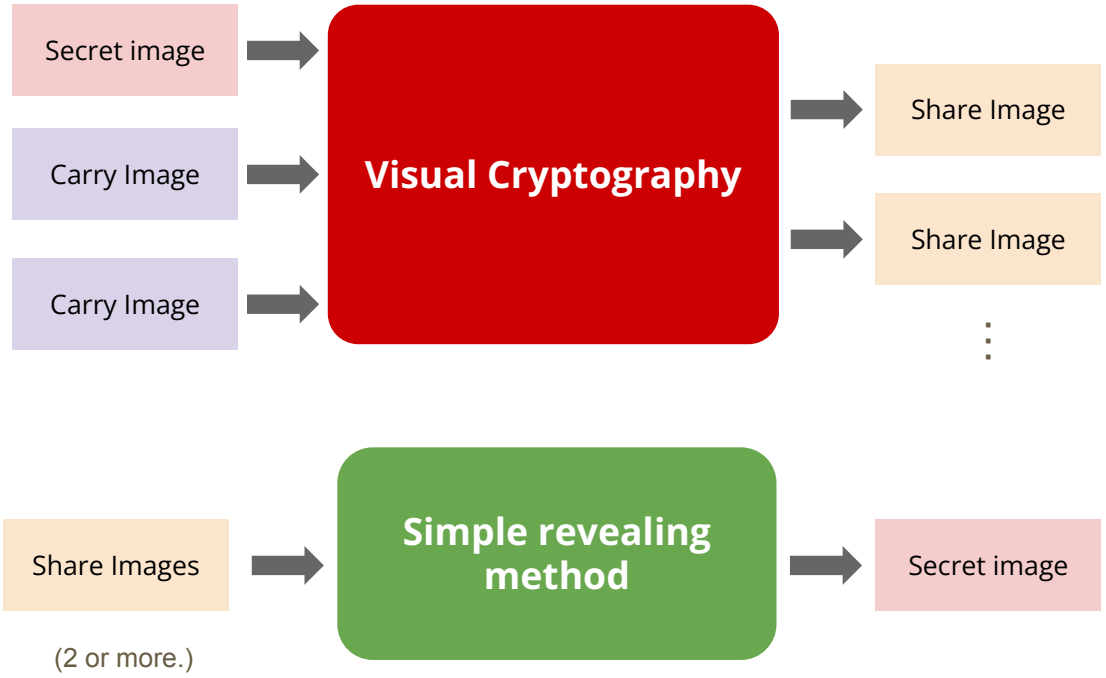
DIP Proposal Report Team 16
Exploring Visual Cryptography: Technique and Advancements

盧智寶, R12922196, 資工碩一
蔡昀燁, R12922104, 資工碩一
鮑鈺文, B09902016, 資工大四

Introduction & Motivation

- Visual cryptography is an encryption technique to encrypt the secret images into multiple share images.
- VC puts the human perception into the decryption process to acquire the information in the original secret images, instead of relying on the complex mathematical theories and computation.
- Halftoning skill discussed in Lecture 6 is a significant basic for VC.

Problem definition

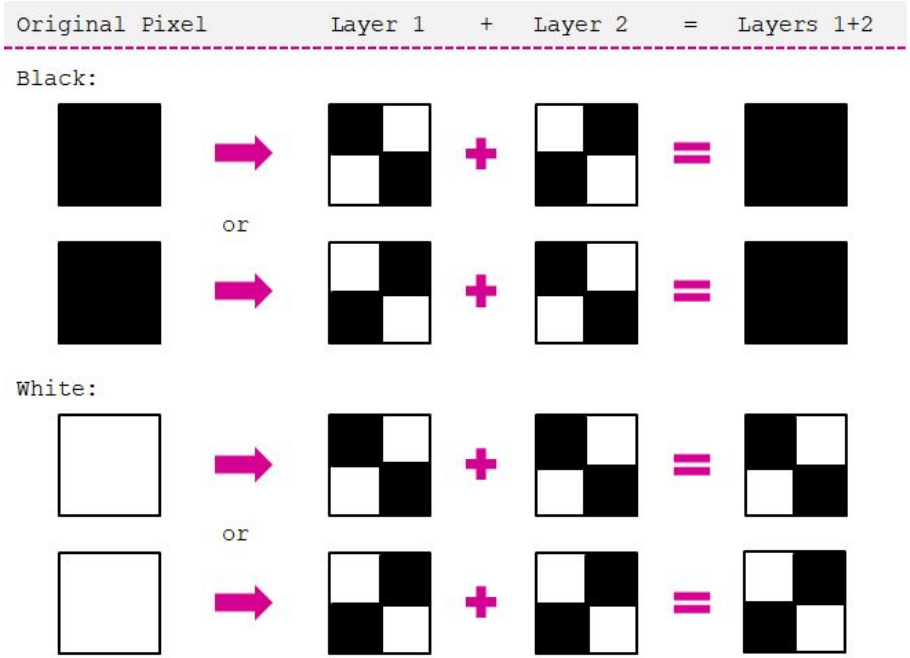


Algorithm

- Method category:
  - Pattern based
  - Error diffusion based
  - Hierarchical VC
  - AMBTC
- Share category:
  - Meaningful
  - Meaningless
- Color:
  - Binary(white & black)
  - **Grayscale**
  - Colorful

Algorithm - Naor and Shamir's pattern based method.

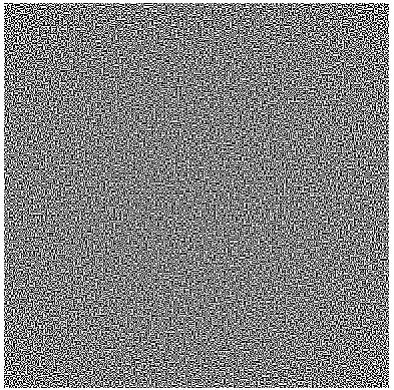
- Simple baseline.
- Secret image: binary image.
- Share image: binary & meaningless.
- Pros:
  - Implement quickly.
- Cons:
  - Easy to be attacked.
  - Pixel expansion.

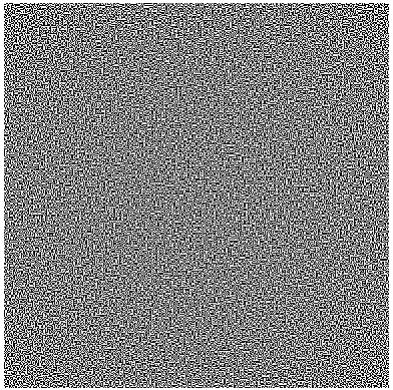


Experimental Results - Naor and Shamir's pattern.

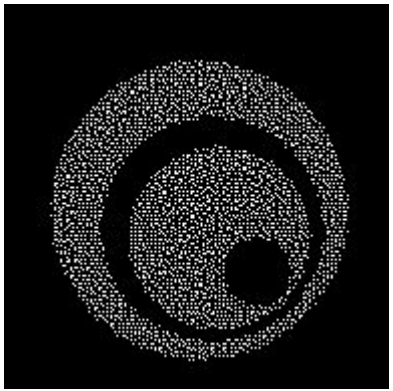
- Secret image:

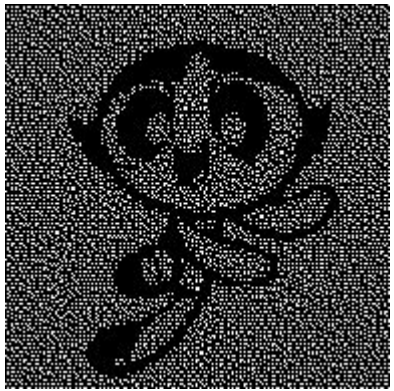
- Share image:





- After stacked:





Algorithm - Chen's pattern based method.

- Can we do better?
  - From meaningless to meaningful.
- Secret image: binary image.
- Share image: binary & meaningful.
- Pros:
  - Harder to be noticed.
- Cons:
  - More complex.
  - Can only deal with black & white picture.

Algorithm - Chen's pattern based method.

