基于差分拓展的近似缩略图保持加密技术

一．摘要：

二．关键词：差分拓展，缩略图保持，图像加密

三．介绍

1.背景介绍

随着移动网络以及摄像头的飞速发展，再加上人民生活水平的不断提高，越来越多人利用电子设备记录生活的点点滴滴，并将其上传到第三方例如阿里、华为、谷歌等提供的云平台存储空间中。这些第三方平台在一方面为我们存储管理照片提供了便利，使我们的电子设备可以腾出更多的空间来拍摄新的照片，但从另一方面来说，却将我们的个人隐私置于危险之中。

目前，个人隐私保护也越来越得到国家和社会的关注，很多平台在数据存储方面都新增了加密功能，更好地保存了用户的隐私。但在在线图片预览方面却存在着隐私性与可用性的矛盾，隐私性要求我们要将图片加密存储，但可用性又要求我们需要为用户提供在线缩略图预览，以便用户管理自己的图片，若用户的每次预览访问都需要平台先解密图片再生成缩略图，这将为平台造成很大的计算负担。为了均衡隐私性和可用性，缩略图保持加密技术越来越重要。

2.已有方法

目前已有各种加密方式来达到此要求，这些方法基本都是以块为单位，独立地对每个块进行操作，使其加密后的块平均像素仍然和原图块平均像素近似甚至达到一样的效果。例如特殊的加密方法TPE【1】；利用对图像块内的像素进行伪随机洗牌来达到缩略图保持加密【2】，这种方法操作简单，且能将缩略图完全保持，但又暴露了平均像素甚至块内像素列表，且不好进行压缩。或者是通过动态区间保留加密【3】方法，只加密低LSB位，使加密后的块内像素仍然保持在一定范围内，从而使加密后平均像素与原平均像素相差无几以达到加密前后缩略图基本一致的效果，但此种方法存在解密失败的可能性。还有利用LSB嵌入【3】来进行调整的方法，将加密后的图像各像素高低位反转，通过调整高位值使得块平均像素基本与加密前保持基本一致以达到加密前后缩略图近似的效果，然而，由于改变了加密后的最低位，在解密时，像素的低位无法恢复，导致解密后的图像与原图不完全一致。如今，这方面的技术越来越多，但也都有优有劣。

3.我们的方法

在了解了图像信息嵌入的方法后，我们考虑将信息嵌入与图像加密相结合，以达到加密的特殊要求——缩略图保持。文献【4】介绍了在加密前进行腾空间，在加密后进行信息嵌入的方法，既保护了图像的隐私，又能满足信息嵌入效果。文献【5】介绍了基于差分扩展的信息嵌入，既简单方便，又有大容量的空间。我们的基于差分扩展的近似缩略图保持加密方法采用腾空间、加密、调整格式，以块为单位，块内分调整区以及嵌入区，在嵌入区利用差分扩展将调整区的MSB位嵌入保存，然后进行常规的图像加密，加密后通过调整调整区像素的MSB位以达到其缩略图与原图像缩略图基本一致的效果。

我们的方法没有使加密前后的缩略图完全一致，一方面保护了用户的隐私，对图像的细节部分模糊化，另一方面降低了计算复杂度以及腾空间强度。当然我们的近似化程度是可以通过变化MSB大小调整的，MSB越大，得到的缩略图与原缩略图越一致，但同时所需要的空间也越大。与LSB嵌入方法不一样的是，我们的方法是完全可逆的，恢复后得到的图像与原图像完全一致，是无损的。

正文

结论

参考文献