Copyright © 2019 Tech Science Press CMC, vol.58, no.2, pp.349-361, 2019

A Weighted Threshold Secret Sharing Scheme for Remote Sensing Images Based on Chinese Remainder Theorem

Qi He[1], Shui Yu[2], Huifang Xu[3, *], Jia Liu[4], Dongmei Huang[5], Guohua Liu[6], Fangqin Xu[3] and Yanling Du[1]

Abstract: The recent advances in remote sensing and computer techniques give birth to the explosive growth of remote sensing images. The emergence of cloud storage has brought new opportunities for storage and management of massive remote sensing images with its large storage space, cost savings. However, the openness of cloud brings challenges for image data security. In this paper, we propose a weighted image sharing scheme to ensure the security of remote sensing in cloud environment, which takes the weights of participants (i.e., cloud service providers) into consideration. An extended Mignotte sequence is constructed according to the weights of participants, and we can generate image shadow shares based on the hash value which can be obtained from gray value of remote sensing images. Then we store the shadows in every cloud service provider, respectively. At last, we restore the remote sensing image based on the Chinese Remainder Theorem. Experimental results show the proposed scheme can effectively realize the secure storage of remote sensing images in the cloud. The experiment also shows that no matter weight values, each service providers only needs to save one share, which simplifies the management and usage, it also reduces the transmission of secret information, strengthens the security and practicality of this scheme.

Keywords: Remote sensing image, security, cloud, storage, weighted threshold.

1 Introduction

With the development of remote sensing (RS) techniques, more and more remotely sensed data are acquisition from different sensors of various platforms, and the amount of remote sensing images increases dramatically. Cloud storage is a service with large storage space, cost effective, which has brought new opportunities for massive remote sensing images. Due to the openness of cloud, the data stored in the cloud possess the risk

[1] Shanghai Ocean University, Shanghai, 201306, China.

[2] Deakin University, 221 Burwood HWY, Burwood, VIC 3125, Australia.

[3] Shanghai Jian Qiao University, Shanghai, 201306, China.

[4] Yanshan University, Hebei, 066004, China.

[5] Electric Power University, Shanghai, 200090, China.

[6] Donghua University, Shanghai, 200051, China.

[*] Corresponding Author: Huifang Xu. Email: 17069@gench.edu.cn.

CMC. doi:10.32604/cmc.2019.03703 www.techscience.com/cmc

of being malicious damaged or deleted by cloud providers. How to ensure the safety of remote sensing images stored in the cloud is a hot research topics.

Encryption is an effective mean of security. If we store encrypted data in clouds, it is easy to cause the ciphertext been tampered, and results in ciphertext not being restored. In order to avoid the situation that ciphertext cannot be restored, we need to create multiple backups for a secret. The secret sharing scheme based on Shamir can create backup for secret and prevent abuse of power, which is more suitable for data security in the cloud environment. Secret sharing scheme distribute a secret S to n participants such that a set of k or more participants can recover the secret S, and a set of k-1 or less shares cannot obtain any information about S which proposed by Thien and Lin in 2002. In the cloud environment, each service provider is a participant in a secret sharing scheme.

In the traditional secret sharing scheme, participants have the same status. While in the real life, different participants have different roles and importance, such as in the company, the position of general staff and managers are different. Therefore, it cannot satisfy the special needs of the real world when we teat participants equally. The weight threshold access structure allows different participants to have different weights, each participant is assigned a weight value, the bigger the weight value, the higher the participant position. The secret image can be reconstructed without distortion, if and only if the sum of the weights of the shadow images in the recovery process is equal or greater than the given weight threshold.

Most of the existing researches on weighted threshold secret sharing are mostly distributed to the participants with multiple secret shares, which caused low utilization of information, and large computation of data. Therefore, in this paper we proposed an improved weighted threshold secret sharing scheme based on the Chinese remainder theorem, introducing and extending Mignotte sequence to share the sensitive area image. By considering the differences of participants' rights, which strengthens the security and practicality of the scheme.

2 Related work

At present, techniques for ensuring remote sensing images security in the cloud includes data encryption storage, security audit and access control of ciphertext. Homomorphic encryption is an important method to protect data security and privacy in the cloud storage environment, and is also one of the most effective methods. However, the data processing efficiency of homomorphic encryption technology is too low, and it needs complex exponential operations, which cannot support the rapid processing of large amounts of data. Therefore, homomorphic encryption storage technology is not an efficient way for secure storage of high volume data security storage. The distributed threshold secret sharing scheme is an effective method to protect cloud data, which can create backups for secret data and prevent the abuse of power, so it is widely used in image encryption [Feng, Qin and Yuan (2015)].