Algorithm 1 Chen's pattern based method

Ensure: The black pixel paramter for black and white block in share and secret images.

for `block` **in** `image` **do**

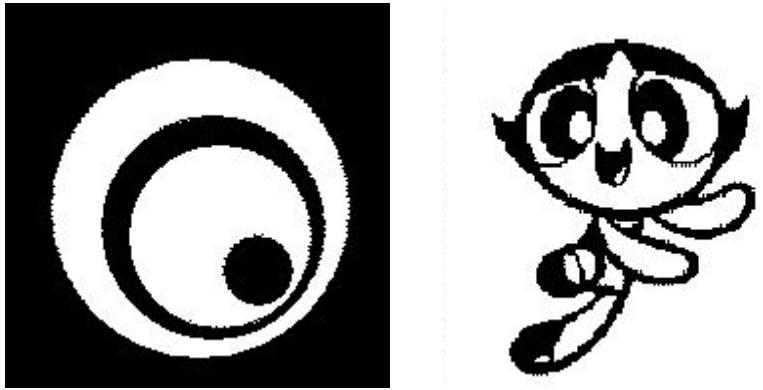
0. Do the preprocessing for both secret and share image block.
1. Calculate the number of black pixels in the block(secret and share).
2. Record the position for all black pixel position for each block.
3. Make sure the number of black pixels in stacked share image are same for secret image block.

end for

Experimental Result - Chen's pattern.

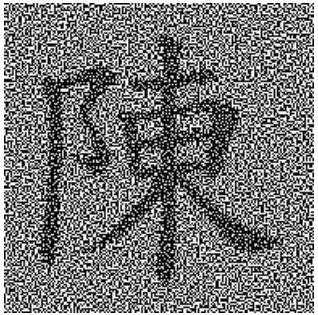
- Input image:

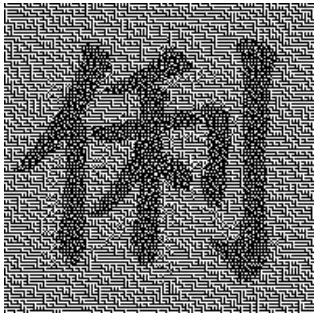
- Secret image:

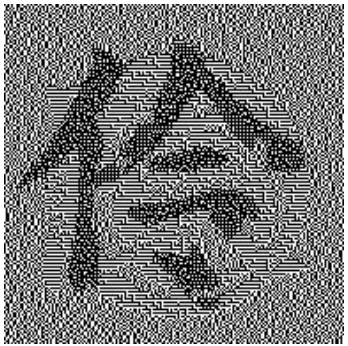


Experimental Result - Chen's pattern.

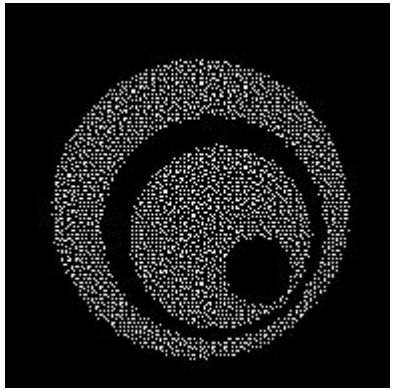
- Share image:

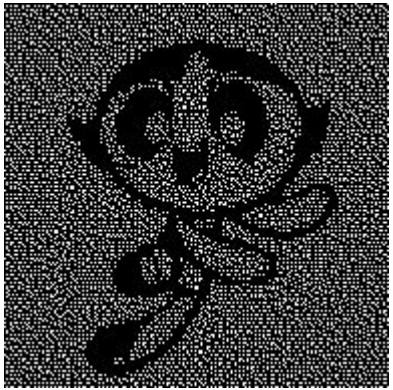






- After stacked:

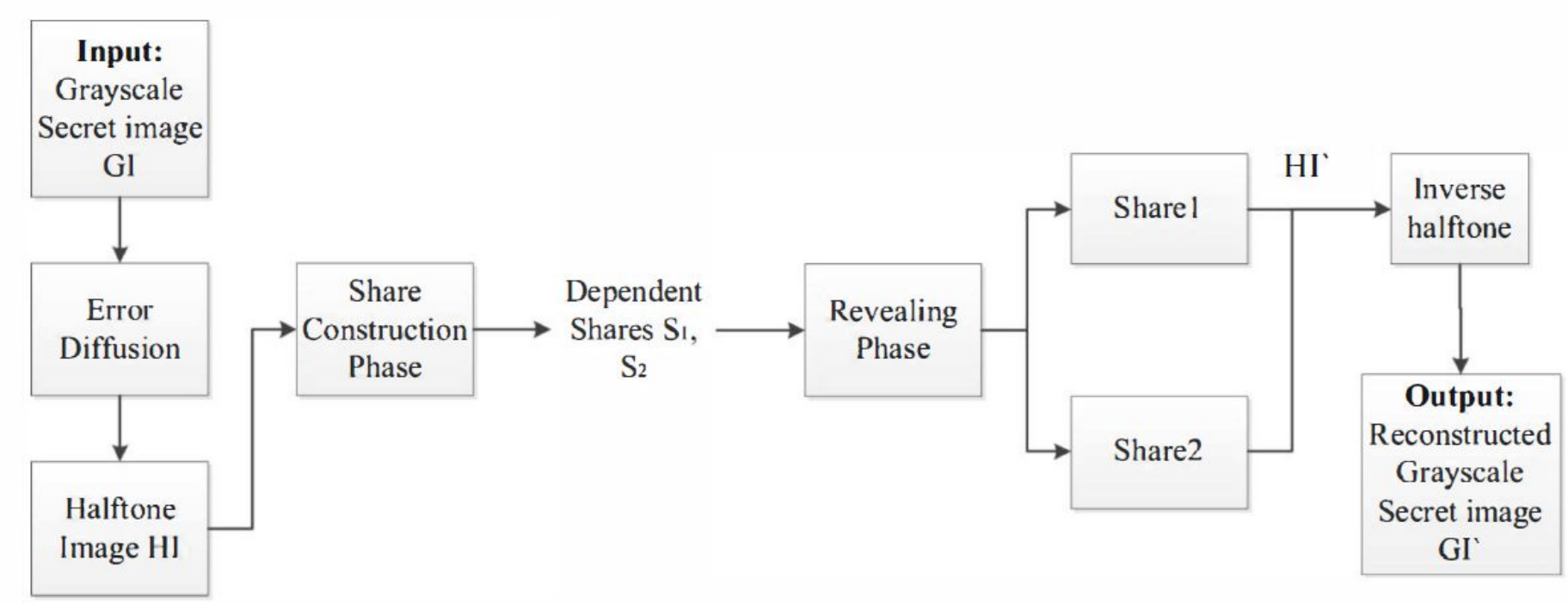




Algorithm - Improved Grayscale Visual Secret Sharing.

- What we really want is to deal with “grayscale image.”
- An intuitive method is do the “halftoning” before apply pattern based method and apply the “inverse halftoning” for the temporary result.
- Secret image: grayscale image.
- Share image: grayscale & meaningful.
- Pros:
  - The visual effect of resultant image is best.
- Cons:
  - We need more calculating resources(not a obvious problem.)
  - The distortion because of inverse halftoning.

Algorithm - Improved Grayscale Visual Secret Sharing.



Experimental Result - IGVSS.

- Input images:

- Secret images:

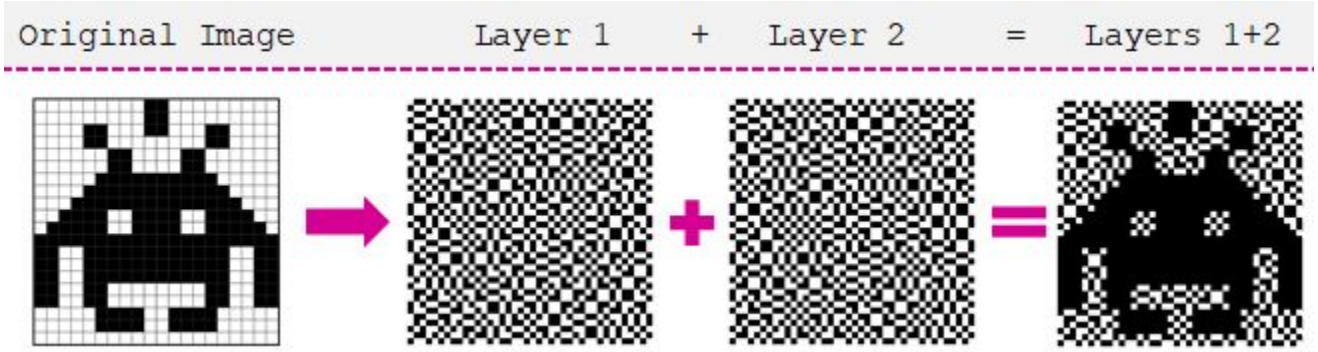
Experimental Result - IGVSS.

