支持隐私保护的加密遥感图像融合算法

沈蒙^{1,2}, 程国华¹, 祝烈煌^{1,2*}

1. 北京理工大学计算机学院, 北京 100081

2. 北京市海量语言信息处理与云计算应用工程技术研究中心, 北京 100081

* 通信作者. E-mail: liehuangz@bit.edu.cn

收稿日期: 2016-10-09; 接受日期: 2016-11-28; 网络出版日期: 2017-03-06

国家自然科学基金 (批准号: 61602039, 61272512, 61300177) 和北京市自然科学基金 (批准号: 4164098, 4121001) 资助项目

摘要 在遥感领域, 卫星拍摄得到的多光谱图像和全色图像均无法满足实际应用需求, 因此需要通过图像融合来获得空间分辨率和光谱分辨率都很高的图像, 从而更加准确地识别和定位图像中的地面物体. 由于图像融合算法对计算能力和存储空间要求较高, 借助公有云平台 (如阿里云) 进行图像融合已经成为一种趋势. 然而, 现有图像融合算法均无法保护图像隐私, 即无法避免云平台服务商或者网络窃听者获取图像信息. 本文提出了一种支持隐私保护的遥感图像融合算法 SecureFusion. 该算法首先对原始多光谱图像和全色图像进行加密, 然后对加密图像采用主成分分析法进行融合, 得到加密的融合图像, 最后对加密的融合图像进行解密恢复出真正的融合图像. 实验结果表明, 与已有算法相比, 本文提出的隐私保护算法可以得到同等质量的融合图像, 算法总体执行时间的增量均值约为 25.9%. 据我们所知, 本文首次提出了针对遥感图像融合的隐私保护算法.

关键词 遥感图像, 隐私保护, 图像融合, 主成分分析, 图像处理, 加密

1 引言

图像融合是数据融合技术前沿中一个相对较新的研究领域^[1], 也是遥感领域获取高质量图像的常用方法. 随着遥感技术的发展, 遥感卫星种类层出不穷, 许多遥感卫星的传感器都能获取不同分辨率的图像, 比如 Landsat8 卫星的传感器可以接收 15 米分辨率的全色图像和 30 米分辨率的多光谱图像. 这两种图像都有各自的优缺点: 全色图像具有较高的空间分辨率, 但是光谱分辨率低, 如图 1(a) 所示; 而多光谱图像的光谱分辨率高, 但空间分辨率较低, 如图 1(b) 所示. 由此可见, 上述两种图像无法兼具高光谱分辨率和高空间分辨率的特性, 因而难以准确识别和定位图像中的地面物体. 为了解决这一问题, 研究者使用图像融合技术, 将全色图像和多光谱图像进行融合, 得到具有高光谱分辨率和高空间分辨率的融合图像. 按照遥感图像融合的层次, 可以将已有图像融合技术大致分为 3 类^[2]: (1) 基于

引用格式: 沈蒙, 程国华, 祝烈煌. 支持隐私保护的加密遥感图像融合算法. 中国科学: 信息科学, 2017, 47: 736–751, doi: 10.1360/N112016-00241
Shen M, Cheng G H, Zhu L H. Privacy-preserving encrypted image fusion algorithm for remote sensing (in Chinese). Sci Sin Inform, 2017, 47: 736–751, doi: 10.1360/N112016-00241

图 1 (网络版彩图) 遥感图像示例

Figure 1 (Color online) Examples of remote sensing images. (a) Panchromatic image; (b) multi-spectral image

像元的融合方法, 包括加权融合法、比值变换法、HIS 变换法和主成分分析变换法等; (2) 基于特征的融合方法, 包括 Bayes 估计法和熵法等; (3) 基于决策的融合方法, 如模糊聚类法等. 在上述各类方法中, 主成分分析变换法能够融合具有 3 个以上波段的图像, 融合后的图像不仅包含了全色图像的空间信息, 也包含了多光谱图像的光谱信息, 并且纹理特征细致清晰, 因而得到广泛应用.

由于主成分分析法涉及特征值、特征向量等计算密集型过程, 需要硬件设备具备较高的计算能力和存储空间. 随着亚马逊 EC2¹⁾、阿里云²⁾等公有云平台的日益普及, 借助云平台提供的计算和存储能力进行图像融合成为未来的发展趋势. 然而, 卫星遥感图像往往包含森林、湖泊等地面物体, 属于一国的机密信息, 如果直接将原始遥感图像传输给第三方 (如公有云平台) 进行融合, 那么图像内容就会泄露给第三方. 同时, 原始遥感图像在传输过程中还可能受到不法分子的攻击, 导致融合图像的质量下降甚至不可用. 因此, 如何利用公有云平台的资源优势进行图像融合, 同时保护图像隐私, 是亟待解决的关键问题.

本文基于已有的主成分分析法, 提出了一种支持隐私保护的加密遥感图像融合算法 SecureFusion. 该算法首先对原始多光谱图像和全色图像进行加密, 然后采用主成分分析法对加密图像进行融合, 得到加密融合图像, 最后对加密融合图像进行解密, 从而恢复出真正的融合图像. 实验结果表明, 与已有算法相比, 本文提出的隐私保护图像融合算法可以得到同等质量的融合图像, 由加解密过程导致的算法执行时间增量平均为 25.9%. 据我们所知, 本文是首个关注遥感图像融合中隐私保护问题的工作.

本文的内容组织如下: 第 2 节简要介绍相关研究工作; 第 3 节问题定义与描述; 第 4 节介绍支持隐私保护的加密遥感图像融合算法; 第 5 节进行性能评价与安全性分析; 第 6 节对全文进行总结.

