CARINTHIA TECH INSTITUTE

Confidential Transmission of Lossless Visual Data: Experimental Modelling and Optimization

KÄRNTEN

Outline

1. Introduction
2. Basic Building Blocks
   - » Lossless Compression
   - » Encryption
   - » Transmission
3. Cost Optimal Configuration of Confidential Visual Data Transmission
4. Conclusion
5. Future work

1. Introduction

- Large amounts of visual content in worldwide distributed database infrastructures

  →urgent need to provide and protect the confidentiality of sensitive visual data when transmitting it over networks of any kind

1. Introduction

- Focused on computationally efficient schemes in a lossless online scenario
  - » Compression factor for visual data
    - – lossless formats: 2 to 3
    - – lossy formats: > 100
  - » Reasons why lossless formats may be preferable
    - – Loss of image data is not acceptable
    - – Low processing power or limited energy ressources
    - – High bandwidth at the communication channel

1. Introduction

- Tried to optimize the interplay of the 3 main steps
  - » Compression
  - » Encryption
  - » Transmission

- Minimal computational effort and energy consumption

1. Introduction

- Modelled costs based on exemplary experimental data
- Derived a cost optimal strategy in the target environment

  Is the compression stage required in any case to result in an overall cost optimal scheme or not?

- Additionally we considered ‚Selective Encryption‘
  - » To trade off computational compexity for security

1.1. Selective Encryption

- Application specific data structures are exploited to create more efficient encryption systems
- Protect the visually most important parts of an image
- Relying on a secure but slow ‚classical' cipher

2. Basic Building Blocks

- The processing chain has always a fixed order
- Compression has to be performed prior to encryption
  - » statistical properties of encrypted data prevent compression from being applied successfully
  - » reduced amount of data decreases the computational demand
- Hardware platform:
  - » 996 MHz Intel Pentium III
  - » 128 MB RAM
- Network
  - » 100 MBit/s Ethernet

2.1. Lossless Compression

- JBIG reference implementation in a selective mode
  - » compression of a different amount of bitplanes of 8 bpp greyscale images
  - » scheme ranges from applying no compression at all to compressing a certain number of bitplanes
    - – started from the MSB bitplane
- instead of applying JBIG to all bitplanes JPEG 2000 in lossless mode was used
  - » compression results were better as compared to full JBIG coding

2.1. Lossless Compression

- 20 test images in 2 sizes
- obtained files sizes and compression timings were averaged for
  - » 512 x 512
  - » 1280 x 1024
- approximate interpolation of the measurement points by a 6th order polynomial
- resulted in the following formulas

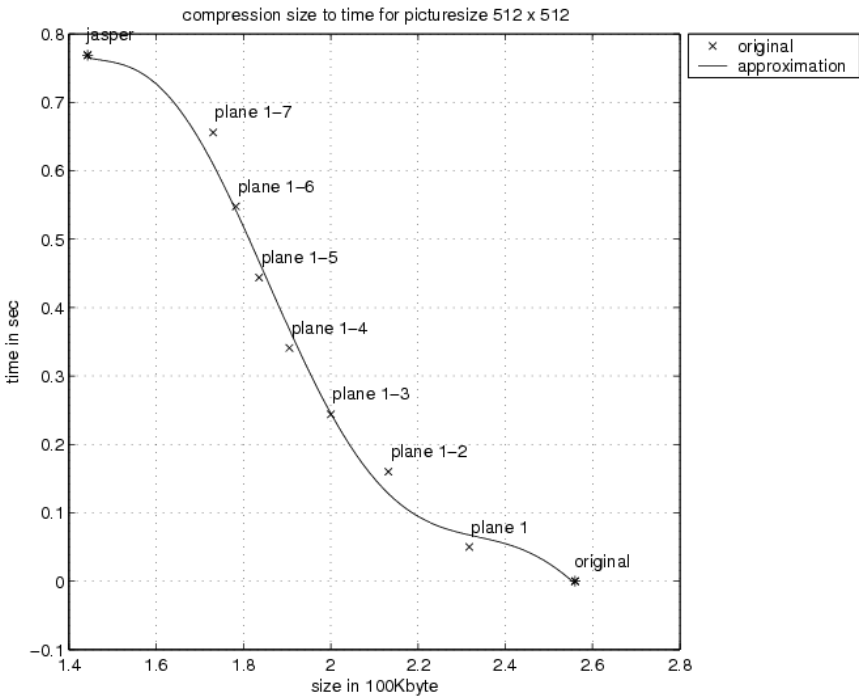
$$t = 7.32x^6 - 90.89x^5 + 463.02x^4 - 1237.72x^3 + 1829.28x^2 - 1417.22x + 450.73$$

