Image Sharing Based on Chinese Remainder Theorem

Institute of Information Systems and Applications
Department of Computer Science
National Tsing Hua University
Hsinchu, Taiwan 30013
http://www.cs.nthu.edu.tw/~cchen

Outline

- Introduction
- Background Review
- Proposed Method
- Experimental Results
- Conclusion

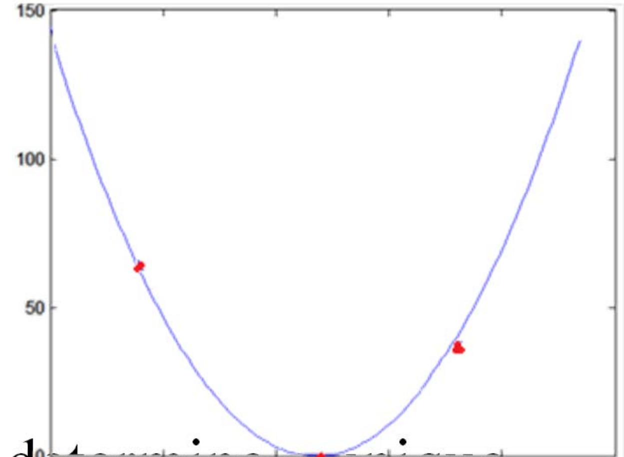
Introduction

- To avoid the information is carried by only a single individual
- Data are partitioned into n shadows and are distributed to n participants
- By collecting at least k out of n shadows, we can completely recover the original data (information)
- A (k,n)-threshold technique based on CRT is introduced

Background Review for (k,n)-threshold Techniques

- The secret value S is used to generate n shadows
- Any k or more shadows can recover the secret value S
- Fewer than k shadows cannot reveal the secret value S
- Commonly used (k,n)-threshold schemes for sharing
- Shamir [Sham1979]
- Blakley [Blak1979]
- Asmuth and Bloom [Asmu1983]

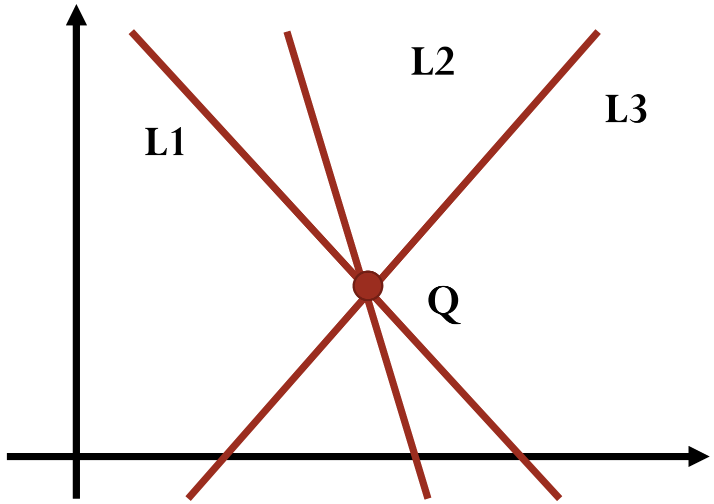
Shamir (1979)



- Based on polynomial interpolation
- Sharing
  - Given k distinct points in the 2-d plane, determine a unique polynomial of degree k-1
  - Put the secret message to the constant term, generate n shadow messages which are distributed to n participants
- Recovering
  - Polynomial interpolation to find the secret message

Blakley (1979)

- Uses the characteristic of geometry
- Sharing
  - Chooses a point Q which contains the secret value S in the k-dimensional space
  - Select n hyper-planes passing through the point Q as n shadows
- Recovering
  - Collect at least k hyper-planes
  - Solving a linear system of equations

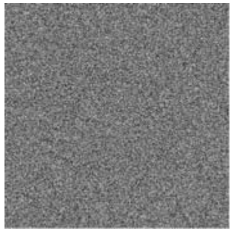
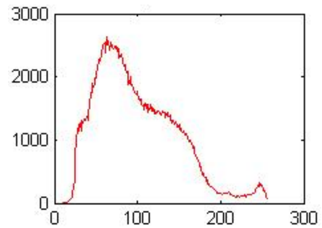


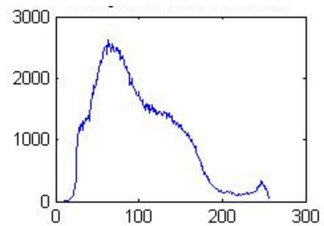
Asmuth and Bloom (1983)

- Requirements
  - A sequence of pairwise relatively prime positive integers
- Sharing
  - Modular arithmetic $I_i \equiv (s + \alpha \cdot m_0) \bmod m_i$
  - Random integer α
- Recovering
  - Based on Chinese Remainder Theorem to solve Congruence Eqs.

Background Review-Thien and Lin (2002)

1. Suppress all pixels whose gray values are larger than 250 to 250.
2. Permute the pixels



3.

k pixels

$$q(x)\equiv a_0+a_1x+\ldots+a_{k-1}x^{k-1} \pmod{251}$$

a_0	a_1	…	a_{k-1}	…

Permuted Image

$q(r_1)$		

. . .

$q(r_n)$		

Shadow Images

Background Review-Thien and Lin

1. Collect any k shadow images.

2.

$q(r_1)$		

. . .

