# 基于免基向量的EMD(*n*, *m*)嵌入模型及其在图像密写上的应用

## 张洋, 邵利平\*, 任平安

(陕西师范大学计算机科学学院西安 710119)   
(slpmaster@163.com)

摘要: 传统EMD嵌入方法通常只能利用0为起始的连续组合数作为秘密信息表达范围, 同时也仅能给出有限的几种EMD嵌入方法, 对于简单EMD、EMD-2和EMD-3, 只能通过*n*个载体数据中调整1个、2个和*n*个来嵌入1个秘密信息, 不仅限制了秘密信息的表达范围也限制了EMD的适用面. 针对以上问题, 结合无权值向量, 提出了一种EMD(*n*, *m*)嵌入模型, 所提模型通过计算*n*个载体数据中最多调整*m*个数据的秘密信息组合来形成嵌密元素调整表, 通过选取嵌密元素调整表行来对载体数据进行调整以嵌入秘密像素信息. 为进一步提高安全性, 给出了一种基于EMD(*n*, *m*)的数字图像密写方法, 首先将载体图像扫描为1维序列, 通过用户密钥结合混沌映射来随机指派嵌密元素数量和最多调整的嵌密元素数量并生成秘密信息组合数和嵌密元素调整表；然后依据嵌密元素数量和秘密组合数分别从载体元素序列和2进制秘密信息序列截取载体元素和2进制秘密信息比特；最后通过对秘密信息比特所映射的置乱嵌密元素调整表行来对截取的载体元素进行调整以嵌入秘密信息. 理论和实验表明, 与传统的EMD嵌入方法相比, 改进的EMD(*n*, *m*)模型避免了权值向量设置的有限性所导致的嵌入容量受限, 并可最大化嵌入容量提高EMD嵌入方法的适用面, 同时可通过与载体和密钥相关的嵌入提取环节来进一步增强嵌入信息的安全性.

### 关键词: EMD; 无权值向量; 嵌密元素调整表; EMD(*n*, *m*)模型; 数字图像密写; 嵌入容量; 图像信息安全 中图法分类号: TP309. 7

#### Free-basisVector BasedEMD(*n*, *m*) Model and Its Application in Image Steganography

##### Zhang Yang, Shao Liping\*, and Ren Ping’an

(School of Computer Science, Shannxi Normal University, Xi’an710119)

**Abstract**: Traditional EMD methods only use 0 and the continuous figure combinations from 1 as the expression range of secret information. There are only several limited kinds of EMD methods such as simple EMD, EMD-2, EMD-3, these embedding methods can only adjust 1, 2 or all at most for *n* carrier data to embed one secret information which limit not only expression range of secret information but also EMD’s application. To address these problems, an EMD model EMD(*n*, *m*) based on non-weight vector was proposed. This model firstly formed the embedding adjustment table of secret information by calculating all *m* out of *n* carrier data combinations and then selected one row from the embedding adjustment table of secret information to embed the corresponding secret information. To further increase security, this paper also proposed an imagesteganographymethod based on EMD(*n*, *m*) model. First this method scanned each carrier into 1D sequence and randomly generated *m* out of *n* carrier data combinations to form the embedding adjustment table by user key and chaotic map. Second this method truncated all carrier sequence elementsand secret information bits respectively according to the carrier number and the number of secret information combinations. Finally secret information was embedded by adjusting carrier elements according to the mapped row by secret information of the scrambled embedding adjustment table. Theory and experiments show, by compared with traditional EMD methods, the improved EMD (*n*, *m*) model avoids the limited embedding capacity brought by the limited scope of the weight vector and it can maximize the application of the EMD method and also further enhance the embedding safety by adding carrier and user key related the embedding- extraction procedures.

###### **Key words:** EMD; non-weight vector; the embedding adjustment table of secret information; EMD(*n*, *m*) model; digital image steganography; embedding capacity; image information security.

（方正书宋10磅）(正文开始双栏排版)

1. **引言**

图像隐写是利用图像冗余和人类视觉掩蔽特性来将秘密信息隐藏于非相关的掩体图像中, 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, 从而最大可能性地保障传输中机密信息的安全.

针对图像隐写, 人们已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[3]等.