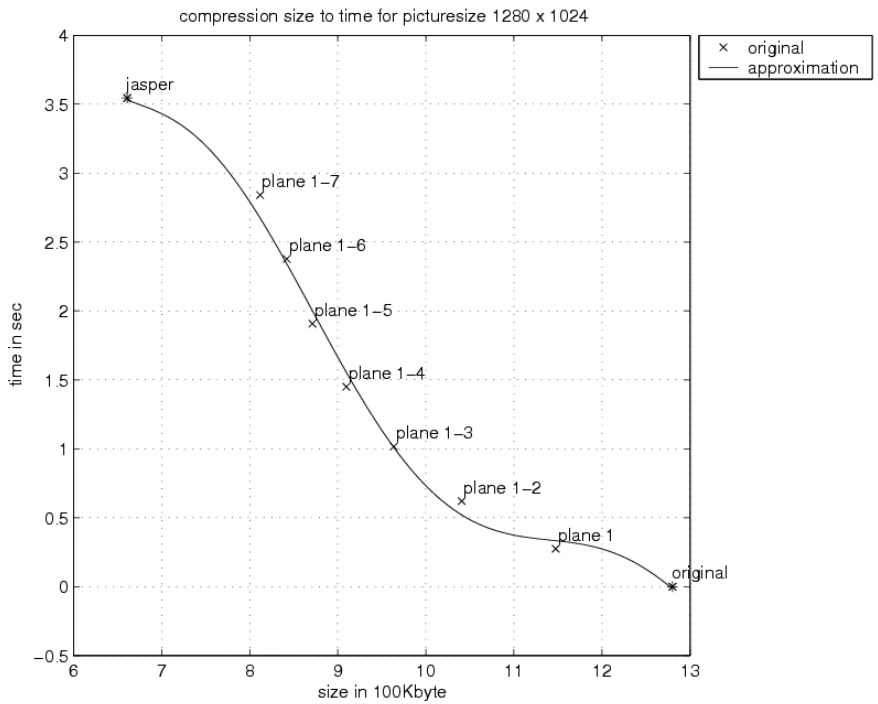
$$t = -0.07x^5 + 1.73x^4 - 21.99x^3 + 153.94x^2 - 562.09x + 841.21$$

x … resulting data size in 100 KByte after compression
t … compression time in seconds

2.1. Lossless Compression

Tradeoff between compression timings and the resulting data amount after compression





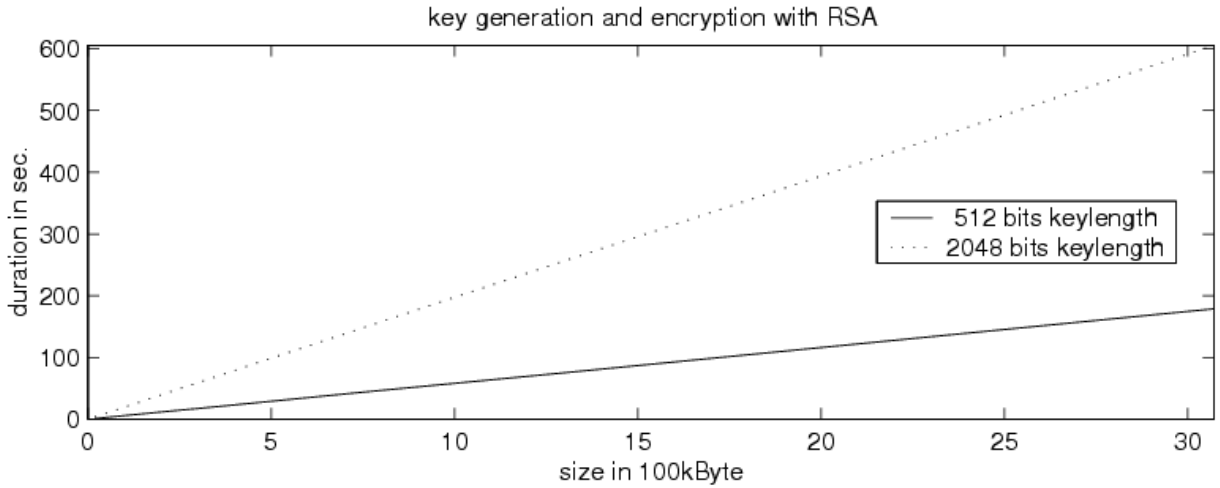
→ decreasing compression time for increasing data size