- Stacked Halftoning image:

- Output images:

Discussions - Pattern based

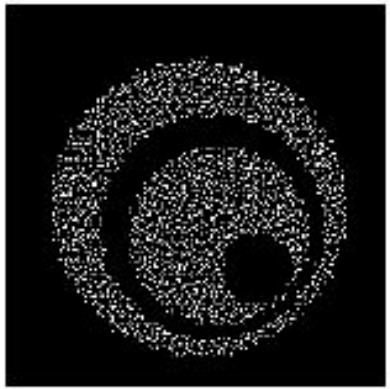
- Pattern based method is simple yet effective baseline.
  - Only you need to do for share image is do the stacking.



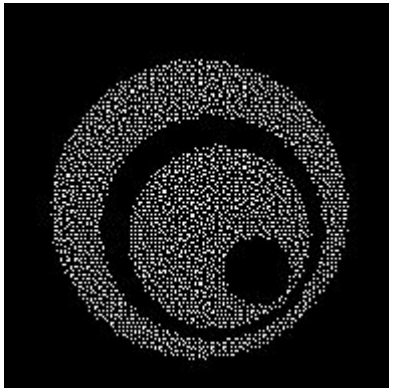
Discussions - Pattern based

- We found some implementation error (e.g. parameter setting or pseudo code) for referenced papers.

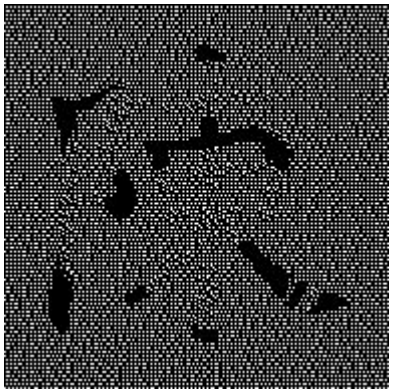
Black block black pixels num: 2
White block black pixels num: 1



Black block black pixels num: 3
White block black pixels num: 2



Black block black pixels num: 2
White block black pixels num: 1



Discussions - Pattern based

- It is originally develop on binary image, but can be extended to the grayscale image easily with the help of halftoning technique.

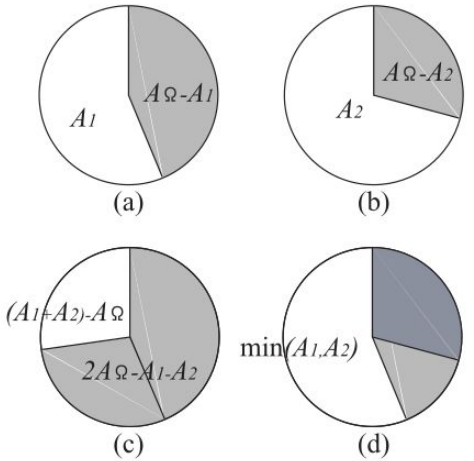
Algorithm - Error-diffusion-based

Extended visual cryptography for natural images

Algorithm - Error-diffusion-based

Extended visual cryptography for natural images

- Fundamentals of the visual cryptography for natural images.
  - A_1 : The pixel value of the carry image 1
  - A_2 : The pixel value of the carry image 2
  - A_Ω : The maximum value of a pixel.
  - The possible value two carry image can create.
    - $A_{secret} = [\max(0, (A_1 + A_2) - A_\Omega), \min(A_1, A_2)]$



Algorithm - Error-diffusion-based

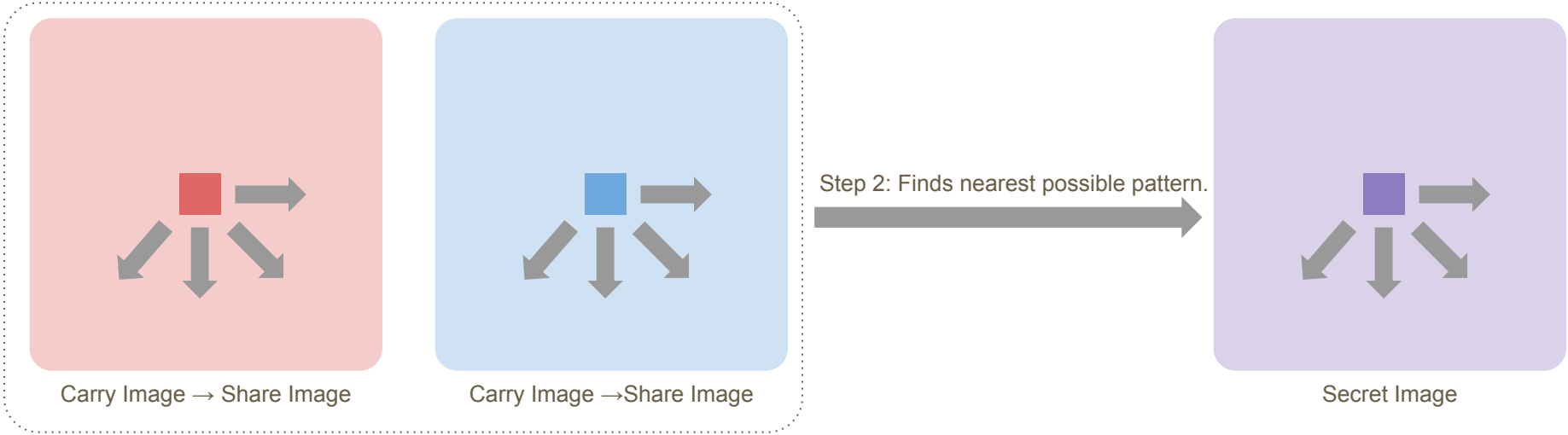
Extended visual cryptography for natural images

- The contrast enhancement
  - Make more pixel satisfy the condition.
    - [max(0, (A1 + A2) - AΩ), min(A1 , A2)]
  - Increase the pixel value of the carry images.
  - Decrease the pixel value of the secret images.

Algorithm - Error-diffusion-based

Extended visual cryptography for natural images

- The error diffusion process



Experimental results - Error-diffusion-based

Input Images

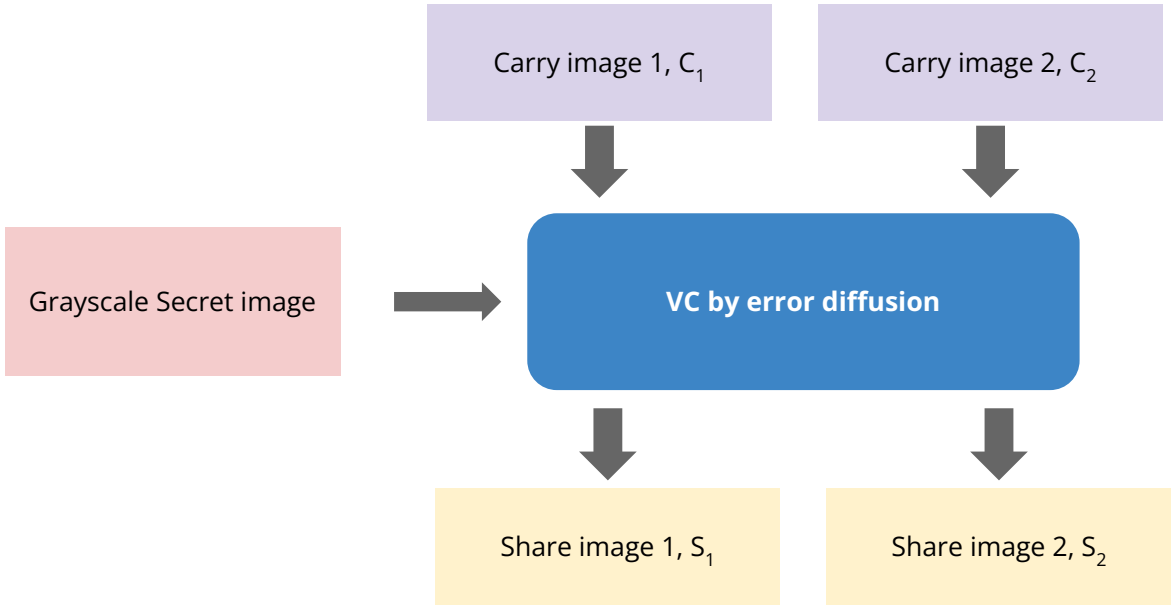
Output Images

Carry / Share Image

Secret Image

Algorithm - Error-diffusion-based

Image Size-Preserving Visual Cryptography by Error Diffusion



Algorithm - Error-diffusion-based

Image Size-Preserving Visual Cryptography by Error Diffusion

1. Normalizes the secret image.
2. Initializes the error as 0 and carry image as 0.5.
3. Assigns the pixel value based on normalized value and error.
    - Determine the value for secret image by the threshold.
    - Find values for share images that make the smallest difference
4. Compute the quantize error.
5. Diffuses the error to the secret image and the two share images.

