桂林電子科技大學
GUILIN UNIVERSITY OF ELECTRONIC TECHNOLOGY

本科毕业设计（论文）外文翻译

（译文）

学　　号	：	1800710238
姓　　名	：	王智坚
学　　院	：	数学与计算科学
专　　业	：	信息与计算科学
指 导 教 师	：	张必山
指导教师职称	：	副教授

2022 年 5 月 16 日

各种全同态加密技术的分析与比较

Pratibha Chaudhary Amity University Uttar Pradesh
pratibha.chaudhary4991@gmail.com

Ritu Gupta Amity University Uttar Pradesh
ritu4006@gmail.com

Abhilasha Singh Amity University Uttar Pradesh

abhilashasingh28@gmail.com

Pramathesh Majumder Amity University Uttar Pradesh

pramathesh@outlook.com

摘　要

可以对加密形式的数据进行计算——这是同态加密的本质. 同态加密解决了在第三方系统（例如云或不受信任的计算机、服务提供商等）上存储数据的安全问题. 最重要的同态加密类别是完全同态加密. 它允许对加密形式的数据进行无限数量的操作，并且系统输出在密文空间内. 本文提供了同态加密的基本原理及其各种分类，即部分同态加密、部分同态加密和完全同态加密. 主要强调全同态加密，研究利用理想格的硬度、整数、误差学习、椭圆曲线密码学等不同的全同态加密方案.

关键词：同态加密(HE); 部分同态加密(PHE); 有点同态加密(SWHE);全同态加密(FHE); 第三方椭圆曲线加密(ECC).

1　引言

在 IT 领域，数据通常在第三方（云或不受信任的计算机、服务提供商等）上存储和处理.因此，出现了两个主要问题.首先，传统加密方案不提供第三方数据的安全性（即存储未加密的数据）.第三方可能会滥用数据.其次，要对加密数据执行任何类型的操作，首先要对其进行解密.这些担忧可能导致发现同态加密，该加密允许以加密形式对存储在第三方的数据执行计算，而无需对其进行解密. 1978 年出现了对加密数据进行计算的想法，称为隐私同态[1].同年 1978 年，他们还引入了 RSA.RSA [1]是非对称加密方案，即具有用于加密的公开密钥（即公共）和用于解密的机密密钥（即秘密），只有授权用户知道.RSA 只允许对加密数据进行乘法运算.允许对加密数据进行加法和乘法无界操作的同态加密方案称为完全同态加密方案.全同态加密方案（FHE）是一个开放的问题.许多研

究人员提出了他们的方案，即 El-Gamal 方案[2]但适用于乘法运算，Paillier 方案[3]但适用于加法运算等.

第一个完全同态加密方案来自 Gentry[4]给出了某种同态加密方案，这是一个值得注意的飞跃. 这是基于硬度理想晶格[5].

同态加密有许多有用的应用程序.例如，Paillier 受雇于在线投票系统和阈值方案 [6]，RSA 用于安全的互联网、银行和信用卡交易[6]，El-Gamal 用于混合系统，也用于安全系统多方计算[6]等

2　调查

在本文中，我们将调查先前在与同态加密相关的密码学领域所做的研究. 研究和分析各种同态加密方案. 提供对称为完全同态加密的同态加密的最佳类别及其各种类别的见解.同态加密概念取自抽象代数.考虑明文 $y_1, y_2, \cdots, y_n$ 和加密方案 E，如果它如下：

A. **可加性：**

$$\begin{aligned}&(y_1 + y_2 + y_3 + \cdots + y_n)\\&= y_1 + E(y_2) + E(y_3) + \cdots + E(y_n)\end{aligned} \tag{1}$$

B. **乘性性质：**

$$\begin{aligned}&(y_1 y_2 y_3 \cdots y_n)\\&= (y_1)E(y_2)E(y_3)\cdots E(y_n)\end{aligned} \tag{2}$$

那么它是同态的.

为了创建任何类型的同态加密方案，我们使用加法和乘法布尔电路（AND 和 XOR 门）的组合. 考虑非对称加密的同态加密方案分为如下四种算法：

$$H = (\text{生成密钥，加密，解密}) \tag{3}$$

所有这些算法的运行时间取决于安全参数 λ.

a).创建密钥算法：

它以安全参数 Ⅳ为输入，即密钥中的位数，并输出密钥 s 和公钥 p.

b).加密算法：

它以明文均 $y_1, y_2, \cdots, y_n$ 作为输入.它将明文分成位 $(0,1), b_1, b_2, \cdots, b_i$ 并输出密文 $c_1, c_2, \cdots, c_i$

$$c = Encrypt(p, b_i) \tag{4}$$

c).评估算法：

以p和函数fun作为输入，输出新的密文

$$c = Evaluate(p, fun, c_i) \tag{5}$$

d). 解密算法：

以密文$c_1, c_2, \cdots, c_i$和 s 为输入，输出明文$y_1, y_2, \cdots, y_i$

$$y_n = Decryp(s, c_i) \tag{6}$$

同态加密分为三类，如图 1 所示：

1. 部分同态加密（PHE）：

它允许加法或乘法运算，即只有一种任意数量的运算. 例如——未填充的 RSA、El-Gamal 等.

2.部分同态加密（SWHE）：

它允许加法和乘法运算，但运算次数是有限的. 例如 BGN [7] 等.

3.全同态加密（FHE）：

它允许任意数量的加法和乘法运算. 例如基于格的[5]、基于整数的[5]、基于错误的学习[14]等.

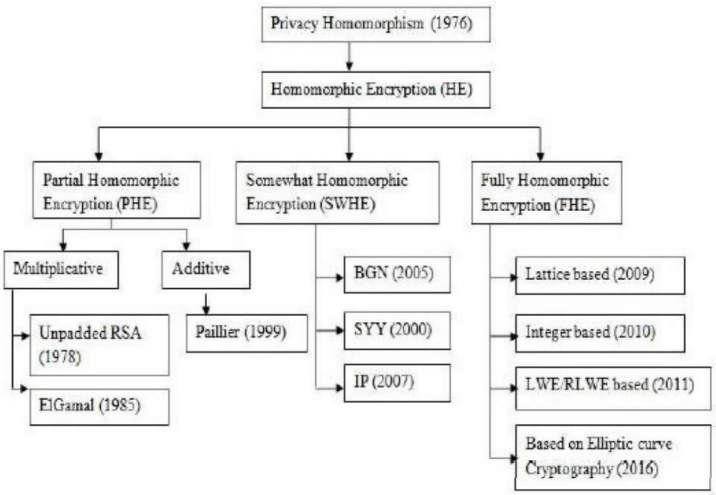

图 1 同态加密方案的分类

3 完全同态加密方案

全同态加密是一种对密文进行任意加密的密码体制. 它允许程序在支持加密系统的

任何类型的功能上运行.

A. 使用 Ideal Lattice (2009)形成的 FHE 方案

Bootstrappable 加密方案是使用理想格[5]创建的，因为：在典型的基于格的算法中，算法的解密电路复杂度比未填充的 RSA 或 ElGamal 等方案要低得多.同态的加法和乘法性质是由理想格所提供的.

包括三个步骤：

构造某种同态加密：构造一种求低阶多项式的方法数量有限的 ADD 和 MULT 操作.A 密文是一种形式

$$c = u + n \tag{7}$$

当u是理想格[5]中的向量，n是一个带有明文m的“误差”或“偏移”或“噪声”向量时，误差分量随着每个同态运算的应用而增加，达到一个不可避免的值，在某一点上不再允许密文解密.

压缩：压缩是用来减少深度解密电路，因为它增加到更高的值.SWHE 方案解密电路工作良好，具有较小的深度.

引导：引导是为了减少噪音而对密文进行加密.如果一个同态加密方案能够评估自己(增广)解密电路，那么它就是可引导的.

B. 不使用引导的完全同态加密：

2010 年，Gentry et. al.提出了利用自举机制实现完全同态加密的思想.这允许对原始数据使用任意数量的加法，但只需一次乘法.

2013 年，Wei et. al.提出了允许任意数目的加法和多重乘法的思想.

基于对称学习的全同态加密方案：

然后，提出了基于对称学习机制的全同态加密方案，该方案主要基于机器学习技术来学习加密模式.该方法避免了自举和机器学习方法的使用，它使用了维数约简机制，从而缩短了原始文本，减少了解密机制的复杂性，不影响附加的假设.

环全同态加密方案：

在此基础上，提出了一种新的 FHE 加密方案--RFHE(环型全同态加密)，该方案不使用降噪机制，而是在降噪过程中加入一个非八元环.之后，刘氏提出了对称满同态加密方案，该方案依赖于非交换域，该方案排除了自举的可能性，并允许对原始数据进行更多的加法和乘法.它不使用噪音教育，而是依赖于类似的 GCD 机制.

C. 完全同态加密方案的实现

为了实现完全同态加密，Gentry 和 Halevi[8]使用了类似于 Smart and vercateren[9]的变体.Smart 和 Vercauteren 在将某些同态加密转换为完全同态加密时，无法实现引导功

能.优化包括自举功能；加密等方面的批处理技术，以实现完全同态定义.在某种程度上同态加密中，密钥生成不需要完全多项式反转[8].

表 1 晶格尺寸和维度中的设置

格子尺寸	尺寸设置（尺寸）
玩具	$512=2^9$
小	$2048=2^{11}$
中	$8192=2^{13}$
大	$32768=2^{15}$

上面的表 1 显示了在实现 FHE 时考虑了几个维度的格点.

表 2 公钥大小范围

格子尺寸	公钥大小	一个引导操作运行时
小	70Mb	30m
大	2.3Gb	30m

上面的表 2 显示了用于小和大格维的公钥大小范围和一个引导操作运行时，并考虑了 1-CPU 64 位机器的一个启动操作运行时，具有较大的[8].

D. **利用整数形成的 FHE 格式**（2010）

Van Dijk 等人[10]提出了使用 Gentry 构造[5]的完全同态加密方案，但定义在整数上而不是理想格上，因为它们在概念上更简单，可以证明使用“基本”技术.Howgrave Graham 分析了近似整数最大公约数（近似 imate GCD）问题[11]的方案使用度.

一般建筑：

创建密钥算法：奇数整数键 $k \in [2n-1, 2n)$.

加密算法 (k, x)：用于加密 $X \in \{0,1\}$，集合密文是一个整数值，其残数 mod p 与明文具有相似的齐次性，类似于 $c = kq + 2r + x$，其中整数 q, r 在绝对值小于 $k/2$ 的情况下随机选取.

解密算法 (k, c)： x=输出(Cmod K)mod 2.

约束：$x + 2r < k/2$并选择 r：$r \approx 2\sqrt{n}$和$q \approx 2n^3$

加法上的同态：

$(x_1) + E(x_1) = x_1 + 2r_1 + kq_1 + x_2 + 2r_2 + kq_2$

$Nois = (x_1 + x_2) + 2(r_1 + r_2)$ ，，其生长线性如图 2(a)所示.

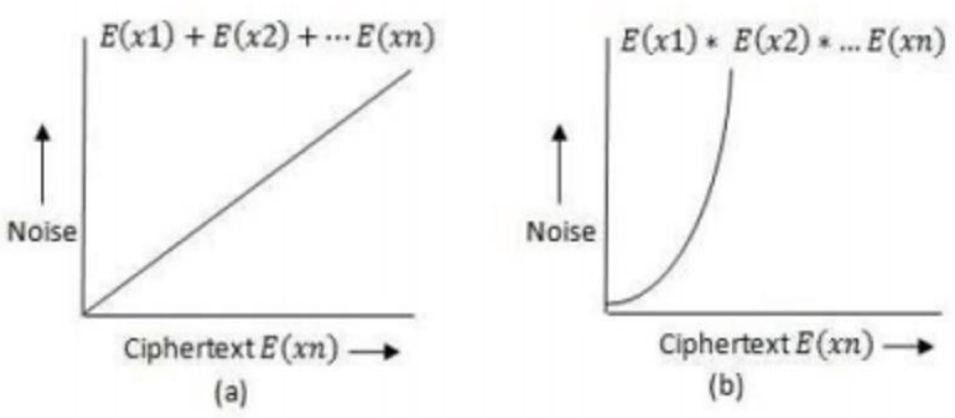

图 2 加密噪声扩展

乘法上的同态：

$$\begin{aligned}&(x_1)E(x_2)\\&=(x_1+2r_1+kq_1)(x_2+2r_2+kq_2)\\&=x_1x_2+2(x_1r_2+x_2r_1+2r_1r_2)+(kq_1q_2+3q_1r_2+x_1q_2+x_2q_1)\end{aligned}\tag{9}$$

如图 2(b)所示， $Nois=x_1x_2+2(x_1r_2+x_2r_1+2x_1)$ ，呈指数增长.