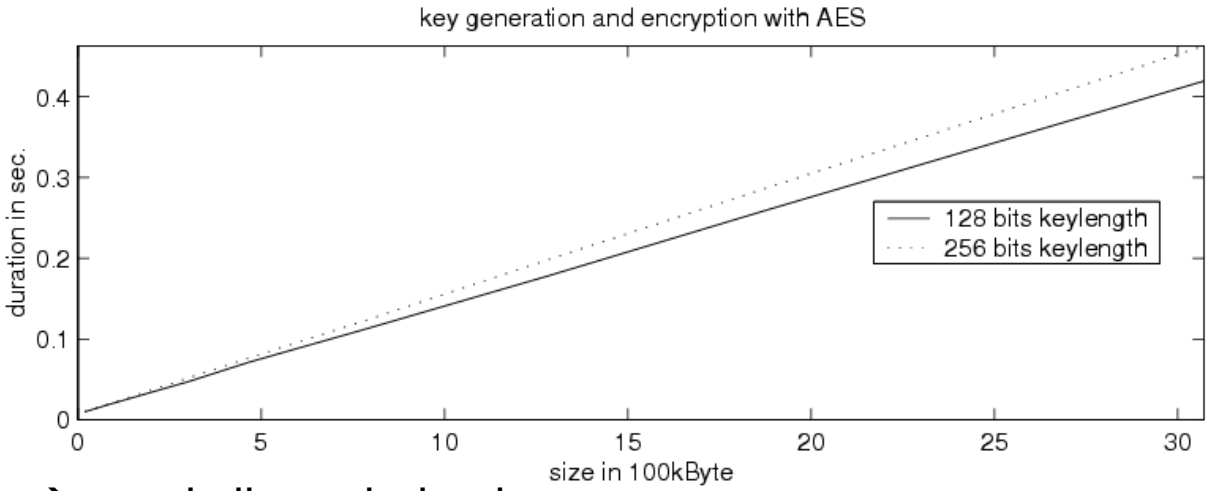
2.2. Encryption

- C++ RSA and C++ AES implementation
- RSA - for reasons of obtaining a rich variety in the overall behaviour of the processing chain
  - » In practice you hardly use public-key systems to encrypt visual data
  - » Time demand of RSA is several orders of magnitude higher as compared to AES
  - » Performance differences among encryption schemes with the exhibited magnitude could result from applying hardware or software based approaches in real-life systems