Algorithm 1 Visual cryptography by error diffusion

Require: a grayscale image f, parameters α and γ
Ensure: share images $S_1 = [s_{1ij}]$ and $S_2 = [s_{2ij}]$

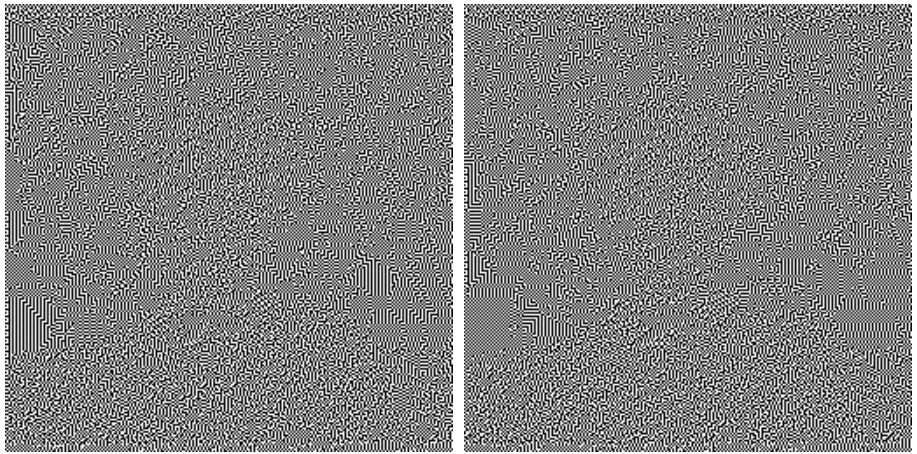
Compute the normalized image $\tilde{f} = [\tilde{f}_{ij}]$ by (1);
Initialize arrays as $e_{ij} = \varepsilon_{1ij} = \varepsilon_{2ij} := 0$;
Initialize arrays as $c_{1ij} = c_{2ij} := \gamma$;
Initialize vectors as $\boldsymbol{b}_0 := \begin{bmatrix}0\\0\end{bmatrix}$, $\boldsymbol{b}_1 := \begin{bmatrix}1\\0\end{bmatrix}$, $\boldsymbol{b}_2 := \begin{bmatrix}0\\1\end{bmatrix}$;
for $i = 0$ to m **do**
  for $j = 0$ to n **do**
    if $\tilde{f}_{ij} + e_{ij} \geq \theta$ **then**
      $b_{ij} := 1$;
      $d_{ij} := \tilde{f}_{ij} + e_{ij} - b_{ij}$;
      $s_{1ij} = s_{2ij} := 1$;
      $\boldsymbol{\delta}_{ij} = \begin{bmatrix}c_{1ij} + \varepsilon_{1ij}\\c_{2ij} + \varepsilon_{2ij}\end{bmatrix} - \begin{bmatrix}1\\1\end{bmatrix}$;
    else
      $b_{ij} := 0$;
      $d_{ij} := \tilde{f}_{ij} + e_{ij} - b_{ij}$;
      Compute

$$t^* = \arg\min_{t\in\{0,1,2\}} \left\| \begin{bmatrix}c_{1ij} + \varepsilon_{1ij}\\c_{2ij} + \varepsilon_{2ij}\end{bmatrix} - \boldsymbol{b}_t \right\|_1 ;$$

      $\begin{bmatrix}s_{1ij}\\s_{2ij}\end{bmatrix} := \boldsymbol{b}_{t^*}$;
      $\boldsymbol{\delta}_{ij} = \begin{bmatrix}c_{1ij} + \varepsilon_{1ij}\\c_{2ij} + \varepsilon_{2ij}\end{bmatrix} - \boldsymbol{b}_{t^*}$;
    end if
    for (k, l) in $\{(0,1), (1,-1), (1,0), (1,1)\}$ **do**
      if $(i + k, j + l) \in \Omega$ **then**
        $e_{i+k,j+l} := e_{i+k,j+l} + w_{kl} d_{ij}$;
        $\begin{bmatrix}\varepsilon_{1,i+k,j+l}\\\varepsilon_{2,i+k,j+l}\end{bmatrix} := \begin{bmatrix}\varepsilon_{1,i+k,j+l}\\\varepsilon_{2,i+k,j+l}\end{bmatrix} + w_{kl}\boldsymbol{\delta}_{ij}$;
      end if
    end for
  end for
end for

Experimental results - Error-diffusion-based

Share Images:

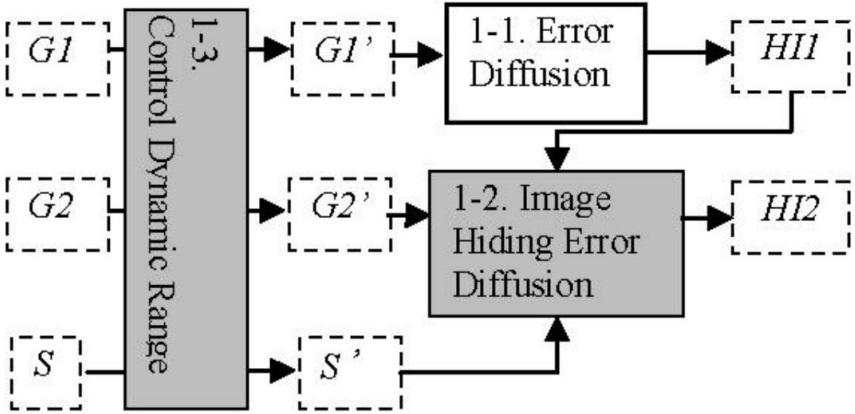


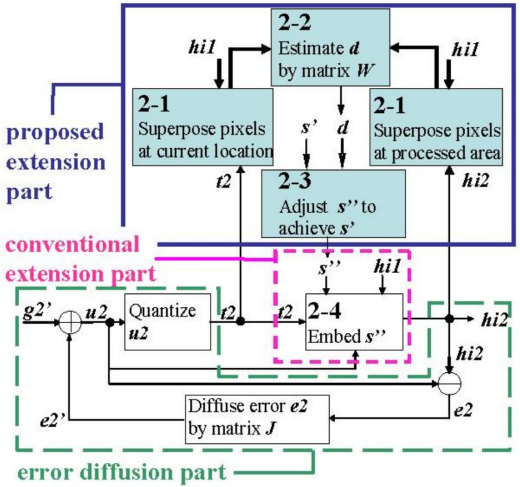
Decrypted Image:

Algorithm - Error-diffusion-based

Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique

- Lack of details to implement
  - The pattern for the share images.
  - The notions for the algorithm are vague.
  - The sizes and shapes of the notations are unspecified.