The traditional shamir secret sharing scheme has poor sharing efficiency, poor flexibility and poor practical use due to the same permissions. Therefore, the secret sharing with weight threshold becomes a hot in data security storage and encryption. In 1999, Morillo et al. [Morillo, Padró and Sáez (1999)] proposed a weighted secret sharing scheme, which is based on a decomposed structure that can only be applied to the case where the number of elements of each minimum authorized subset is 2. Zhang et al. [Zhang and Zhang (2013)] proposed a weighted threshold secret sharing scheme which requires solving the congruent polynomial equations, the computational complexity is large. Then, the weighted threshold secret sharing scheme was first proposed based on the Mignotte sequence [Shao (2014)]. The scheme first constructs the weighted Mignotte sequence and completes the secret sharing and recovery process based on the Chinese remainder theorem. The scheme reduced secret share size of the privileged participants, but the system parameters are harsh and the system is too complicated. Iftene based on Asmuth and Bloom scheme achieve a more secure weighted threshold secret sharing scheme, which need to construct the weighted Asmuth-Bloom sequence [Harn and Miao (2014); Harn and Hsu (2015)].

Wang et al. [Wang, Zhou and Li (2015)] proposed a weighted secret sharing scheme based on the Chinese remainder theorem, it can effectively solve the problem of sharing pictures with different weights. Many verifiable secret sharing schemes are proposed to solve the deception attack in secret sharing. The verifiable secret sharing scheme [Harn and Miao (2014); Li, Ma and Guo (2015)] increased the secret sharing process and improved the security of secret sharing. In order to increase the security and practicability of the scheme, many dynamic weighted secret sharing schemes are proposed [Wu and Tseng (2011); Harn and Lin (2010)]. When the reconstruction fails, the cheating behavior of the participants can be found by verifying the identity of the participants [Hsu and Harn (2014)]. However, the scheme cannot prevent the cheater from obtaining the secret, and the attacking from semi honest participants. Meanwhile, the scheme can only share a secret at the same time, and the algorithm needs to be performed again when updating the secret.

The existing researches on the image encryption mainly solve the security problem in the centralized storage environment. In the open cloud storage environment, the security problem of remote sensing image is rarely involved. So, this paper proposes an encryption scheme for remote sensing images in a cloud environment combined with the large quantities, large scale and high sensitivity characteristics of remote sensing images, Fig. 1 shows the flow chart of the scheme proposed in this paper. In Fig. 1 we know that the scheme consists of four steps: the construction of weighted Mignotte sequences, the calculation of the hash value based on the gray value of the remote sensing image, the secret image sharing process and the secret image recovery process. While the secret image core process is divided into three stages: preparation, sharing and recovering. In this scheme, each participant only needs to keep a secret share, it can reduce the transmission of secret information, and improve the security of secret.

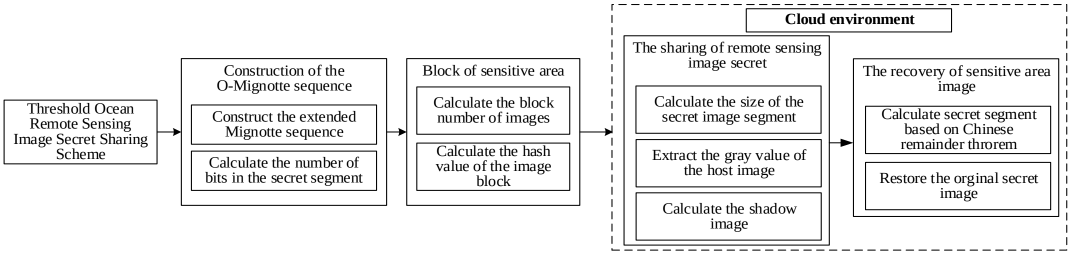
Threshold Ocean Remote Sensing Image Secret Sharing Scheme
Construction of the O-Mignotte sequence
Construct the extended Mignotte sequence
Calculate the number of bits in the secret segment
Block of sensitive area
Calculate the block number of images
Calculate the hash value of the image block
Cloud environment
The sharing of remote sensing image secret
Calculate the size of the secret image segment
Extract the gray value of the host image
Calculate the shadow image
The recovery of sensitive area image
Calculate secret segment based on Chinese remainder throrem
Restore the orginal secret image

Figure 1: Process of weighted threshold secret sharing scheme based on extended Mignotte

3 A weighted secret sharing scheme based on extended mignotte sequence

In this paper, we first block the remote sensing image and use the hash algorithm to calculate the average gray value of each image block based on the gray value of the remote sensing image, in the last we obtain the secret share by the quantization operation. The secret image can be reconstructed without distortion when the weight of the participants is equal to or greater than the weight threshold. In this paper, this section describes and defines the research problems, and gives the extended Mignotte sequence based on the weighted threshold of the sensitive area remote sensing image secret sharing.

