# 图像类型的保密计算

成 雯[1]
CHENG Wen

**摘 要** 图像检索在涉及图像的各种应用领域具有越来越重要的地位。当进行图像检索时，在完全不同类型的图像里去检索会增加很多不必要的开销。同时很多图像中包含大量的隐私信息，如果不进行适当的保护，检索过程极易泄露隐私信息。为避免泄露隐私信息，针对图像类型是否相同进行保密判定，基于 Paillier 加密算法和 0-r 编码方法设计了一个高效、安全的协议，该协议结合图像检索方案可以减少因不同类型的图像检索的不必要性。协议不仅简单快速，并且用模拟范例证明了其安全性。

**关键词** 图像检索；安全多方计算；图像类型；Paillier；0-r 编码

doi：10.3969/j.issn.1672-9528.2024.03.043

## 0 引言

安全多方计算（secure multi-party computation，SMC）最早由姚期智教授 [1] 提出，它是指互不信任的参与者想在不泄露自己私密数据的情况下，进行合作计算进而获得期望的结果。经过几十年的发展 [2]，现已成为隐私保护不可或缺的关键技术，在信息安全 [3-4] 和网络安全 [5-6] 等方面发挥着重要的作用。

图像检索 [7] 在医疗、军事、生活等领域具有广泛应用。在计算机视觉中可以检测、跟踪目标位置，在大量图像中找到与已有模板最接近的一个图像 [8]。通过搜索引擎基于图像内容进行图像检索，常见的操作有由缩略图找原图、以图检图等。只有当图像类型相同或相似时，图像检索才是有价值的，如果是不同类型的图像，检索是没有意义的。但图像中包含大量的敏感信息，为了防止这些私人信息泄露，就需要使用安全多方计算对参与者的私有图像进行保密处理。

目前还没有学者研究图像类型的保密计算，关于图像检索安全计算的方案大多是基于云服务器对保密图像进行检索以及其他操作。用户将加密的图像上传给云服务器，云通过加密图像搜索、共享等操作将处理结果返回给用户。文献 [9] 基于 LSH（locality sensitive hashing）算法提出了保护隐私的近似图像检测方案。用户使用 LSH 算法将图像数据的密文存储在云端。当需要查询时，生成查询令牌发送到云，云将近似图像检测结果返回。文献 [10] 设计了安全有效的 NDD（near-duplicate detection）系统，将 LSH 与多密钥可搜索加密结合起来，允许用户访问在不同密钥下加密的近似图像，并设计了基于混淆电路的安全协议，以获得准确的检测结果。文献 [11] 提出了 SSIR（secure similarity image retrieval）方案，将存储、计算能力有限的客户端的图像处理以及外包搜索操作交给云，利用 SGX（software guard extension）技术提出了一种新的基于内容的图像检索安全方案。

本文针对图像类型保密计算的必要性，在判定图像类型是否一致时，基于 Paliiler 加密算法设计了一个改进方案。本文贡献如下。

（1）本文提出先判定图像类型的一致性，再进行图像检索，这样减少了不同类型图像进行检索的不必要性。

（2）在判定图像类型是否一致时，利用 0-r 编码方法设计了一个快速、安全的协议。

（3）本文提出的协议是简单快速的，当图像类型一致时，并没有增加过多的计算开销，但当图像类型不一致时，大大提高了计算效率。

## 1 预备知识

### 1.1 安全性定义

半诚实参与者：通常，半诚实参与者是指参与者在执行中会忠实地履行协议，但可能会保留中间结果，将其他参与者的私密数据或其他信息推出来。

假设 $f(f_1,f_2):\{0,1\}^*\times\{0,1\}^*\longrightarrow\{0,1\}^*\times\{0,1\}^*$ 是概率多项式函数，两个参与者的输入为 $x$、$y$，共同执行协议 $\pi$ 计算函数 $f(x,y)$。协议 $\pi$ 的输入为 $(x,y)$，执行协议时第 $i$ 个参与者接收到的消息序列记为：

