A Variable Threshold Image Secret Sharing Method

Shanzheng Liu, Hang Zhang, Ying Yu, Hongliang Cai, Dan Tang*

School of Software Engineering, Chengdu University of Information Technology, Chengdu, Sichuan, 610225, China
*Corresponding author’s e-mail: 1477392934@qq.com

Abstract. Image secret sharing has been widely discussed in recent years because of its high security. The threshold variable image secret sharing method is a hot research topic recently. The Lagrange interpolation method is easy to establish. Therefore, most of the existing secret sharing schemes are based on Lagrange interpolation polynomials. However, when the secret is updated, the existing secret sharing scheme needs to re-establish the polynomial, and the original computing resources cannot be utilized. When the cheater is found, it is not convenient to add or delete participants flexibly, resulting in a large waste of computer resources. Therefore, an image secret sharing method with variable threshold based on Newton interpolation method is proposed, which can reduce the computational complexity of the system and the amount of repeated computation. The experimental results show that the method is superior when the threshold is changed.

1. Introduction

Image secret sharing technology belongs to an important branch of cryptography research. Dividing secret information into several small parts is helpful to prevent information from being too concentrated and abused, and it is of great significance to protect the security and integrity of secret[1]. At present, some secret sharing methods are mostly based on Lagrange interpolation[2] for image secret restoration. When cheaters are found, it is not convenient to dynamically add or delete participants[3]. Therefore, it has become a hot research problem to study how to minimize the consumption of computing resources under the condition of variable threshold.

In recent years, many scholars use Lagrange interpolation to restore secret images. Thien and Lin et al.[4] used PISSS method to encrypt the image. In the secret information recovery stage, the Shared information was combined with Lagrange interpolation method to restore the image. Pang et al.[5] also used Lagrange interpolation to restore secret image information in their multi-secret sharing scheme[6]. Lagrange interpolation is widely used because of its compact formula structure and convenience in theoretical analysis.

However, in the calculation, when the interpolation point increases or decreases by one, all the corresponding basic polynomials need to be recalculated, so the whole formula will change, which is very tedious. However, Newton interpolation method[7] is composed of multi-order difference quotient, which is more flexible and simple in calculation. Especially when nodes are added, only one item is needed in calculation, which makes up for the deficiency of Lagrange interpolation polynomial. Newton interpolation method is closely related to other aspects of numerical calculation and is suitable for functions with relatively complex structure. Therefore, Newton interpolation method is more suitable for threshold variable image secret sharing method.

The organization of this paper is as follows: section 2 introduces the relevant background, including
the introduction of image secret sharing method, and Newton interpolation method. Section 3 describes
the threshold variable image secret sharing method proposed in this paper, and describes the process of
increasing threshold and reducing threshold in detail. In section 4, the computational complexity of
Lagrange interpolation and Newton interpolation is compared when the threshold is increased or
decreased. The computational complexity is divided into addition and subtraction parts and
multiplication and division parts for comparison. Section 5 summarizes the threshold variable image
secret sharing methods of two different methods.

2. Related background

2.1. Image secret sharing
Secret sharing technology was originally proposed by Shamir et al.[8] A secret information sharing
method based on the characteristics of polynomials. This method splits the secret into n parts, and only
when k or more Shared parts are obtained can the secret be recovered. No less than k copies can be obtained. Later, this method was gradually extended to images, and the process of taking images as
secret information was mainly divided into the stages of secret image splitting and secret recovery. In
the encryption stage, polynomial is used to split, and when decrypting, Newton interpolation method
and Lagrange interpolation method can be selected[9]. According to the principle of the algorithm, the
calculation amount required is also different. The specific split process is as follows:

![Figure 1. Image secret sharing schematic](image)

2.2. Newton interpolation
As a commonly used numerical fitting method, Newton interpolation is also a form of algebraic
interpolation. It is widely used in experimental analysis because of its simple and flexible calculation.
First, the definition of difference quotient is introduced, and the function \( f(x_i) \) and a series of
unequal \( x_0, x_1, \ldots, x_n \) (\( i = j, x_i! = x_j \)) the value of \( f(x_i) \) \( f(x_i, x_j) \) calls \( f(x) \) the first difference quotient
at the points \( x_i \) and \( x_j \), and it is denoted as: \( f[x_i, x_j] = (f(x_i) - f(x_j))/(x_i - x_j) (i! = j, x_i! = x_j) \).

