文章编号:1671-4598(2016)04-0195-04 DOI:10.16526/j.cnki.11—4762/tp.2016.04.057 中图分类号:TP309 文献标识码:A

适用于字符串加密的全同态加密方案

梅 宇,孙霓刚,李雪佳
(常州大学 信息科学与工程学院,江苏 常州 213000)

摘要:现有的全同态加密思想主要实现对整数进行加密,在密文的状态下可以实现加、减、乘、除等四则运算,将其密文进行解密得到的结果与对明文做相同运算的结果一致,然而当加密对象为字符串的时候这些运算将变的毫无意义;为了使得全同态加密算法可以应用在字符串中,设计了一个可以适用于字符串加密的全同态加密算法;首先介绍了全同态加密算法在整数上的实现原理,通过对中国剩余定理的证明过程中发现了中国剩余定理具备定位字符的能力,然后将中国剩余定理引入整数上全同态加密的思想中;引入的中国剩余定理便是可以在加密过程中实现字符串的定位,避免出现加密完成后无法按照原有顺序回复出原文;最后通过举例论证的方式,验证了实现字符串全同态加密算法的的正确性;从而丰富了全同态加密算法的使用范围。

关键词:中国剩余定理;全同态加密;字符串

Fully Homomorphic Encryption Scheme Applied to String Computer Engineering

Mei Yu, Sun Nicang, Li Xuejia
(School of Information Science & Engineering, Changzhou University, Changzhou 213000, China)

Abstract: Existing full state encryption thought is mainly encrypted integers. Under the secret state, it can conduct add, subtract, multiply, divide and other operations. The results of private texts decryptions are consistent with the results of plain text. However, when the encrypted object becomes the string, these operations will become meaningless. In order to make full state encryption algorithm can be used in the string, the design applies to a whole string of state encryption algorithm. Firstly it introduced full state encryption algorithm theory on integers. During the prove process of Chinese Remainder Theorem, it could be found that Chinese Remainder Theorem has ability to locate character and then introduced Chinese remainder theorem into integer full state encryption thoughts. Introduced Chinese remainder theorem can locate strings in the encryption process and avoid the problem that after the completion of encryption, it could not return to original text based on original order. Finally, by way of example argument, it proved the correctness of string full text encryption algorithm. Thus the application range of full text encryption algorithm could be enriched.

Keywords: Chinese remainder theorem; fully homomorphic encryption; character string

0 引言

全同态加密思想是由 Rivest 等人在 1978 年提出的,希望在不对密文进行解密的条件下,对密文进行任何运算,得到的结果解密后与明文进行相应运算的结果相同。这个思想提出后,国内外研究人员进行了大量的研究,直到 2009 年 Gentry 提出来基于理想格的全同态加密方案,并对该方案进行了详细论述。此后国内外学者都提出来许多改进的全同态加密方案。但这些方案的加密对象都是对整数进行加密。当加密对象为“字符串”的时候,现有的算法将毫无办法。

在“大数据时代”,数据信息越来越中重要。数据的存储方式最常见的便是以字符串的形式进行存储。因此设计出一种可以适用于字符串的全同态加密算法,不仅可以扩展当前全同态加密算法的应用范围,还可以使得全同态加密更加具备实用性。通过对中国剩余定理的研究发现,中国剩余定理具备了对字符串进行定位的功能,这一功能很好地解决了同态加密在对字符串加密时候,出现乱序的现象。因此在文章中通过中国剩余定理对字符串进行相应的处理,然后通过同态加密算法对其进行处理。最终得到理想的结果。

收稿日期:2015-10-20; 修回日期:2015-11-12。
基金项目:国家自然科学基金(61103172)。
作者简介:梅 宇(1989-),男,硕士研究生,主要从事信息安全,密码学方向的研究。

1 全同态加密

全同态加密用一句话来说就是:可以对加密数据做任意功能的运算,运算的结果解密后是相应于对明文做同样的运算结果。同态加密有点穿越的意思,从密文空间穿越到明文空间,但穿越的时候是要被蒙上眼睛的。

