

A Safe Sharing Authentication Scheme for Marine Images on Cloud

Yong-jun Li¹, Liang Zhou², Zhuo-ka Li²

¹Personnel department, Shanghai Ocean University, Shanghai 201306, China

²Network & Information Center, Shanghai Municipal Educational Examinations Authority, Shanghai 200433, China

Abstract. Nowadays, Cloud computing has become a very hot technology. with the emergence of cloud storage model, more and more users choose cloud to store the image data, while it brings challenges for image data security and usability due to the openness of cloud. An image authentication scheme is proposed to protect the ocean remote sensing image confidentiality on cloud, combining the Hash function and the threshold scheme, detecting the changes of the image data in sensitive regions and verifying the consistency for Encryption and Recovery images, The sensitive-region image can't be restored when the case that more than $n-k$ out of n sub-secrets get lost or tampered happened. To avoid this, this paper divided the sensitive region image into blocks, and implemented secret sharing for each sub block, guarantee the lossless recovery of partial image and enhance the availability of image data. Through experiment contrast analysis, the algorithm can effectively prevent fraud during the process of secret image recovery, and it is more safe than the traditional methods.

1. Introduction

Cloud storage environment requires higher standard for data security. With the development of remote sensing technology, the data of marine remote sensing image is increased by TB per day[1]. The emergence of cloud storage, more and more users choose to immigrate remote sensing image data and its application to the cloud. In the military, marine remote sensing image data is useful, has an important strategic significance for the war, the enemy intelligence surveillance and target locking . Marine remote sensing images with large scale, sensitive, and other characteristics, the practical application of marine remote sensing image in the port, bay and islands of information is the core of image data, image data and sensitive area change. Therefore, the safety and accuracy of the remote sensing image in the sensitive area is of guiding significance to the marine environment monitoring, marine resources management, marine disaster early warning and rescue. However, the openness of the cloud storage environment makes remote sensing image data managers lose controlling over the security of the data. Therefore, how to ensure the confidentiality of sensitive area in the cloud storage environment is the key issue.

In cloud storage environment, data is usually stored in plaintext, lack of data privacy protection, therefore, the encryption of data is the key to protect the confidentiality of data. For the effective protection of the security sensitive area of marine remote sensing image, secret sharing method Hash verify the threshold based on the secret sharing scheme, first by Shamir and Blakley independently proposed threshold secret sharing scheme is the shared secret information generating sub secret, if and only if or more participants can recover the joint secret. With the explosive growth of the marine



remote sensing data, the core area of the image encryption is becoming more and more important, and in the process of image restoration in the presence of false secret will result in poor image quality after data recovery, which greatly reduces the accuracy of the image data after recovery. Therefore, this paper uses hash function to detect whether the digital image tampering, a hash function is very sensitive to the data of each bit changes, small changes will make the generated hash values are changed, which can effectively prevent the recovery process, because the participants provide false secret and lead to the occurrence of recovery the secret of distortion, to ensure that the sensitive area of ocean remote sensing images before and after the restoration of data consistency and accuracy.

2. Related works

At present, the cloud environment often uses homomorphic encryption technology for data encryption, which uses vector and matrix of various calculation for encryption and decryption, so it is with low efficiency and high cost. KAmara and his fellows at the Microsoft research institute put forward a encryption storage framework[2] for the public cloud, which is less secure. Feng C.S[3] presents a decentralized cloud storage security framework that does not guarantee data integrity.

For image encryption, many studies has carried out at home and abroad, the early by statistical properties characterization of image hash of image is encrypted, though the method of LAN has stronger robustness, but for tiny disturbance is not sensitive to illegal, so it is lack of security[4]. Lou D.C[5] presents a method based on image block luminance histogram to extract the hash, the method adopts the brightness of each image block histogram feature, a malicious attacker can be generated with the same brightness histogram but image semantic content completely different image block image hash forged, so the method to extract the hash value of the security of the poor also[6]. NiuXia priests and others with gray levels image block as image characteristics to generate the hash, first of all, the image block, get the middle hash, and through the compression technology eventually to the hash of the image sequence. Colour histogram is used to characterize the image features, by capturing the image color histogram, the image region partition, and with the color to represent the image segments of each region. The two images were measured by measuring the overlap between the two images. Because in the process of getting color histogram, need to comprehend the image of the most representative of color, there is strong subjectivity, so the robustness is not strong. Swaminathan and his fellows have proposed an image Hashing algorithm based on the Fourier transform. Fourier transform, the algorithm first will be the image and under polar coordinates will be multiplied by the Fourier coefficient of every Angle amplitude random weight coefficient, produced by key to linear accumulative sum, fixed-length Hash sequence is obtained by quantitative compressed again. However, the attacker can fake the image by manipulating the phase information of the Fourier coefficient and keeping the image Hash value unchanged. Monga and his fellows introduced non-negative matrix factorization (NMF) into image Hashing, with non-negative constraints, NMF is different from such as singular value decomposition (SVD) traditional matrix dimension reduction techniques, such as in the literature, NMF is first used to decompose the randomly selected from the input image sub-block, NMF is on the second image decomposition and projection onto the random vector approximation matrix, obtained by series approximation matrix elements in the final Hash value, experiments show that this method has good robustness, but higher computational complexity[7].