Discussions - Error-diffusion-based

Pros:

- Native to grayscale images
- Appealing result for natural images

Cons:

- Sensitive to parameters for some instances (eg. contrast)
- The robustness and privacy is not guarantee most of the time

Discussions - Error-diffusion-based

The range of the pixel value for error-diffusion-based methods

- Extended visual cryptography for natural images

w/ enhancement

w/o enhancement

Share Images

Decrypted Image

Discussions - Error-diffusion-based

The range of the pixel value for error-diffusion-based methods

- Image Size-Preserving Visual Cryptography by Error Diffusion
  - $$\tilde{f}_{ij} = \alpha \frac{f_{ij} - \min\{f_{ij}\}}{\max\{f_{ij}\} - \min\{f_{ij}\}},$$

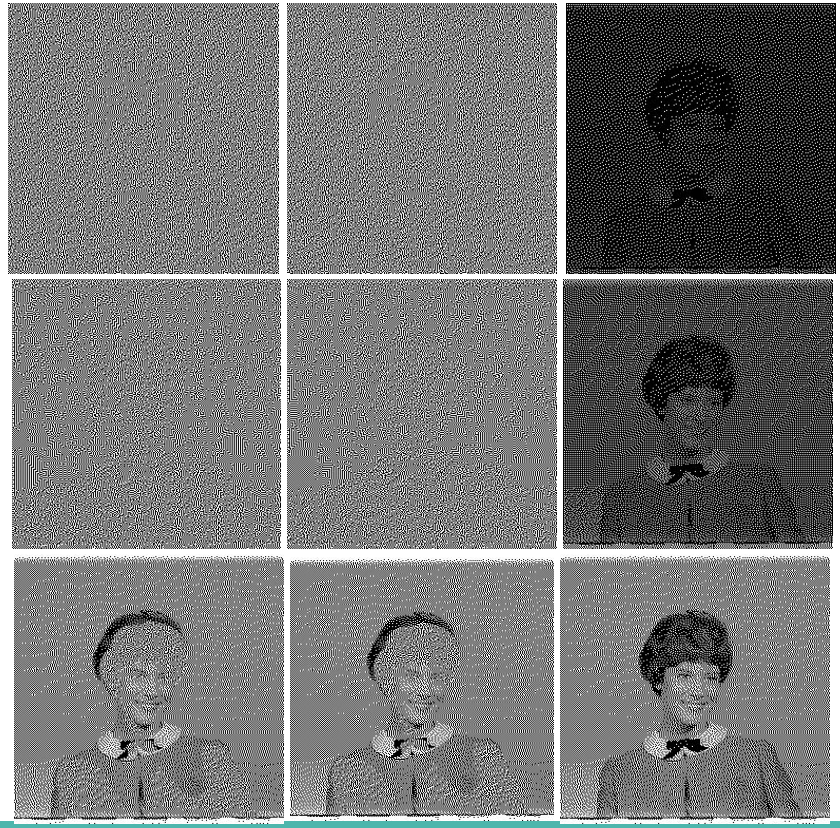
Discussions - Error-diffusion-based

$$\tilde{f}_{ij} = \alpha \frac{f_{ij} - \min\{f_{ij}\}}{\max\{f_{ij}\} - \min\{f_{ij}\}},$$

α = 0.25

α = 0.5

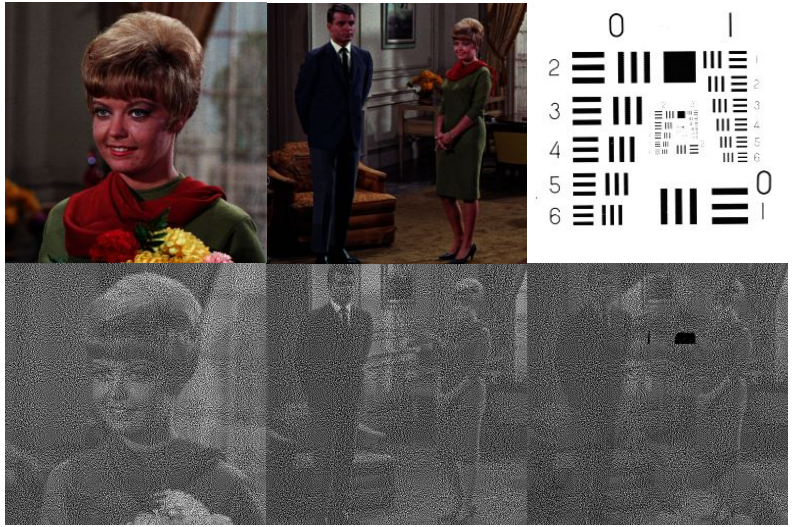
α = 1



Discussions - Error-diffusion-based

Apply to binary secret images

- Extended visual cryptography for natural images

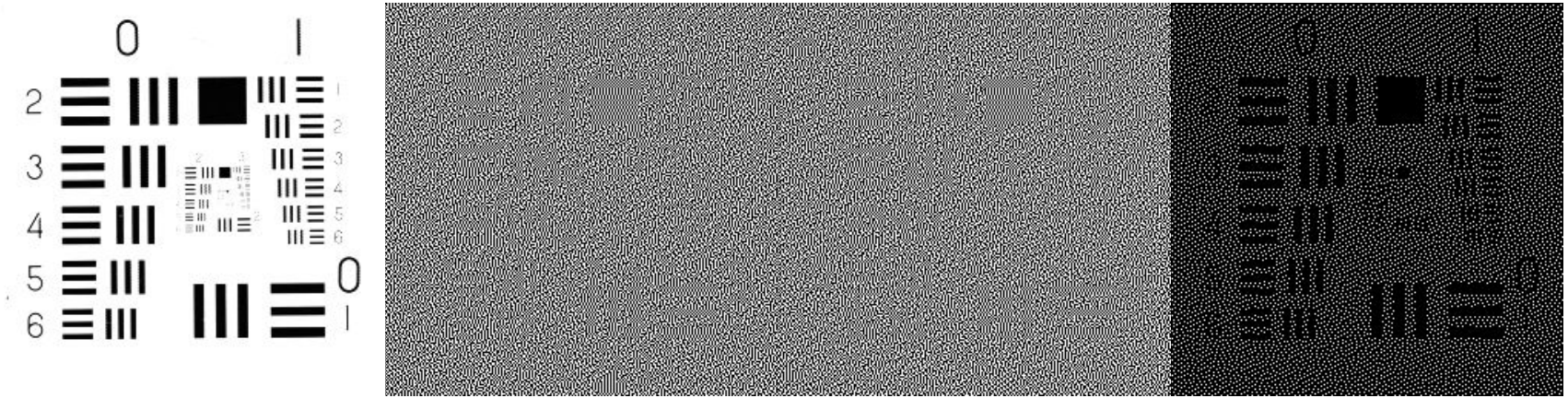


Share Images Decrypted Image

Discussions - Error-diffusion-based

Apply to binary secret images

- Image Size-Preserving Visual Cryptography by Error Diffusion (α = 0.1)



Secret Image

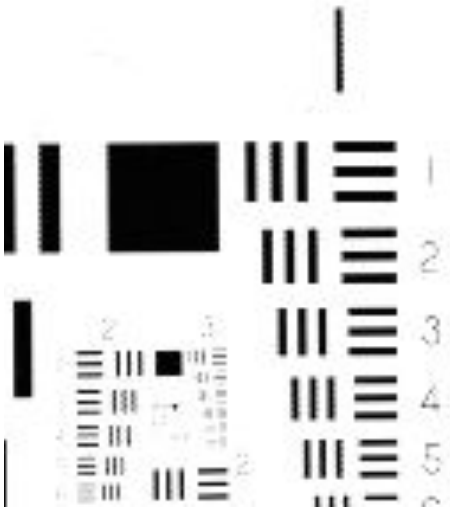
Share Images

Decrypted Image

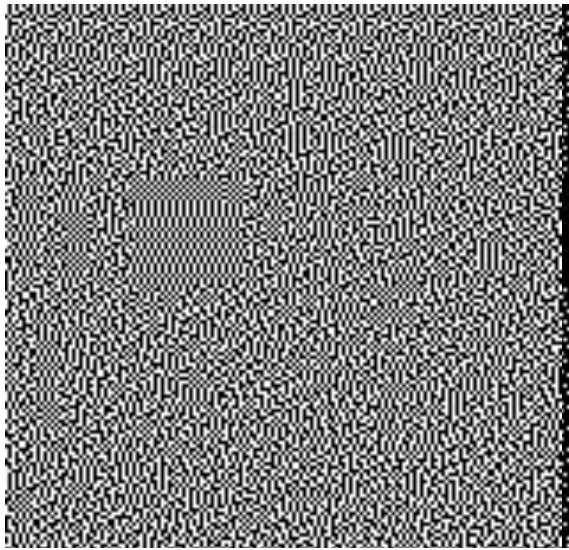
Discussions - Error-diffusion-based

Apply to binary secret images

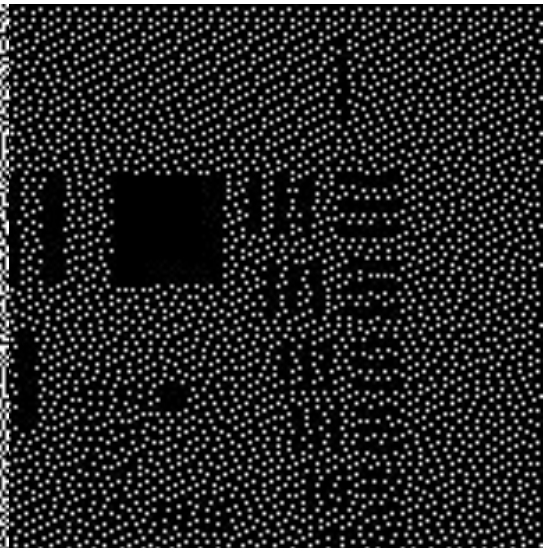
- Image Size-Preserving Visual Cryptography by Error Diffusion