Gentry[4-5] 构造同态加密的思想包括 4 个部分:密钥生成算法、解密算法、加密算法和评估算法。所谓的全同态加密包括两种基本的同态类型:加法同态和乘法同态。

1.1 全同态加密原理

定义一下符号,E:加密算法,m:明文,e:加密结果,f:针对明文的计算操作。

原理 $e=E(m)$,$m=E'(e)$。针对 E 构造 F 使得 $F(e)=E(f(m))$,因此 E 就是对于 f 的同态加密算法。而全同态就是指,给出任意的 f,都可以构造出相应的 F。全同态的目的在于找到一个可以在密文数据上进行任意次数的加密算法,是对密文数据进行某种操作的结果等于对明文做相应操作的结果。

1.2 全同态加密算法实现

为了简便,在本文中使用了 Gentry 所提出的对称全同态

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

加密算法[6]。

KeyGen（λ）根据安全参数 λ 产生 ηbit 的奇数 p 作为算法的私钥。

Encrypt（sk，m）对于明文 $m=\{0,1\}$，计算密 $c=m+2r+pq$ 其中 r 为随机选取 ρbit 的整数，q 是一个很大的整数。

Decrypt（sk，c）计算 $m=(c \bmod p) \bmod 2$，恢复明文。

$c \bmod p$ 的值称为噪声。如果 $m+2r<p/2$，则 $c \bmod p=m+2r$，因此 $(c \bmod p) \bmod 2=(m+2r) \bmod 2=m$。通过上述分析可知，要保证解密结果的正确性：$m+2r<p/2$。

1.3 同态性验证

假设两组明文 m_1，m_2 分别对其加密：$c_1=m_1+2r_1+pq_1$，$c_2=m_2+2r_2+pq_2$；则

$c_1+c_2=(m_1+2r_1+pq_1)+(m_2+2r_2+pq_2)=(m_1+m_2)+2(r_1+r_2)+p(q_1+q_2)$；

$c_1 * c_2=(m_1+2r_1+pq_1) * (m_2+2r_2+pq_2)=m_1m_2+2(2r_1r2+r_1m_1+r_2m_2)+p[pq_1q_2+q_2(m_1+2r_1)+q_1(m_2+2r_2)]$；

当 $(m_1+m_2)+2(r_1+r_2)<p/2$ 时，$((c_1+c_2) \bmod p) \bmod 2=[(m_1+m_2)+2(r_1+r_2)] \bmod 2=m_1+m_2$，当 $m_1m_2+2(2r_1r_2+r_1m_2+r_2m_1)<p/2$ 时，$((c_1 * c_2) \bmod p) \bmod 2=[m_1m_2+2(2r_1r_2+r_1m_2+r_2m_1)] \bmod 2=m_1m_2$

综上所述，上面的方案满足加法同态与乘法同态，但是方案存在噪声，随着密文的运算次数的增加，噪声也会随之增长，当噪声大于 $p/2$ 时，上述等式便不成立。加法运算得到的噪声等于各自噪声之和，乘法运算得到的噪声等于各自噪声之积。对于如何降低噪声，使之实现任意处运算不在本文的讨论范围内。

2 中国剩余定理

2.1 公式

用现代语言来来描述，中国剩余定理给出了以下一元线性同余方程组[7]：

$$(s):\begin{cases} x \equiv a_1(mod m_1) \\ x \equiv a_2(mod m_2) \\ \quad \cdots \\ x \equiv a_n(mod m_n) \end{cases}$$

有解的判定条件，并用构造法给出了在有解的情况下解的具体形式：

中国剩余定理说明[8-9]，假设整数 m_1，$m_2 \cdots m_n$ 两两互质，对于任意的整数 $a1$，$a2 \cdots an$ 方程组（s）有解，并且通解可以通过以下构造：

