A Secure Digital Camera (SDC) for Real-Time Security and Copyright Protection of Multimedia

Saraju P. Mohanty

Dept. of Computer Science and Engineering

University of North Texas.

Email: smohanty@cse.unt.edu

Outline of the Talk

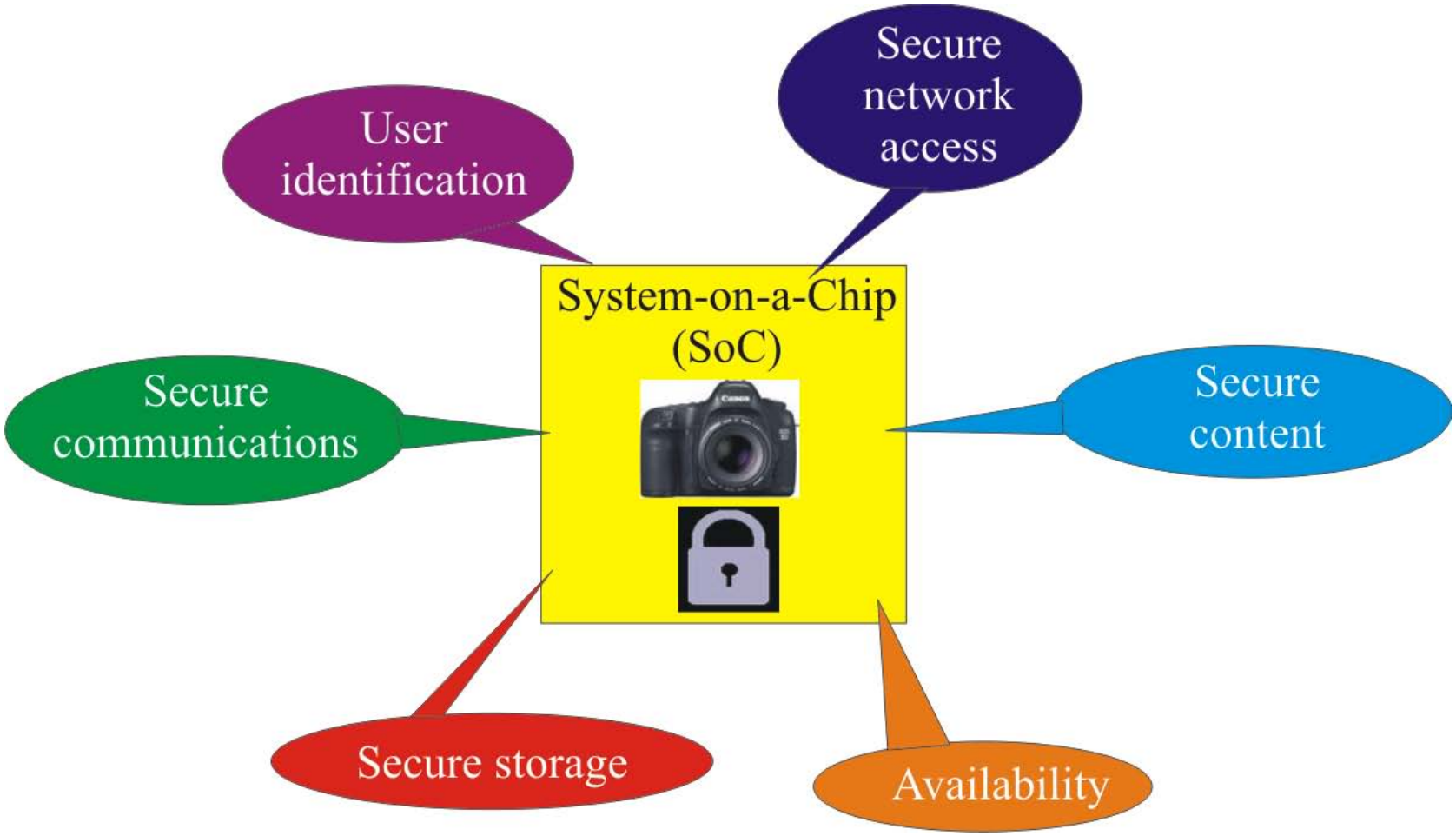
- Digital Rights Management (DRM).
- Our Proposed Secure Digital Camera (SDC) for real-time DRM.
- Our Low-Power Watermarking Chip for the SDC.
- Research Challenges for Security, Power (Battery), and Performance Tradeoffs.
- Application Scenarios for the SDC.

Digital Rights Management (DRM)

Mobile Electronic Appliances

- Access, store, and process multimedia data.
- Consume power (energy).
- Embedded systems designed as System-on-Chips (SoCs).

Security Requirements in SoCs :
The Big Picture



- Content security is of our interest which will be handled through digital rights management (DRM) facility.

DRM : Definition

- Digital Rights Management (DRM) is a generic term that refers to any of several technologies used by publishers, creators, or owners to control (restrict) access and usage of digital data.

- Typically a DRM system:
  - Protects intellectual property by encrypting the data so that it can only be accessed by authorized users.

    and/or
  - Marks the content with a digital watermark so that the content can not be freely distributed.

DRM : Associated Techniques

- Watermarking / Steganography: Embed additional data into a multimedia object visibly or invisibly.
- Cryptography / Scrambling / Hashing: Transform multimedia data from plain form to another form using various functions.
- … and many more … techniques.

DRM : Examples

Watermarking

Cryptography

- Judicious use of both encryption and watermarking necessary for multilayer protection through DRM.

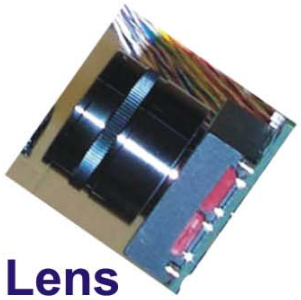
Our Solution for DRM: Secure Digital Camera (SDC)

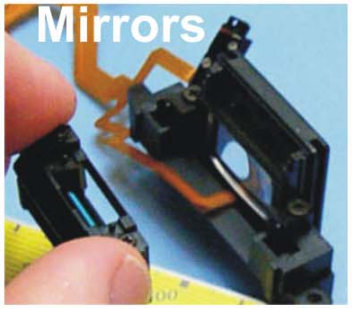
Secure Digital Camera

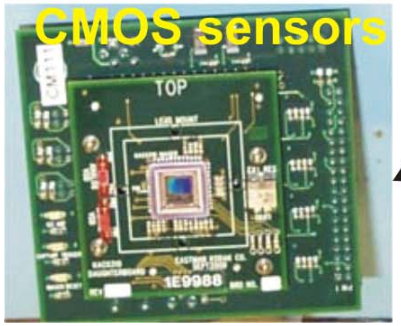
- An apparatus (system-on-a-chip, SoC) with standards features of digital camera and built in facility for real-time, low-cost, low-power DRM.

- For a given image/video SDC needs to prove:
  - Copyright (visible watermarking)
  - Extent of tampering (invisible-fragile watermarking)
  - Source of image i.e. camera information, place, or date (invisible-robust or visible watermarking)
  - Owner's, Creator's, or Cameraman's information (invisible-robust or visible watermarking)
  - …….. and more.