3.1 Description and definition of the problem

This paper constructs a secret image sequence of the remote sensing image based on the Mignotte sequence, the secret image is decomposed into different secret sharing, and recorded as the shadow image. In the secret reconstruction stage, the secret share is recovered based on the Chinese remainder theorem. Then, the secret shares are filled into the corresponding position in the image according to the number and the secret image is obtained. Now we describe and define the related concepts of the remote sensing image secret sharing scheme based on extended Mignotte sequences.

DEFINITION 1: Weighted Threshold Remote sensing Image Secret Sharing Scheme. The weighted threshold secret sharing scheme is expressed as (ω, w, n) , ω is the weight held by the participant, *w* is threshold value. n is a participant set U , for any subset $U^{'}$ of U . It can restore the secret image when $\sum_{u\in U^{'}} \omega(u) \geqslant w$.

Definition 2: Remote sensing image data set. The remote sensing image dataset is a four tuple $I(id, r, L, b_n)$, *id* is the number of the image, *r* is the resolution of remote sensing image, *L* is latitude and longitude of the remote sensing image, b_n the number of bands for remote sensing images.

Definition 3: *O-Mignotte* sequence. *O-Mignotte* as a sequence of remote sensing images. Firstly, constructing a Integer prime Sequence $d_1^{'}, d_2^{'}, ..., d_n^{'}$ .According to the participant weight vector $\omega = (\omega_1, \omega_2, .., \omega_n)$,and extending $d_1^{'}, d_2^{'}, ..., d_n^{'}$ to $(d_1^{'})^{\omega_1}, (d_2^{'})^{\omega_2}, ..., (d_n^{'})^{\omega_n}$.

3.2 Weighted threshold remote sensing image secret sharing

In this paper, the Chinese remainder theorem can be used to reconstruct remote sensing image by its set of remainder numbers, this set of remainder numbers is obtained by taking a set of two mutually integers.

Theorem 1: As known *O-Mignotte* sequence is $(d_1')^{\omega_1},(d_2')^{\omega_2},...,(d_n')^{\omega_n}$ recorded as $d=(d_1')^{\omega_1},(d_2')^{\omega_2},...,(d_n')^{\omega_n}$,and remote sensing image secret segments are $S_1',S_2',...,S_n'$ .Then, the Congruence Equations are:

$$\begin{cases} x \equiv S_1' \bmod (d_1')^{\omega_1} \\ x \equiv S_2' \bmod (d_2')^{\omega_2} \\ ...... \\ x \equiv S_n' \bmod (d_n')^{\omega_n} \end{cases} \quad (1)$$

There is a unique solution in the sense of modular m congruence: $x \equiv D_1 D_1' S_1' + D_2 D_2' S_2' + ... + D_n D_n' S_n' \bmod d$.

Among them $D_i = d/(d_i')^{\omega_i}$; $D_i' D_i \equiv 1(\bmod (d_i')^{\omega_i})$, $1 \leqslant i \leqslant n$;

Proof. By definition 4, we know $(d_1')^{\omega_1},(d_2')^{\omega_2},...,(d_n')^{\omega_n}$ is a primitive sequence. When $i \neq j$, there is $((d_i')^{\omega_i},(d_j')^{\omega_j})=1$. As $D_i = d/(d_i')^{\omega_i}$, so $(D_i,(d_i')^{\omega_i})=1$,then $(D_1,(d_1')^{\omega_1})=(D_2,(d_2')^{\omega_2})=...=(D_n,(d_n')^{\omega_n})=1$. As $(D_i,(d_i')^{\omega_i})=1$, there is one D_i' which it satisfied $D_i' D_i \equiv 1(\bmod (d_i')^{\omega_i})$. In addition, when $i \neq j$,by $((d_i')^{\omega_i},(d_j')^{\omega_j})=1$ and $D_j = d/(d_j')^{\omega_j}$,we get $S_j' D_j' D_j \equiv 0(\bmod (d_i')^{\omega_i})$ .According to the above formula we have: $D_1 D_1' S_1' + ... + D_n D_n' S_n' \equiv D_i D_i' S_i' + \sum_{j \neq i} D_j D_j' S_j' \bmod (d_i')^{\omega_j} \equiv a_i + \sum_{j \neq i} 0 \equiv D_i D_i' S_i' \equiv S_i' \bmod (d_i')^{\omega_i}$.

