

How to Secretly Share the Treasure Map of the Captain?

Naveed ISLAM, William PUECH and Robert BROUZET

naveed.islam@lirmm.fr, william.puech@lirmm.fr, robert.brouzet@unimes.fr

LIRMM, UMR 5506 CNRS, Université Montpellier II

THE PROBLEM:

To securely share an image between a group members exploiting additive homomorphic property of public key cryptosystem such as Paillier encryption scheme.

OUR APPROACH:

1. Asymmetric cryptosystem of Paillier is applied for encryption of $l+1$ images, where one is the secret image to be shared and all the other are individual secret images used for shared trust and security.
2. Due to additive homomorphic property of Paillier, addition operation over the plain text will give same result as multiplication over ciphered text.
3. Extraction of secret image is possible only if the individual secret images are available.

1- Paillier Algorithm [1]

- Select two large primes, p and q .
- Calculate the product $n=p \times q$, such that $\gcd(n, \Phi(n)) = 1$, where $\Phi(n)$ is Euler Function.
- Choose a random number g , where g has order multiple of n or $\gcd(L(g^\lambda \bmod n^2), n) = 1$, where $L(t) = (t-1)/n$ and $\lambda(n) = \text{lcm}(p-1, q-1)$.
- The public key is composed of (g, n) , while the private key is composed of (p, q, λ) .
- The Encryption of a message $m < n$ is given by:
 - $c = g^{m+r} \bmod n^2$
- The Decryption of ciphertext c is given by:
 - $m = (L(g^\lambda \bmod n^2) / L(g^\lambda \bmod n^2)) \bmod n$

2- Homomorphic Encryption

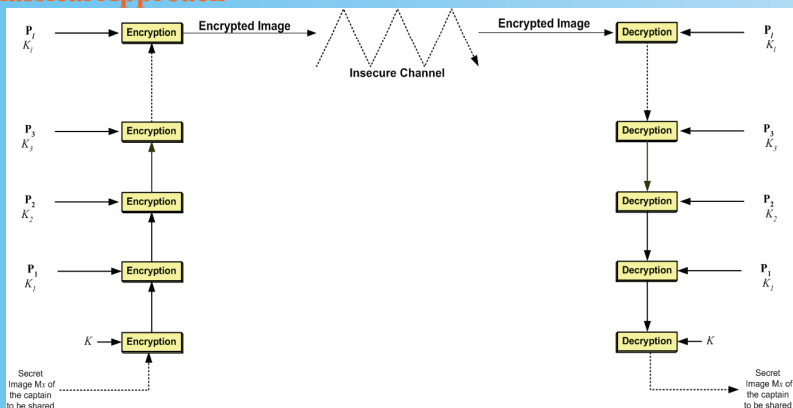
$$E(x \otimes y) = E(x) \oplus E(y)$$

The generalized additive homomorphic property of Paillier encryption follows that

