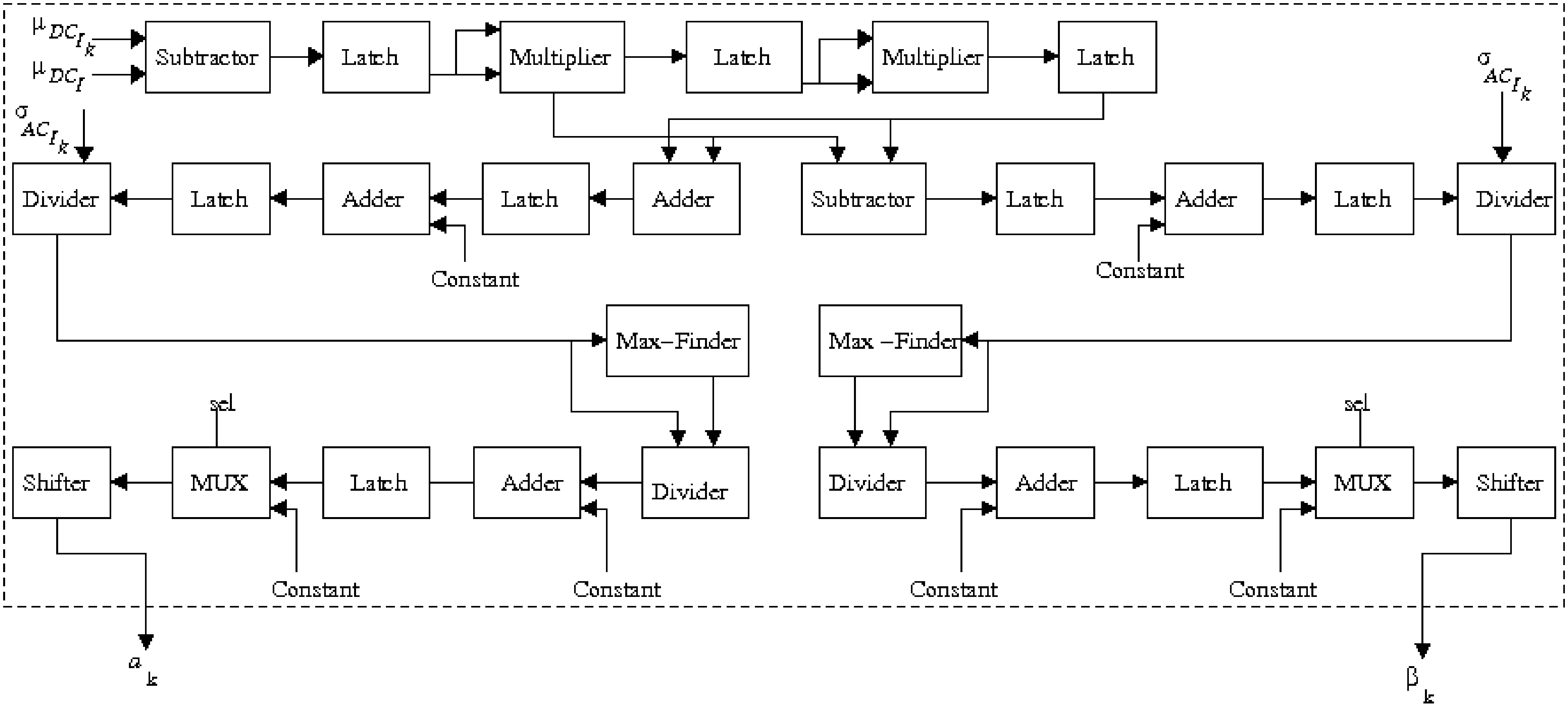
The Proposed Architecture (Perceptual Analyzer Module)



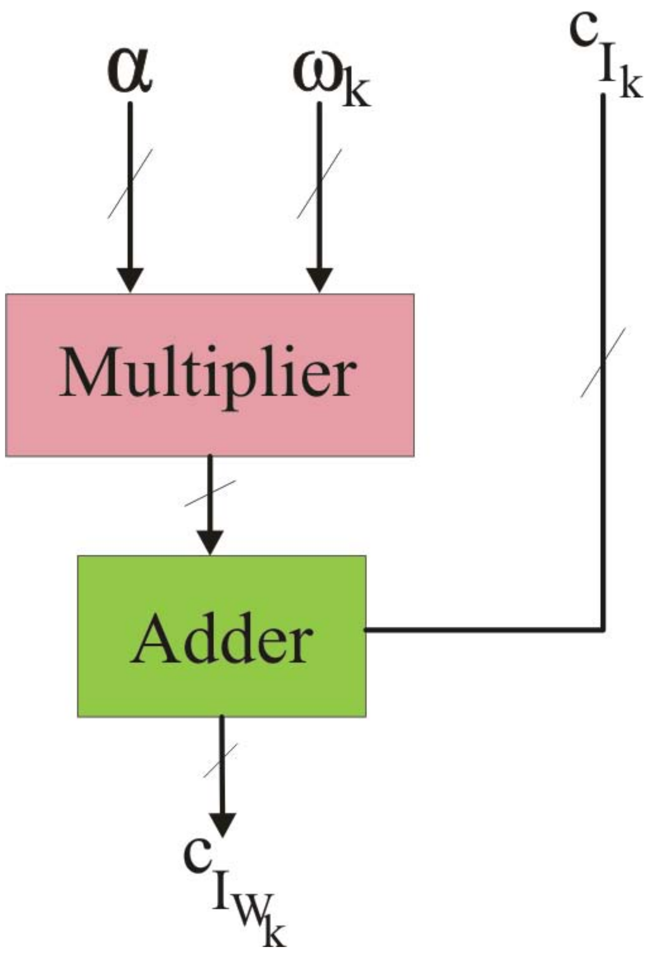
The Proposed Architecture (Scaling and Embedding Factor Module)



The Proposed Architecture (Scaling and Embedding Factor Module)