2 相关工作

2.1 图像融合方法

通过进行图像融合, 可以弥补卫星传感器的不足, 得到空间分辨率和光谱分辨率都很高的遥感图像, 常见的图像融合算法有比值 (Brovey) 变换法, HIS 变换法和 PCA 变换法^[3]. 比值变换法是基于代

1) Amazon elastic compute cloud. <https://aws.amazon.com>.

2) Ali cloud cloud computing. <https://www.aliyun.com>.

图 2 主成分分析变换法流程图

Figure 2 Flow chart of principal component analysis transformation method

数运算的,它是通过将多光谱图像的 3 个波段 B, G, R 进行归一化后的结果与全色图像相乘得到融合后图像的 3 个波段 Bnew, Gnew, Rnew 完成融合. HIS 变换法和 PCA 变换法是基于空间变换的. HIS 变换法是通过让多光谱图像在 RGB 空间和 HIS 空间之间转换来完成图像融合的. PCA 变换法也称主成分分析变换法,由 Karhunen 和 Loeve 首先提出,所以也称为 K-L 变换^[4].将其应用到图像融合中是将多个波段的多光谱图像进行降维处理,提取出其主成分,从而将多光谱图像用几个相互独立的主要波段表示出来,具体流程如图 2 所示.

2.2 图像加密技术

在公共信道传输图像时,图像加密技术是最有效的保护图像隐私的方法^[5],它是指对原始图像进行某种变换,使处理后得到的图像与原始图像形成视觉差异,达到图像加密的作用,保护图像的隐私.图像置乱技术就是一种重要的图像加密技术^[6],它是指将一幅表达某种信息的图像变成一幅看起来杂乱无章的图像,若想要从中恢复其原本的信息要花费巨大的代价,从而起到保护图像隐私的作用.由于图像置乱过程方法的选取、方法的融合以及方法的参数有很多种,因此组合起来的结果会千差万别,因此从安全角度考虑图像置乱加密技术是可行的.图像置乱加密技术分为对图像的空域、频域、空域和频域同时进行的置乱加密.基于像元点位置的置乱加密是图像空域置乱加密中的一种,它是指通过对图像进行某种变换来移动图像中像元点的位置,干扰图像中的信息.通常该置乱加密过程要满足变换是到其自身的一一映射和满映射.常见的置乱变换技术有 Arnold 变换^[7]、幻方^[8]、骑士巡游变换^[9]、Hilbert 曲线^[10]等.由于混沌^[11,12]系统具有遍历性、混沌性、指数发散性,并且对系统初值和参数具有很高的敏感性,因此混沌序列也常常被用于图像置乱加密中. Logistic 映射是一个典型的混沌系统,常被应用于密码系统中.其映射方程式如式 (1) 所示:

$$x_{n+1} = \mu x_n - \mu x_n^2 \quad n = 0, 1, 2, \dots, \mu, \quad (1)$$

其中 μ 为分岔参数,范围为 $(0, 4]$, $0 < x < 1$. 当 $3.569946 \leq \mu \leq 4$ 时, Logistic 映射处于混沌状态,此时混沌系统的状态是最好的,没有周期,不收敛,并且敏感依赖初值.目前在图像加密技术的基础上已经有加密图像检索的相关研究,例如 Liu 等^[13]提出的一种基于密文检索的对称加密方法,文献^[14, 15]提出的基于非对称的密文检索方法,黄冬梅等^[16]提出的一种基于 Henon 映射的加密遥感图像的检索方案.但是目前在加密图像融合领域,还缺乏针对性研究.

图 3 (网络版彩图) 支持隐私保护的图像融合系统模型

Figure 3 (Color online) Privacy-preserving image fusion system model

3 问题定义与描述

3.1 系统模型

支持隐私保护的图像融合是指在不泄露图像内容隐私的情况下,对原始多光谱图像和原始全色图像进行融合操作,得到与原始图像相比具有高光谱分辨率和高空间分辨率的融合图像。

如图 3 所示,支持隐私保护的图像融合系统模型主要包含 3 类角色,分别为

- 图像持有者: 掌握原始图像信息,需要借助第三方云平台对图像进行融合.为了保护图像内容隐私,图像持有者通常会对原始图像进行加密.
- 第三方云平台: 接收图像持有者的加密原始图像,执行加密图像融合算法,得到加密融合图像.
- 授权用户: 接收第三方云平台的加密融合图像,进行授权解密并使用融合图像.

上述模型中当授权用户并非图像持有者时,本文假设图像持有者和其他授权用户之间存在一个安全的信道能够传递图像解密密钥。

3.2 威胁模型

由于本文算法的目的是实现在不泄露图像信息的情况下完成加密图像融合的操作,因此在此假设两个图像持有者都是诚实的,他们不会与其他人(外部窃听者、敌手或第三方)进行共谋来泄露图像的信息.基于上述系统模型,本文主要关注以下 3 类潜在威胁:

- (1) 外部窃听者. 在图像持有者与第三方进行(原始或者融合)图像传输过程中,外部敌手由于某些特定的目的,会窃听图像信息.这是一种较弱的敌手,通常对图像进行加密就可以抵御这种敌手.
- (2) 半诚实第三方. 这里的第三方云平台是指图像融合算法的执行人.本文假设第三方云平台会准确无误地执行图像融合算法,但是在图像融合过程中会通过统计分析等方式来推测图像的信息.
- (3) 恶意敌手. 恶意敌手能够对图像进行任意的恶意行为,比如在图像传输过程中进行攻击图像或者窥探图像内容等行为.恶意敌手具有最强的攻击力和破坏力.