2.2. Encryption

Amount of data encrypted in relation to processing time





$t = 5.81x \quad (RSA \quad 512bit)$

$t = 19.72x \quad (RSA \quad 2048bit)$

$t = 0.01x \quad (AES \quad 128bit)$

$t = 0.02x \quad (AES \quad 256bit)$

→ purely linear behaviour

2.3. Transmission

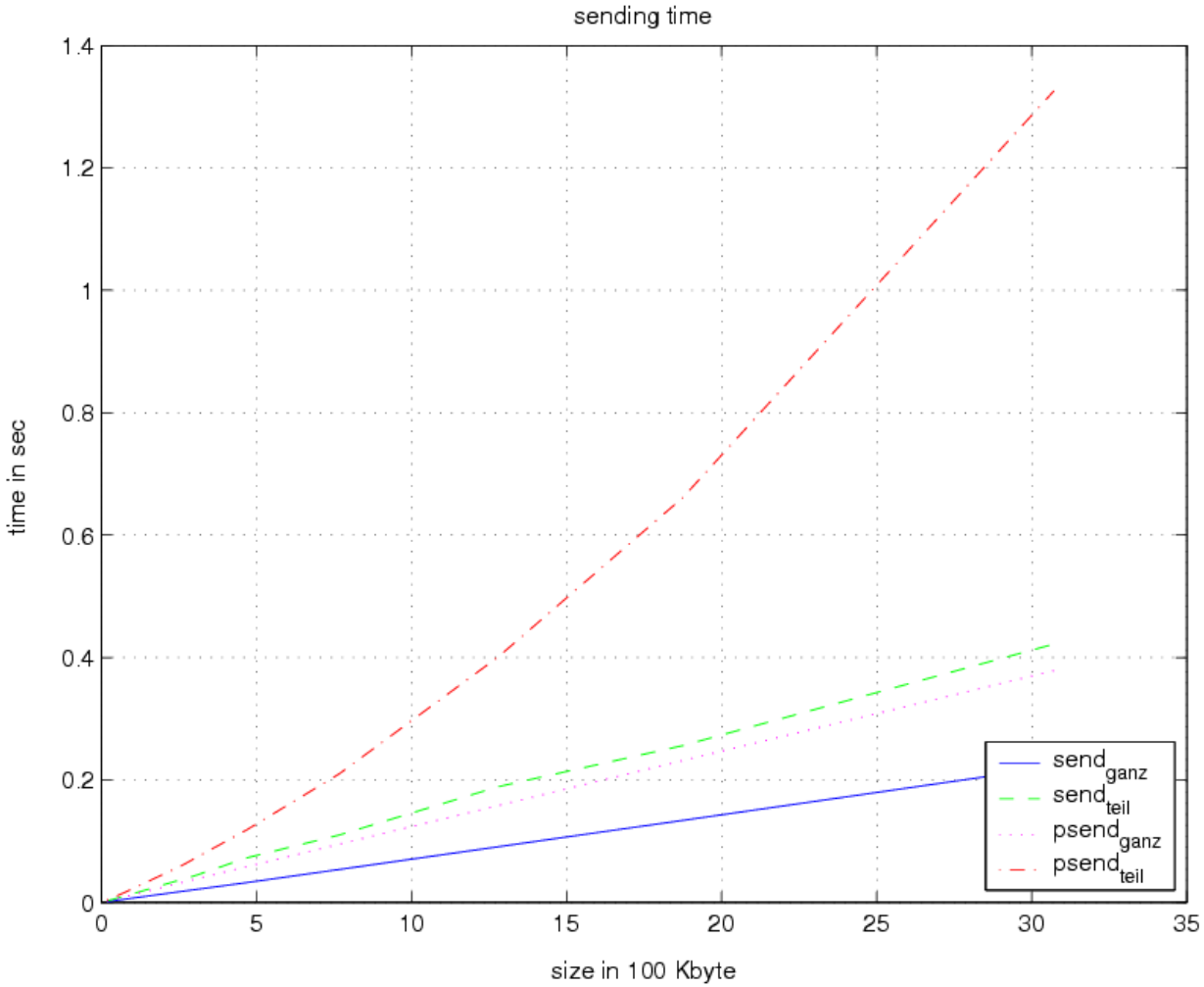
- Message passing library PVM

- 4 different modes
  - » pvm_send - sends a message stored in the active send buffer to the PVM process identified by tid
  - » pvm_psend - takes a pointer to a buffer buf, its length len, and its data type datatype and sends this data directly to the PVM task indentified by tid
  - » ganz - data is sent as a whole block
  - » teil – data is sent in pieces of 1 KByte

- Again data size is varied and the time required to transmit the data is measured and fitted by a polynomial

2.3. Transmission

Transmission time related to data size



$t = 0.01x$ $(pvm\_send,\ teil)$

$t = 0.02x$ $(pvm\_psend,\ teil)$

$t = 0.007x$ $(pvm\_send,\ ganz)$

$t = 0.01x$ $(pvm\_psend,\ ganz)$

2.3. Transmission

- AES encryption and transmission operate on a similar level of time demand
- RSA is much more expensive
- As expected both processing stages exhibit linear behaviour

3. Cost Optimal Configuration of Confidential Visual Data Transmission

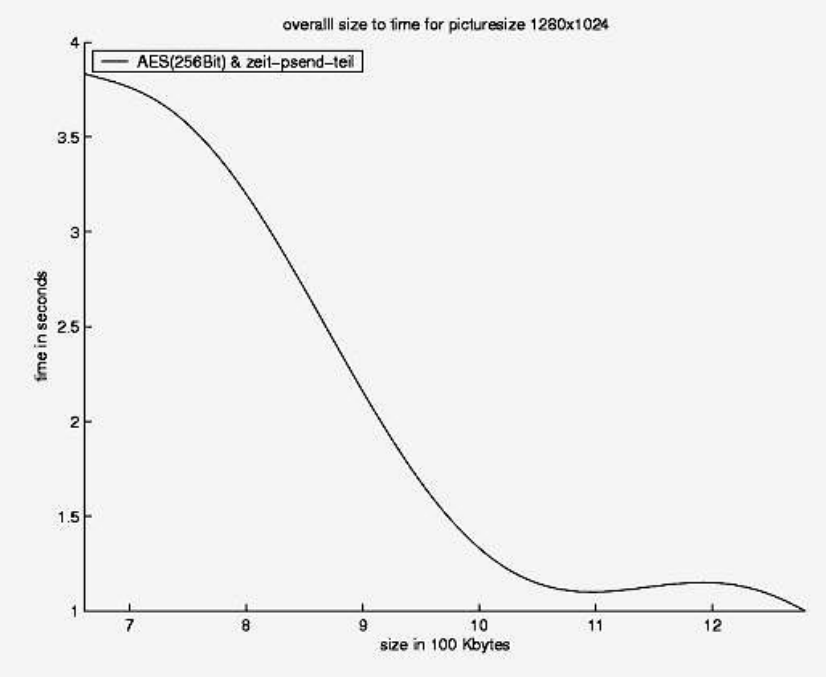
- Processing chain: compression – encryption – transmission has a fixed order but keeps a certain scope in the degree of execution (e.g. SE)