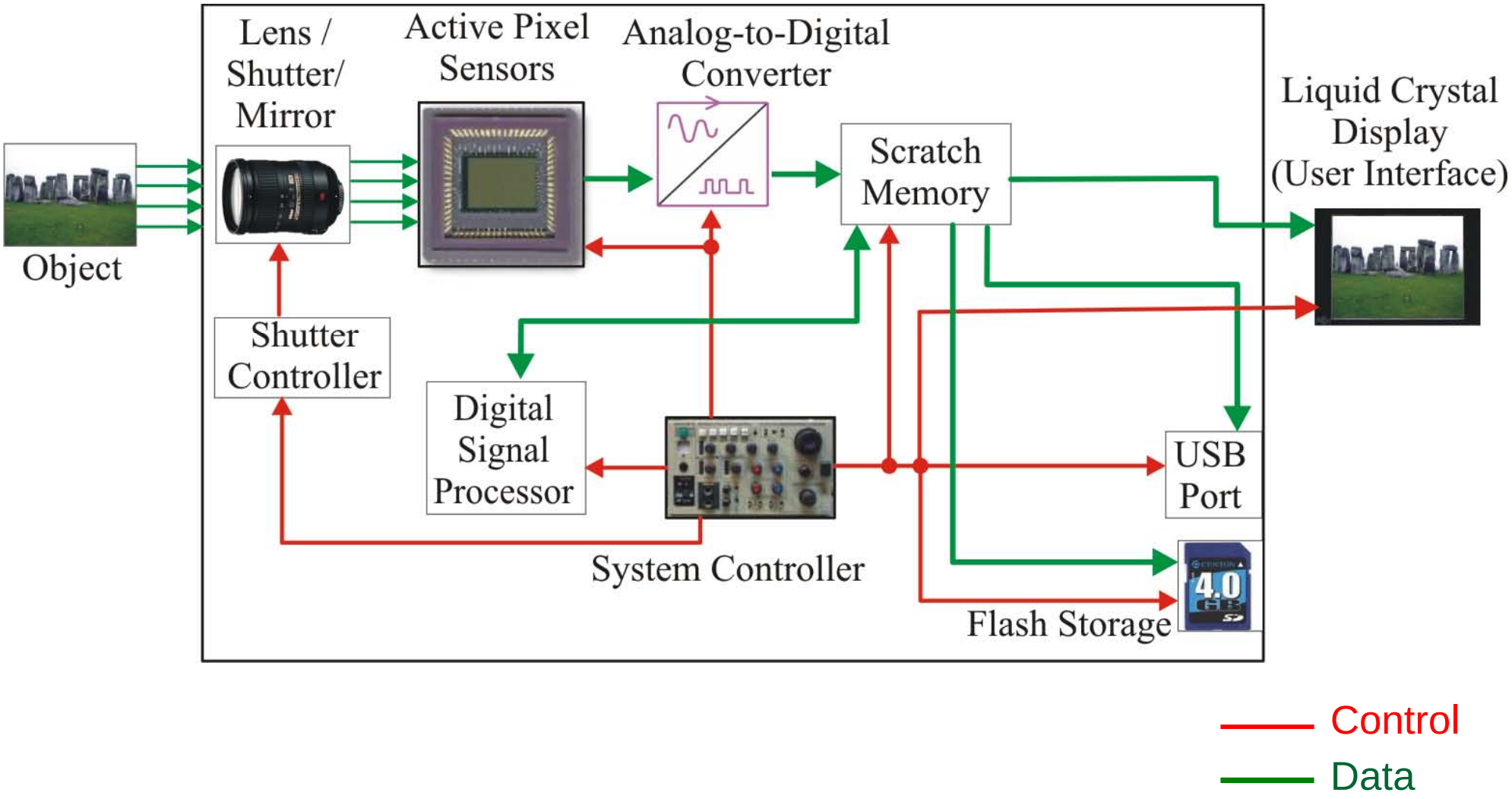
Digital Camera : Internals



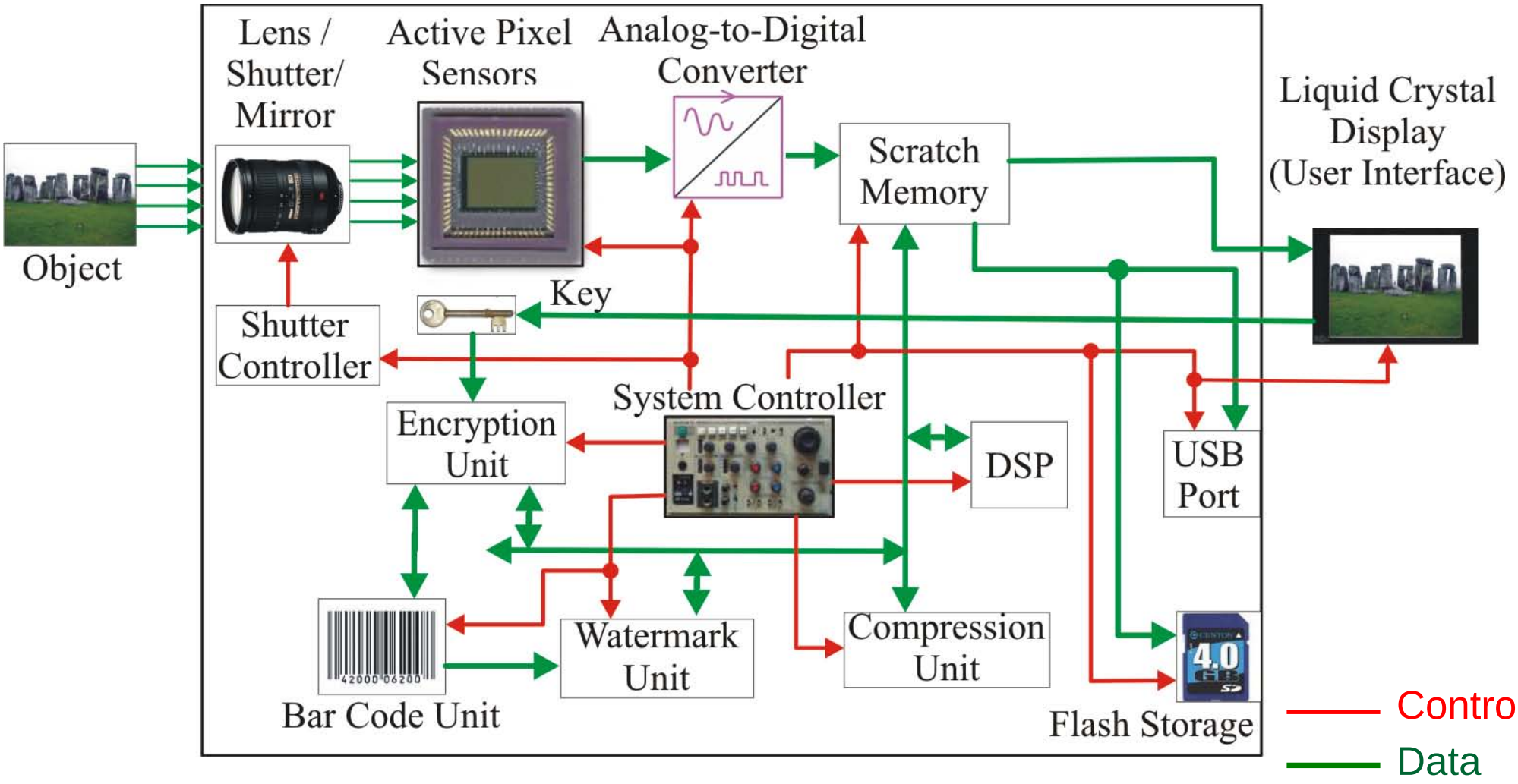




Digital Camera : Typical System



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



Hardware Based DRM : Advantages

- Easy integration with multimedia hardware, such as digital camera, camcorder, network processor, GPU, etc.
- Low-power consumption compared to software.
- High-performance compared to software.
- Higher reliability and availability compared to software.
- More useful for real-time applications like digital video broadcasting.
- Low-cost compared to having explicit software.
- DRM right at the source end will ensure that the information is always protected.
- DRM integrated with multimedia producing appliance will be more acceptable as legal evidence.

Existing Digital Cameras with Watermarking Capability

Epson PhotoPC 3000Z:

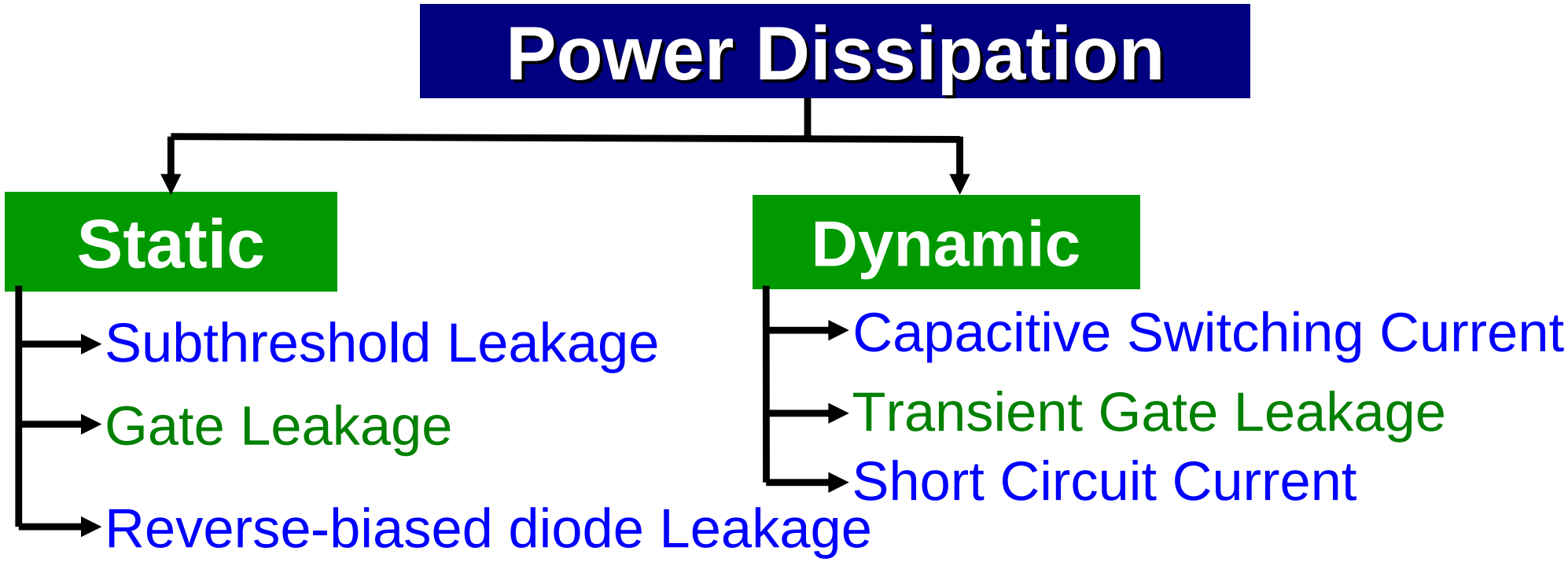
- Watermarking is invisible.
- Requires optional watermarking offline software for embedding and viewing of watermark.

Kodak DC-290:

- Watermarking is visible.
- Watermarking capabilities built into camera.

A Low-Power Watermarking Chip for the SDC

Power Dissipation in Nano-CMOS Based Systems



- Almost the entire consumer electronic industry today is driven by nano-CMOS technology.
- Their low-power design is necessary to: reduce energy and cooling costs, to increase battery life, and more.

Our Low-Power Design Approach

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

NOTE: We also have developed methods for gate oxide and subthreshold leakage power reduction.

Highlights of our Proposed Chip

- DCT domain processing.
- First to insert both visible and invisible watermarks.
- First low-power design for watermarking using dual voltage and dual frequency.
- Uses pipelined and parallelization for better performance.
- Uses decentralized controller scheme to indirectly implement clock gating for power reduction.

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, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions on Image Processing*, Vol. 6, No. 12, 1997, pp. 1673-1687.

NOTE: Highest cited papers in respective category.

Invisible Watermarking Algorithm : Original Version

- DCT of the entire original image is computed assuming it as one block.
- Perceptually significant regions of the image are selected as the 1000 largest AC 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:

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

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 3 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. Determine the blocks containing edges in the original image.
4. Find the local and global statistics (μ, σ) of original image using DC-DCT and AC-DCT coefficients.
5. Calculate the scaling and embedding factors.
6. 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:

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

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

- α_k and β_k are then scaled to the ranges (α_{min}, α_{max}) and (β_{min} , β_{max}), respectively.