3.3 设计目标

- (1) 安全性: 图像融合算法能抵抗 3.2 小节中提到的 3 类威胁.
- (2) 准确性: 在保护图像隐私的同时, 本文算法得到的融合图像与已有的、不支持隐私保护的算法得到的融合图像具有同等质量.
- (3) 高效性: 本文算法的计算复杂度与不支持隐私保护的图像融合算法差别较小, 因加解密导致的运算时间增量在可接受的范围内.

4 支持隐私保护的遥感图像融合算法

本节将重点描述支持隐私保护的图像融合算法 SecureFusion 的设计与实现过程.

4.1 加密原始图像

为了保护图像中的隐私信息, 图像持有者在将图像发送给第三方之前要先对原始图像进行置乱加密. 令原始图像为 $B(i, j), 1 \leq i \leq M, 1 \leq j \leq N$, 其中 M 和 N 分别为图像的长和宽. 则图像持有者根据式 (1) 的特点设定参数 μ 和密钥 x_0 的初值, 然后生成混沌序列 $\{X\}$, 为了使产生的混沌序列具有更好的混沌特性, 去除 $\{X\}$ 中的前 200 个值. 接着对序列 $\{X\}$ 进行排序产生一个图像置乱加密的序列 $\{\text{Ind}\}$, 其中的元素表示排序后序列 $\{X\}$ 中的元素在排序前序列 $\{X\}$ 中的位置.

设定迭代次数 r , 利用序列 $\{\text{Ind}\}$ 对图像中的像元点位置进行置换. 置换是从第一个像元点开始逐个进行置换, 令 t 和 q 分别为 Ind_k/N 的商和余数, 置换规则如式 (2) 所示. 将每一次迭代产生的置乱图像作为下一次迭代置乱的输入图像. 当迭代次数达到 r 时, 迭代停止, 得到加密后的原始图像 $E(i, j), 1 \leq i \leq M, 1 \leq j \leq N$. 图像加密完成后, 图像持有者将加密的图像发送给第三方进行图像融合,

$$B(i, j) \longleftrightarrow \begin{cases} B(t, N), & q = 0, \\ B(t + 1, q), & q \neq 0. \end{cases} \quad (2)$$

4.2 加密图像的融合

第三方在收到来自图像持有者的加密图像 $E(i, j)$ 后, 根据第 2 节中提到的主成分分析变换法对加密的多光谱图像和加密的全色图像进行图像融合来得到加密融合图像. 第三方先用式 (3) 计算加密多光谱图像的协方差矩阵 ES_{ij} , 并计算协方差矩阵 ES_{ij} 特征值和特征向量, 让特征值满足 $\lambda_1 > \lambda_2 > \dots > \lambda_m$, 相应的特征向量顺序为 $\varphi_1, \varphi_2, \dots, \varphi_m$,

$$\text{ES}_{ij} = \frac{1}{M \times N} \sum_{k=1}^N (\text{EX}_{ik} - G_i)(\text{EX}_{jk} - G_j), \quad i, j \in [1, m], \quad (3)$$

$$G_i = \text{Gray}(\text{EX}_i) = \frac{\sum_{k=1}^{M \times N} \text{EX}_{ik}}{M \times N}, \quad i \in [1, m], \quad (4)$$

其中, EX_i 表示加密多光谱图像中的各个波段; EX_{ik} 为加密多光谱图像第 i 个波段中的第 k 个像元点的值, i 表示波段号; m 表示最大的波段号; G_i 为加密多光谱图像各个波段的灰度均值, 其计算过程如式 (4) 所示.

然后根据式 (5) 用特征向量矩阵对加密多光谱图像进行主分量正变换, 将得到的第一主分量与加

密全色图像进行直方图匹配,并用匹配后的结果替换加密多光谱图像的第一主分量.设替换后的第一主分量为 $EI_k, k \in [1, N]$,

$$\begin{bmatrix} EI_k & EX_{2k}^* & \cdots & EX_{mk}^* \end{bmatrix} = \begin{bmatrix} EX_{1k} & EX_{2k} & \cdots & EX_{mk} \end{bmatrix} \begin{bmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1m} \\ \varphi_{21} & \varphi_{22} & \cdots & \varphi_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_{m1} & \varphi_{m2} & \cdots & \varphi_{mm} \end{bmatrix}, \quad (5)$$

其中, EX_{mk} 表示多光谱图像第 m 波段中的像元点, EX_{mk}^* 表示进行主分量正变换后的多光谱图像第 m 波段中的像元点.

最后根据式 (6) 对得到的加密多光谱图像进行主分量逆变换,得到加密的融合图像 $Enrgb(i, j)$, $1 \leq i \leq M, 1 \leq j \leq N$. 并将加密的融合图像发送至图像所有者或其他授权用户.

$$\begin{bmatrix} EX_{1k} & EX_{2k} & \cdots & EX_{mk} \end{bmatrix} = \begin{bmatrix} EI_k & EX_{2k}^* & \cdots & EX_{mk}^* \end{bmatrix} \begin{bmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1m} \\ \varphi_{21} & \varphi_{22} & \cdots & \varphi_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_{m1} & \varphi_{m2} & \cdots & \varphi_{mm} \end{bmatrix}^{-1}, \quad (6)$$

其中, EX_{mk} 表示进行主分量逆变换后多光谱图像第 m 波段的像元点,也就是融合图像中第 m 波段的像元点, EX_{mk}^* 的含义与式 (5) 中含义相同.