这是一个对称格式，但很容易转化为非对称格式.公钥是使用“零加密”(特别是整数)形成的.

$$p=kq_i+2r_i\tag{10}$$

在上面描述的 q_i,r_i 是私钥，加密解密用于解密密文.由于这里存在不有效的算法，为了在多项式时间内从给定的 pis 中恢复 k ，因此该方案被认为是安全的.

E. FHE 计划使我们在错误中学习(2011)

带误差学习(LWE)是文[12]所提到的偶数后量子算法在实际时间内最难解决的问题之一.Regev 首次提出了“从错误中学习”问题[13]，它将格问题的最坏情况下的硬度降低为带误差的学习问题(LWE)[14].Brakerski 和 Vaik Untanathan 提出了用环学习与误差(RLWE)相结合的化学方法[14].RLWE 采用多项 LWE(PLWE).为了理解 RLWE 的假设，例如，在一个具有形式 (r_i,kr_i+y_i) 的环上取无同源样本，其中 k 是随机的“秘密环元素”，在环中是均匀随机的，而 I 是“小 P 环元素，窃听者不能区分随机对的.”这一系列样品中的环元素[14].这进一步归结为 SVP 的最坏情况.该方案也是利用 Gentry 的自举和压缩技术[5]从 Swhe 构造的.为了避免在该方案中压缩，以依赖 LWE[14]的“稀疏”版本为代价，将最坏的硬问题降到最坏的情况.压扁的交替是线性化的.再线性化减小了密文的大小.生成密钥所需的格基的非生成.RLWEScheme 是圆形的，这意味着它允许安全地加密它的自秘密密钥.环元素与 LWE 相比，RLWE 具有更高的效率，对于秘密密钥的线性函数而

言，RLWE 是循环安全的(与密钥相关的安全).

F. 使用椭圆曲线密码形成的 FHE（2016)

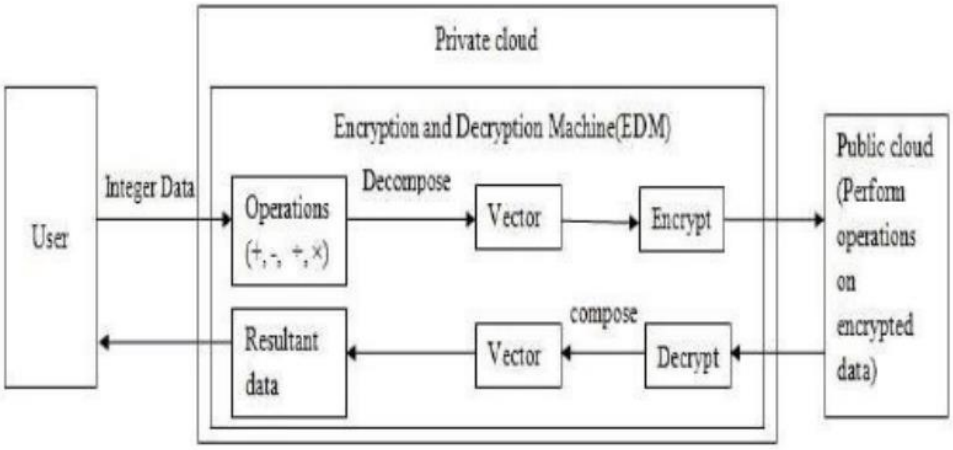

图 3 基于椭圆曲线密码学的同态加密

表 3 全同态加密方案的比较

财产	基于理想晶格	基于整数	环学习与错误	基于椭圆曲线密码学
年内推出	2019	2010	2011	2016
硬度	最近向量问题，稀疏子集和问题	近似 GCD 问题	环错误学习	关于已知基点的任意椭圆曲线分量的离散对数是不切实际的
安全	更多的	较少的	超过预期理想的	最多
易用	较少的	更多的	小于预期的	更多的
限制	公钥大小太大	降低安全性	不适用	不支持浮点计算
效率	高效的	效率最低的	比理想更高效基于格的	最有效率的

上面的图 3 显示了同态所涉及的步骤使用椭圆曲线密码学进行加密.用户想要要处理数据，首先它会进入私有云. 私人的云有加解密机(EDM) 负责加解密数据. 公共云执行计算以加密形式对数据进行操作并返回获得的结果返回到 EDM. EDM 将提供所需的结果数据返回给用户

4 增值结果

我们的目标是实现一个实际可行的无限制的 FHE 方案.FHE 方案的一个例子如下：

1.基于晶格的方案在 IBM 系统×3500 服务器[8]和 6Intel xeon2.4GHz 处理器[16]上使用语言 C++和 NTL 库实现.

2.基于整数的方案是在 SAGE 软件上实现的英特尔核心 i5,3.30 GHz x4,8 Gb RAM[17].

3.RLWE 是在 HELib 中使用 C-++语言和一个数学库 NTL[18]实现的.

4.利用基于 HE 的椭圆曲线密码学对 GPS 数据[14]进行了实证评估和测试.

通过对上述全同态加密方案进行深入研究和分析，进行了比较具有硬度、引入年份、方案安全性、效率等性能.比较的结果列于表 1 中.

5　结论

和未来工作同态加密存在于 30 年后仍是有待研究的问题.各种同态加密方案都有一定的改进范围.该改进可以在任何方面完成，如改进密钥的生成或加密、解密等.实现成本很高，同态加密方案的复杂性也很高.它在将来可以减少.本文对同态加密方案进行了分类，重点关注各种类型的 FHE.在实际应用中实现了基于格、整数、误差环学习和椭圆曲线密码学的 FHE 方案.上面提供了每个方法的示例.FHE 并不是在每个平台上都是实际实现的.上述 FHE 方案支持单个用户设置尽管应用程序从不同用户获取多个数据的[19].

参考文献

[1] Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. Foundations of secure computation, 4(11), 169-180.

[2] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), 469-472.

[3] Paillier, P. (1999, May). Public-key cryptosystems based on composite degree residuosity classes. In Eurocrypt (Vol. 99, pp. 223-238).

[4] Gentry, C. (2009). A fully homomorphic encryption scheme. Stanford University.

[5] Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In STOC (Vol. 9, No. 2009, pp. 169-178).

[6] Parmar, P. V., Padhar, S. B., Patel, S. N., Bhatt, N. I., & Jhaveri, R. H. (2014). Survey of various homomorphic encryption algorithms and schemes. International Journal of Computer Applications, 91(8).

[7] Boneh, D., Goh, E. J., & Nissim, K. (2005, February). Evaluating 2- DNF Formulas on Ciphertexts. In TCC (Vol. 3378, pp. 325-341).

[8] Gentry, C., & Halevi, S. (2011, May). Implementing Gentry's FullyHomomorphic Encryption Scheme. In EUROCRYPT (Vol. 6632, pp. 129-148).

[9] Smart, N. P., & Vercauteren, F. (2010, May). Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In Public Key Cryptography (Vol. 6056, pp. 420-443).

[10] Van Dijk, M., Gentry, C., Halevi, S., & Vaikuntanathan, V. (2010, May). Fully homomorphic encryption over the integers. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 24-43). Springer Berlin Heidelberg.

[11] Howgrave-Graham, N. (2001, March). Approximate integer common divisors. In CaLC (Vol. 1, pp. 51-66).

[12] Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2017). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. arXiv preprint arXiv:1704.03578.

[13] Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), 56(6), 34.

[14] Brakerski, Z., & Vaikuntanathan, V. (2011, August). Fully homomorphic encryption from ring-LWE and security for key dependent messages. In Annual cryptology conference (pp. 505-524). Springer, Berlin, Heidelberg.

[15] Hong, M. Q., Wang, P. Y., & Zhao, W. B. (2016, April). Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing. In Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on (pp. 152-157). IEEE.

[16] Smart, N. P., & Vercauteren, F. (2014). Fully homomorphic SIMD operations. Designs, codes and cryptography, 1-25.

[17] Gerasimov, A. N., Epishkina, A. V., & Kogos, K. G. (2017, February). Research of homomorphic encryption algorithms over integers. In Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian (pp. 398-403). IEEE.

[18] Halevi, S., & Shoup, V. (2013). Design and implementation of a homomorphic-encryption library. IBM Research (Manuscript), 6, 12- 15.

[19] Tourky, D., ElKawkagy, M., & Keshk, A. (2016, October). Homomorphic encryption the “Holy Grail” of cryptography. In Computer and Communications (ICCC), 2016 2nd IEEE International Conference on (pp. 196-201). IEEE.

基于同态密码方法的分布式图像加密

Debasis Das
Department of Computer Science and Information Systems
BITS Pilani, K.K. Birla Goa Campus,
Zuarinagar, Goa-403726, India.
Email: debasisd@goa.bits-pilani.ac.in

摘　要

本研究的目的是开发一种新颖的图像加密方法，可用于显着提高加密图像的安全性.为了解决这个图像安全问题，我们提出了一种分布式同态图像加密方案，其中感兴趣的图像是可见电磁频谱中的图像.在我们的加密阶段，红绿蓝 (RGB) 图像首先被分成其组成的通道图像，然后每个通道的像素的数值强度值被写入为较小像素强度子值的总和，导致有每个 R、G 和 B 通道图像的几个分量图像.同态加密函数用于使用加密密钥对每个分量图像中的每个像素强度子值进行单独加密，从而形成分布式图像加密方法.可以在传输和/或存储之前压缩每个加密的组件图像.在我们的解密阶段，必要时对每个加密的分量图像进行解压缩，然后使用加密函数的同态特性将每个加密分量图像中单独加密的像素强度子值的乘积转换为它们的总和的加密，在应用相应的解密函数和解密密钥之前，为每个通道图像恢复原始像素的强度值，然后恢复原始 RGB 图像.此外，RGB 图像加密和解密的特殊情况，其中每个通道的像素强度值被写入为仅两个子值的总和，并使用软件进行模拟.生成的密码图像经过一系列安全测试和分析.这些测试的结果表明，我们提出的同态图像加密方案是健壮的，可以抵抗安全攻击，并增加了相关加密图像的安全性.我们提出的同态图像加密方案产生了高度安全的加密图像.

关键词：分布式图像加密；同态加密；图像加密；Paillier 密码系统；RGB 图像加密

1　引言

这项研究解决了信息安全问题，通常也称为网络安全，尤其是图像安全.加密图像的安全性总是可以通过新的加密方法和方法来提高.因此，不断研究能够有效保护信息并对抗任何恶意网络行为的新加密方案.我们的目标是开发一种新颖的同态图像加密方案，该方案可用于在通过不安全通道传输图像之前对其进行加密，而不会影响其内容，然后使用解密过程恢复加密的图像.加密方案还应保护存储在计算机服务器或文件中的图像.我们提出的同态图像加密方案的应用领域包括来自卫星的机密图像、军事应用图像、工业应用图像、某些类型的医学图像、指纹图像以及来自任何需要的可见电磁频谱中的其他图像.防止安全漏洞并确保其机密性和完整性.多年来，来自学术界、工业界和其他领域

的各种研究人员已经开发并在文献中介绍了图像加密方案.在这些图像加密方案中，可以列出基于混沌的加密，在某些情况下，在加密来自图像的像素强度值时，使用具有混沌行为的序列或方程组.许多研究人员已经提出了基于混沌的方法 [4]、[9]、[15]、[16]、[23]、[25].例如，Z. H. Guan、F. Huang 和 W. Guan [25] 提出了一种基于混沌的图像加密算法，该算法使用 Arnold 猫图打乱特殊域中像素的位置，同时使用 Chen 的混沌系统改变每个像素的强度值.R. Tao、X. Meng 和 Y. Wang 在 [17] 中提出了一种基于多阶分数阶傅里叶变换 (FRFT) 的图像加密方案，他们从中通过对插值图像的不同阶逆离散 FRFT 求和获得加密图像.在 [12] 中，L. D. Singh 和 K. M. Singh 讨论了一种椭圆曲线密码系统，其中将图像加密方案应用于一组像素以获得相应的密码图像. G. Ye 和 X. Huang 在 [6] 中提出了一种图像加密方案，该方案使用心电图 (ECG) 信号生成用于加密纯图像的初始加密密钥.在[11]中，J. Zhou、X. Liu、OC Au 和 Y. Yan Tang 提出了一种有效的图像加密然后压缩 (ETC) 系统，该系统在预测误差域中运行并为其加密提供高安全级别和压缩图像.