Visible Watermarking Algorithm : Modifications

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

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

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

- Remove σ_{ACImax}:

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

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

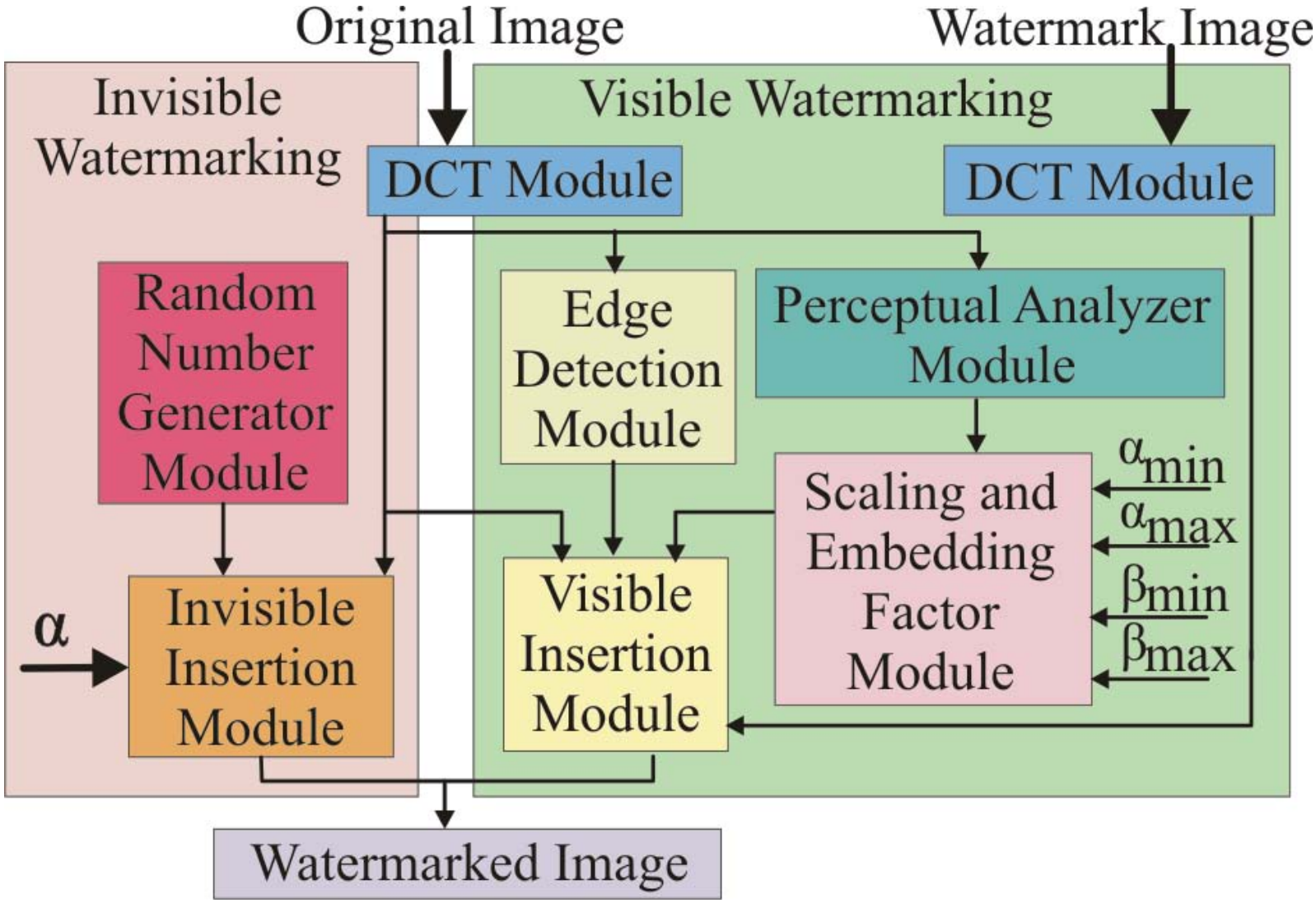
- Remove exponential using Taylor series:

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

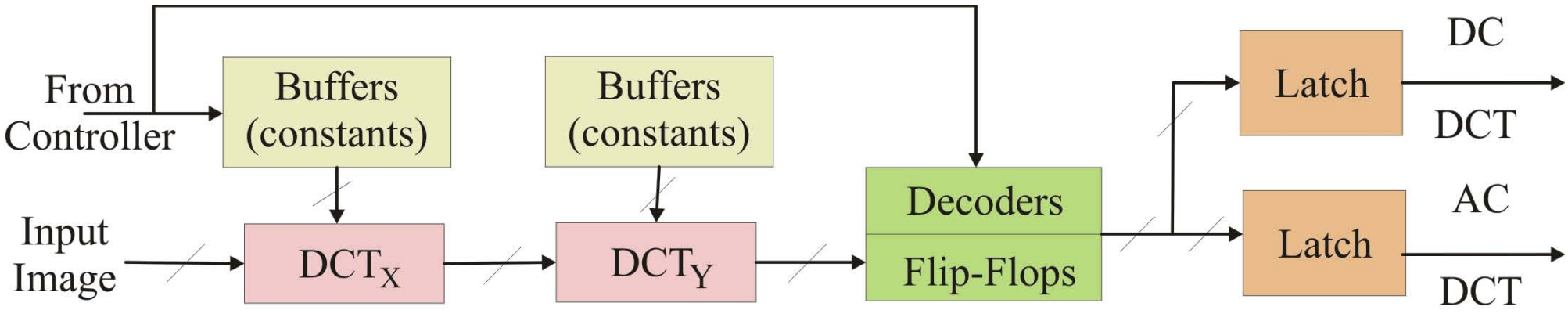
$$\beta^c{}_k = \frac{1}{\sigma_{AC_{Ik}}}\left\{(\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^2 - (\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^4\right\}$$

- Scale to the ranges $(\alpha_{min}, \alpha_{max})$ and $(\beta_{min}, \beta_{max})$, respectively.

The Proposed Architecture



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))

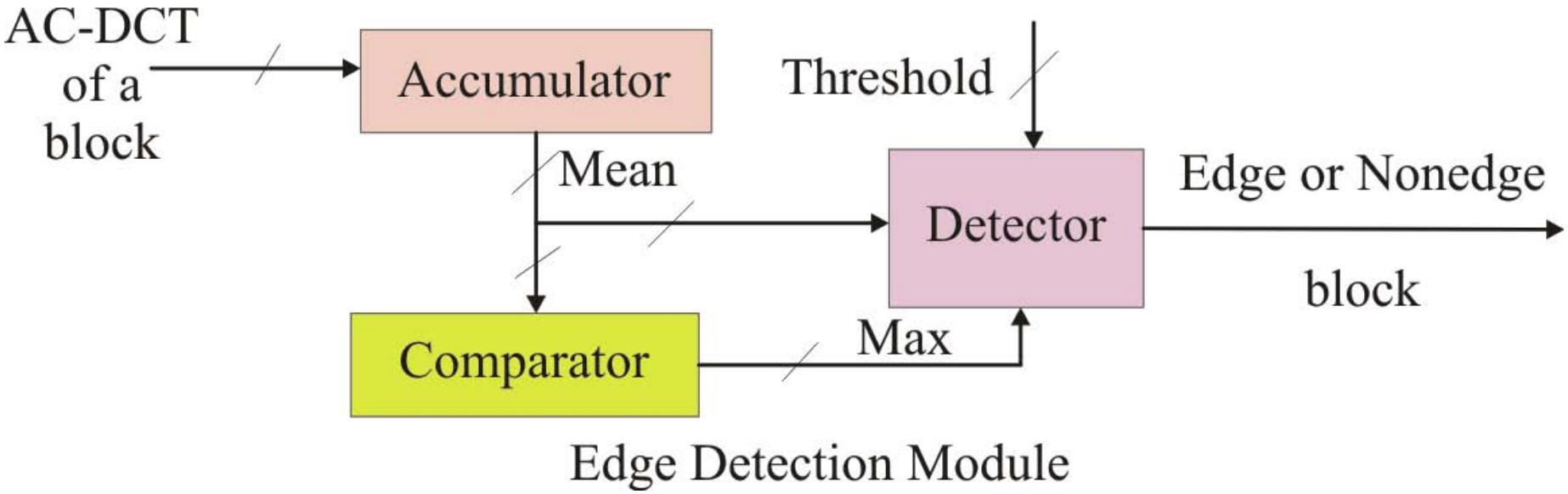
x20=((in20*c00) + (in21*c01) + (in22*c02) + (in23*c03))

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

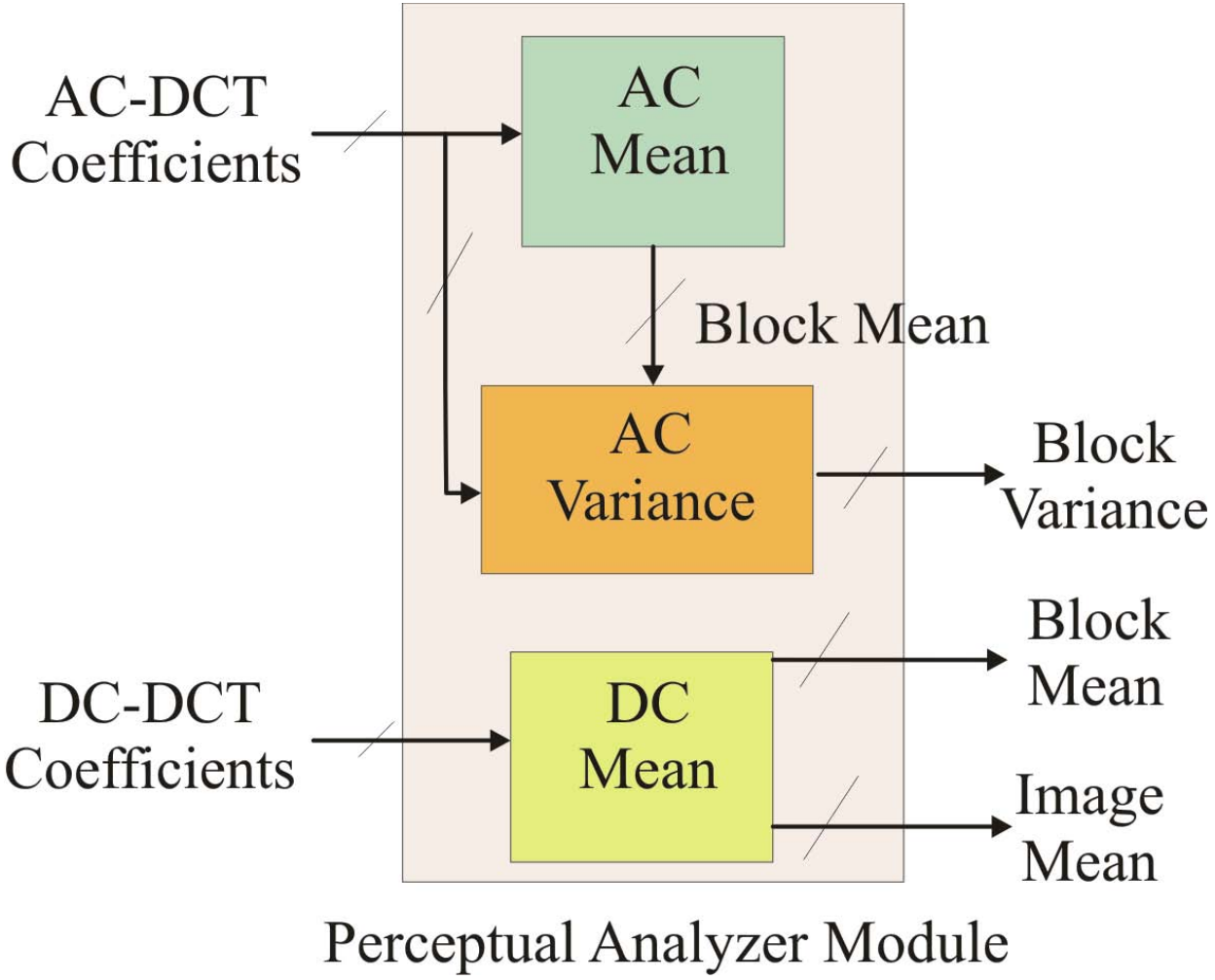
The Proposed Architecture … (Edge Detection Module)