It means x is a solution of the equations.

If y can also satisfy the equations, we get $x \equiv y(\bmod (d_1')^{\omega_1}), x \equiv y(\bmod (d_2')^{\omega_2}),...,$ $x \equiv y(\bmod (d_k')^{\omega_k})$, that is $(d_1')^{\omega_1} \mid (x-y),(d_2')^{\omega_2} \mid (x-y),...,(d_n')^{\omega_n} \mid (x-y)$. As $(d_1')^{\omega_1},(d_2')^{\omega_2},...,(d_n')^{\omega_n}$ is a primitive sequence, we have $d \mid (x-y)$,that is $x \equiv y(\bmod d)$ .So $x \equiv D_1 D_1' S_1' + D_2 D_2' S_2' + ... + D_n D_n' S_n'$ is the only positive integer solution of the equations, then the theorem is proved.

1) *O-Mignotte* threshold secret sharing scheme

O-Mignotte threshold secret sharing scheme, we construct *O-Mignotte* sequence on the basis of Mignotte sequence, and complete the secret sharing and recovery process based on Chinese remainder theorem. Assuming n is the number of participants, P is a collection of all the subsets of the participants, $\omega = (\omega_1, \omega_2,..,\omega_n)$ is the weight sequence of each participant, w is the weight threshold of access structure, and it satisfied $2 \le w \le \sum_{i=1}^{n} \omega_i$. We call the $(\omega, w, n) - Mignotte$ sequence a weighted sequence under this condition.

The traditional threshold secret sharing scheme based on *M*ignotte sequence does not implement the weighting of the participants. So the secret distributor builds an extended *O-Mignotte* sequence according to the weight assignment. So that the extended *O-Mignotte* sequence has equivalent effects to the traditional Mignotte sequence. The construction of *O-Mignotte* sequence is a key part of the weighted threshold secret sharing scheme. Specific steps are as follows:

Step1: Let w is the weight threshold of the access structure, which it satisfied $2 \leqslant w \leqslant \sum_{i=1}^{n} \omega_i$;

Step2: Constructing a prime sequence $d_1^{'}, d_2^{'}, ..., d_n^{'}$;

Step3: According to the weight of participant $\omega = (\omega_1, \omega_2, .., \omega_n)$, extending $d_1^{'}, d_2^{'}, ..., d_n^{'}$ to $(d_1^{'})^{\omega_1}, (d_2^{'})^{\omega_2}, ..., (d_n^{'})^{\omega_n}$;

Step4: Public *O-Mignotte* sequence;

Step5: When the sequence is constructed, then calculating α, β , which it satisfied $\beta < S_i < \alpha$, among them $\alpha = \prod_{i=0}^{t-1} d_i^{'}$, $\beta = \prod_{i=0}^{t-2} d_{n-i}^{'}$. By letting $b = \log_2(\alpha - \beta)$, we regard the remote sensing image as a series of b-bit segments.

2) Remote-sensing image secret sharing

The secret sharing of remote sensing image uses the constructed weighted sequence to decompose the secret image into many secret shares with different weights, each secret share is recorded as shadow images, and is distributed to different participants. While the secret image sharing process is divided into three stages: preparation, sharing and recovering. In the preparation phase the remote sensing image is divided into blocks, and we calculated the hash value of each image. We use the gray value of the remote sensing image as the image feature to generate the hash value. Fig. 2 shows a diagram of the secret image sharing process, according to Fig. 2 we know that this process is also divided into three phases. Firstly, we block the remote sensing images, and calculate the gray value for each image block to obtain a gray mean value sequence as the middle hash of images. Then, we calculate the average of the gray mean value sequence, note as $\overline{M}$. Finally, we compare the middle hash with $\overline{M}$ one by one, greater than $\overline{M}$, which we code as 1, less than $\overline{M}$, which we code as 0. Based on the above, we obtain the value of the image by connecting the coding value, see algorithm 1.