- Constrictions:
  - » Level of complexity (compression)
  - » Level of security (encryption)
  - » Limited transmission bandwidth (transmission)

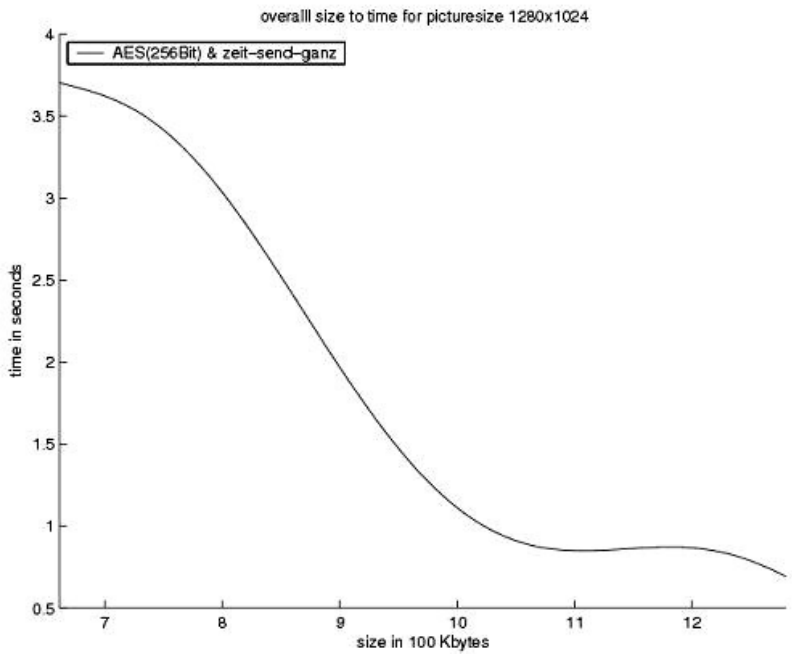
- Goal: Identify the cost optimal way (in terms of processing time) to operate the processing chain

3. Cost Optimal Configuration of Confidential Visual Data Transmission

- First configuration
  Image: 1280 x 1024 image
  Cipher: AES



(a) AES(256) with PVM mode psend_teil



(b) AES(256) with PVM mode send_ganz

3. Cost Optimal Configuration of Confidential Visual Data Transmission

- First configuration

  Image: 1280 x 1024 image

  Cipher: AES

  » *Overall behaviour are almost identical to the approximated interpolation of the modeling equation*

(a) $$t = -0.07x^5 + 1.73x^4 - 21.99x^3 + 153.94x^2 - 562.05x + 841.21$$

(b) $$t = -0.07x^5 + 1.73x^4 - 21.99x^3 + 153.94x^2 - 562.07x + 841.21$$

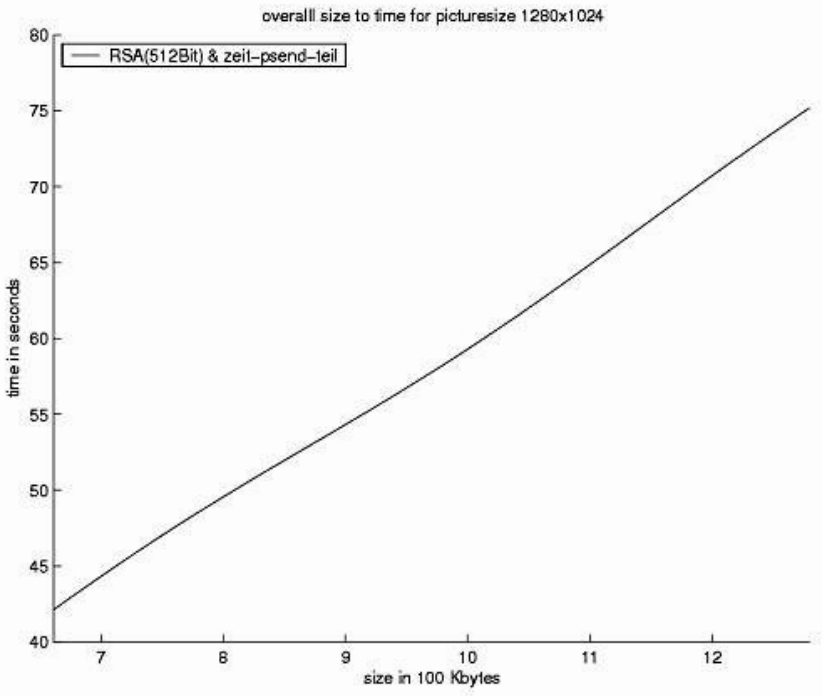
==> Optimal operation mode: ***No compression at all***

