An Experimental Study on Energy Consumption of Video Encryption for Mobile Handheld Devices

UCIrvine
University of California, Irvine

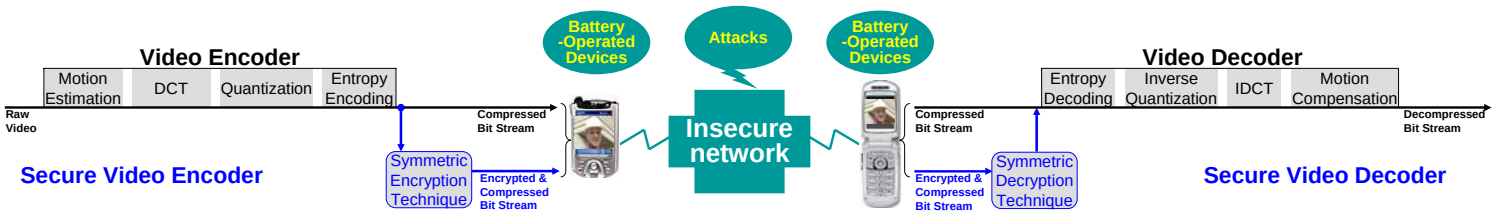
Kyoungwoo Lee, Nikil Dutt and Nalini Venkatasubramanian
School of Information and Computer Sciences

Overview of Secure Video Applications

Problem and Motivation

- Mobile multimedia applications are vulnerable to security attacks in wireless networks
- Significant computation for video encryption is expected on battery-operated mobile devices

▶ **Evaluate symmetric video encryption schemes from the perspective of energy consumption both analytically and experimentally**



Analytical Study of Video Encryption Schemes with respect to Energy Consumption

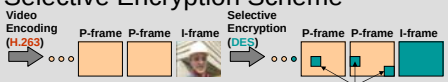
Studied Video Encryption Schemes

(1) Naive Encryption Scheme

❑ $Energy_{Naive} = e_{DES} * S_{Total}$

- e_{DES} - energy to encrypt one byte by DES
- S_{Total} - size of the whole video data

(2) Selective Encryption Scheme



❑ $Energy_{Selective} = e_{DES} * S_{IB}$

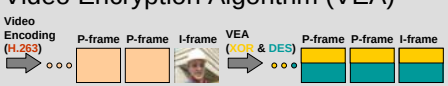
- S_{IB} - size of Intra-blocks in video data

(3) Zig-Zag Permutation Scheme

❑ $Energy_{Zig\text{-}Zag} = e_{overhead}$

- $e_{overhead}$ - energy to shuffle coefficients

(4) Video Encryption Algorithm (VEA)



❑ $Energy_{VEA} = \frac{1}{2} * (e_{DES} + e_{XOR}) * S_{Total}$

- e_{XOR} - energy for XOR

Analytical Comparison of Video Encryption Schemes

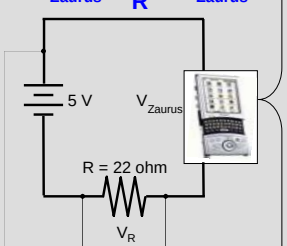
Algorithm		Security	Speed	Size	Drawback	Relative Energy
Naive	Encryption of all frames	High	Slow	No Change	Significant Computation	100 %
Selective	Partial encryption (e.g. Intra-blocks)	Moderate	Fast	No Change	Moderate Security	59 %
Zig-Zag	Shuffling coefficients from Quantization	Very Low	Very Fast	Big Increase	Breaks efficiency of Video Encoding	< 1 %
VEA	XORing and Half Encryption using even byte distribution	High	Fast	No Change	Not applicable for H.263 without even distribution	50 %

▶ **Naïve encryption scheme consumes twice the energy of Selective encryption scheme**

Experimental Study on Tradeoffs between Security and Energy Consumption

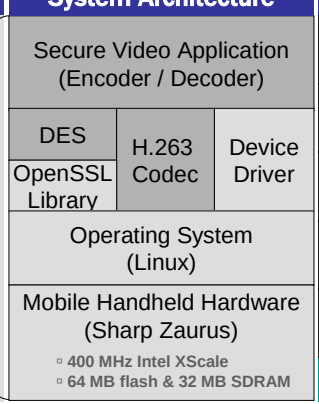
Experimental Setup

$$P_{Zaurus} = \frac{V_R}{R} * V_{Zaurus}$$



Power Measurement System

System Architecture

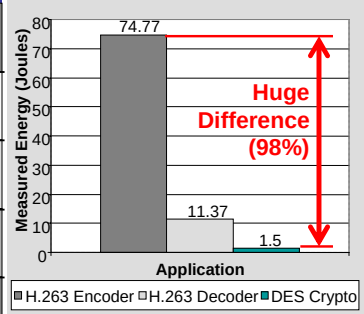


Energy Consumption for Varying Quality & Security

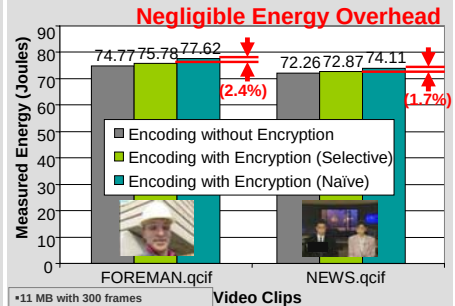
Quality (Quant Scale)	Security (Full vs. Partial)	Measured Energy (J)	Energy Overhead
High (Quant = 1)	High (Full)	128.2	13 %
	Low (Partial)	111.0	
Mid-High (Quant = 4)	High (Full)	92.05	9 %
	Low (Partial)	83.56	
Appropriate for mobile video: Mid-Low (Quant = 10)	High (Full)	77.62	2 %
	Low (Partial)	75.78	
Appropriate for mobile video: Low (Quant = 31)	High (Full)	70.44	1 %
	Low (Partial)	69.89	

▶ **Energy overhead for full video encryption is NEGLIGIBLE**

Experimental Results



▶ **Encryption consumes negligible energy as compared to encoding**



▶ **Energy consumption of encryption is negligible irrespective of video clips**

http://forge.ics.uci.edu/