设 $M=m_1 * m_2 * \ldots * m_n=\prod_{i=1}^{n} m_i$ 是整数 m_1，$m_2 \cdots m_n$ 的乘积，并设 $Mi=M/mi$ $i \in (1,2 \cdots n)$ 是除了 mi 以外的 $n-1$ 个整数的乘积。设 $t_i=M_i^{-1}$ 为 Mi 模 mi 的数论倒数 $t_iM_i \equiv 1(mod m_i)$ $\forall i \in \{1,2 \ldots n\}$ 的方程组（s）的通解：$x=a_1t_1M_1+a_2t_2M_2+\cdots+a_nt_nM_n+kM=kM+\sum_{i=1}^{n} a_it_iM_i$ $k \in z$；在模 M 的意义下，方程组（s）只有一个解：$x=\sum_{i=1}^{n} a_it_iM_i$。

3 字符串数据的同态加密算法

3.1 算法描述

与整数的同态加密不同，整数加密后能够实现对密文的加、减、乘、除运算对字符串是毫无意义。了实现字符串的同态加密，通过利用中国剩余定理将字符串转换，然后利用同态算法进行加密处理。具体步骤如下：

（1）假设一个字符串 B，截取该字符串中的每一个字符并将其转换为对于的 ASCII 码，将其对应的 ASCII 码分别记为 b_1，b_2，…，b_k。（其中 k 为字符串中字符的个数）。

（2）由中国剩余定理中的要求，选取 k 个两两互为指数的正整数，分别记为：m_1，m_2，…，m_k 其中（$m_i>121$）。

（3）有中国剩余定理的同余式组：

$$\begin{cases} x \equiv b_1(mod m_1) \\ x \equiv b_2(mod m_2) \\ \quad \cdots \\ x \equiv b_k(mod m_k) \end{cases}$$

（4）由中国剩余定理可知，该同余式组的通解为：$x=\sum_{i=1}^{n} a_it_iM_i(modM)$。

其中：$M=m_1 * m_2 * \cdots * m_k$，$M_i=M/m_i$（$i=1,2 \cdots, k$），$t_i=M_i-1$（$i=1,2,\cdots,k$）。$x$ 便是需要加密的数值。

（5）根据全同态加密算法解密后可以得到加密数据 x，根据公式 $b_i=x \bmod m_i$，可以复原每个字符串中字符多对应的 ASCII 码值。

3.2 算法正确性证明

3.2.1 字符串与加密数据的对应关系

从假设可知，对于任意的 $i \in \{1,2,\cdots,k\}$。由于 $\forall j \in \{1,2 \ldots k\}, j \neq i$，$\gcd(m_i,m_j)=1$。所以得出 $\gcd(m_i,M_i)=1$。

因此可以说明存在一个整数 t_i 可以使得 $b_it_iM_i \equiv 0(mod m_j)$，这样的 t_i 叫做 M_i 模 m_i 的数论倒数。由此可知[10]：

$b_it_iM_i \equiv b_i * 1 \equiv b_i(mod m_i)$

$\forall j \in \{1,2 \ldots n\}, j \neq i, b_it_iM_i \equiv 0(mod m_j)$。因此 $x=b_1t_1M_1+b_2t_2M_2+\cdots+b_kt_kM_k$ 满足以下等式：

$$x=b_it_iM_i+\sum_{i \neq j} b_jt_jM_j \equiv b_i+\sum_{i \neq j} 0 \equiv b_i(mod m_i)$$

