一种基于无权值向量的改进EMD图像密写算法

张 洋11, 邵利平21)\*

1) (陕西师范大学计算机科学学院 西安 710119)  
2) (中文工作单位名称 中文城市名 邮编)  
(通讯作者的E-mail地址)

**摘 要**:正文传统EMD算法使用基向量组合出的权值向量生成连续正整数嵌入秘密信息,因此权值向量组合出的非连续正整数未得到利用,限制了秘密信息的嵌入范围,同时基向量的存在降低了密写的安全性,针对以上问题,提出一种无权值向量的改进EMD图像密写算法,在该算法中无基向量且对嵌密元素和最大可改变的嵌密元素进行随机生成,避免密写分析者获取到基向量后直接提取出秘密信息,并针对固定的嵌密元素和最大可改变的嵌密元素生成嵌密元素调整表组合出所有可嵌密的情况,使秘密信息的嵌入量达到最大,同时置乱嵌密元素调整表,进一步增强密写安全性。实验表明,与传统EMD算法相比,所提算法在保证相同的视觉质量的情况下,嵌入的秘密信息数量最多,同时安全性最高。（方正书宋8.5磅）.

**关键词**:关键词1; 关键词2; 关键词3; 关键词4  
中图法分类号: TP391.41

#### Title（英文题目每个实词首字母大写）（Times *N*ew Roma*n* 13.5磅）

##### Author 11,2), Author 21)\*, a*n*d Author 32)（如Wa*n*g Yi*n*g, Wa*n*g Xiaoyi*n*g）

1) (英文工作单位, 英文城市名 邮编)（英文单位每个单词全拼,每个实词首字母大写；英文单位名称和城市名排斜体；邮编排正体）  
2) (英文工作单位, 英文城市名 邮编)

**Abstract**: text.

###### **Key words:** text1; text1; text3; text4

**0引言**

近年来,伴随着计算机和网络技术的发展,越来越多的图像在网络中传输,在给用户提供方便的同时,也带来了一系列的安全隐患。对图像的不当使用和恶意篡改,不仅会涉及个人隐私,也会给社会带来严重的负面影响。

针对数字图像信息安全,人们已提出了多种方法,如：①将明文图像转换为密文图像的数字图像加密技术；②将秘密信息隐藏于非相关载体中的数字图像隐写技术；③给图像添加版权认证标识,对图像的真实性和完整性,来源者和使用者进行认证的数字图像水印技术；④结合现有技术特点对图像的真实性和完整性进行甄别的数字图像盲取证技术以及⑤将机密图像拆分为影子图像,利用部分分发影子图像重构秘密图像的数字图像信息分存技术。

其中,数字图像隐写技术是利用数字图像的冗余和人类视觉的掩蔽特性,来将秘密信息隐藏于非相关的图像载体中,从而进行隐蔽通信,使得非法攻击者难以从海量的公开传输图像中提取出隐蔽的秘密信息信息,从而最大程度地保障传输中的机密信息的安全。

针对数字图像隐写,人们已经提出了多种数字图像密写嵌入方法。例如致力于提升秘密信息嵌入容量的BPCS方法[1]和PVD方法[2]以及致力于提高图像视觉质量的EALSBMR方法等。

现有的图像密写方法通常分为2类,空域密写方法和变换域密写方法。比较典型的变换域密写方法主要有F3密写,F4密写和F5密写方法等,它们都是载体图像DCT变换后,在量化后的非零DCT系数上嵌密,但由于量化后的DCT系数中零值较多,因此秘密信息嵌入量极低。相对于变换域密写方法,空域密写方法不仅能提供较大的嵌入容量,也能较大地保持嵌密图像的视觉质量。

