Ch4 多媒体数据加密

马晓静
lindahust@mail.hust.edu.cn

大纲

- 概述
- 案例

多媒体数据加密-概述

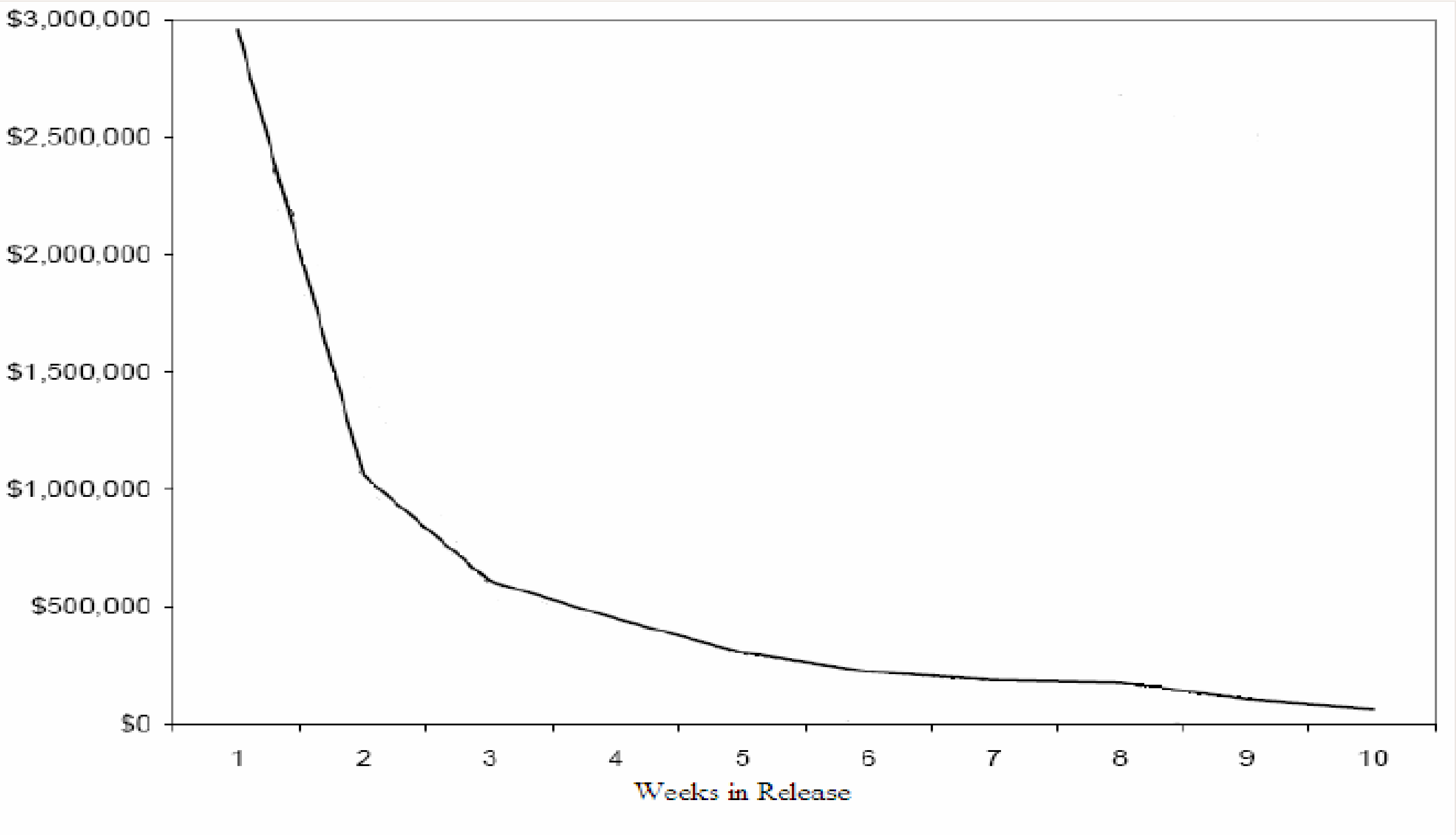
内容加密

- 把加密技术应用到多媒体数据上，根据多媒体应用的不同场景可能需要特殊的应用方式。
- 使多媒体数据的内容视觉上无法辨认或者视觉质量降质到不可接受。

需求

- 复杂度
- 内容安全
- 压缩效率
- 错误鲁棒
- 自适应和可扩展

多媒体数据加密的安全性



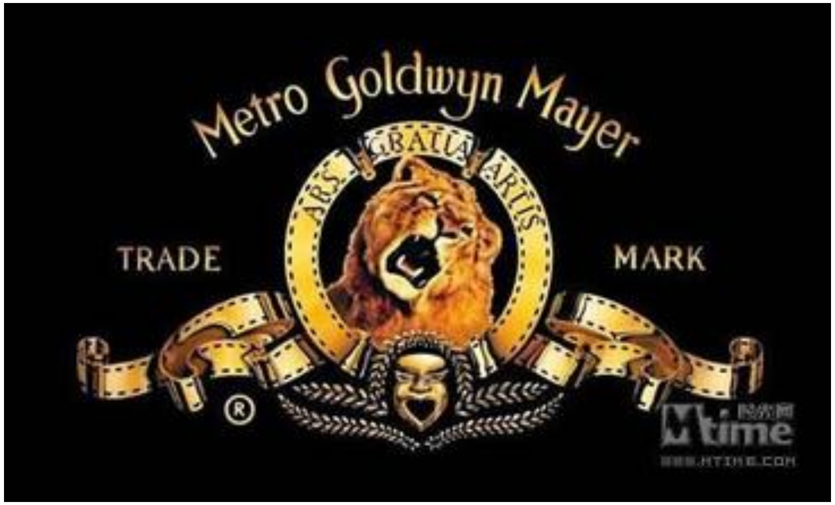
安全攻击

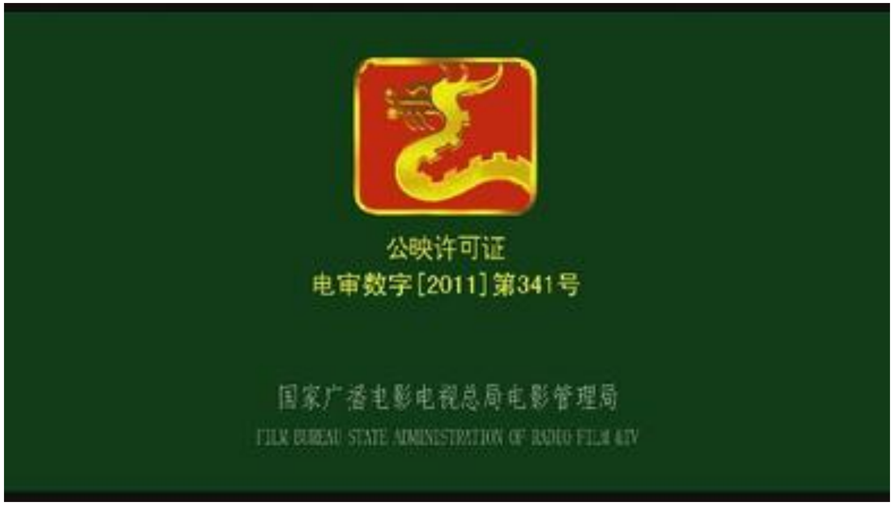
- 完全破解
  - 通过寻找到密钥完全恢复明文比特流
- 视觉破解
  - 没有密钥，但是可以变换得到视觉质量可接受的数据，或者恢复部分内容信息
- 局部破解
  - 推测出局部的明文比特流或者内容信息
- 信息揣测
  - 获得关于密钥和明文比特流的某些信息

安全攻击

- 特有攻击：利用多媒体数据独特之处
  - 统计攻击
    - 利用多媒体数据不同部分之间的关系推测明文或降低强力攻击的搜索空间
  - 基于错误隐藏的攻击
    - 将加密的那部分数据当做错误，用错误隐藏和错误恢复技术来试图恢复该部分对应的明文数据。

已知明文攻击




公映许可证
电审数字[2011]第341号

国家广播电影电视总局电影管理局