说明 x 为上述方程组（s）的一个解。

此外，假设 x_1，x_2 都是方程组（s）的解，对于任意的 $i \in \{1,2,\cdots,k\}$，$x_1-x_2 \equiv 0(mod m_i)$，由条件可知 $m1$，$m2$，…，mk 是互为质数的，得到 $M=m1 * m2 * \cdots * mk$ 是整除 $x1-x2$。应此上述方程组（s）的任意两个解之间必然相差 M 的整数倍数。而另一方面，

$$x=b_1t_1M_1+b_2t_2M_2+\cdots+b_kt_kM_k$$

是方程组的一个解，应此我们可以得到方程组解所有的形式：

$$b_1t_1M_1+b_2t_2M_2+\cdots+b_kt_kM_k+kM=kM+\sum_{i=1}^{k} b_it_iM_i(k \in z)$$

所以可以得到方程组的解的集合：

$$\{kM+\sum_{i=1}^{k} b_it_iM_i\}(k \in z)$$

模 M 的意义下：其结果为

$$\sum_{i=1}^{k} b_it_iM_i(modM)$$

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

至此，通过文中分析得到了方程组的解 $x=\sum_{i=1}^{k}b_it_iM_i$，将其展开：

$$x=b_1t_1M_1+b_2t_2M_2+\ldots+b_kt_kM_k$$

根据设计的算法第五步计算：$b_i=x \bmod m_i$。即 $b_1=x \bmod m_1$，…，$b_k=x \bmod m_k$。分析如下：

$$b_1=x\bmod m_1=(b_1t_1M_1+b_2t_2M_2+\cdots+b_kt_kM_k)\bmod m_i=(b_1t_1M_1)\bmod m1+(b_2t_2M_2)\bmod m_2+\cdots+(b_kt_kM_k)\bmod m_k$$

因为 $M_i=M/m_i=(m_1*m_2*\cdots*m_k)/m_i$，由此公式可知，$M_i$ 不是 m_i 的整数倍，即 M_i/m_i 有余数，而 $M_{i\neq i}/m_i$ 没有余数。因此 $b_1=x \bmod m_1=(b_1t_1M_1+b_2t_2M_2+\cdots+b_kt_kM_k)\bmod m_i=(b_1t_1M_1)\bmod m_1+(b_2t_2M_2)\bmod m_2+\cdots+(b_kt_kM_k)\bmod m_k=(b_1t_1M_1)\bmod m_1=b_1t_1M_1$。又因为，$t_i$ 与 M_i 模 m_i 的数论倒数，所以 $t_iM_i=1(\bmod m_i)$

所以得到 $b_1=b_1$，同理可知，$b_2=b_2$，$b_3=b_3$，…，$b_k=b_k$。

综上所述，证明了本文提出的利用字符串和加密数值之间的对应关系，在下面的一节中对加密方案的可行性进行分析。

3.2.2　对所得方程组解进行同态加密

根据上文提出的字符串同态加密算法的结果，得到了需要加密的 x 的整数值，将整数 x 转化为二进制，通过 2.2 节中提出的同态加密算法，对其结果进行加密。（注：文中的同态加密算法一次只能加密 1 bit，效率比较慢。在全同态加密算发相关的文章中，通过各种改进方法一次可以加密多 bit。在本文中，为了简化描述，选取了一次加密 1 bit 的同态加密算法）。因此，可以说明上述同余方程组的解是可以利用同态加密算法的。因此本文提出的方案具有正确性。

方案的安全性是基于近似最大公约数问题，下面给出近似最大公约数问题的定义：

定义：近似最大公约数问题（approximate-GCD problem）。随机选择 n 个大整数 p 的近似倍数 a_1，a_2，a_3，…，a_n，根据 a_1，a_2，a_3，…，a_n，求出 p 的过程就称为近似最大公约数问题。

3.2.3　举例论证

给定一个字符串 AB，则 A 的 ASCII 码值为：$b_1=41$，B 的 ASCII 码值为：$b_2=42$；随机取两个互为质数的 $m_1=122$，$m_2=123$。由中国剩余定理得出同余方程组：

$$\begin{cases}x=b_1(\bmod m_1)\\x=b_2(\bmod m_2)\end{cases}=\begin{cases}x=41(\bmod 122)\\x=42(\bmod 123)\end{cases}$$