现有的图像密写方法通常分为两类, 变换域密写和空域密写方法. 比较典型的变换域密写方法有F3密写, F4密写和F5密写方法等[4], 他们都是在掩体图像量化后的非零DCT系数上进行嵌密, 但由于量化后的DCT系数中零值较多, 因此秘密信息的嵌入量极低. 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[5], 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密写的秘密信息嵌入量大, 密写图像视觉质量较高, 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[6], 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, 否则随机地对载体图像像素值, 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, 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[7], 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[3]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并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质量较之前的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2比特秘密信息. 这也为后面进行更大容量嵌入的EMD方法[8]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, 由于EMD嵌入方法第载体的视觉质量影响较小, 且能进行大容量的嵌入, 目前已得到了普遍重视, 例如: 文献[9]给出了基于EMD和差值扩展的可逆信息隐藏方法; 文献[10]采用插值扩展的方法将掩体图像的水平和垂直分辨率拓展为原图像的2倍, 在未拓展像素上进行秘密信息EMD嵌入并利用差值扩展像素恢复载体图像. 文献[11]在文献[9]的基础上, 进一步给出了利用掩体图像中未拓展像素的高位比特和边缘图像进行秘密比特调整嵌入, 然后在调整嵌入后像素的高位比特进行EMD嵌入的可逆信息隐藏方法. 结合EMD, 文献[12]将秘密信息按序号的奇偶分别嵌入到2幅同样的掩体图像中, 并通过比较嵌入后掩体图像对应像素的差异来对掩体图像进行可逆恢复. 文献[13]将哈夫曼编码的秘密信息字符通过EMD方法嵌入到随机选取的2个或3个连续的掩体像素中进行传输.

经典的EMD方法是通过对*n*个载体数据最多进行1次来嵌入一个进制的数, 由于在嵌入时只对*n*个载体数据中的1个数据进行调整, 因此具备较高的视觉嵌入质量. 为提高EMD方法的嵌入容量,文献[14]中给出了EMD-2方法, 即对*n*个载体数据最多进行2个而嵌入一个更大进制的数, 其基本思路是EMD方法中的基向量由调整为, 其中, 从而可利用基向量组合出范围内的的所有整数, 将EMD方法的嵌入容量由提高为. 沿着文献[14]的思路, 文献[15]将*n*个载体像素的最多元素调整数量约束为*n*,将基向量设置为,考虑到对嵌入掩体视觉质量的影响, 将每个载体元素的调整量控制为. 文献[16]将基向量由拓展为, 并将对每个载体像素的调整由拓展为, 从而可组合出范围内的所有整数, 从而将嵌入容量拓展为. 在文献[15]工作的基础上, 文献[17]将每个载体像素的调整量拓展为, 从而可嵌入1个进制数. 文献[18]通过约定每个像素的调整方式数, 将基向量设置为, 从而可嵌入一个进制数. 文献[19]给出了基于矩阵的MEMD嵌入方法, 通过构造规模特殊矩阵且满足矩阵元素所在的任意一个规模的矩阵小块包含中的所有元素, 从而可将像素对作为位置坐标, 按坐标调整最小原则改变像素对值来嵌入1个进制的数.

对EMD方法还可进行有效的组合以提供更大的嵌入容量. 例如文献[14]给出的2EMD方法, 即分别对和个数据连续使用2次EMD方法嵌入, 可嵌入1个进制的数. 文献[20]将2*k*+1个连续像素和第*k*个像素构成2*k*个像素分组, 对每个分组采用EMD方法嵌入1个5进制数. 文献[21]将对像素调整的EMD嵌入方法转换为对像素低位比特位的调整嵌入, 从而可在更大范围内进行嵌入.

在上面所给出的EMD嵌入方法中, 对于2个像素的调整上, MEMD方法相对于传统的EMD和EMD-2算法具有较大的嵌入容量, 但MEMD方法很难拓展为多个像素, 一方面高维矩阵的构造规则较为复杂, 在计算机中难以有效得存储, 而另一方面, 通常取值较小, 当=3时, 对图像像素的最大修改量已经为, 当取值较大, 会对嵌入载体产生较大影响, 从而降低安全性. 对于文献[16-18], 其嵌入容量提升取决于对载体像素的修改量, 文献[16]的修改量为, 文献[17]的修改量为, 文献[18]中, 若*c*大于2, 则修改量则会大于1, 因此文献[16-18]都会对嵌入掩体视觉质量产生较大影响. 文献[11, 14-18]的基本出发点是选取特殊的基向量, 从而通过特定的基向量组合来构造出0为起始的连续组合数, 而特定的嵌入策略会降低密写的安全性; 对于文献[14-17], 由于基向量不能充分有效地组合, 从而限制了秘密信息的表达范围, 使得嵌入容量十分有限; 而对于文献[11, 15], 尽管能达到嵌入范围内的最大容量, 但仅能提供有有限的几种调整方案, 对于文献[11], 仅能对*n*个载体数据调整1个嵌入, 对于文献[15]仅能对所有的像素进行调整和不调整嵌入, 导致现有的EMD嵌入方法适用面较窄, 从而不能在图像视觉嵌入质量和嵌入容量上进行较好地折中.

