Context

Why protect ?

- Privacy, property, forgery
- Avoid leaks (or trace them)
  - Medical data
    (Greenbone Networks Study, september 2019)

Greenbone Networks Study, (september 2019)

Monde/France

- 399 M/2.94 M medical images
- 24 M/54.000 patient records
- 500 faulty servers
- DICOM (Protocol)

3D Protection

3D Data Hiding

- Watermarking
- High-Capacity Data Hiding
- Steganography

Selective Encryption

- Confidential Protection
- Sufficient Protection
- Transparent Protection

V. Favier, N. Zemiti, O. Caravaca Mora, G. Subsol, G. Captier, R. Lebrun, L. Crampette, M. Mondain, B. Gilles
"Geometric and mechanical evaluation of 3D-printing materials for skull base anatomical education and endoscopic surgery simulation - a first step to create reliable customized simulators".
PloS ONE, 12, December 2017.

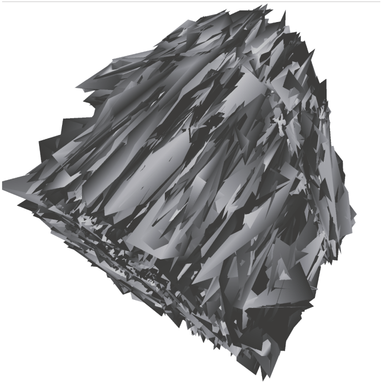
3D Protection

3D Data Hiding

- Watermarking
- High-Capacity Data Hiding
- Steganography

Selective Encryption

- Confidential Protection
- Sufficient Protection
- Transparent Protection



V. Favier, N. Zemiti, O. Caravaca Mora, G. Subsol, G. Captier, R. Lebrun, L. Crampette, M. Mondain, B. Gilles
"Geometric and mechanical evaluation of 3D-printing materials for skull base anatomical education and endoscopic surgery simulation - a first step to create reliable customized simulators".
PloS ONE, 12, December 2017.

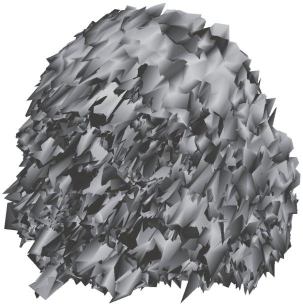
3D Protection

3D Data Hiding

- Watermarking
- High-Capacity Data Hiding
- Steganography

Selective Encryption

- Confidential Protection
- Sufficient Protection
- Transparent Protection



V. Favier, N. Zemiti, O. Caravaca Mora, G. Subsol, G. Captier, R. Lebrun, L. Crampette, M. Mondain, B. Gilles
"Geometric and mechanical evaluation of 3D-printing materials for skull base anatomical education and endoscopic surgery simulation - a first step to create reliable customized simulators".
PloS ONE, 12, December 2017.

3D Protection

3D Data Hiding

- Watermarking
- High-Capacity Data Hiding
- Steganography

Selective Encryption

- Confidential Protection
- Sufficient Protection
- Transparent Protection

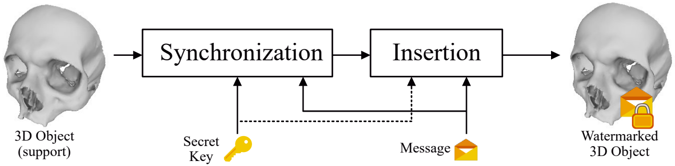
V. Favier, N. Zemiti, O. Caravaca Mora, G. Subsol, G. Captier, R. Lebrun, L. Crampette, M. Mondain, B. Gilles
"Geometric and mechanical evaluation of 3D-printing materials for skull base anatomical education and endoscopic surgery simulation - a first step to create reliable customized simulators".
PloS ONE, 12, December 2017.

3D Data Hiding

Definition

The art to insert hidden message in data:

- Confidentiality: Statistical invisibility
- Robustness: Transformation resistance
- Capacity: Embedded message size



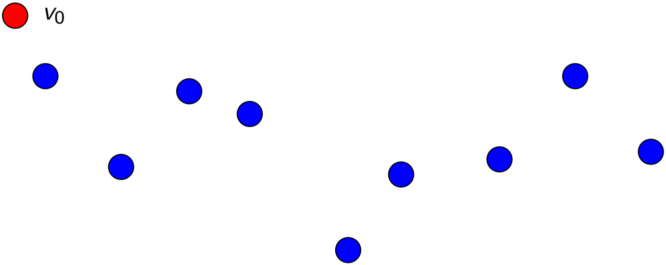
Interests

- Content Enrichment (Metadata)
- DRM (Trace, history logs)
- Integrity (Modification, forgery)

High-Capacity 3D Data Hiding

Hamiltonian Path Quantization (HPQ)