在这项研究中提出了一种范式转换，其中一个普通图像被分解成多个分量图像，每个图像都使用同态函数属性加密以获得多个分量密码图像.然后对加密的组件密码图像进行解密和组合以获得原始图像.

论文的组织如下：在第二节中，提出了所提出的图像密码方案. 第三节提供了性能和安全性分析结果，第四节是论文的结论.

2　提议的图像密码方案

考虑以下两个命题和相关的加密和解密方案[14].

命题 1

设$g(i,j)$是M行N列图像的二维数组表示，其中(i,j)是每个像素的空间坐标，对于$i = 1,2,3,\ldots,M$和$J = 1,2,3,\ldots,N$.让图像的数据类为无符号 8 位整数，导致每个像素强度值在区间$[0,(L-1)] = [0,255]$中，其中$L = 256$是像素强度级别的数量.让每个像素的强度值y属于有限伽罗瓦域$Zp = \{0,1,2,\ldots(p-1)\}$，其中$p$是选择为等于$p = 257$的素数.对于 8-位图像，每个像素的强度值$y$在区间 [0,255] 内，但我们选择$p = 257$，即最接近的素数为 255.这可能导致像素强度值为 256，超出范围 [0,255].所以，如果出现y=256，可以进行特殊处理来说明，或者映射为y=255，由于冗余或其他因素，对实际图像影响很小.请注意，相同的概念可以应用于具有无符号 16 位整数或其他数据类的图像.

命题 2

设 E 是从有限域 Zp 映射的同态加密函数，使得 $E(y_1 + y_2 + y_3 + \ldots + y_k) = E(y_1) \times E(y_2) \times E(y_3)\ldots E(y_k)$，对于 Zp 中的所有 y_k，k 是一个正整数，使得 $1 <$

$k < L$，其中 L 是像素强度级别的数量. 这意味着 k 个像素强度子值 $y_1, y_2, y_3, \ldots, y_k$ 的总和的加密等于它们各自加密的乘积，反之亦然.

A. 同态图像加密

设E为同态加密函数，设y为图像$g(i,j)$中像素的强度值，其中i=1,2,3,...M 和j=1,2,3,....,N，其中M和N分别是数字图像中像素的行数和列数.可以将一个像素的强度值 y 写为 k 个像素的强度子值的总和，如下所示：

$$y = y_1 + y_2 + y_3 + \cdots + y_k = \sum_{n=1} ky \tag{1}$$

其中像素分量的数量 k，也称为像素强度子值的数量，也对应于分量图像的数量，是一个整数，使得$1 < k < L$，其中L是像素强度级别的数量.当像素强度子值的个数大于像素强度值时，即$k > y$，需要进行额外的特殊处理，其中$d = k - y$的差值可用于求出原始像素值y.现在，要使用同态加密函数 E 加密像素的强度值 y，可以编写：

$$E(y) = E(y_1 + y_1 + y_1 + \cdots + y_1) \tag{2a}$$

$$= E\left(\sum_{n=1}^{k} y_n\right) \tag{2b}$$

$$= \prod_{n=1}^{k} \left(E(y_n)\right) \tag{2c}$$

$$E(y) = E(y_1) \times E(y_2) \times E(y_3) \cdots E(y_k) \tag{2d}$$

(2)d 中 $E(y)$ 的最终表达式具有深远的意义.可以同时或在不同时间使用相同或不同的加密密钥对每个$E(y_k)$ 执行分布式和或并行或顺序加密处理.每个 $E(y_k)$ 也可以由相同或不同位置的相同或不同处理器计算.这可以大大提高加密图像的安全性，因为入侵者可能无法访问可以存储在不同位置或以不同时间间隔传输的所有$E(y_k)$.此外，如果每个 $E(y_k)$ 使用不同的加密密钥，则可以访问某些解密密钥的对手可能无法访问其他解密密钥，从而导致无法在没有全部解密的情况下解密所有对应的加密组件图像键.此外，每个y_k可以随机生成，唯一的要求是它们的总和应等于y.同样需要注意的是，k的值越大，加密图像越安全，但计算成本也越高.

此外，每个加密值$E(y_k)$可能是一个非常大的整数，在相关图像的像素强度值范围$[0, (L-1)]$之外. 因此，为了从图像的角度使这些$E(y_k)$有意义，可以将$(mod\ p)$应用于每个加密值$E(y_k)$，将它们映射回 Zp，并获得像素的强度值.范围$[0, (p-1)]$从图像的角度来看可能是有意义的.例如像素强度值范围是[0,255] 对于 8 位图像的情况，可以选择p为p= 257.因此，我们可以写成：

$$C_1 = E(y_1) \tag{3}$$

$$C_2 = E(y_2) \tag{4}$$

$$\vdots$$

$$C_k = E(y_k) \tag{5}$$

将 mod p 应用于上述方程，我们有

$$C_{p1} = C_1 \, mod \, p = E(y_1) \, mod \, p \tag{6}$$

$$C_{p1} = C_2 \, mod \, p = E(y_2) \, mod \, p \tag{7}$$

$$\vdots$$

$$C_{pk} = C_k \, mod \, p = E(y_k) \, mod \, p \tag{8}$$

数量 $C_{p1}, C_{p2} \ldots, C_{pk}$ 表示每个像素强度子值 $y_1, y_2, \ldots, y_k$ 的加密值. 它们还表示将被传输或存储的安全图像像素的强度子值.

同样重要的是要注意解密所需的另一个数量. 它是小于或等于$(E(y_k)/p)$ 的最大整数，也称为$(E(y_k)/p)$或$(b(y_k)/pc)$的底数.它也表示当$E(y_k)$除以p.这个量不是秘密的，也可以通过其他方式加密并在发送端传输以增加安全性，也可以在接收端计算.无需$(b(y_k)/pc)$重构 在接收方解密$E(y_k)$可能很困难，所以，我们可以写：

$$qt_1 = \left\lfloor \frac{E(y_1)}{p} \right\rfloor \tag{9}$$

$$qt_2 = \left\lfloor \frac{E(y_2)}{p} \right\rfloor \tag{10}$$

$$\vdots$$

$$qt_k = \left\lfloor \frac{E(y_k)}{p} \right\rfloor \tag{11}$$

B. 同态图像解密阶段

设 $Cp_1 = E(y_1) \, mod \, p$，$Cp_2 = E(y_2) \, mod \, p$，，$Cp_3 = E(y_3) \, mod \, p$，，并且一般来说 $Cp_k = E(y_k) \, mod \, p$，，是映射的各个加密像素强度子值 到 Zp，并且在接收端可用，其中E是同态加密函数.另外，让 $qt_1 = b(E(y_1)/pc))$, $qt_2 = b(E(y_2)/pc))$, $qt_3 = b(E(y_3)/pc))$, ..., $qt_k = b(E(y_k)/pc))$ 是在接收端也可用的解密参数.要解密加密像素强度值 $E(y)$ 并获得像素强度值 y，必须首先重构或计算各个加密像素强度子值 $E(y_1)$，$E(y_2)$, $E(y_3)$, ..., 和 $E(y_k)$ 如下：

$$E(y_1) = qt_1 \times p + C_{p1} \tag{12}$$

$$E(y_2) = qt_2 \times p + C_{p2} \tag{13}$$

$$\vdots$$

$$E(y_k) = qt_k \times p + C_{pk} \tag{14}$$

其中 $qt_k \times p + Cp_k$ 是每个 k 值的不同常数整数.一旦计算了上述（12）到（14）的量，就可以将相应的解密函数 D 应用到（15）中的以下乘积中并恢复y. 首先，计算乘积.

$$E(y_1) = E(y_1) \times E(y_2) \times E(y_3) \times \cdots \times E(y_k) \tag{15}$$

应用解密函数给出：

$$D[E(y)] = D[E(y_1) \times E(y_2) \times \cdots \times E(y_k)] \tag{16}$$

$$D[E(y)] = D\left[\prod\nolimits_{n=1}^{k} E(y_n)\right] \tag{17}$$

$$D[E(y)] = D\left[E\left(\sum_{n=1}^{k} y_n\right)\right] \tag{18}$$

$$D[E(y)] = D[E(y_1 + y_2 + y_3 + \cdots + y_k)] \tag{19}$$

$$D[E(y)] = y_1 + y_2 + y_3 + \cdots + y_k \tag{20}$$

$$D[E(y)] = y \tag{21}$$

请注意，从（17）到（18）的转换是使用加密函数 E 的同态属性实现的. 此外，如果每个像素强度子值 y_k 的加密/解密密钥不同，则可以首先解密每个 $E(y_k)$，然后相加 $y_1 + y_2 + y_3 + \cdots + y_k$ 得到像素强度值y. 为了实现效率，图像的像素强度值可以作为矩阵而不是单个像素一起处理.

C. k=2 分量图像的特殊情况实现

为了实现所提出的图像加密方案并验证所提出的理论方法将提供预期结果，我们选择实现 $k = 2$ 的特殊情况，其中k是像素强度子值y_1, y_2 的数量,我们也将其命名为像素分量的数量.

1) $k = 2$ 分量图像的特殊情况加密阶段实现：设 $y = y_1 + y_2$ 和 $E(y) = E(y_1) \times E(y_2)$. 我们需要一个具有上述同态性质的加密函数 E，其中两个像素强度子值y_1和 y_2 之和的加密等于各个加密子值$E(y_1)$和$E(y_2)$. 考虑具有加密和解密功能的 Paillier 密码系统[3]、[18]、[24]，其中值 y 可以加密如下：

$$E(y) = g^y x^n \, mod \, N^2 \tag{22}$$

其中 $N = s \times q$，并且 s, q 是两个素数，而 x 是一个随机数，使得$x \in Z * N = \{1,2,\ldots,(N-1)\}$，$g$为阶数为 N 的倍数的整数,即$g\hat{}l \equiv 1(mod\, N)$，$g = 1 + N$ 当素数 s 和 q 的长度相同时，N满足这个条件.

还可以注意到，Paillier 加密方案是一种也是概率性的公钥密码系统. 为了加密方案是安全的，公钥 N 必须是一个非常大的整数，例如超过 300 位.可以证明 Paillier 加密

函数是同态的并且满足 $k=2$ 对于(22)，我们可以用 Paillier 加密函数和相同的公钥N加密两个像素强度子值y_1和y_2中的每一个 如下：

$$C_1 = E(y_1) = g^{y_1} x_1^N \ mod\ N^2 \tag{25}$$

和

$$C_2 = E(y_2) = g^{y_2} x_2^N \ mod\ N^2 \tag{26}$$

将(6)和(7)中所示的 mod p应用到上述方程 (23)和 (24)中，k=2 给出

数量C_{p1}和C_{p2}代表对应于每个像素强度子值y_1和y_2的密码值.这些加密值 C_{p1}和C_{p2}表示将被传输或存储的安全图像像素强度子值.

2）$k = 2$分量图像的特殊情况解密阶段实现：对于像素强度子值$k = 2$的特殊情况，假设使用相同的密钥对y_1和y_2进行加密，Cp_k和qt_k来自(8) 和 (11) 在接收器的前端可用. 在应用解密函数 D 之前，必须首先使用 $k = 2$ 的 (14) 中的表达式计算加密像素强度子值$E(y_1)$和$E(y_2)$，如下所示：

$$E(y_1) = qt_1 \times p + C_{p1} \tag{27}$$

和

$$E(y_2) = qt_2 \times p + C_{p2} \tag{28}$$

使用方程(16)到(21)对于k=2，可以写成

$$D[E(y_1) \times E(y_2)] = D[E(y_1 + y_2)] = D[E(y)] = y \tag{29}$$

在(2) d 的上下文中应用 Paillier Decryption 函数时，我们可以这样写：

$$C = E(y) = E(y_1) \times E(y_2) \tag{30}$$

和

$$y = \frac{L\left(C^\lambda \ mod\ N^2\right)}{L(g^\lambda \ mod\ N^2)} \ mod\ N \tag{31}$$

$$y = \left[L\left(C^\lambda \ mod\ N^2\right) \times \left(\left(L\left(g^\lambda \ mod\ N^2\right)\right)^{-1} \ mod\ N\right)\right] mod\ N \tag{32}$$

其中$N = s \times q$，并且s、q是素数，当s和q的长度与前面所述的相同时，g可以设置为$g = 1 + N$. 参数 λ 由$s-1$和$q-1$的最小公倍数给出，而函数 $L(U)$ 定义为

$$L(U) = \frac{(U-1)}{N} \tag{33}$$

3) 提议的图像加密方案框图：图 1 显示了特殊情况实现的框图，其中像素强度子值 k = 2.可以扩展图 1 中的分量图像同态加密子块 根据k的值增加到 3、4、5、6 或更多，以产生更多的加密组件图像并增加安全性.