最早期的空域密写方法为LSB密写嵌入方法,即用秘密信息替换载体图像的最低比特位,由于载体图像最低比特位全部携带秘密信息,而图像的最低比特位对图像视觉质量影响极小,因此LSB密写秘密信息的嵌入量大,密写图像视觉质量高,但秘密信息易改变低位信息比特的统计特性,因此安全性不高。对LSB密写方法的改进,引入了LSBM方法[4],即LSB匹配方法,相对于LSB密写方法,LSB匹配方法的策略是,当秘密信息和载体图像的最低比特位相同时不做改变,否则随机的对载体图像像素值加减1,由于像素值整体增加或减少的概率相等,因此可抵抗简单LSB密写分析方法,但其秘密信息的嵌入容量相比于LSB密写并未实质地提高。为减轻对载体的影响,后续又提出了LSBMR密写方法[5],即即LSB匹配重访方法,其原理是在两个连续的像素中最多只对其中一个加减1从而嵌入2比特秘密信息,由于LSBMR方法不是直接用秘密信息替换载体图像的最低比特位,且明显降低了对载体图像的修改率,因此,LSBMR方法在提高密写图像质量的基础上提高了其安全性。为了进一步提高图像的嵌入质量,EALSBMR方法[6]被提出,即边缘自适应LSB匹配重访方法,可根据秘密信息长度和载体图像自身平滑程度自适应的嵌入秘密信息,优先选择图像较粗糙区域进行嵌入,避免了对载体图像平滑区域的修改,因此EALSBMR密写方法下的密写图像图像质量较之LSBMR更好。

LSBMR方法最独特的地方是对两个载体数据中至多改变一个便可嵌入两比特秘密信息。这也为后面进行更大容量嵌入的EMD方法提供了很多借鉴。EMD方法,即全方向扩展方法,是对载体进行微小修改以进行大容量嵌入的一种有效的嵌入方法[7],通过对*n*个载体数据最多加减1来嵌入一个进制的数。为进一步提高嵌入容量,文献[8]给出了EMD-2方法和2-EMD方法,EMD-2方法允许对*n*个载体数据最多进行2个加减1而嵌入一个更大进制的数,2-EMD方法即连续用两次EMD方法可嵌入一个进制的数,相比于EMD方法,EMD-2方法和2-EMD方法更大程度的提高了秘密信息嵌入容量。在EMD方法的基础上也能实现对载体数据的全方位改变,即[9],即在n个载体数据的每一位都可能改变的基础上嵌入一个进制的数,带来更大的嵌入容量。

但现有的EMD嵌入方法还存在着很多问题,还有很多提升空间,主要表现在：

1) 传统的EMD方法通常采用特定的权值向量,以*n*个载体数据进行调整嵌入的EMD方法为例,对于简单EMD方法,其嵌入的权值向量为；对于EMD-2方法,当*n*=2时,其嵌入的权值向量设定为(1,3),当*n*>2时,其嵌入的基向量设定为；对于EMD-*n*方法,其嵌入的权值向量被设定为3的幂次。而特定的嵌入策略降低了密写的安全性,若知道对应的密写方法和获取对应的密写载体,则可从中容易地提取嵌入的秘密信息。

2)传统的EMD嵌入方法通常只能利用权值向量进行组合形成的1为起始的连续组合数以及0即不进行调整来作为秘密信息的表达范围,这使得权值向量不能进行充分有效的组合,从而限制了秘密信息的表达范围,使得嵌入容量十分有限。对于EMD-2方法,其嵌入的容量通常达不到其嵌入的理论值。

对于传统的简单EMD方法和MED-*n*方法,尽管能达到该调整范围内的最大的嵌入容量,但传统的EMD方法仅能提供有限的几种调整方案,例如对*n*个载体数据仅调整1个的简单EMD方法,对*n*个载体数据仅调整2个的EMD-2方法和对*n*个载体数据调整*n*个载体数据的EMD-*n*方法,由此严重制约EMD方法的适用面,使得EMD方法不能在图像视觉嵌入质量和嵌入容量上进行较好地折中。

**1EMD(*n*,*m*)**

**1.1**EMD经典模型

EMD算法基本模型一致,包括*n*个载体数据组成的向量,基向量,取模参数*X*,秘密信息为*d*,以及由定义的函数*f*,如式(1),

 (1)

