Region of Interest Encryption – State of the Art

Andreas Unterweger

Department of Computer Sciences
University of Salzburg

May 29, 2013

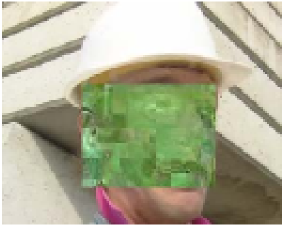
Scope

- Content
  - Description and use cases of RoI encryption
  - RoI encryption method classification
  - Presentation of selected encryption methods
  - Summary, conclusion and outlook
- Limitations
  - RoI-only encryption (no full encryption methods)
  - Format-compliant encryption
  - Video formats (no picture formats)
  - No formats which support RoI encryption natively

  → No (Motion) JPEG 2000 encryption methods!

What is RoI encryption?

- Encryption of dedicated parts (spatial areas) of a picture or video
- Rest of the picture/video remains untouched
- Not to be confused with selective encryption



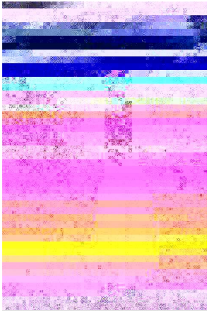
Source: Kim et al. (2007)

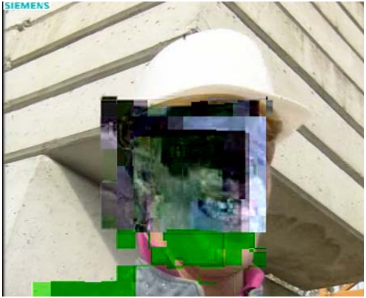
Selective vs. RoI encryption

- **Selective** encryption **enciphers the whole picture** by changing only some parts of it or its bit stream
- **RoI** encryption **preserves everything outside the RoIs**
- Terminology not used consistently throughout the literature
- RoI encryption as a special case of selective encryption

What is **not** RoI encryption?

- Encrypting the whole picture
- Pictures with drift in non-RoI picture areas





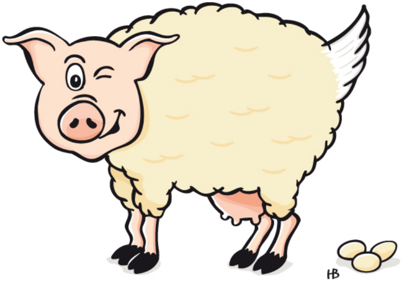
Sources: Auer et al. (2013), Kim et al. (2007)

Why RoI encryption?

- Privacy (e.g., in surveillance videos)
  - Disguise (parts of) objects
    - Faces/people
    - License plates/vehicles
    - Buildings
    - ...
  - Disguise actions
    - Hand/body movements
    - Object movements
    - ...
- Content control (e.g., in movies)
  - Censorship
  - Trade mark disguise
  - Parental control
  - ...

The ideal RoI encryption approach

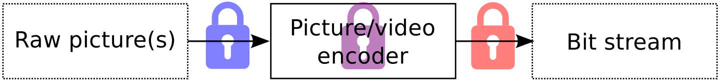
- Format-compliant
- Secure
- Fast
- No overhead



Source: Baumgärtner (2010)

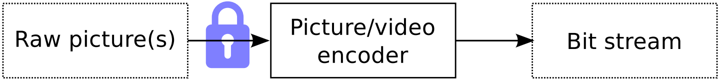
Categorization of approaches

- Before compression
- During compression
- After compression



Overview of pre-compression approaches

- Encrypt RoIs in original picture before compression
- Advantages
  - Largely compression-independent
  - RoIs are easily separable from the rest (no drift)
  - Usually fast (no decoding required)
- Disadvantages
  - Requires compression robustness considerations
  - Possibly reduces compression efficiency
  - May require communication with the encoder (RoI locations)


Raw picture(s)

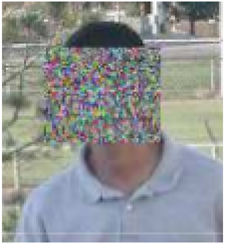
Picture/video encoder

Bit stream

Selected approaches I

- DES/AES encryption (Boult, 2005)

