# 免基向量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, 在采用特殊基向量的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*个来嵌入秘密信息,不仅限制秘密信息表达范围和EMD的适用面, 同时也降低了密写的安全性. 针对以上问题,提出了免基向量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*个数据的组合数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. 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EMD嵌入方法相比, 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; 基向量;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 Applications in Image Steganography

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

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

**Abstract**: Traditional EMD(exploiting modification direction) 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 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视觉掩蔽特性来将秘密信息隐藏于非相关掩体中, 使得非法攻击者难以从海量公开传输图像中找到含密掩体并从中提取出隐蔽的秘密信息.

针对图像隐写, 人们已提出了多种数字图像密写嵌入方法.如致力于提升秘密信息嵌入容量的BPCS(Bit-Plane Complexity Segmentation)方法[1]和PVD(Pixel-Value Differencing)方法[2]以及致力于提高图像视觉质量的边缘自适应LSB匹配重访方法: EALSBMR(Edge Adaptive Image Steganography Based on LSB)方法[3]等.

现有图像密写通常分为2类: 变换域密写和空域密写. 比较典型的变换域密写有F3密写,F4密写和F5密写方法等[4], 它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, 空域密写不仅能提供较大嵌入容量, 也能较大地保持嵌密图像视觉质量.

早期空域密写为LSB(Least Significant Bit)密写[5], 即用秘密信息替换载体图像最低比特位, 由于最低比特位对图像视觉质量影响极小, 因此LSB密写嵌入量较大, 密写图像视觉质量较高, 但嵌入秘密信息易改变图像低位比特统计特性, 因此安全性不高. 对LSB密写的改进, 引入了LSBM(LSB Matching)方法[6], 即LSB匹配方法, 相对于LSB密写方法, LSB匹配方法策略是: 当秘密信息和载体图像最低比特位相同时不做改变, 否则随机对载体像素值, 由于像素值整体增加或减少概率相等, 因此可抵抗简单LSB密写分析, 但其秘密信息嵌入容量相比于LSB密写并未实质提高. 为减轻对载体影响, 后续又提出了LSBMR(LSB Matching Revisited)密写方法[7], 即LSB匹配重访方法, 其原理是在两个连续像素中最多只对其中一个进行1次嵌入而嵌入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最低比特位且明显降低了对载体像素修改, 因此LSBMR方法在提高密写图像质量的同时也提高了安全性. 为进一步提高嵌入图像视觉质量, EALSBMR方法[3]进一步根据秘密信息长度和载体图像自身平滑程度自适应地嵌入秘密信息并优先选择图像粗糙区域进行嵌入, 避免了对载体图像平滑区域修改, 因此EALSBMR密写的视觉质量较之前LSBMR更好.

但无论是EALSBMR还是LSBMR方法, 最独特的地方是对两个载体数据至多改变1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, 是对载体微小修改以进行大容量嵌入的一种有效嵌入方法, 由于EMD嵌入方法对载体视觉质量影响较小, 且能进行大容量嵌入, 目前已得到普遍重视, 例如: 文献[9]给出的基于EMD和差值扩展的可逆信息隐藏方法; 文献[10]采用插值扩展将掩体图像水平和垂直分辨率拓展为原图像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]基础上, 进一步给出利用掩体图像未拓展像素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.

经典EMD方法是通过对*n*个载体数据最多进行1次修改来嵌入一个进制的数, 由于在嵌入时只对*n*个载体数据中1个数据进行调整, 因此具备较高的视觉嵌入质量,但嵌入容量较小. 为提高EMD方法嵌入容量,文献[14]给出了EMD-2方法, 即对*n*个载体数据最多进行2次修改而嵌入一个更大进制数, 其基本思路是将EMD方法中的基向量由调整为, 其中, 从而可利用基向量连续组合出范围内所有连续正整数, 对每个载体数据进行调整和不调整,从而将EMD方法的嵌入容量由提高为. 沿着文献[14]思路,文献[15]给出了EMD-*n*方法, 将*n*个载体像素最多调整数量约束为*n*,从而将基向量设置为,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, 因此可嵌入一个进制数.文献[16]将基向量由拓展为, 给出了方法, 并将每个载体像素调整由拓展为,将嵌入容量进一步拓展为. 在文献[16]基础上, 文献[17]将每个载体像素调整量拓展为, 给出了算法, 从而可嵌入1个进制数. 文献[18]给出了EMD-*cn*方法, 通过约定每个像素调整方式数, 将基向量设置为, 从而可嵌入一个进制数.文献[19]文献[18]原理相似, 首先约定待嵌入秘密信息为*cn*进制数, 嵌入基向量同样取,为提高安全性,增加了范围内安全系数.