From the definition of difference agreement, it can be seen that: high order difference quotient is
the difference quotient of two low order difference quotient. Using difference quotient, the solution of
Newton interpolation can be expressed as follows:

\[
N_n(x) = f(x_0) + f[x_0,x_1](x - x_0) + f[x_0,x_1,x_2](x - x_0)(x - x_1) + \cdots + f[x_0,x_1,\ldots,x_n](x - x_0)(x - x_1)\cdots(x - x_{n-1}).
\]

The interpolation formula in the form of difference quotient is called Newton interpolation formula. The general recurrence formula is:

\[
N_{k+1}(x) = N_k(x) + (x - x_0)(x - x_1) \cdots(x - x_k)f[x_0,\ldots,x_k,x_{k+1}].
\]

Because the calculation of Newton interpolation method is relatively simple, especially when the
node is added, only one item is added in the calculation, which greatly reduces the computational
complexity of the system and reduces the amount of repeated calculation.

3. Threshold variable image secret sharing method
Since 1979, image secret sharing has developed into a variety of methods after in-depth study by many
researchers, but there are also many problems. When some participants or secret distributors provide
false secret keys when reconstructing the secret, the receiver will not get the image secret information. When the cheater is found or the secret key needs to be added, the secret threshold needs to be updated dynamically. This paper uses Newton interpolation method to adjust the threshold, first carries on the feasibility analysis to Newton interpolation method, then through the comparison experiment with Lagrange interpolation method, proves the superiority of Newton interpolation method in the transformation threshold.

3.1. Increase threshold process
When more participants are needed to share secret information, the threshold value needs to be increased to introduce new participants. Image secret sharing is to set up multiple discrete data \((1, s_1), (2, s_2), \ldots (k, s_k)\) in the finite field \(GF(p)\) through image \(S\) and assign them to different shares. When the threshold needs to be added, only new discrete data needs to be added; However, in secret recovery stage, different polynomial \(f(x)\) restored by different Numbers of discrete data will result in different secret information. At this time, it is necessary to flexibly add or modify the secret information that already exists in the Shared share, so as to achieve the final secret recoverable effect. Taking a single pixel value of a secret image as an example, the process of increasing the threshold using Newton interpolation is as follows:

Step 1: When new data are added, \(N[k + 1] = a_{k+1}x_{k+1}\) data items should be added for the original split polynomial, and the final polynomial is \(f(x) = a_0x + a_2x^2 + \ldots + a_kx^k + a_{k+1}x^{k+1}\).

Step 2: The k pixel value in the image \(S\) is taken out again and substituted into the newly added item \(N[k + 1]\). The data value obtained is correspondingly increased to the same pixel position of each share.

Step 3: Data is selected from the image \(|S|/k + 1\) as the \(k + 1\) bit data, substituted into polynomial \(f(x)\), and the value of the polynomial is stored as the pixel value in the \(k + 1\) share.

Step 4: When the pixel is split, there is a remainder of \(|S|/k + 1\), and 0 is supplemented for the data.

Step 5: Step 1, step 2 and step 3 shall be executed successively to complete the processing of each pixel value in the image \(S\). Image splitting process is completed.

Step 6: In the secret image recovery stage, \(k + 1\) point pair data can be substituted into polynomial \(f(x)\) to restore the secret image.

Step 7: Remove the supplementary data, and the secret restoration of the image is complete.