$$view_i^{\pi}(x,y)=(x(y),r_i,m_1^i,\cdots,m_t^i) \tag{1}$$

式中：$r_i$ 是第 $i$ 个参与者产生的随机数，$m_j^i$ 是第 $i$ 个参与者收到的第 $j$ 个消息。输出函数定义为：

$$output^{\pi}=(output_1^{\pi}(x,y),output_2^{\pi}(x,y)) \tag{2}$$

1. 山西省财政税务专科学校 山西太原 030000

式中：$output_i^{\pi}(x,y)(i\in\{1,2\})$ 为第 $i$ 个参与者的输出。

定义 1 半诚实协议的安全性。假设参与者都是半诚实参与者[12]，如果存在概率多项式时间算法 $S_A$、$S_B$，使得下式成立，则认为协议 $\pi$ 保密地计算了 $f$。

$$\{S_A(x,f_1(x,y)),f_2(x,y)\}_{x,y}\overset{c}{\equiv}\{view_1^{\pi}(x,y),output_2^{\pi}(x,y)\}_{x,y} \quad (3)$$

$$\{f_1(x,y),S_B(y,f_2(x,y))\}_{x,y}\overset{c}{\equiv}\{output_1^{\pi}(x,y),view_2^{\pi}(x,y)\}_{x,y} \quad (4)$$

式中：$\overset{c}{\equiv}$ 表示计算不可区分。

1.2 Paillier 加密算法

Paillier 加密算法[13]一般由以下三个算法组成。

（1）*KeyGen*：选取安全参数 $k$，选择两个素数 $p$、$q$，其中 $N=p\times q$，$\lambda=lcm(p\text{-}1,q\text{-}1)$ 是 $p$-1 和 $q$-1 的最小公倍数。随机选择 $g\in Z_N^*$ 使得 $\gcd(L(g^{\lambda}\bmod N^2),N)=1$ 定义为 $L(x)=\frac{x-1}{N}$。算法的公钥为 $(g,N)$，私钥为 $\lambda$。

（2）*Encrypt*：选择随机数 $r\in Z_n^*$，计算明文 $m$ 对应的密文。

$$c=E(m)=g^m r^N \bmod N^2 \quad (5)$$

（3）*Decrypt*：为解密密文 $c$，计算：

$$m=D(c)=\frac{L(c^{\lambda}\bmod N^2)}{L(g^{\lambda}\bmod N^2)}\bmod N^2 \quad (6)$$

Paillier 算法加密过程需要选择随机数参与运算，因此对于相同的明文选用不同的随机数会产生不同的密文，算法具有加法同态性，具体如下：

$$E(m_1)E(m_2)=E(m_1+m_2) \quad (7)$$

$$E(m_1)^{m_2}=E(m_1m_2) \quad (8)$$

为简便计算，本文选取的 $g$ 都为 1+$kN$（$k$ 为正整数）形式，在加密、解密时，都仅需要一次模指数运算。

## 2 图像类型的保密判断

虽然已有多位学者图像检索进行了研究，但本文与之前研究不同，考虑到图像类型不同而进行检索是完全没有意义的，本文提出了图像类型的保密判断方案。

当进行图像检索时，希望得到的是相同类型的图像，假设被检索的图像是人物类的，那么在风景类、建筑类等图像里去检索则没有任何意义。为了减少不必要的计算，本文在图像检索之前要先保密地判断图像是否属于同一类型。

对图像类型进行保密判断时，直接判断在实际操作中不方便，所以本文将所有图像类型表示到一个大集合中，就可以将问题转化为判断对应位置的集合元素是否相同。具体步骤如下。

（1）将所有的图像类型表示为一个大集合，集合中的元素按照双方商定的顺序进行排列。

（2）判断图像类型是否相同，其实就是比较对应位置的集合元素是否相同。分别选择图像类型对应的集合元素，若图像类型一致，则选取到的集合元素必然相同；反之，集合元素必然不同。