文献[20]给出了基于矩阵的MEMD嵌入方法, 通过构造特殊矩阵且满足矩阵元素所在的任意一个规模矩阵小块都包含中的所有元素, 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个进制数.文献[21]选取基向量, 在2个连续像素上嵌入1个进制数的EMD方法, 本质上同文献[20]是等价的, 两者都等同于文献[18]给出的EMD-*cn*方法在*n*=2时的情况, 文献[22]在2*k*+1个载体像素上将第*k*+1个像素值作为参考和其余2*k*个像素组成像素对后利用EMD嵌入2*k*个5进制的数, 文献[23]将像素对按高低比特位组合, 以高比特位组合产生的随机数作为基向量, 将嵌密过程中需调整的基向量用低比特位表示, 并利用高比特位在嵌密过程中的不变性嵌密.

对EMD方法还可进行有效组合以提供更大嵌入容量. 例如2EMD方法[14], 即分别对和个数据连续使用2次EMD方法嵌入1个进制数. 文献[22]将2*k*+1个连续像素和其中第*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[23]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个像素调整上, MEMD方法相对于传统EMD和EMD-2算法具有较大嵌入容量, 但MEMD方法很难拓展为高维MEMD方法, 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存储, 而另一方面, MEMD方法中的通常取值较小, 当=3时, 对图像像素最大修改量已为, 当取值较大, 会对嵌入载体产生较大影响, 从而降低安全性.但究其本质*n*维MEMD方法本质上等价为*n*个像素进行调整的EMD-*cn*方法[18].对于文献[16-19], 其嵌入容量提升取决于对载体像素修改量, 文献[16]的修改量为, 文献[17]修改量为, 文献[18]和文献[19]中, 若*c*大于2, 则修改量会大于1, 因此文献[16-19]都会对嵌入掩体视觉质量产生较大影响. 文献[8,14-19]基本出发点是选取特殊基向量, 从而通过特定的基向量组合来构造出1为起始的连续组合数, 结合不调整和根据连续组合数调整载体数据来嵌入秘密信息,而特定嵌入策略会降低密写的安全性; 对于文献[14],当*n*>2时和文献[16-17], 由于基向量不能充分有效地组合, 从而限制了秘密信息表达范围, 使得嵌入容量十分有限; 而文献[8,15]尽管能达到嵌入范围内最大容量, 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]仅能对所有像素进行不确定数量的调整和不调整嵌入, 导致现有EMD嵌入方法适用面较窄, 从而不能在嵌入图像视觉质量和嵌入容量上进行较好折中.

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*个载体数据最多调整*m*个数据的秘密信息的所有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[8,14-19]选取特殊基向量, 同时也避免了文献[16-19]会对嵌入掩体视觉质量产生较大影响. 为进一步提高安全性, 本文进一步给出了一种基于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EMD嵌入方法相比, EMD(*n*, *m*)模型避免了基向量设置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节给出免基向量EMD(*n*, *m*)嵌入模型; 第4节给出基于EMD(*n*, *m*)的数字图像密写方法; 第5节实验; 第6节对本文工作进行总结, 并给出下一步研究工作.

1. **经典EMD嵌入模型**

文献[8]给出了经典EMD嵌入方法,即通过对*n*个载体数据最多进行1次修改来嵌入一个进制数,其基本原理是按式(1)计算映射值

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

若和待嵌入数相同,则不做调整,反之则按式(2)计算和之差模值,按式(3)对中元素进行调整, 使得调整后的对应的式(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EMD[8]嵌入方法进行拓展, 可给出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)本质对应为式(4), 即通过与模*X*内积来计算映射值.

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

而式(2)本质对应为式(5),判断待嵌入秘密信息是否和等价.

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

若两者不等，则通过中元素调整，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)更广泛的形式对应为式(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,若对这个连续正整数中每个正数每次只进行调整,则可通过调整组合出个数,加上对不调整, 即式(4)中*f*=*d*,因此可通过对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(4)映射值和*X*进制数相等.记通过式(6)调整所能组合出的最大正数为,由于对调整必定会组合出最小正整数1，若，此时表明通过对调整组合出的正整数不重复, 因此可达到对应嵌入策略的最大嵌入容量.