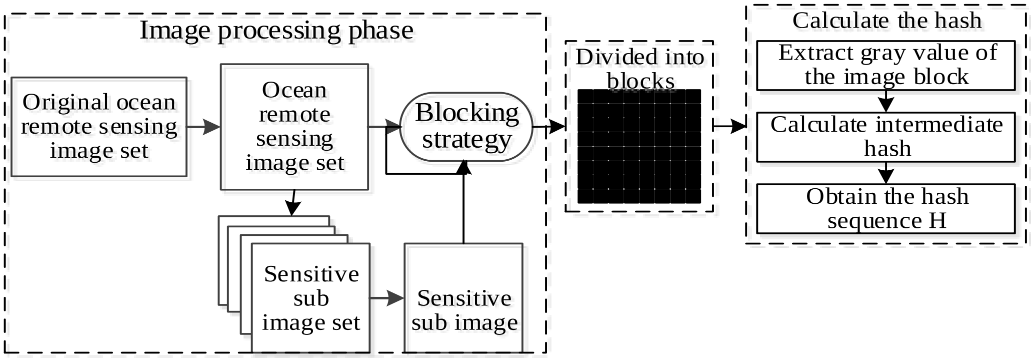
Image processing phase
Original ocean remote sensing image set
Ocean remote sensing image set
Blocking strategy
Sensitive sub image set
Sensitive sub image
Divided into blocks
Calculate the hash
Extract gray value of the image block
Calculate intermediate hash
Obtain the hash sequence H

Figure 2: Process of remote sensing image hash based on gray value

The specific algorithm 1 is as follows:

Input: Remote sensing image $I(id,r,L,b_n)$

Output: The hash sequence of remote sensing image $H(T^{'})$

Step1: Block remote sensing image N into $N_1,N_2,...,N_i$, i is equal to the length of the hash sequence;

Step2: Extarct the gray value matrix of $N_1,N_2,...,N_i$, calculate the mean value of each matrix, noted as $M_1,M_2,...,M_i$; Merge $M_1,M_2,...,M_i$, we will get a sequence with i length, and take the sequence as Middle hash. Then, we calculate the average of the gray mean value sequence $\overline{M}$, note as M_d .Among them $M_d = median(M_i), \quad j=1,2,...,i;$

Step3: Compare the middle hash with $\overline{M}$ one by one, and take the comparing result as a binary sequence. Then, we can obtain the hash H .

For remote sensing image $I(id,r,L,b_n)$, its size is $l\times l$. Firstly, converting multiband images into single-band images T_0, and then dividing the T_0 into $m\times m$ block images. It approximately need to be divided into $\lceil l/m \rceil^2$ blocks, the corresponding gray value is recorded as N(M). Calculating the mean of each matrix $\{M_1,M_2,...,M_i\}$,and taking it as middle hash. And then we calculate the mean M_d of middle hash value, and compare M_d with the middle hash one by one. Finally, we get the hash sequence $H(A^{'})$.

The sharing is the key stage for generating shadow image. Firstly, calculating the size of the remote sensing image according to the number of secret segments, and distributing them to different participants, see algorithm 2. Fig. 3 shows the basic flow of the secret image sharing process.

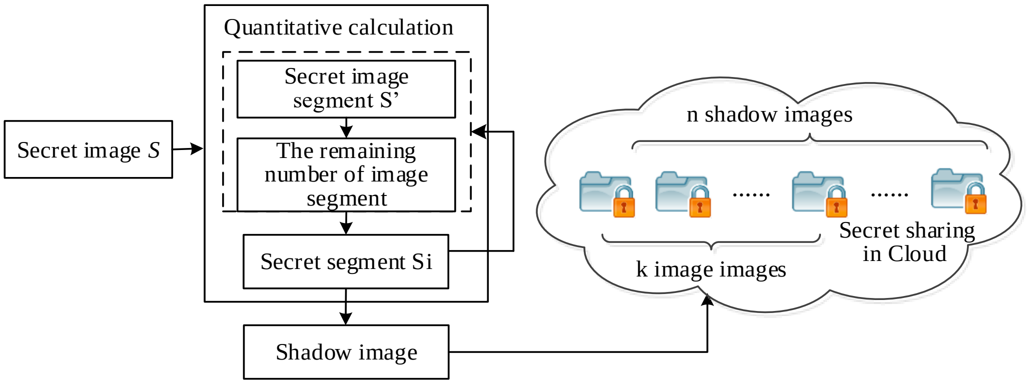

Figure 3: The procedure of secret image sharing

The specific algorithm 2 is as follows:

Input: Remote sensing image

Output: r shadow images

Step 1: Calculating the number of secret images:

$$n = c = \left\lfloor \frac{m \times m}{b} \right\rfloor \tag{2}$$

Step 2: Using the formula to adjust the secret image segment:

$$S = \{S_{\ i} = Binary(H_i) \mid i = 1, 2, ..., \frac{count(H)}{b}\} \tag{3}$$

$$S_i^{'} = S_i + 2^b \times \left\lfloor (\alpha - 1 - S_i) / 2^b \right\rfloor \tag{4}$$

Step 3: Using the formula $x_k = S_i^{'} \bmod d_k$ to calculate the remaining number of secret image segments. Among it $1 \le k \le n$;

Step 4: Recording x_k as the shadow image of each secret segment;

Step 5: Repeat Step 3, until all the secret segments S_i are process.