3. Cost Optimal Configuration of Confidential Visual Data Transmission

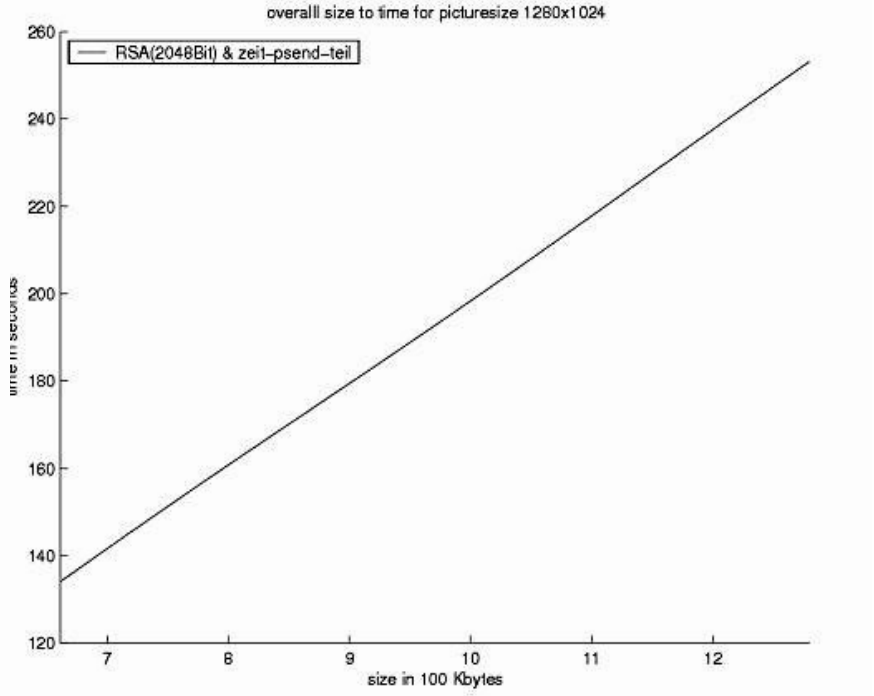
- Second configuration

  Image: 1280 x 1024 image

  Cipher: RSA



(a) RSA (512) with PVM mode psend_teil



(b) RSA(2048) with PVM mode send_ganz

3. Cost Optimal Configuration of Confidential Visual Data Transmission

- Second configuration

  Image: 1280 x 1024 image

  Cipher: RSA

  » *Curves monotonically increasing (unaffected by key size)*

(a) $t = -0.07x^5 + 1.73x^4 - 21.99x^3 + 153.94x^2 - 556.26x + 841.21$

(b) $t = -0.07x^5 + 1.73x^4 - 21.99x^3 + 153.94x^2 - 542.35x + 841.21$

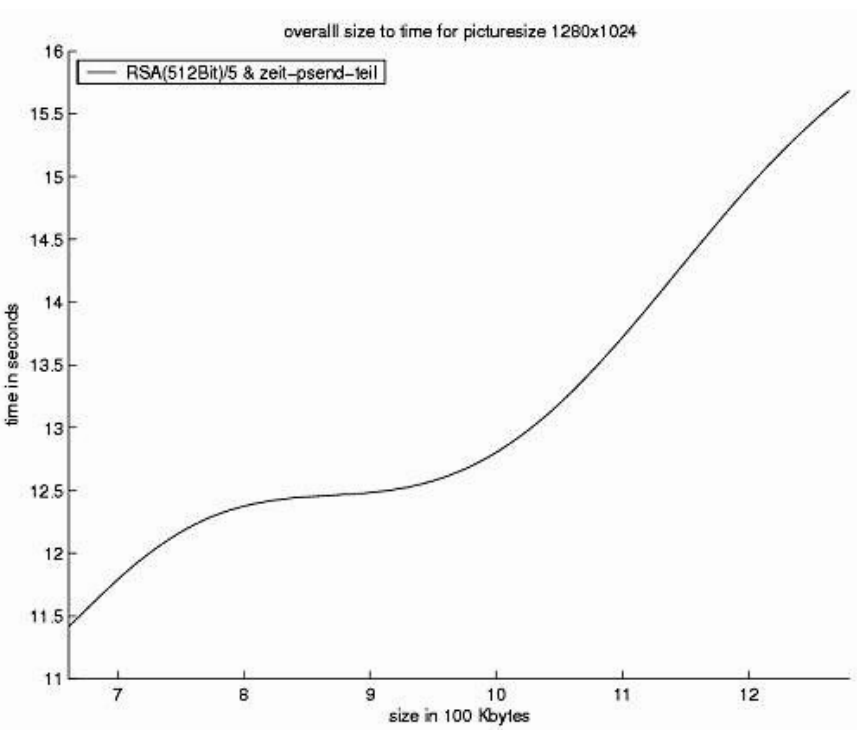
==> Optimal operation mode: ***Maximal compression***