In the secret sharing process, Lagrange interpolation method is different from Newton interpolation method. Newton interpolation method only needs to calculate new nodes, while Lagrange interpolation method needs to re-establish polynomials to calculate all pixel values in the share.

3.2. Decrease threshold process
In the process of secret image sharing, when the data of the deceiver or a participant is found to be invalid, it is necessary to remove the invalid data and reduce the threshold value of the secret image. Taking the single pixel of the secret image as an example, the process of using Newton interpolation to reduce the threshold is as follows:

Step 1: When reducing the data, \(N[k] = a_kx_k\) data items need to be eliminated for the original polynomial, and the final polynomial is \(f(x) = a_0x + a_2x^2 + \ldots + a_kx^k\).

Step 2: The k-bit pixel value in the image \(S\) is taken out again and substituted into the elimination item \(N[k]\). The pixel value corresponding to the same pixel position of each share is subtracted by \(N[k]\) and stored as the pixel value again.

Step 3: Data is selected from the image \(|S|/k - 1\) as the k-1st bit data, substituted into the polynomial \(f(x)\), and the value of the polynomial is stored as the pixel value in the k-1st share.

Step 4: When pixel splitting is carried out, when there is a remainder of \(|S|/k - 1\), 0 is supplemented for the data.
Step 5: Step 1, step 2 and step 3 shall be executed successively to complete the processing of each pixel value in the image S. Image splitting process is completed.

Step 6: In the secret image recovery stage, k-1 point pair data can be substituted into polynomial \( f(x) \) to restore the secret image.

Step 7: Remove the supplementary data, and the secret restoration of the image is complete.

In the process of secret image sharing, Lagrange interpolation needs to establish a new polynomial due to the change of the number of data, so it needs to consume a lot of computational resources.

3.3. Feasibility verification
In the process of dynamic adjustment threshold using bovine interpolation, the secret image is still split by polynomial. Since the secret image is stored secretly as the polynomial coefficient, when the threshold is increased, only a new coefficient needs to be added to the polynomial. Similarly, when the threshold is reduced, the coefficient of the redundant polynomial can be deleted; When secret image restoration is carried out, the size of threshold is adjusted dynamically and the data of existing shares needs to be modified. During the calculation, it is necessary to increase or decrease the data items in the corresponding polynomial, which greatly reduces the calculation amount. Therefore, this method is feasible.

4. The experiment
With the same threshold, the computation of an image pixel is compared between Newton interpolation and Lagrange interpolation. In the computer, the calculation principle of addition and subtraction and multiplication and division is different, so the experiment part needs to be analyzed concretely. Obviously, both addition and subtraction and multiplication and division of the calculation of Newton interpolation is significantly less than Lagrange interpolation.

4.1. The increase in threshold
In order to ensure the security and integrity of the secret image, the secret sharing organizer needs to let more participants recover the important secret information under certain scenarios, and more participants can increase the complexity of secret recovery; When the computer environment is relatively complex and the network transmission is slow, in order to reduce the transmission amount of secrets and shorten the transmission time, it is also necessary to increase the threshold of image secret sharing.

4.1.1. Add and subtract
Because the structure of Newton interpolation method is more flexible, when the dynamic increase threshold, only a new item is needed to restore the image secret, without repeated calculation; However, the Lagrange interpolation method needs to re-establish the polynomial and calculate multiple shares, which will increase the calculation amount; In the process of increasing the threshold, the computation required by Newton interpolation is much less than that of Lagrange interpolation. The results are as follows.

![Figure 2. Schematic diagram of addition and subtraction calculation](image-url)
4.1.2. Multiplication and division
Due to the different principles of multiplication and division, addition and subtraction, and the different bits of data, the amount of computation consumed by the computer is different. When the threshold is increased, the computational complexity of multiplication and division required by Newton interpolation is much less than that of Lagrange interpolation. The results are as follows.