同以上文献不同, 本文提出了一种免基向量的EMD(*n*, *m*)嵌入模型, 所提模型通过计算*n*个载体数据中最多调整*m*个数据的秘密信息组合来形成嵌密元素调整表, 通过选取嵌密元素调整表行来对载体数据进行调整以嵌入秘密信息. 避免了文献[8-18,20-21]中基向量对应的权值向量只能组合出连续正整数而导致的可嵌入的秘密信息范围较小这一缺陷, 同时避免了文献[15-18,21]中基向量对应的权值向量绝对值较大时密写图像视觉质量不高这一缺陷. 为进一步提高安全性, 给出了一种基于EMD(*n*, *m*)的数字图像密写方法, 首先将载体图像扫描为1维序列, 通过用户密钥结合混沌映射来随机指派嵌密元素数量和最多调整的嵌密元素数量并生成秘密信息组合数和嵌密元素调整表; 然后依据嵌密元素数量和秘密组合数分别从载体元素序列和2进制秘密信息序列截取载体元素和2进制秘密信息比特; 最后通过对秘密信息比特所映射的置乱嵌密元素调整表行来对截取的载体元素进行调整以嵌入秘密信息. 理论和实验表明与传统的EMD嵌入方法相比, 改进的EMD(*n*, *m*)模型避免了基向量设置的有限性所导致的嵌入容量受限, 并可最大化嵌入容量提高EMD嵌入方法的适用面, 同时可通过与载体和密钥相关的嵌入提取环节来进一步增强嵌入信息的安全性.

以下本文第2节给出经典的EMD嵌入模型, 第3节给出基于免基向量EMD(*n*, *m*)嵌入模型；第4节给出一种基于EMD(*n*, *m*)的数字图像密写方法；第5节实验; 第6节对本文的工作进行总结, 并给出下一步的研究工作.

1. **经典EMD嵌入模型**

文献[8]给出了经典的EMD嵌入方法,即通过对*n*个载体数据最多进行1次来嵌入一个进制数,其基本原理是：

按式(1)计算的映射值

|  |  |
| --- | --- |
|  | (1) |

若和待嵌入数相同,则不做调整,反之则按式(2)计算映射值和之间的模差值,按式(3)对中的元素进行调整，使得调整后的式(1)映射值与相等.

|  |  |
| --- | --- |
|  | (2) |
|  | (3) |

式(3)中, 和分别是的第个元素, 和第个元素.

对文献[8]的EMD嵌入方法进行拓展, 实际给出了经典的基于基向量的EMD嵌入模型, 包括由*n*个载体数据构成的载体向量,对应的基向量以及要嵌入的秘密信息**,其中为模*X*对应的剩余类集.

在该模型中,式(1)的本质对应为式(4), 即通过与内积来计算的映射值.

|  |  |
| --- | --- |
|  | (4) |

而式(2)的本质对应为式(5), 即判断待嵌入的秘密信息是否和是否模*X*等价.

|  |  |
| --- | --- |
|  | (5) |

若两者不等，则通过对中的元素进行调整，使得按式(4)计算的映射值等价为待嵌入的*X*进制数秘密信息**,因此式(3)的更广泛形式对应为式(6)

|  |  |
| --- | --- |
|  | (6) |

记对应为通过调整可组合出的1为起始的连续正整数数量,若对中每个元素每次只进行调整,则可通过调整组合出个数,加上对的不调整, 则式(4)实际对应为0,因此可通过对的调整和不调整组合出个连续组合数，刚好为个状态, 因此当取模数时,总能通过式(6)对进行调整，使得式(3)映射值和*X*进制数**相等.

在文献[8]中,取值为,对中的每个元素每次最多只能调整1次, 因此可通过对任意选定的元素进行调整可产生个范围内的连续正整数,因此. 对中每个元素每次只进行调整，可组合出总共个数,即*k*=1, 而当式(4)的计算结果等价为时,则对应为0,即不调整, 因此通过对的调整和不调整可组合出总共个状态，因此模数取值为，从而可嵌入1个进制数**，由于文献[8]每次最多只调整1个数，并且基向量本身就是1为起始的连续正整数，因此对应为调整数量的最大值,因此可达到*n*个载体数据每次调整1个的嵌入容量最大值.

但文献[8]每次对*n*个载体数据最多进行1次调整来嵌入一个进制数, 尽管具备了较高的嵌入视觉质量,但所能提供的嵌入容量十分有限.

为进一步提高嵌入容量,文献[14]在文献[8]的基础上给出了EMD-2算法, 将对*n*个载体数据每次最多调整的载体数据个数由1个扩展为2个,并通过选取特殊的基向量使得通过对载体向量调整能组合出更大范围内的1为起始的连续组合数. 文献[14]选取的基向量如式(7)所示:

|  |  |
| --- | --- |
|  | (7) |

式(7)中,当时,可通过调整由中的元素按1,3-1,3,3+1连续组合出4个正整数1,2,3,4, 即,由于是调整，因此,故当时可嵌入1个进制数.