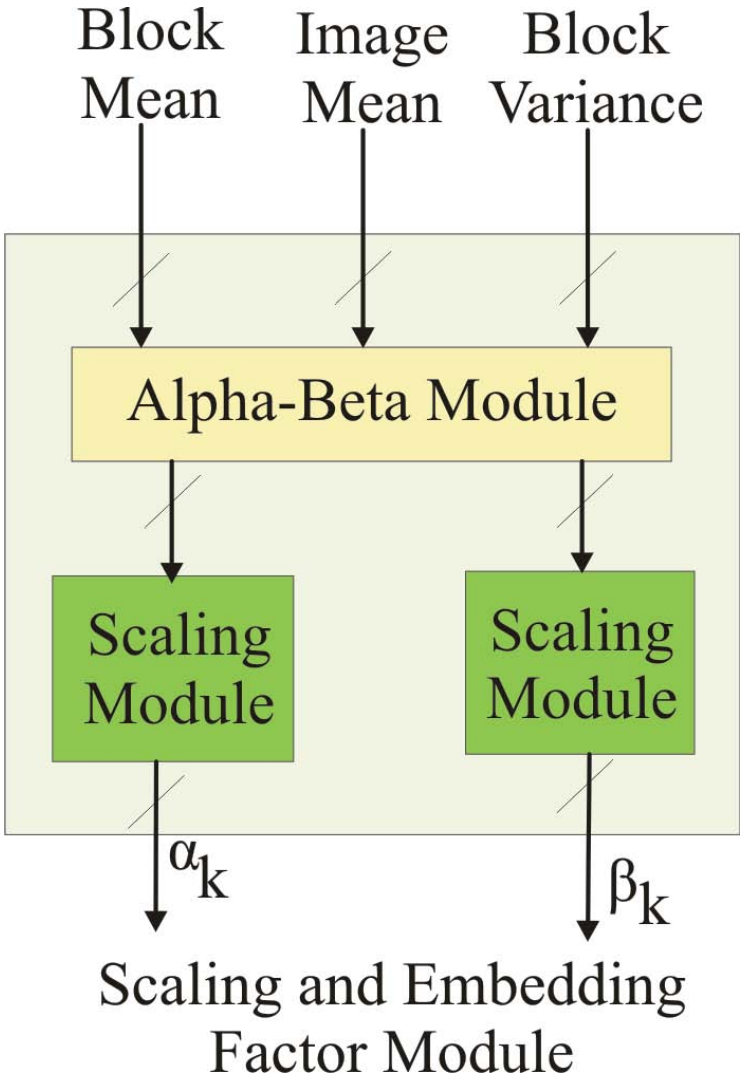
Edge Detection Module

- 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: $$|\mu_{AC_{Ik}}| > \tau |\mu_{AC_{\mathrm{Im}ax}}|$$

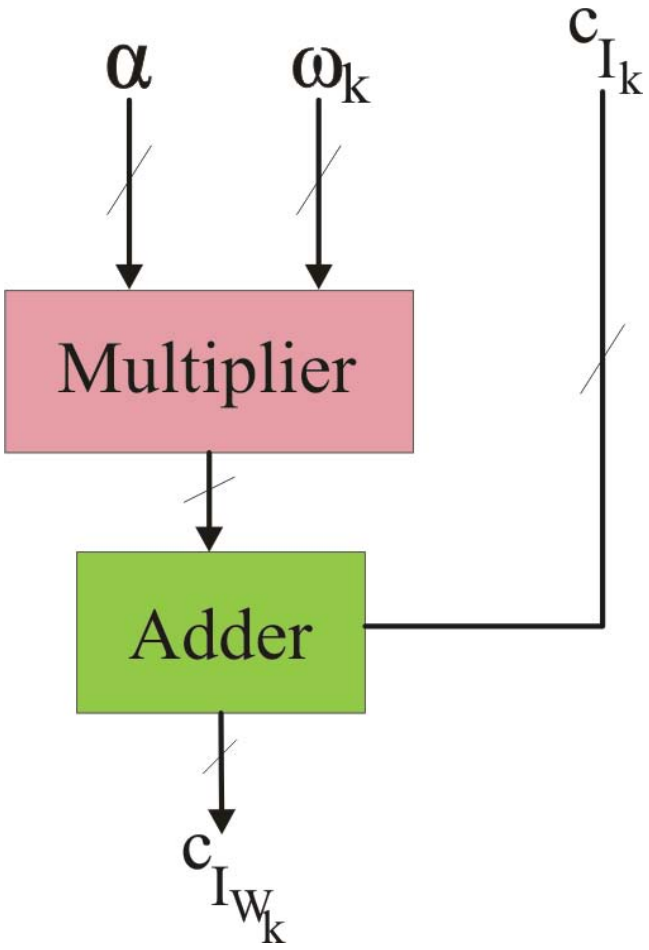
The Proposed Architecture … (Perceptual Analyzer Module)



The Proposed Architecture …
(Scaling and Embedding Factor Module)



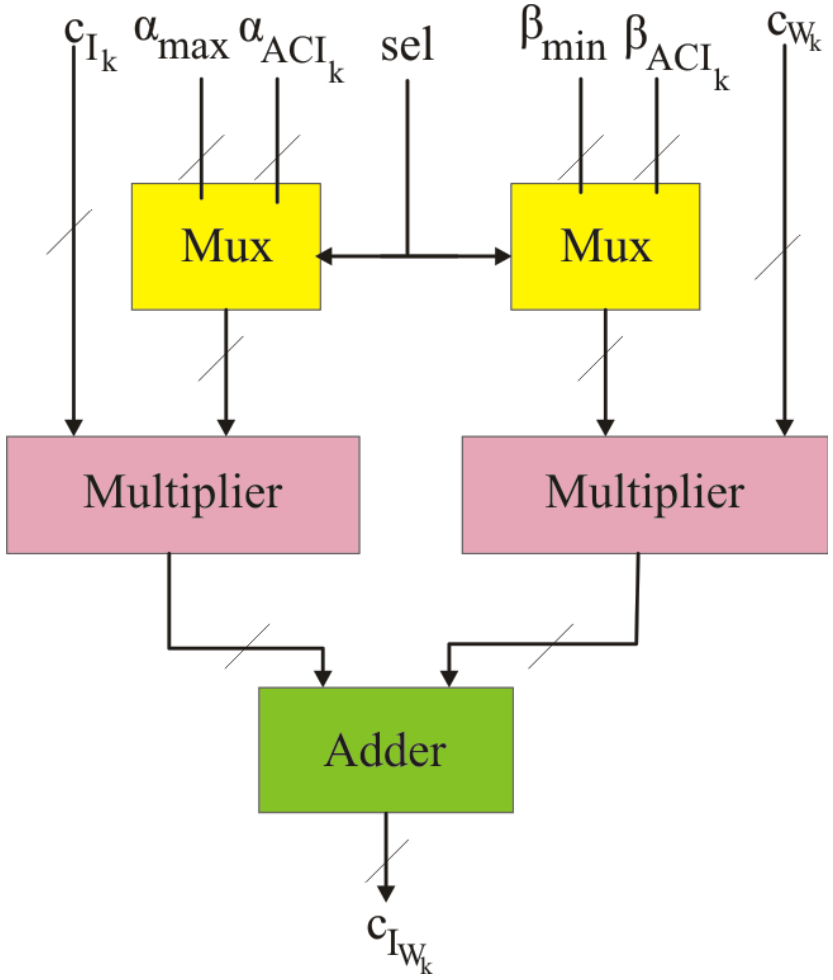
The Proposed Architecture … (Invisible Insertion Module)



Invisible insertion process:

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

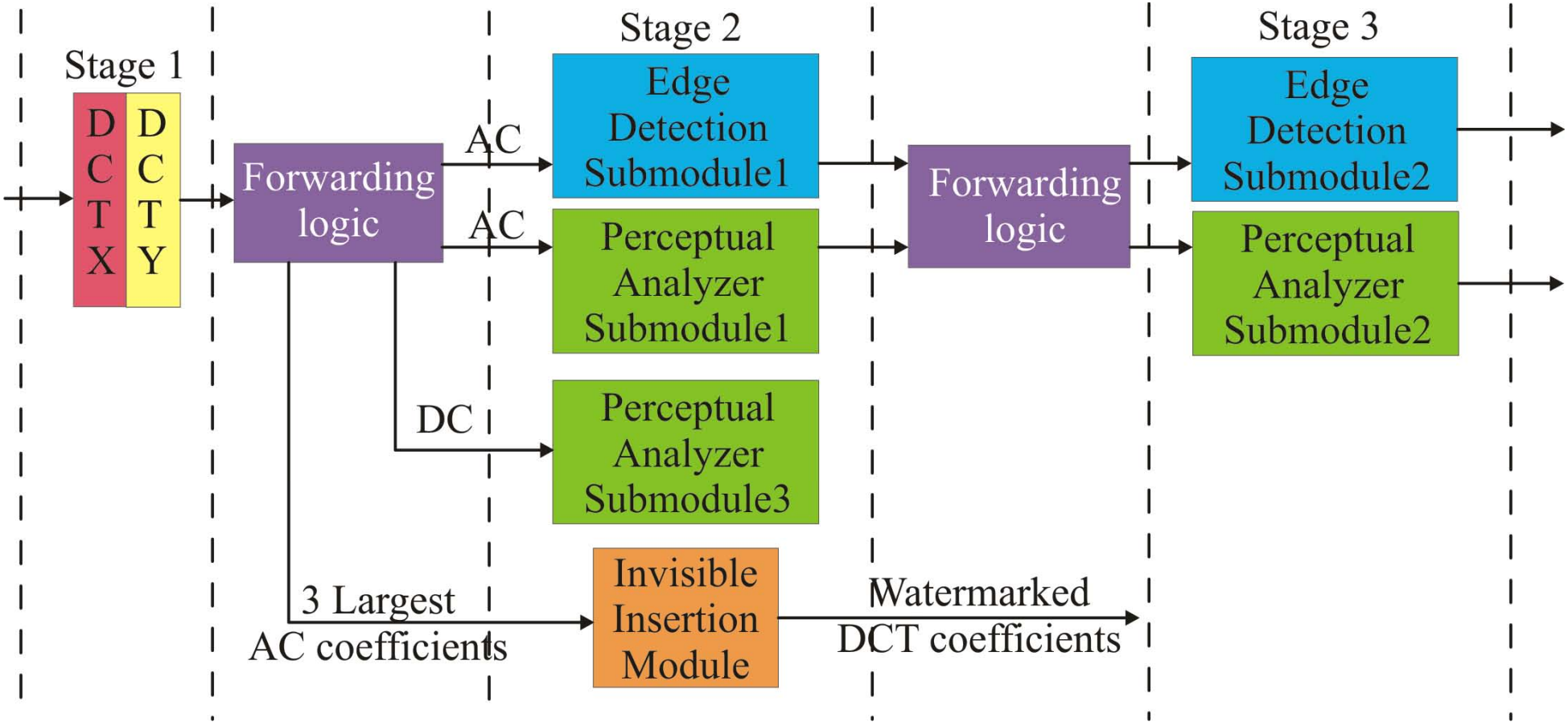
The Proposed Architecture … (Visible Insertion Module)



Visible insertion process:

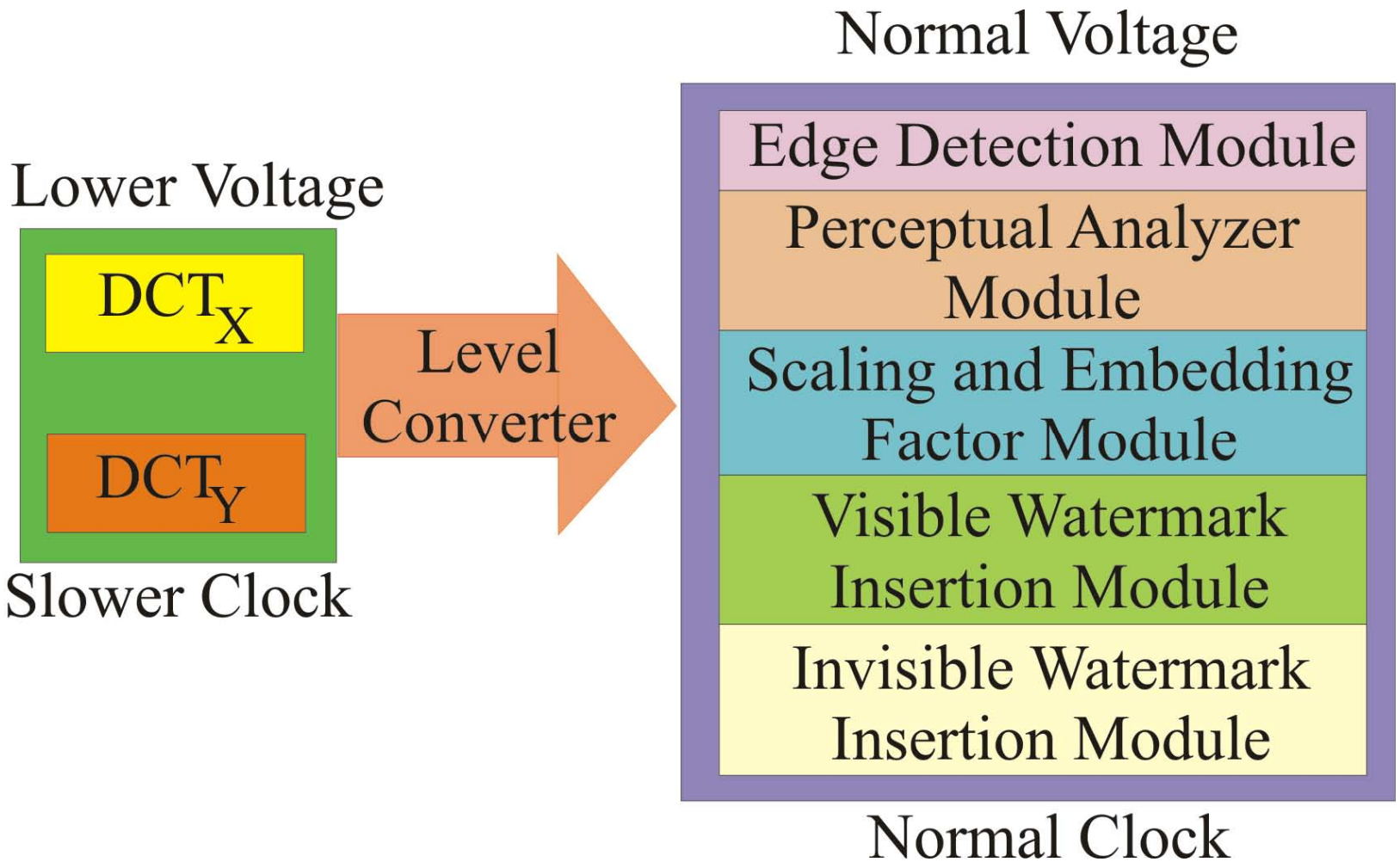
$$c_{I_{W_k}} = \alpha_k c_{I_k} + \beta_k c_{W_k}$$

The Proposed Architecture : Pipeline and Parallelism



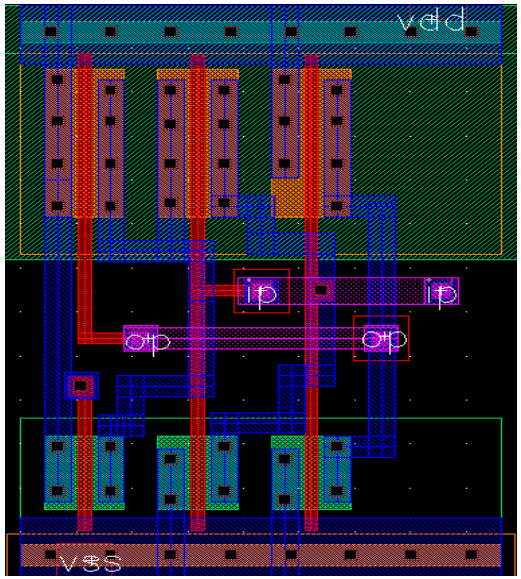
- The visible architecture has 3 stage pipeline and the invisible architecture has 2 stage pipeline.

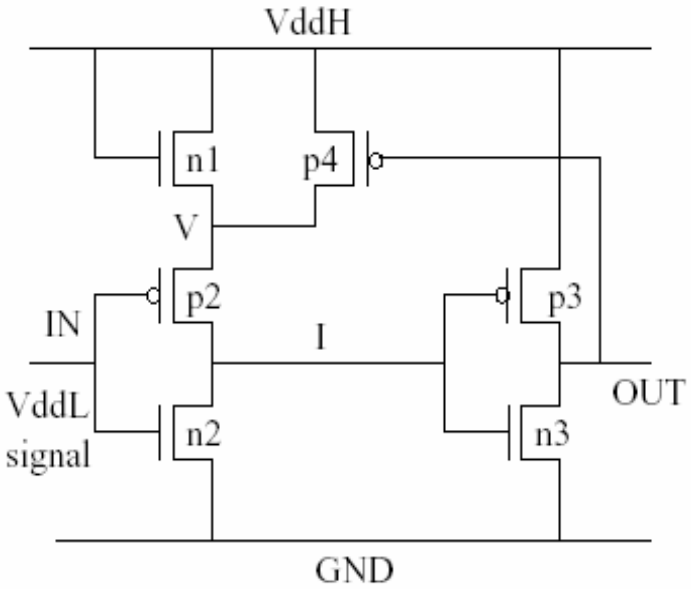
The Proposed Architecture : Dual Voltage and Frequency



