# 基于同态密码方法的分布式图像加密

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。

关键字：分布式图像加密、同态加密、图像加密、PaillierCryptographicSystem、RGB 图像加密。

# 一、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。

# 二、 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

设是M行N列图像的二维数组表示，其中是每个像素的空间坐标，对于和。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=中，其中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，其中是选择为等于的素数。对于8-位图像，每个像素的强度值在区间 [0,255] 内，但我们选择=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=256，可以进行特殊处理来说明，或者映射为=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 ，对于 Zp 中的所有 ， 是一个正整数，使得 ，其中 是像素强度级别的数量。 这意味着 个像素强度子值 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

设为同态加密函数，设为图像中像素的强度值，其中 和 ，其中和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写为个像素的强度子值的总和，如下所示：

其中像素分量的数量 ，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，其中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，需要进行额外的特殊处理，其中的差值可用于求出原始像素值。 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：

(2)d 中 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 执行分布式和或并行或顺序加密处理。每个 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。此外，如果每个 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，每个可以随机生成，唯一的要求是它们的总和应等于。同样需要注意的是，的值越大，加密图像越安全，但计算成本也越高。

此外，每个加密值可能是一个非常大的整数，在相关图像的像素强度值范围 之外。 因此，为了从图像的角度使这些有意义，可以将应用于每个加密值，将它们映射回 Zp，并获得像素的强度值。范围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，可以选择为= 257。因此，我们可以写成：

将 应用于上述方程，我们有

数量 表示每个像素强度子值 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 的最大整数，也称为或的底数。它也表示当除以。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。无需重构 在接收方解密可能很困难，所以，我们可以写：

B. 同态图像解密阶段

设 ，，，，，并且一般来说 ，，是映射的各个加密像素强度子值 到 Zp，并且在接收端可用，其中是同态加密函数。另外，让 , , , ..., 是在接收端也可用的解密参数。要解密加密像素强度值 并获得像素强度值 ，必须首先重构或计算各个加密像素强度子值 ，,, ..., 和 如下：

其中 是每个值的不同常数整数。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。 首先，计算乘积。

应用解密函数给出：

请注意，从（17）到（18）的转换是使用加密函数 的同态属性实现的。 此外，如果每个像素强度子值 的加密/解密密钥不同，则可以首先解密每个 ，然后相加 得到像素强度值。 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 的特殊情况，其中是像素强度子值 的数量,我们也将其命名为像素分量的数量。

1) 分量图像的特殊情况加密阶段实现：设 和 。 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和 之和的加密等于各个加密子值和。 考虑具有加密和解密功能的 Paillier 密码系统 [3]、[18]、[24]，其中值 可以加密如下：

其中 ，并且 是两个素数，而 是一个随机数，使得，为阶数为的倍数的整数，即， 当素数 和 的长度相同时， 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 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和中的每一个 如下：

和

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

和

数量和代表对应于每个像素强度子值和的密码值。这些加密值 和表示将被传输或存储的安全图像像素强度子值。

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

和

使用方程 (16) 到 (21) 对于 k = 2，可以写成

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

和

其中，并且是素数，当和的长度与前面所述的相同时，可以设置为。 参数 由 和 的最小公倍数给出，而函数 定义为

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 。可以扩展图 1 中的分量图像同态加密子块 根据的值增加到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：针对 k = 2 个分量图像提出的特殊情况图像加密方案。

# 三、 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，质数和，每 165 位是

=1352318060071620614427506863919044316971851975663670066189817846916761074376030537953500829276656130249253598608770933002374219101956801142939 47567777974339655680621

和

=61599275563119689204225566492771724864296690581662139357940729257768885406090709024547872520964035633288261474750330107825840672796400600750 3687722380089774424939227.

和的位数分别为 546 位和 548 位。因此，用于加密的公钥 的值有 329 位和 1093 位，由下式给出

N=833018128313352036165812028938761904191512668904551362732364681607018389028803357833367866512069718197388149783138232536324446481100155132776532099225547400460018876566048064044754229926275045888767207297660757847207087214804418983183540509698865985893995996890095100921352234625385021610968 21345036062518664770571190023246619967.