4.2. Threshold decreases
In the process of secret sharing, when it is found that there are cheaters among the participants or the secret sharing organizer, it is necessary to delete the cheaters in time, adjust the threshold size and save the calculation cost.

4.2.1. Add and subtract
In the process of reducing threshold, the calculation amount of Newton interpolation method is different due to the different location of removing threshold node. When the removed deceiver is in the last item, the maximum item of Newton interpolation can be directly removed. When its position is in the first few items, all the data items participating in the calculation after this item need to be modified. Lagrange interpolation method is different from Newton interpolation method. When the threshold is updated, the polynomial needs to be re-established for calculation. In the process of reducing the threshold, Newton interpolation requires much less computation than Lagrange interpolation. The experimental results are shown below:

4.2.2. Multiplication and division
The process principle is the same as above. Because when the computer carries out the computation, the execution multiplication and division method and the addition and subtraction method principle is different, the computation quantity is different. When the threshold is reduced, the computational complexity of multiplication and division required by the two algorithms is as follows:
4.3. Experiment
The experimental process includes secret image splitting and reconstruction. After the split can get two shares. After adding the new share, the image is secretly reconstructed. The reconstructed image is consistent with the original image and the secret sharing of the image is completed. The original image $S$ corresponds to the restored image $S'$ and multiple shares are shown below.

![Figure 6. Schematic diagram of feasibility verification](image)

Figure 6. Schematic diagram of feasibility verification

Figure a is the secret image, b and c are the two generated shared images, d is the newly added shared image, and e is the restored image. The secret share is $1/2$ the size of the original image, and the reconstructed image is the same size as the original image. According to the above experimental results, it is feasible to use Newton interpolation method for image secret sharing.

5. Conclusion
The threshold variable image secret sharing method proposed in this paper combines the image secret sharing method with Newton interpolation method and replaces the traditional Lagrange interpolation method. The structure of Newton interpolation polynomial is more flexible and convenient to adjust the threshold structure dynamically. When the threshold is adjusted, only the corresponding items need to be increased or decreased, which saves a lot of calculation process and greatly shortens the calculation time.

When the threshold is adjusted, only the corresponding part needs to be modified. From the above experiments, it can be seen that the method proposed in this paper can save several times of computation when the threshold is variable, and has strong practicability and low computational complexity, and it can save a lot of calculation process and greatly shortens the calculation time.

References
[1] Shamir, A. (1979) How to share a secret. Communications of the ACM. Commun., 22: 612-613.
[2] Naor, M., Shamir, A. (1996) Visual cryptography II: Improving the contrast via the cover base. In: Lomas M. (eds) Security Protocols. Security Protocols 1996. Lecture Notes in Computer
[3] Blakley, G. (1979) Safeguarding cryptographic keys. In: AFIPS 1979 National Computer. New York. pp. 313-317.

[4] Thien, C., Lin, J. (2002) Secret image sharing. Computers & Graphics. Commun., 26(5): 765-770.

[5] Pang Liao-jun, Wang Yu-min. A new (t,n) muti-secret sharing scheme based on Shamir’s secret sharing. Applied Mathematics and Computation, 2005, 167(2): 840-848.

[6] Lin T Y, Wu T C. (t,n) threshold verifiable multisecret sharing scheme based on factorization intractability and discrete logarithm modulo a composite problems. IEE Proc. Comput Digit Tech. 1999, 146(5): 264-268.

[7] Lain C S, Harn L and Lee J Y. On the design of single-key-lock mechanism based on Newton’s interpolating polynomial. IEEE Trans. on Software Engineering, 1989, 15(9): 1185-1187.

[8] Naor, M., Shamir, A. (1994) Visual cryptography. Lecture Notes in Computer Science. Commun., 950(9), 1-12.

[9] Carpentieri M, De Santis A, Vaccaro U. Size of shares and probability of cheating in threshold schemes. Advances in Cryptology—EUROCRYPT’93, Springer-Verlag, 1994: 118-125