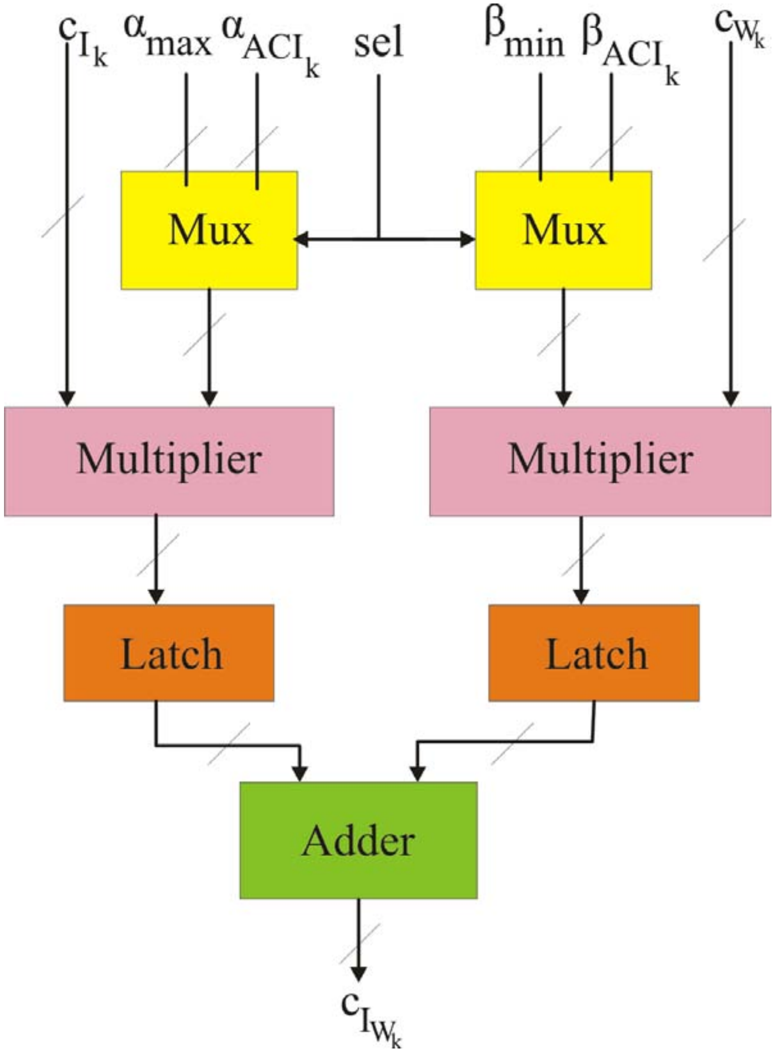
The Proposed Architecture (Invisible Insertion Module)



Invisible insertion process:

$$c_{I_{W_k}} = c_{I_k} + \alpha\omega_k$$

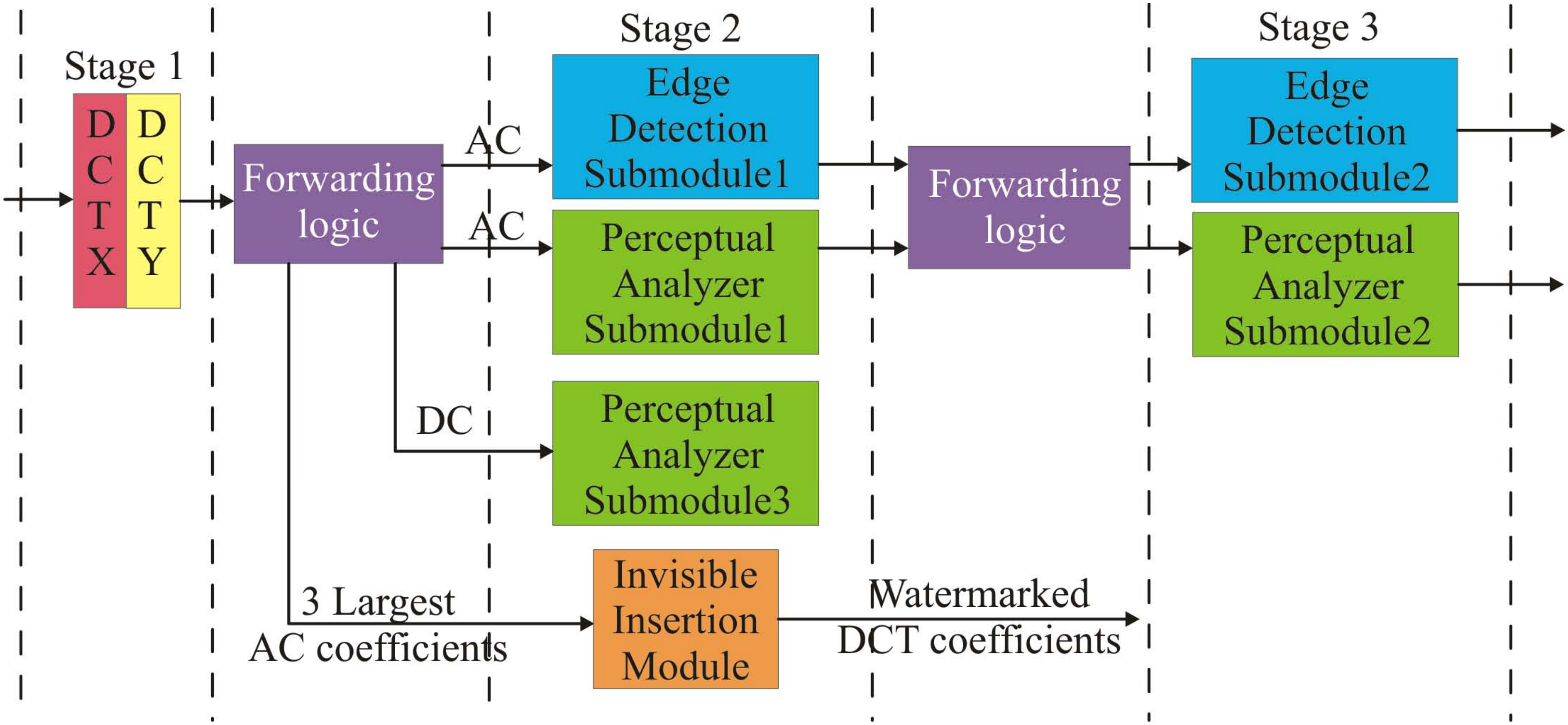
The Proposed Architecture (Visible Insertion Module)