当时,借助调整，由基向量可连续组合出个1为起始的连续正整数, 因此可嵌入1个进制数.然而在时,通过调整会使得基向量的组合可能会产生重复元素，例如2-1也能组和出1, 而直接选中中的第0个元素也是1,EMD-2算法的嵌入容量远未达到EMD-2算法所能达到的理论嵌入容量的上限.

结合文献[8]和文献[14]的工作,文献[15]给出了EMD-*n*算法,即*n*个载体数据的每个载体数据都可进行调整, 进而嵌入1个进制的数,文献[18]选取的基向量如式(8)所示:

|  |  |
| --- | --- |
|  | (8) |

当时，包含3个元素, 可通过1,-1+3,3,1+3,-1-3+9,-3+9,1-3+9,-1+9,9,1+9,1-3+9,3+9,1+3+9连续组合出13个正整数, 即,因此借助调整, 由式(8)可连续1为起始的正整数的数量可按式(9)计算:

|  |  |
| --- | --- |
|  | (9) |

由于是调整, 因此, 故文献[17]给出EMD-*n*算法可嵌入1个进制数.

除了EMD-2算法和EMD-*n*算法以外, 文献[16]在文献[8]的基础上,给出了EMD-*n*算法，将中任意1个数据的修改量由拓展为并且中的每个数据都可进行修改，EMD-*n*算法的基向量如式(10)所示:

|  |  |
| --- | --- |
|  | (10) |

对于EMD-*n*算法,文献[16]给出的嵌入容量*X*如式(11)所示:

|  |  |
| --- | --- |
|  | (11) |

同文献[16]相类似,文献[17]将*n*个载体数据中任意1个数据的最大调整量扩展为,给出了EMD-*n*算法, 其选取的基向量如式(12)所示:

|  |  |
| --- | --- |
|  | (12) |

对于EMD-*n*算法,文献[17]给出的嵌入容量*X*如式(13)所示:

|  |  |
| --- | --- |
|  | (13) |

当*x*=2时, 式(13)蜕变为式(11), 式(12)蜕变为式(10), 因此文献[16]和文献[17]本质是同类的方法,只是文献[17]在时,选择了另外一种基向量.但无论是EMD-*n*算法还是EMD-*n*算法,其嵌入容量都远未达到其理论上限，以下以EMD-*n*算法为例，来分析一下其实际应达到的理论嵌入容量上限:

由式(10)给出的知: 通过调整, 由中元素组合出的最小正数,最大正数如式(13)所示:

|  |  |
| --- | --- |
|  | (12) |

若中元素组合出的整数没有重复值且所有组合出的数值连续，则理论上式(10)应组合出的连续正整数数量估值应为:,而嵌入容量*X*的理论估值应为,因此远大于式(10)的实际嵌入容量,对于EMD-*n*算法其结论也类似.

除了基于行向量调整的EMD方法以外,文献[19]结合数独阵的性质,还给出了基于矩阵的MEMD算法, 通过构造规模特殊矩阵且满足矩阵元素所在的任意一个规模的矩阵小块包含中的所有元素, 从而可将像素对作为位置坐标, 按坐标调整最小原则改变像素对值来嵌入1个进制的数.

表1给出了一个具体的例子

表1 MEMD算法特殊矩阵举例

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 |
| 8 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 |
| 6 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 |
| 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 4 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 |
| 3 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 |
| 2 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 |
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

嵌入进制的秘密信息时, 将载体像素对替换为中以载体像素对对应的坐标元素为中心的范围内与秘密信息相等的值对应的坐标.

假设, 载体像素对为, 秘密信息序列为, 由于中以坐标对应的元素6为中心的范围内值为的元素对应的坐标为. 因此密写后的像素值为.

MEMD方法相对于传统的EMD和EMD-2算法具有较大的嵌入容量, 但MEMD方法很难拓展为多个像素, 一方面高维矩阵的构造规则较为复杂, 在计算机中难以有效得存储, 而另一方面, 通常取值较小, 当=3时, 对图像像素的最大修改量已经为, 当取值较大, 会对嵌入载体产生较大影响, 从而降低安全性.

对于文献[16]和文献[17]，也有类似的问题，因此本文将对每个载体像素的最大修改量控制为，将少量溢出像素的修改量控制为,以减少对嵌入载体的视觉质量影响.