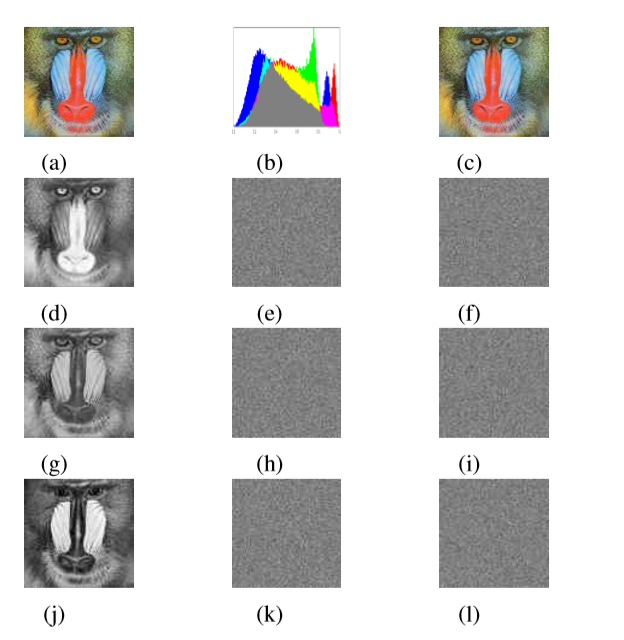
图 2 (a) 所示的原始 RGB 图像通过分离其 R、G 和 B 通道图像中的每一个进行通道处理，如图 1 和图 2 所示。分别参见2 (d)、2 (g)和2 (j)。 这些通道图像中的每一个都通过在对每个图像进行加密之前首先将其分解为两个分量图像来单独处理。例如，将图2(d)中的R-Channel原始图像R分解为此处未示出的两个分量图像R1和R2，然后进行加密以产生图2(d)所示的加密分量图像R1和R2。 分别参见 2 (e) 和 2 (f)。 类似地，G 和 BChannel 原始图像各有两个分量图像，它们被加密以产生图 1 和图 2 所示的加密分量图像 G1 和 G2。 2 (h) 和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

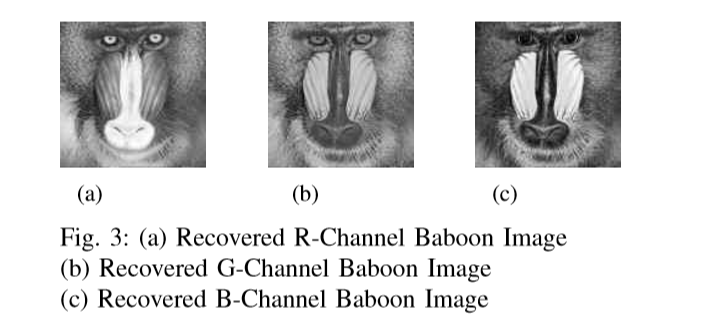
(k) 加密狒狒组件图像 B1；

(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。



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 l 是第 l 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。

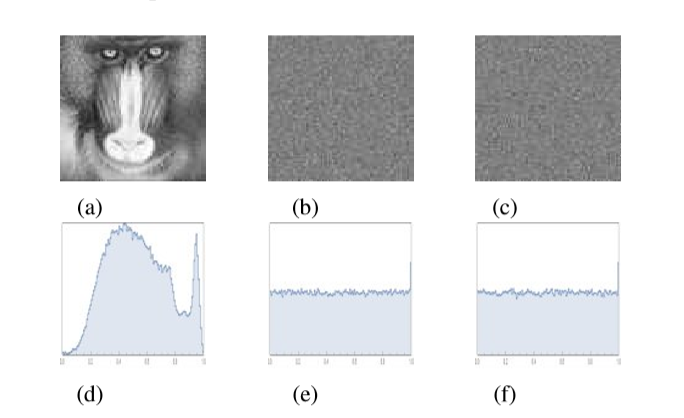


图 4：（a）原始 R 通道狒狒图像 R；

(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：

其中 N 是图像的总像素数，DR,G,B 的定义由下式给出：

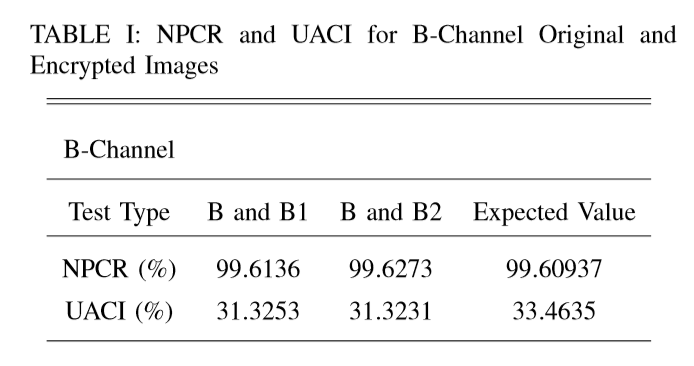
其中和分别表示图像和中相应颜色分量 R、G 和 B 的值。 给定两个随机图像，可以找到期望值的表达式为