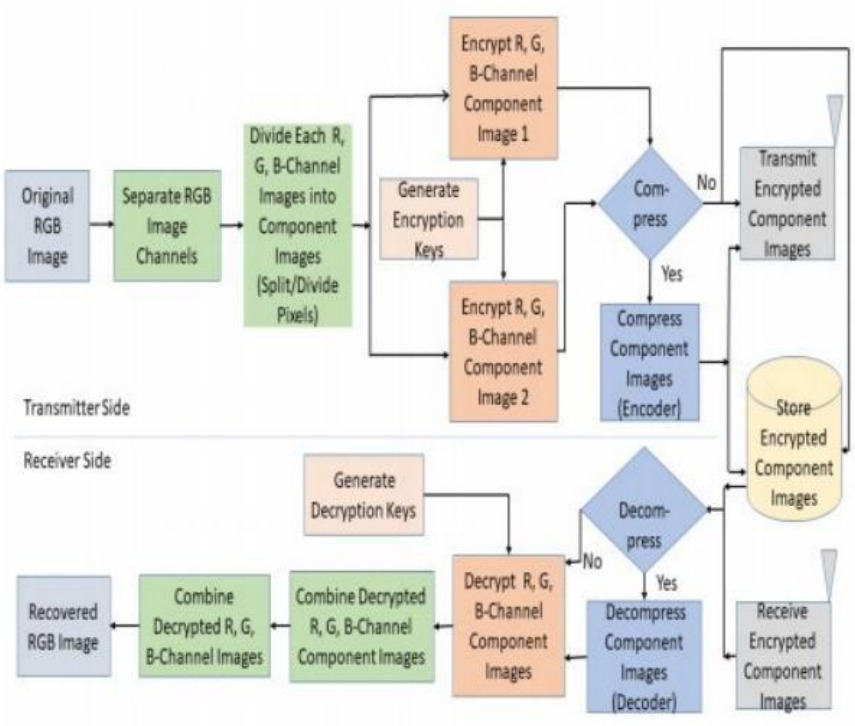

图 1 k = 2 分量图像提出的特殊情况图像加密方案.

3　性能和安全分析结果

性能和安全性分析旨在验证所提出的同态图像加密方案是否满足某些所需的性能测试并能抵抗安全攻击. 这种性能和安全分析包括相关分析、信息熵、密码循环、直方图分析、选择明文攻击和蛮力攻击. 仿真结果是从我们编写并使用笔记本电脑运行的 Mathematica 软件获得的，该笔记本电脑具有以下规格的处理器：Intel (R) Core(TM) i3-4030U CPU @ 1.90 GHz 1.90 GHz.

A. 输入输出和加密组件图像

本研究中使用的测试图像（Baboon）来自南加州大学信号与图像处理研究所图像集[22].

本章介绍和讨论了恢复的图像和密码图像. 我们使用我们的 Mathematica 代码实现随机生成我们的私钥，质数s和q，每 165 位是

s =135231806007162061442750686391904431697185197566367006618981784691676107437603053795350082927665613024925359860877093300237421910195680114293947567777974339655680621

和

q =615992755631196892042255664927717248642966905816621393579407292577688854060907090245478725209640356332882614747503301078258406727964006007503687722380089774424939227.

s和q的位数分别为 546 位和 548 位.因此，用于加密的公钥$N = s \times q$的值有 329 位和 1093 位，由下式给出

N =8330181283133520361658120289387619041915126689045513627323646816070183890288033578333678665120697181973881497831382325363244464811001551327765320992255474004600188765660480640447542299262750458887672072976607578472070872148044189831835405096988659858939959968900951009213522346253850216109682134503606251866477057119002324661996 7.

图 2 (a) 所示的原始 RGB 图像通过分离其 R、G 和 B 通道图像中的每一个进行通道处理，如图 1 和图 2 所示.分别参见 2 (d)、2 (g)和 2 (j). 这些通道图像中的每一个都通过在对每个图像进行加密之前首先将其分解为两个分量图像来单独处理.例如，将图 2(d)中的 R-Channel 原始图像 R 分解为此处未示出的两个分量图像 R1 和 R2，然后进行加密以产生图 2(d)所示的加密分量图像 R1 和 R2. 分别参见 2 (e) 和 2 (f). 类似地，G 和 BChannel 原始图像各有两个分量图像，它们被加密以产生图 1 和图 2 所示的加密分量图像 G1 和 G2. 2 (h) 和 2 (i) 用于 G 通道.

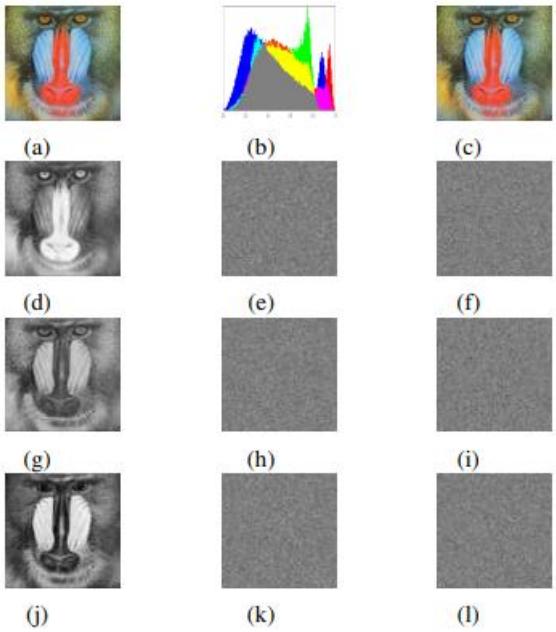

图 2：（a）原始狒狒 RGB 图像；(b) 原始狒狒 RGB 图像的直方图；
(c) 恢复的狒狒 RGB 图像；(d) 原始 R 通道狒狒图像 R；
(e) 加密狒狒组件图像 R1；(f) 加密狒狒组件图像 R2；
(g) 原始 G 通道狒狒图像 G；(h) 加密狒狒组件图像 G1；
(i) 加密狒狒组件图像 G2；(j) 原始 B 频道狒狒图像 B；
(k) 加密狒狒组件图像 B1；(l) 加密狒狒组件图像 B2

图 2 (k) 和 2 (l) 对应于 B 通道原始图像的加密分量图像. 图 2 (b) 显示了接下来

讨论的原始狒狒图像的直方图，而图 2 (c) 显示了通过组合恢复的 R、G 和 B 通道图像获得的恢复 RGB 图像. 分量图像的数量不仅限于每个通道有两个分量图像的特殊情况. 例如，R 通道分量图像也可以扩展到 R3、R4、R5、...Rk，如第 II 节所述. 在接收端，每个通道的加密分量图像用于恢复相应的原始通道图像. 例如，图 1 和图 2 中的加密组件图像 R1 和 R2. 图 2 (e) 和 2 (f) 用于恢复图 3 (a) 所示的 R 通道图像. 对 G 和 B 通道图像采取了类似的方法. 此外，将图 3 中恢复的 R、G 和 B 通道图像组合起来形成图 2(c) 中恢复的 RGB 图像.

B. 直方图分析

数字图像的直方图提供有关其像素强度值分布的信息.

(a)　　(b)　　(c)

图 3：(a) 恢复的 R 通道狒狒图像
(b) 恢复的 G 通道狒狒图像
(c) 恢复的 B 通道狒狒图像

对于强度水平在离散区间[0,L−1]中的图像，直方图由离散函数 $h(l) = nl$ 给出，其中 1 是第 1 个强度值，nl表示 具有强度值 l 的图像.[19]对由我们提出的同态图像加密方案产生的密码图像进行直方图分析，对每个通道图像及其相关的加密分量图像进行. 因此，图 4(a)中的 RChannel 原始图像 R 的直方图分析如图 4(d)所示，并且是不均匀的，而图 4(a)中的加密分量图像 R1 和 R2 的直方图分析是不均匀的. 图 4 (b) 和 4 (c) 的直方图在图 3 和图 4 中.分别为 4(e)和 4(f)； 这也表明加密算法能够为每个加密的分量图像生成类似均匀分布的像素强度值；因此，可以抵抗直方图分析攻击.

G 和 B 通道原始图像的类似直方图以及相关的加密组件图像 G1、G2、B1 和 B2 也提供了类似的结果.

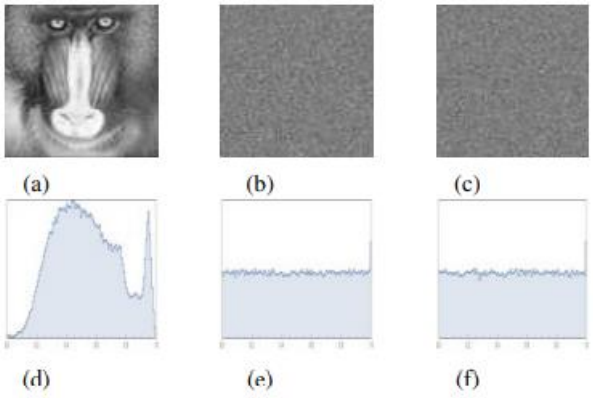

图 4：（a）原始 R 通道狒狒图像 R；(b)加密狒狒组件图像 R1；

(c)加密狒狒组件图像 R2；(d)原始 R 通道狒狒图像 R 的直方图；

(e)加密狒狒组件图像 R1 的直方图；(f)加密狒狒组件图像 R2 的直方图；

C. **密码循环**

图像加密方案的要求之一是生成与原始纯图像非常不同的加密图像. 为了量化对应的明文图像和密码图像对之间的这种差异，可以使用由像素变化率 (NPCR) 数和统一平均变化强度 (UACI) [5]、[9] 表示的两个标准，[10]、[20]、[21]. NPCR 和 UACI 也可用作安全测试以防止差异攻击，包括对密码图像进行轻微更改并观察结果的变化. 一方面，测量两个图像 C 和 C0 之间颜色分量差异的平均像素数的 NPCR 表达式由下式给出：

$$[NPCR]_{R,G,B} = \frac{\sum_{i,j}[D_{R,G,B}(i,j)]}{N} \times 100\% \tag{34}$$

其中 N 是图像的总像素数，DR,G,B 的定义由下式给出：

$$D_{R,G,B}(i,j) \triangleq \begin{cases} 0, & C_{R,G,B}(i,j) = C'_{R,G,B}(i,j) \\ 1, & C_{R,G,B}(i,j) \neq C'_{R,G,B}(i,j) \end{cases} \tag{35}$$

其中$C_{R,G,B}(i,j)$和$C'_{R,G,B}(i,j)$分别表示图像C和C'中相应颜色分量R、G 和 B 的值. 给定两个随机图像，可以找到 NPCR 期望值的表达式为

$$E(NPCR) = (1 - 2^{-L_{R,G,B}}) \times 100\% \tag{36}$$

其中$L_{R,G,B}$表示用于对每个颜色分量 R、G 或 B 进行编码的位数.例如，给定两个随机图像，每个图像的大小为 512×512 和 24 位真彩色，每个 R 为 8 位， G、B 通道（$LR = LG = LB = 8$），NPCR 的期望值由下式给出：

$$[NPCR]_R = [NPCR]_G = [NPCR]_B = 99.609375\% \tag{37}$$

另一方面，UACI 的表达式定义为

$$UACI_{R,G,B} = \frac{1}{N}\left[\sum_{i,j}\frac{\left|C_{R,G,B}(i,j) - C'_{R,G,B}(i,j)\right|}{2^{L_{R,G,B}} - 1}\right] \times 100\% \tag{38}$$

其中$L_{R,G,B}$分别表示用于红色 (R)、绿色 (G) 或蓝色 (B) 的每个颜色分量的位数. 给定两个随机图像，UACIR,G,B 的期望值由下式给出

$$E\left(UACI_{R,G,B}\right) = \frac{\frac{1}{(2^{2L_{R,G,B}} - 1)\left(\sum_{i=1}^{2^{L_{R,G,B}}} i(i+1)\right)}}{2^{L_{R,G,B}} - 1} \times 100\% \tag{39}$$

对于每个通道使用 8 位编码的 RGB 图像，我们有以下期望值：

$$E(UACI_R) = E(UACI_G) = E(UACI_B) = 33.46354\% \tag{40}$$

执行 NPCR 和 UACI 分析比较由我们的图像加密方案产生的明文图像和密码图像，B 通道的结果如表 I 所示.R 和 G 通道图像也获得了类似的结果，但未显示 这里. 从表 I 中可以看出，原始 B 通道图像 B 与其关联的加密分量图像 B1 和 B2 之间的 NPCR 分别为 99.6136 和 99.6273.这些值非常接近预期值 99.60937，因此，加密算法在改变 B 通道分量图像 B1 和 B2 中的像素强度值时表现非常好. 原始 B 通道图像 B 与其对应的加密分量图像 B1 和 B2 之间的 UACI 值非常接近表 I 中的预期值 33.4635；因此，加密算法在这种情况下也表现良好.