3. Cost Optimal Configuration of Confidential Visual Data Transmission

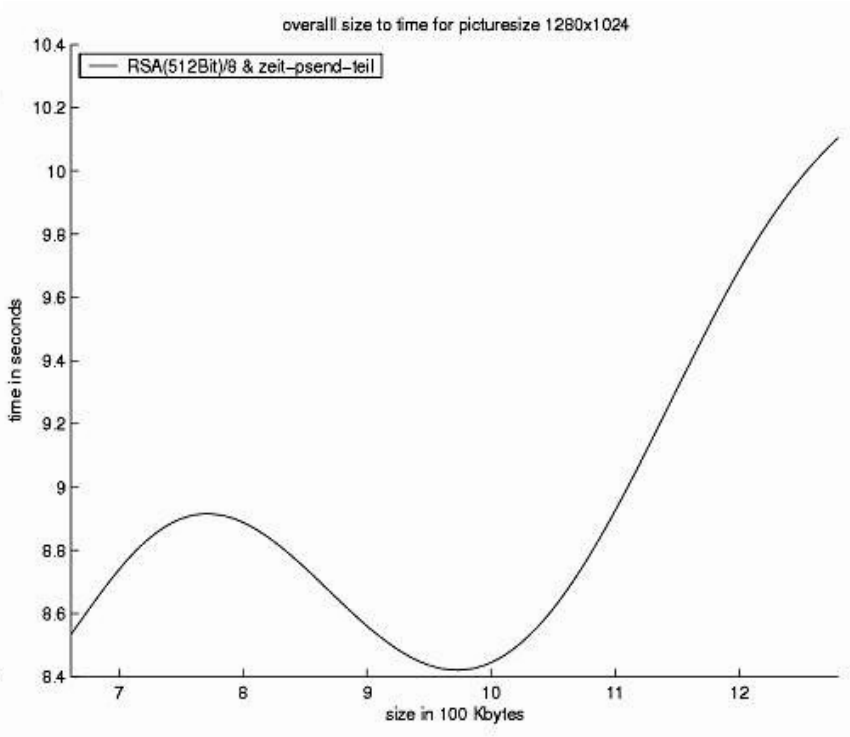
- Third configuration – Selective Encryption

  Image: 1280 x 1024 image

  Cipher: RSA (512bit key)



(a) 20% encrypted with mode psend_teil



(b) 12.5% encrypted with mode send_ganz

3. Cost Optimal Configuration of Confidential Visual Data Transmission

- Third configuration – Selective Encryption
  Image: 1280 x 1024 image
  Cipher: RSA (512bit key)

  » *Curve b (12.5% encryption) showing local minimum*

(b) $$t = 0.71x^5 + 1.73x^4 - 21.99x^3 + 153.94x^2 - 561.34x + 841.21$$

$$t' = 3.55x^4 + 6.91x^3 - 65.96x^2 + 307.88x - 561.34$$

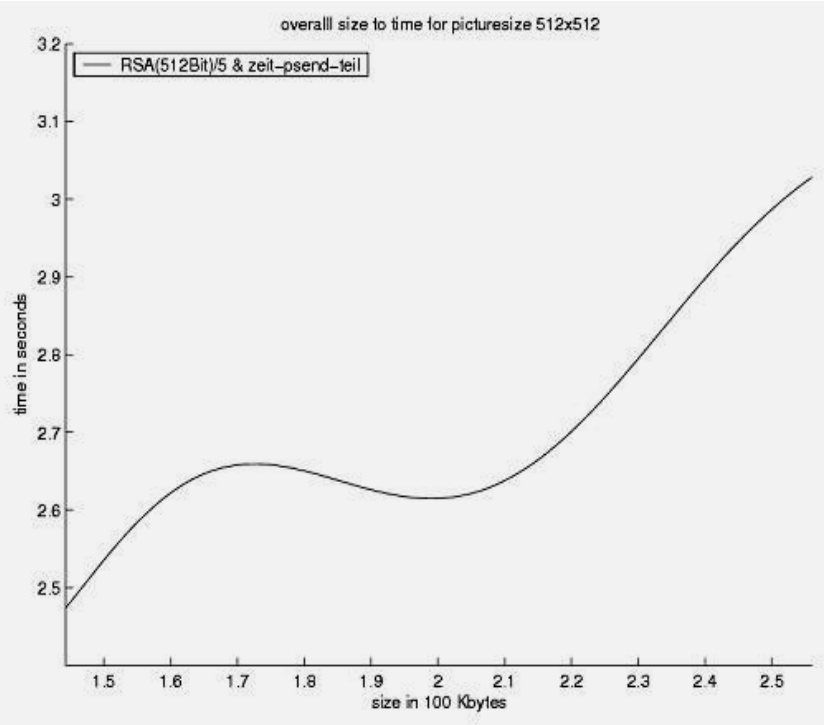
$$x_1 = 7.72$$
$$x_2 = \underline{9.71}$$