In 1994, Naor and Shamir put forward a new image encryption technology - image secret sharing, the basic idea of this method is to put the secret image segmentation into sub image, any image and above the shadow image, can restore the original image. The flaw in the scheme is that the size of the shadow image is larger than the original secret image, and the image is distorted. The existing study of image encryption methods mainly solved the security problem of centralized storage environment, under the open cloud storage environment, according to the safety of the Marine remote sensing image problem, the above image encryption method for certain deficiencies. Considering marine remote sensing images with large quantities, large scale and high sensitive features, we put forward a cloud environment marine remote sensing image authentication scheme based on secret sharing, effectively protect the sensitive areas of marine remote sensing image data in cloud environment .

3. Marine remote sensing image authentication scheme Based on secret sharing

Marine remote sensing image is a kind of big data, and it is very important to protect the sensitive area of remote sensing image in the cloud storage environment. In this paper, the image of the sensitive region of the remote sensing image is segmented by the method of minimum external matrix. At the same time, the image is divided into blocks, and each sub image block is processed by secret sharing scheme, which effectively avoids the problem that the secret is lost or tampered with.

3.1. Issue description

In order to ensure the security of remote sensing data in cloud environment, this paper proposes an image authentication scheme to improve the accuracy of remote sensing image data in the cloud environment. For the original remote sensing image set of the ocean, the image of the remote sensing image is restored by using the high security cloud environment, which is shown in figure1:



Figure 1. Storage and acquisition of Ocean remote sensing image on cloud

The method of hash function and threshold secret sharing is used to verify the consistency of the image before and after restoration. The related concepts of the cloud environment under the marine remote sensing image secret sharing scheme in the description and definition, data including the sensitive area of ocean remote sensing image sensitive sub image data sensitive area image data of marine remote sensing data set, marine remote sensing image sets, marine remote sensing image collection and recovery set.

In the authentication scheme, through the combination of hash function and threshold secret sharing method, the consistency of the image before and after restoration is verified to ensure the accuracy of the recovered secret image data. The gray value of the image is used as the image feature to calculate the hash value of the image in the sensitive area of the ocean remote sensing image. For sensitive area images (k, n) threshold secret sharing, using the method of projection matrix based on L.Bai image secret sharing, the value as a shared secret gray matrix, through the matrix transformation secret matrix generates a plurality of low dimension matrix, as a sub secret. The specific implementation scheme of the secret sharing scheme of the image of the sensitive area of the remote sensing image in the cloud environment is shown in Figure 2.

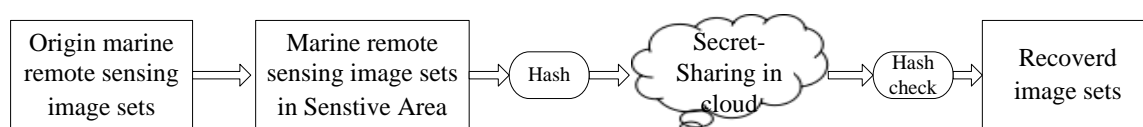


Figure 2. Ocean remote sensing image authentication scheme on cloud

In Figure 2, the encryption of the original ocean remote sensing image can be used to encrypt the remote sensing image data of the sensitive area after segmentation. The sensitive area of the marine remote sensing image secret sharing, first calculate the hash sequence image encryption, and the use of secret generating projection matrix method based on L.Bai, and the generated sub secret stored in the cloud environment. In the recovery phase image, gray image restoration is calculated again value hash sequence matrix, compared with hash sequence image encryption before if consistent, that image can be recovered, on the other hand, indicates that the restored image distortion. In order to restore the image, we need to choose the sub secret to restore the image.

Sensitive area image for ocean remote sensing image secret sharing, first on sensitive areas of images are divided into blocks, and every block is the sensitive area of sub images to calculate the hash sequence, then use the generated sub secret projection matrix method based on L.Bai, and the generated sub secret stored in the cloud environment. In the recovery phase of the sub image, the hash sequence of the gray value matrix of the restored image is calculated again.

3.2. Secret sharing algorithm for ocean remote sensing image

The projection matrix of secret sharing scheme based on L.Bai is not validated on image quality after recovery, leading to the recovery of the image after the data accuracy is not high, this paper use hash function to verify the restored image based on, in order to ensure the accuracy of data recovery after image information. Image sub block after the sensitive area of cloud under the environment of the secret sharing of marine remote sensing image includes image sensitive area on marine remote sensing image secret sharing and the marine remote sensing image secret sharing, image sensitive area on marine remote sensing image secret sharing algorithm in 1, and the secret sharing scheme in sensitive area of image blocks after the marine remote sensing image the image of the implementation of algorithm . The Algorithm is as follows:

Input: ocean remote sensing images in sensitive area $T(id, S, q, A, H)$.

