SCIENCE CHINA
Information Sciences

• LETTER •

February 2021, Vol. 64 129102:1–129102:3
https://doi.org/10.1007/s11432-018-9572-x

Secure fusion of encrypted remote sensing images based on Brovey

Junzhi YANG[1], Guohua CHENG[2] & Meng SHEN[2,3*]

[1]*School of Information and Electronics, Beijing Institute of Technology, Beijing* 100081*, China;*
[2]*School of Computer Science, Beijing Institute of Technology, Beijing* 100081*, China;*
[3]*Key Lab of Information Network Security of Ministry of Public Security* (*The Third Research Institute of Ministry of Public Security*)*, Shanghai* 201204*, China*

Received 14 June 2018/Accepted 21 August 2018/Published online 16 July 2020

Citation Yang J Z, Cheng G H, Shen M. Secure fusion of encrypted remote sensing images based on Brovey. Sci China Inf Sci, 2021, 64(2): 129102, https://doi.org/10.1007/s11432-018-9572-x

Dear editor,

In the field of image fusion, panchromatic images captured by the Satellite Pour l'Observation de la Terre (SPOT) [1] have high spatial resolutions, whereas their spectral resolutions are relatively low. On the other hand, multispectral images have high spectral resolutions; however, their spatial resolutions are low. Because the two types of images captured by satellites cannot meet the demand [2], image fusion is generally necessary in practice. Remote sensing images require large storage spaces, and image-fusion operations may contain complex computations, making it difficult to execute on ordinary computers. Cloud storage [3] has the advantage of large storage space and computing resources, making it quite suitable. However, remote sensing images usually contain confidential information, requiring encryption prior to cloud delivery [4]. Based on existing research, and by combining the technical features of image fusion and image encryption, we propose an encrypted remote-sensing image fusion scheme based on Brovey [1], which can realize remote image sensing fusion in the cloud while protecting image privacy.

System model. There are three participants to our scheme: an image owner, the cloud, and an authorized user. The image owner possesses the original remote-sensing images and encrypts them with an encryption key prior to outsourcing to the cloud. Then, the owner sends a secret image decryption key to the authorized users/receivers over a secure channel. The cloud allows fusion of the encrypted panchromatic image and the encrypted multispectral image, providing the encrypted and fused remote sensing image for transmission to the authorized receiver. In our scheme, we assume that the cloud is "honest and curious", implying that it will execute the encrypted image fusion operation correctly and will also analyze the image content to obtain some original information. The authorized user is authorized by the image owner and has need-to-know. This authorized user stores the image decryption key sent by the owner and uses it to decrypt the fusion image. In fact, the authorized user can also be the image owner.

Introduction of the scheme. The image owner uses the Arnold transform [5] for image scrambling encryption. The positive transformation formula is shown as Eq. (1), and the inverse transformation formula is shown as Eq. (2), where x_{n+1}, y_{n+1} is the location after transforming; x_n, y_n is the location before transforming; a and b are the keys of the transformation; and N is the height and width of the remote sensing image.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod \ (N), \tag{1}$$

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} ab+1 & -b \\ -a & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod \ (N). \tag{2}$$

Given an original remote sensing image, $\mathrm{Img}(i, j)$, $1 \leqslant i \leqslant M$, $1 \leqslant j \leqslant M$, where M is the height and width of images. The image owner uses positive transformation to encrypt $\mathrm{Img}(i, j)$, shown as Algorithm 1. Then the owner obtains the encrypted image, $\mathrm{EncImg}(i, j)$, which will be outsourced to the cloud for its encrypted image fusion operation.

Algorithm 1 ImageEncryption(a, b, n)

Require: $1 \leqslant i \leqslant M \bigwedge 1 \leqslant j \leqslant M \bigwedge 1 \leqslant k \leqslant n$;
while $k \neq n$ **do**
  while $i \neq M$ **do**
    while $j \neq M$ **do**
      $i_{\mathrm{new}} \Leftarrow (((i-1) + b(j-1)) \bmod M) + 1$;
      $j_{\mathrm{new}} \Leftarrow ((a(i-1) + (ab+1)(j-1)) \bmod M) + 1$;
      $\mathrm{EImg}(i_{\mathrm{new}}, j_{\mathrm{new}}) \Leftarrow \mathrm{Img}(i, j)$;
      $j \Leftarrow j + 1$;
    end while
    $i \Leftarrow i + 1$;
  end while
  Img $\Leftarrow$ EncImg;
  $k \Leftarrow k + 1$;
end while