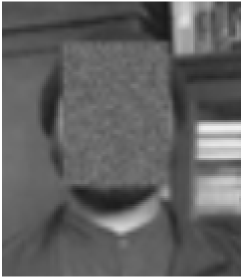
- Advantages
  - Algorithm and key size can be chosen relatively freely
- Disadvantages
  - RoIs hard to compress (quasi random data)
  - Only lossless RoI compression allowed (fragile decoding)
  - DES/AES block size consideration necessary



Selected approaches II

- Chaotic encryption (Rahman et al., 2010)

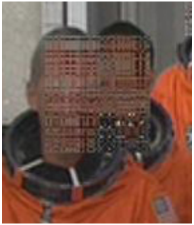
- Advantages
  - Encrypted signal characteristics not completely random
- Disadvantages
  - RoIs still relatively hard to compress
  - Only loss-less RoI compression allowed (fragile decoding)



Selected approaches III

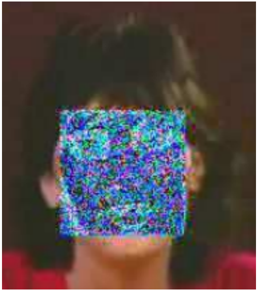
- Permutations (Carrillo et al., 2009; Dufaux et al., 2010)

- Advantages
  - Lossy compression can be applied to RoIs to some extent
  - Encryption strength depends on block size ($16 \cdot 16$ and $4 \cdot 4$ used)
- Disadvantages
  - RoIs are harder to compress than the rest
  - Compression-induced quality loss higher in RoIs



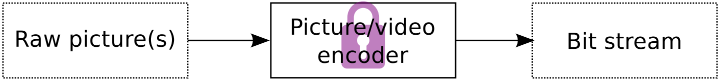
Selected approaches IV

- PRNG-based n-MSB bit plane scrambling (Dufaux et al., 2005)
- Advantages
  - Lossy compression can be applied to RoIs to some extent
  - Encryption strength depends on number of scrambled bits
- Disadvantages
  - RoIs are harder to compress than the rest
  - Compression-induced quality loss higher in RoIs



Overview of in-compression approaches

- Encrypt RoIs during compression
- Advantages
  - Implementation is relatively easy (full encoder control)
  - Compression performance degradation can be influenced
- Disadvantages
  - Encoder has to be modified
  - Limited to one particular format (or even implementation)
  - Drift has to be considered (relatively easy to avoid)

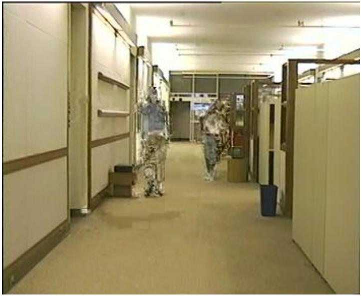


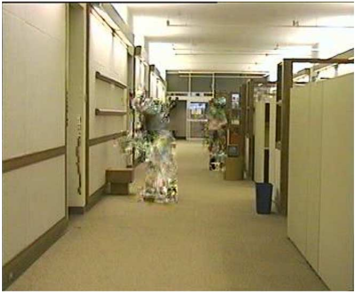
In-compression drift avoidance

- Full encoder control → limit prediction to avoid drift
- Don't use RoI data to predict non-RoI data
  - Limit motion estimation search range
  - Limit intra prediction modes
  - Use slices and/or slice groups (H.264 only)
- Use RoI data to predict other RoI data
- Advantages
  - All RoI data is available – encrypted and unencrypted
  - Reduced number of possibilites may speed up RDO
- Disadvantages
  - Implementing correct prediction constraints may be hard
  - Compression efficiency deteriorates

Commonly used methods I

- All DCT-based formats (MPEG-2 Video, MPEG-4 Part 2, H.264):
  - AC coefficient sign scrambling[1]
  - AC coefficient value scrambling[2]





Sources: Dufaux & Ebrahimi (2010), Dufaux & Ebrahimi (2008)

[1] e.g., Dufaux & Ebrahimi (2005), Dufaux & Ebrahimi (2006), Dufaux & Ebrahimi (2008), Dufaux & Ebrahimi (2010), Meibing et al. (2008), Tong et al. (2010)

[2] Dufaux & Ebrahimi (2005), Chattopadhyay & Boult (2007), Sohn et al. (2009), Tong et al. (2009)

Commonly used methods I – Details

Common aspects:

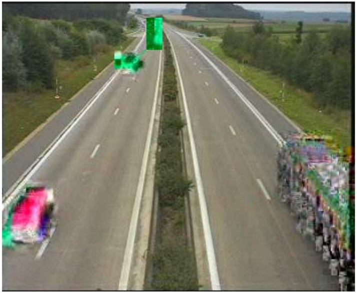
- Advantages
  - Fast
  - Moderate bitrate overhead ($\approx 10\%$)
  - Error concealment is hard
- Disadvantages
  - Security depends on number of non-zero AC coefficients per block

Additional aspects for AC coefficient value scrambling:

- Advantages
  - Even larger attack complexity
  - Error concealment is very hard
- Disadvantages
  - Overhead due to drift correction may be large (up to 250% for Dufaux's & Ebrahimi's (2008) approach according to Dai et al. (2011))

Commonly used methods II

- All DCT-based formats (MPEG-2 Video, MPEG-4 Part 2, H.264):
  - DC coefficient value scrambling
    - DC coefficients only[3]
    - Together with AC coefficients[4]
  - DC sign scrambling (e.g., combined with AC sign scrambling[5])



Source: Dufaux & Ebrahimi (2008)

[3] Wu & Wu (1997)

[4] Wu & Wu (1997), Chattopadhyay & Boult (2007), Dufaux & Ebrahimi (2008)

[5] Sohn et al. (2009)

Commonly used methods II – Details

- DC coefficients are coded relative to their spatial predecessors in all commonly used picture and video formats → differences are modified

  Common aspects:

- Advantages
  - Very fast
  - Very low bitrate overhead (0–3.5% according to Sohn et al. (2009))
- Disadvantages
  - Very easy to attack (set all differences to zero)

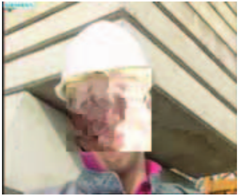
  Additional aspects for DC sign scrambling:

- Advantages
  - Even easier to implement
  - Even lower bitrate overhead
- Disadvantages
  - Even easier to attack (plausible values)

Selected H.264-specific approaches I

- PRNG-based intra mode scrambling (Tong et al., 2009)[6]
- Restriction of prediction modes to avoid drift

- Advantages
  - Forbidden modes make drift control easier
- Disadvantages
  - High bitrate overhead due to restrictions ($\approx$ 12% with QP 28)

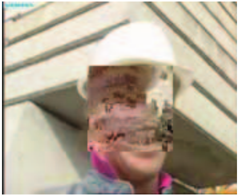


[6] Extended in Dai et al. (2011)

Selected H.264-specific approaches II

- PRNG-based MVD sign scrambling (Tong et al., 2009)[7]
- ME search range restrictions to avoid temporal drift
- FMO to avoid spatial drift

- Advantages
  - Scrambling operation is very simple
- Disadvantages
  - High bit rate overhead (≈ 17% with QP 28)
  - Limited to baseline profile due to use of FMO



[7] Extended in Dai et al. (2011)

Selected H.264-specific approaches III

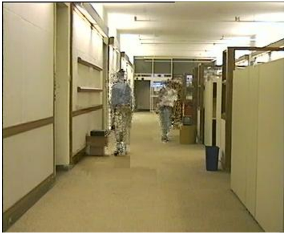
- Previous two methods of Tong et al. (2009) combined with Dufaux's & Ebrahimi's (2008) methods to avoid drift
- FMO to avoid spatial drift
- Forced intra blocks to avoid temporal drift

- Advantages
  - Drift is easier to contain
- Disadvantages
  - Enormous bit rate overhead ($\approx$ 50-180% with QP 28)
  - Limited to baseline profile due to use of FMO

Selected H.264-specific approaches IV

- PRNG-based AC coefficient shuffling (Dufaux & Ebrahimi, 2008)
- FMO to avoid spatial drift
- Forced intra blocks to avoid temporal drift

- Advantages
  - Hard to attack (huge key space)
- Disadvantages
  - Significant overhead (4-11%)
  - Elimination of implausible coefficient values may be possible
  - Limited to baseline profile due to use of FMO



Selected H.264-specific approaches V

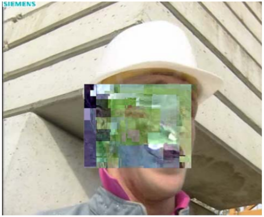
- AC coefficient scrambling at CABAC level (Meibing et al., 2012)
- Scrambling of values' TU prefix in regular coding mode
- Complete value randomization in bypass coding mode
- Additional AC coefficient sign scrambling at bit stream level