4.3 解密融合图像

图像所有者或者其他授权用户为了获取到融合图像的原有信息,要将收到的来自第三方的加密融合图像 $Enrgb(i, j), 1 \leq i \leq M, 1 \leq j \leq N$ 进行解密. 根据图像置乱加密的步骤,图像所有者或者其他授权用户使用解密的参数和密钥根据式 (1) 生成混沌序列 $\{X\}$, 并对其排序得到序列 $\{Ind\}$. 然后利用生成的序列 $\{Ind\}$ 对加密融合图像中的像元点位置进行置换,此时的置换是从最后一个像元点开始逐个向前进行置换,其置换规则与式 (2) 所述规则相同. 将每一次迭代产生的置乱图像作为下一次迭代置乱的输入图像,当达到迭代次数 r 时迭代终止,得到原始的融合图像 $Res_rgb(i, j), 1 \leq i \leq M, 1 \leq j \leq N$.

5 性能评价与安全性分析

本节将对第 4 节中设计的算法的性能与安全性进行实验验证与分析,并着重回答以下问题.

- 本文提出的支持隐私保护的图像融合算法是否能达到与传统算法相同的图像融合效果?
- 本文提出的算法效率如何? 考虑隐私保护而造成的算法运行时间开销有多大?
- 本文提出的算法在图像隐私保护和安全性方面表现如何?

5.1 实验环境设置

本节中的实验采用两台 PC 机,其中一台作为图像所有者,主要进行图像的加解密操作;另一台模拟第三方云平台,主要进行加密图像融合操作.其中作为第三方的 PC 配置是 Intel(R) Core(TM) i5 2.5 GHz 处理器, 4 GB 内存.

图 4 (网络版彩图) 原始多光谱图像
Figure 4 (Color online) Original multi-spectral image

图 5 原始全色图像
Figure 5 Original panchromatic image

图 6 (网络版彩图) 加密多光谱图像
Figure 6 (Color online) Encrypted multi-spectral image

图 7 加密全色图像
Figure 7 Encrypted panchromatic image

实验所用图像为 Landsat8 遥感图像的波段图像, Landsat8 共有 11 个波段, 其中的第 4~6 波段合成的图像常用来做植被分析, 具有 30 米的分辨率; 第 8 波段图像是高空间分辨率图像, 具有 15 米的分辨率. 将 Landsat8 第 4~6 波段合成的图像作为多光谱图像, 第 8 波段图像作为全色图像. 为了便于实现, 在多光谱图像和全色图像上分别截取出大小为 1000 像素 $\times$ 1000 像素的区域作为原始图像, 如图 4 和 5 所示分别为输入的原始多光谱图像和原始全色图像. 实验共使用了 50 对原始多光谱图像和原始全色图像.

实验对比采用的基线算法是传统的主成分分析 (PCA) 图像融合算法, 该算法不支持图像隐私保护. 所有算法均采用 Matlab 7.0 完成. 对于本文所提出的算法, 随机选取图像加密参数 $\mu = 3.97376213$, 密钥 $x_0 = 0.632781$, 迭代次数 $r = 1$.

5.2 图像融合效果分析

采用 5.1 小节的参数及密钥设置得到的加密多光谱图像和加密全色图像分别如图 6 和 7 所示. 在不考虑隐私保护的情形中, 传统 PCA 方法对多光谱图像和全色图像进行融合得到的融合图像如图 8 所示. 图像所有者将加密后的多光谱图像和加密的全色图像发送给第三方进行加密图像融合, 得到的加密融合图像如图 9 所示. 第三方将加密的融合图像发送给其他授权用户, 解密后的融合图像如图 10 所示.

将不支持隐私保护情况下和支持隐私保护情况下得到的融合图像进行相等性测试, 实验结果表明

图 8 (网络版彩图) 原始融合图像
Figure 8 (Color online) Original fusion image

图 9 (网络版彩图) 加密融合图像
Figure 9 (Color online) Encrypted fusion image

图 10 (网络版彩图) 解密后融合图像
Figure 10 (Color online) Fusion image obtained by decryption

在这两种情况下得到的融合图像完全相同. 由此可以说明在支持隐私保护的情况下可以保证融合图像的准确性. 下面将对支持隐私保护时得到的融合图像与原始的多光谱图像进行质量评价来分析图像融合的效果.

图像质量评价可以从定性和定量两个方面来分析^[17]. 定性分析主要是通过人眼目视观察来进行, 而定量分析主要是针对图像的灰度均值、标准差、信息熵、平均梯度、相关系数等几方面指标进行量化分析. 由于定性分析仅仅能在图像差别较大时判别图像质量的好坏, 当图像差别较小时无法具体判别哪一副图像的质量更好, 所以在此对图像进行定量分析. 根据图像定量分析的通用标准, 本文将从信息熵、均值、标准差、平均梯度、相关系数等 5 个方面对图像融合的效果进行量化分析.

各指标的含义和计算方式如下所示. 其中各关键参数的含义为: i 为图像的波段数, X_{kp} 和 YX_{kp} 为融合图像和原始图像中像元点的值, M 和 N 分别为图像的宽和高, P_{ij} 为出现像元值为 (i, j) 的概率.

(1) 信息熵: 与图像含有信息的丰富程度正相关. 其计算过程如式 (7) 所示:

$$H(X_1, X_2, \dots, X_i) = \sum_{j_1, j_2, \dots, j_i=0}^{255} P_{j_1, j_2, \dots, j_i} \times \log_2 P_{j_1, j_2, \dots, j_i}. \quad (7)$$

(2) 均值: 图像灰度的均值, 反映图像的平均亮度, 均值越大图像越亮. 其计算过程为

$$\text{Avg}(X) = \frac{\sum_{k=0}^{M-1} \sum_{p=0}^{N-1} X_{kp}}{M \times N}. \quad (8)$$

表 1 图像融合效果对比
Table 1 Quantitative comparison of image fusion results

Image	Mean	Standard deviation	Information entropy	Average gradient	Correlation coefficient
Original multi-spectral image	103.495	57.2562	6.398	13.103	—
Fusion image with PCA	98.371	49.492	6.673	14.685	0.7565
Fusion image with SecureFusion	98.371	49.492	6.673	14.685	0.7565