* Corresponding author (email: shenmeng@bit.edu.cn)

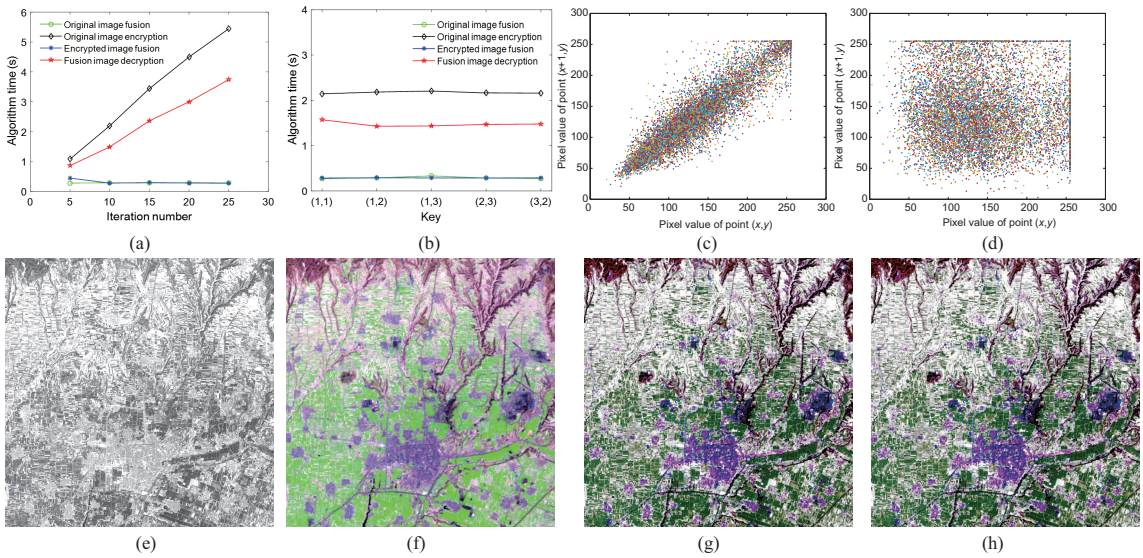

Figure 1 (Color online) Evaluation results of the proposed scheme. (a) Iteration number effect on scheme efficiency; (b) key-changing effect on scheme efficiency; (c) correlation between adjacent pixels in non-encrypted image; (d) correlation between adjacent pixels in encrypted image; (e) original panchromatic image; (f) original multispectral image; (g) original fusion image; (h) fusion image obtained by the proposed scheme.

The cloud uses the Brovey transform [6] method for encrypted image fusion, shown as Eq. (3), where R, G, and B comprise the band of the multispectral image; Pan is the band of the panchromatic image; R_{new}, G_{new}, and B_{new} is the band of the fusion image.

$$\begin{cases} R_{\text{new}} = \dfrac{R}{R+G+B}\text{Pan}; \\ G_{\text{new}} = \dfrac{G}{R+G+B}\text{Pan}; \\ B_{\text{new}} = \dfrac{B}{R+G+B}\text{Pan}. \end{cases} \tag{3}$$

Given an encrypted panchromatic image, $\text{EPImg}(i,j)$, and an encrypted multispectral image, $\text{EMImg}(i,j)$, the cloud uses Algorithm 2 to obtain the encrypted fusion image, $\text{EFImg}(i,j)$, sending it to the authorized user. The authorized user receives the encrypted fusion image, $\text{EFImg}(i,j)$, from the cloud and uses the inverse transformation rule from Eq. (2) to decrypt it, obtaining the original fusion image, $\text{FImg}(i,j)$.

Algorithm 2 EncryptedImageFusion

Require: $1 \leqslant i \leqslant M \bigwedge 1 \leqslant j \leqslant M \bigwedge k = 1$;
while $i \neq M$ **do**
  while $j \neq M$ **do**
    $\text{tmp} \Leftarrow \text{EMImg}(i,j,1)+\text{EMImg}(i,j,2)+\text{EMImg}(i,j,3)$;
    while $k \neq 4$ **do**
      $\text{EFImg}(i,j,k) \Leftarrow (\text{EMImg}(i,j,k)/\text{tmp}) \times \text{EPImg}(i,j)$;
      if $\text{EFImg}(i,j,k) < 0$ **then**
        $\text{EFImg}(i,j,k) \Leftarrow 0$;
      else if $\text{EFImg}(i,j,k) > 255$ **then**
        $\text{EFImg}(i,j,k) \Leftarrow 255$;
      end if
      $k \Leftarrow k+1$;
    end while
    $j \Leftarrow j+1$;
  end while
  $i \Leftarrow i+1$;
end while