Secret Image



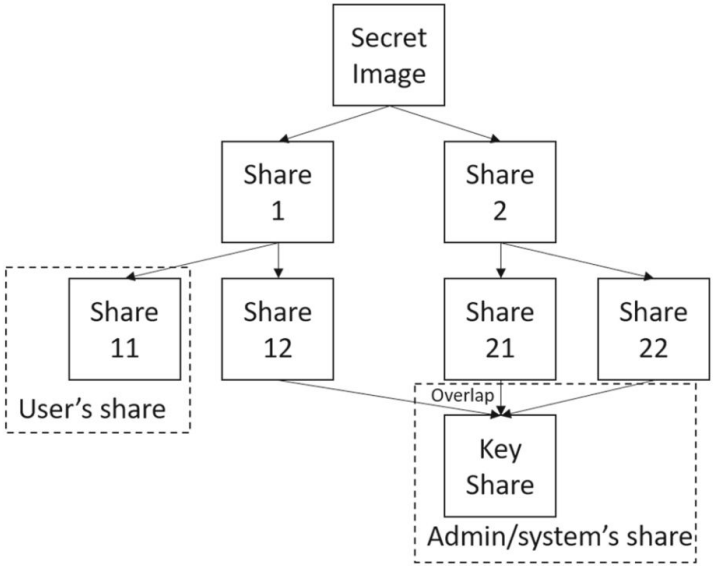
Share Images



Decrypted Image

Algorithm - Hierarchical VC

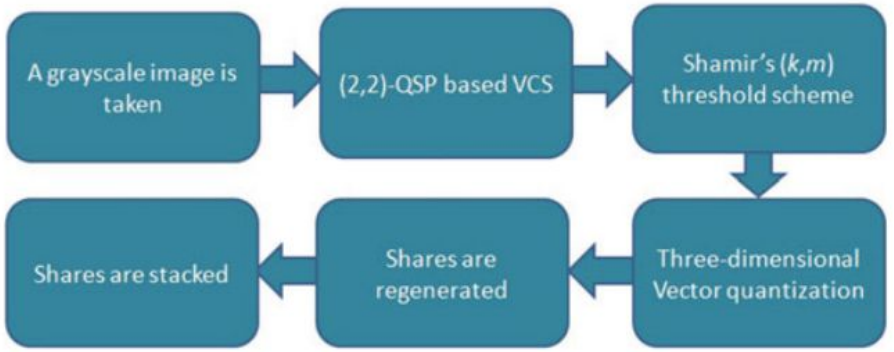
- Encrypt and decrypt secret images using multi levels.
- Pros
  - Enhanced Security
  - Access Control
- Cons
  - Time Complexity
  - Storage Overhead
  - Share Dependency



Algorithm - Hierarchical VC

A Hierarchical Image Cryptosystem Based on Visual Cryptography and Vector Quantization

- Two Level VC
  1. (2, 2)-QSP
  2. Shamir's (k, m)
- Vector Quantization
  - Reduce Storage
- Level-by-Level Decryption

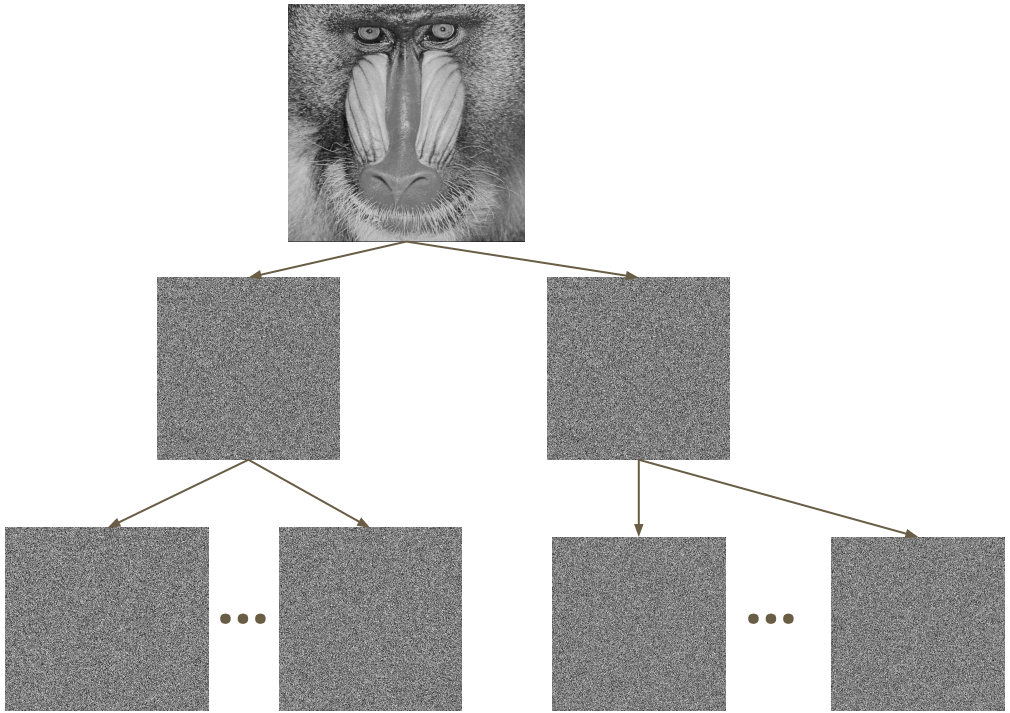


Experiment- Hierarchical VC

Secret Images

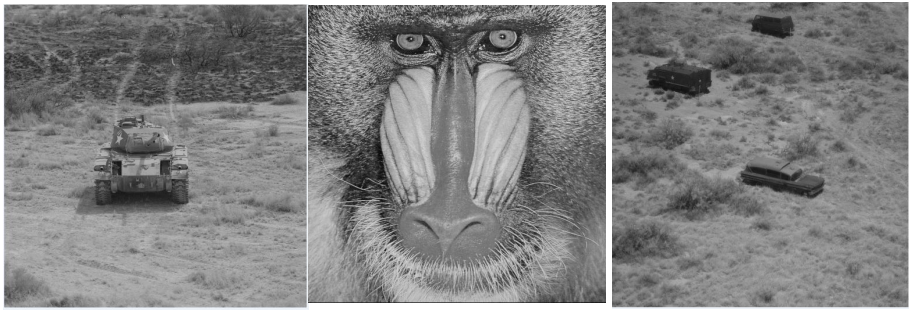
Level 1
(2, 2)-QSP based

Level 2
Shamir's (k, m)



Experiment- Hierarchical VC

Secret Images



Decrypt Images

Discussion- Hierarchical VC

A Hierarchical Image Cryptosystem Based on Visual Cryptography and Vector Quantization

- Pros :
  - Security
  - Hard to decrypt secret by shares
- Cons:
  - Time
  - Memory
  - Decrypted image loss a large of details

Discussion- Hierarchical VC

- Storage Overhead:
  - Just like original paper, I use 512 x 512 secret image.
  - Apply to (3, 6) shamir scheme.