3) Remote sensing image secret restoration

After the sharing of the remote sensing image is completed, any participant whose weight is equal to or greater than the weight threshold can use their shadow images to generate the secret segments based on Chinese Remainder Theorem, and the original secret image can be recovered without distortion according to the secret segment d_i. Fig. 4 shows the recovery process of the secret image. See algorithm 3.

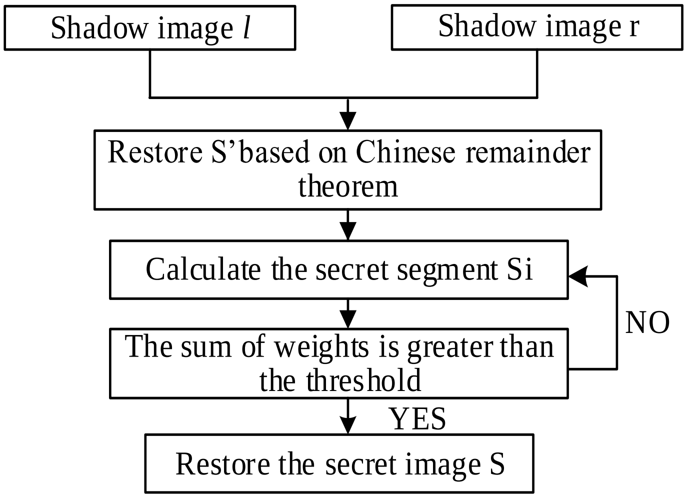
Shadow image *l*
Shadow image r
Restore S'based on Chinese remainder theorem
Calculate the secret segment Si
The sum of weights is greater than the threshold
NO
YES
Restore the secret image S

Figure 4: The procedure of secret image recovery

The specific algorithm 3 is as follows:

Input: r shadow images

Output: Original secret image

Step1: The weight vector of each participant is $\omega = (\omega_1, \omega_2, .., \omega_k)$

Step2: Use A=(u1, u2,…,uk) to restore the image of the secret segment S_i;

Step3: Restructure $S_i^{'}$ based on the Chinese remainder theorem. The formula is as follows:

$$\begin{cases} S_i^{'} \equiv x_1 \bmod d_1 \\ \cdots \\ S_i^{'} \equiv x_r \bmod d_r \end{cases} \tag{5}$$

Step 4: Calculating the secret segments $S_i = S_i^{'} \bmod 2^b$;

Step 5: Repeating the above steps until all S_i are extracted;

Step 6: When the sum of the weights of the participants is equal to or greater than the threshold. Taking S_i as the *i*th b-bit segment, and then placing S_i into the corresponding position, and recovering the original secret image;

Step 7: When $\sum_{i=1}^{t} w_i \leqslant t$, we need to select new participants to restore the secret image.

4 Experimental results and analysis

The experiment uses Matlab2010 to obtain the remote sensing image of Hangzhou area TM image acquired in April 16, 2015.The format of image is TIFF, the size is 1024×1024, the resolution is 30m.From the third section, we split the selected images to obtain sensitive area remote sensing images, as shown in Fig. 5, and extracting the single band gray image, as shown in Fig. 6.

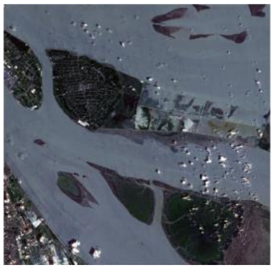

Figure 5: Remote sensing image

Figure 6: Single band image

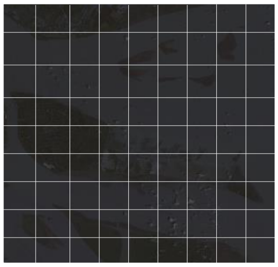

Figure 7: Block image

4.1 Experimental results

In (k,n) weighted threshold secret sharing scheme based on *O-Mignotte* sequence, we use (4, 5) threshold secret sharing scheme to experiment, that is t=4, n=5. For the convenience of calculation, we construct an appropriate sequence: 17, 19, 23, 29, 31, assume that the weight of each participant is $\omega_1 = 1,\ \omega_2 = 2,\ \omega_3 = 1,\ \omega_4 = 2,\ \omega_5 = 3$. According to the weight of the participant, extending *O-Mignotte* to 17, 19, 19, 23, 29, 29, 31, 31, 31, that is 17, 192, 23, 292, 313, record as ((1, 2, 1, 2, 3), 4, 5)-Mignotte According to the previous condition, we can figure out α and β .