FILM BUREAU STATE ADMINISTRATION OF RADIO FILM &TV

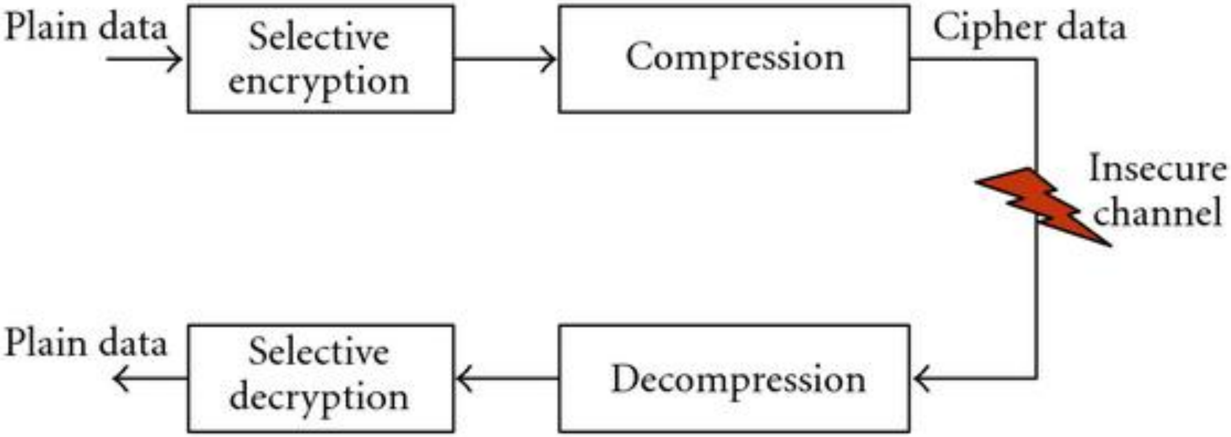
在多媒体数据里很容易去猜测一个局部的多媒体数据，如音频里存在的一段静默，图像或者视频里的一个平缓区域。

多媒体数据加密方法

- 传统方法
- 选择加密
- 特殊加密
    - 压缩与加密联合方案
    - 可扩展加密

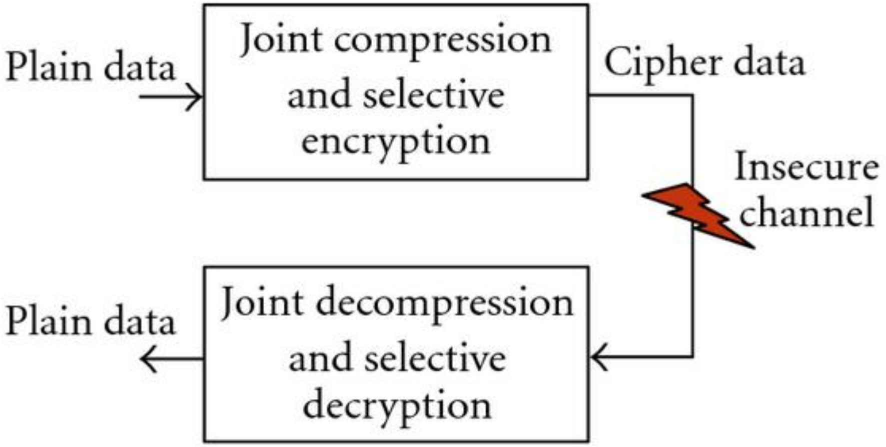
Selective Encryption

- When encryption is performed with respect to compression
- Pre-compression
  - Inherently format compliant
  - Inapplicable for lossy compression
  - Bandwidth expansion, not compression friendly



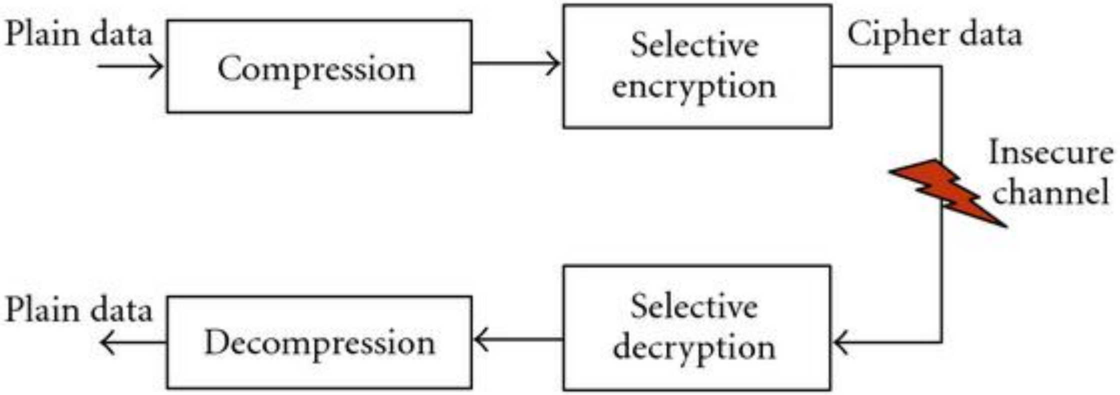
Selective Encryption

- In-compression
  - Joint compression and encryption
  - Modifications of both encoder and decoder
  - Adversely impact format compliance and compression friendliness