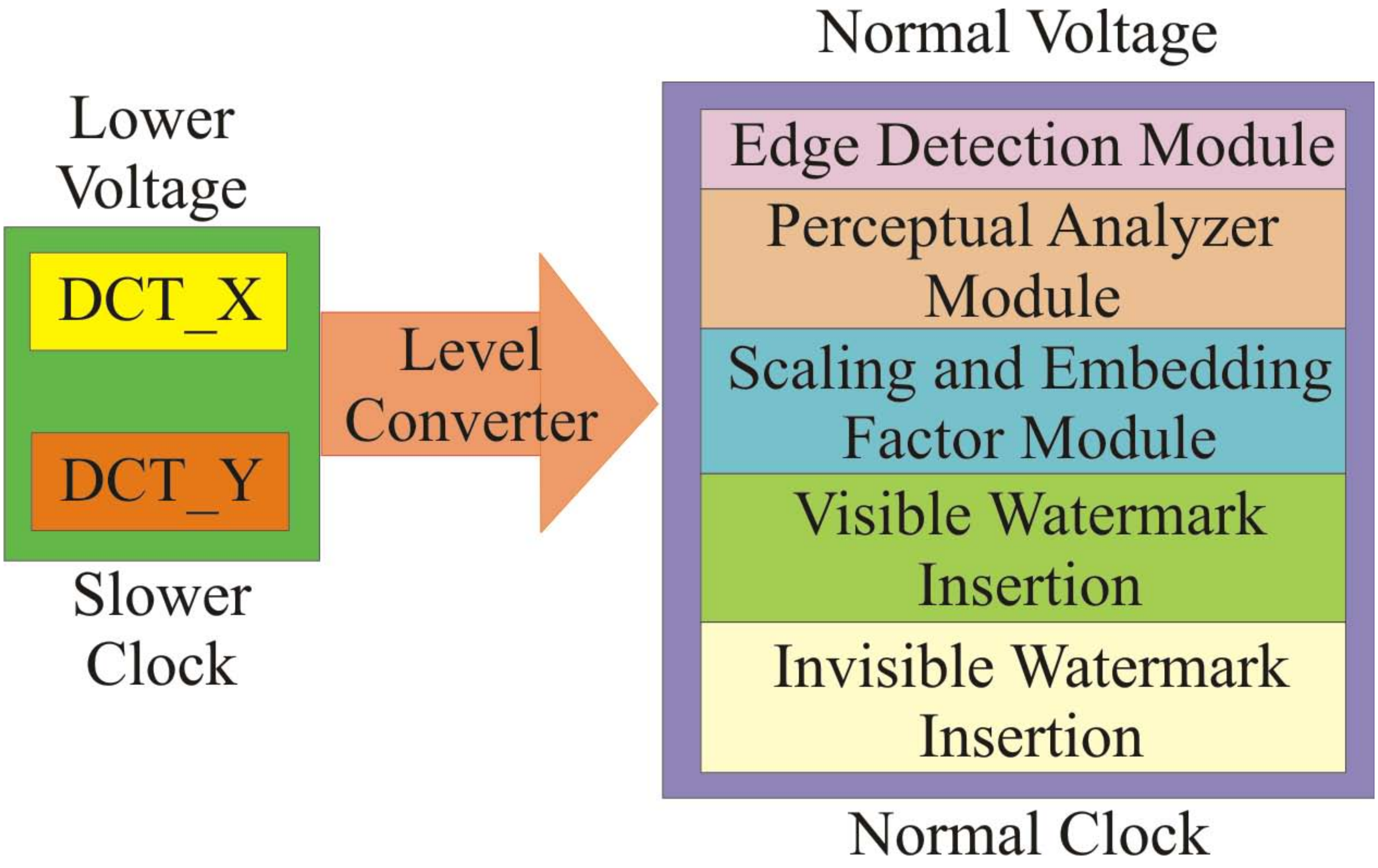
Visible insertion process:

$$c_{I_{W_k}} = \alpha_k c_{I_k} + \beta_k c_{W_k}$$

The Proposed Architecture: Pipeline and Parallelism


Stage 1
DCTX
DCTY
Forwarding logic
AC
AC
DC
3 Largest AC coefficients
Stage 2
Edge Detection Submodule1
Perceptual Analyzer Submodule1
Perceptual Analyzer Submodule3
Invisible Insertion Module
Watermarked DCT coefficients
Forwarding logic
Stage 3
Edge Detection Submodule2
Perceptual Analyzer Submodule2