$$\alpha = \prod_{i=1}^{t} d_i = 17 \times 19 \times 19 \times 23 = 141151$$

$$\beta = \prod_{i=0}^{t-2} d_{n-i} = 31 \times 31 \times 31 = 29791$$

In the secret image sharing stage, the secret image is regarded as a series of b-bit and we calculate $b = \lfloor \log_2(\alpha - \beta) \rfloor = 16$, that is, every 16 bits in the original secret image is treated as a secret segment. In order to obtain image share as a series of b-bit, in this paper, the image is divided into blocks using a formula $n = \left\lfloor \frac{m \times m}{b} \right\rfloor = 5$ by adopting a hash algorithm based on gray value of remote sensing image, we can get $m \times m = 9 \times 9$. The result of the block is shown in Fig. 7. After that, we calculate the image block hash value based on remote sensing image gray value method, see Tab. 1. According to algorithm 2, the values of the five secret segments are calculated as follows S1=30430, S2=23124, S3=42682, S4=26325, S5=14439, the specific construction process is shown in Fig. 8. According to algorithm 2, we can calculate $S_1^{'} = 95966$, $S_2^{'} = 88660$, $S_3^{'} = 108218$, $S_4^{'} = 91861$, $S_5^{'} = 79975$ and then calculate the remaining number of five secret segments, respectively x1=1, x2=301, x3=10, x4=92, x5=6593. Then we distributed shadow image of the first segment to each participant. Each person can only save a sub image share, regardless of the size of the participants.

Table 1: Hash sequence of remote sensing image

0	1	1	1	0	1	1	0	1
1	0	1	1	1	1	0	0	1
0	1	1	0	1	0	0	1	0
1	1	0	0	0	1	0	1	0
0	1	1	0	1	0	1	1	1
0	1	0	0	1	1	0	0	1
1	0	1	1	0	1	0	1	0
1	0	0	1	1	1	0	0	0
1	0	0	1	1	1	0	0	0
0	1	1	0	0	1	1	1	0

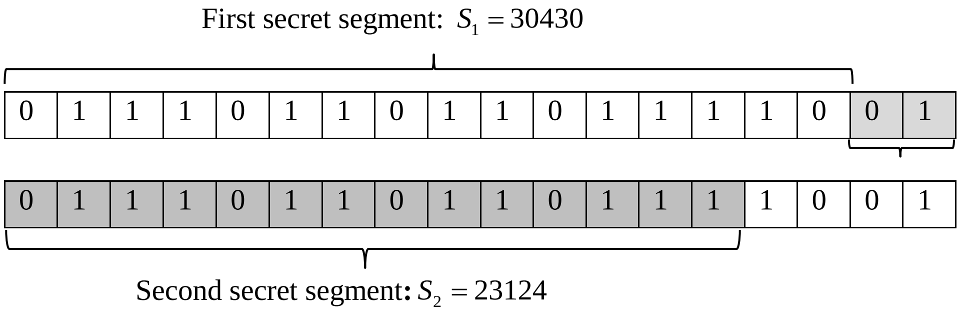
First secret segment: $S_1 = 30430$
0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 0 0 1
0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 0 0 1
Second secret segment: $S_2 = 23124$

Figure 8: The construction of 16-bit secret segments

4.2 Discussion

In order to verify the validity of the remote sensing image based on the extended Mignotte sequence. In this paper we verify the validity from security and correctness two aspects.

1) Security analysis

In order to verify the security of the scheme, we select participant 1 (weight is 1) and participant 4 (weight is 2) to restore the secret image. We know that x4=92. According to the Chinese remainder theorem:

$$\begin{cases} S_1^{'} \equiv 1 \bmod 17 \\ S_1^{'} \equiv 92 \bmod 29^2 \end{cases}$$

We can figure out $S_1^{'} = 10184$ and S1=10184. The results show that the first secret segment value is unequal to the original image. So we cannot restore the original secret image when the shadow images do not meet the weight threshold. It verified the security of this scheme.