$$\left(\prod_{i=1}^l E(m_i) \right) = E\left(\sum_{i=1}^l m_i \right)$$

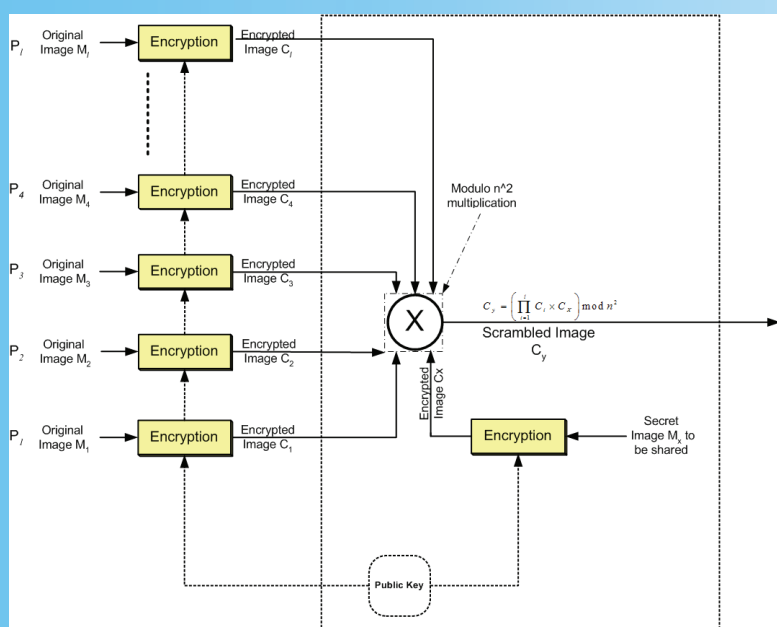
3- Classical Approach

a. Classical Approach

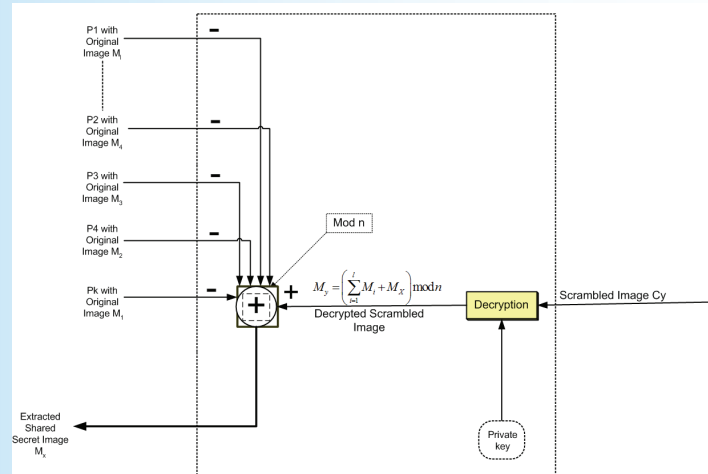


4- Proposed Approach

a. Overview of proposed encryption method

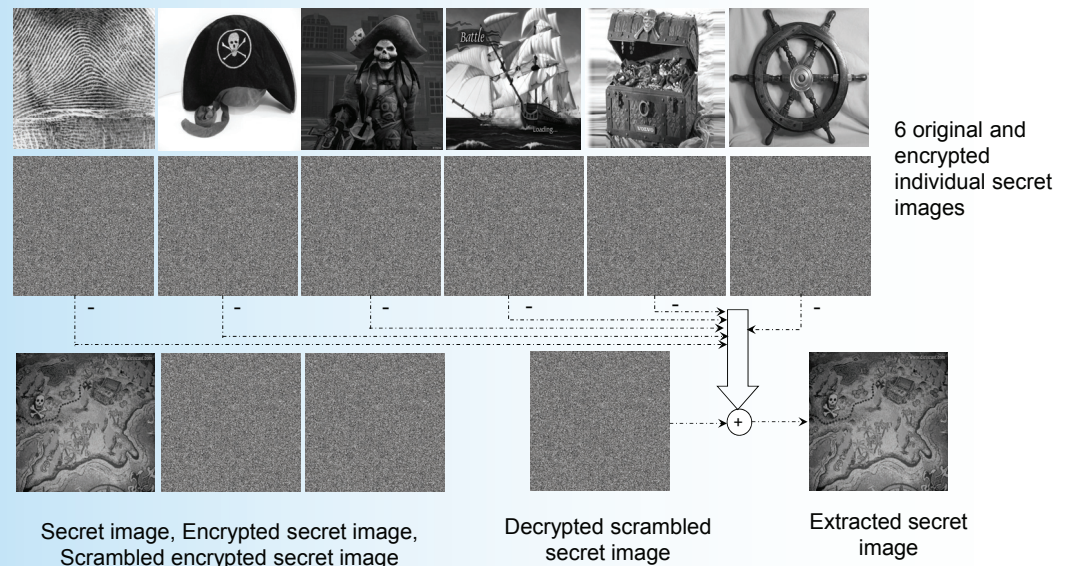


b. Decryption and Extraction of the protected shared image



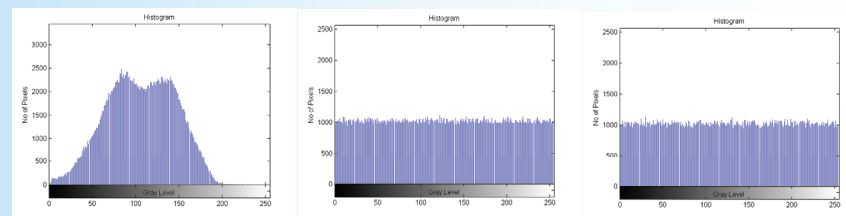
5- Experimental Results

Example:



6- Security Analysis

Histogram:



Entropy and Local Standard deviation:

	Original Image	Transferred Scrambled Image	Redundancy
1st Order Entropy	7.28 b/p	7.99 b/p	0.01 b/p
2nd Order Entropy	13.35 b/p	15.80 b/p	0.20 b/p
Local Standard Deviation	38.70	73.86	

Correlation of Adjacent Pixels:

	Original Image	Transferred Scrambled Image
Horizontal	0.8287	1.7112×10^{-4}
Vertical	0.8529	0.0027
Diagonal	0.7905	0.0034

7- Conclusions

- Secret sharing of images exploiting homomorphic properties of Paillier algorithm using carrier images is a new concept.
- Double security is provided, one in the shape of the private key and second in the shape of the secret image.
- Extraction of original image from the transferred image is possible with the help of carrier images.
- The proposed method can be used on any public key cryptosystem satisfying homomorphic properties.