(3) 标准差: 体现了图像中像元值与灰度均值之间的离散程度. 标准差越大, 则图像灰度分布越分散. 其计算过程为

$$\text{Std}(X) = \frac{\sqrt{\sum_{k=0}^{M-1} \sum_{p=0}^{N-1} (X_{kp} - \text{Avg}(X_{kp}))^2}}{\sqrt{M \times N}}. \quad (9)$$

(4) 平均梯度: 反映图像相邻行列间变换的速率. 该值越大, 图像越清晰. 其计算过程为

$$\text{Gra}(X) = \frac{\sum_{k=0}^{M-1} \sum_{p=0}^{N-1} \sqrt{(X_{(k+1)p} - X_{kp})^2 + (X_{k(p+1)} - X_{kp})^2}}{M \times N}. \quad (10)$$

(5) 相关系数: 指融合图像相对原始图像的光谱特性保持程度. 相关系数越接近于 1, 图像保真度越好. 其计算过程为

$$\rho_i = \frac{\sum_{k=1}^{M \times N} (YX_{ik} - \overline{YX_{ik}})(X_{ik} - \overline{X_{ik}})}{\sqrt{\sum_{k=1}^{M \times N} (YX_{ik} - \overline{YX_{ik}})^2 (X_{ik} - \overline{X_{ik}})^2}}, \quad i \in [1, m]. \quad (11)$$

对图 4, 8 和 10 进行定量评价, 结果如表 1 所示. 可以看出, 解密后的融合图像的各项指标均与传统方法得到的融合图像相同, 不会因图像加密而导致融合效果的损失. 这一结果对其余实验图像均成立, 篇幅所限不再逐一展示. 与原始多光谱图像相比, 融合图像的信息熵和平均梯度增加, 说明融合图像的信息更加丰富、清晰度更高. 因此, 本文算法能够得到高质量的融合图像.

5.3 图像融合算法效率分析

运行时间是衡量算法效率的核心指标, 本文所提出的图像融合算法的运行时间主要包括 3 部分: 原始图像加密时间、加密图像融合时间、融合图像解密时间 (图像在各角色之间的传输时间暂不考虑). 而传统的图像融合算法不涉及加解密过程, 其运行时间主要是图像融合时间. 本小节将通过调节参数取值, 分析参数对隐私保护图像融合算法的影响.

(1) 固定迭代次数 $r = 1$, 令密钥 x_0 从 0.00001 到 0.1 每次呈 10 倍变化, 得到算法运行时间如图 11 所示; 令密钥 x_0 从 0.1 到 0.9 按步长 0.1 递增, 结果如图 12 所示. 图中的每一项时间分别是在相同条件下运行 10 次得到的时间均值.

由图 11 和 12 可以看出, 本文所提出的算法运行时间在密钥 x_0 倍增和递增时保持稳定, 因此密钥取值的变化对算法运行时间影响较小. 传统算法的运行时间在 13 s 左右, 本文算法用时在 16 s 左右. 将本算法涉及的 3 部分进行分解, 可以看出加密图像融合的时间与传统算法的图像融合时间大致相同, 均为 13 s 左右. 因此, 运行时间的增加主要是由原始图像加密、融合图像解密造成的, 这两个环节的运行时间都在 1 s 左右. 由图 11 和 12 的结果可计算得到, 与传统图像融合算法相比, 本算法的运行时间增量均值为 25.9%.

图 11 (网络版彩图) 倍增密钥 x_0 与算法时间

Figure 11 (Color online) Algorithm execution time with multiplicative x_0

图 12 (网络版彩图) 递增密钥 x_0 与算法时间

Figure 12 (Color online) Algorithm execution time with additive x_0

图 13 (网络版彩图) 迭代次数与算法时间

Figure 13 (Color online) Algorithm execution time with varying iterations

(2) 固定密钥 $x_0 = 0.632781$, 将迭代次数 r 从 1 到 20 递增, 得到的算法运行时间如图 13 所示。

可以看出, 原始图像融合时间与加密图像融合时间不随迭代次数的增加而增加, 一直维持在 13 s 左右; 原始图像加密时间与融合图像解密时间随迭代次数的增加而呈类似线性增加。

通过综合分析密钥和迭代次数的实验结果, 可以得出结论: 本文所提出的算法运行时间是与密钥取值无关的, 即密钥在取值范围内的变化, 不会导致算法运行时间的剧烈变化; 本文算法会随着迭代次数的增大而呈线性增加。

5.4 隐私保护与安全性分析

针对图像融合的隐私性和安全性开展的攻击, 按照攻击手段的性质大致可以分为两类: 被动攻击和主动攻击。被动攻击是指敌手通过统计分析的方法, 对图像内容进行猜测和推断, 从而达到获取图像隐私信息的目的。而主动攻击是指敌手可以通过尝试不同的参数对加密图像进行解密, 或者通过控制传输信道对加密图像开展剪切攻击、噪声攻击等行为。本小节将分别分析所提出的算法在上述两类

表 2 密钥变化对加密图像统计分析值的影响
Table 2 Statistical analysis of the encrypted image with varying keys

Statistic	Original image	Key x_0								
		0.00001	0.0001	0.001	0.01	0.1	0.3	0.5	0.7	0.9
Horizontal correlation	0.9275	-0.0121	-0.0086	-0.0111	-0.0128	-0.0132	-0.0058	-0.0032	-0.0069	-0.0133
Vertical correlation	0.9099	0.00017	-0.00038	-0.00019	0.00018	0.0012	0.0017	0.0018	0.00064	0.00057
Right opposite angles correlation	0.8561	-0.00031	-0.00029	0.00010	-0.0017	-0.0011	0.00032	-0.000076	0.00041	-0.0022
Left opposite angles correlation	0.877	0.00057	0.00039	0.00022	0.00085	0.00016	-0.00099	-0.001	0.0014	0.00065
Average move distance	-	521.4309	520.9178	521.5568	521.2322	521.0533	521.1658	521.5278	521.2874	521.3996
Fixed point percentage	-	0.000001	0	0	0	0.000002	0	0.000001	0.000001	0.000001

攻击下的隐私保护性能 and 安全性.