根据*f*与*d*的关系式修改对应的从而嵌入秘密信息。EMD算法中,,因此, EMD算法原理：*n*个载体数据中最多一个加减1从而嵌入一个进制的数。假设待嵌入的秘密信息为*d*,若,则不改变,否则记*s*为式(2)：

 (2)

根据*s*与*n*的关系将对载体数据的改变分为以下两种情况,如式(3)：

(3)



EMD算法处理溢出时的情况：将要溢出的数向欲溢出的反方向改变1后重新在新的数据上嵌密。

**1.2**EMD(*n*,*m*)算法

由于EMD算法中基向量必须生成连续正整数，因此基向量组合情况有限，组合出的非连续正整数未得到利用，因此限制了可嵌入的秘密信息序列长度，本文提出EMD(*n*，*m*)算法无基向量且可充分利用嵌密元素个数和最多可改变发的嵌密元素个数生成秘密信息组合数和嵌密元素调整表，根据秘密信息组合数求得可嵌入的秘密信息序列长度，进而转换为十进制数*d*，取嵌密元素调整表的第*d*行和载体元素序列进行设定的计算即可得到嵌密元素序列，根据嵌密元素序列和载体元素序列的差值序列即可得到秘密信息。EMD(*n*，*m*)充分利用嵌密元素个数和最多可改变发的嵌密元素个数的组合情况，达到最大嵌入容量。

EMD(*n*，*m*)算法中直接给定*n*和*m*，按式(4)计算*n*个嵌密元素最多改变*m*个嵌密元素所能嵌入的秘密信息组合数，

 (4)

式(1)中，表示*n*个嵌密元素仅改变*i*个元素所对应的组合数, 表示被改变的*i*个元素进行调整的全部情况。

将中的数按顺序用3进制数表示三进制数中的0,1,2分别取-1,0,1，将转换后的-1,0,1序列中非零元素个数不大于*m*的序列添加到维嵌密元素调整表中。按式(5)计算应截取的秘密信息的长度，

 (5)

式(5)中，为剩余秘密信息序列长度，从载体图像对应的一维序列中取*n*个元素作为载体序列，取嵌密元素调整表的第*d*行(*tdi*)*n*，按式(6)计算嵌密元素序列。

 (6)

式(6)中，为溢出避免函数，用于避免，，具体执行的功能如式(7)所示：

 (7)

根据*n*，*m*计算嵌密元素调整表 ，取载体图像和嵌密图像对应的*n*个元素，计算其差值序列，在中找到此序列对应的行号即为嵌入的秘密信息十进制形式。

**1.3**EMD(*n*,*m*)算法安全性增强策略

由于EMD(*n*，*m*)算法存在安全隐患即得到载体图像和嵌密图像就可根据嵌密元素个数和最多可改变的嵌密元素个数顺利求出秘密信息，因此EMD(*n*，*m*)算法的安全性需得到提升。

首先，动态生成嵌密元素个数和最多可改变的嵌密元素个数，用户给定系统参数，初始值和消除暂态效应的迭代次数参数*IT*，以及嵌密元素数量*n*的最大值*nmax*，由和按式(6)生成随机数，抛弃前*IT*个随机数；

 (8)

取式(6)连续生成的4个随机数和，按式(9)，式(10)生成截取的嵌密元素个数和最多可改变的嵌密元素个数，

 (9)

 (10)

根据*n*，*m*计算嵌密元素调整表 ，取载体图像和嵌密图像对应的*n*个元素，计算其差值序列，在中找到此序列对应的行号即为嵌入的秘密信息十进制形式。式(9)和式(10)中， “”’为向下取整函数；其次, 置乱嵌密元素调整表,按式(11)将第*i*行作为第行, 式(11)中同余参数的具体生成规则为将按式(12)映射为,将按式(13)映射为,将和分别作为式(8)的系统参数和初始值，将式(8)产生的随机数*R*式(14)量化为，反复执行式(8)直至和互质，将作为*a*，为消除暂态效应，将式(8)迭代产生的前,个随机数抛弃。

 (12)

 (13)

 (14)