- Synchronization: Nearest Neighbour Halmitonian Path (NNHP)
- Insertion: Spherical coordinates (r, θ, ϕ)

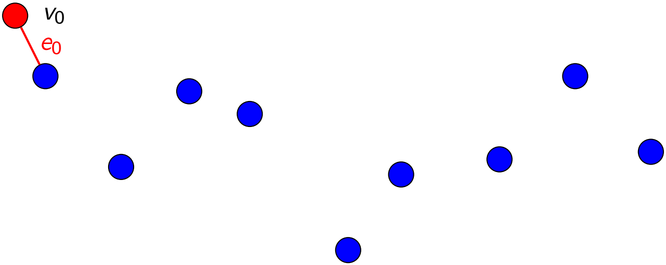


Vincent Itier and William Puech
High capacity data hiding for 3D point clouds based on Static Arithmetic Coding.
Multimedia Tools Applications, Springer, 2017

High-Capacity 3D Data Hiding

Hamiltonian Path Quantization (HPQ)

- Synchronization: Nearest Neighbour Halmitonian Path (NNHP)
- Insertion: Spherical coordinates (r, θ, ϕ)

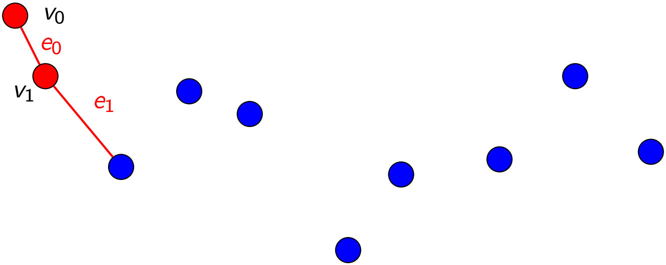


Vincent Itier and William Puech
High capacity data hiding for 3D point clouds based on Static Arithmetic Coding.
Multimedia Tools Applications, Springer, 2017

High-Capacity 3D Data Hiding

Hamiltonian Path Quantization (HPQ)

- Synchronization: Nearest Neighbour Halmitonian Path (NNHP)
- Insertion: Spherical coordinates (r, θ, ϕ)

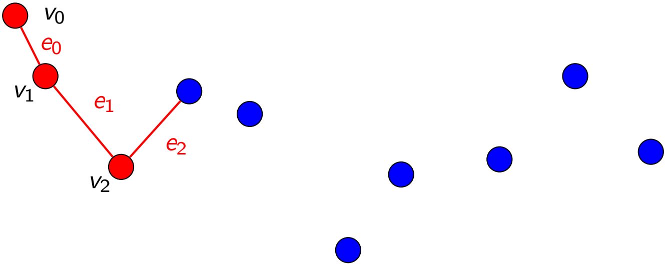


Vincent Itier and William Puech
High capacity data hiding for 3D point clouds based on Static Arithmetic Coding.
Multimedia Tools Applications, Springer, 2017

High-Capacity 3D Data Hiding

Hamiltonian Path Quantization (HPQ)

- Synchronization: Nearest Neighbour Halmitonian Path (NNHP)
- Insertion: Spherical coordinates (r, θ, ϕ)

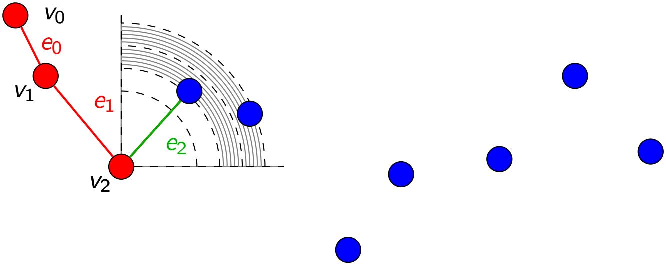


Vincent Itier and William Puech
High capacity data hiding for 3D point clouds based on Static Arithmetic Coding.
Multimedia Tools Applications, Springer, 2017

High-Capacity 3D Data Hiding

Hamiltonian Path Quantization (HPQ)

- Synchronization: Nearest Neighbour Halmitonian Path (NNHP)
- Insertion: Spherical coordinates (r, θ, ϕ)

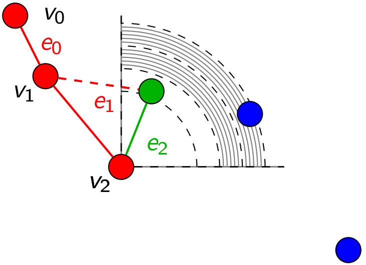


Vincent Itier and William Puech
High capacity data hiding for 3D point clouds based on Static Arithmetic Coding.
Multimedia Tools Applications, Springer, 2017

High-Capacity 3D Data Hiding

Hamiltonian Path Quantization (HPQ)