$q(r_k)$		

Shadow Images

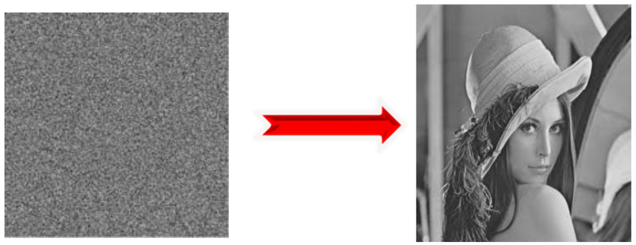
Polynomial interpolation

$$q(x) \equiv a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} \pmod{251}$$

a_0	a_1	…	a_{k-1}	…

Permuted Image

3. Permute the pixels inversely.



Background Review-Thien and Lin

- Distortion
  - Suppress pixels whose gray values are larger than 250 to 250.

a_0	a_1	…	a_{k-1}	…

Permuted Image

If p<250→store p

If p≥250→store 250 and p-250

250	a_0-250	…	a_{k-2}	a_{k-1}

Array E

Chinese Remainder Theorem

- Let $m_1, m_2, \ldots, m_k$ be integers with $\gcd(m_i, m_j)=1$ whenever $i \neq j$. There exists a unique solution x for the following simultaneous congruence equations in $[0, m_1 m_2 \cdots m_k)$

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv a_k \pmod{m_k}$$

Solution for Chinese Remainder Theorem

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\dots$$
$$x \equiv a_k \pmod{m_k}$$

$Step\ \ 1: Let\ z_i \equiv m_1 * m_2 * \ldots * m_{i-1} * m_{i+1} * \ldots * m_k$

$Step\ \ 2:$ Solve $\mathrm{y_i}$ for $\mathrm{y_i * z_i \equiv 1 \ (mod\ m_i)}$

$Step\ \ 3: \mathrm{x \equiv a_1 y_1 z_1} + \ldots + a_k y_k z_k \ \mathrm{(mod\ m_1 \ldots m_k)}$ is the solution

Background Review-
Mignotte's Scheme vs. Asmuth's Scheme

Mignotte's Scheme	Asmuth's Scheme
gcd(m_i, m_j)=1, for $1 \le i < j \le n$ $\prod_{i=1}^{k} m_i > \prod_{i=0}^{k-2} m_{n-i}$	gcd(m_i, m_j)=1, for $0 \le i < j \le n$ $\prod_{i=1}^{k} m_i > m_0 \cdot \prod_{i=0}^{k-2} m_{n-i}$
$I_i \equiv s \bmod m_i$	$I_i \equiv (s + \alpha \cdot m_0) \bmod m_i$
CRT	CRT

Background Review-Ulutas (Sharing)

1. Select a set $\{m_0 < m_1 < \ldots < m_n\}$ which satisfies

   (i) $\gcd(m_i, m_j) = 1$, for $1 \le i < j \le n$ (ii) $M = \prod_{i=1}^{k} m_i > m_0 * \prod_{i=1}^{k-1} m_{n-i+1}$

2.

p_0	p_1	…		
		…		
		…		p_n

Secret Image

If $p \ge m_0$

$y = p - m_0 + \alpha \times m_0$

$0 \le \alpha \le t$

If $p < m_0$

$y = p + \alpha \times m_0$

$t+1 \le \alpha < m_1 * \ldots * m_k$

$t \in [0, m_0)$

$y_i \equiv y \bmod m_i$ for $i=1,2,\ldots n$

y_1	

y_2	

. . .

y_n	

Shadow Images

Background Review-Ulutas (Revealing)