Plain data
Joint compression and selective encryption
Cipher data
Insecure channel
Plain data
Joint decompression and selective decryption

Selective Encryption

- Post-compression
  - Compression friendly
  - Encryption and decryption do not need modifications at encoder or decoder sides



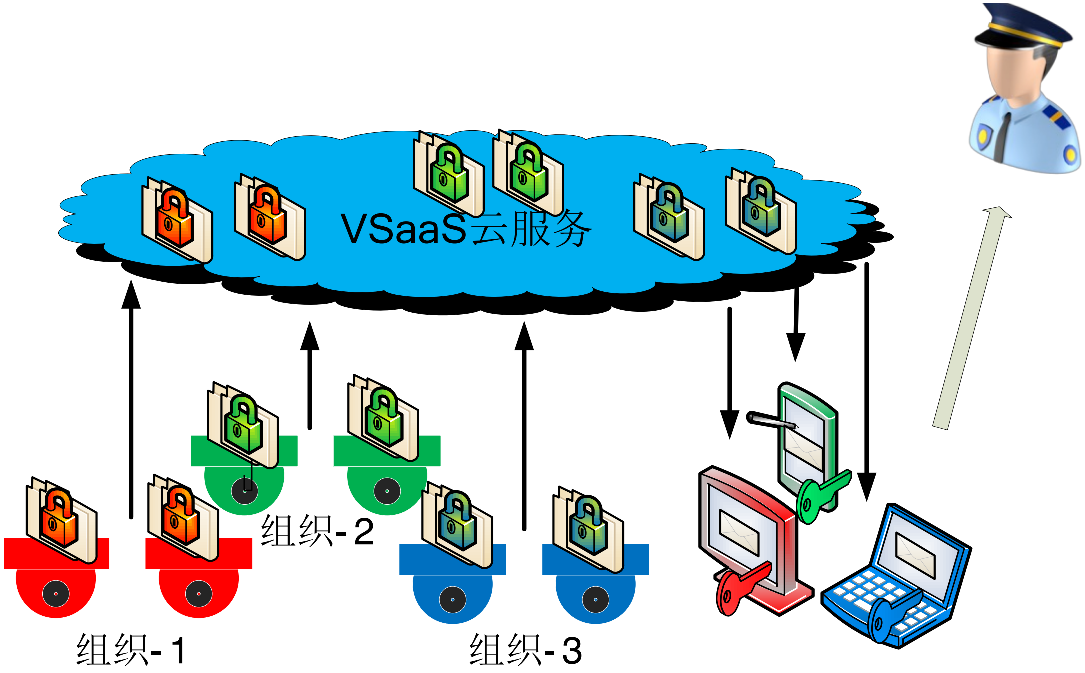
多媒体加密-案例一 -监控视频隐私区域保护

如何在保护隐私的同时实现运动检测？

- 基于对象的区域加密

基于对象的区域加密

- 隐私区域保护的模型
- 云端：
  - 隐私区域不可见
  - 非隐私区域可见
- 授权用户
  - 隐私区域非隐私区域均可见

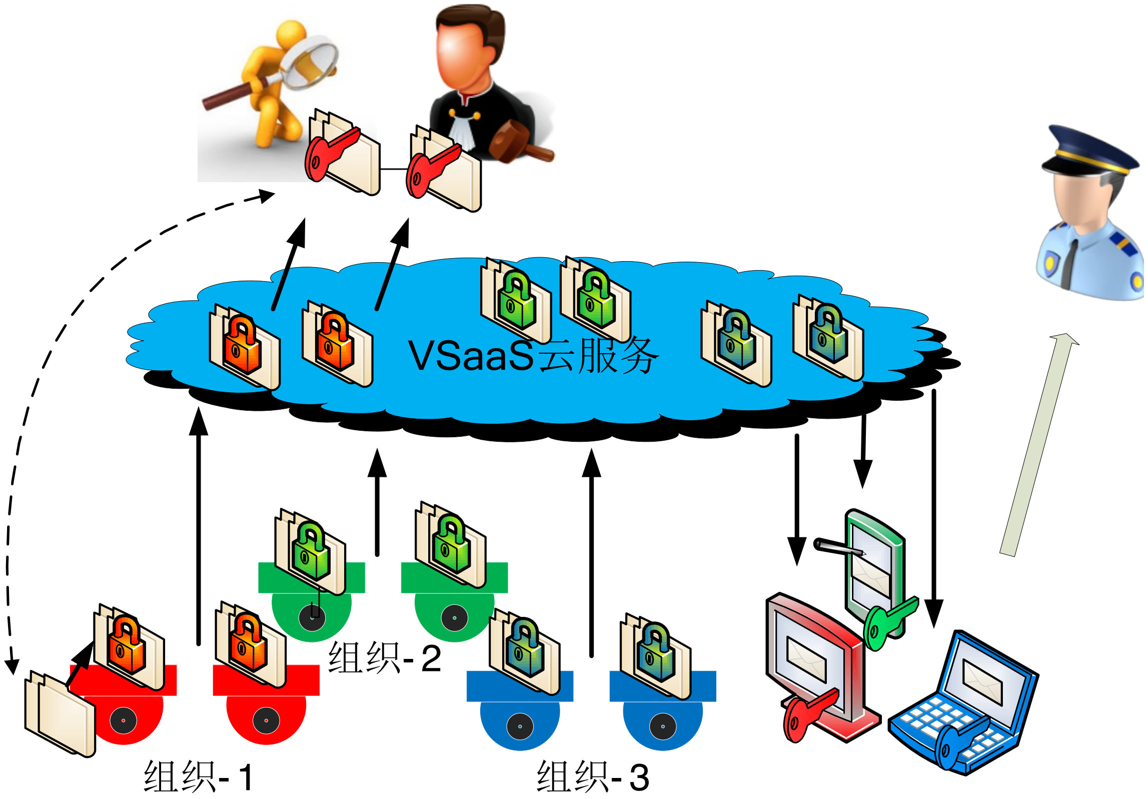


Evaluation

- Intelligibility / Unintelligibility
- Cryptographic Security
- Compression Efficiency
- Computational Complexity
- Integration in Existing Surveillance Architecture / Utility for Surveillance
- Full reversibility
  - the recovery of the unaltered original compressed video for the authorized users
  - surveillance videos can be considered as "proof of evidence/occurrence" if and only if their origin and integrity can be trusted
  - Hasn't been achieved efficiently