5.4.1 算法应对统计分析的能力

首先对图像统计分析进行简要介绍, 然后分析算法应对统计分析的能力.

(1) 统计分析介绍. 对于一幅加密图像, 敌手可能通过以下 3 种统计分析手段来试图获取图像中的信息:

(i) 图像中相邻像元的相关度. 该值可以反映图像的扩散程度. 原始图像中相邻像元之间的相关度通常很大, 一种好的图像置乱加密算法应该让加密后的图像相邻像元之间的相关度趋近于零. 图像中相邻像元间的相关性分为水平相关度、垂直相关度和对角相关度.

(ii) 平均移动距离. 加密图像中的平均移动距离是指所有像元点移动距离总和的平均值, 当所有像元点都没有移动时, 平均移动距离最小, 等于零; 当所有元素都移动到对角线位置时平均移动距离达到最大值, 但是此时的加密图像也具有了确定性, 因此进行图像加密时要注意不要让平均移动距离达到最大值. 在实验参数有多种可能取值的情况下, 如果平均移动距离始终维持在某一固定范围内, 那么说明加密图像具有很好的隐私保护性能.

(iii) 不动点比例. 该值是指在图像置乱加密结束后, 没有移动位置的像元点数目占有所有像元点的数目的比例. 理想情况下不动点的比例是零, 也就是说所有的像元点都移动到了其他位置.

(2) 隐私保护性能分析. 算法的隐私保护性能分析主要从密钥 x_0 变化和迭代次数 r 变化两个方面进行研究.

(i) 固定迭代次数 $r = 1$, 将密钥 x_0 分别进行倍增变化 (从 0.00001 到 0.1 以 10 为步长倍增) 和递增变化 (从 0.1 到 0.9 以 0.2 为步长递增), 分析算法在上述指标体系下的性能.

当密钥呈现这两种变化方式时, 实验得到加密图像中相邻像元的相关度、像元点的平均移动距离与不动点比例如表 2 所示. 可以看出, 原始图像中各个方向上的相关度接近于 1, 说明相邻像元间的相关度很大; 加密图像中各个方向上的相关度都接近于 0, 像元点的平均移动距离始终在 521 左右, 不动

图 14 (网络版彩图) 加密图像中相邻像元的相关度与迭代次数关系图

Figure 14 (Color online) Correlation between adjacent pixels in encrypted image with different iterations

图 15 (网络版彩图) 原始图像中相邻像元间的相关关系

Figure 15 (Color online) Correlation between adjacent pixels in the original image

图 16 (网络版彩图) 加密图像中相邻像元间的相关关系

Figure 16 (Color online) Correlation between adjacent pixels in the encrypted image

点比例接近于 0, 说明加密图像中相邻像元间几乎不存在任何相关度, 几乎所有像元点都发生了移动.

(ii) 固定密钥 $x_0 = 0.632781$, 迭代次数 r 取值为 1 到 20. 加密图像中相邻像元的相关度与迭代次数之间的关系如图 14 所示. 可以看出, 当 $r = 1$ 时, 加密图像中相邻像元间的水平相关度为 -0.0089 , 垂直、右对角和左对角相关度均在 0 和 ± 0.001 之间波动, 几乎接近于 0; 当迭代次数逐渐增加时, 加密图像中相邻像元间的水平、垂直、右对角和左对角相关度均在 0 和 ± 0.004 之间波动, 都接近于 0. 综合看来, 随着迭代次数的增加, 加密图像中相邻像元间几乎不存在任何相关度.

经计算, 迭代次数变化时, 加密图像中像元点的平均移动距离始终为 521.2507, 不动点比例始终为 0, 该两类数值始终维持不变. 因此, 迭代次数对平均移动距离和不动点比例均没有影响.

当密钥 $x_0 = 0.632781$, 迭代 1 次时, 抽取图 5 和 7 中 $100 \text{ 像素} \times 100 \text{ 像素}$ 像元大小的图像块, 图 15 和 16 分别为原始图像和加密图像在垂直方向上相邻像元间的相关性. 可以看出, 原始图像相邻像元间呈线性关系, 而加密图像相邻像元间呈随机分布对应的关系, 因此加密后的图像有效保护了图像内容.

图 17 (网络版彩图) 使用错误和正确密钥解密得到的图像 (其中 (a)~(c) 使用错误密钥, (d) 使用正确密钥)

Figure 17 (Color online) Examples illustrating decryption with incorrect and correct keys. (a) $x_0 = 0.10000001$; (b) $x_0 = 0.63278099$; (c) $x_0 = 0.63278101$; (d) correct key x_0

上述分析说明, 当迭代 1 次时, 本文使用的加密算法可以有效打乱原始图像中相邻像元的相关度, 从而保护图像隐私. 迭代次数增加不会明显提高隐私保护效果. 结合图 13 展示的算法时间, 取 $r = 1$ 可以兼顾算法效率和隐私保护性能.

(3) 统计分析实验小结. 根据 (i) 和 (ii) 的实验结果表明, 当密钥不同, 迭代次数相同时, 图像相邻像元间相关性趋近于 0, 像元点平均移动距离约为 521, 不动点比例趋近于 0, 说明图像置乱加密达到了很好的效果, 并且仅仅迭代一次就可以达到很好的置乱效果, 从而很好地保护原始图像的隐私. 当取相同密钥, 迭代次数不同时, 图像相邻像元间相关性趋近于 0, 但是迭代次数对平均移动距离和不动点比例并没有影响.