The Proposed Architecture: Dual Voltage and Frequency

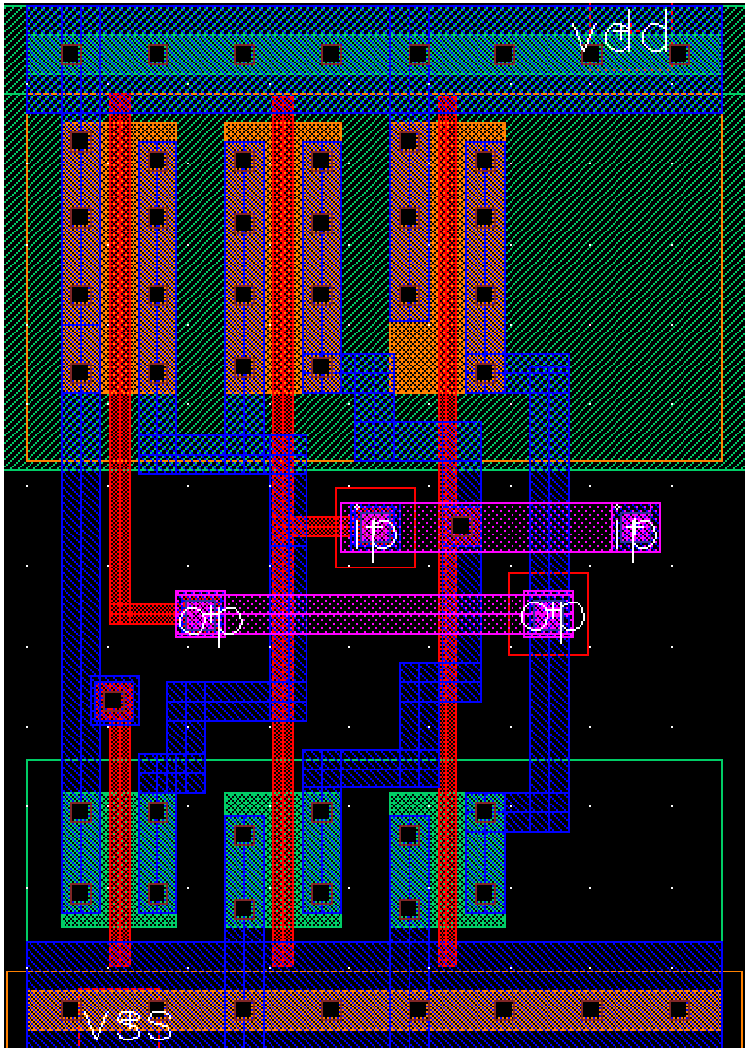

Normal Voltage
Lower Voltage
DCT_X
DCT_Y
Slower Clock
Level Converter
Edge Detection Module
Perceptual Analyzer Module
Scaling and Embedding Factor Module
Visible Watermark Insertion
Invisible Watermark Insertion
Normal Clock

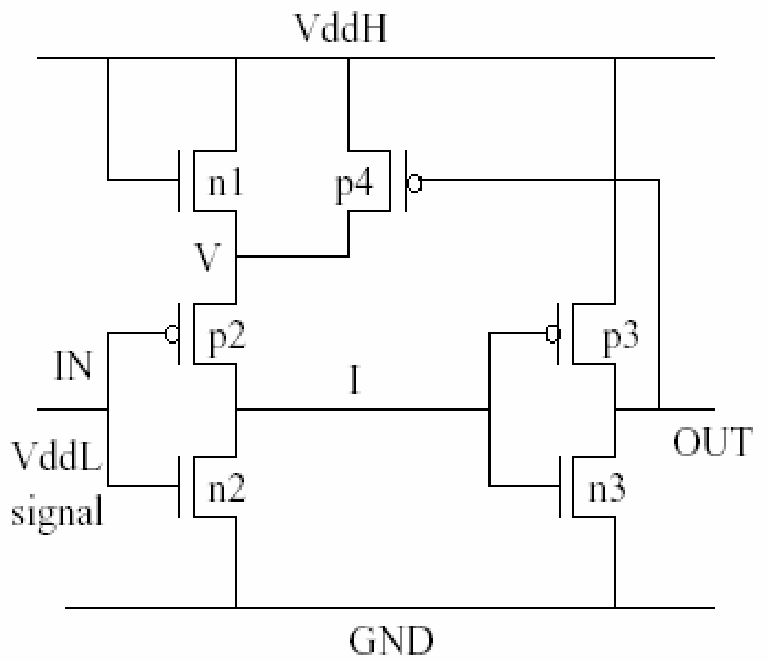
Dual Voltage: Level Converters

- Level converters required to step up the low voltage to high voltage.
- Traditional level converter: Differential Cascode Voltage Switch (DCVS).
- In this work: Single Supply Level Converters – faster, better power consumption, needs single voltage supply only.

Reference: R.Puri et. al., "Pushing ASIC performance in a power envelope" in the Proceedings of the Design Automation Conference, 2003, pp. 788-793.