表 1 NPCR 和 UACI 用于 B 通道原始和加密图像

B-通道			
测试类型	B,B1	B,B2	期望值
NPCR (%)	99.6136	99.6273	99.60937
UACI (%)	31.3253	31.3231	33.4635

D. 相关分析结果和讨论

可见电磁频谱范围内的许多图像都有冗余，有时会导致水平、垂直和对角线方向的相邻像素之间存在高度相关性.一个好的图像加密方案应该打破相邻像素之间的这种相关性并将其值降低到几乎为零；因此，生成的图像更能抵抗统计攻击.包括 A. Soleymani、A. Daneshgar、A. Kano [2]、[4]、[5]、[7]-[10]、[12]、[20] 在内的几位作者讨论了相关系数的表达式 [21].

$$r_{XY} = \frac{cov(X,Y)}{\sigma_X \sigma_Y} \tag{41}$$

其中$cov(X,Y)$和$\sigma_X\sigma_Y$分别是X和Y的标准差的协方差和乘积. 相邻像素对的协方差和标准偏差具有以下形式

$$cov(X,Y)=\frac{1}{N}\sum_{i=1}^{N}\left[(x_i-\mu_X)(y_i-\mu_y)\right] \tag{42}$$

其中x_i和y_i是随机选择的相邻像素对的值，N是来自图像的相邻像素对 (x_i,y_i) 的总数，μ_X和μ_y分别是 X 和 Y 的平均值或期望值，并给出经过

$$\mu_X=\frac{1}{N}\sum_{i=1}^{N}x_i\ ,\ \mu_Y=\frac{1}{N}\sum_{i=1}^{N}y_i \tag{43}$$

使用方差，标准差σ_X和σ_Y的表达式为：

$$\sigma_X=\left(\frac{1}{N}\sum_{i=1}^{N}(x_i-\mu_X)^2\right)^{\frac{1}{2}}\ ,\ \sigma_Y=\left(\frac{1}{N}\sum_{i=1}^{N}(y_i-\mu_Y)^2\right)^{\frac{1}{2}} \tag{44}$$

使用一组 N = 2500 个随机的水平和垂直方向的相邻像素对进行相关性分析，比较每个通道的原始图像及其相关的加密组件密码图像. G 通道图像的这种相关性分析的结果显示在表 II 中.还对 R 和 B 通道图像进行了相关分析，它们提供了类似的结果.表二显示原始 G 通道图像 G 中相邻像素强度值对在水平和垂直方向高度相关，相关系数值接近 1.然而加密分量图像 G1 和 G2 的相邻对非常不相关像素的强度值，因为相关的相关系数接近 0.这些 G 通道图像相关分析的结果也显示在图 5 中.水平和垂直方向上相邻像素对的相关性；并因此通过使它们更能抵抗统计相关攻击来提高加密图像的安全性.

表 2 2500 相邻像素的相关系数狒狒 G 通道图像对

G-通道			
方向	B,B1	B,B2	期望值
水平	0.86158	−0.000659307	0.00697017
竖直	0.760878	0.0401025	−0.00679211

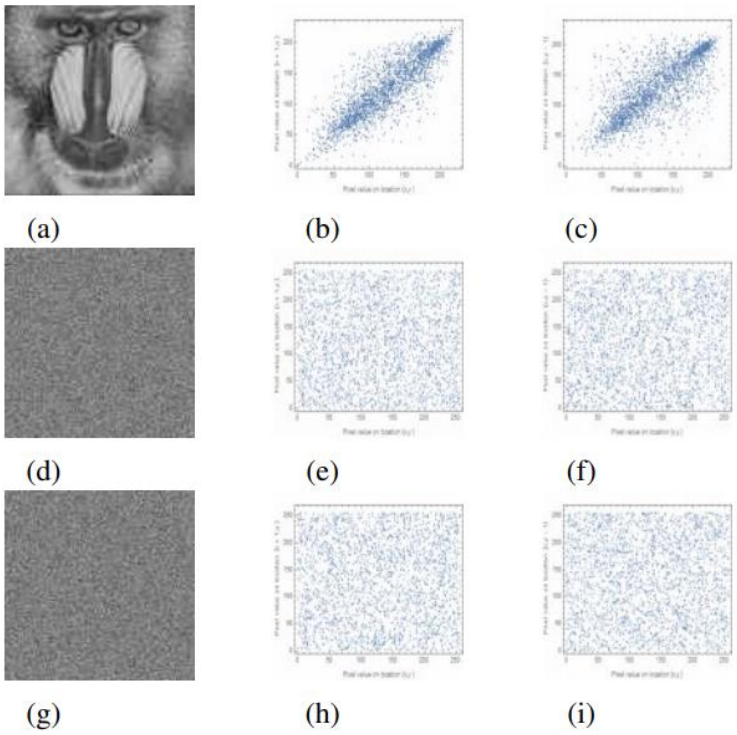

图 5:　(a) G 通道原始狒狒图像 G；(b)图像 G 的水平相关性；
(d)加密分量图像 G1；(c)图像 G 的垂直相关性；
(e)图像 G1 的水平相关性；(f)图像 G1 的垂直相关性；
(g)加密分量图像 G2；(h)图像 G2 的水平相关性；
(i)图像 G2 的垂直相关性
N = 2500 个相邻的随机像素对.

E. 信息熵

可以使用其信息熵来评估随机变量的不确定性程度. 在随机性的所有特征中，熵是最重要的特征之一. 给定具有 N 个符号的源 S，其中 N = 2k 和 k 是用于表示符号 Si 的位数，可以按如下方式获得信息熵 h(S) [4], [5], [10], [19]、[20]、[23]：

$$h(S) = -\sum_{i=0}^{N-1} p(S_i) lo\, g_2[p(S_i)] \tag{45}$$

其中$p(S_i)$是符号S_i的出现概率，N 是源生成的符号总数，

并且使用对数基数 2 来表示以位为单位的熵. 当 S 是真正的随机源时，对于所有 i，$p(S\_i) = 1 + 2k$，熵可以计算为

$$h(S) = k \tag{31}$$

我们的熵分析结果在表 III 中给出. 表 III 显示了每个加密通道分量图像 R1、R2、G1、G2、B1 和 B2 的熵值非常接近预期值 8.因此，这些加密分量图像是真正随机的；

因此，我们提出的同态图像加密方案足够健壮，可以防止熵攻击.

表 3 Baboon R、G 和 B 通道的熵分析图片

R-通道		
密文 R1	密文 R2	期待值
7.94141	7.94136	8
G-通道		
密文 G1	密文 G1	期待值
7.94062	7.94512	8
B-通道		
密文 G1	密文 G1	期待值
7.94333	7.94229	8

F. 选择明文攻击

在选择的明文攻击中，除了加密算法之外，对手还可以访问至少一对明文和密文，并试图找到加密密钥的结构. 如果找到了密钥，则可以使用找到的密钥 [12]、[13]、[23] 解密使用此密钥加密的所有过去和未来的密码. 我们提出的同态加密方法可以抵抗这种类型的攻击，因为当使用相同的加密密钥多次加密相同的原始图像时，它总是会产生不同的密码图像，如图 6 所示. 对于加密的 G 和 B 通道图像也获得了类似的结果，但此处未显示.

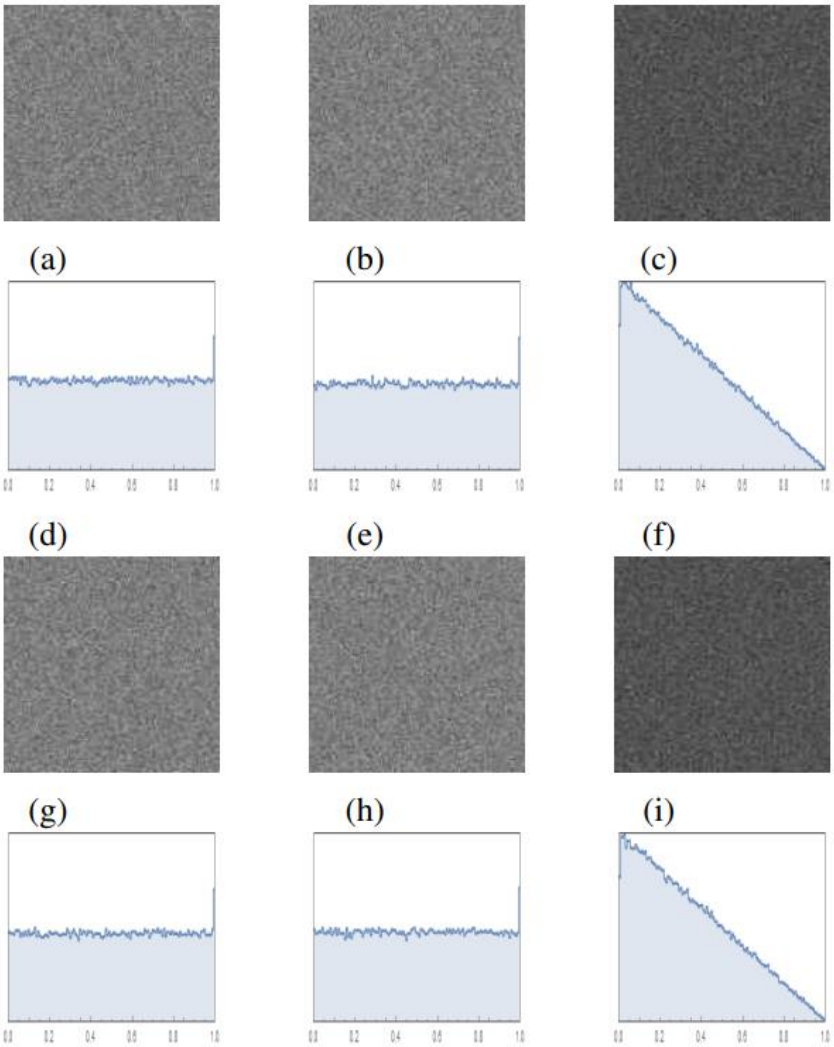

图 6 (a) 加密比较.图像 R11 及其 Hist.在(d)中；
(b) 加密比较.(e)中的图像 R12 及其直方图；
(c) 像素差异|R11-R12|及其 (f)中的直方图；
(g) (j)中的加密分量图像 R21 及其直方图；
(h) (k) 中的加密分量图像 R22 及其直方图；
(i)像素差异|R21−R22|及其（1）中的直方图.

G. 时间和恢复图像质量分析结果和讨论

本节介绍并讨论表 IV 和 V 中 R 通道恢复图像的时序和质量结果.时序仿真结果是使用配备 Intel (R) 处理器和 Core(TM) i3-4030U CPU @ 1.90 GHz 1.90 GHz 的膝上型计算机获得的，当使用不同速度的处理器时，它们会发生变化.计时结果也可以根据用于实现加密和解密功能的算法的效率而改变.在表 IV 中，由组件映像 R1 加密时间 (R1ET) 和组件映像 R2 加密时间 (R2ET) 表示的列分别给出了加密组件映像 R1 和 R2 所需的时间，以秒 (S) 或分钟 (min) 为单位，而列解密时间 (DT) 提供了解密和恢

复 R 通道原始图像所需的时间.在表 V 中，NPCR（像素数变化率）列给出了比较 RChannel 原始图像和恢复图像的数据，以显示由于加密和解密过程而发生变化的相应像素值的百分比，当加密图像不会被压缩.

表 4 R 通道时序分析

R-通道				
n(像素)	n(比特)	R1ET	R2ET	DT
4	11	31.42 S	30.89 S	16.27 S
8	27	55.59S	54.25 S	29.85 S
20	65	2.18 min	2.17 min	1.79 min
60	197	6.05 min	6.03 min	5.99 min
100	330	10.60 min	10.54 min	10.81 min
150	496	17.32 min	17.73 min	18.65 min
200	662	23.42 min	23.38 min	25.75 min
249	827	32.95 min	32.57 min	38.73 min
329	1093	53.18 min	53.69 min	64.43 min

希望此 NPCR 列的值尽可能小，这意味着原始和恢复的 R 通道图像几乎相同，并且在加密和解密操作期间丢失的信息很少. RGBNPCR 列给出了比较原始和恢复的 RGB 图像的数据，类似于之前的 NPCR 列. 最后，名为 Quality 的最后一列包括诸如 VL＝ 非常低、H＝ 高、VH＝ 非常高等术语，这些术语是根据前两列所示的百分比结果来判断恢复图像质量的主观定性描述，即 NPCR 和 RGBNPCR 列； 这表明当公共加密密钥的位数 N≥20 时，可以获得非常高质量的恢复图像. 对于 G 和 B 通道获得了类似的表.