根据上述有关图像隐私保护性能的实验, 可以得出结论, 本文算法可以打乱图像中像素点的位置, 扰乱攻击者对图像原有信息的判断, 保护图像隐私信息.

5.4.2 算法应对主动攻击的能力

本节首先通过密钥敏感性分析, 验证敌手猜测解密密钥时的算法安全性, 然后以剪切攻击和噪声攻击为例, 分析算法在两类场景下的安全性.

(1) 密钥敏感性分析. 对于如图 9 所示的加密融合图像, 假设敌手分别使用错误密钥 0.10000001, 0.63278099, 0.63278101 解密图像, 得到的解密图像分别如图 17(a)~(c) 所示, 其中图 17(d) 为使用正确密钥 $x_0 = 0.632781$ 解密后的图像. 从图 17(a)~(c) 可以看出, 本算法对于初值密钥非常敏感, 即使密钥之间相差很小 (例如图 17(b) 使用的错误密钥与正确密钥仅相差 1×10^{-8}), 也无法解密得到正确的图像.

图像加密过程中参数 μ 可取 $[3.569946, 4]$ 区间内的任意实数, 密钥 x_0 可取 $(0, 1)$ 内的任意实数. Logistic 映射混沌系统对参数 μ 的初值非常敏感, 由图 17 可见算法对密钥初值也非常敏感. 在双参数构成的庞大取值空间内, 敌手若想通过穷举法来试出正确的密钥, 那么其计算量将是异常巨大的, 几乎难以实现. 因此, 本文提出的算法可以有效应对敌手猜测密钥尝试解密的攻击行为.

(2) 抗攻击性分析. 图像在传输过程中可能会受到攻击者的破坏, 下面对得到的加密融合图像进行剪切攻击实验和加入噪声实验, 分析算法的安全性.

(i) 剪切攻击实验. 剪切攻击是指把图像中的一部分剪切掉, 从而扰乱图像的信息, 增加图像处理的难度. 对得到的加密融合图像进行剪切攻击, 随机选取剪切部分, 面积约占图像总面积的 20%. 受到剪切攻击的加密融合图像如图 18(a) 所示, 对应的解密图像如图 18(b) 所示. 对比图 18(a) 和 (b) 可知, 解密图像上有许多扰乱信息的杂点, 但是基本可以恢复出图像的原貌. 如果受到剪切攻击的范围

图 18 (网络版彩图) 受到攻击的加密图像及其解密图像

Figure 18 (Color online) Example illustrating encrypted images under attacks and their corresponding decrypted images. (a) Shear attack encrypted image; (b) decrypted image of (a); (c) noise attack encrypted image; (d) decrypted image of (c)

表 3 受到攻击的融合图像的质量评价参数
Table 3 Quantitative comparison of image fusion results

Image	Mean	Standard deviation	Information entropy	Average gradient	Correlation coefficient
Fusion image without attack	98.371	49.492	6.673	14.685	0.7565
Fusion image with shear attack	86.600	56.739	6.250	10.077	0.587
Fusion image with noise attack	99.847	50.738	6.622	16.541	0.699

越大, 那么杂点也就会越多, 对原始图像信息的获取难度也会增加.

(ii) 噪声攻击实验. 椒盐噪声攻击是指在图像中加入不同颜色的噪声点, 从而影响图像质量, 增加图像处理的难度. 在原始全色图像中加入密度为 0.02 的椒盐噪声. 受到椒盐噪声攻击的全色图像如图 18(c) 所示, 对应的解密图像如图 18(d) 所示. 对比图 18(c) 和 (d) 可知, 解密图像上有许多扰乱信息的杂点, 但对原始图像中信息的获取影响不大.

表 3 中给出了受到剪切攻击和噪声攻击时得到的融合图像和未受到攻击时得到的融合图像的质量评价数据. 可以看出, 受到攻击的融合图像在均值、标准差、信息熵、平均梯度和相关系数都与未受到攻击的融合有所偏差, 但变化不大, 说明受到攻击的融合图像解密后仍保持较好的亮度 (由均值体现)、信息量 (由信息熵体现) 和光谱特性 (由相关系数体现). 对比图 10, 18(b) 和 18(d), 同时结合表 3 中的数据可以发现, 受到剪切攻击或椒盐噪声攻击的加密融合图像与原始融合图像相比, 解密出的融合图像上存在部分扰乱信息的杂点, 但是仍可以恢复出大致的原始图像轮廓, 对地物的识别影响较小, 这说明本文算法具有较强的抗剪切攻击能力和抗噪声攻击能力.

6 结论

本文提出了一种支持隐私保护的加密图像融合算法 SecureFusion, 该算法首先对原始图像进行加密, 然后将加密的图像发送给第三方进行加密图像的融合, 最后由请求者对得到的加密融合图像进行解密获得原始的融合图像. 实验表明, 本算法得到的融合图像质量与不支持隐私保护的算法完全相同, 且具备较强的抗攻击性, 通过调整参数取值可以将算法执行时间的增量保持在可控范围内. 本文采用的图像置乱加密算法仅对图像像元位置进行了置乱, 没有改变像元值, 今后将对加密算法进行改进和完善.