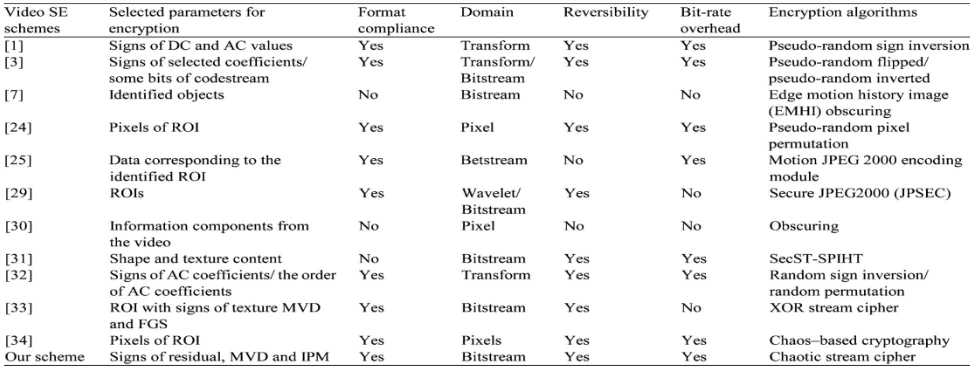
无损的区域加密

- 云端：
  - 隐私区域不可见
  - 非隐私区域可见
- 授权用户
  - 恢复监控摄像头录制的原始压缩视频



基于对象的区域加密

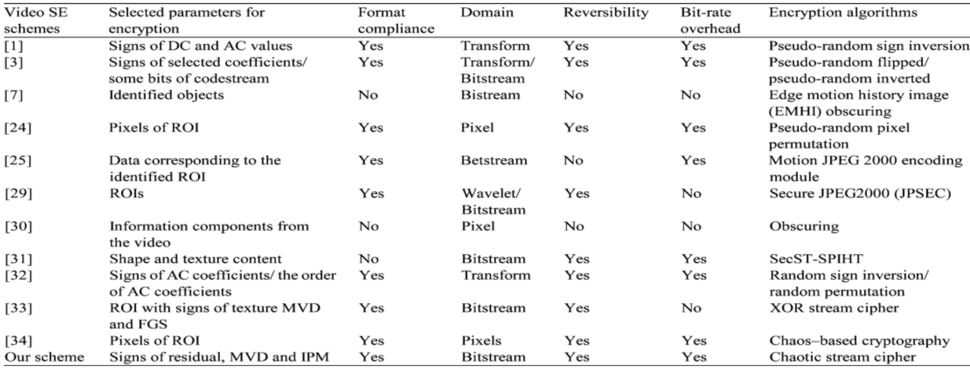
- 根据在视频压缩的哪个过程中实现来分类
  - **空域**:扰乱后压缩。影响压缩效率。
  - **变换域**：压缩过程中扰乱。需要修改编码器，且速度慢。
  - **压缩域**：压缩后扰乱。比特流中不同部分的依赖关系被破坏。



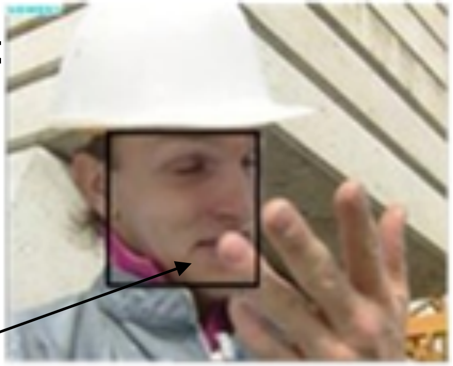
Video SE schemes	Selected parameters for encryption	Format compliance	Domain	Reversibility	Bit-rate overhead	Encryption algorithms
[1]	Signs of DC and AC values	Yes	Transform	Yes	Yes	Pseudo-random sign inversion
[3]	Signs of selected coefficients/ some bits of codestream	Yes	Transform/ Bitstream	Yes	Yes	Pseudo-random flipped/ pseudo-random inverted
[7]	Identified objects	No	Bistream	No	No	Edge motion history image (EMHI) obscuring
[24]	Pixels of ROI	Yes	Pixel	Yes	Yes	Pseudo-random pixel permutation
[25]	Data corresponding to the identified ROI	Yes	Betstream	No	Yes	Motion JPEG 2000 encoding module
[29]	ROIs	Yes	Wavelet/ Bitstream	Yes	No	Secure JPEG2000 (JPSEC)
[30]	Information components from the video	No	Pixel	No	No	Obscuring
[31]	Shape and texture content	No	Bitstream	Yes	Yes	SecST-SPIHT
[32]	Signs of AC coefficients/ the order of AC coefficients	Yes	Transform	Yes	Yes	Random sign inversion/ random permutation
[33]	ROI with signs of texture MVD and FGS	Yes	Bitstream	Yes	No	XOR stream cipher
[34]	Pixels of ROI	Yes	Pixels	Yes	Yes	Chaos–based cryptography
Our scheme	Signs of residual, MVD and IPM	Yes	Bitstream	Yes	Yes	Chaotic stream cipher

基于对象的区域加密

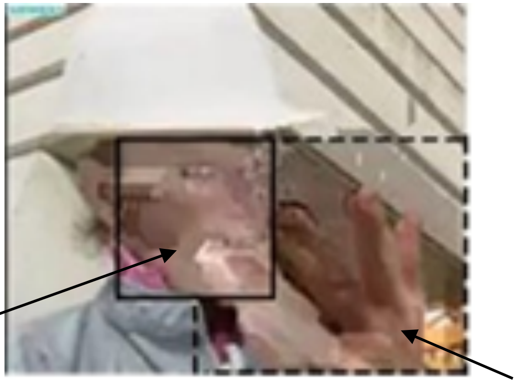
- 根据在视频压缩的哪个过程中实现来分类
  - **<u>空域</u>**:扰乱后压缩。影响压缩效率。
  - **<u>变换域</u>**：压缩过程中扰乱。
  - **<u>压缩域</u>**：压缩后扰乱。
    - 需解决问题：非隐私区域失