- Advantages
  - Little impact on compression efficiency
- Disadvantages
  - Issue of drift not discussed

Selected H.264-specific approaches VI

- MVD sign and AC coeffcient sign scrambling (Kim et al., 2007)
- Constrained motion estimation to avoid temporal drift
- Interpolation and inter-layer prediction restrictions for SVC support

- Advantages
  - Only available approach for SVC RoI encryption
- Disadvantages
  - Coding efficiency significantly decreases with increasing RoI size
  - High total overhead ($\approx 11\%$ for $48 \cdot 48$ RoI in CIF video)



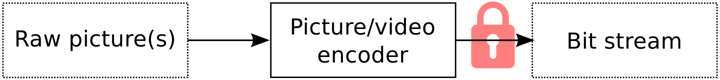
Other approaches worth mentioning

Encryption approaches which could be adopted for RoI encryption:

- All DCT-based formats (MPEG-2 Video, MPEG-4 Part 2, H.264)
  - Block shuffling (e.g., Zeng & Lei (2003))
  - Motion vector scrambling (e.g., Zeng & Lei (2003))
  - Scanning order permutation (e.g., Shadid, Chaumont & Puech (2009))
- H.264-specific
  - CAVLC codeword reordering (Mian, Jia & Lei (2007))
  - Selective CAVLC code word replacement of AC-coefficient-value-related syntax elements (Dubois, Puech & Blanc-Talon (2011))
  - Selective Exponential Golomb code word suffix replacement before CABAC entropy coding (Shadid, Chaumont & Puech (2009))

Overview of post-compression approaches

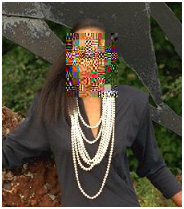
- Encrypt RoIs in compressed bit stream
- Advantages
  - No need to modify the original picture or the encoder
  - Allows for relatively slim encryption/decryption black boxes
- Disadvantages
  - RoI detection requires some form of decoding
  - Avoiding drift may be complex
  - Possibly very hard to do in a format-compliant way



Selected approaches I

- (Motion) JPEG scrambling (Unterweger & Uhl, 2012)
- PRNG-based code word flipping and value scrambling

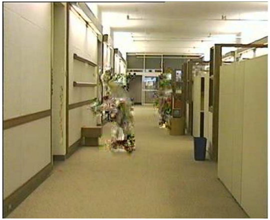
- Advantages
  - Length-preserving
  - Fast (detailled measurements in Auer et al. (2013))
  - No temporal drift by design (JPEG is for pictures, not videos)
- Disadvantages
  - RoI encryption only proposed as (trivial) extension to full encryption



Selected approaches II

- DC and AC sign scrambling (Dufaux et al., 2008)
- Implemented for MPEG-4 Part 2 (also applicable to MPEG-2 Video)

- Advantages
  - Simple bit flipping operation (signs are stored uncompressed)
  - Length-preserving in encrypted frames
- Disadvantages
  - Drift requires analyzing all subsequent frames for RoI references
  - Drift compensation requires selective re-encoding → very slow



Selected approaches III

- Slice data encryption (Iqbal, Shahabuddin & Shirmohammadi, 2010)
- Limited to H.264 streams where RoIs are separate slices

- Advantages
  - Easy to implement
  - Spatial drift contained through slice borders
- Disadvantages
  - No discussion of temporal drift
  - Requires slices corresponding to RoIs in original stream
  - Known plaintext attacks easy (encryption is XOR with 8-bit key)
  - Format compliance claim dubious (no details)

Issues affecting all approaches

- How to signal RoIs?
  - Implicitly (through signal characteristics)
  - Explicitly (through in- or out-of-band signalling)
- How to avoid attacks?
  - Explicit RoI locations may make attacks easier
  - Signal characteristics of natural images limit plaubsible "plain text"
- How to ensure security?
  - Selection of parts to be encrypted is hard (how much is enough?)
  - Recognizability (no reliable metrics for heavily distorted images yet)

Conclusion

- Pre-compression approaches are often encoder-bound
- In-compression approaches are researched extensively
- Post-compression approaches are sparse → research opportunities
- No approach is perfect
- Open issues offer further research possibilites

Thank you for your attention!

Questions?