参考文献

- 1 Yang Y, Han C Z, Kang X, et al. An overview on pixel-level image fusion in remote sensing. In: Proceedings of the IEEE International Conference on Automation and Logistics, Jinan, 2007. 2339–2344
- 2 Xing S. Research on multi-source remote sensing image registration and fusion technology registration. Dissertation for Master Degree. Zhengzhou: PLA Information Engineering University, 2004 [邢帅. 多源遥感影像配准与融合技术的研究. 硕士学位论文. 郑州: 解放军信息工程大学, 2004]
- 3 Chen C, Li Y Q, Liu W, et al. SIRF: simultaneous satellite image registration and fusion in a unified framework. IEEE Trans Image Process, 2015, 24: 4213–4224
- 4 Lin Z. The cell image segmentation based on the K-L transform and OTSU method. In: Proceedings of the International Conference on Multimedia and Signal Processing (CMSP), Guilin, 2011. 25–28
- 5 Zhang Y, Hou W G. A fast image encryption algorithm using plaintext-related confusion. In: Proceedings of the IEEE Information Technology, Networking, Electronic and Automation Control Conference, Chongqing, 2016. 293–297
- 6 Deng S J, Zhang D G, Pu Z L. Digital image scrambling algorithm based on chaotic system. Comput Sci, 2008, 35: 238–240 [邓绍江, 张岱固, 濮忠良. 一种基于混沌的图像置乱算法. 计算机科学, 2008, 35: 238–240]
- 7 Yang Y, Yang J, Feng J C. Algorithm based on arnold and RSA for optimal selection of large prime numbers in image encryption. Comput Sci, 2013, 40: 178–180 [杨洋, 杨洁, 冯久超. 一种基于 Arnold 置乱和优化大素数选取方案的 RSA 数字图像加密算法. 计算机科学, 2013, 40: 178–180]
- 8 Wen M G, Huang S C, Han C C. An information hiding scheme using magic squares. In: Proceedings of the International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), Fukuoka, 2010. 556–560
- 9 Kumar J, Nirmala S. Securing the contents of document images using knight moves and genetic approach. In: Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, 2015. 1091–1095
- 10 Li X M, Tao R, Dai L L, et al. Reality-preserving image encryption associated with the generalized Hilbert transform. In: Proceedings of the IEEE International Symposium on Industrial Electronics, Orlando, 2009. 1909–1913
- 11 Avasare M G, Kelkar V V. Image encryption using chaos theory. In: Proceedings of International Conference on Communication, Information & Computing Technology (ICCICT), Mumbai, 2015. 1–6
- 12 Veenus P K, Sivasankar K, Vivek P K, et al. The implementation of chaotic encryption scheme for images. In: Proceedings of International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Thuckalay, 2015. 588–592
- 13 Liu Q, Wang G J, Wu J. An efficient privacy preserving keyword search scheme in cloud computing. In: Proceedings of the International Conference on Computational Science and Engineering, Baton Rouge, 2009. 715–720
- 14 Boneh D, Crescenzo G D, Ostrovsky R, et al. Public key encryption with keyword search. In: Advances in Cryptology—EUROCRYPT 2004. Berlin: Springer, 2004. 506–522
- 15 Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. In: Proceedings of the ACM Workshop on Cloud Computing Security, Chicago, 2009. 55–66
- 16 Huang D M, Geng X, Wei L F, et al. Secure retrieval scheme for remote sensing image based on Henon mapping. J Softw, 2016, 27: 1729–1740 [黄冬梅, 耿霞, 魏立斐, 等. 基于 Henon 映射的加密遥感图像的检索方案. 软件学报, 2016, 27: 1729–1740]
- 17 Zhou J C, Dai R W, Xiao B H. Review on image quality assessment. Comput Sci, 2008, 35: 1–4 [周景超, 戴汝为, 肖柏华. 图像质量评价研究综述. 计算机科学, 2008, 35: 1–4]

Privacy-preserving encrypted image fusion algorithm for remote sensing

Meng SHEN^{1,2}, Guohua CHENG¹ & Liehuang ZHU^{1,2*}

1. School of Computer Science, Beijing Institute of Technology, Beijing 100081, China;

2. Beijing Engineering Research Center of High Volume Language Information Processing and Cloud Computing Applications, Beijing 100081, China

* Corresponding author. E-mail: liehuangz@bit.edu.cn

Abstract In the field of remote sensing, multi-spectral images and panchromatic images captured by satellites cannot meet the actual demand on imaging. Image fusion is usually performed to obtain a fused image with high spatial and spectral resolutions, which enables better recognition and positioning of objects. As the image fusion algorithm requires extremely high computing power and storage, public clouds such as Ali cloud appear as promising platforms for image fusion. This paper proposes SecureFusion, a novel privacy-preserving algorithm for image fusion on public clouds. In this algorithm, the multi-spectral image and the panchromatic image are encrypted first. Next, these encrypted images are fused by using the principal component analysis (PCA) method to obtain the encrypted fusion image. Finally, the real fusion image is obtained by decrypting the encrypted fusion image. Experimental results show that compared with the existing algorithms, the proposed privacy-preserving image fusion algorithm can achieve the same quality of the fused image, which increases the entire execution time by 25.9% on average. To the best of our knowledge, this is the first privacy-preserving algorithm for image fusion.

Keywords remote sensing image, privacy protection, image fusion, principal components analysis, image processing, encryption

Meng SHEN was born in 1988. He received his Ph.D. degree in computer science from Tsinghua University, Beijing, China, in 2014. Presently, he is an assistant professor in the Department of Computer Science at the Beijing Institute of Technology. His research interests include virtual resource management and privacy preserving algorithms in cloud computing.

Guohua CHENG was born in 1994. She is a graduate student in the Department of Computer Science at the Beijing Institute of Technology. Her research interests include image fusion and privacy preserving algorithms.

Liehuang ZHU was born in 1976. He is a professor in the Department of Computer Science at the Beijing Institute of Technology. His research interests include cryptography, network and information security.