Single Supply Level Converter: Key Element in our Circuit





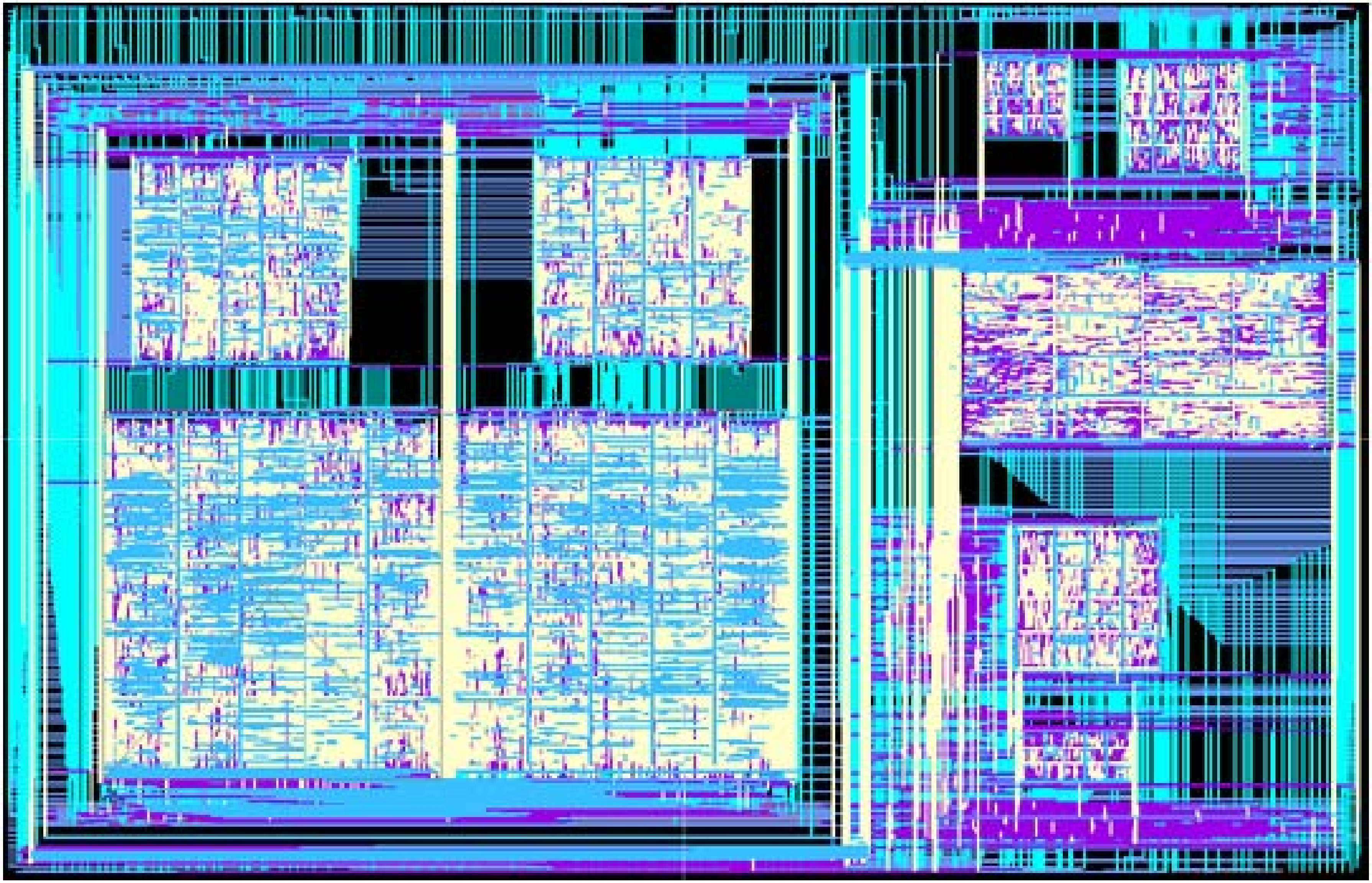
Prototype Chip Implementation

Tools used for the design

Tools used	Purpose
NC launch	VHDL simulator
Silicon Ensemble	Placement and routing
Abstract Generator	Abstract generation from layout
NCSU-Design Kit	Layout Editor
Design Analyzer	Verilog netlist generation
Nanosim	Power and delay calculations

Standard Cell Design Style adopted. Standard Cells obtained from Virginia Tech: TSMC 0.25µm.