y_1

y_2

⋮

y_k

Shadow Images

CRT→y

$$\alpha = \left\lfloor \frac{y}{m_0} \right\rfloor$$

If $\alpha \leq t$

$p = m_0 + y \bmod m_0$

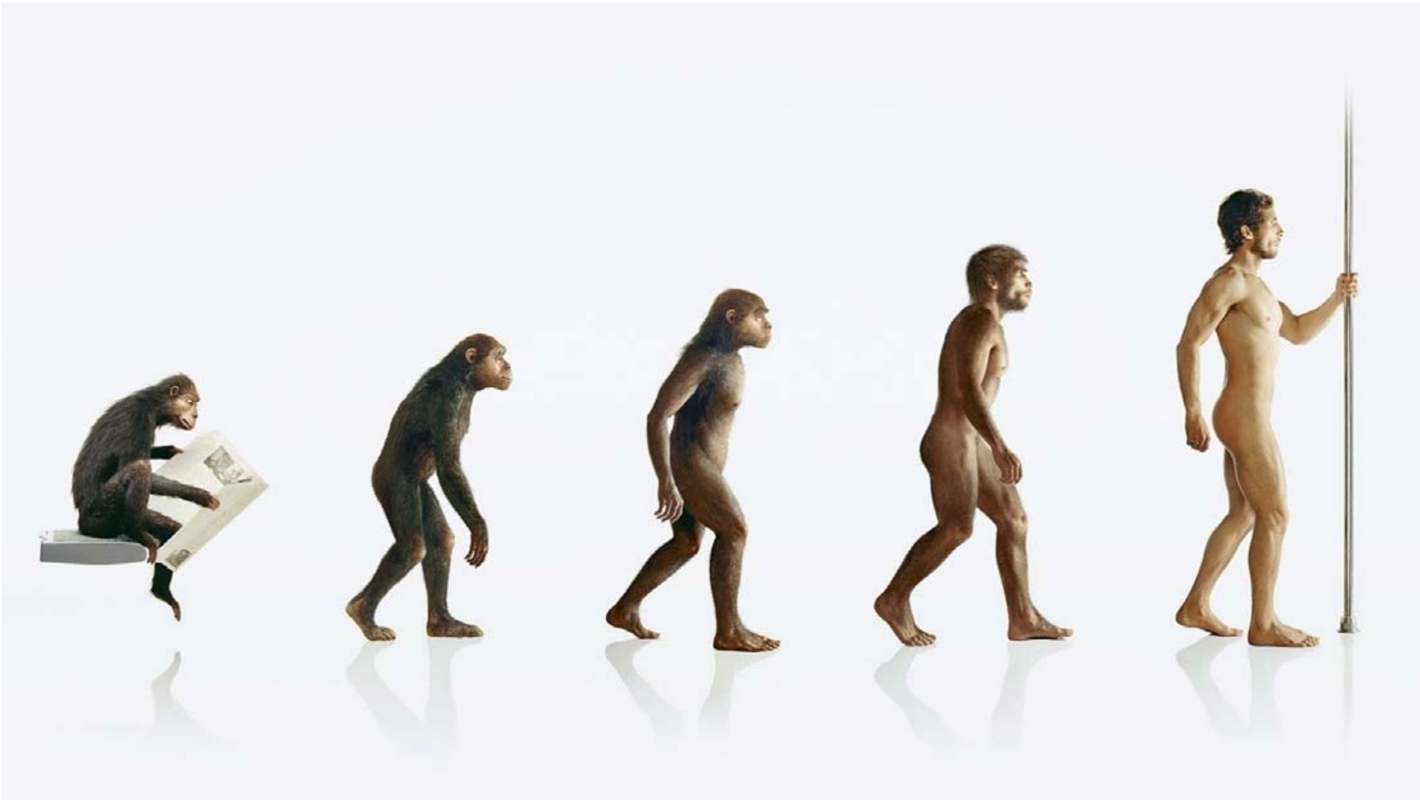
Else

$p = y \bmod m_0$

If $p \geq m_0$	If $p < m_0$
$y = p - m_0 + \alpha \times m_0$	$y = p + \alpha \times m_0$
$0 \leq \alpha \leq t$	$t+1 \leq \alpha < m_1 * \ldots * m_k$

$t \in [0, m_0]$

Proposed Method



https://lh4.ggpht.com/T7Qsp9L8qYLtaLk4-4Zgt8Nwy_FfvnDdxSL8c3BSF2Lk5X-CKjfxGjhbfbyHy5iHsB3YRA=s151

Proposed Method

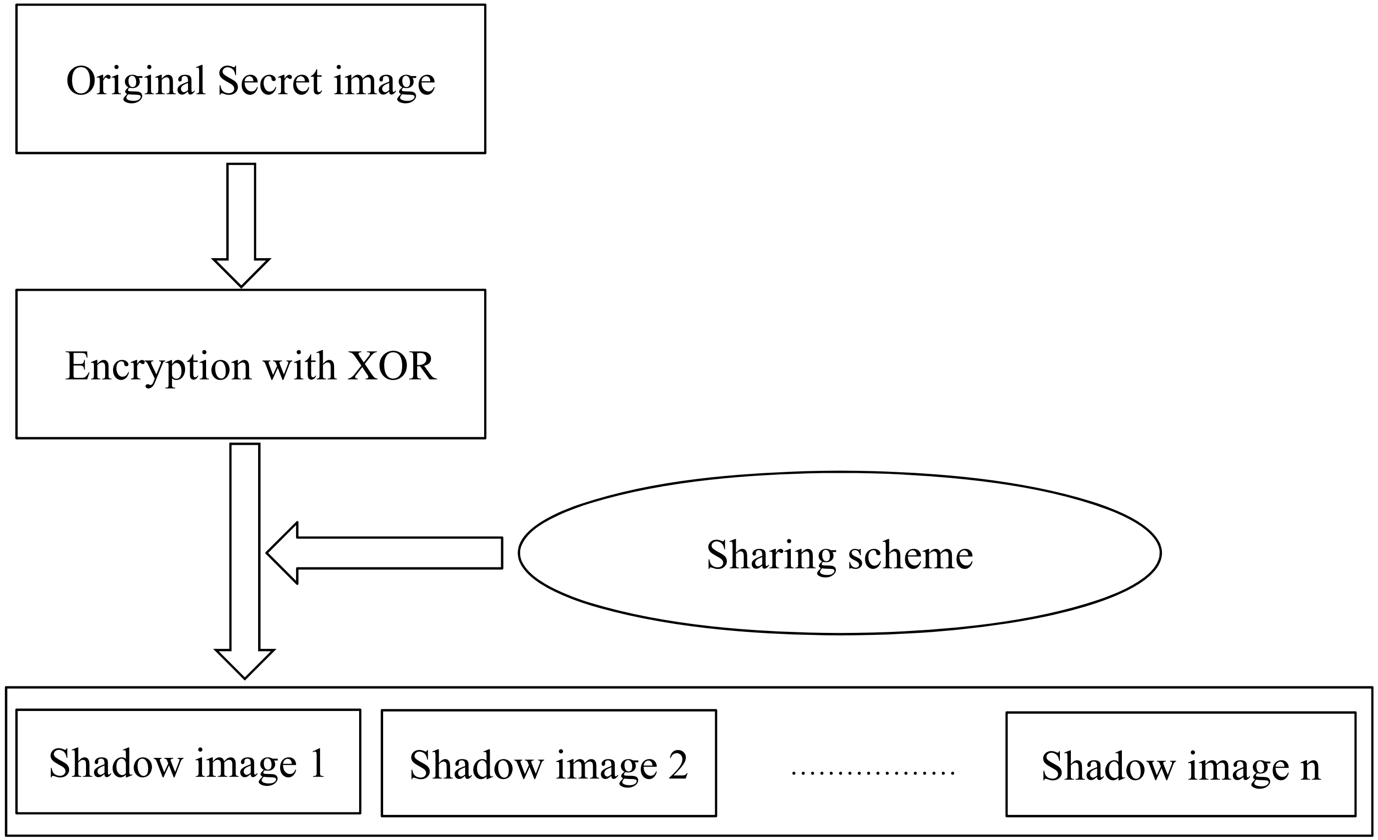
- Based on Ulutas scheme [Ulut2009], we proposed a method which uses the color image as the secret image.
- There are three values R, G, and B in each pixel of the color image, we need to compute these three values respectively.
- To strengthen the robustness and the reliability of our method, we encrypt the secret values using the simple exclusive-or (XOR) cipher with a 24-bit long key.