2) Correctness analysis

After generating the shadow image, we began to recover the secret image. In the process of image recovery, when the weight of the participants is equal to or greater than the weight threshold, we can recover the original secret image without distortion by using their shadow image and d_i . It is known that the weight of each participant is $\omega_1 = 1$，$\omega_2 = 2$，$\omega_3 = 1$，$\omega_4 = 2$，$\omega_5 = 3$. In this paper, we firstly select participant 1, participant 3 and participant 5 to restore the secret image, $\omega^{'} = \omega_1 + \omega_3 + \omega_5 = 5$,which satisfied $\omega^{'} \geq \omega$ .The shadow images of Participant 1 Participant 3 and Participant 5 are respectively x1=1, x3=10, x5=6593. According to the Chinese remainder theorem:

$$\begin{cases} S_1^{'} \equiv 1 \bmod 17 \\ S_1^{'} \equiv 10 \bmod 23 \\ S_1^{'} \equiv 6593 \bmod 31^3 \end{cases}$$

We can get $S_1^{'} = 95966$, $S_1 = 30430$,it is found that $S_1 = 30430$ is equal to the original secret image. Therefore, we can recovery the first segment of the secret image. Similarly, we can calculate the other four secret segments, and restore the original secret image by filling the secret segment into the corresponding position. Therefore, we verified the correctness of the proposed scheme.

5 Summary and future work

In this paper, we propose an extended weighted threshold remote sensing image sharing scheme based on the Chinese remainder theorem. Combining with the large volume and large scale characteristics, we construct an extended remote sensing image sequence according to the weight of cloud service providers based on the Mignotte sequence. The secret image is divided into several secret shares, we record the secret shares as the shadow image.

Experimental results show the scheme we provide can effectively realize the secure storage of remote sensing images in the cloud. In addition, we take the weights of cloud service providers into consideration, the experiment shows that no matter what the weight value size, each service providers only needs to save one share, which simplifies the management and usage, it strengthens the security and practicality of this scheme.

Acknowledgement: This research was partly supported by (National Natural Science Foundation of China under 41671431, 61572421, and Shanghai Science and Technology Commission Project 15590501900.

References

Feng, C. S.; Qin, Z. G.; Yuan, D. (2015): Techniques of secure storage for cloud data. *Chinese Journal of Computers*, vol. 38, no. 1, pp. 150-163.

Harn, L. (2014): Secure secret reconstruction and multi-secret sharing schemes with unconditional security. *Security & Communication Networks*, vol. 7, no. 3, pp. 567-573.

Harn, L.; Hsu, C. F. (2015): Dynamic threshold secret reconstruction and its application to the threshold cryptography. *Information Processing Letters*, vol. 115, no. 11, pp. 851-857.

Harn, L.; Miao, F. (2014): Weighted secret sharing based on the chinese remainder theorem. *International Journal of Network Security*, vol. 16, no. 6, pp. 420-426.

Harn, L.; Lin, C. S. (2010): (n, t, n) verifiable secret sharing scheme. *Information Sciences*, vol. 180, no. 16, pp. 3059-3064.

Huang, D. P.; Wang, H. Y. (2012): Dynamic threshold secret sharing scheme. *Journal of Tsinghua University*, vol. 46, no. 1, pp. 102-105.

Hsu, C. F.; Harn, L. (2014): Multipartite Secret Sharing Based on CRT. *Wireless Personal Communications*, vol. 78, no. 1, pp. 271-282.

Li, M.; Ma, S.; Guo, C. (2015): A novel weighted threshold secret image sharing scheme. *Security & Communication Networks*, vol. 8, no. 17, pp. 3083-3093.

Morillo, P.; Padró, C; Sáez, G. E. (1999): Weighted threshold secret sharing schemes. *Information Processing Letters*, vol. 70, no. 5, pp. 211-216.

Shang, X. J.; Zhang, D. U. (2013): Publicly verifiable and renewable multi-secret sharing scheme. *Application Research of Computers*, vol. 30, no. 12, pp. 3794-3793.

Shao, J. (2014): Efficient verifiable multi-secret sharing scheme based on hash function. *Information Sciences*, vol. 278, no. 10, pp. 104-109.

Wang, M. (2005): Secret sharing among weighted participants. *Journal of Beijing Electronic Science & Technology Institute*, vol. 20, no. 4, pp. 481-485.

Wang, F.; Zhou, Y.; Li, D. (2015): Dynamic threshold changeable multi-policy secret sharing scheme. *Security & Communication Networks*, vol. 8, no. 18, pp. 3653-3658.

Wu, T. Y.; Tseng, Y. M. (2011): A pairing-based publicly verifiable secret sharing scheme. *Journal of Systems Science and Complexity*, vol. 24, no. 1, pp. 186-194.

Zhang, Y. S.; Zhang, Z. J. (2013): Dynamic and verifiable secret sharing among weighted participants. *Journal of Systems Science & Complexity*, vol. 20, no. 4, pp. 481-485.