Shamir's Secret Image Sharing

Alexander Yudnikov, Nikolay Skuratov

Project report

1 Abstract

Secret sharing schemes is one of basic cryptographical concept. Main goal of the project is to study Shamir's secret sharing scheme and apply it to image. Towards solving this task, image can be both grey scale and RGB and we want distributed keys also to be an images. Main idea is to encode source image in such way, so we could securely apply Shamir's secret sharing scheme to share an image between users.

2 Related Work

First, let's introduce Shamir's secret sharing scheme [1]:

1. Given k points in 2-d plane $(x_1, y_1), \dots (x_l, y_k)$, where is one and only one polynomial $q(x)$ of degree $k-1$ such that $q(x_i) = y_i$ for all i.
2. Data D is a number or can be made a number.
3. Dividing D on D_i we pick random k-1 degree polynomial:
   $q(x) = a_0 + a_1 x + \dots + a_{k-1}x^{k-1}$,
   where $a_0 = D$, $D_1 = q(1), \dots D_n = q(n)$.
4. Knowing any k subset of D_i's $q(x)$ could be found by interpolation and then evaluate $D = q(0)$.

This process is made more precise by using modular arithmetic instead of real arithmetic. The set of integers modulo a prime number p forms a field in which interpolation is possible. Given an integer valued data D, we pick a prime p which is bigger than both D and n. Coefficients $a_1, \dots, a_{k-1}$ are randomly chosen from uniform distribution over $[0, p)$. Items $D_1, \dots, D_n$ are computed modulo p.

Let's evaluate this method by looking on following example. Assume $k-1$ of n pieces are revealed. For each value D' in $[0, p)$ one and only one polynomial $q'(x)$ of $k-1$ can be constructed such that $q'(0) = D'$ and $q'(i) = D_i$ for $k-1$

given arguments. Those p possible polynomials are equally give nothing about real value of D.

This scheme is quite far from real life nowadays for several reasons, for example, in some real life tasks we need to give priority or privileges to some users[2]. Also, there visual secret sharing schemes, which are working not with numbers, but with pixels or blocks of pixels, to which modular arithmetic is applied[3]. Trying more complex schemes, like the one discussed in [3], could be done in future. Problem with most of visual cryptography schemes, that most of them is working with binary or black/white images, what is not actual nowadays.

3 Experiment Setup

We are doing our experiments with the following pipeline:

1. We find effective and secure way to encode image in order to apply to this number or byte string Shamir's secret sharing scheme.
2. We divide encoded image into parts, in order to apply sharing scheme[1].
3. For each part we construct polynomial and divide this part as a secret.
4. From each part we take a share to form a key. Key is formed as 128x128 greyscale image.
5. Then, we decode image by combining k out of n keys and evaluate it.

4 Obtained results

In this experiment we follow the setup described above. We read an image as a byte-like object an encode it as a HEX string. Then we divide it into parts of 4 bytes and for each part we construct a polynomial and obtain a set of shares for each part. Taking a share from each part we construct set of keys and distribute them as 128x128 greyscale images(Fig. 2). Keys are the greyscaled images filled with zeros(black pattern in the bottom of the image) to be resolution of 128x128. Example of original image and encoded you can see on Fig. 1.

Instead of encoding it as a HEX string, to provide more security we can encode an image with AES or RSA and share AES key or RSA public key with scheme described above. But still some encoded images could not resist differential and other types of attacks, so not authorized users can access the data. But in order to prevent it we can apply some techniques, such as chaos mapping[4].

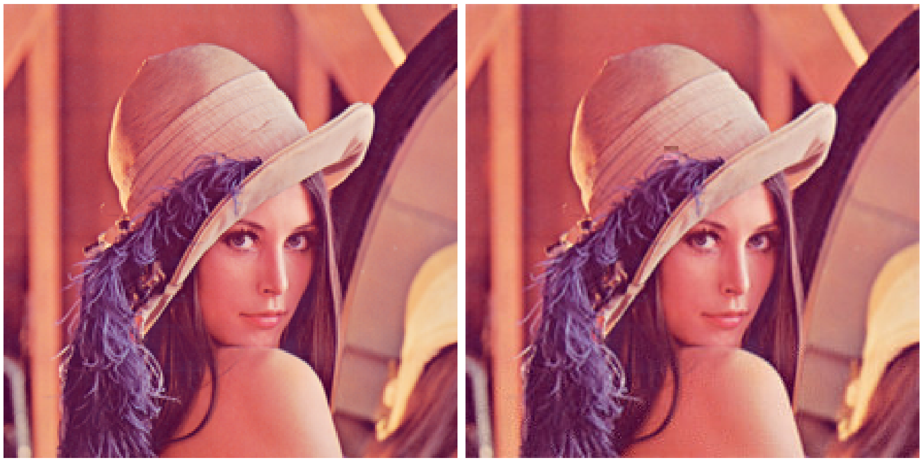

Figure 1: Image before transforming and sharing and after.

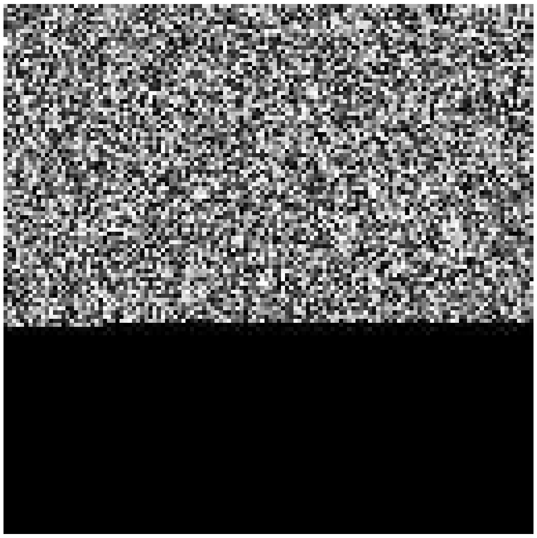

Figure 2: Example of Generated Key

5 Conclusion

We managed to securely divide and share an image and reconstruct and decode it buy combining obtained . We can reconstruct image after combining obtained image keys, while in most cases of image encoding and sharing keys are text or string files. Dividing an image into parts allows us not only to apply Shamir's secret sharing scheme, but also gives us more security by rising complexity of polynomial reconstruction task. Also it is crucial to fight calculation inaccuracy, what can lead to image artifacts in decoded image, what remains the main challenge in implementing such scheme.

6 GIT

On the following link you can find our code:
https://github.com/KrowosDogg/blockchain_sk2019_project

References

[1] Shamir A. *"How to share a secret"* Commun. ACM — New York City: ACM, 1979. — Vol. 22, Iss. 11. —P. 612–613

[2] Zhen Wu, Yi-Ning Liu, Dong Wang and Ching-Nung Yang *"An Efficient Essential Secret Image Sharing Scheme Using Derivative Polynomial"* Symmetry. 11. 69. 10.3390/sym11010069.

[3] Manami Sasaki ; Yodai Watanabe *"Visual Secret Sharing Schemes Encrypting Multiple Images."*, IEEE Transactions on Information Forensics and Security (Volume: 13 , Issue: 2 , Feb. 2018)

[4] Sankpal, Priya Vijaya, P. *"Image Encryption Using Chaotic Maps: A Survey."*, Proceedings - 2014 5th International Conference on Signal and Image Processing, ICSIP 2014. 102-107. 10.1109/ICSIP.2014.80.