Dual Voltage : Level Converters

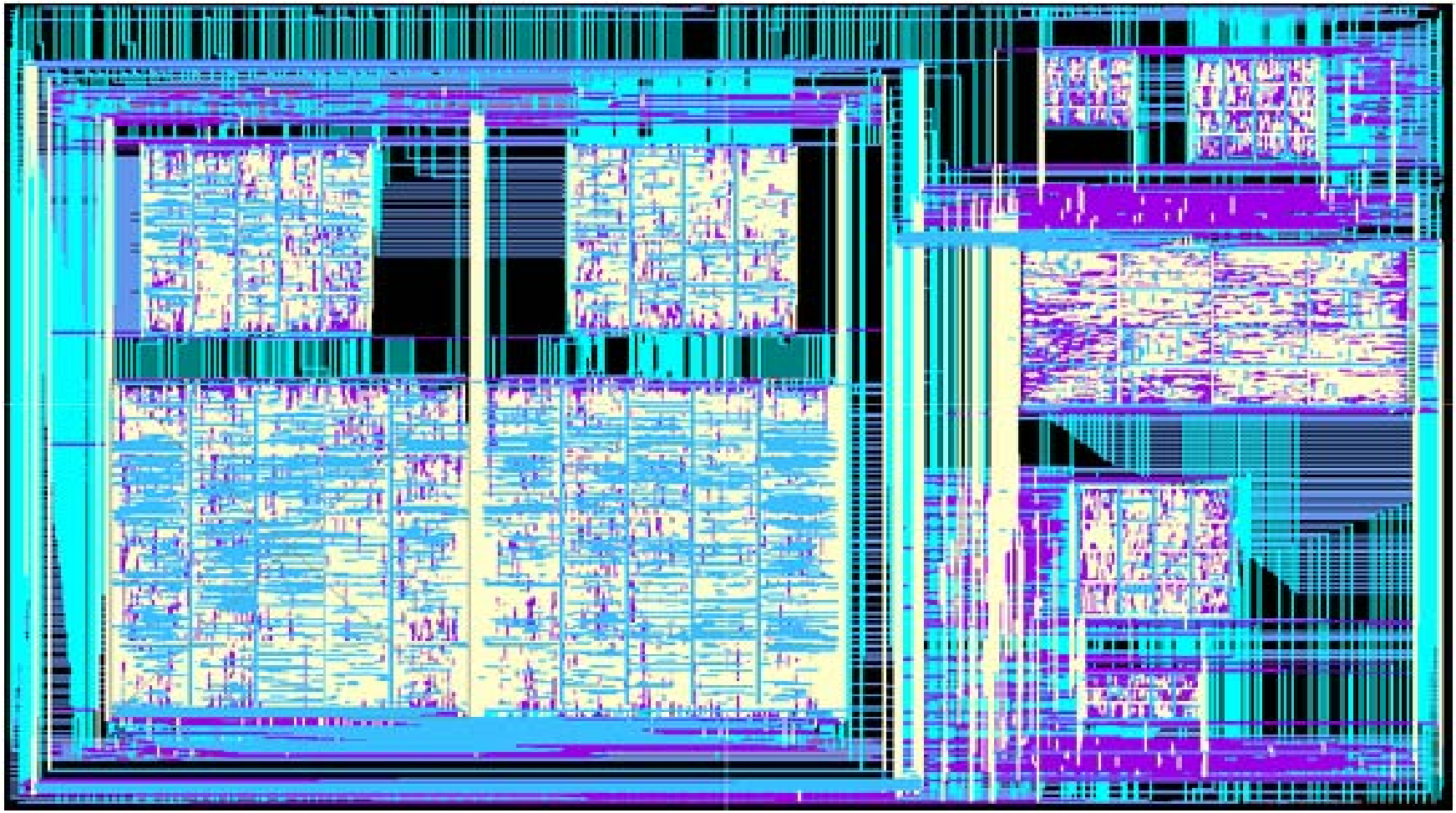
- Level converters required to step up the low voltage to high voltage.
- Single supply level converter is used as it is faster and consumes less power for its operation.





NOTE: Design of a 90nm CMOS based universal voltage level converter is currently in under progress using Cadence process design kit called gpdk_90nm.

Prototype Chip : Layout



NOTE: Standard cell design style adopted. Standard cells are obtained from Virginia Tech: TSMC 0.25µm.

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 Consumption: 0.3mW

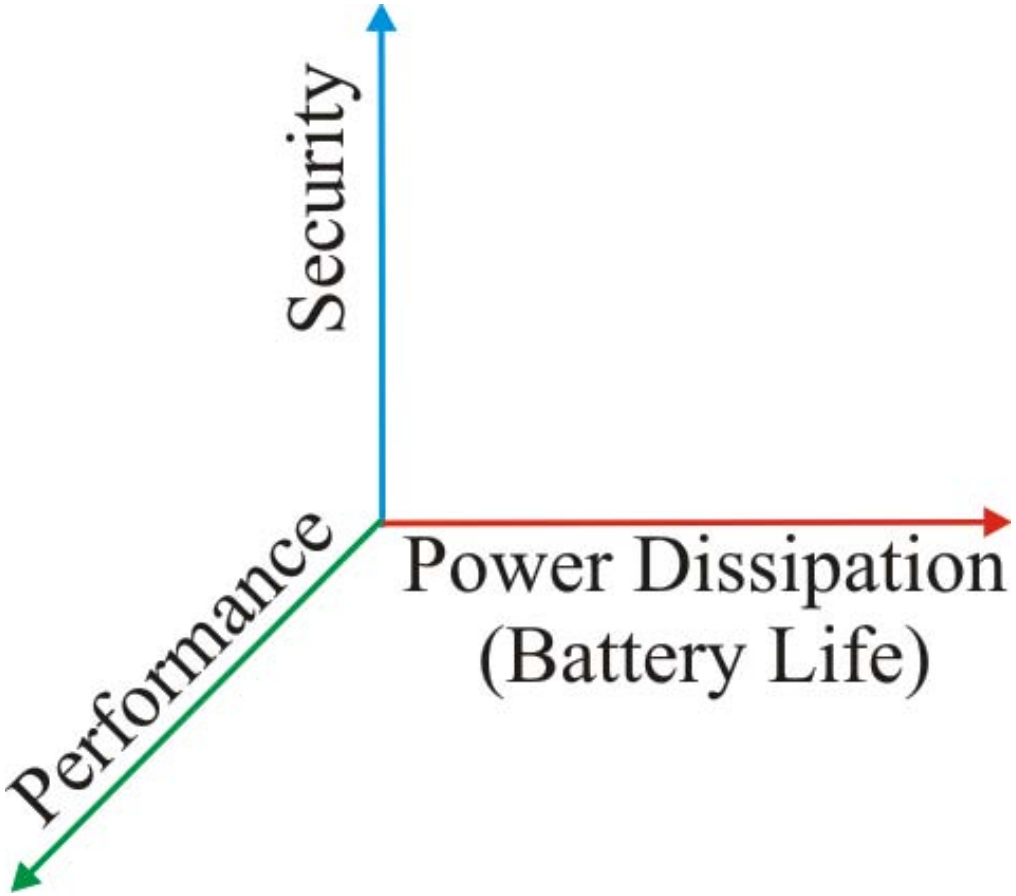
NOTE: Lowest power consuming watermarking chip available at present.

Research Challenges for Security, Power, and Performance Tradeoffs

Secure SoC Design : Two Modes

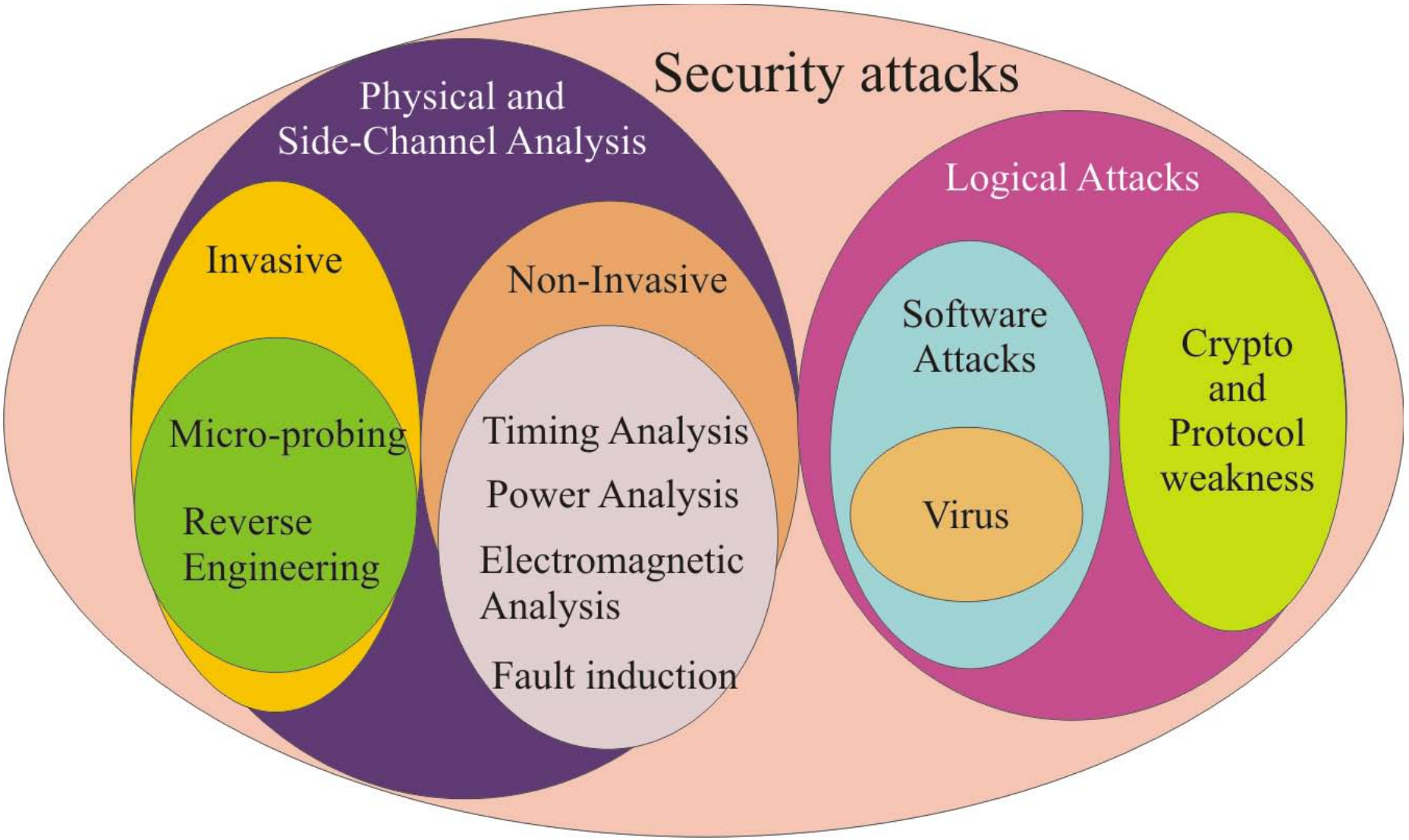
- Addition of DRM features in SoC:
  - Algorithms
  - Protocols
  - Architectures
  - Accelerators / Engines
- Consideration of DRM as a dimension in the design flow:
  - New design methodology
  - Design automation or computer aided design (CAD) tools for fast design space exploration.