- Synchronization: Nearest Neighbour Halmitonian Path (NNHP)
- Insertion: Spherical coordinates (r, θ, ϕ)

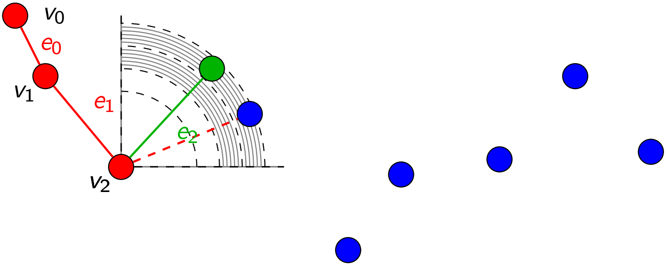


Vincent Itier and William Puech
High capacity data hiding for 3D point clouds based on Static Arithmetic Coding.
Multimedia Tools Applications, Springer, 2017

High-Capacity 3D Data Hiding

Hamiltonian Path Quantization (HPQ)

- Synchronization: Nearest Neighbour Halmitonian Path (NNHP)
- Insertion: Spherical coordinates (r, θ, ϕ)



Vincent Itier and William Puech
High capacity data hiding for 3D point clouds based on Static Arithmetic Coding.
Multimedia Tools Applications, Springer, 2017

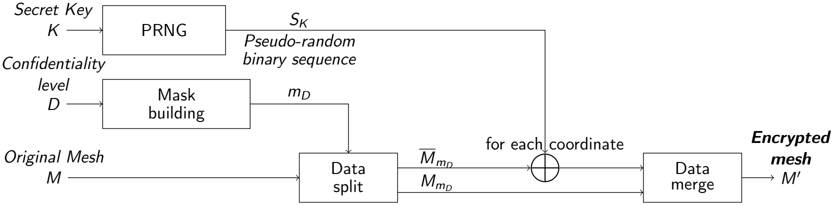
3D Selective Encryption - Method overview

Selective encryption

- Reversible
- Controlled visual confidentiality level

Format-compliant

- Viewable encrypted mesh
- Size preservation

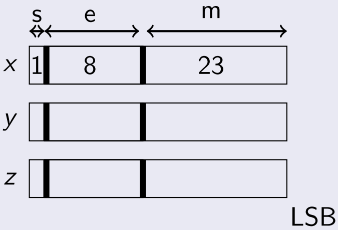


3D Selective Encryption - Data representation

Mesh

- Geometry (Vertices)
- Connectivity (Faces)

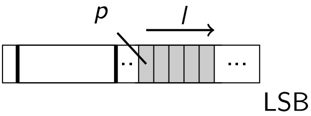
Vertex



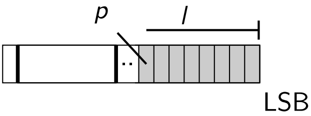
3D Selective Encryption - Mask construction

Confidentiality level $D =< p, l >$

- p, position of first bit to encrypt $p \in [\![0\ ;\ 22]\!]$
- l, number of bits to encrypt $l \in [\![1\ ;\ p+1]\!]$

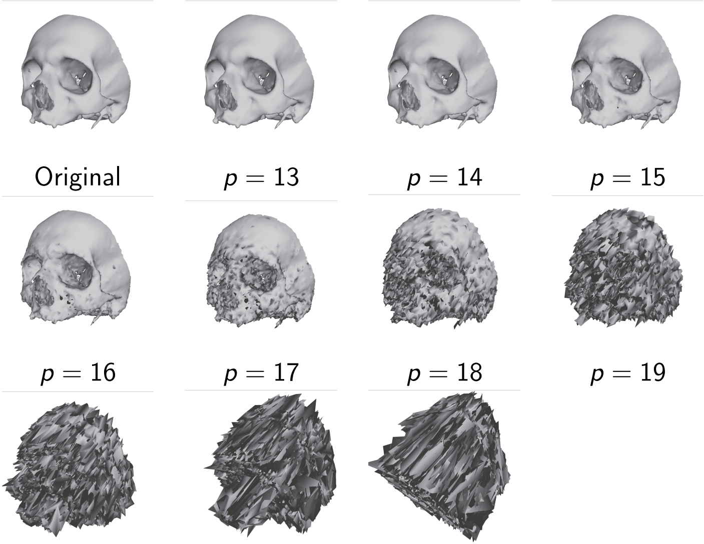


D-SW mask ($D =< p, l >$)



D-LSB mask
($D =< p, l = p + 1 >$)