2.1 问题描述及计算原理

问题描述：Alice 和 Bob 各自拥有一张图像，现要保密判断两张图像的类型是否一致。

计算原理：假设他们拥有的图像类型分别为 $x_1$、$x_2$，首先商定图像类型集合为 $T=\{t_1,\ldots,t_n\}$，分别代表人物类、食物类、风景类等，其中 $x_i(i\in\{1,2\})\in T$。若 $x_i=t_k$，则记 $x_i$ 的序号为 $(x_i)_{ind}=k$，这样就将判断图像类型是否相同，转化为了判断集合中对应位置的元素是否相同，可以利用 0-r 编码方法解决。

本文在多数据相等的保密判定协议[14]上进行了改进。具体如下：Alice 按照 0-r 编码方法将 $x_1$ 进行编码，得到数组 $v$ 并发送给 Bob。Bob 根据 $x_2$ 在集合中的对应位置进行挑选，若 $v_{x_2}$ 为 0，则图像类型一致；反之则不属于一类。

编码方法：参与者将自己的数据 $x_i$，通过以下方法表示为对应的数组 $v$，其中：

$$v_i=\begin{cases}0, & x_i=t_i,\\ r_i, & otherwise.\end{cases} \quad (9)$$

为方便描述，假设图像类型都用数字来表示，Alice 拥有的图像类型为 2，Bob 拥有的图像类型为 3，共同商议的图像类型集合为 $T=\{1,2,3,4,5,6,7,8,9,10\}$。

Alice 按照上述编码方法得到数组 $v$，将数组 $v$ 发送给 Bob。Bob 选择对应第 3 位的数组元素 $v_3$，$v_3$ 是一个随机数，表示两张图像并不属于同一类。在这种情况下，图像检索是没有意义的。

有些图像类型难以明确，如同时有人物、风景、建筑或食物类等内容时，会涉及如何界定。双方在明确图像类型集合的排列顺序后，Alice 可以利用 1-0 编码方法，选择对应的图像类型位置都设定为 1，其余为 0。而 Bob 则选择所有图像类型对应的位置。假设共同商议的图像类型集合为 $T=\{1,2,3,4,5,6,7,8,9,10\}$，Alice 拥有的图像类型为 2、3、7，则得到数组 $v=\{0,1,1,0,0,0,1,0,0,0\}$。Bob 拥有的图像类型为 3、7、9，则选择对应第 3、7、9 位的数组元素 $v_3$、$v_7$、$v_9$，其中 $v_9=0$ 是一个随机数，$v_3=v_7=1$。因此计算 $c=v_3+v_7+v_9=2$，两张图像是有部分类型相同的，进一步结合图像检索方案进行计算。若两个图像类型完全不一致，即 $c=0$，则没有必要检索该图像。

为叙述简单，定义 $T(P_1,P_2)$ 如下：

$$T(P_1,P_2)=\begin{cases}1, & \text{图像类型一致}\\ 0, & \text{其他.}\end{cases} \quad (10)$$

2.2 图像类型的保密判定协议

协议 1 图像类型的保密判定协议

输入：Alice 输入图像 $P_1$，Bob 输入图像 $P_2$。

输出：$T(P_1,P_2)$

准备阶段：Alice 和 Bob 共同确定图像类型集合 $T=\{t_1,\ldots,t_n\}$。

（1）Alice 将自己图像类型 $x_1$ 得到数组 $v=\{v_1, \ldots, v_n\}$，其中 $v_i = v_{(x_1)_{ind}} = E(0)$，并选取 $n-1$ 个随机数 $r_k (k \neq i,\ r_k \in Z_n^*)$ 使得 $v_k = r_k$，将数组 $v$ 发送给 Bob。

（2）Bob 选取随机数 $r(r \in Z_n^*)$，并根据 $x_2$ 选择 $v_{x_2}$，计算 $c = v_{x_2}^r$，将 $c$ 发送给 Alice。