$M=m_1*m_2=122*123=15\ 006$；则 $M_1=M/m_1=123$，$M_2=M/m_2=122$；由 $t_iM_i\equiv 1(\bmod m_i)$ 可知：$t_1M_1\equiv 1(\bmod m_1)$ 可推出 $t_1=1$，$t_2M_2\equiv 1(\bmod m_2)$ 推出 $t_2=122$。根据上述中国剩余定理的通解公式：

$$x=\sum_{i=1}^{k}b_it_iM_i(\bmod M)=[b_1t_1M_1+b_2t_2M_2](\bmod M)=(41*1*123+42*122*122)\bmod 15\ 006=14\ 925$$

将 x 转换为二进制为 11 1010 0100 1101。将该二进制从左到右依次即为：C_{13}，C_{12}，C_{11}，…，C_0。对每一位进行文中提到的同态加密算法进行加密，在这里只选取 C_0，C_1 作为代表。

选取特定的数值，设 $p=11$，$q=5$，$C_0=m_0=1$，$C_1=m_1=0$，随机选去 $r_1=1$，则有以下等式成立：

$C_0=Enc(m_0)=m_0+2r_1+pq=1+2*1+11*5=58$；

$C_0(\bmod p)=58 \bmod 11=3$；

$m_0'=3 \bmod 2=1$；

$C_1=Enc(m_1)=m_1+2r_1+pq=0+2*1+11*5=57$；

$C_1(\bmod p)=57 \bmod 11=2$；

$m_1'=2 \bmod 2=0$；

…

所以对二进制数据加密的结果为：……..57，58 解密后的结果：11 1010 0100 1101，恢复为十进制为 14925。根据 $bi=x \bmod mi$ 恢复出原来字符串所对应的 ASCII 码值。

$b_1=x \bmod m_1=14925 \bmod 122=41$，对应的字符是 A；

$b_2=x \bmod m_2=14925 \bmod 123=42$，对应的字符是 B；

因此，对字符串加密进行了复原，但这只是对单个字符串进行加密的，当然也可以对字符串进行运算如 A+B 和 A*B 等运算，运算的步骤和单个字符串的步骤相同，通过类型的方法即可恢复，由于篇幅问题，在本文中就不作展开论述。只是我们要注意同态加密的条件：噪声要小于 p/2，必须是在选取参数的时候注意。

3.2.4　实验结果与分析

上一个小节中对适用于字符串的全同态加密算法的正确性进行验证。通过对字符串“AB”代入文中所设计的算法，通过了转化、加密、解密等步骤最终完整的恢复出了字符串“AB”，没有打破原文字符串的顺序，实验的结果与预期所设计的一样。证明了文中所提出的适用于字符串的全同态加密的正确性。在实验过程对选取字符串“AB”将其转化为 ASCII 码，然后通过中国剩余定理将字符串所对应的 ASCII 码，转化成一个整数 X，最后通过对 X 使用同态加密算法，得到密文 Y。在解密阶段，根据算法提出的公式进行解密，这样便可以得到了字符串“AB”所对应的 ASCII 码，便于恢复出相应的字符串。

通过对整个实验结果和过程进行分析，虽然实验的结果是正确时。但是在算法的加密阶段，对二进制数据的加密是按照一位一位进行加密的，这样的效率肯定不高。为了提高算法的加密的效率，有一个改进的思想，在全同态加密算法实现的时候，加密公式为：$c=m+2r+pq$。将其修改为 $c=m+4r+pq$。同时对解密公式进行修改为 $=(c \bmod p) \bmod 4$。这样可以对二进制数据每次可以加密两位数据，在一定的程度上提高了加密的效率。对相应算法的改进，还需考虑到算法参数的选取、算法噪声的分析等多个方面，同时也为以后的研究提供了方向。

4　结束语

本文所提出的利用中国剩余定理实现字符串的同态加密算法，在具体的实现过程中还是会存在一些问题，比如：素数的选取和存储等问题以及 x 值过大的问题，都对同态加密算法的效率产生比较大的影响。但在安全性方面，它还是保留了整数同态加密特点。