Secure SoC Design Space Exploration



- Multidimensional design space, 3 are shown.
- More the security processing more the energy consumption and slower the performance.

Different Forms of Attacks on SoCs

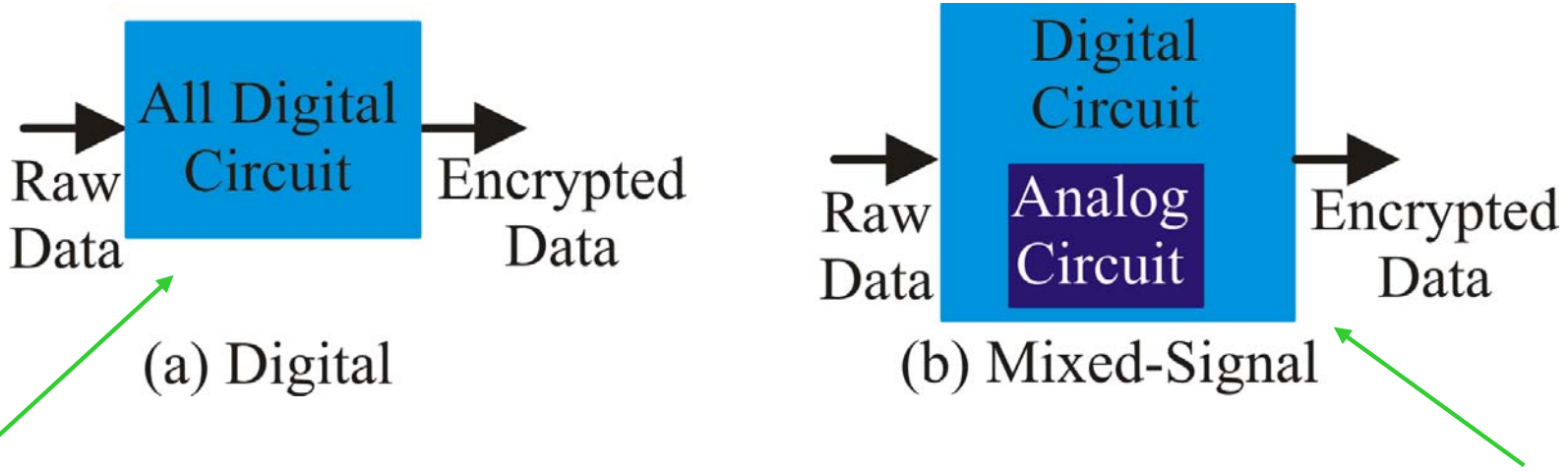


Secure Digital Camera :
AMS-SoC Research Challenges

- Development of hardware amenable algorithms.
- Building efficient VLSI architectures.
- Hardware-software co-design for security, power, and performance tradeoffs.
- Analog mixed-signal system-on-a-chip (AMS-SoC) design for security, power, and performance tradeoffs.

Analog-Digital Mixed-Signal Design

- A side channel attack is any attack based on information gained from the physical implementation of an encryption system.
- Static CMOS based circuit implementation are vulnerable to such attacks.

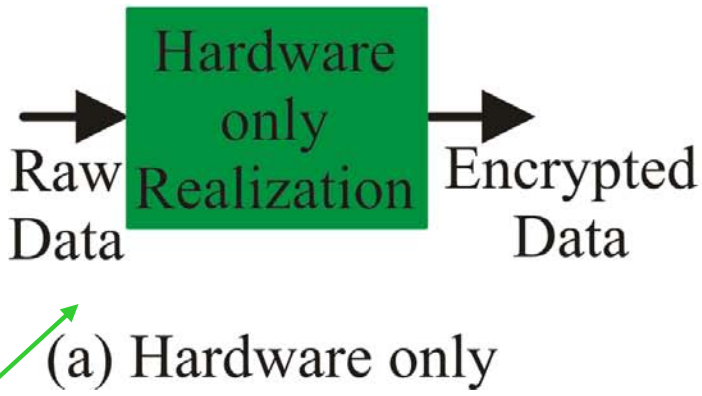


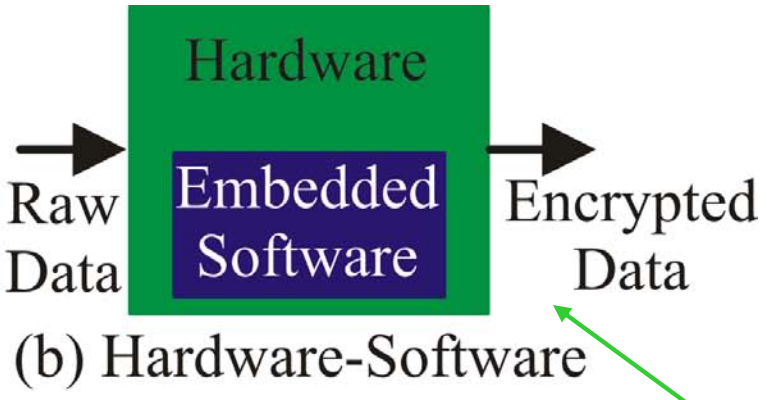
Vulnerable to side channel attack.

May abstract switching activity and reduce information leaking.

Hardware-Software Co-Design

- With the same philosophy, hardware with embedded software based encryption system can be considered.



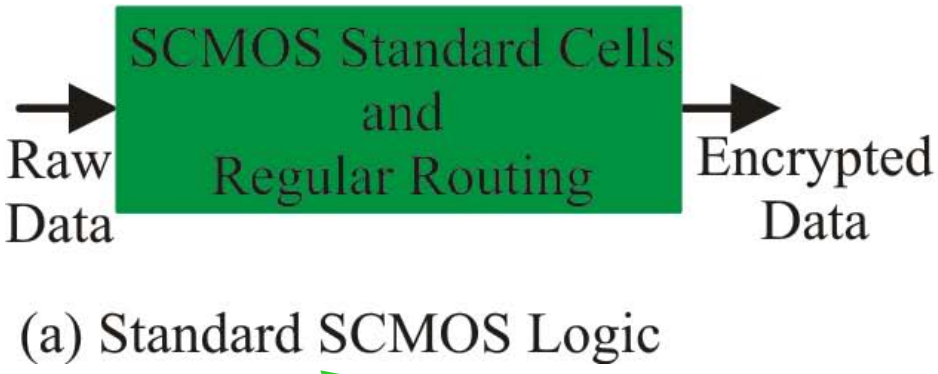


Vulnerable to side channel attack.

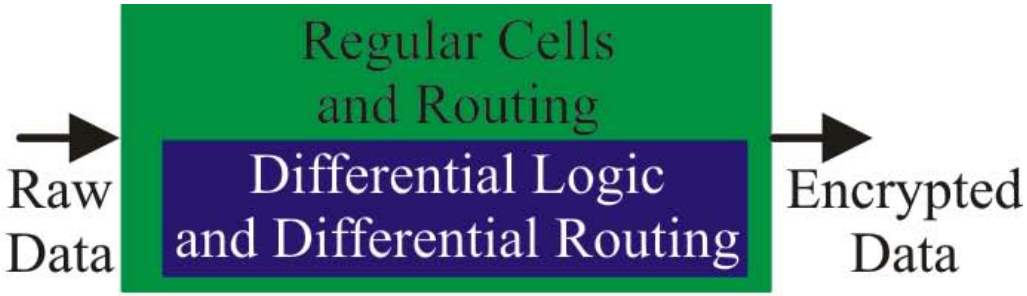
May abstract switching activity and reduce information leaking.

SCMOS Logic and Differential Logic Digital Circuit

- Develop logic styles and routing techniques such that power consumption per cycle is constant and capacitance charged at a node is constant.



(a) Standard SCMOS Logic



(b) Differential Logic and Routing

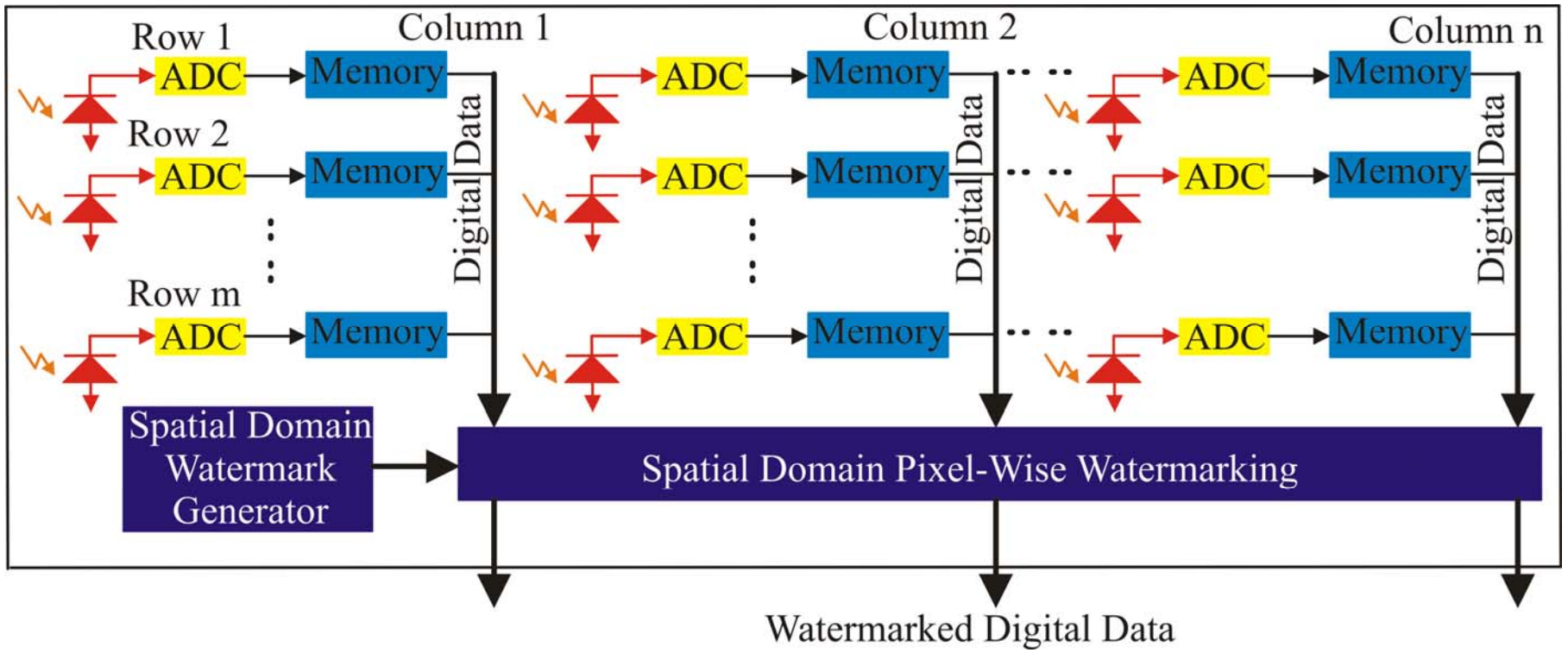
Vulnerable to side channel attack.