Video SE schemes	Selected parameters for encryption	Format compliance	Domain	Reversibility	Bit-rate overhead	Encryption algorithms
[1]	Signs of DC and AC values	Yes	Transform	Yes	Yes	Pseudo-random sign inversion
[3]	Signs of selected coefficients/ some bits of codestream	Yes	Transform/ Bitstream	Yes	Yes	Pseudo-random flipped/ pseudo-random inverted
[7]	Identified objects	No	Bistream	No	No	Edge motion history image (EMHI) obscuring
[24]	Pixels of ROI	Yes	Pixel	Yes	Yes	Pseudo-random pixel permutation
[25]	Data corresponding to the identified ROI	Yes	Betstream	No	Yes	Motion JPEG 2000 encoding module
[29]	ROIs	Yes	Wavelet/ Bitstream	Yes	No	Secure JPEG2000 (JPSEC)
[30]	Information components from the video	No	Pixel	No	No	Obscuring
[31]	Shape and texture content	No	Bitstream	Yes	Yes	SecST-SPIHT
[32]	Signs of AC coefficients/ the order of AC coefficients	Yes	Transform	Yes	Yes	Random sign inversion/ random permutation
[33]	ROI with signs of texture MVD and FGS	Yes	Bitstream	Yes	No	XOR stream cipher
[34]	Pixels of ROI	Yes	Pixels	Yes	Yes	Chaos–based cryptography
Our scheme	Signs of residual, MVD and IPM	Yes	Bitstream	Yes	Yes	Chaotic stream cipher



视频
隐私区域



受保护的
隐私区域

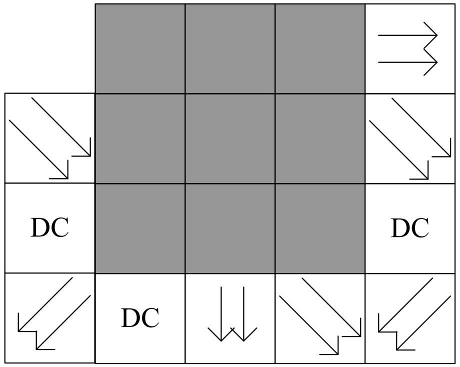
非隐私区域
失真现象

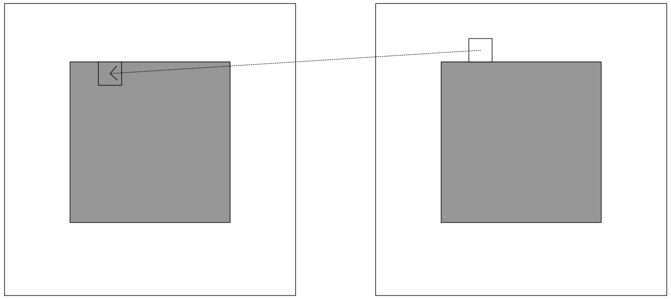
Why Drift?

- H.264
  - Intra-frame prediction to reduce the spatial redundancy
  - Inter-frame prediction to reduce the temporal redundancy

Distortion Drift

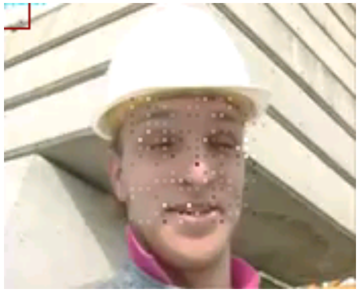
- If the privacy region is scrambled or encrypted
- If the block in the non-privacy region is predicted from the privacy region
- Distortion Drift in the non-privacy region
  - Intra
  - Inter



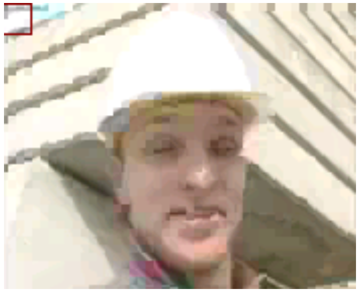


失真漂移与视觉安全

- 直接消除漂移?
  - 利用我们之前提出的漂移失真去除方法？



扰乱帧



预测帧

- 必须保留隐私区域的漂移失真以保护隐私区域视觉保密性，同时消除非隐私区域的漂移失真。

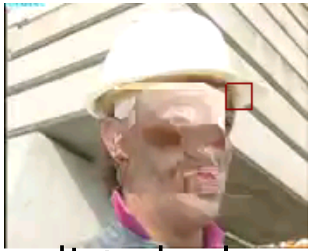
How to deal with it?

- Compensate the distortion drift in the non-privacy region after scrambling.

Intra-frame Compensation signal - an example

- MB(8,2), (0,0) .
- Prediction mode: 1 horizontal

Predicted value
(before scrambling)



Predicted value
(after scrambling)

Compensation signal in
the pixel domain

Compensation signal
in the compressed
domain

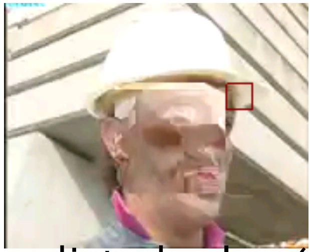
$$
\begin{matrix} 97, & 97, & 97, & 97 \\ 82, & 82, & 82, & 82 \\ 72, & 72, & 72, & 72 \\ 70, & 70, & 70, & 70 \end{matrix}
\quad - \quad
\begin{matrix} 79, & 79, & 79, & 79 \\ 73, & 73, & 73, & 73 \\ 90, & 90, & 90, & 90 \\ 132, & 132, & 132, & 132 \end{matrix}
\quad = \quad
\begin{matrix} 18, & 18, & 18, & 18 \\ 9, & 9, & 9, & 9 \\ -18, & -18, & -18, & -18 \\ -62, & -62, & -62, & -62 \end{matrix}
\quad \xrightarrow{\text{DCT, Q}} \quad
\begin{matrix} -2, & 0, & 0, & 0 \\ 4, & 0, & 0, & 0 \\ -1, & 0, & 0, & 0 \\ 0, & 0, & 0, & 0 \end{matrix}
$$

Add to the original quantized DCT coefficients.
Then current block is reconstructed after compensation. Move to the next compensation block.

Intra-frame Compensation Block Recovery - an example

- MB(8,2), (0,0) .
- Prediction mode: 1 horizontal

Predicted value (after de-scrambling)



Predicted value (before de-scrambling)