3D Selective Encryption - Experimental results



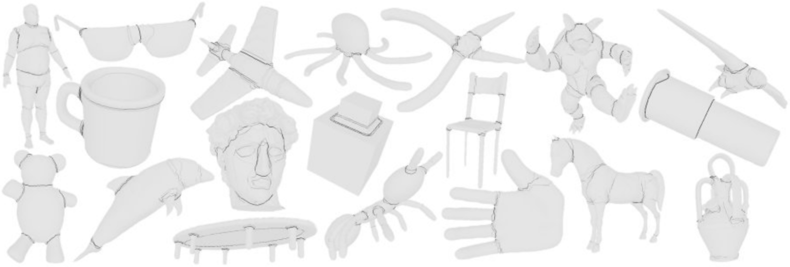
Original | $p = 13$ | $p = 14$ | $p = 15$

$p = 16$ | $p = 17$ | $p = 18$ | $p = 19$

$p = 20$ | $p = 21$ | $p = 22$

3D Selective Encryption as a function of Confidentiality level $D =< p, p + 1 >$

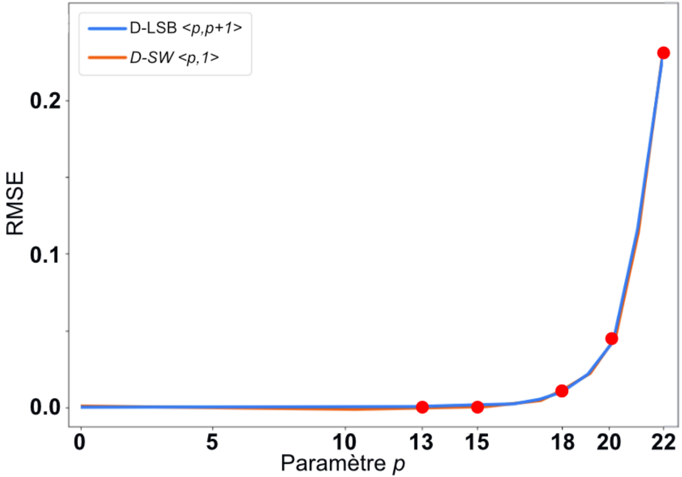
3D Selective Encryption - Experimental results

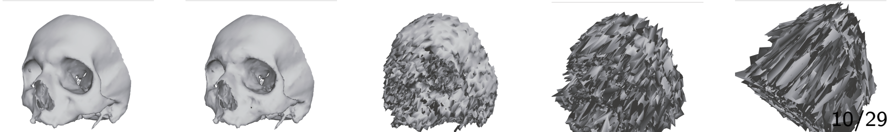


Experimental setup

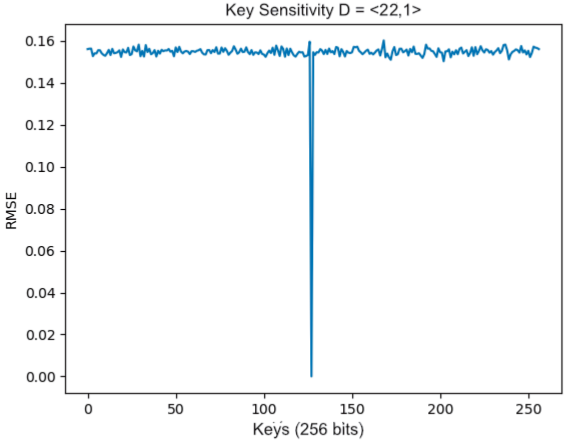
- 380 3D Objects from Princeton Mesh Segmentation Database
- Metric : Root Mean Square Error (*RMSE*)
- Parameters : $D =< p, l = 1$ bit $>$ and $D =< p, l = p + 1$ bits $>$

3D Selective Encryption - Statistical Analysis



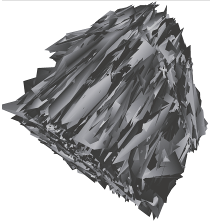


3D Selective Encryption - Secret key sensitivity

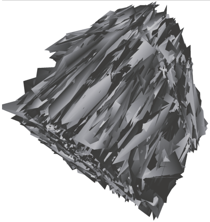


RMSE between M and M_{K_w} as a function of the secret key K and keyset $\mathbb{K} = \{K_w | d_{Hamming}(K, K_w) = 1\}$.

M'



M_{K_0}



3D Selective Encryption - Robustness analysis

Selective data encryption

- Encrypted bit quantity lower than full encryption
- Weak against attacks guessing content rather than attacks guessing secret key

Example

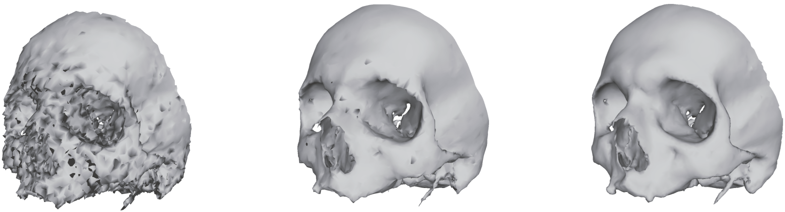
- $D =< p, 1 >$ (D-SW mask)
- N vertices
- 3 bits per vertex (3.125% of geometry)