Overall Prototype Chip: Layout



Prototype Chip: Floor Plan

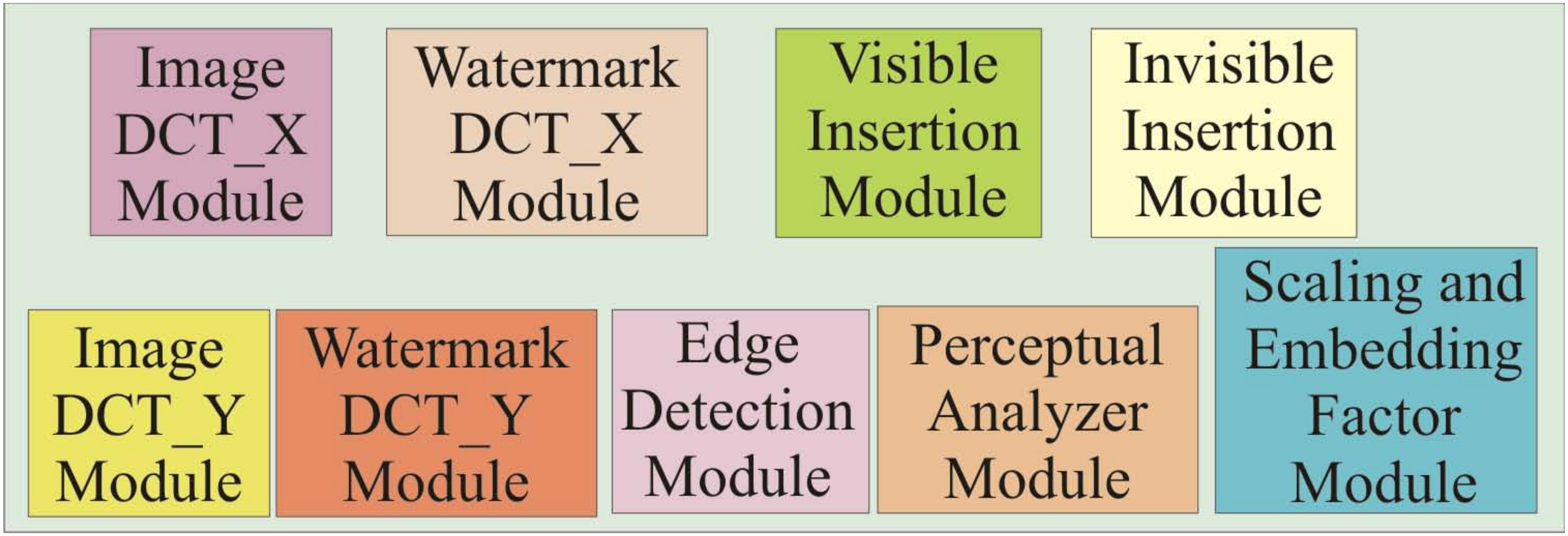


Image DCT_X Module

Watermark DCT_X Module

Visible Insertion Module

Invisible Insertion Module

Image DCT_Y Module

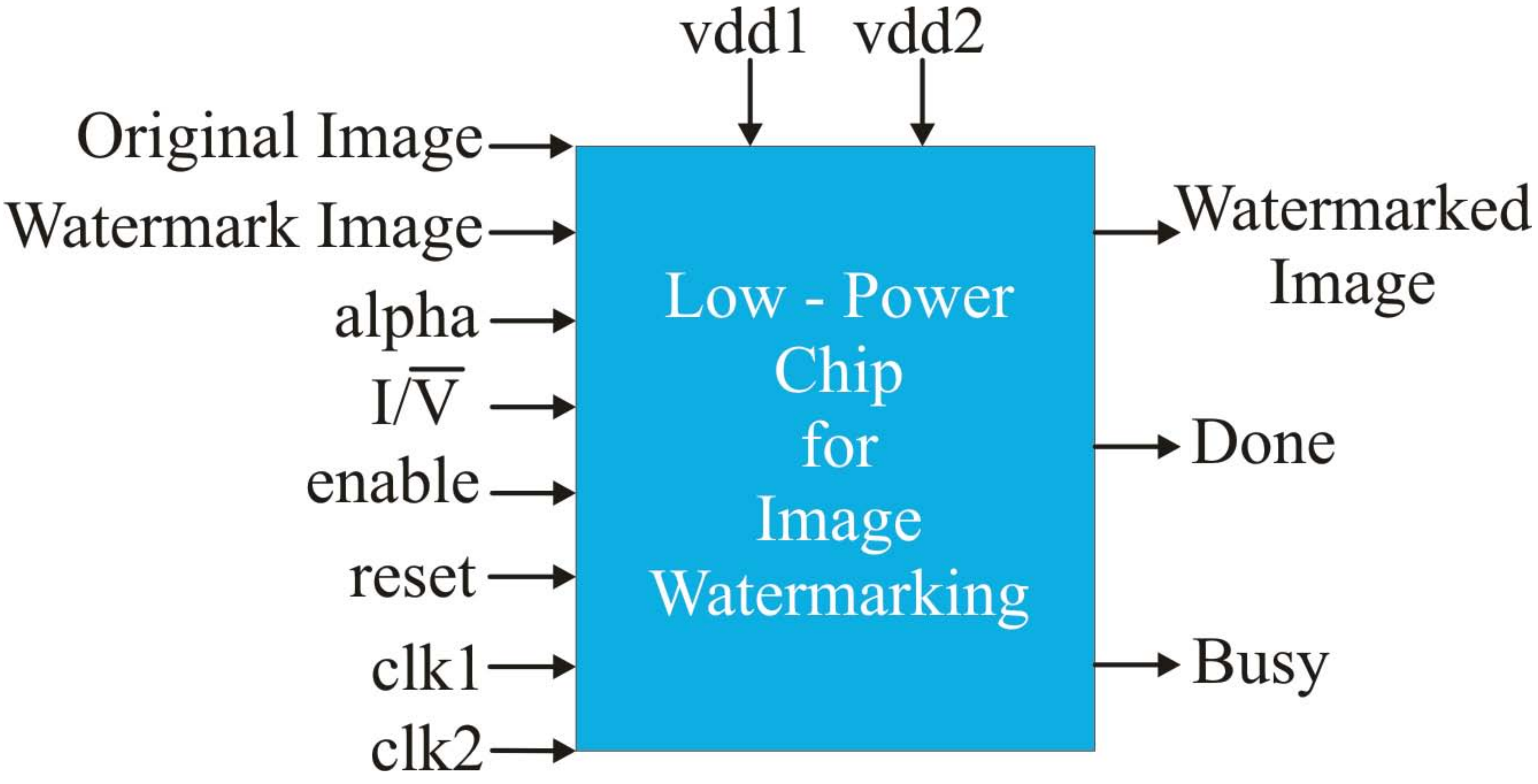
Watermark DCT_Y Module

Edge Detection Module

Perceptual Analyzer Module

Scaling and Embedding Factor Module

Prototype Chip: Pin Diagram



Prototype Chip: Statistics

Technology: TSMC 0.25µm

Total Area : 16.2 sq mm

Dual Clocks: 284MHz and 71MHz

Dual Voltages: 2.5V and 1.5V

No. of Transistors: 1.4million

Power (dual voltage and frequency): 0.3mW

Chip (single voltage and frequency): 1.9mW

NOTE: Lowest power consuming watermarking chip available at present.

Related Works (Hardware Systems/Circuits)

Work	Type	Target Object	Domain	Technology	Chip Power
Strycker, 2000	Invisible Robust	Video	Spatial	NA	NA
Tsai and Lu 2001	Invisible Robust	Video	DCT	0.35µ	62.8 mW
Mathai, 2003	Invisible Robust	Image	Wavelet	0.18µ	NA
Mohanty 2003	Robust Fragile	Image	Spatial	0.35µ	2.05 mW

Secure Digital Camera (SDC): Analog-Mixed Signal System-on-a-Chip (AMS-SoC) Design Challenges

Secure Digital Camera: Alternatives

- New CMOS sensor with DRM
- New ADC with DRM
- Independent DRM (Watermarking, Encryption, etc) processors
- New DRM (Watermarking, Encryption, etc) co-processor for DSP
- New Instruction Set Architecture for RISC to support DRM at micro architecture level

Secure Digital Camera: AMS-SoC Design Challenges

- Development of hardware amenable algorithms
- Building efficient VLSI architectures
- Hardware-software co-design for power, performance, security, area, and cost tradeoff

Secure Digital Camera: AMS-SoC Design Challenges

- Analog, Digital, Mixed-Signal VLSI design for power, performance, security, area, and cost tradeoff
- System-Level Power Management techniques for power and performance

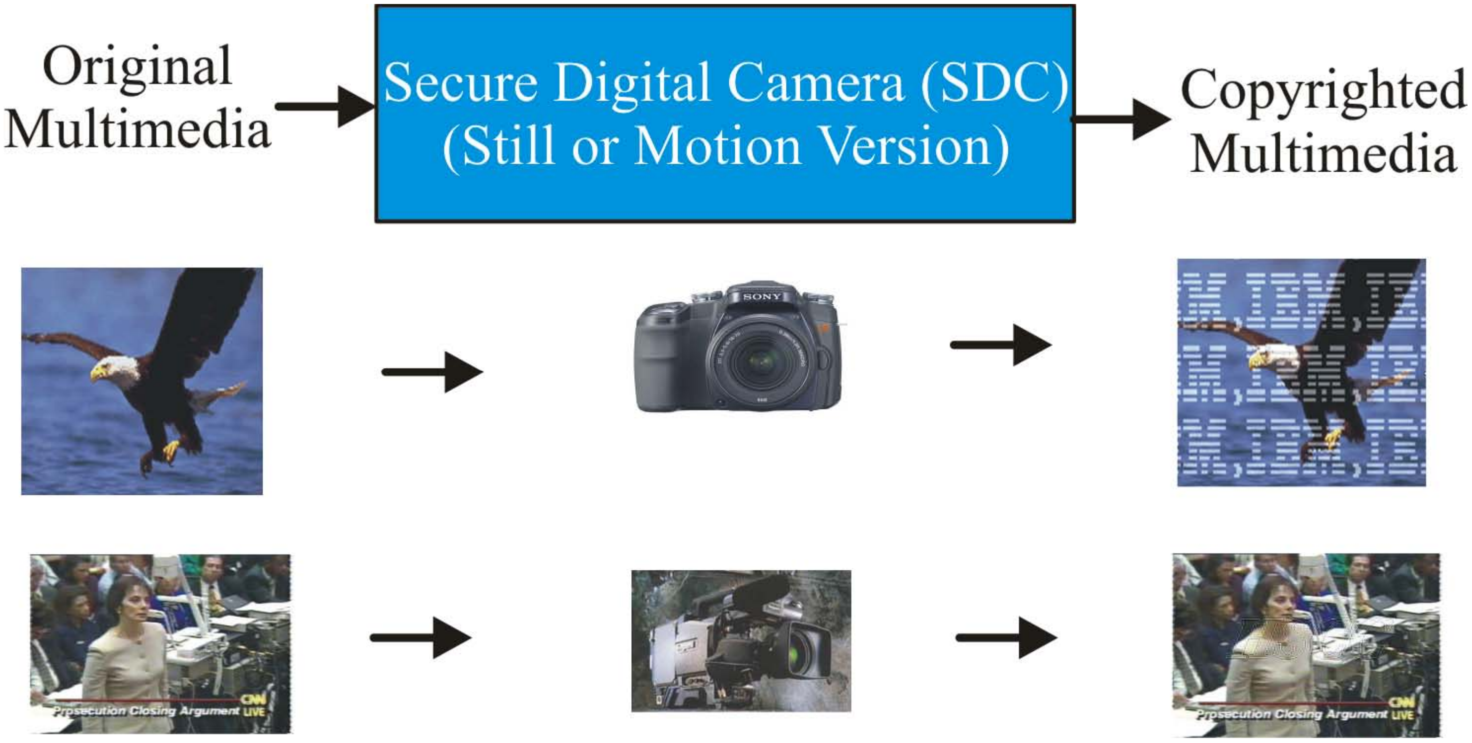
Secure Digital Camera (SDC): Application Scenario

