Secure Image Sharing: Comparative Insights into Visual Cryptography and Random Grid Models

1 Analytical Study on 2-out-of-2 Share Generation in Visual Cryptography

1.1 Abstract

Secret sharing-based schemes of visual cryptography permit secret image encryption and provide a secure method for accessing sensitive visual information. In the modern (k, n) secret sharing scheme, the secret image is partitioned into n shares. Any k out of n shares can reconstruct the secret. Many schemes such as (2, 2) VCS and segment-based approaches have been proposed. However, most methods work on binary images, limiting their usage in color image applications. Challenges like pixel expansion, alignment issues, flipping, and distortion remain largely unresolved.

1.2 Visual Cryptography

Visual cryptography, introduced by Moni Naor and Adi Shamir (1994), allows encryption of visual information into multiple shares, which can be decrypted visually by overlaying the shares. Different access structures include:

- **(2, 2) Threshold VCS:** Simple scheme using two shares.
- **(2, n) Threshold VCS:** Any 2 out of n shares can decrypt.
- **(n, n) Threshold VCS:** All n shares required to decrypt.
- **(k, n) Threshold VCS:** At least k of n shares required.

1.3 Basic Approach

Visual cryptography involves breaking each pixel into subpixels. For (2, 2) schemes:

- A black pixel is shared such that overlaying reveals black.
- A white pixel is shared to preserve transparency in overlay.
- Pixel expansion varies (2 or 4 subpixels).

1.4 Proposed Algorithm: DHCOD

The DHCOD (Data Hiding in Halftone Images using Conjugate Ordered Dithering) is a modified version of DHCED:

Steps:

1. Add noise to secret image $H \rightarrow H_1$.
2. Convert H_1 to binary: $H_1 \rightarrow H_2$.
3. Generate share X_1: halftoned from cover image X.
4. Generate share X_2:

$$X_2(i,j) = \begin{cases} X_1(i,j), & \text{if } H_2(i,j) \text{ is white} \\ X_1(i,j) \oplus \sim H_2(i,j), & \text{if } H_2(i,j) \text{ is black} \end{cases}$$

2 Analytical Study on Random Grid Technology

2.1 Abstract

Random Grid (RG) technology encrypts visual information into shares without pixel expansion. It creates multiple cipher grids that reveal no information individually but reconstruct the original when overlaid. RG ensures original image dimensions and allows visual decryption.

2.2 Random Grid Technology

Naor-Shamir's approach involves pixel expansion. Kafri and Keren proposed RG-based schemes to retain original size. RG schemes provide:

- No pixel expansion.
- High randomness and secrecy.
- Lightweight image processing.

2.3 2-out-of-2 Random Grid Algorithm

Algorithm Steps:

1. **Input:** Image I of size height $\times$ width.
2. **Output:** Cipher grids R_1 and R_2 (same size).
3. **Step 1:** Randomize R_1 with black/white pixels.
4. **Step 2:** For each pixel (x, y) in I:
   - If white: $R_2[x, y] = R_1[x, y]$
   - If black: $R_2[x, y] = 1 - R_1[x, y]$

Pseudocode:

Listing 1: Kafri-Keren 2-out-of-2 RG Algorithm

```
Input: Image I [height][width]
Output: R1, R2

WHITE = 0
BLACK = 1

# Step 1: Randomize R1
for row in range(height):
    for col in range(width):
        R1[row][col] = RANDOM(WHITE, BLACK)

# Step 2: Generate R2
for row in range(height):
    for col in range(width):
        if I[row][col] == WHITE:
            R2[row][col] = R1[row][col]
        else:
            R2[row][col] = 1 - R1[row][col]
```

3 Comparative Study

3.1 Methodological Comparison

- **VCS:** Uses pixel expansion; each pixel maps to subpixels; decoding through overlaying.
- **Random Grid:** Matrix grid with random generation; no pixel expansion; depends on logical XOR and image complementation.

3.2 Performance

Both techniques have linear time complexity $O(n)$, where n is the number of pixels. Each pixel is independently processed—making both approaches scalable.

3.3 Advantages and Disadvantages

(2,2) Visual Cryptography Scheme

Advantages:

- Simple visual decryption.
- Theoretically robust and well-documented.
- Effective for binary images.

Disadvantages:

- Pixel expansion increases size.
- Reconstructed image has low quality.
- Requires strict codebook structure.

Random Grid Visual Cryptography (RGVC)

Advantages:

- No pixel expansion.
- Perfect secrecy with no information leakage.
- Easy to implement—no codebooks needed.
- Customizable contrast schemes.

Disadvantages:

- Requires precise alignment.
- Limited support for colored images.
- Harder to intuitively understand.

Conclusion

This study provides a comparative view of (2,2) visual cryptography and random grid-based image security techniques. While visual cryptography is simpler and foundational, random grid methods offer more efficient storage and secrecy benefits. The choice depends on application-specific requirements such as image quality, computation limits, and alignment constraints.