Guessing probability for 3 bits fo all N vertices

$$P = \frac{1}{2^{3\times N}}$$

3D Selective Encryption - Mesh processing attacks

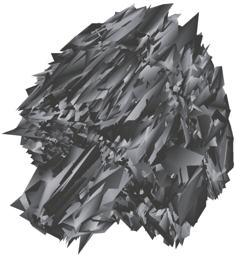
- Laplacian smoothing ($\lambda = 0.3$ and 100 iterations)
- $D =< 17, 18 >$ (Transparent protection)



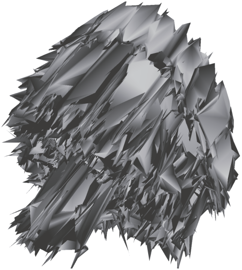
Encrypted Smoothed Original

3D Selective Encryption - Mesh processing attacks

- Laplacian smoothing ($\lambda = 0.3$ and 100 iterations)
- $D =< 21, 22 >$ (Sufficient protection)



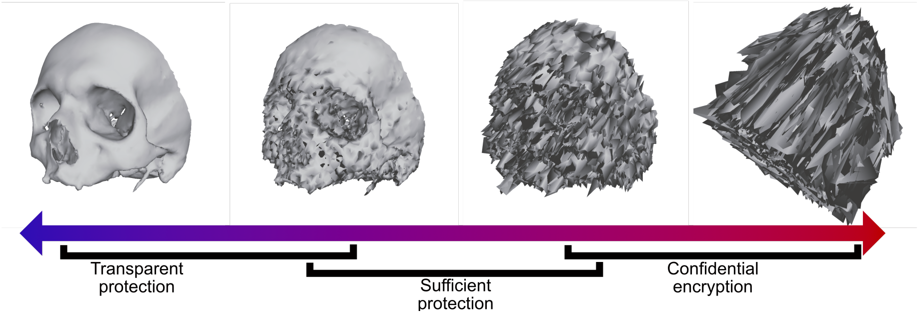
Encrypted



Smoothed

Original

3D Selective Encryption - Conclusion

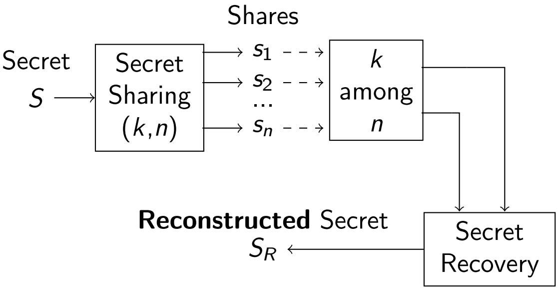


[beugnon2019icme] Sébastien Beugnon, William Puech and Jean-Pierre Pedeboy
From Visual Confidentiality To Transparent Format-Compliant Selective Encryption Of 3D Objects.
IEEE International Conference on Multimedia & Expo, 2018

Secret Sharing

Secret Sharing

- Threshold cryptography method (k, n)
- Distribution of n shares
- Secret recovery when at least k participants



Secret Sharing

Secret Sharing

- Threshold cryptography method (k, n)
- Distribution of n shares
- Secret recovery when at least k participants

Interests

- Critical data storage
- Confidentiality
- Reliability

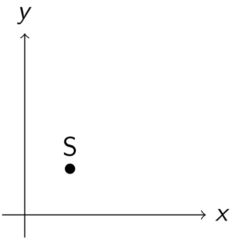
Approaches

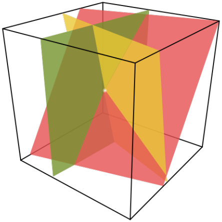
- G.R. Blakley (1979)
- A. Shamir (1979)

Secret Sharing - Blakley

Blakley's scheme (1979)

- Secret S is a k-D point
- *Shares* $s_i | i \in \{1, n\}$ are k-D hyperplanes



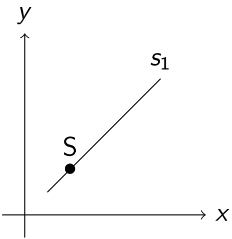


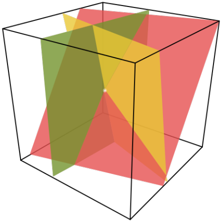
G. R. Blakley
Safeguarding Cryptographic Keys.
International Workshop on Managing Requirements Knowledge (AFIPS), 1979

Secret Sharing - Blakley

Blakley's scheme (1979)