1	0	1	0	1	1	0	1

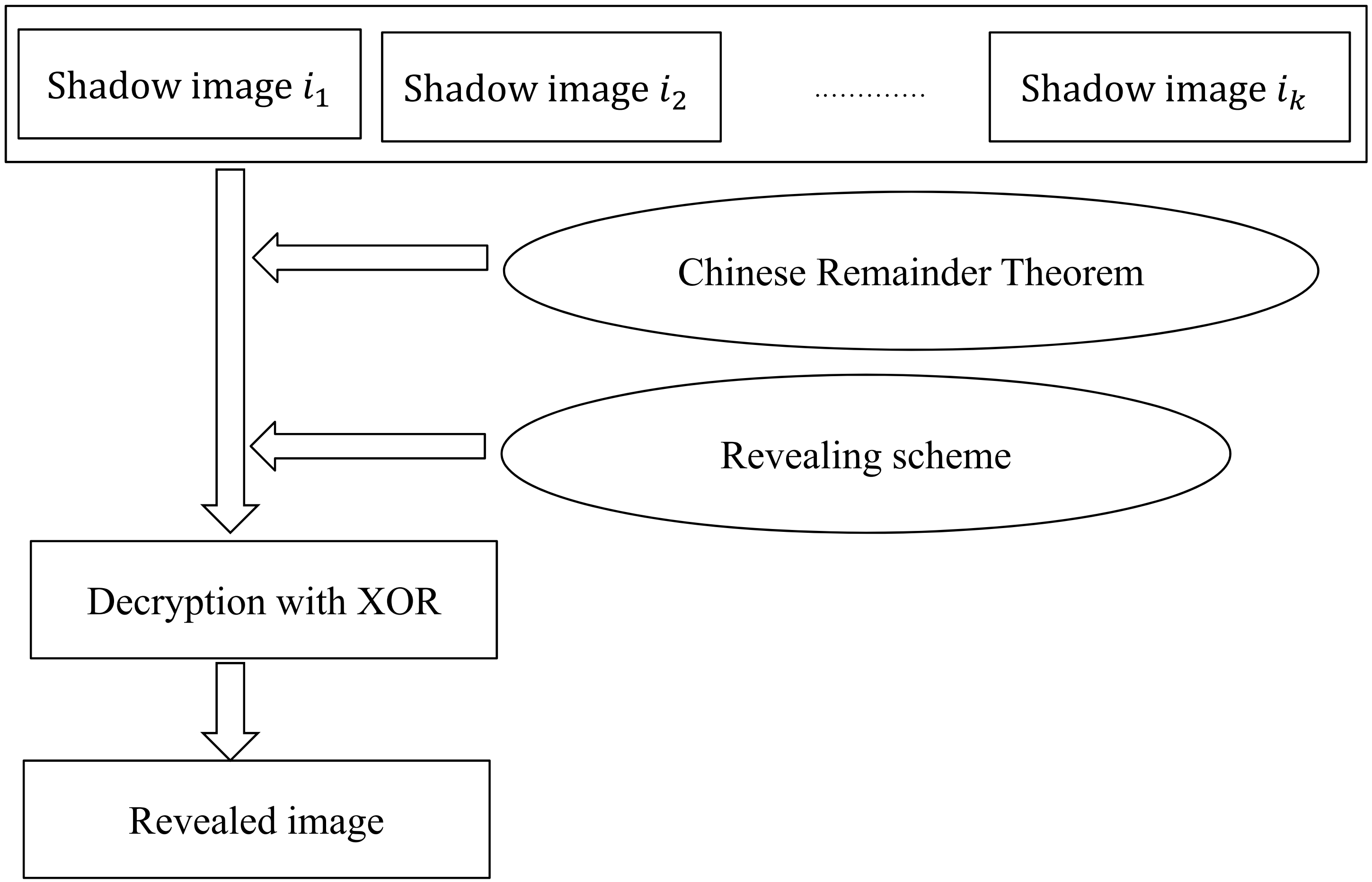
Last significant bit

+random integer→shares

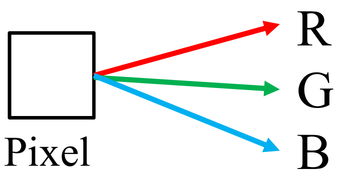
The Proposed Sharing Method



The Proposed Revealing Method