表 5 R 通道恢复图像质量分析

R-通道				
n(像素)	n(比特)	NPCR	RGBNPCR	质量
4	11	16.56%	41.89%	VL
8	27	0.068%	0.18%	H
20	65	0.025%	0.055%	VH
60	197	0.0256%	0.056%	VH
100	330	0.026%	0.056%	VH
150	496	0.0256%	0.056%	VH
200	662	0.0256%	0.056%	VH
249	827	0.0256%	0.056%	VH

表 5 R 通道恢复图像质量分析（续表）

329	1093	0.0256%	0.056%	VH

H. 图像压缩结果和讨论

本节提供表 VI 中所示的 R 通道图像压缩结果.对于每个加密的通道组件图像 R1 和 R2，使用我们的模拟程序找到压缩前后的字节数.该表的最后一列显示，对于 R、G 和 B 通道加密图像，加密图像数据大小减少了大约等于 3.5 的因子.这意味着传输加密数据所需的带宽和时间更少，并且需要更少的内存来存储此加密信息以供将来解密处理.对于 G 和 B 通道加密图像也获得了类似的结果.

表 6 图像压缩结果

R-通道			
图片	加密前	加密后	还原比
密文 R1	2097304	594648	1 : 3.53
密文 R2	2097304	594768	1 : 3.53

4　结论

在这项研究中，提出了一种新颖的图像加密方案，该方案使用同态函数属性对图像进行加密，并为每个明文图像生成多个密码图像.在加密阶段，将原始 RGB 图像分离为其 R、G 和 B 通道图像，然后将每个通道图像中的每个像素强度值划分或分解为若干像素强度子值的和，以产生许多分量通道图像使用相同的加密密钥分别加密，必要时进行压缩，然后传输或存储.在解密方面，必要时对加密的分量通道图像进行解压缩，然后使用相同的密钥解密并组合以产生 R、G 和 B 通道恢复图像中的每一个，这些图像也被组合以获得恢复的 RGB 图像.仿真结果表明，关联的组件密码图像可以承受范围广泛的安全和分析攻击，包括直方图分析、熵分析、相关分析、选择明文攻击、蛮力攻击等.此外，还获得了高质量的恢复通道图像和恢复的 RGB 图像，这意味着由于应用我们提出的加密、解密和其他图像加密和处理操作而丢失的信息非常少.我们提出的同态图像加密方案可用于需要高度安全加密图像的非实时应用，例如机密卫星图像、一些机密医学图像、机密指纹图像以及可见电磁频谱范围内的任何机密图像.然而，如果实现更快的加密和解密算法，以及使用更快的微处理器或硬件，实时应用程序可能是可能的.我们的主要贡献是制定了一种新颖的同态图像加密方案，其中原始图像中的每个像素强度值都写为几个子值的总和，从而产生许多组件图像，这些图像被加密以产生许多相应的密码图像；因此，增加了相关图像的安全性.该公式包括加密和解密阶段，以及一个特殊情况实现的框图.未来的研究可能包括使用同态加密和解密函数，这将需要更少的计算时间，用

于可能的实时应用.当使用适当的同态函数和特殊的快速处理方法时，我们提出的加密方案也有可能扩展到视频加密.我们提出的方法可以应用于任何可以映射到大于 1 的数字的数据.例如，可以使用我们的方法加密从 a 到 z 映射到大于 1 的数字的字母，将每个数字写成几个数字的总和，然后使用同态加密函数对每个加密函数进行加密，并按照我们的方法中描述的必要步骤来提高安全性.

参考文献

[1] A. Daneshgar and B. Khadem, “A self-synchronized chaotic image encryption scheme," Signal Processing: Image Communication 36 (2015) 106-114. www.elsevier.com/local/image

[2] A. Soleymani, Md. J. Nordin, and Z. Md. Ali, “A novel public key Image encryption based on elliptic curves over prime group field," Journal of Image and Graphics, Vol. 1, No. 1, March, 2013.

[3] A. K. A. Hassan, “Reliable implementation of Paillier cryptosystem," Iraqi Journal of Applied Physics, IJAP, Vol. 10, No. 4, October-December 2014, pp. 27-29

[4] A. Daneshgar and B. Khadem, “A self-synchronized chaotic image encryption scheme," Signal Processing: Image Communication 36 (2015) 106-114. www.elsevier.com/local/image

[5] A. Kanso, M. Ghebleh, “ A novel image encryption algorithm based on a 3D chaotic map," Commun Nonlinear Sci Numer Simulat 17 (2012) 2943–2959, www.elsevier.com/locate/cnsns

[6] G. Ye and X. Huang, “An image encryption algorithm based on autoblocking and electrocardiography," Published by the IEEE Computer Society. April-June 2016.

[7] G. Zhang, and Q. Liu, “A novel image encryption method based on total shuffling scheme," Optics Communications 284 (2011) 2775–2780, www.elsevier.com/locate/optcom

[8] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons and Fractals 21 (2004) 749–761, www.elsevier.com/locate/chaos

[9] H.S. Kwok, Wallace K.S. Tang, “A fast image encryption system based on chaotic maps with finite precision representation, " Chaos, Solitons and Fractals 32 (2007) 1518–1529, www.elsevier.com/locate/chaos

[10] H. Liu, X. Wang, and A. kadir, “Image encryption using DNA complementary rule and chaotic maps , " Applied Soft Computing 12 (2012) 1457–1466, www.elsevier.com

[11] J. Zhou, X. Liu, O. C. Au, and Y. Yan Tang, “Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation," IEEE Transactions on Information Forensics and Security, VOL. 9, NO. 1, January 2014.

[12] L. D. Singh and K. M. Singh, “Image Encryption using elliptic curve cryptography, " Procedia Science 54 (2015) 475-481, www.sciencedirect.com

[13] M. Kumar, D. C. Mishra, and R. K. Sharma, “A first approach on an RGB image encryption, "Optics

And Lasers in Engineering 52 (2014) 27–34, www.elsevier.com/locate/optlaseng

[14] Mamadou I. Wade, “ Distributed mage encryption based on a homomorphic cryptographic approach , " Ph.D. Dissertation, Howard University, May 2017

[15] N.K.Pareek,V.Patidar,andK.K.Sud,“Imageencryptionusingchaotic logistic map, " Image and Vision Computing 24 (2006) 926-934, www.elsevier.com/locate/optlaseng

[16] P. P. Dang and P. M. Chau, “Image encryption for secure internet multimedia applications, " IEEE Trans. On Consumer Electronics, Vol. 46. No. 3, August 2000.

[17] R. Tao, X. Meng, and Y. Wang, “Image encryption with multiorders of fractional fourier transforms, " IEEE Trans. Inf. Forensics and Security, Vol. 5, No 4, Dec 2010.

[18] R. Rivest, Lecture Notes 15, Computer and Network Security: “Voting, homomorphic encryption," October, 2002

[19] R. C. Gonzalez and R. E. Woods, “Digital image processing.,"3rd ed. Person Education Inc., 2008.

[20] R. Rhouma, S. Meherzi, and S. Belghith, “OCML-based colour image encryption, " Chaos, Solitons and Fractals 40 (2009) 309–318, www.elsevier.com/locate/chaos

[21] S. Mazloom and A. M. E-Moghadam, “Color image encryption based on coupled nonlinear chaotic map, " Chaos, Solitons and Fractals 42 (2009) 1745–1754, www.elsevier.com/locate/chaos

[22] “ University of Southern California, signal and image processing institute" http://sipi.usc.edu/database/

[23] Y. Zhou, L. Bao, C. L. P. Chen “A new 1D chaotic system for image encryption," Signal Processing 97 (2014) 172–182, www.elsevier.com/locate/sigpro

[24] Yi Xun, P. Russell, B. Elisa, “ Homomorphic encryption and applications " 2014 XII, 126 p. 23 illus., http://www.springer.com/978-3-319-12228-1

[25] Z. H. Guan, f. Huang, and W. Guan , “ Chaos-based image encryption algorithm , " Physics Letters A 346 (2005) 153-157 , www.sciencedirect.com ; www.elsevier.com/locate/pla

基于同态加密和多方计算的安全云计算算法

Debasis Das Department of Computer Science and Information Systems BITS Pilani, K.K. Birla Goa Campus, Zuarinagar, Goa-403726, India. Email: debasisd@goa.bits-pilani.ac.in

摘　要

云计算是一种发展中的技术，它对许多安全问题还不清楚.不受信云中的数据可以使用加密算法进行加密.随机化这些数据提供了更多的安全性，这可以通过在云中填充的概念来实现.在本文中，用户的数据使用加密方案，称为最优非对称加密填充(OAEP)和基于 RSA(即 HE-RSA)的混合加密算法，以允许多方在保持完整性和机密性的同时计算其输入的函数.同态加密(HE)是对加密数据执行的，无需在计算强大的云中进行解密，安全多方计算(SMPC)，以确保用户的安全和隐私.在本文中，我们提出了一种将多方计算与同态加密相结合的方案，以允许加密数据的计算不需要解密.本文描述了我们在云模型中使用的加密技术，并将其管理费用与同态加密和多方计算进行了比较.

关键词：云计算; 最佳不对称加密填充; 同态加密; 多方计算

1　介绍

需要一个适当的或更合适的大数据基础设施[1]来支持大规模的存储和处理.如今，世界以数据为中心，因此大数据处理和分析已经成为任何大型机构最重要的工作.云计算是一种提供方便的、按需的访问来共享计算资的变化.源的模型.组织可以简单地连接到云，并在适当使用的基础上使用可用的资源.云计算已经成为一种使用共享计算资源分析大数据的工具，同时可以轻松地处理数据[1]的量和种类上云提供了许多优点，如更多的容错能力和多因素身份验证，以保护云中的信息.然而，由于这些属性，云计算也带来了维护数据的机密性和完整性的风险.在过去的几年中，由于恶意和侵入性行为，云中数据泄露的数量不断增加.加密保持数据的安全，但如果我们丢失加密密钥.因此，为了防止对云的恶意攻击，有必要开发有效的加密技术[3], [4]，以抵抗主动攻击，并不解密地对加密数据进行计算.基于云计算的解决方案在过去的几年中变得越来越流行.云计算平台从大数据云中进行分析和提取有用的信息.云计算的一个主要问题是云数据的隐私和机密性[5], [6], [7].一种解决方案是将加密后的数据发送到云中.然而，我们仍然需要支持对加密数据的有用计算，而全同态加密(FHE)[8], [9], [10], [11]是支持对加密数据进行计算的一种方法.我们注意到，虽然存在其他用来实现安全计算的机制，但它们通常需要不同的数据提供者来交换信息.因为 FHE 方案是公钥方案，所以 FHE 更适合于我们有许多数据源的场景.

安全多方计算(MPC)[12], [13]保证每个人都学习联合计算的正确输出，但不学习其他人的输入，即使执行计算的一些用户可能是主动或被动恶意的.安全的 MPC 可以为任意的计算和任意数量的各方来完成.因此，我们可以将安全的 MPC 协议视为编译器，它将一个函数的规范作为输入，并输出一个安全地计算该函数的协议.因此，我们可以将安全的 MPC 协议视为编译器，它需要一个映射的规范作为输入，而输出是一种安全地计算函数的协议.安全的 MPC[14], [15]提供了保密性和完整性，这是比完全同态加密和可验证的计算要好得多.可以对云环境中的任意计算和任意数量的各方执行可靠的 MPC.

我们的模式的好处是：将多方计算与同态加密相结合；提出了使用最优非对称加密填充(OAEP)-同态加密(HE)-RSA 进行加密的方案.

在第二节中，我们描述了相关的工作.在第三节中，我们定义了安全云计算的问题声明.在第四节中，我们描述了目标.在第五节中，我们描述了我们的贡献.然后，在第五节和第七节中，我们描述了密码技术，并详细描述了我们的方案.在第八节中，我们将描述这些结果.最后，在第九节中，我们总结并描述了通过我们的方法所实现的目标.