May abstract switching activity and reduce information leaking.

Secure Digital Camera : Different Design Alternatives

- New CMOS sensor with DRM.
- New ADC with DRM.
- Independent DRM (watermarking, encryption, etc.) processors.
- DRM (watermarking, encryption, etc.) co-processor for DSP.
- New instruction set architecture for RISC to support DRM at micro-architecture level.

Secure Digital Pixel Sensors (SDPS)

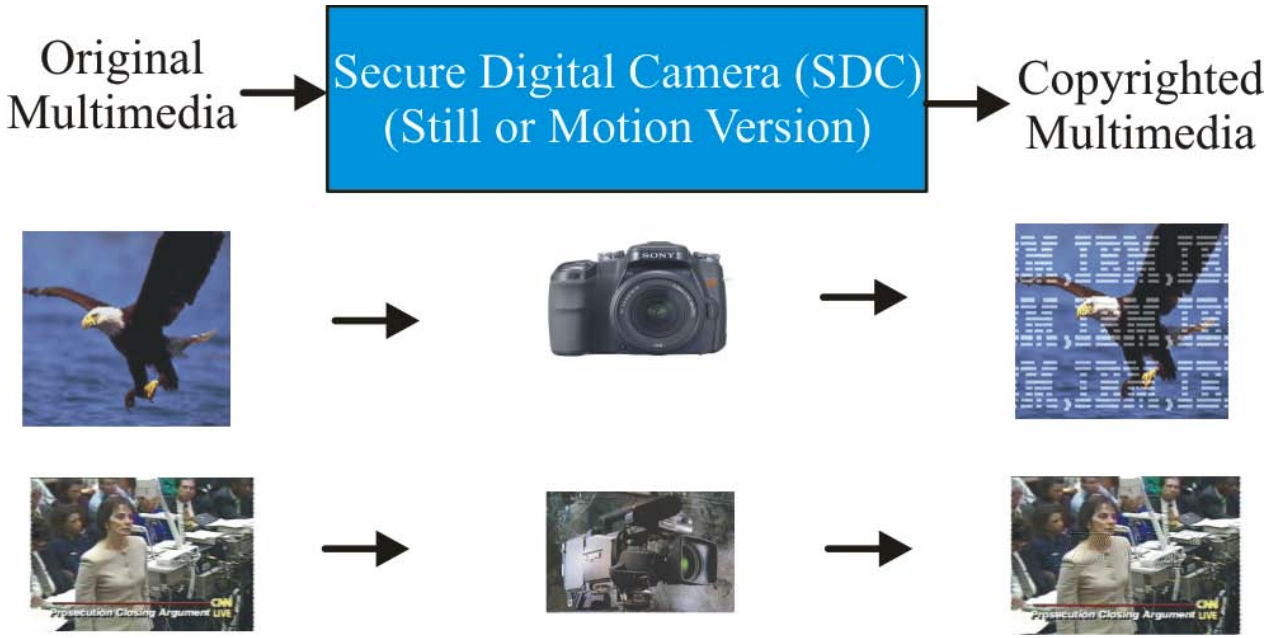


- Spatial-domain pixel-wise watermarking schemes will have less computational overhead.
- Additional circuitry will have minimal power dissipation overhead.

Secure Digital Camera (SDC): Application Scenarios

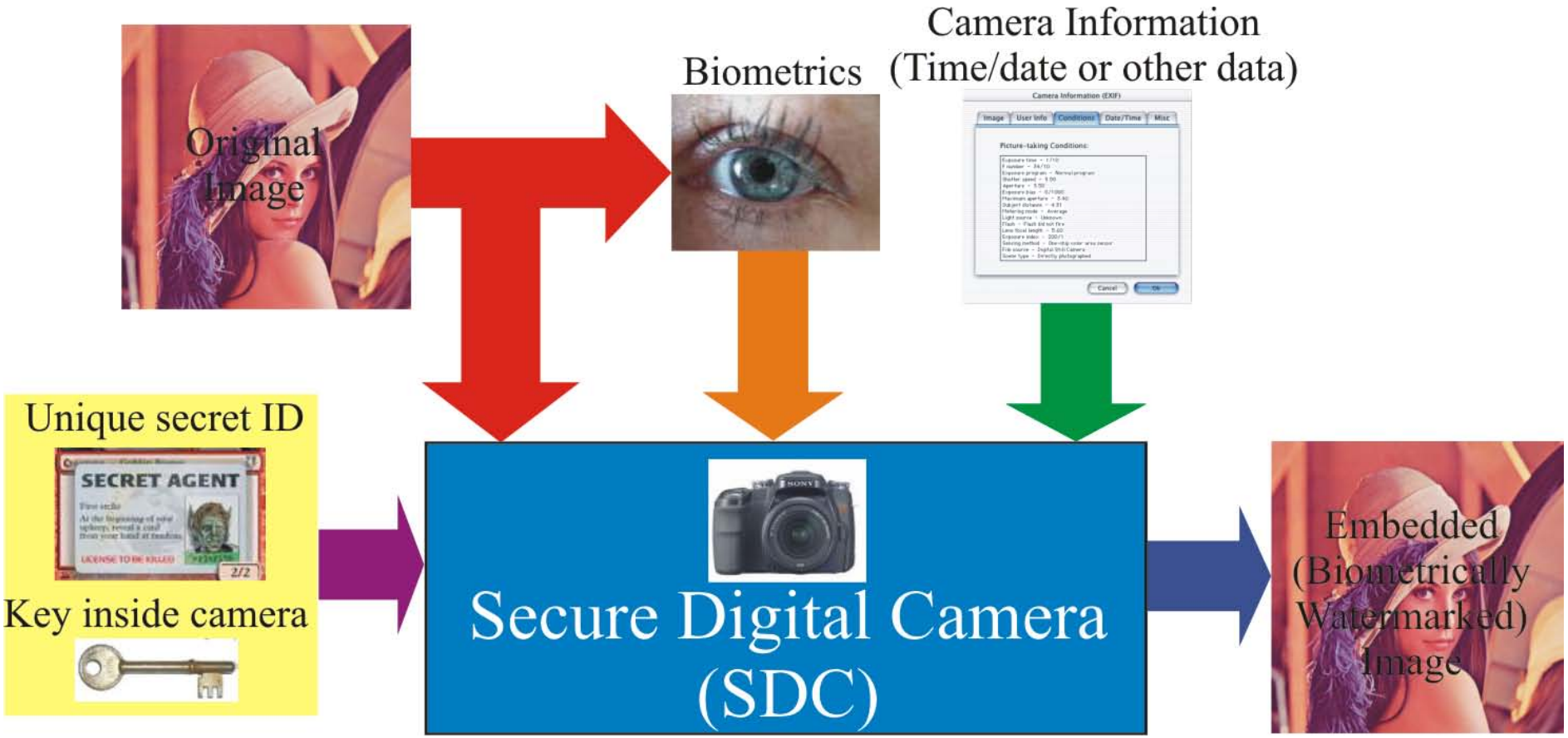
Application: Copyright Protection

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



NOTE: Can enhance revenue of movie/broadcasting industry.

Application: Biometric Based Authentication



NOTE: Can be useful for **homeland security**, e-passport.

Conclusions

Summary

- A low-cost low-power camera is introduced that can perform DRM in real time.
- Hardware assisted DRM has several advantages over software only.
- Structure of SoCs that will realize the secure digital camera is an ongoing research.
- A low-power watermarking chip is designed that consumes 0.3mW power.
- SDC to be realized as an SoC will involve security, power, and performance tradeoffs.
- Design automation or computer-aided design (CAD) tools would be necessary for fast and automatic AMS-SoC design space exploration.

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)*, 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. 141-144, 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. Ravi, A. Raghunathan, P. Kocher, S. Hattangady, "Security in Embedded Systems: Design Challenges," *ACM Transactions on Embedded Computing Systems (TECS),* Volume 3 , Issue 3, August 2004, pp. 461 – 491.
- **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.
- R. Puri et. al., "Pushing ASIC Performance in a Power Envelope," in the *Proceedings of the Design Automation Conference (DAC)*, 2003, pp. 788-793.

References …

- **S. P. Mohanty**, N. Ranganathan, and R. K. Namballa, "VLSI Implementation of Invisible Digital Watermarking Algorithms Towards the Development of a Secure JPEG Encoder," in the *Proceedings of the IEEE Workshop on Signal Processing System*, pp. 183-188, 2003.
- D. Hwang, K. Tiri, A. Hodjat, B.C. Lai, S. Yang, P. Schaumont, I. Verbauwhede, "A AES-Based Security Coprocessor IC in 0.18-μm CMOS with Resistance to Differential Power Analysis Side-Channel Attacks", *IEEE Journal of Solid-State Circuits (JSSC), vol.44, issue 4, pp.781-792, 2006.*
- K. Tiri, and I. Verbauwhede, "A Digital Design Flow for Secure Integrated Circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), vol.25, no.7, pp.1197-1208, 2006.*
- 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 ….

Thank You

For more information:

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