In the area of interest [6.6, 13]

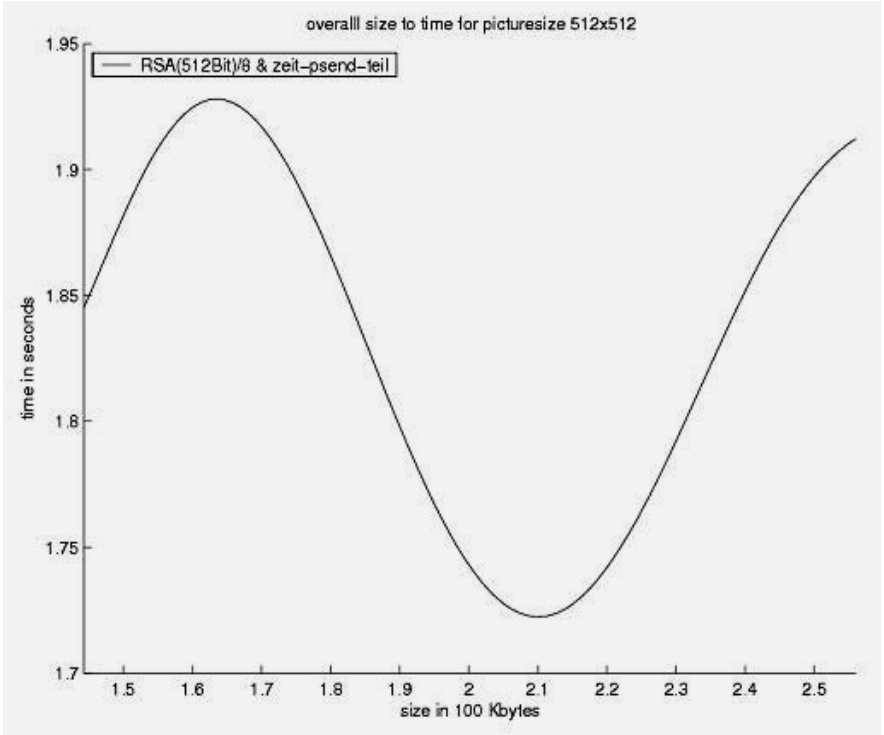
==> Optimal operation mode: ***Compression of 3 out of 8 bitplanes with JBIG***

3. Cost Optimal Configuration of Confidential Visual Data Transmission

- Fourth configuration – Selective Encryption
  Image: 512 x 512 image
  Cipher: RSA (512bit key)



(a) 20% encrypted with mode psend_teil



(b) 12.5% encrypted with mode send_ganz

3. Cost Optimal Configuration of Confidential Visual Data Transmission

- Third configuration – Selective Encryption
  Image: 512 x 512 image
  Cipher: RSA (512bit key)

  » *Curve b (12.5% encryption) showing local minimum*

(b) $t = 7.32x^6 - 90.89x^5 + 463.02x^4 + 1237.72x^3 1829.28x^2 - 1416.47x + 450.73$

$t' = 43.93x^5 - 454.43x^4 + 1852.1x^3 - 3713.16x^2 + 3658.56x - 1416.47$

$x_1 = 1.64$
$x_2 = \underline{2.10}$

In the area of interest [1.4, 2.6]

==> Optimal operation mode: ***Compression of 2 out of 8 bitplanes with JBIG***

4. Conclusion

- Introduced:
  - » Confidential transmission of visual data in lossless format
- Investigated:
  - » A model of the costs in the 3 main steps

    compression – encryption – transmission
- Depending on the type of encryption involved, the optimal configuration of the entire system may be to operate:
  - » Without compression
  - » Full compression
  - » Partial compression

5. Future Work

- Inclusion of constraints alleged by the target environment into the optimization:
  - » Limited bandwidth
  - » Certain level of security in selective encryption

- Modeling the dependency between selective compression and selective encryption

CARINTHIA TECH INSTITUTE

KÄRNTEN

Thanks for your attention