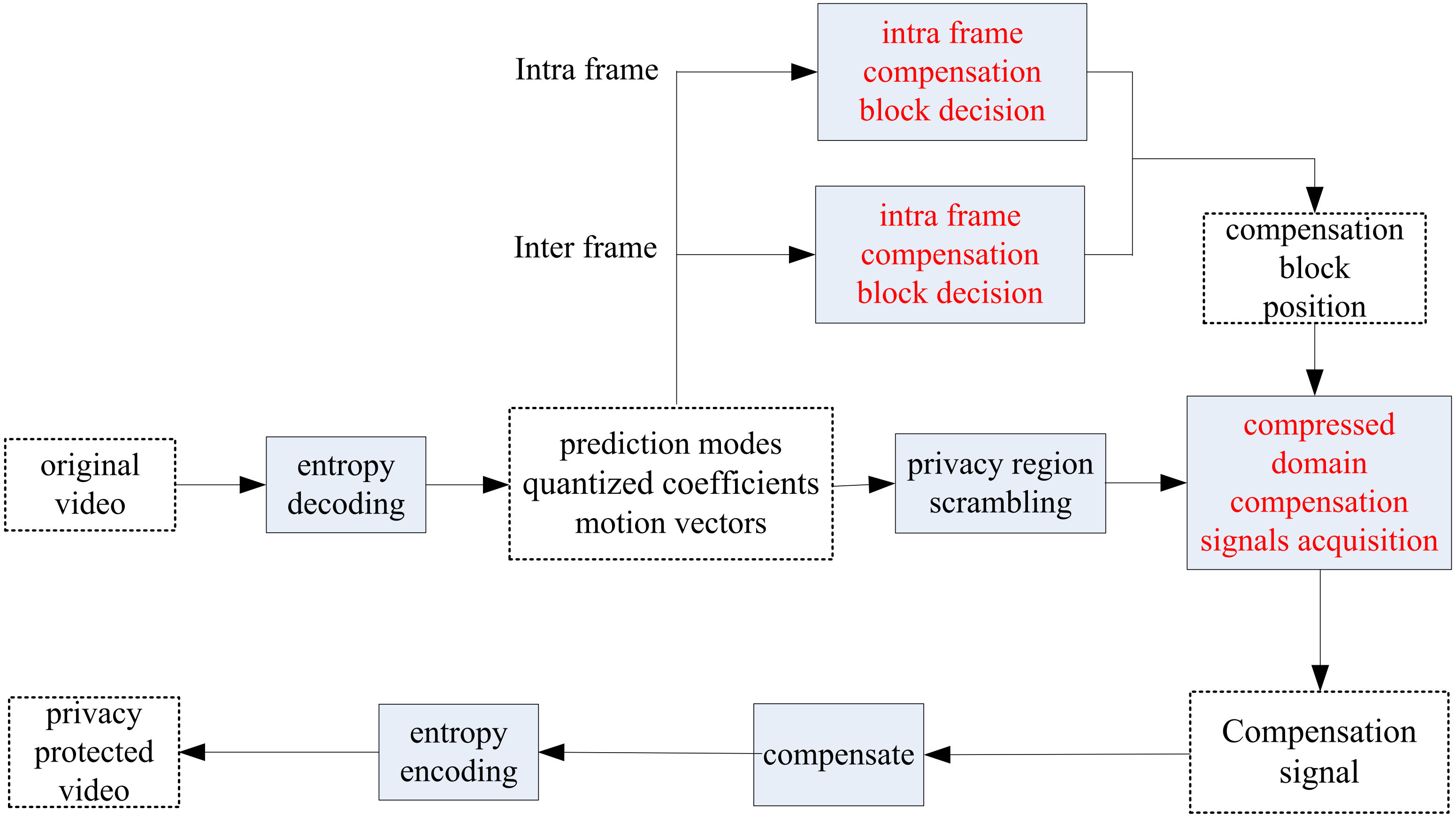
$$\begin{matrix} 97, & 97, & 97, & 97 \\ 82, & 82, & 82, & 82 \\ 72, & 72, & 72, & 72 \\ 70, & 70, & 70, & 70 \end{matrix} \quad - \quad \begin{matrix} 79, & 79, & 79, & 79 \\ 73, & 73, & 73, & 73 \\ 90, & 90, & 90, & 90 \\ 132, & 132, & 132, & 132 \end{matrix} \quad = \quad \begin{matrix} 18, & 18, & 18, & 18 \\ 9, & 9, & 9, & 9 \\ -18, & -18, & -18, & -18 \\ -62, & -62, & -62, & -62 \end{matrix} \quad \xrightarrow{\text{DCT, Q}} \quad \begin{matrix} -2, & 0, & 0, & 0 \\ 4, & 0, & 0, & 0 \\ -1, & 0, & 0, & 0 \\ 0, & 0, & 0, & 0 \end{matrix}$$

Subtract from the compensated quantized DCT coefficients, get the original quantized DCT coefficients.
Then current block is reconstructed (recovered). Move to the next compensation block.

Main Idea

- Scrambling in the compressed domain
  - DCT, IPM, MV et al.
- Compensation in the compressed form
  - Find the directly affected blocks (intra, inter)
  - Get the difference of the predicted values before and after scrambling, then compensate in the compressed domain
- Recovery
  - Get the difference of the predicted values before and after de-scrambling
  - Remove the compensation signal in the compressed domain

Framework


Intra frame
intra frame compensation block decision
Inter frame
intra frame compensation block decision
compensation block position
original video
entropy decoding
prediction modes quantized coefficients motion vectors
privacy region scrambling
compressed domain compensation signals acquisition
privacy protected video
entropy encoding
compensate
Compensation signal

Framework-Scrambling

1. Find the compensation blocks
   - I frame, based on Intra-frame prediction modes
   - P frame, based on MV.
2. Scrambling the privacy region
   - Random sign inversion of quantized DCT Coefficients
3. Get the compensation signal of the first compensation block in I frame
   - Get the difference of the predicted block before and after scrambling.
   - DCT and quantization.
   - Add to the original quantized DCT coefficients.
   - Reconstruct the compensated version of current block
4. Get the compensation signal of next compensation block in I frame
   - Get the difference of the predicted block before and after scrambling.
   - DCT and quantization.
   - Add to the original quantized DCT coefficients.

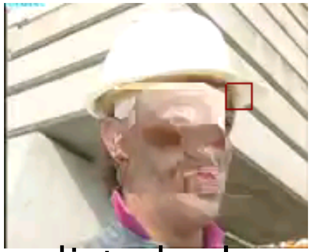
……

5. Get the compensation signal of compensation blocks in P frames and compensate them (frame by frame).

Intra-frame Compensation signal - an example

- MB(8,2), (0,0) .
- Prediction mode: 1 horizontal

Predicted value (before scrambling)



Predicted value (after scrambling)

Compensation signal in the pixel domain

Compensation signal in the compressed domain

$$\begin{matrix}97, 97, 97, 97\\ 82, 82, 82, 82\\ 72, 72, 72, 72\\ 70, 70, 70, 70\end{matrix} \; - \; \begin{matrix}79, 79, 79, 79\\ 73, 73, 73, 73\\ 90, 90, 90, 90\\ 132, 132, 132, 132\end{matrix} \; = \; \begin{matrix}18, 18, 18, 18\\ 9, 9, 9, 9\\ -18, -18, -18, -18\\ -62, -62, -62, -62\end{matrix} \; \xrightarrow{\text{DCT, Q}} \; \begin{matrix}-2, 0, 0, 0\\ 4, 0, 0, 0\\ -1, 0, 0, 0\\ 0, 0, 0, 0\end{matrix}$$

Add to the original quantized DCT coefficients.