The Proposed Sharing Method



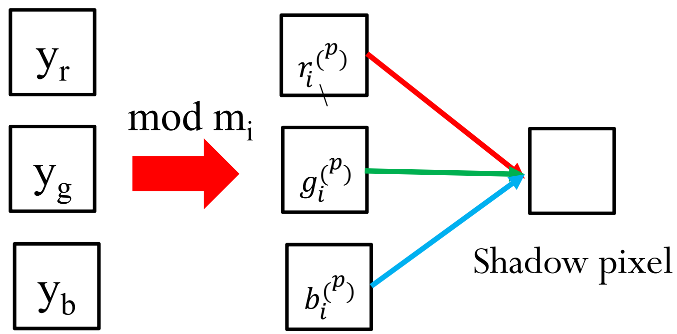
XOR

R R R R R R R R G G G G G G G G B B B B B B B B

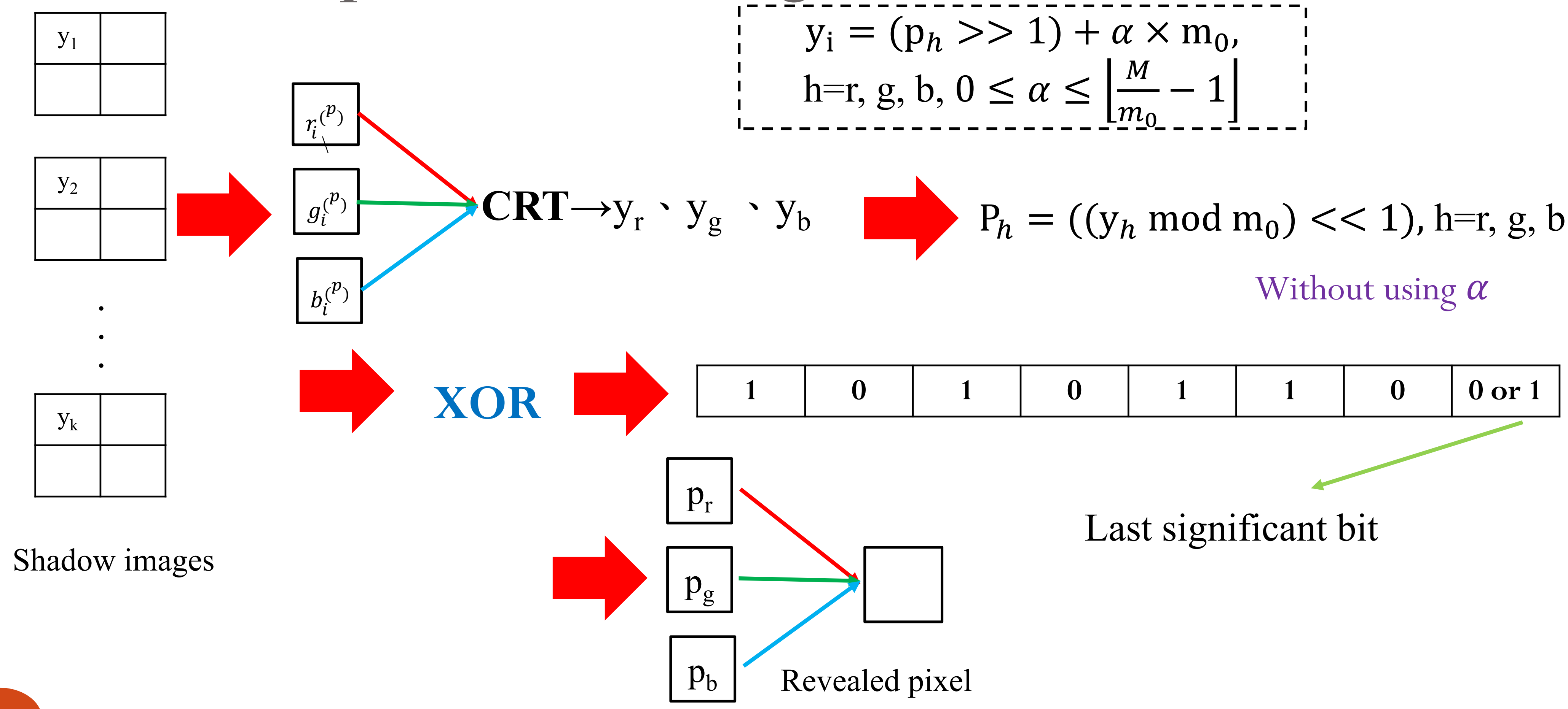
$\oplus$ 1 0 0 1 0 1 0 1 1 0 0 1 0 1 0 0 0 1 1 0 1 0 1 1