Evaluation. We take the 8th band of Landsat as the panchromatic image, and we take the synthetic image of the 4th, 5th, and 6th bands of Landsat as the multispectral image in our experiment. Additionally, we take 1000×1000 areas from the panchromatic image and the multispectral image, respectively, as our experimental images. We implement the proposed scheme using Matlab R2015b on a 2.7-GHz Intel Core Processor.

The image encryption key of our scheme is $K = \{a, b, n\}$, where a and b have the same meaning, as shown in Eq. (1). Eq. (2) and n represent the number of iterations to encrypt images. We change (a, b) and n in K, respectively, to explore the effect of image encryption key-changing on scheme efficiency, including the times of image encryption, encrypted image fusion, image decryption, and image fusion, without privacy preservation. We fix a and b in K and increase n step-by-step. The efficiency of the proposed scheme is shown in Figure 1(a). We conclude that the number of iterations has no effect on the efficiency of encrypted image fusion without privacy preservation. More iterations lead to more encryption and decryption times. Thus, we fix n in K and change (a, b). The efficiency of the proposed scheme is shown in Figure 1(b). We conclude that the changing of (a, b) in K has no effect on scheme efficiency.

The original panchromatic and multispectral images in our experiment are shown in Figures 1(e) and (f), respectively. The original fusion image obtained by Brovey transformation is shown in Figure 1(g). The fusion image obtained by our scheme is shown in Figure 1(h). We find that Figures 1(g) and (h) are, visually, nearly the same. To confirm our conception, we compare the images on the computer, showing that they are the same. Furthermore, we conduct a qualitative evaluation [7] of Figures 1(g) and (h) from the aspect of mean, standard deviation, information entropy, average gradient, and correlation coefficient. These aspects are commonly used to evaluate images. The results show that these quality evaluation values are all the same.

Correlation between adjacent pixels in an image is a type of statistical analysis. We analyze the correlation of adjacent pixels in non-encrypted and encrypted images in Figure

1(e). Results are shown in Figures 1(c) and (d). We find that pixel distribution in the non-encrypted image is approximately linear, and pixel distribution in the encrypted image is dispersed, further indicating that our image encryption algorithm resists the statistical correlation analysis between adjacent pixels in the image.

Conclusion and future work. We proposed an encrypted image-fusion scheme based on the Brovey, which ensures both image privacy and encrypted image fusion in the cloud. The experimental results show that our scheme ensures the quality of the fusion image and its privacy preservation. In future works, we will research encrypted images fusion as pixel values are changed.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant No. 61602039), and in part by Key Lab of Information Network Security of Ministry of Public Security (The Third Research Institute of Ministry of Public Security) (Grant No. C18604).

References

1 Wang Z J, Ziou D, Armenakis C, et al. A comparative analysis of image fusion methods. IEEE Trans Geosci Remote Sens, 2005, 43: 1391–1402

2 Shen M, Ma B L, Zhu L H, et al. Cloud-based approximate constrained shortest distance queries over encrypted graphs with privacy protection. IEEE Trans Inf Forensic Secur, 2018, 13: 940–953

3 Ahmad N. Cloud computing: technology, security issues and solutions. In: Proceedings of the 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, 2017. 30–35

4 Zhu L H, Tang X Y, Shen M, et al. Privacy-preserving DDoS attack detection using cross-domain traffic in software defined networks. IEEE J Sel Areas Commun, 2018, 36: 628–643

5 Manikandan V M, Masilamani V. An efficient visually meaningful image encryption using Arnold transform. In: Proceedings of IEEE Students' Technology Symposium (TechSym), Kharagpur, 2016. 266–271

6 Zhao J L, Huang L S, Yang H, et al. Fusion and assessment of high-resolution WorldView-3 satellite imagery using NNDiffuse and Brovey algotirhms. In: Proceedings of IEEE International Geoscience and Remote Sensing Symposium (IGARSS), Beijing, 2016. 2606–2609

7 Xia Q, Hu Z Q, Li J H, et al. Quality evaluation of different remote sensing image fusion methods (in Chinese). Geospatial Inf, 2013, 11: 49–51