Then current block is reconstructed after compensation. Move to the next compensation block.

Framework- Recovery

1. Find the compensation blocks
   - I frame, based on Intra-frame prediction modes
   - P frame, based on MV.
2. De-scrambling the privacy region
3. Get the compensation signal of the first compensation block
   - Get the difference of the predicted block before and after de-scrambling.
   - DCT and quantization.
   - Remove the compensation signal from the quantized DCT coefficients.
   - Reconstruct current block—recovery the original one. (The predicted value is the same to the original, the recovered residual Quantized DCT coefficients is the original).
4. Get the compensation signal of next compensation block
   - Get the difference of the predicted block before and after de-scrambling.
   - DCT and quantization.
   - Remove the compensation signal from the quantized DCT coefficients.
   - Reconstruct this block—recovery the original one. (The predicted value is the same to the original, the recovered residual Quantized DCT coefficients is the original).

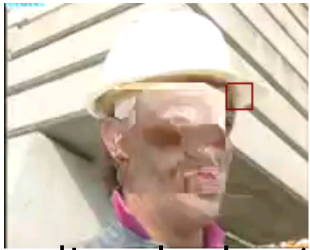
……

5. Get the compensation signal of compensation blocks in P frames, and recover them (frame by frame).

Intra-frame Compensation Block Recovery - an example

- MB(8,2), (0,0) .
- Prediction mode: 1 horizontal

Predicted value (after de-scrambling)



Predicted value (before de-scrambling)

$$\begin{matrix} 97, 97, 97, 97 \\ 82, 82, 82, 82 \\ 72, 72, 72, 72 \\ 70, 70, 70, 70 \end{matrix} - \begin{matrix} 79, 79, 79, 79 \\ 73, 73, 73, 73 \\ 90, 90, 90, 90 \\ 132,132,132,132 \end{matrix} = \begin{matrix} 18, 18, 18, 18 \\ 9, 9, 9, 9 \\ -18,-18,-18,-18 \\ -62,-62,-62,-62 \end{matrix} \xrightarrow{\text{DCT, Q}} \begin{matrix} -2, 0, 0, 0 \\ 4, 0, 0, 0 \\ -1, 0, 0, 0 \\ 0, 0, 0, 0 \end{matrix}$$

Subtract from the compensated quantized DCT coefficients, get the original quantized DCT coefficients.
Then current block is reconstructed (recovered). Move to the next compensation block.

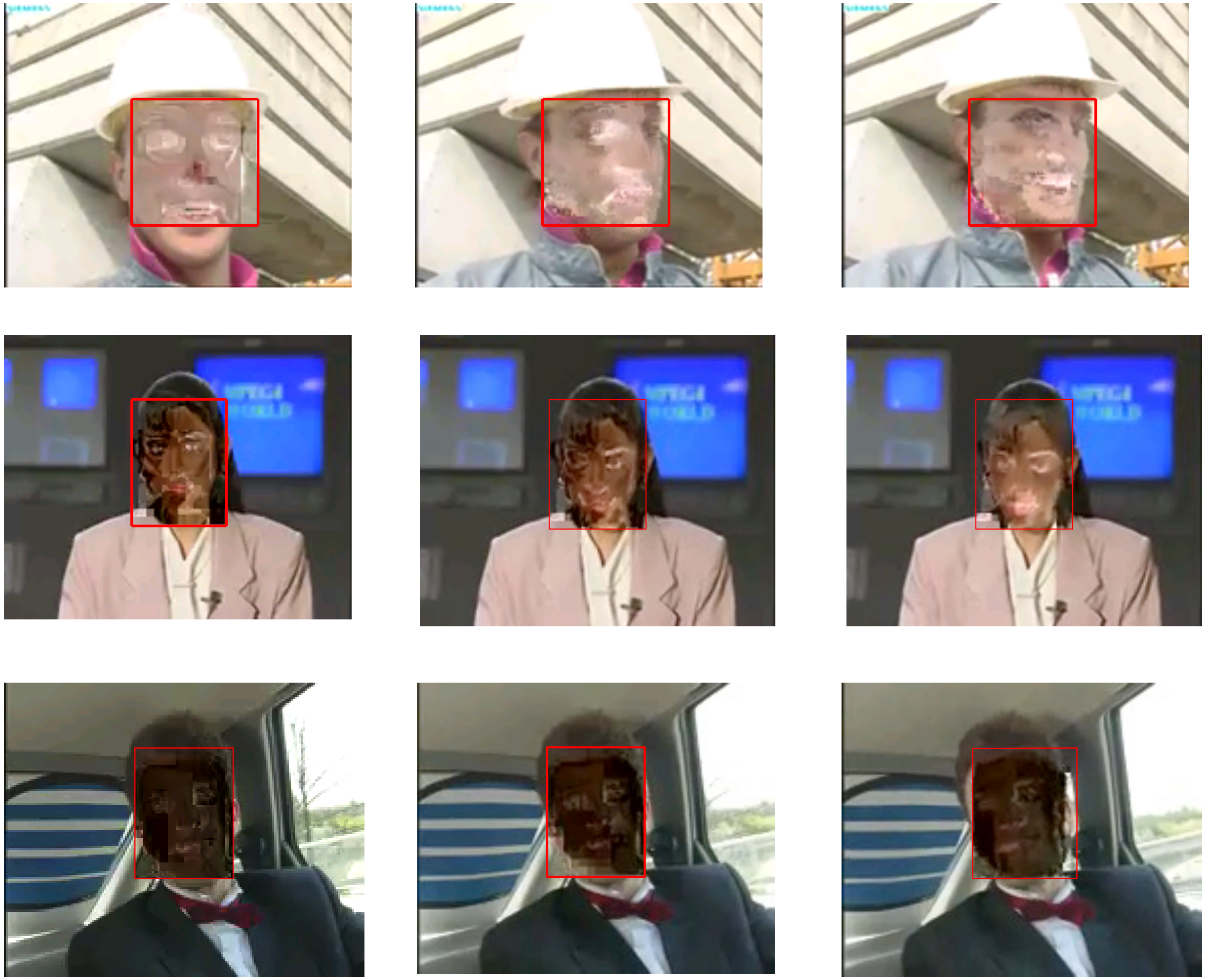
Extension Discussion

- Scramble IPM/MV.
- Intra-frame Prediction Modes (IPM) and Motion Vectors (MV) are encoded in a predicted manner.
  - Each IPM/MV is predicted from IPM/MV of nearby, previously coded blocks/partitions.
  - The difference between the current IPM/MV and the predicted IPM/MV is encoded and transmitted.
- Thus, the codes corresponding to IPM/MV should be updated after scrambling.
- Since the prediction information of non-privacy region is preserved, the authorized user can still find the compensation block and can recover the original compressed video.