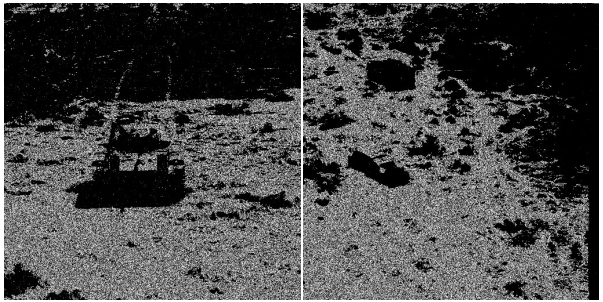
	(2, 2)-QSP (Level 1)	Shamir VC (Level 2)	Vector Quantization
Mandrill	2*263 (KB)	2*6*263 (KB)	2*585 (KB)
Tank	2*263 (KB)	2*6*263 (KB)	2*530 (KB)

Discussion- Hierarchical VC

- Decrypted image losses a large of details
  - Round to integer
  - Decrypt with Lagrange basis formula.
  - Accumulating errors with two-level decryption.
- Sensitive to the selection of shares.
  - Sometimes decryption will fails.

Input Images

Decrypt Images



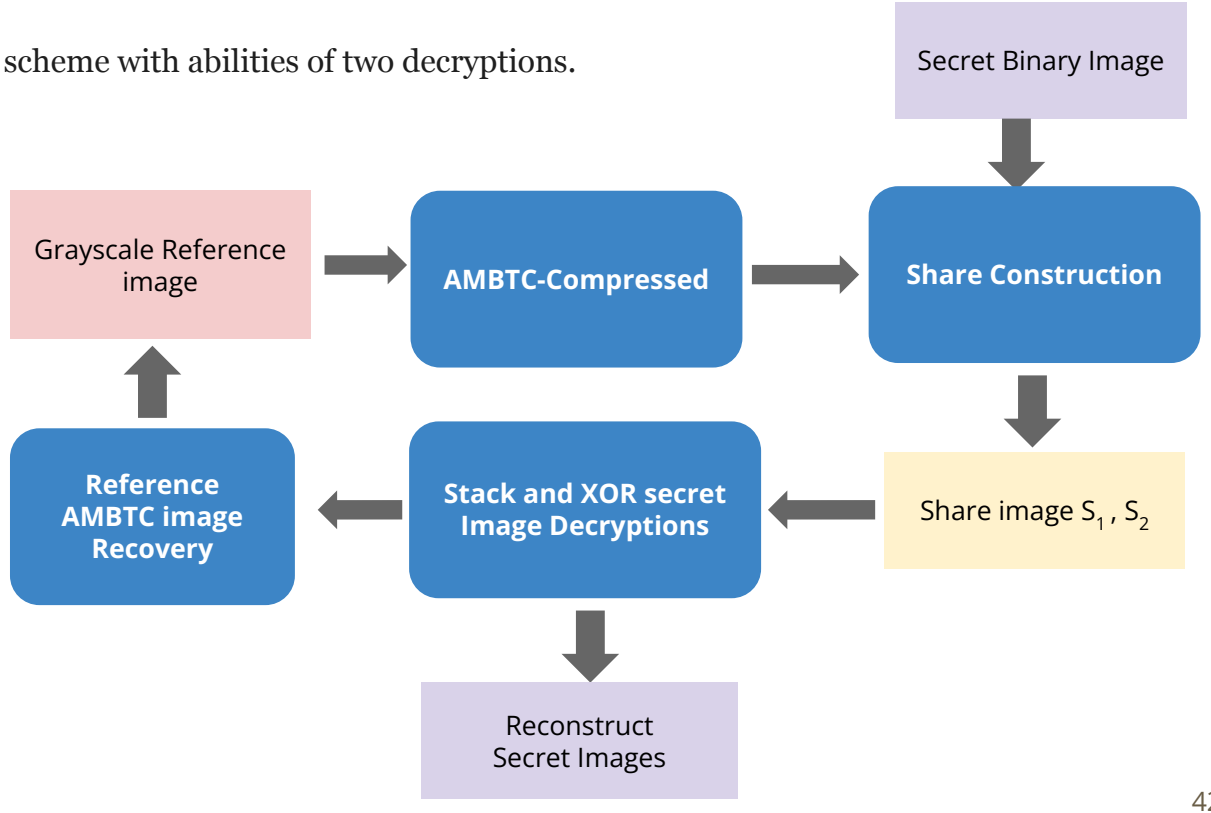
Algorithm - AMBTC

- Using AMBTC-compressed image to add secret images.
- Pros
  - Meaningful
  - Less Storage
  - Easy to decrypt secret. (Stack or XOR operation)
- Cons
  - Limit the type of secret images.

Algorithm - AMBTC

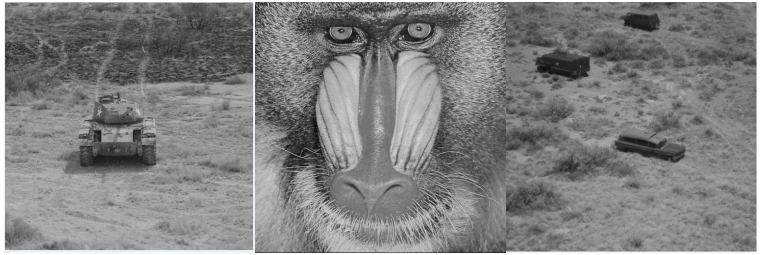
Reversible AMBTC-based secret sharing scheme with abilities of two decryptions.

- AMBTC-Compressed
- Share Construction
- Reconstruct
  - Partial: Stacking
  - Complete: XOR
- Recover algorithm



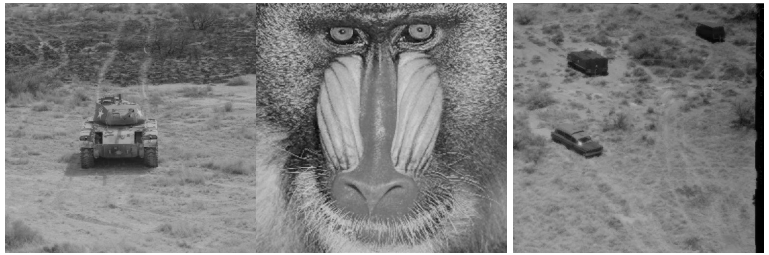
Experiment- AMBTC

References



Secret

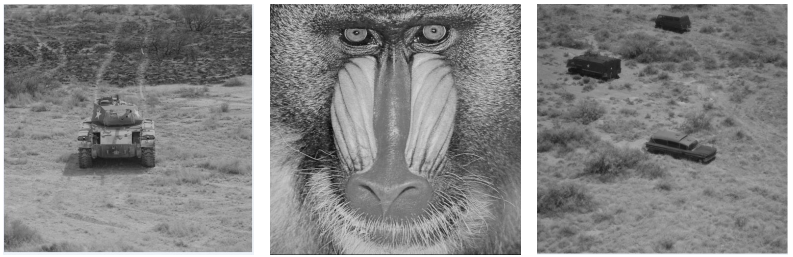
Shares



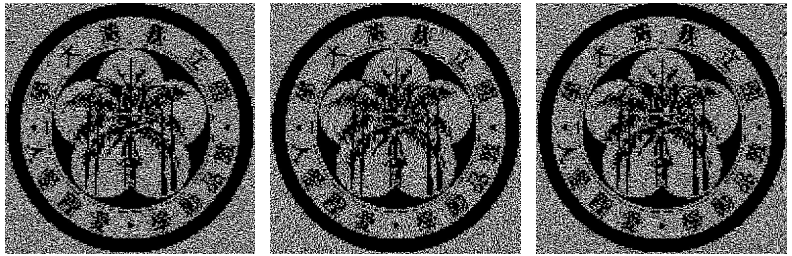
PSNR: 32.8 PSNR: 28.6 PSNR: 35.4

Experiment- AMBTC

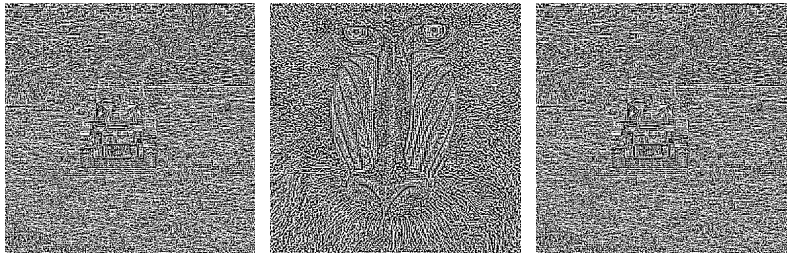
References



Stack



Recovery Bitmap



Secret

XOR

Discussion- AMBTC

- Less Storage

	Original Size	AMBTC-Compressed
Tank	262 (KB)	2*(12.3+12.3+53.9) (KB)
Mandril	263 (KB)	2*(12.3+12.3+53.4) (KB)
Car	262 (KB)	2*(12.3+12.3+53.6) (KB)

- Can only extend (2, m)-scheme along with additional reference images.