and

Conclusions

Application: Copyright Protection

- Publicly available images
- Digital Library
- DVD Video
- Digital TV Broadcasting

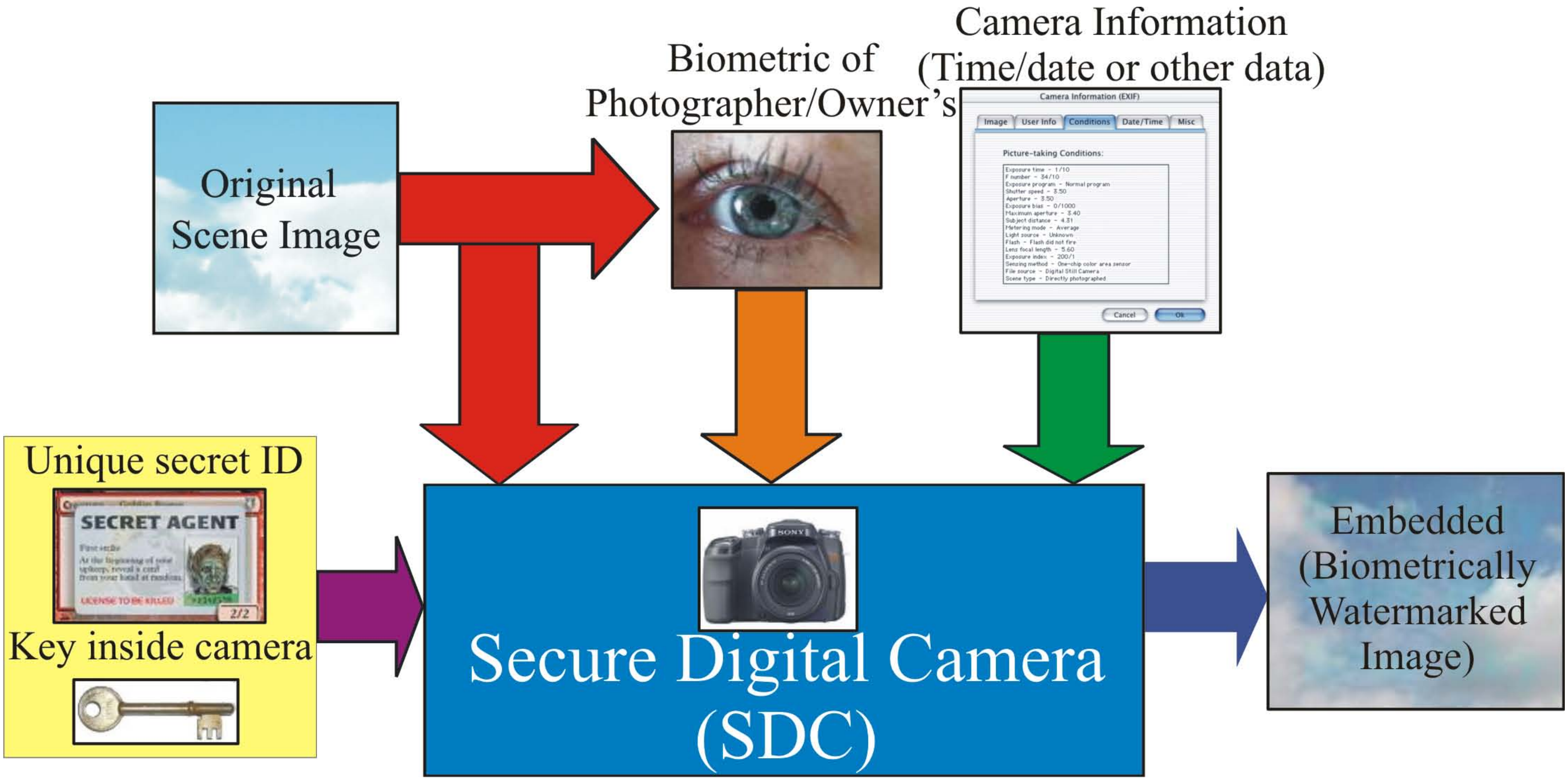


Original Multimedia

Secure Digital Camera (SDC) (Still or Motion Version)

Copyrighted Multimedia

Application: Biometric Based Authentication



Original Scene Image

Biometric of Photographer/Owner's

Camera Information (Time/date or other data)

Camera Information (EXIF)

Picture-taking Conditions:

```
Exposure time - 1/10
F number - 34/10
Exposure program - Normal program
Shutter speed - 3.50
Aperture - 3.50
Exposure bias - 0/1000
Maximum aperture - 3.40
Subject distance - 4.31
Metering mode - Average
Light source - Unknown
Flash - Flash did not fire
Lens focal length - 5.60
Exposure index - 200/1
Sensing method - One-chip color area sensor
File source - Digital Still Camera
Scene type - Directly photographed
```