小结

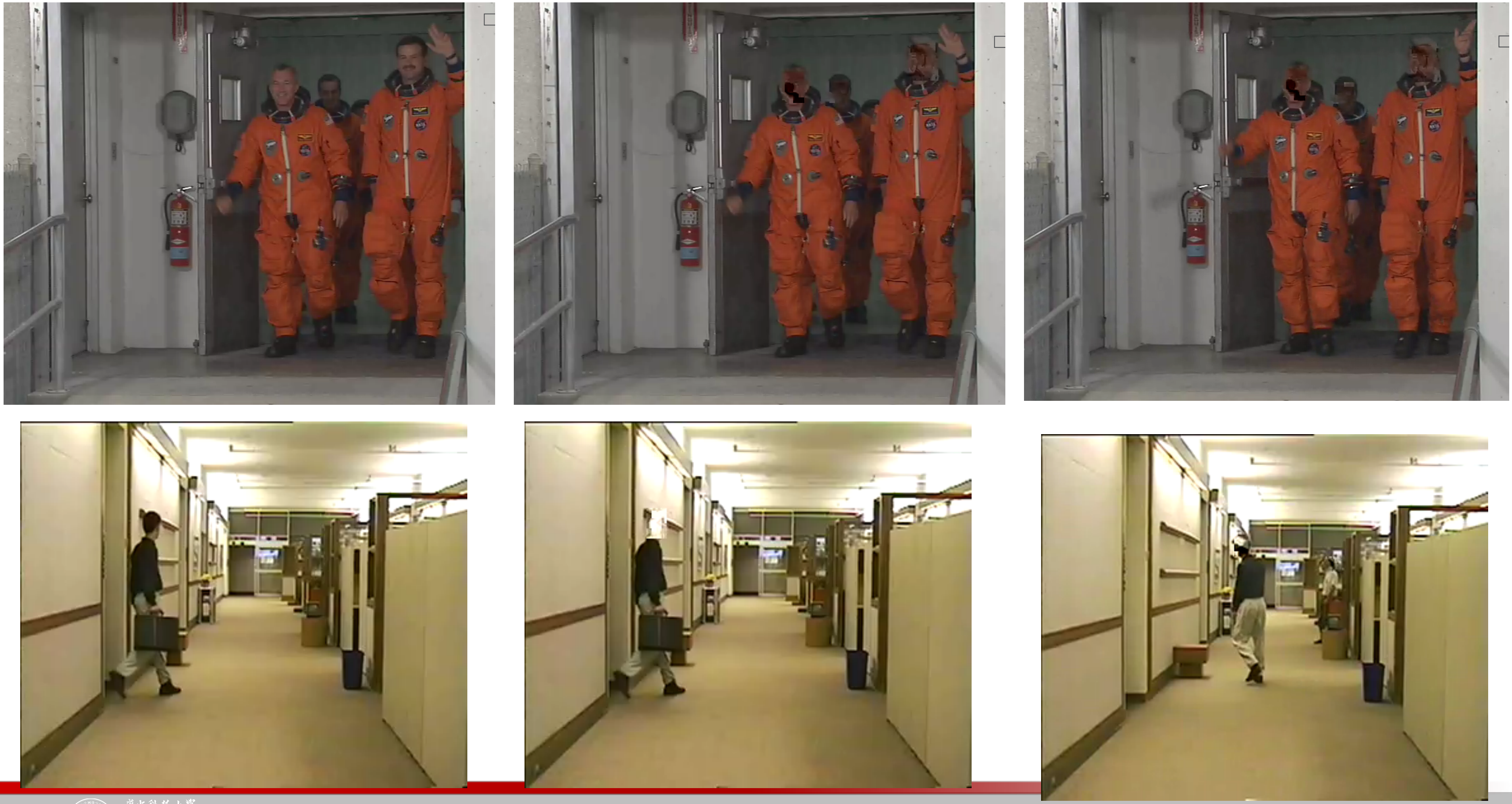
- 解决思路
  - 隔离有损重编码
    - 在压缩域进行隐私保护：加密系数符号与帧内预测模式
    - 在压缩域解决非隐私区域失真问题
  - 根据预测值之差计算压缩域补偿信号
  - 逐块处理。补偿并重建后再处理下一块，可保证加密与解密时预测值之差一致。
  - 解密恢复时同样逐块处理，根据预测值之差计算并移除压缩域补偿信号。
  - 解决了帧内与帧间漂移问题。

Experimental Results



Experimental Results

- 视觉效果



Experimental Results

PSNR of privacy region

Test sequence	QP=20	QP=28	QP=33	QP=40
Forman	16.88	16.88	16.87	12.47
Akiyo	10.97	12.36	10.60	9.84
Claire	11.52	11.33	9.69	10.93
Carphone	11.55	12.40	10.60	9.84

PSNR of non-privacy region

Test sequence	QP=20	QP=28	QP=33	QP=40
Forman	50.32	35.94	41.98	38.10
Akiyo	40.25	39.40	42.84	35.07
Claire	50.39	44.29	42.37	39.31
Carphone	49.14	46.48	42.84	35.07

SSIM of privacy region

Test sequence	QP=20	QP=28	QP=33	QP=40
Forman	0.37	0.37	0.31	0.32
Akiyo	0.11	0.17	0.12	0.10
Claire	0.12	0.10	0.17	0.10
Carphone	0.11	0.10	0.15	0.10

SSIM of non-privacy region

Test sequence	QP=20	QP=28	QP=33	QP=40
Forman	0.99	0.99	0.99	0.98
Akiyo	0.99	0.99	0.99	0.98
Claire	0.99	0.99	0.99	0.99
Carphone	0.99	0.99	0.99	0.98

Experimental Results

Bit rate over head with QP 28(kb/s)

Test sequence	Unscrambled video	Proposed method	Over head
Foreman	151.50	156.80	3.50%
Akiyo	39.22	40.40	3.00%
Claire	45.25	46.93	3.72%
Carphone	114.11	117.81	3.24%

Experimental Results

Time consumption comparison (ms/frame)

Test sequence	Exisiting Method	Proposed method
Forman	5763.70	46.82
Akiyo	5356.53	26.78
Claire	5506.92	27.53
Carphone	6081.33	47.36

思考？

- Fully Reversible Privacy Protection for H.264 compressed Surveillance Video
- Quick
  - Preserve the prediction information, avoid re-encoding
- Can be easily integrated to the existing video surveillance system
- 进一步思考？