全同态加密技术是一种能对密文数据进行数学运算的加密机制，在数据库加密和云服务中有比较广泛的应用。本文提出的方案，实现对字符串进行加密，丰富了同态加密的应用范围，在同态加密的原理上对其进行扩展，并验证了算法的正确

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

性。但还存在一些不足之处，是以后所研究的重点。

参考文献：

[1] Riverst R，Shamir A，Dertouzos M. On data banks privacy homomorphisms [J]. Foundations of Secure Computation，1978，7 (1)：169-177.

[2] 石中盘，蔡萃燕. 面向数据库加密的秘密同态算法的研究 [J]. 计算机应用研究，2009，26 (4)：1535-1537.

[3] 陈智罡，王 箭. 全同态加密研究 [J]. 计算机应用研究，2014，31 (6)：1624-1631.

[4] Gentr Y. Fully homomorphic encryption using ideal lattices [A]. Proc of the 41st Annual ACM symposium on Theory of Compting [C]. NewYork：ACM Press，2009：169-178.

[5] Boneh D，Gentr，Ygentr Y. A fully homomorphic encryption scheme [D]. Stanford：Stanford University，2009.

[6] 林如磊，王 箭，等. 整数上全同态加密方案的改进 [J]. 计算机应用研究，2013，30 (5)：1515-1519.

[7] 杨坤伟，李吉亮，等. 中国剩余定理在密码学中的研究 [J]. 计算机技术与发展，2014，24 (1)：238-241.

[8] 陈代梅，范希辉，等. 基于同余方程和中国剩余定理的混淆算法 [J]. 计算机应用研究. 2015，32 (1)：1588-1592.

[9] 杨 波. 现代密码学 [M]. 北京：清华大学出版社，2003.

[10] 陈泽文，张龙军，王育民. 一种基于中国剩余定理的群签名方案 [J]. 电子学报，2004，32 (7)：1062-1065.

(上接第 194 页)

移速度与所选取的 8 点所在列的积分方向的夹角都不大于 $e1+e2$；如果沿这个方向正好有像元，则能得到以下等式：

$$\tan(e1+e2)\times(x_G-x_O)=x\cdot a \tag{4}$$

另外还要考虑到 CCD 芯片在安装时有一定的安装误差 μ，因此需要对上式进行修正如下：

$$\tan(e1+e2)\times(x_G-x_O)+\mu=x\cdot a \tag{5}$$

在公式 (5) 中，$e1$、$e2$ 根据误差分析得出，x_G、x_O 为像面位置，μ 为安装误差，根据安装精度确定。从而可以计算的出重叠像元数 x。

3 实验结果与分析

某相机像面由五块 TDICCD 拼接而成，每片 CCD 的总像元数为 4 096，通过 TDICCD 拼接使拍摄的行像元数大于 20 000个，对应地面覆盖宽度大于 10 km。调制传递函数值下降 5%对成像质量无本质影响，根据公式 (3) 计算得出在 96 级积分级数下允许的偏流角误差不大于 12′，由此确定偏流角的总误差 $e2$。由于偏流机构的约束，侧摆角最大为 15°时像面上各点与中心偏流角最大误差不超过 1′。根据测量获得 x_G 为 108.735 mm，x_O 为 73.535 mm，CCD 安装误差 μ 为 0.002 mm，CCD 像元尺寸为 0.008 75 mm。将以上数值代入公式 (5) 进行求解得出重叠像元数 $x=15.441\ 3$。

像元重叠数应该为不小于 x 的整数，因此像元重叠数应大于 15。

根据以上分析计算，在进行像面拼接时，相邻两片 CCD 之间的重叠像元数应大于 15，在实际的设计中，考虑到偏流角误差 12′有可能在相机工作过程中增大，在计算出的重叠像元数上加入一倍的余量；再考虑到结构的误差在拍摄过程中有可能变化，再加入 8 个像元的余量，这样也给 CCD 拼接带来了方便之处，降低了拼接难度，因此选取像元重叠数为 40。当选取 CCD 像元重叠数为 40 时，TDICCD 拼接后总的像元数为 20 320，对应的地面覆盖宽度为 10.16 km，满足拍摄的行像元数大于 20 000，地面覆盖宽度大于 10 km 的要求。