Encrypted R, G, B values

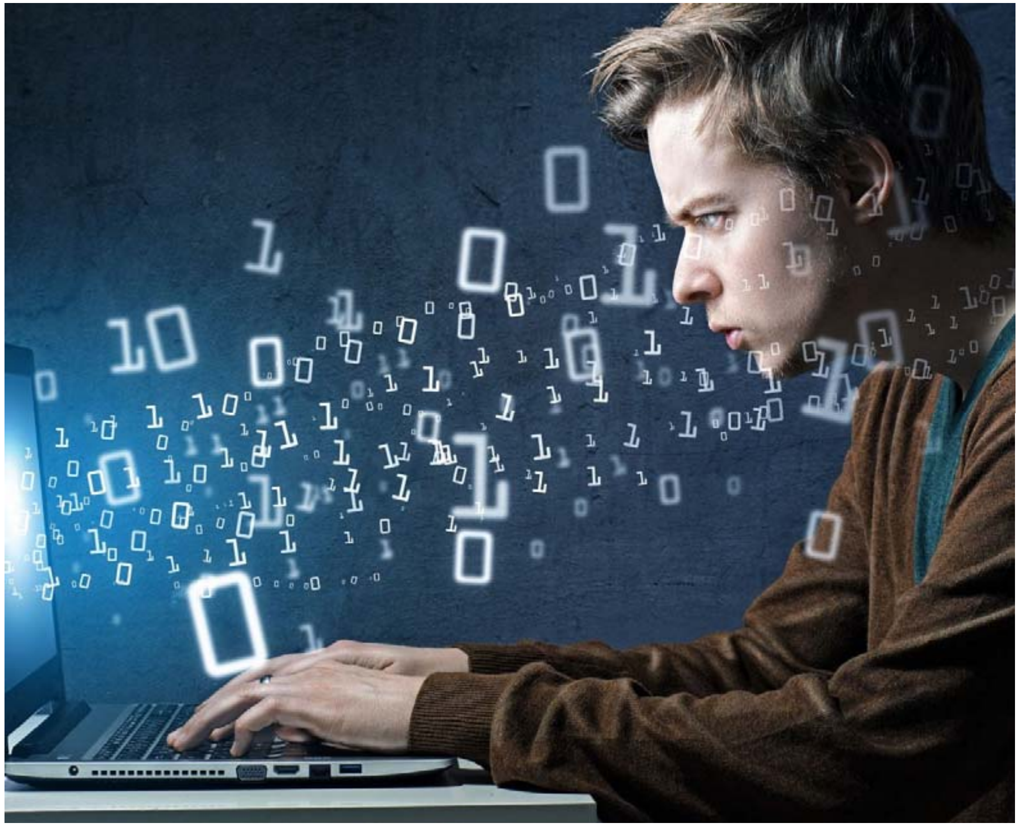
1. Do the XOR operation on each R,G,B values
2. Determine a set of integers $\{m_0, m_1, m_2, \ldots, m_n\}$ which satisfies
   (i) $m_0=128<m_1<\ldots<m_n<256$; (ii) $\gcd(m_i, m_j) = 1$, for $0\leq i<j\leq n$;
   (iii) $M = \prod_{i=1}^{k} m_i > m_0 * \prod_{i=1}^{k-1} m_{n-i+1}$
3. $y_h = (p_h >> 1) + \alpha \times m_0$,
   h=r, g, b, $0 \leq \alpha \leq \left\lfloor \frac{M}{m_0} - 1 \right\rfloor$
4.