- Secret S is a k-D point
- *Shares* $s_i | i \in \{1, n\}$ are k-D hyperplanes



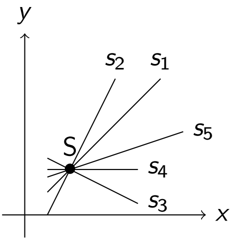


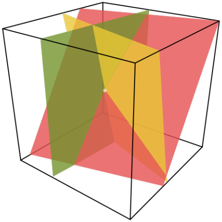
G. R. Blakley
Safeguarding Cryptographic Keys.
International Workshop on Managing Requirements Knowledge (AFIPS), 1979

Secret Sharing - Blakley

Blakley's scheme (1979)

- Secret S is a k-D point
- *Shares* $s_i | i \in \{1, n\}$ are k-D hyperplanes



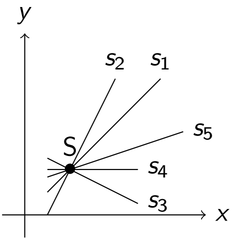


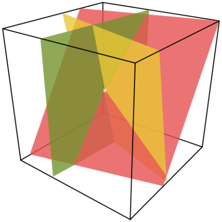
G. R. Blakley
Safeguarding Cryptographic Keys.
International Workshop on Managing Requirements Knowledge (AFIPS), 1979

Secret Sharing - Blakley

Blakley's scheme (1979)

- Secret S is a k-D point
- *Shares* $s_i | i \in \{1, n\}$ are k-D hyperplanes





G. R. Blakley
Safeguarding Cryptographic Keys.
International Workshop on Managing Requirements Knowledge (AFIPS), 1979

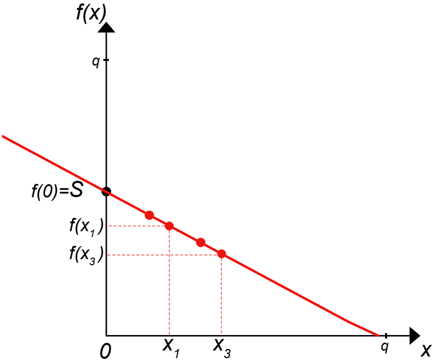
Secret Sharing - Shamir

Secret Sharing $(k,\ n)$ (Shamir, 1979)

Polynomial Interpolation:

$$f(x) = \sum_{i=0}^{k-1} a_i \times x^i$$

- Finite field $\mathbb{F}_q$ where q is prime
- $S = a_0 = f(0)$
- *Share* $s_j = (x_j, f(x_j))$ where $j \in [\![0\ ;\ n[\![$ and $x_j \in \mathbb{F}_q^*$



A. Shamir
How to Share a Secret.
Communications of the ACM, 1979

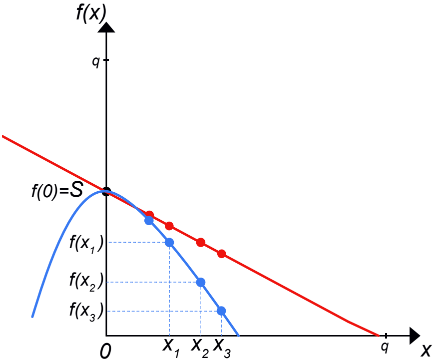
Secret Sharing - Shamir

Secret Sharing $(k,\ n)$ (Shamir, 1979)

Polynomial Interpolation:

$$f(x) = \sum_{i=0}^{k-1} a_i \times x^i$$

- Finite field $\mathbb{F}_q$ where q is prime
- $S = a_0 = f(0)$
- *Share* $s_j = (x_j, f(x_j))$ where $j \in [\![0\ ;\ n[\![$ and $x_j \in \mathbb{F}_q^*$



A. Shamir
How to Share a Secret.
Communications of the ACM, 1979

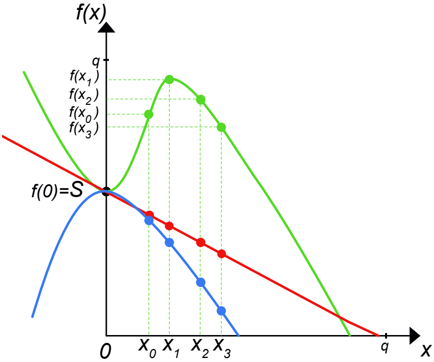
Secret Sharing - Shamir

Secret Sharing $(k,\ n)$ (Shamir, 1979)

Polynomial Interpolation:

$$f(x) = \sum_{i=0}^{k-1} a_i \times x^i$$

- Finite field $\mathbb{F}_q$ where q is prime
- $S = a_0 = f(0)$
- *Share* $s_j = (x_j, f(x_j))$ where $j \in [\![0\ ;\ n[\![$ and $x_j \in \mathbb{F}_q^*$