（3）Alice 进行解密。如果 $D(c)=0$，公布 $T(P_1, P_2)=1$，否则公布 $T(P_1, P_2)=0$。

这里需要注意的是，当出现图像类型难以明确时，只需将协议 1 修改为协议 2，如下文所示。

（1）Alice 将自己图像所属类型 $X$（长度为 $m$）按照 1-0 编码方法得到数组 $v=\{v_1, \ldots, v_n\}$，其中 $v_i = v_{(X_i)_{ind}} = E(1)$（$i \in \{1, \ldots, m\}$），并选取 $n-m$ 个 $E(0)$ 使得 $v_k = E(0)$，将数组 $v$ 发送给 Bob。

（2）Bob 选取随机数 $r(r \in Z_n^*)$，并根据自己的图像类型 $Y$（长度为 $l$）选择 $v_{Y_j}$（$j \in \{1, \ldots, l\}$），计算 $c = v_{Y_1} \cdots v_{Y_l}^r$，将 $c$ 发送给 Alice。

（3）Alice 用私钥进行解密。如果 $D(c)=0$，公布 $T(P_1, P_2)=0$，否则公布 $T(P_1, P_2)=1$。

## 3 方案分析

### 3.1 协议 1 分析

正确性分析：Alice 和 Bob 共同确定集合 $T$，如果 Alice 和 Bob 的图像类型是一致的，那么 Bob 通过挑选得到的是 0；如果图像类型不一致，Bob 挑选到的必然是随机数。由于 0 和随机数 $r$ 相乘仍为 0，某个随机数和随机数 $r$ 相乘结果也为随机数，所以 Bob 选取随机数 $r$ 经过计算得到 $c$ 后，依然可以保持结果的区分性。而 Alice 通过解密，就可以判断图像类型是否相同。

安全性分析：由于 Alice 拥有私钥可以解密，如果 Bob 挑选完直接发给对方，会泄露信息，但是 Bob 选取随机数 $r$ 重新计算后，在保证正确性的同时，也不会让 Alice 了解额外信息。而 Bob 没有私钥，他得到的都是与随机数不可区分的密文。因此协议 1 是安全的。

**定理 1** 协议 1 在半诚实模型下是安全的。

证明：通过构造满足等式（3）和（4）的模拟器 $S_A$、$S_B$ 来证明定理 1。

首先为 Alice 构造满足（3）式的模拟器 $S_A$。

接收到输入 $(P_1, T(P_1, P_2))$ 后，$S_A$ 做如下模拟。

（1）根据输入 $(P_1, T(P_1, P_2))$ 随机选择 $P_2'$，使得 $T(P_1, P_2') = T(P_1, P_2)$。

（2）$P_1$ 根据图像类型 $x_1$ 按照协议 1 中所描述的方法构造数组 $v$。

（3）$P_2'$ 根据图像类型 $x_2'$，在数组 $v$ 中选择数据 $v_{x_2'}$，并选择随机数 $r'$ 计算 $c' = v_{x_2'}^{r'}$。

通过计算得到结果 $T(P_1, P_2')$。令：

$$S_A(P_1, T(P_1, P_2')) = \{P_1, c', T(P_1, P_2')\} \quad (11)$$

在协议 1 中：

$$view_1^{\pi}(P_1, P_2) = \{P_1, c, T(P_1, P_2)\} \quad (12)$$

$$output_1^{\pi}(P_1, P_2) = output_2^{\pi}(P_1, P_2) = T(P_1, P_2) \quad (13)$$

式中：$P_1$、$P_2$ 是 Alice 和 Bob 的输入，$c$ 是 Bob 计算后发给 Alice 的。

按照协议 1，Alice 得到的 $c$ 包含 $x_2$ 和随机数 $r$，并不能得到 $x_2$ 的值。模拟器 $S_A$ 得到的 $c'$ 也包含 $x_2'$ 和随机数 $r'$，Alice 也得不到 $x_2'$ 的任何信息。所以 $c \overset{c}{\equiv} c'$，故：

$$\{S_A(P_1, T(P_1, P_2)), T(P_1, P_2)\}_{P_1, P_2} \overset{c}{\equiv} \{view_1^{\pi}(P_1, P_2), output_2^{\pi}(P_1, P_2)\}_{P_1, P_2} \quad (14)$$