同文献[16]和文献[17]相类似，当时,文献[14]也存在着基向量不能最大化1为起始的连续正整数数量,从而难以达到理论嵌入容量的最优值。而对于文献[8, 15], 尽管能达到嵌入范围内的最大容量, 但仅能提供有有限的几种调整方案, 对于文献[8], 仅能对*n*个载体数据调整1个嵌入, 对于文献[15]仅能对所有的像素进行调整和不调整嵌入, 导致现有的EMD嵌入方法适用面较窄, 从而不能在图像视觉嵌入质量和嵌入容量上进行较好地折中.

文献[8, 14-18]的基本出发点是选取特殊的基向量, 从而通过特定的基向量组合来构造出0为起始的连续组合数, 而特定的嵌入策略会降低密写的安全性.

同以上方法不同，本文给出了。。。

文献[14-18]中都存在基向量对应的权值向量只能组合成连续正整数的情况, 因此基向量的组合未得到充分利用, 限制了秘密信息的嵌入范围,同时基向量的存在会降低密写的安全性,若得到每组的载体数据个数, 则很容易通过基向量计算出秘密信息. 文献[14, 18]对载体数据的修改依赖具体的参数, 如文献[17]中, *x*取值过大, 密写图像的视觉质量就会受到影响. 因此这些参数只能限制在较小的范围. 为克服上述文献[14-18]中列举出的缺陷, 本文提出EMD(*n*, *m*)算法, 避免基向量的使用同时能根据每组的载体数量充分组合出类似于EMD-2算法中的权值向量, 使秘密信息的嵌入量达到最大. 本文进而通过随机生成嵌密元素个数和最多可改变的嵌密元素个数以及置乱嵌密元素调整表提出了安全性增强的EMD(*n*, *m*)算法.

**3EMD(*n*, *m*)模型**

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*)模型中直接给定*n*和*m*, 根据*n*和*m*生成嵌密元素调整表，依次取*n*个载体数据，根据秘密信息和嵌密元素调整表行的对应关系调整载体数据。EMD(*n*, *m*)模型由于*n*和*m*固定，因此生成嵌密元素调整表行数固定，所以每组嵌入的秘密信息容量相等。

EMD(*n*, *m*)模型算法嵌入步骤：

1.记分辨率为**的**比特载体图像为,，记秘密信息对应为长度为*l*的2进制比特位串序列为，记剩余秘密信息序列为，初始化，将扫描为1维载体元素序列**，记的剩余序列为，初始化，记，其中为剩余S的长度,记为已嵌入秘密信息的载体元素序列，初始化，确定嵌密元素个数*n*以及最多可改变的嵌密元素个数*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(4)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.

2. 初始化全0的维嵌密元素调整表 。首先初始化计数变量，将按3进制数进行表示，并用长度为的1维向量进行存储，其中对应为的第i位3进制位，将映射为；统计中的非零元素数量，若，则将嵌入到的第*k*行，置*k*=*k*+1；反复执行直至*k*=。

3. 记为秘密信息序列，其中为剩余秘密信息序列的长度，按照式(5)确定当前截取的2进制位串序列的长度，按照式(6)从中截取长度为的比特位串，并按照式(7)对进行更新, 按照式(8) 将取出的个2进制位串序列转换为对应的10进制数*d*；

|  |  |
| --- | --- |
|  | (5) |
|  | (6) |
|  | (7) |
|  | (8) |

式(7)中， 表示剩余秘密信息的长度，式(8)中，表示个2进制位串中的第个比特.

4.按照式(9)从中取前*n*个元素作为并按照式(10)更新；根据秘密信息d取的第*d*行第*d*行(*td*i)*n*，记为，按照式(11)将调整为，

|  |  |
| --- | --- |
|  | (9) |
|  | (10) |
|  | (11) |

式(11)中, 为溢出避免函数, 用于避免, , 具体执行的功能如式(12)所示:

|  |  |
| --- | --- |
|  | (12) |

按照式(13)将添加到中，按照式(14)将重构为秘密图像

|  |  |
| --- | --- |
|  | (13) |
|  | (14) |

EMD(n, m)模型算法提取步骤：

1. 输入原始的载体图像,和载密图像，，将和扫描为1维元素序列和，记和的剩余序列分别为和，初始化，，记为已提取的秘密信息序列，初始化，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，根据*n*生成嵌密元素调整表，按式(15)分别从和中提取前个元素作为和，按式(16)更新和；