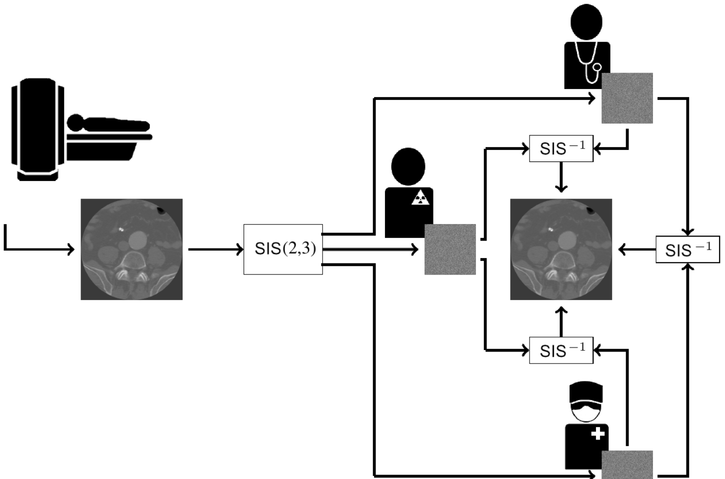


A. Shamir
How to Share a Secret.
Communications of the ACM, 1979

Secret Image Sharing

Secret Image Sharing

- *shares* = images



Secret Image Sharing

Secret Image Sharing

- *shares* = images

Constraints

- Image size preservation
- Shared pixel are independant
- Lossless
- No secret key

Secret Image Sharing

Approaches

- Polynomial-based Secret Image Sharing (PSIS)
- Visual Cryptography (VC)

Methods (VC)

- Visual cryptography (M. Naor et A. Shamir, 1994)
- Application of Visual Cryptography to Biometric Authentication (N. Askari *et al.*, 2015)

Methods (PSIS)

- Secret Image Sharing (C. Thien and J. Lin, 2002)
- Secret image sharing with user-friendly shadow images (C. Thien and J.Lin, 2003)
- Sharing and hiding secret images with size constraint (Y. Wu, C. Thien and J. Lin, 2004)

Secret 3D Object Sharing

Secret 3D Object Sharing

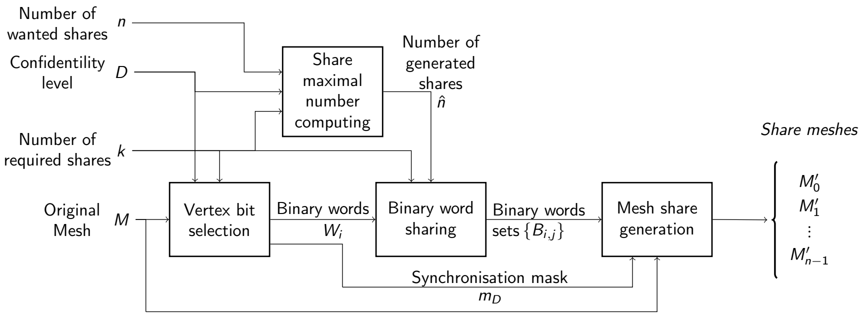
- *shares* = meshes

Constraints

- Visualisable encrypted meshes
- Controlled visual confidentiality level
- Size preservation and same number of vertices

Sébastien Beugnon, William Puech and Jean-Pierre Pedeboy
Format-Compliant Selective Secret 3D Object Sharing Scheme.
IEEE Transactions on Multimedia, 2019

Selective Secret 3D Object Sharing - Method overview



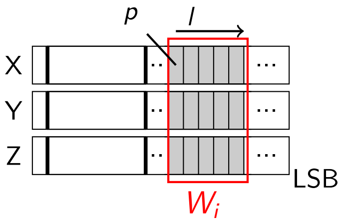
Method

- Sharing independently each vertex $v_i | i \in [\![1 \; ; \; N_v]\!]$
- Selection of sharing data space

Selective Secret 3D Object Sharing - Vertex bit selection

Confidentiality level $D =< p, l >$

- p, position of first bit to share $p \in [\![0\ ;\ 22]\!]$
- l, number of bits to share $l \in [\![1\ ;\ p+1]\!]$



Selective Secret 3D Object Sharing - Binary word sharing

Sharing parameters

- $2 <= k <= n_{max}$

Using Shamir's Scheme

- Secret is W_i
- Defined on Galois field GF($2^{(3*l)}$)
- $B_{i,j} = f(x_j) = W_i + ... + a_{k-1} \times x_j^{k-1}$

Maximum number of shares

$$n_{max} = |GF(2^m)| - 1 = |GF(2^{3\times l})| - 1 = 2^{(3\times l)} - 1$$

Secret 3D Object Sharing - Binary word sharing

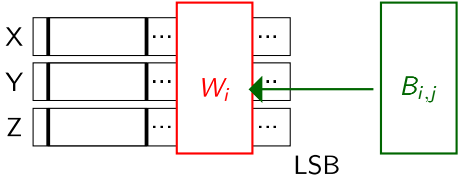
Using Blakley's scheme

- W_i is fragmented into small blocks as coordinate of secret point S
- Transform share hyperplane coefficients into a binary word $B_{i,j}$