同样地，可为 Bob 构造满足式（4）的模拟器 $S_B$ 使得

$$\{T(P_1, P_2), S_B(P_2, T(P_1, P_2))\}_{P_1, P_2} \overset{c}{\equiv} \{output_1^{\pi}(P_1, P_2), view_2^{\pi}(P_1, P_2)\}_{P_1, P_2} \quad (15)$$

### 3.2 协议 2 分析

正确性分析：两个参与者共同商定图像类型集合 $T$, 若 Alice 和 Bob 的图像类型完全一致，Alice 经过 1-0 编码方法得到的数组，Bob 经过挑选后得到的全部都是 1，与随机数相乘为随机数，经过 Alice 解密后得到随机数，应进一步结合图像检索方案进行计算。若 Alice 和 Bob 的图像类型部分一致，Bob 经过挑选后得到的部分是 1，部分是 0，经过计算后得到的数据为大于等于 1 的整数，与随机数相乘仍为随机数，两张图像有部分相似应进一步结合图像检索方案进行计算。若 Alice 和 Bob 的图像类型完全不一致，Bob 经过挑选后得到的全部都是 0，0 与随机数相乘为 0，经过 Alice 解密后得到结果为 0，可知两张图像类型完全不一致，不需要进行后续的图像检索。

通过分析可知，Alice 通过解密结果为随机数或 0，就可以判断复杂场景下的图像类型是否相同。

安全性分析：由于 Alice 拥有私钥，如果 Bob 挑选完直接发给对方，经过 Alice 解密后会泄露信息，但是 Bob 选取随机数 $r$ 重新计算后，保证正确性的同时，也不会让 Alice 了解额外信息。而 Bob 没有私钥，他得到的都是与随机数不可区分的密文。因此协议 2 是安全的。

**定理 2** 协议 2 在半诚实模型下是安全的。

证明：可分别为 Alice 和 Bob 构造满足等式（3）和（4）的模拟器 $S_A$、$S_B$ 来证明定理 2。此处不再详细说明。

## 4 效率分析

本文提出了保密判断图像类型的方案，可以避免在图像类型不一致时进行不必要的计算。由于本文提出的协议都是基于两方的，并且目前没有文献研究保密判定图像类型。因此只对本文协议进行效率分析，并对方案的执行时间与相似度准确性进行模拟实验。

计算复杂性：为了方便计算，只考虑最耗时的模指数运算。Paillier 加密算法中加密、解密、密文模指数一次都只需要一次模指数运算。

协议 1 中不论集合范围有多大，Alice 只需加密集合对应位置的元素，其余位置均为随机数。因此 Alice 加密、解密

各需要 1 次模指数运算，Bob 计算密文模指数需要 1 次模指数运算，共需要 3 次模指数运算。

通信复杂性：使用通信次数来分析协议的通信复杂性。

协议 1 共需要 3 次通信。协议 1 的计算复杂性和通信复杂性分析结果如表 1 所示。

表 1 计算复杂性和通信复杂性分析结果

| | 参与者个数 | 模指数运算次数 | 通信次数 |
|---|---|---|---|
| 协议 1 | 2 | 3 | 3 |

由表 1 可知，协议 1 的计算复杂性和通信复杂性很小，同时减少了不同类型图像进行检索的不必要性。

实验测试：为了进一步验证协议的效率，通过模拟实验来测试方案的执行时间及准确性。实验测试环境为 Windows 10，64 位操作系统，处理器参数为 Intel(R) Core(TM) i5-4590S CPU@3.00GHZ，4 GB 内存，用 Java 语言编程实现，忽略了协议预处理时间。