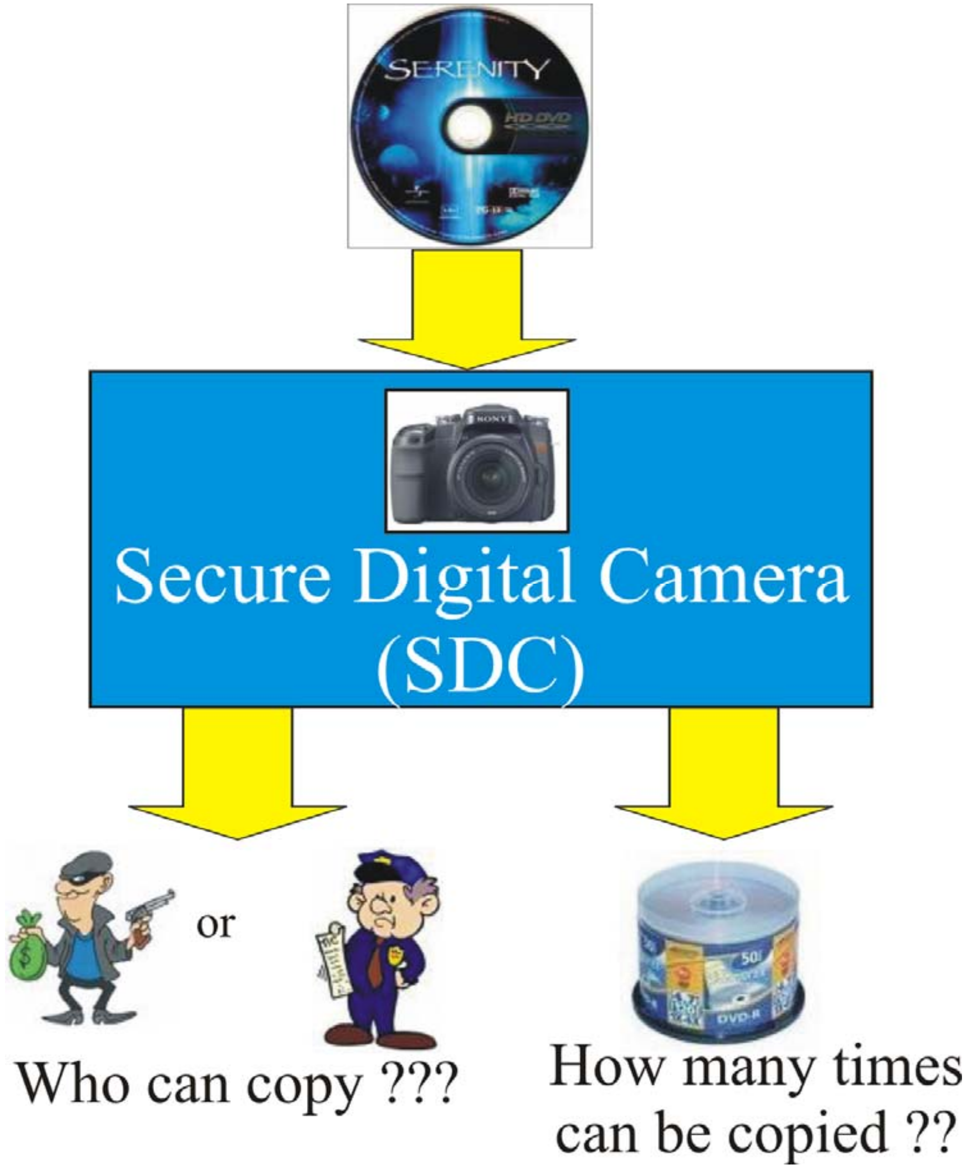
Unique secret ID

Key inside camera

Secure Digital Camera (SDC)

Embedded (Biometrically Watermarked Image)

Application: Usage Control



Secure Digital Camera (SDC)

or

Who can copy ???

How many times can be copied ??

Summary Conclusion

- A low-cost low-power camera introduced that can perform DRM in real time.
- Hardware assisted DRM has several advantages over software only.
- Structure of SoC that will realize such Digital Camera is an ongoing research.
- A low-power watermarking chip is designed that consumes 0.3mW power.

References

- **S. P. Mohanty**, et al., "VLSI Architecture of an Invisible Watermarking Unit for a Biometric-Based Security System in a Digital Camera", in *Proceedings of the 25th IEEE International Conference on Consumer Electronics (ICCE)*, pp. in press, 2007.
- O. B. Adamo, **S. P. Mohanty**, E. Kougianos, and M. Varanasi, “VLSI Architecture for Encryption and Watermarking Units Towards the Making of a Secure Digital Camera”, in *Proceedings of the IEEE International SOC Conference (SOCC)*, pp. in press, 2006.
- **S. P. Mohanty**, et al., “A Dual Voltage-Frequency VLSI Chip for Image Watermarking in DCT Domain”, *IEEE Transactions on Circuits and Systems II (TCAS-II)*, Vol. 53, No. 5, May 2006, pp. 394-398.
- N. M. Kosaraju, M. Varanasi, and **S. P. Mohanty**, “A High-Performance VLSI Architecture for Advanced Encryption Standard (AES) Algorithm”, in *Proceedings of the 19th IEEE International Conference on VLSI Design (VLSID)*, pp. 481-484, 2006.

References

- **S. P. Mohanty**, et al., “A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S^2DC) Design”, *IEEE Transactions on VLSI Systems (TVLSI)*, Vol. 13, No. 8, Aug 2005, pp. 1002-1012.
- G. R. Nelson, et al., “CMOS Image Sensor with Watermarking Capabilities”, in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, 2005, pp. 5326-5329.
- P. Blythe and J. Fridrich, “Secure Digital Camera,” in *Proceedings of Digital Forensic Research Workshop (DFRWS)*, 2004.
- **S. P. Mohanty**, N. Ranganathan, and R. K. Namballa, “VLSI Implementation of Invisible Digital Watermarking Algorithms Towards the Development of a Secure JPEG Encoder”, *Proceedings of the IEEE Workshop on Signal Processing System*, pp. 183-188, 2003.
- http://www.iprsystems.com, http://www.eifonline.org, http://www.trl.ibm.com/projects/RightsManagement/datahiding/index_e.htm,http://www.ctr.columbia.edu/~cylin/vismark/vismark.html, and more web sites ….

UNIVERSITY OF NORTH TEXAS™

Thank You

For more information:

http://www.cse.unt.edu/~smohanty