The Proposed Revealing Method



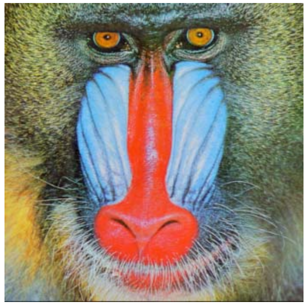
Experimental Results

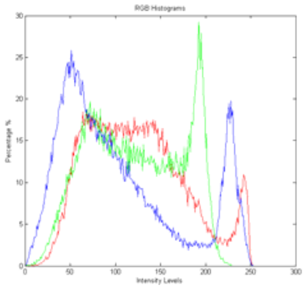


http://blog.toggl.com/wp-content/uploads/sites/5/2014/10/programmer-at-work.jpg

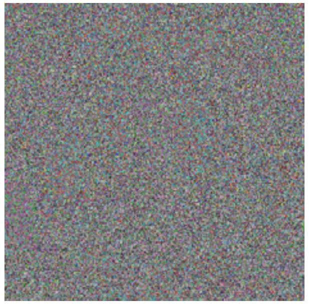
Experimental Results - Mandrill

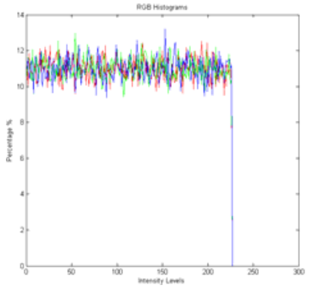
Original image



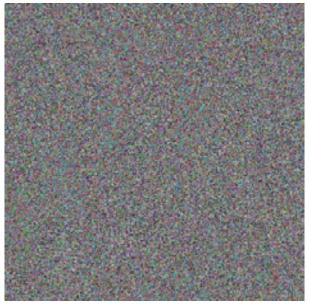


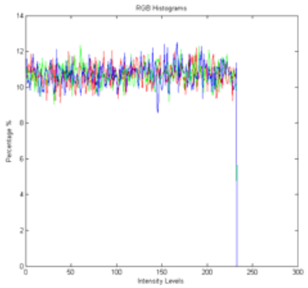
Shadow image1



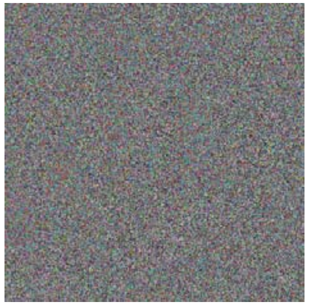


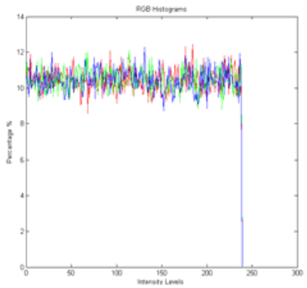
Shadow image2



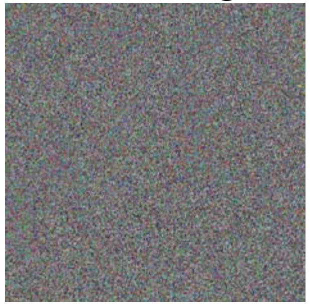


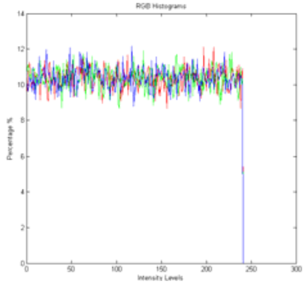
Shadow image3



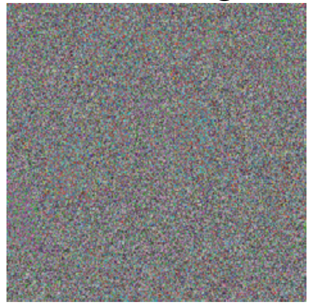


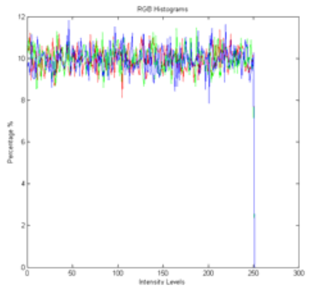
Shadow image4



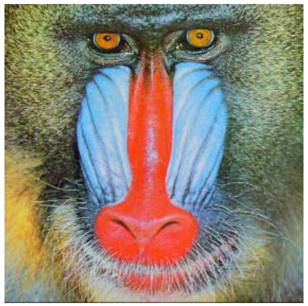


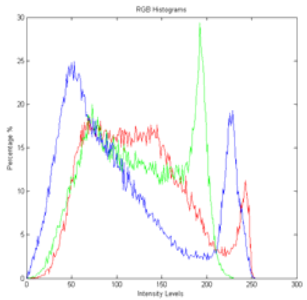
Shadow image5





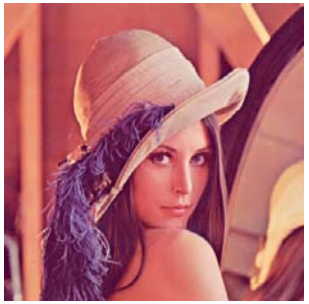
Revealed image



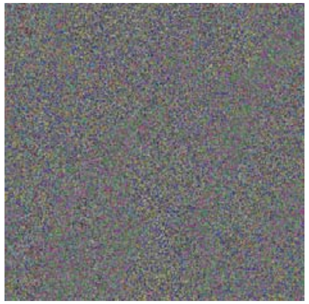


Experimental Results - Lenna

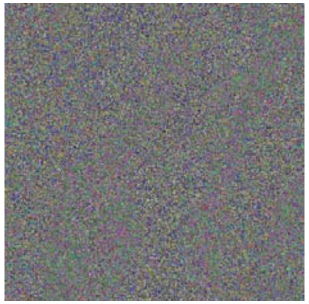
Original image



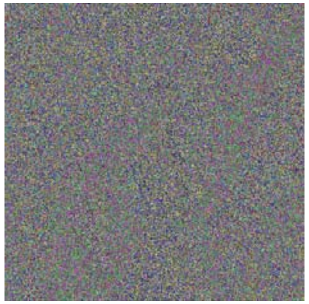
Shadow image1



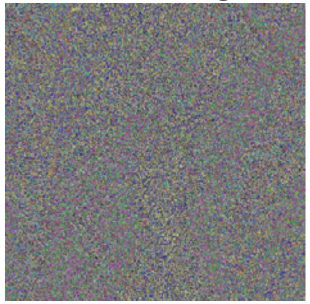
Shadow image2



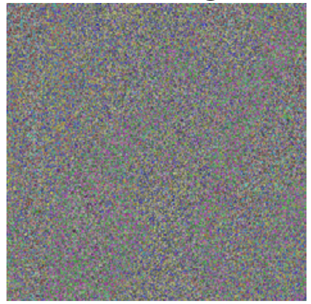
Shadow image3

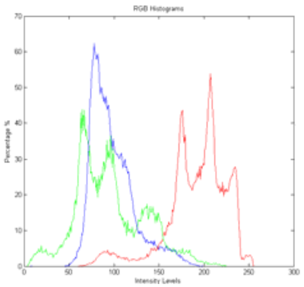


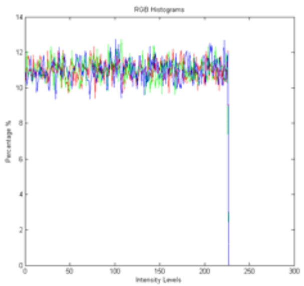
Shadow image4

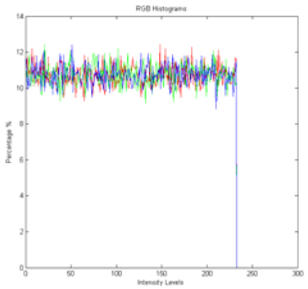


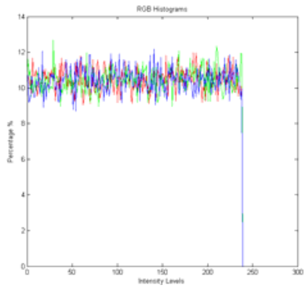
Shadow image5

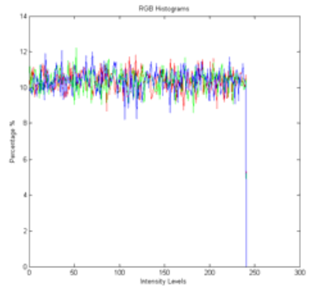