实验选取协议 1 中集合范围为 10，并选取 100 次实验的平均运行时间作为实验结果。由实验结果可知，其中 1、2、7、8 组图像类型不同，其余组图像类型相同。当图像类型不同时，方案平均运行时间为 4.5 ms; 当图像类型相同时，方案平均运行时间为 41.4 ms。综上所述，模拟实验中方案运行时间都很短，证明协议 1 是高效的，实验结果如图 1 所示。

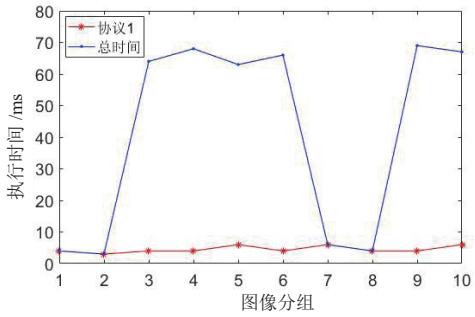


图 1 不同图像分组的方案执行时间

## 5 结论

本文利用 Paliiler 加密算法，提出了对图像类型一致性进行保密判定，结合 0-r 编码方法，设计了图像类型的保密判定协议。当图像类型一致时，没有增加过多的计算开销；但在图像类型不一致时可以大大提高图像检索效率。今后将继续研究高效、快速的图像检索方法，并将其应用到更多的场景中。

**参考文献：**

[1] YAO A C. Protocols for secure computations[C]//The 23rd IEEE Symposium of Computer Science.Piscataway:IEEE, 1982: 160-164.

[2] GOLDREICH O, MICALI S, WIGDERSON A. How to play any mental game[C]//The 19th Annual ACM Conference on Theory of Computing. New York:ACM, 1987: 218-229.

[3] 吴丽进，何金栋，谢新志．云计算环境中的计算机网络安全技术 [J]. 信息技术与信息化，2018,224(11):113-115.

[4] DUAN R, GU C X, ZHU Y F, et al. An identity-based fully homomorphic encryption over NTRU lattice[J]. Acta electronica sinica, 2018, 46(10): 2410-2417.

[5] 苏盛辉，孙国栋．基于多离散对数问题的公钥密码的分析 [J]. 电子学报，2018, 46(1): 218-222.

[6] 成雯，李顺东，王文丽．秘密区间与阈值的保密判定 [J]. 计算机科学与探索，2020,14(5):760- 768.

[7] LIU H, ZHAO Q J, WANG H, et al. An image-based near-duplicate video retrieval and localization using improved edit distance[J]. Multimedia tools appl, 2017, 76(22): 24435-24456.

[8] FUCHS K, GRUNDMANN T, FLEISCH E. Towards identification of packaged products via computer vision: convolutional neural networks for object detection and image classification in retail environments[C] //The 9th International Conference on the Internet of Things. New York: ACM, 2019: 26:1-8.

[9] WU Y L, WANG X, JIANG Z L, et al. Towards secure cloud data similarity retrieval: privacy preserving near-duplicate image data detection[C]//The 18th Algorithms and Architectures for Parallel Processing International Conference. Berlin: Springer, 2018:374-388.

[10] CUI H L, YUAN X L, ZHENG Y F, et al. Enabling secure and effective near-duplicate detection over encrypted in-network storage[C]//The 35th Annual IEEE International Conference on Computer Communications. San Francisco, USA. New York:ACM, 2016:1-9.

[11] YAN H Y, CHEN Z, JIA C F. SSIR: secure similarity image retrieval in IoT[J]. Information sciences, 2019,479:153-163.

[12] GOLDREICH O. The fundamental of cryptography: basic applications[M]. London: Cambridge University Press. 2004.

[13] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//International Conference on the Theory and Application of Cryptographic Techniques Prague. Berlin:Springer, 1999: 223-238.

[14] 窦家维，李顺东．数据相等问题的安全多方计算方案研究 [J]. 电子学报，2018, 46(5): 1107-1112.

**【作者简介】**

成雯（1996—），女，山西晋中人，硕士研究生，助教，研究方向：信息安全、密码学等。

（收稿日期：2023-07-21）