2　相关工作

M.Tebba 等人[2]提出了一种对云中的加密数据执行操作的技术，它将在计算后提供类似的结果，就像我们直接处理原始数据一样.Z.Wang 等人[3]给出了移动云计算中身份管理中同态签名的新定义.S.Yakoubov 等人[4]进行了一项关于保护云中大数据分析的加密方法的调查.C. Rong 等人[5]对云计算中不同的安全挑战进行了一项调查.C. Gentry[6]计算了加密数据的任意函数，它描述了一种保持信息私有的完全同态加密技术，但这使得一个工人不拥有私有解密密钥来计算数据的任何结果，即使数据的目的真的很复杂.C. Wang 等人[7]提出了一种具有两个显著特征的有效方案，以确保用户在云数据的正确性.Y.Yu 等人[8]研究了云中共享数据的三种审计机制中的主动对手攻击，并提出了一种解决方案，在不牺牲这些机制的任何理想特性的情况下解决这个弱点.L.Wei 等人[9]提出了一种隐私欺骗抑制和安全计算审计协议，或 SecCloud，这是第一个连接云中安全存储和安全计算审计的协议.A. Lopez-Alt 等人[10]展示了一种新的加密方案，他们称之为多密钥 FHE. F.F.Moghaddam 等人[11]提出了一种基于 RSASmall-e 和高效 RSA 的云计算环境混合加密算法.E. Shen 等人[13]利用安全多方计算的概念，提出了一种被称为云中加密安全计算[14]的方案.这是一种加密方法，它支持信息共享和分析，同时保持敏感输入保密，更快更容易为应用程序软件开发人员使用.M.Bellare 等人[12]提出了基于 RSA 的最优不对称加密方法.这项工作旨在在云计算通信中使用密码学的概念，并提高安全性.

D. Zissis 等人[18]解决了云计算安全问题的细节，他们提出了基于 SSO 和 LDAP 的公钥基础设施操作，以确保所涉及的数据和通信的身份验证、完整性和机密性.该解决方案提供了一个水平级别的服务，适用于所有牵连实体，实现了一个安全网格，在此网格

中维护了基本的信任.C. Hongbing 等人[20]提出了一种替代方法，称为云环境的安全大数据存储和共享方案.该租户将大数据划分为已排序的部分，并将其存储在多个云存储服务提供商之间.该方案不是保护大数据本身，而是使用活板门功能保护各个数据元素映射到每个提供者.论文[15]介绍了所综述的云计算问题.在本文中，[15]的作者讨论了大数据与云计算、大数据存储系统和 Hadoop 技术[17]、[19]之间的关系.此外，还调查了研究挑战，重点是可伸缩性、可用性、数据完整性、数据转换、数据质量、数据异构性、隐私、法律和监管问题以及治理.最后，总结了需要大量研究努力的开放式研究问题.

J.Zhou 等人[16]提出了一个方案称为安全和隐私保护协议基于云的车辆 DTN 解决抵抗层添加攻击的开放问题通过外包隐私保护聚合传输证据生成多个资源限制车辆云从执行任何单向活板门功能只有一次.车辆隐私很好地不受云和交通经理的保护.

3　针对安全云计算的问题公式化

考虑三方合作伙伴(如图所示 1)：在云中存储数据的用户 Alice；Alice 希望与之共享数据的用户 Bob；以及存储 Alice 数据的云服务提供商.要使用该服务，Alice 和 Bob 首先下载一个由数据处理器、数据验证器和令牌生成器组成的客户端应用程序.在第一次执行时，Alice 的应用程序会生成一个加密密钥.我们将把这个密钥称为主密钥，并假设它存储在 Alice 的系统上，并且对云服务提供商保密.云安全是根据可用性、完整性和机密性来衡量的，而加密技术很容易受到许多攻击，如：

A. 可用性

在这种情况下，云服务提供商有多个服务器.当一个服务器发生故障时，就没有安全问题，因为另一个服务器已准备好提供服务.

B. 完整性

数据的完整性是指数据的正确性和可信性.它确保了对敏感数据的计算是正确的.未经授权的用户不能更改这些数据.

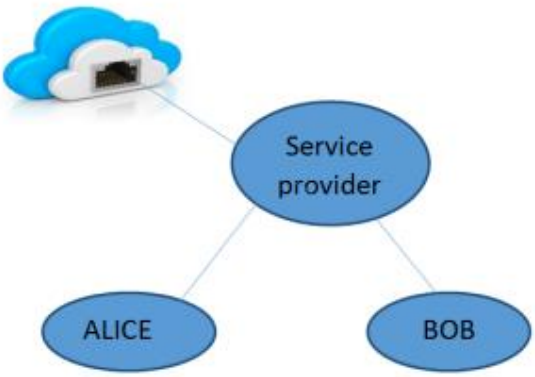

图 1 各种密码技术下的云架构

C. 机密性

机密性是为了防止攻击者接触到敏感信息，同时确保授权用户能够访问这些信息.服务要求用户使用他们的数据来信任云.但在不受信任的云计算中，数据所有者并不信任云计算.因此，对用户侧的保护是必要的.用户在存储到云之前使用公钥对数据进行加密.

D. 循环攻击

在此攻击中，密码文本被反复加密，并计算迭代次数，直到原始文本出现.它可以解密任何密码文本.

E. 密码文本攻击

在这种攻击中，明文和密码文本都是攻击者所知道的，他可以使用它来发现私有指数，一旦发现它就很容易找到.多方希望对其输入执行操作.这就需要解密他们的数据.这在不受信云的情况下带来了安全问题.

多方能否使用能够抵抗攻击的高效加密技术来存储其数据，并在不解密其数据的情况下执行计算？

4 增值目标

云环境需要用户数据的保护和机密性，同时直接利用云网络中实体的计算能力.本文关注一个吸引多种研究的问题，即云计算的数据加密.云环境要求用户数据的安全性和机密性，同时直接利用对加密数据的云网络中实体的计算能力.在本文中，我们提出了一种将多方计算与同态加密相结合的方案，以允许计算加密的数据而不需要解密.

5 我们的贡献

在本文中，我们提出了一种有效的加密技术，在多方数据加密.用户的数据使用填充方案最优非对称加密填充(OAEP)以及基于 RSASmalle 和高效 RSA(HE-RSA)的混合加密

算法进行加密.为了允许多方在其输入上计算一个函数，同时保持完整性和机密性.同态加密是对加密数据进行的，无需在计算强大的云中解密.该方案将多方计算与同态加密相结合，允许加密数据的计算无需解密.这种性质的输出允许在云环境中保持机密性和完整性.

6　用于安全云计算的加密技术

A. 初步和注意事项

$$G: \{0,1\}^{K0} \rightarrow \{0,1\}^{K0} \tag{1}$$

G 是基于散列函数的掩码生成函数使用 RFC 3447 定义的 SHA1.G 扩展 K0 位 r 到 K-K0 位.

$$H: \{0,1\}^{K-K0} \rightarrow \{0,1\}^{K-K0} \tag{2}$$

H是 SHA-256 哈希函数.H将$K-K0$位减少到 $K0$位.r是大小为$K0$的随机种子.

B. OAEP 密码系统

这是由贝拉雷和罗格威（[12]）提出的一种填充方案，它通过添加一个随机性元素来防止密文的部分解密.

编码操作

选择随机整数r，使其为$1 < r < n$.

$$r \leftarrow \{0,1\}^{K0} \tag{3}$$

$$S = (M \,||\, 0^{K1}) \oplus \mathrm{G(r)} \tag{4}$$

$$t = r \oplus H(s) \tag{5}$$

Return $s \,||\, t$

译码操作

$$r = t \oplus \mathrm{H(s)} \tag{6}$$

$$S = (M \,||\, 0^{K1}) \oplus \mathrm{G(r)} \tag{7}$$

r是大小为$K1$的随机种子.

C. HE-RSA

基于 RSASmalle 和高效 RSA(HE-RSA)[11]的混合加密算法.引入了有效的 RSA 方案，采用一般的 h 阶线性群，有意从整数 mod 环中随机选择值$n.n$被用作公钥和私钥的模量.它的长度，通常以位表示，是键的长度.

$$p,q \in prime, n = p.q \tag{8}$$

$$\varphi(n) = (p-1)(q-1) \tag{9}$$

$$\Upsilon(n,h) = (p^h - p^0)(p^h - p^1)..(p^h - p^{h-1})(q^h - q^0)..(q^h - q^{h-1}) \tag{10}$$

选择随机整数 r 使得$1 < r < n$并且$gcd(r,\Phi) = 1$和$gcd(r,\Upsilon) = 1$

计算e使得$r.e\ =\ 1mod\Phi, 1\ <e<\ \Phi(n)$

计算 d 使得$d.e\ =\ 1mod\Upsilon, 1\ <d<\ \Upsilon(n)$

公钥：(e,n)

密钥：(r,d,n)

D. 同构加密

可以使用同态加密[2], [11], [20]对加密数据执行操作.当使用密钥解密时，这些操作的结果与我们对原始数据执行的操作相同.乘法同态加密，它只允许在原始数据上的产品.

$$E(x.y)\ =\ E(x).E(y)$$

7　提出的安全云计算算法

所提出的安全云计算算法保证了云中单个数据的安全和隐私性[21], [22]，并增强了同态加密和多方计算(MPC)等安全机制.

该算法主要基于密钥生成、加密、同态加密(HE)、多方计算(MPC)和欺骗等四个阶段.其主要目标是在这四个阶段中最小化运行时间、成本和开销.在所提出的算法中，与现有的一些算法(即 RSA)相比，密钥生成过程中的指数数（在第 1 步中）得到了扩大.此外，该算法还实现了一个双重加密过程（在步骤 2 中），以防止对一些现有技术的一般攻击.在步骤 3 中，我们集成了完全同态加密和多方计算，允许在云中不解密地计算加密数据（在步骤 4 中）.

要与云中的各种服务交互并存储由这些服务生成/处理的数据，需要多种安全功能.假设 Alice 和 Bob 分别将数据发送到 M1 和 M2 到云中，在使用 HE-RSA 加密之前，使用最优不对称加密填充(OAEP)方案对爱丽丝的数据(M1)进行填充，得到密文 C1，如图所示 2.

Alices 数据 (M1) 使用 Optimal Asymmetric 填充.

算法 1 安全云计算算法

第 1 步：密钥生成算法：$keygen(p,q)$

随机选择两个大素数p ,q 并计算 $n=p.q.$

$\mathscr{O}(n)=(p\ -\ 1)(q\ -\ 1)$

$\Upsilon(n,h)=(ph\ -\ p0)(ph\ -\ p1).....(ph\ -ph-1)(qh\ -\ q0)(qh\ -\ q1).....(qh\ -\ qh-1)$

选择随机整数r使得$1\ <r<n$并且$gcd(R,\Phi)\ =\ 1$和$gcd(R,\Upsilon)\ =\ 1$

计算e使得 $r.e\ =\ 1$ 对 $\Phi, 1\ <e<\ \Phi(n)$

计算d使得$d.e\ =\ 1$对$\Upsilon, 1\ <d<\ \Upsilon(n)$

公钥(pk): (e,n)

密钥：(r,d,n)

第 2 步：加密：$Enc(M,pk)$

假设 Sender 和 Receiver 向 M1 和 M2 发送数据分别到云端

$G:\{0,1\}^{K0} \rightarrow \{0,1\}^{K0}$

$H:\{0,1\}^{K-K0} \rightarrow \{0,1\}^{K-K0}$

$r \leftarrow \{0,1\}^{K0}$

$S = (M \,||\, K1) \oplus G(r)$

$t = r \oplus H(s)$

$C \leftarrow \leq S \geq^{e} \ mod\ n \ \geq^{e} \ mod\ n$

Return C

第 3 步：同态和多方计算同态计算在 Sender 和接收方分别加密数据 C1 和 C2.