在轨道侧摆 14.66°时，相机拍摄的原始图像和拼接后的图像如图 5 所示。

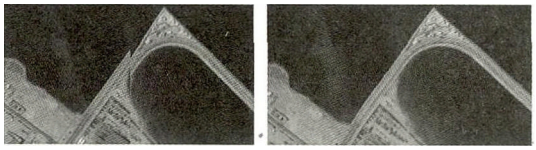

图 5 原始图像和拼接图像

图中左图为相邻两片 CCD 获得的原始图像数据，右图为拼接后的图像数据。图像匹配结果为重叠像元数为 25.58，与理论上计算基本一致。从而验证了计算方法的正确性。

4 结论

选取偏流角误差处于最大值时进行分析，且加入了 CCD 芯片安装的最大误差，计算出的重叠像元数是任意相邻两片 CCD 在拼接处像移速度与 TDICCD 列方向有最大的偏差时所需要重叠的像元个数为大于 15。在实际设计中考虑 CCD 座之间的相互位置及用于固定 CCD 座的螺钉孔位的影响，则搭接时交错的像元数要留有一定像元的余量，从而能够完全解决像面上相邻两片 CCD 拼接处有缝隙，拍摄后的图像信息不完整且不能正常拼接的问题。通过实例分析，由于每片 CCD 总像元数为 4 096，可以设定在 40 个像元，即占总像元数的 0.98%。地面覆盖宽度降低 80 m。通过 TDICCD 拼接使拍摄的行像元数为 20 320 个，对应地面覆盖宽度为 10.16 km，满足地面覆盖宽度大于 10 km 的要求。对空间相机像面 CCD 拼接重叠像元数进行计算为空间相机像面机械拼接及相机整体能否满足指标要求提供设计依据。

参考文献：

[1] 李伟雄，闫得杰，徐抒岩，等. 空间相机地心距误差修正 [J]. 光学 精密工程，2012，20 (5)：1126-1133.

[2] 武星星，刘金国. 应用地球椭球的三线阵立体测绘相机像移补偿 [J]. 光学精密工程，2011，19 (8)：1794-1800.

[3] 张树青，丁亚林，李友一，等. 斜视步进画幅遥感相机像移补偿方法研究 [J]. 红外与激光工程，2008，37 (3)：501-505.

[4] 张凤英，刘文怡，杨 慧，等. 远程遥测姿态控制系统设计 [J]. 计算机测量与控制，2015，23 (1)：102-105.

[5] 闫得杰，韩诚山，李伟雄. 飞行器侧摆和前后摆及控制误差的优化设计 [J]. 光学精密工程，2009，17 (9)：2224-2229.

[6] 杨秀彬，金 光，张 刘，等. 卫星后摆补偿地速研究及成像仿真分析 [J]. 宇航学报，2010，31 (3)：912-917.

[7] 翟林培，刘 明，修吉宏. 考虑飞机姿态角时倾斜航空相机像移速度计算 [J]. 光学精密工程，2006，14 (3)：490-494.

[8] 樊 超，李英才，易红伟. 偏流角对 TDI CCD 相机像质的影响分析 [J]. 光电工程，2007，34 (9)：70-73.

[9] 李伟雄，徐抒岩，闫得杰. 影响空间相机偏流角估值误差的参数 [J]. 红外与激光工程，2011，40 (8)：1530-1536.

[10] 闫得杰，徐抒岩，韩诚山. 飞行器姿态对空间相机像移补偿的影响 [J]. 光学精密工程，2008，16 (11)：2199-2203.

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net