|  |  |
| --- | --- |
|  | (15) |
|  | (16) |

按式(17) 由计算

|  |  |
| --- | --- |
|  | (17) |

式(17)中，为提取函数，其执行的具体功能如式(18)所示，式(18)中为提取溢出函数，用于避免，将2和-2分别转换为-1和1；

|  |  |
| --- | --- |
|  | (18) |

从嵌密元素调整表搜索出对应的行号*d*并按照式(18)转换为对应的2进制序列，其中；

|  |  |
| --- | --- |
|  | (18) |

将按照式(19)连接到尾部，直到，

|  |  |
| --- | --- |
|  | (19) |

算法举例，假设载体序列为， ，，按式(4)可计算3个嵌密元素最多调整3个嵌密元素所能嵌入的秘密信息组合数；将中的数按顺序用3进制数表示，并将表示成的3进制数中的0, 1, 2分别用-1, 0,1替代，如表2所示，

|  |  |  |  |
| --- | --- | --- | --- |
| 表2 | | | |
| 0 | -1 | -1 | 1 |
| 1 | -1 | -1 | 0 |
| 2 | -1 | -1 | 1 |
| 3 | -1 | 0 | 1 |
| 4 | -1 | 0 | 0 |
| 5 | -1 | 0 | 1 |
| 6 | -1 | 1 | 1 |
| 7 | -1 | 1 | 0 |
| 8 | -1 | 1 | 1 |
| 9 | 0 | -1 | 1 |
| 10 | 0 | -1 | 0 |
| 11 | 0 | -1 | 1 |
| 12 | 0 | 0 | 1 |
| 13 | 0 | 0 | 0 |
| 14 | 0 | 0 | 1 |
| 15 | 0 | 1 | 1 |
| 16 | 0 | 1 | 0 |
| 17 | 0 | 1 | 1 |
| 18 | 1 | -1 | 1 |
| 19 | 1 | -1 | 0 |
| 20 | 1 | -1 | 1 |
| 21 | 1 | 0 | 1 |
| 22 | 1 | 0 | 0 |
| 23 | 1 | 0 | 1 |
| 24 | 1 | 1 | 1 |
| 25 | 1 | 1 | 0 |
| 26 | 1 | 1 | 1 |

由于表2中每行1和-1的数量总和不大于3，因此，表2即为维的嵌密元素调整表，其中第1列对应为行号，第2~4列对应为中的列，即将转换为*n*位3进制数构成的向量并分别用进行表示. 假设27进制的秘密信息d=20,因此取 中的第20行,按照式(11)计算嵌密后的元素序列，由于256溢出，因此按照式(12)将调整为，提取秘密信息时，按照式(17)计算嵌密后的元素序列和载体序列的差值序列,由于-2溢出，因此按照式(18)计算最终的，从表2中取出对应的行号20即为嵌入的17进制秘密信息。

**4EMD(*n*, *m*)模型安全性增强策略**

由于EMD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(8)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) |

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,

|  |  |
| --- | --- |
|  | (11) |

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) |

每次嵌入秘密信息时，动态生成的嵌密元素个数*n*和最多可改变的嵌密元素个数*m*，嵌入方法和第3节中类似。

**5实验**

实验测试环境为Windows 10操作系统, CPU为Inter(R) Core(TM) i5-6600, 主频为3.31GHz, 内存为8.00GB,, 实验编码语言为Java jdk1.8.0\_65, 测试图像为的256色灰度图像Lena, Man, Pepper, Women, 如图1(a)-图1(f)所示,



a. Women b. Lena



c. Pepper d. Man

图1

本文采用峰值信噪比和秘密信息嵌入率衡量密写算法的优劣, 峰值信噪比PSNR >38dB时, 说明图像的视觉质量较高, 不易引起察觉. 式(15)为峰值信噪比的计算公式,

|  |  |
| --- | --- |
|  | (15) |

式(15)中, MSE表示两幅图像的均方误差, 计算公式如式(16),

|  |  |
| --- | --- |
|  | (16) |

式(16)中, 和分别表示载体图像和载体图像修改后的图像.

秘密信息嵌入率根据每个载体数据携带的秘密信息比特数进行衡量, 假设在*n*个载体数据中嵌入*s*比特的秘密信息, 则秘密信息嵌入率ER计算公式如式(17) ,

|  |  |
| --- | --- |
|  | (17) |

**4.1**EMD(*n*,*m*)模型的正确嵌入和正确提取实验

为验证EMD(*n*,*m*)算法的可行性, 分别在3组*n*, *m*值下进行实验,对应的嵌密元素数量*n*和最多可改变的嵌密元素数量*m*分别为*n=3*时, *m*=1;*n*=6时, *m*=2;*n*=10时, *m*=4, 由于实验中针对不同载体图像每次嵌入时都随机生成不同二进制秘密信息序列, 将秘密信息输出为二值图像, 如图2所示,

12副秘密信息二进制图像B

图2

首先验证正确嵌入, 按EMD(*n*,*m*)模型将图2对应的秘密信息序列分别嵌入图1对应的载体图像中后得到的密写图像如图3所示,

12副密写图像C’

图3

其次验证正确提取, 根据3组*n*, *m*值利用载体图像和密写图像按照提取算法分别从图1和图3对应的载体图像-密写图像中提取秘密信息, 并将提取出的秘密信息输出为二值图像, 如图4所示,

12副正确密钥提取出的秘密信息图像B’

图4

实验表明,图2和图4中的所嵌入的秘密信息和所提取出的秘密信息完全一致,因此本文所提EMD(*n*,*m*)算法可保证秘密信息的正确嵌入和正确提取.