其中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（），NPCR的期望值由下式给出：

另一方面，UACI 的表达式定义为

其中分别表示用于红色 (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

对于每个通道使用 8 位编码的 RGB 图像，我们有以下期望值：

执行和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。

D. 相关分析结果和讨论

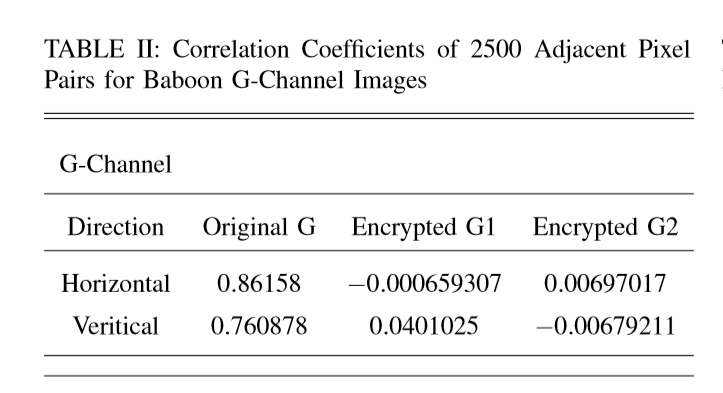
可见电磁频谱范围内的许多图像都有冗余，有时会导致水平、垂直和对角线方向的相邻像素之间存在高度相关性。 一个好的图像加密方案应该打破相邻像素之间的这种相关性并将其值降低到几乎为零； 因此，生成的图像更能抵抗统计攻击。 包括 A. Soleymani、A. Daneshgar、A. Kano [2]、[4]、[5]、[7]-[10]、[12]、[20] 在内的几位作者讨论了相关系数的表达式 , [21]。

其中和分别是和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

其中和是随机选择的相邻像素对的值，是来自图像的相邻像素对 的总数，和分别是和的平均值或期望值，并给出经过

使用方差，标准差和的表达式为：

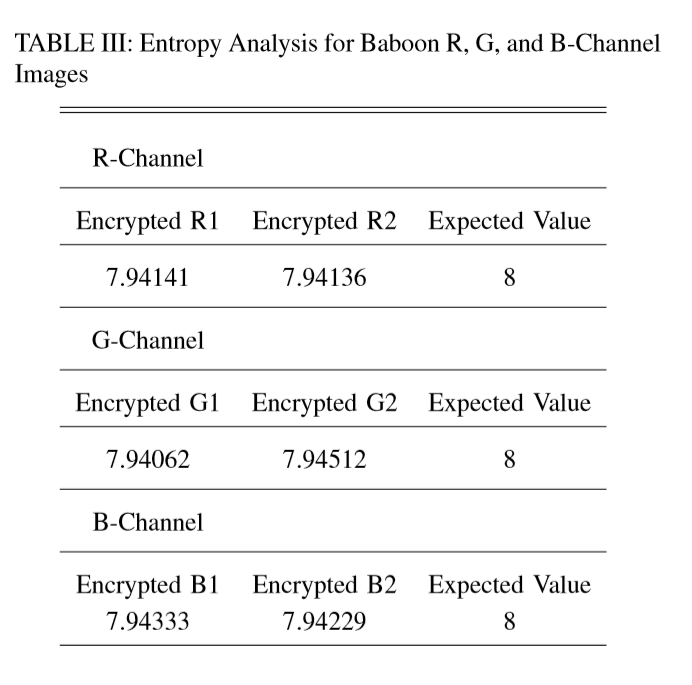
使用一组 N = 2500 个随机的水平和垂直方向的相邻像素对进行相关性分析，比较每个通道的原始图像及其相关的加密组件密码图像。 G 通道图像的这种相关性分析的结果显示在表 II 中。还对 R 和 B 通道图像进行了相关分析，它们提供了类似的结果。表二显示原始G通道图像G中相邻像素强度值对在水平和垂直方向高度相关，相关系数值接近1。然而加密分量图像G1和G2的相邻对非常不相关像素的强度值，因为相关的相关系数接近 0。这些 G 通道图像相关分析的结果也显示在图 5 中。水平和垂直方向上相邻像素对的相关性；并因此通过使它们更能抵抗统计相关攻击来提高加密图像的安全性。



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]：

其中是符号的出现概率，N 是源生成的符号总数，

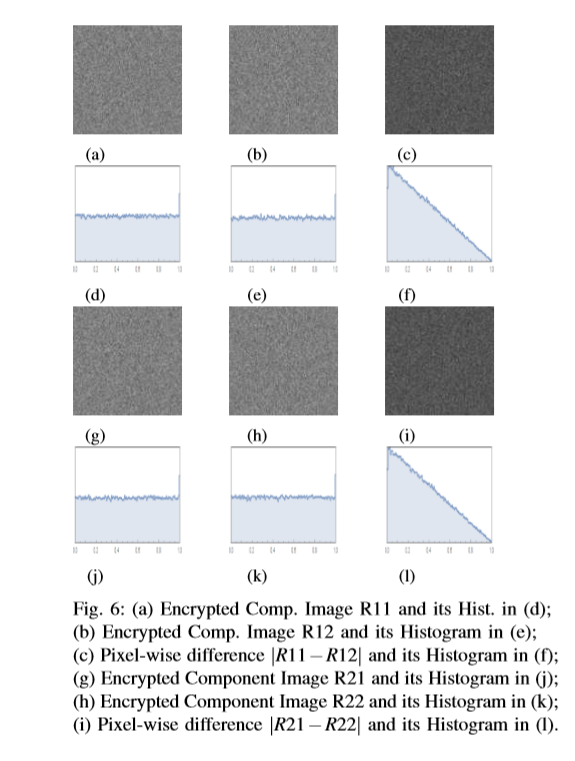


并且使用对数基数 2 来表示以位为单位的熵。 当 S 是真正的随机源时，对于所有 ，，熵可以计算为

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。

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。



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。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。

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。

# 四、 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

[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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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