$C1 = ((M1)e\ mod\ n)e\ mod\ n$

$C2 = ((M2)emod\ n)e\ mod\ n$

$C1.C2 = [((M1)e\ mod\ n)e\ mod\ n][((M2)emod\ n)e\ mod\ n]$

$= ((M1)e\ mod\ n)e((M2)e\ mod\ n)e\ mod\ n$

$= ((M1M2)e\ mod\ n)e\ mod\ n$

$LetC = C1.C2, M = M1M2$

$C = (Me\ mod\ n)e\ mod\ n$

第 4 步：解密：Dec(C,sk)

发送者和接收者使用解密计算的数据他们各自的私钥

$W \leftarrow (Cr\ mod\ n)d\ mod\ n$

$Parse\ W\ as\ s \,||\, t$

$r \leftarrow H(s) \oplus t$

$M1 \leftarrow s \oplus G(r), parseM^{-1}\ as\ M \,||\, Z$

加密填充（OAEP）在使用 HE-RSA 加密之前的填充方案，

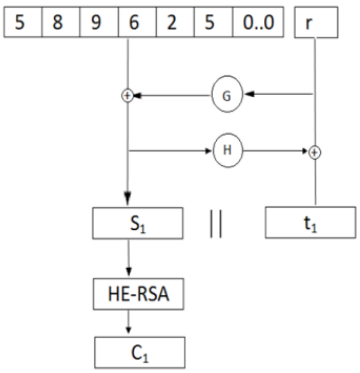

图 2 发送方数据 M1（加密过程）

产生密文 C1（如图 2 所示）.在使用 HE-RSA 加密之前，

使用最佳非对称加密填充（OAEP）方案对接收器的数据（M2）进行填充，

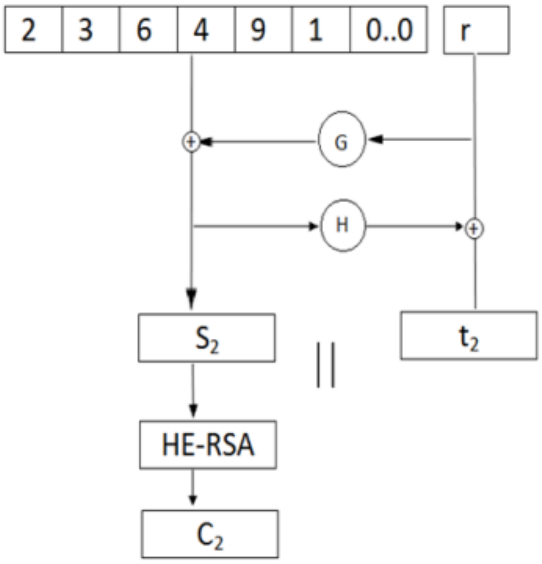

图 3 接收数据 M1（加密过程）

从而生成密文 C2（如图 3 所示）.同态加密产生的数据 C 使用发送方的私钥解密，然后使用 OAEP 解码（如图 4 所示）.由同态加密产生的数据 C 使用接收器的私钥进行解密，然后使用 OAEP 进行解码(如图所示 5).例如，同态加密要求所有用户和结果的最终接收者共享一个密钥来加密输入和解密结果，如果他们属于不同的组织，这可能很难安排.此外，同态加密不允许对使用不同密钥加密的数据进行计算（而不会产生额外的重大开销），因此用户不可能允许对他们参与计算的数据进行不同的访问.

安全多方计算(MPC)适合于利用半可信的云设置.MPC 杠杆是诚实的政党的存在，而不必要知道哪些各方是诚实的，以实现数据和计算的机密性和完整性.

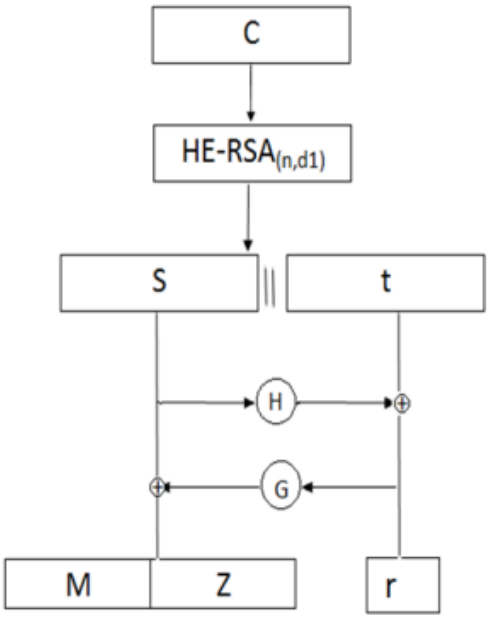

图 4 发送方数据（解密过程）

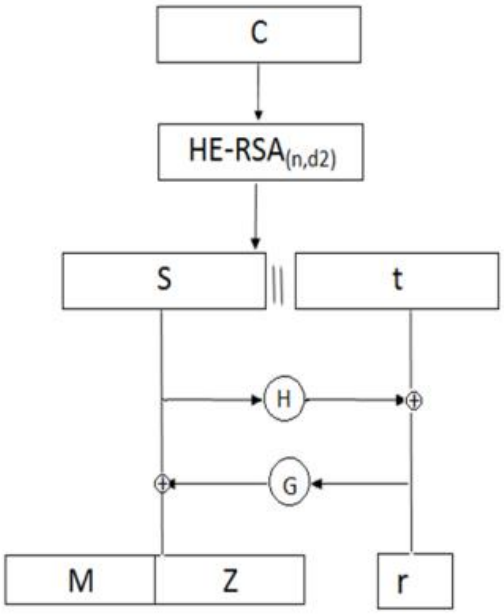

图 5 接收方数据（解密）

多方计算提供的安全保证比 FHE 更弱，但效率可以更高.在 MPC 中，没有一方了解到关于数据的任何信息，但如果有足够多的一方被对手破坏并汇集他们的信息，他们就可以破坏机密性.MPC 的相对效率，以及半可信云模型在现实世界中的适用性，使其成为更实际的安全云计算的一个很有前途的候选者.

8 结果

将同态加密和多方计算（HE+MPC）相结合后，数据的机密性和完整性得到了维护，

其开销小于同态加密，但大于多方计算.因此，我们收到了基于同态加密和多方计算的中等开销（如表 1 所示）.图 6 总结了各种计算中每种技术的近似效率和成本，描绘了在不安全计算中产生的乘法性能开销.除了效率低下之外，同态加密还有其他局限性.

表 1 加密方法的比较

密码技术	机密性	完整性	交互性	开销
HE	是	否	否	更多开销
MPC	是	是	是	更少开销
HE+MPC	是	是	是	中等开销

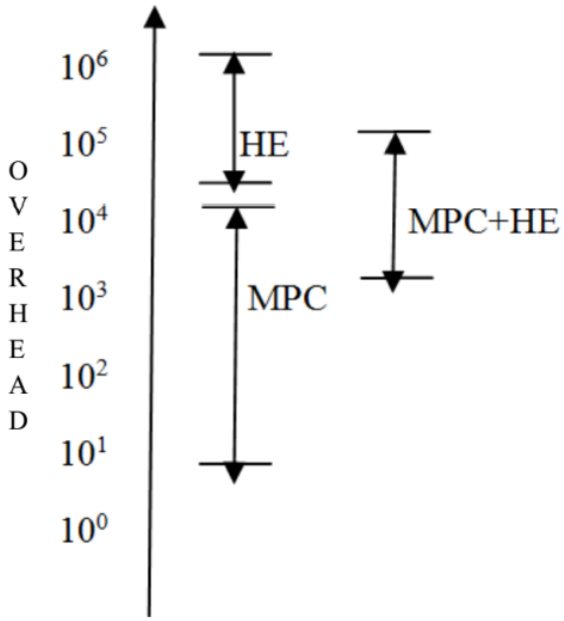

图 6 乘法性能的图形描述同态引起的不安全计算的开销加密 (HE)、多方计算 (MPC) 和同态加密 + 多方计算 (HE + MPC).

9 结论

在本文中，我们提出了一种安全的云计算模型，利用基于同态加密(HE)和多方计算(MPC)的高效加密技术加密用户数据，然后对用户数据进行操作，同时保持完整性和机密性.输出与对原始数据进行的操作相同.一方可以共同执行计算，而不向另一方透露其数据.在这里，我们设计并开发了专门为私有半可信云设置而设计的安全同态加密和多方计算技术.此设置允许开发人员将私有云与保护它所需的加密技术(即 HE+MPC)一起设计.

10 致谢

这项工作得到了美国政府科技部(DST)科学与工程研究委员会(SERB)颁发的早期职

业研究奖的部分支持.印度新德里(项目编号：ECR/2015/000256)和 2017-bilpianiK.KBirlaGoa 校园研究启动基金(RIG)奖.

参考文献

[1] Mcll P Gracc T. The NIST definition of cloud computing,NIST Special Publication,2009, pp. 800-145.

[2] Tebaa M,Haiji S.E,Ghazi A.E. Homomorphic Encryption Applied to the Cloud Computing Security,Proceedings of the world Congress on Enginecring,London,U.K.，Vol.1,No.1，2014,Pp.4-6.

[3] Wang z,Sun G,Chcn D.A new defininion of homomorphic signarure for idenfiry management in mobile cloud compuring, Journal of Computerand Systcm Scicnccs,Vo1. 80,NO.3,2014,pp. 546-553.

[4] Yakoubov s,Gadepally v, SchearN, Shen E，Yerukhimovich A.A Survey of Cryptographic Approaches to Seauring Big-Data Analyricsin the Cloud,IEEE High Performance Extreme Computing Confcrcnce(HPEC),2014, pp. l-6.

[5] Rong C ,NguyenST，Jaatun MG.Beyond lighrning: Asurvey on security challenges in cloud compufing，Computers and ElectricalEng inecring，Vol.39,No.1，2013,Pp.47-54.

[6] Gentry C.Compuring Arbitrary Foncions of Encrypted Data, Commu-nications of the ACM,vo1. 53,No. 3,2010,pp. 97-105.

[7] WngC, Wang Q.Rcn K,Lou W. Ensuring Data Storage Security inCloud Compufing, Quality of Service, 2009,Pp. 1-9.

[8] YuY. Niua L, Yang,G, Mu 'Y,Susilow.On the security of auudiring mechanisms for secuwre coud storage，Future GcncrationComputcr Systcms,Vol. 30,2014 Pp.127-132.

[9] wei'L,Zhu H,CaoZ, Dong x,JiaW, Chen Y,Vasilakos AV. Securiry and privncy for storage and computation in cloud computing,Information Scicnccs, Vol. 258,2014, Pp. 371-386.

[10] Lopez-Alt A,Tromer V,VaikuntanathanE.On-the-Fly Multiparty Computation on the Cloud via Mulrikey Fully Homomorplic Encryption,Proceaiings of the forty-fourth annual ACM symposiuim on Theory of computing, 2012,pp. 1219-1234.

[11] Brakerski Zand VaikuntanathanE.Efficient fiually homomorphic encryption from(s tandard)LWE,SIAM Joumal on Computing,Vol.43,No.2,2011, Pp. 831-871.

[12] Bellarc M. and Rogawayy P. Optimal Asymmetric Encryprion How to Encrypr with RSA，Advances in Cryptology Eurocrypt 94 Proceedings，vol.950,1995, Pp.1-19.

[13] Shen E,Varia M.Cunningham RK, Vesey WK. Cryptog raphically Secure Computation，IEEE Computcr Socicty，Vol.48,No.4，2015,pp.78-81.

[14] Zissis D, Lckkas D.Addressing cloudl computing security issues, FutureGencration Computer Systcms,Vol.28, No. 3,2012,pp. 583-592.[15] Hashem IAT,Yaqoob L,AnuRr NB,Mokhtar N, Gani A, Khan S.U.

[15]The rise of 'big data’on cloudi computing: Review and open res earchis sues,Infomation Systcms,2015,Vol.47,pp. 98-1 15.

[16]ZhouJ,Dong x,Co. z，VasilakosAv. Secure and Privacy Pres erving Protocol for Cloud-based Vehicular DTNs,IEEE Transactionson Information Forensics and Security,In formation Systems,Vo. 10，No.6,2015,Pp. 1299 -13 14.

[17]Zhao J, Wang L, Tao J, Chen J, Sun w, Ranjan R, Kolodziej J, Strcit A,Gcorgakopoulos D.A securiry framework in G-Hadoop for big datacompuring across distributed Cloud data cenires，Journai of Compuerand System Sciences,Vol.80, No.5,2014,Pp. 994-1007.

[18]Zucch R, Khoshgoftaar TM,Wald R.lntrusion detection and Big Heteogeneous Dafa: a Survey，Joumal of Big Data，Springer，Vol.2,No. 3,2015, pp.1-40.

[19]Hongbing ℃,Chunming R,Kai H,Weihongw, Yanyan L. Secure Big Data Storage aund Sharing Scheme for Cloud Teanis,ChinaCommunications,2015, pp. 106-115.

[20]Jajodia_S, Kant K,Samarati ,Singhal _A, Swarup v, WangC. Secure Cloud Compuring, Springer Scicnce+-Business Media,2014, pp.1-350.

[21]D. Das, R. Mism, A Raj Approximating Geographic Routing using Coverage Tree Heuristis for Wireless Network, Wireless Networks (WINE),Springer Us, Vol. 21. No. 4, 2015, pp.1 109-1118.

[22]T Limbasiya, D. Das, Secure Message Transmission Algoritlon for Vehide to Vehicle (V2V) Comunication, IEEE Region 10 Conference (TENCON)201 6, Technologies for Smart Nation, Singapore, 22-25 Now. 2016, Singapore, pp. 2507-2512.