**4.2**加入安全性策略的EMD(*n*,*m*)模型的正确嵌入和正确提取实验

为验证加入安全性策略的EMD(*n*,*m*)算法的可行性, 分别在3组密钥即,,及;,,及;,,及下进行实验. 每组秘钥对应的秘密信息二值图像, 如图5所示,

12副秘密信息二进制图像B’

图5

第一组密钥下的密写图像为图6, 第一组密钥下的密写图像为图7,第一组密钥下的密写图像为图.

第一组密钥下的密写图像

图6

第二组密钥下的密写图像

图7

第三组密钥下的密写图像

图8

在正确密钥下提取出的秘密信息对应的图像为图9:

正确密钥下的密写图像

图9

未验证密钥敏感性利用随机得到的密钥如,,及进行秘密信息提取，提取结果如图10,

错误密钥下的密写图像

图10

实验表明,图5和图9中的所嵌入的秘密信息和所提取出的秘密信息完全一致, 因此EMD(*n*,*m*)模型在不同密钥下的可正确嵌入和准确提取, 但分析图5和图10知, EMD(*n*,*m*)模型在错误密钥下提取出的信息和所嵌入的秘密信息完全不同,可见EMD(*n*,*m*)模型错误密钥下不能正确提取秘密信息, 因此, 加入安全性策略的EMD(*n*,*m*)模型密钥敏感性得到验证, 其安全性更高.

**4.3**EMD(*n*,*m*)模型视觉质量对比实验

表2分析了4.1节3组*n*, *m*值下不同载体图像嵌密后得到密写图像的PSNR,表3分析了4.2节3组密钥下不同载体图像嵌密后得到密写图像的PSNR.

表2 EMD(*n*,*m*)模型在3组*n*, *m*值下PSNR对比

|  |  |  |  |
| --- | --- | --- | --- |
| PSNR | 第一组*n*,*m* | 第二组*n*,*m* | 第三组*n*,*m* |
| Lena | 12.123 | 12.123 | 12.123 |
| Man |  |  |  |
| Women |  |  |  |
| Pepper |  |  |  |

表3EMD(*n*,*m*)模型在不同密钥下的PSNR对比

|  |  |  |  |
| --- | --- | --- | --- |
| PSNR | 密钥1 | 密钥2 | 密钥3 |
| Lena | 12.123 | 12.123 | 12.123 |
| Man |  |  |  |
| Women |  |  |  |
| Pepper |  |  |  |

由表2可见，EMD(*n*,*m*)模型在不同*n*, *m*值下都能确保密写图像的PSNR>38dB, 因此, EMD(*n*,*m*)模型下密写图像的视觉质量能得到保证.由表3可见, 不同密钥下的密写图像PSNR>38dB,因此加入安全性策略的EMD(*n*,*m*)模型下的密写图像的视觉质量仍能得到保证.

为将加入安全性策略的EMD(*n*,*m*)模型和部分参考文献中的算法进行比较, 在同等嵌密元素数量*nmax*=3和嵌入同等数量秘密信息实现文献[8,15-18]算法, 并将实现的文献[8,15-18]算法中的PSNR和EMD(*n*,*m*)算法的PSNR进行比较, 如表4.

表4 EMD(*n*,*m*)模型和其他算法的PSNR对比

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PSNR | Lena | Man | Women | Pepper |
| 文献8 | 12.123 | 12.123 | 12.123 | 12.123 |
| 文献15 |  |  |  |  |
| 文献16 |  |  |  |  |
| 文献17 |  |  |  |  |
| 文献18 |  |  |  |  |
| EMD(*n*,*m*) |  |  |  |  |