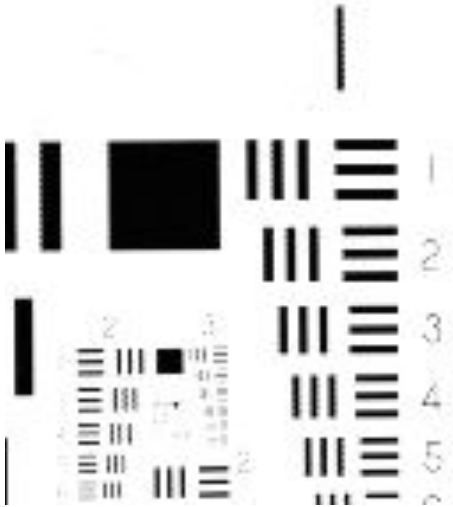
Discussions

Comparison

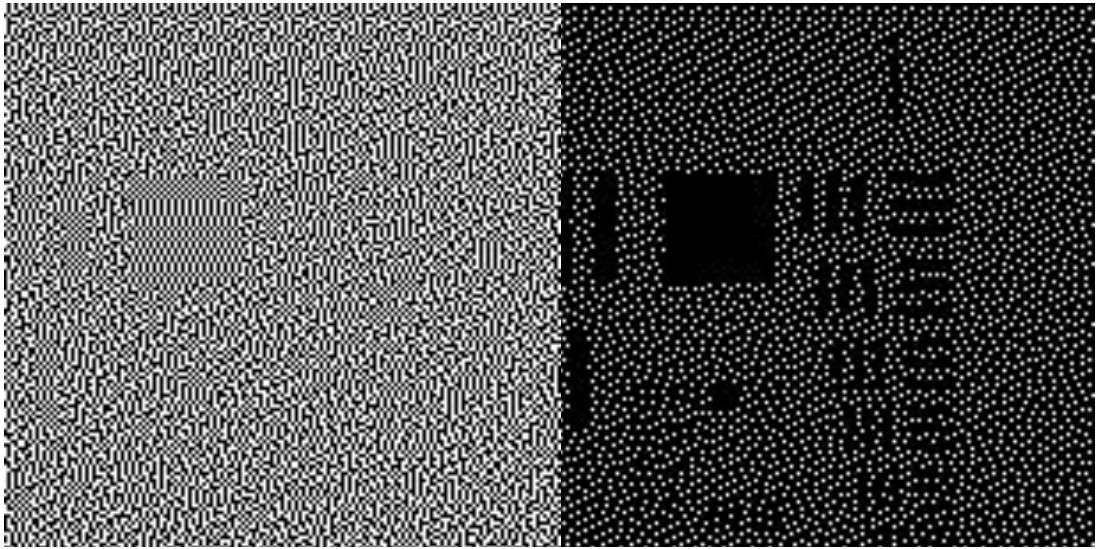
Method	Image type	(k, m) - scheme	Meaningful share	Pixel expansion
Naor and Shamir's	Binary	(2, 2)	Meaningless	Yes
Chen's pattern	Binary	(m, m)	Meaningful	No
IGVSS	Grayscale	(2, 2)	Meaningful	Yes
EVC	Grayscale	(2, 2)	Meaningful	Yes
Qing Ye's method	Grayscale	(2, 2)	Meaningless	No
Hierarchical VC	Grayscale	2*(k, m)	Meaningless	No
AMBTC	Binary + Grayscale	(2, 2)	Meaningful	No

Discussions

The type of the image may be not mutable.



Secret Image



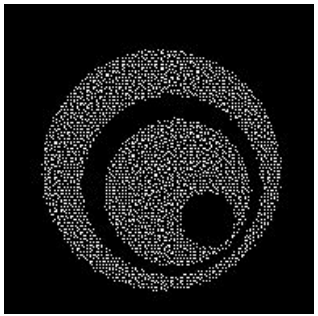
Share Images

Decrypted Image

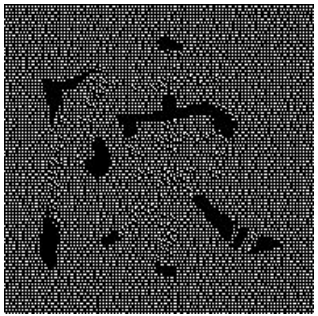
Discussions

Most of the methods are sensitive to parameters

Black block black pixels num: 3
White block black pixels num: 2



Black block black pixels num: 2
White block black pixels num: 1

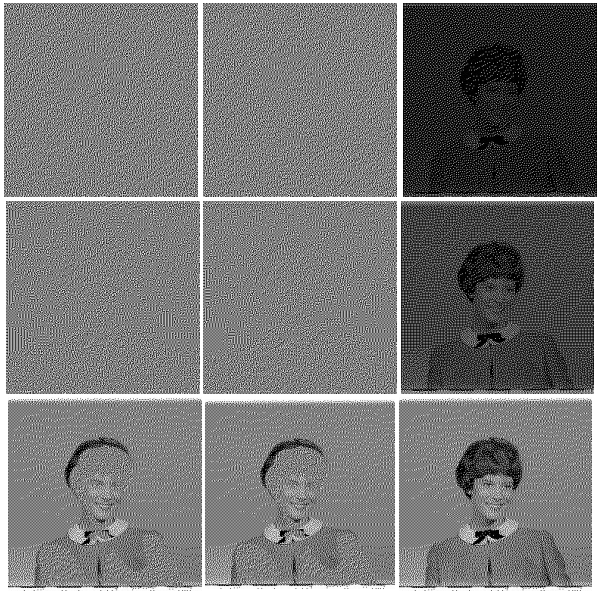


$$\tilde{f}_{ij} = \alpha \frac{f_{ij} - \min\{f_{ij}\}}{\max\{f_{ij}\} - \min\{f_{ij}\}},$$

α = 0.25

α = 0.5

α = 1



Discussions

Lack of metric for the robustness and privacy-preserving of the share images

- Common metrics for visual cryptography
  - Peak Signal-to-Noise Ratio (PSNR)
  - Unified Average Changing Intensity (UACI)
  - Number of Pixel Change Rate (NPCR)

Reference

1. Nakajima, Mizuko, and Yasushi Yamaguchi. "Extended visual cryptography for natural images." (2002).
2. Inoue, Kohei, Kenji Hara, and Kiichi Urahama. "Image Size-Preserving Visual Cryptography by Error Diffusion." ITC-CSCC, 2018.
3. Myodo, Emi, et al. "Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique." 2007 IEEE International Conference on Multimedia and Expo. IEEE, 2007.
4. 101 Computing.net. Visual cryptography, 2020. https://www.101computing.net/visual-cryptography/.
5. Moni Naor and Adi Shamir. Visual cryptography. In Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia,Italy, May 9–12, 1994 Proceedings 13, pages 1–12. Springer, 1995.
6. Chen Li-Ling and Wang Shuenn-Shyang. Visual cryptography for meaningful shares. Master's thesis, Tatung University, Jan 2007.
7. A. John Blesswin and P. Visalakshi. An improved grayscale visual secret sharing scheme for visual information security. In 2013 Fifth International Conference on Advanced Computing (ICoAC), pages 560–564, 2013.
8. DAS, Surya Sarathi, et al. A hierarchical image cryptosystem based on visual cryptography and vector quantization. In: *Contemporary Advances in Innovative and Applicable Information Technology: Proceedings of ICCAIAIT 2018*. Springer Singapore, 2019. p. 3-11.
9. OU, Duanhao; SUN, Wei. Reversible AMBTC-based secret sharing scheme with abilities of two decryptions. Journal of Visual Communication and Image Representation, 2014, 25.5: 1222-1239.