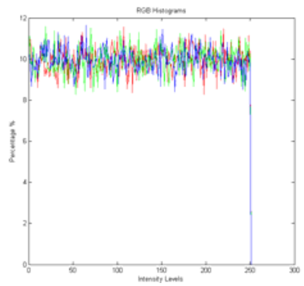




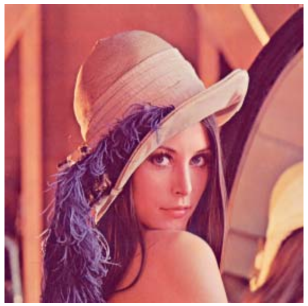


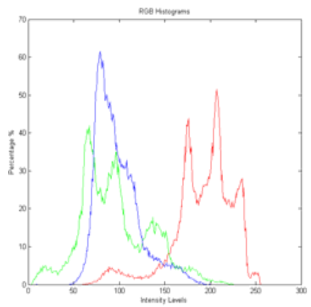






Revealed image

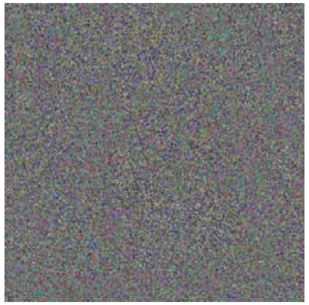




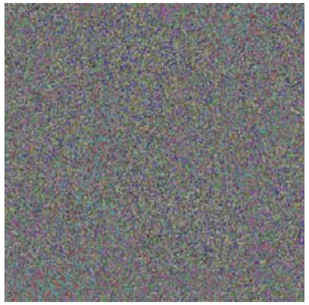
Experimental Results - Peppers

Original image

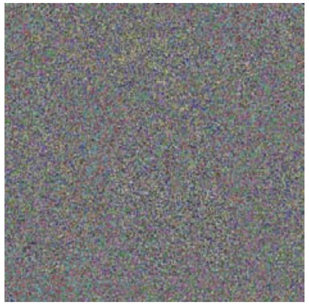
Shadow image1



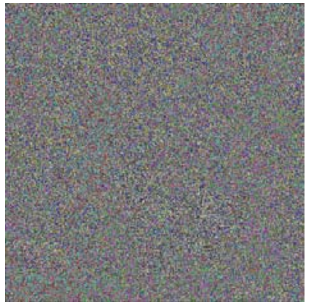
Shadow image2



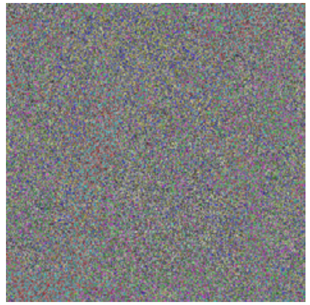
Shadow image3

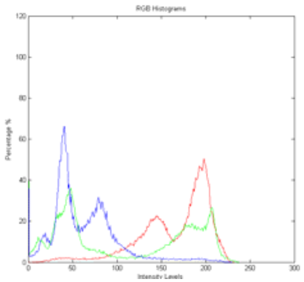


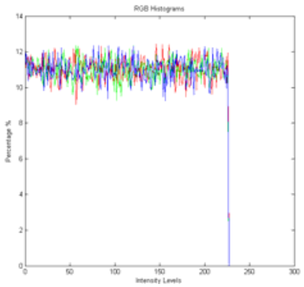
Shadow image4

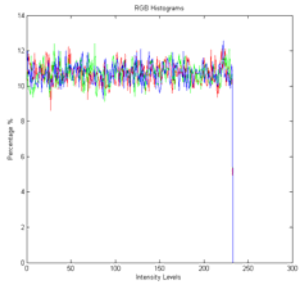


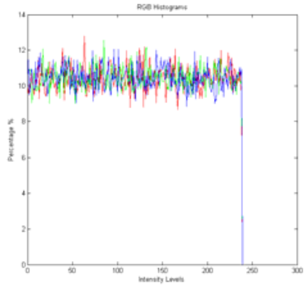
Shadow image5

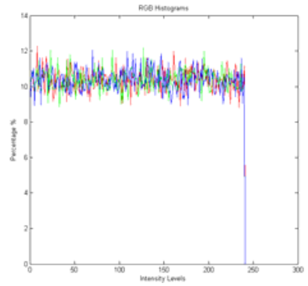


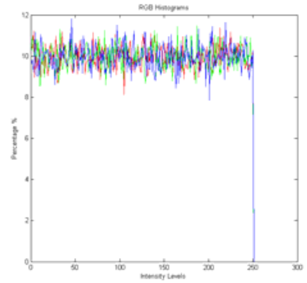




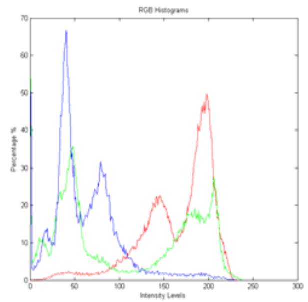








Revealed image



Experimental Results

- Sharing time and revealing time of three secret images

	Sharing time (sec.)	Revealing time (sec.)
Baboon	6.37	4.10
Lenna	6.57	4.13
Peppers	6.31	3.93

Conclusion

http://www.oldinsuranceguy.com/wp-content/uploads/2013/12/conclusion-diagram-in-blank.jpg

Conclusion

- Based on Ulutas's scheme, we proposed a secret image sharing method which uses color image as secret image and Chinese remainder theorem to reveal the secret image.
- In our method, we can only reveal a distortion image. Generally speaking, naked eyes cannot distinguish the difference between the secret image and distortion image with only the difference of the least significant bit.