数据分析。。。

**4.4**EMD(*n*,*m*)模型秘密信息嵌入率ER分析

经典EMD[8]算法在*n*个载体数据中最多将1个而嵌入1个2*n*+1进制的数, 因此经典EMD[8]算法秘密信息嵌入率如式(18)所示,

|  |  |
| --- | --- |
|  | (18) |

本文所提EMD(*n*,*m*)模型在*n*个载体数据中最多将*m*个载体数据而嵌入1个进制的数, 因此EMD(*n*,*m*)模型秘密信息嵌入率如式(19)所示,

|  |  |
| --- | --- |
|  | (19) |
| 分析文献[15]-[18]的秘密信息嵌入率。。。 |  |

**6结语**

参考文献**(References):**

1. Kawaguchi E, Eason R O. Principle and Applications of BPCS-Steganography[J]. Proceedings of SPIE - The International Society for Optical Engineering, 1999, 3528:464-473.
2. Wu D C, Tsai W H. A steganographic method for images by pixel-value differencing[J]. Pattern Recognition Letters, 2003, 24(9-10):1613-1626.
3. Huang F, Zhong Y, Huang J. Improved Algorithm of Edge Adaptive Image Steganography Based on LSB Matching Revisited Algorithm[M]// Digital-Forensics and Watermarking. Springer Berlin Heidelberg, 2014:201-214.
4. 王朔中. 数字密写和密写分析[M]. 清华大学出版社, 2005.67-73
5. Andrew D. Ker. Improved Detection of LSB Steganography in Grayscale Images[C]// International Conference on Information Hiding. Springer-Verlag, 2004:97-115.
6. Ker A D. Improved Detection of LSB Steganography in Grayscale Images[C]// International Conference on Information Hiding. Springer-Verlag, 2004:97-115.
7. Mielikainen J. LSB matching revisited[J]. IEEE Signal Processing Letters, 2006, 13(5):285-287.
8. Zhang X P, Wang S Z.Efﬁcientsteganographic embedding by exploiting modiﬁcation direction. IEEE Communication Letter, 2006, 10(11):781-783.
9. Shen S Y, Huang L H. A data hiding scheme using pixel value differencing and improving exploiting modification directions[J]. Computers & Security, 2015, 48:131-141.
10. [CF Lee](http://xueshu.baidu.com/s?wd=author%3A%28ChinFeng%20Lee%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson), [KC Chen](http://xueshu.baidu.com/s?wd=author%3A%28KaiChin%20Chen%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson), Reversible Data Hiding by Reduplicated Exploiting Modification Direction Method[C],// International Conference on Intelligent Information Hiding and Multimedia Signal Processing,2011
11. Lee C F, Weng C Y, Chen K C. An efficient reversible data hiding with reduplicated exploiting modification direction using image interpolation and edge detection[J]. Multimedia Tools & Applications, 2016:1-24.
12. Qin C, Chang C C, Hsu T J. Reversible data hiding scheme based on exploiting modification direction with two steganographic images[J]. Multimedia Tools & Applications, 2015, 74(15):5861-5872.
13. Ali M. Ahmad/ Ghazali Sulong/ / Mohammed Hazim Alkawaz/ Tanzila Saba, / Ghazali Sulong, / Mohammed Hazim Alkawaz, et al. Data Hiding Based on Improved Exploiting Modification Direction Method and Huffman Coding[J]. Journal of Intelligent Systems, 2014, 23(4):451-459
14. Kim H J, Kim C, Choi Y, et al. Improved modification direction methods[J]. Computers & Mathematics with Applications, 2010, 60(2):319-325.
15. Niu X, Ma M, Tang R, et al. Image Steganography via Fully Exploiting Modification Direction[J]. International Journal of Software Engineering & Its Applications, 2015, 9(5):243-254.
16. Kim C, Shin D, Shin D, et al. Improved Steganographic Embedding Exploiting Modification Direction in Multimedia Communications[J]. Secure & Trust Computing Data Management & Applications, 2010, 186:130-138.
17. Kim C. Data hiding by an improved exploiting modification direction[J]. Multimedia Tools & Applications, 2014, 69(3):569-584.
18. Lee C F, Chang C C, Pai P Y, et al. Adjustment hiding method based on exploiting modification direction[J]. International Journal of Rock Mechanics & Mining Sciences & Geomechanics Abstracts, 2015, 33(7):A302.
19. [CC Chang](http://xueshu.baidu.com/s?wd=author%3A%28Chin-Chen%20Chang%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson), [KN Chen](http://xueshu.baidu.com/s?wd=author%3A%28Kuo-Nan%20Chen%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson), [HC Lin](http://xueshu.baidu.com/s?wd=author%3A%28Huang-Ching%20Lin%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson).Novel Magic Matrices Generation Method for Secret Messages Embedding[J].International Journal of Computer Sciences and Engineering Systems,2011,3(5):0973-4406.
20. Wang Z H, The D, Kieu, et al. A novel information concealing method based on exploiting modification direction[J]. Journal of Information Hiding & Multimedia Signal Processing,2010,1(1):1-9.
21. Lee C F, Chang C C, Wang K H. An improvement of EMD embedding method for large payloads by pixel segmentation strategy[J]. Image & Vision Computing, 2008, 26(12):1670-1676.