Output: a sensitive remote sensing image data set after restoration $C_{Z_1}^{Z_0}$.

Step 1: Extract Grey scale matrix A of sensitive area images from ocean remote sensing images T ;

Step 2: A hash sequence of sensitive region images of ocean remote sensing images is calculated, named $H(A)$;

Step 3: The sensitive areas are divided into molecular images;

Step 4: For Z^0 L.Bai threshold secret sharing, obtained n secret;

Step 5: Recover images base on sub secret;

Step 6: Merge sub images.

4. Experiment and analysis

In order to verify the validity of the proposed scheme for remote sensing image authentication based on secret sharing in cloud environment, this paper verifies the method in 2 aspects: correctness and security.

4.1. Accuracy analysis

Experiments were conducted using Matlab 2010 to capture the sensitive region images of the Shanghai images obtained in July 2016. The image format is TIFF format, the size is 1024 * 1024, the image resolution of 30m. and using hash sequence sensitive area image of the original remote sensing image of the secret sharing scheme to restore the hash sequence matrix are compared, whether the secret image verification recovered correctly. In the process of image restoration in secret, the first choice to restore the image, after the restoration, by comparing the original image and the restore image found the secret image after the restoration of the damaged, which indicates that there exists at least one false sub secret. the restored image is not consistent with the original image, indicating that there is also false secret. Therefore, the existence of false secret leads to the poor quality of image restoration and greatly reduces the accuracy of image data recovery. In order to obtain the secret image lossless, we re-select the sub secret image, gray generation recovery value matrix, the hash sequence calculated by

gray image before and after the restoration of the value of the hash sequence consistent matrix, verify the correctness of the proposed method.

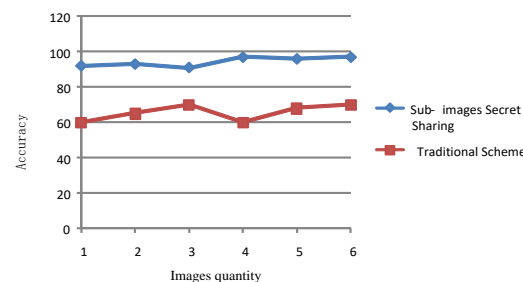


Figure 3. Comparison of data accuracy

4.2. Security analysis

The experiment carried out 10 secret sharing of each scene image, and the vertical coordinate in Figure 3 was the ratio of the restoration of image accuracy, and the abscissa was the label of image. The experimental results show that the image data sharing the highest safety sensitive areas for marine remote sensing image block after sub images using this method, and the sensitive area of the traditional image secret sharing method to restore the image of the lowest safety data. Therefore, in the cloud environment, the secret sharing of the sub images of the sensitive images of the remote sensing images in the cloud environment has obvious advantages in ensuring the security of the data.

5. Conclusion

In the cloud storage environment, based on Shamir secret sharing system, combined with the sensitive property of the hash function of data changes, a threshold secret sharing authentication method is studied, which can prevent the fraud, through the sensitive area of Marine remote sensing image data is encrypted, greatly reduce the time needed for image encryption. Through analysis of experimental results, this method has high security, effectively detected the deceiver, avoid the restoration of image distortion, to protect the image data confidentiality. In addition, in order to avoid the threshold secret sharing scheme, due to some secret lost cause the whole image unrecoverable, we divide sensitive areas of the image into small pieces, then process each image block to ensure that each part of the image lossless recovered. Finally, we found the data security of the sub-images method is the most secure.

6. Reference

- [1] Takabi H, Joshi J B D and Ahn G J 2010 Security and privacy challenges in cloud computing environments *J. IEEE Security & Privacy*. **6** 24-31
- [2] Xue M, Xue W and Shu J 2015 A Secure Storage System Over Cloud Storage Environment *J. Chinese Journal of Computers*. **8** 31-32
- [3] Feng C S, Qin Z G and Yuan D 2015 Techniques of Secure Storage for Cloud Data *J. Chinese Journal of Computers*. **15** 109-112
- [4] Pang LJ, Pei QQ, Jiao LC and Wang YM 2008 An identity(ID)-based threshold multi-secret sharing scheme *J. Journal of Software*. **10** 2739-2745
- [5] Lou D C and Liu J L 2000 Fault resilient and compression tolerant digital signature for image authentication *J. Consumer Electronics*. **46** 31-39
- [6] Wang GL and Qing S 2005 Security Notes on Two Cheat-Proof Secret Sharing Schemes *J. Journal of Computer Research and Development*. **11** 1924-1927
- [7] Monga V and Mihçak M K 2007 Robust and Secure Image Hashing via Non-Negative Matrix Factorizations *J. Information Forensics & Security IEEE Transactions on*. **3** 376-390.