Maximum number of shares

$$n_{max} = \prod_{j=0}^{k-2} C_1^{2^{|a_j|}} = \prod_{j=0}^{k-2} 2^{|a_j|}$$

Secret 3D Object Sharing - Shared 3D object generation



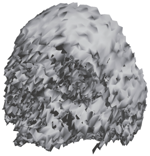
- Substitute selected vertex data by binary word from sharing process

Secret 3D Object Sharing - Results

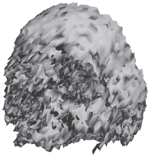
Application

- $(k = 3, n = 4)$
- $D =< 18, 19 >$

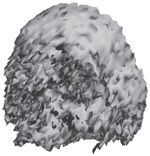
- Sharing



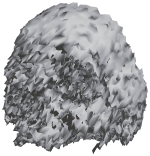
M'_0



M'_1



M'_2



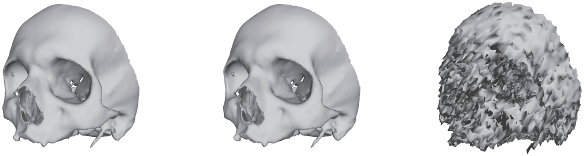
M'_3

Secret 3D Object Sharing - Results

Application

- $(k = 3, n = 4)$
- $D =< 18, 19 >$

- Reconstruction

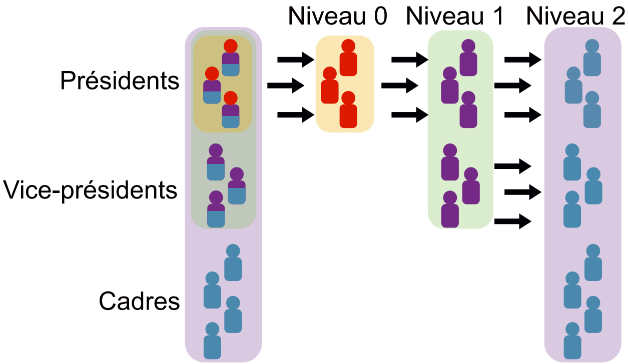


(M_0', M_1', M_2') (M_0', M_1', M_3') (M_0', M_1')

Hierarchical Secret Sharing

Multilevel hierarchy

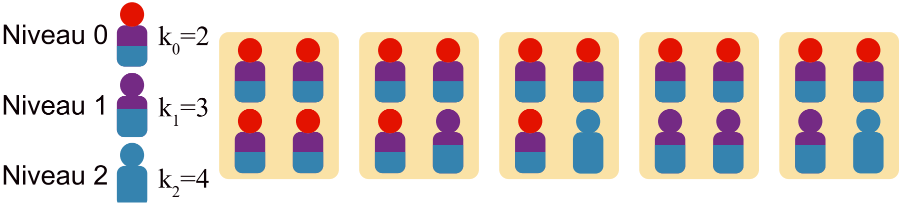
- L levels
- $\mathbf{k} = (k_0, \ldots, k_{L-1})$, with $k_i < k_j$ such as $\forall i, j \in [\![0\ ;\ L[\![, i < j$
- $\mathbf{n} = (n_0, \ldots, n_{L-1})$



Hierarchical Secret Sharing

Tassa's hierarchy (2007)

- Based on Shamir's scheme
- Using derived from the polynomial

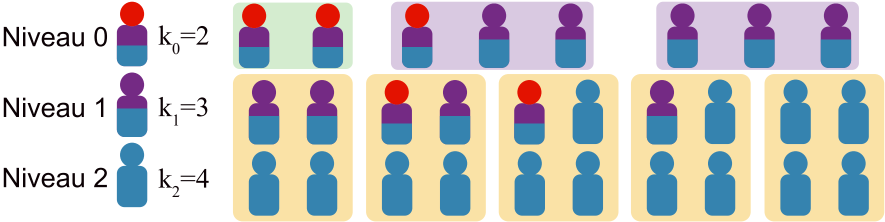


T. Tassa
Hierarchical threshold secret sharing.
Journal of cryptology, 2007

Hierarchical Secret Sharing

Belenkiyes hierarchy (2008)

- Same as Tassa
- The secret is hidden in the last coefficient



M. Belenkiy
Disjunctive Multi-Level Secret Sharing.
IACR Cryptology ePrint Archive, 2008

Priority Access Hierarchy (PAH)

Definition

- Hierarchy more realist of industrial usecase
- Using derived from the polynomial
- Distributing polynomials' coefficients