在文献[8]中,取值为,对中每个元素每次最多只调整1次, 因此可通过对任意选定元素进行调整产生个范围内连续正整数,因此. 对中每个元素每次只进行调整,可组合出总共个数,此时*k*=1, 而当式(4)计算结果等价为时,则对应为0,即不调整, 因此通过对调整和不调整组合出总共个状态,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,等价于直接选择基向量中元素，因此,而, 故,因此可达到*n*个载体数据每次调整1个的最大嵌入容量.

但文献[8]每次对*n*个载体数据最多只进行1次调整来嵌入一个进制数, 尽管具备了较高的视觉嵌入质量,但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]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的1为起始的连续组合数. 文献[14]选取基向量如式(7)所示:

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

式(7)中,当时,可通过调整由中元素按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, 同时由于,因此达到了此种嵌入策略最大值.而当时,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,通过调整会使基向量组合可能产生重复元素, 例如2-1也能组合出1, 而直接选中中第1个元素也是1,因此当时, EMD-2算法的嵌入容量为, 此时由于选择的不恰当, 未达到对应嵌入策略的最大值.

结合文献[8]和文献[14]工作,文献[15]给出了EMD-*n*算法,即*n*个载体数据每个都可进行调整, 进而嵌入1个进制数,文献[15]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, 由式(8)可组合出以1为起始的连续正整数, 其中数量可按式(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.由于本身也是中所有元素相加, 因此,因此EMD-*n*算法可达到所采用嵌入策略的最大嵌入容量.

除了EMD-2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个数据修改量由拓展为, 并且中每个数据都可进行修改,EMD-*n*算法基向量如式(10)所示:

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

对于EMD-*n*算法,文献[16]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,选取的基向量如式(12)所示:

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

对于EMD-*n*算法,文献[17]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]本质是同类方法,只是文献[17]在时,选择了另一种基向量.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*算法为例来分析其实际应达到的理论嵌入容量上限:

由式(10)知: 通过调整由中元素组合出的最小正数,最大正数如式(14)所示:

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

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)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)实际嵌入容量,对于EMD-*n*算法其结论也类似.

同时文献[16-17]载体像素的最大修改量分别为和,此时会对嵌入载体产生较大影响, 从而会降低安全性.

文献[18]给出的EMD-*cn*同文献[15]相类似,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.若每个像素只允许进行调整和不调整, 则基向量对应为, 则文献[18]中方法实际对应为文献[15]. 同文献[15]一样, 文献[18]可达到所采用嵌入策略的最大嵌入容量，但当时，对载体最大修改量会达到, 因此同文献[16-17]一样, 会对载体视觉质量造成较大影响.



除了基于向量调整的EMD方法以外,文献[20]结合数独阵性质给出了基于矩阵的MEMD算法, 通过构造特殊矩阵且满足矩阵元素所在的任意一个规模矩阵小块都包含范围内所有元素, 从而可将2个像素值构成的像素对作为所构造特殊矩阵元素位置坐标,按坐标调整最小原则改变像素对值来嵌入1个进制数.

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

图1 MEMD嵌入实例

图1给出了MEMD方法的嵌入实例,这里假设所有像素取值范围为,则由像素可构造位置坐标, 在图中找到元素值6,如黑色边框所在位置元素, 假设实际需要嵌入的秘密值为1, 如灰色阴影方块元素, 因此可将修改为来嵌入秘密值1.

MEMD相对于传统的EMD和EMD-2具有较大的嵌入容量, 但MEMD很难拓展为高维MEMD方法, 一方面高维矩阵构造规则较为复杂, 在计算机中难以有效存储, 而另一方面MEMD方法中通常取值较小, 当=3时, 对图像像素最大修改量已为, 当取值较大会对嵌入载体产生较大影响从而降低安全性.*n*维MEMD方法本质上等价为*n*个像素进行调整的EMD-*cn*方法[18].

以上文献[8,14-19]基本出发点是选取特殊基向量,通过特定基向量组合构造出1为起始的连续正整数,根据这些正整数对应的权值向量调整载体数据来嵌入秘密值, 而特殊基向量一方面会降低密写的安全性, 而另一方面基向量难以选取和构造以达到嵌入策略所对应的最大嵌入容量, 例如文献[14]和当时的文献[16]和文献[17].文献[8,15,18-19]尽管能达到所给出嵌入策略的最大嵌入容量, 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[15,18-19]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, 从而不能在嵌入图像视觉质量和嵌入容量上进行较好地折中.

同以上文献[8,14-19]不同, 本文给出了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*个数据的秘密信息所有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. 避免文献[8,14-19]选取特殊基向量. 为避免文献[16-19]对载体修改量较大这一问题,本文将对每个载体像素最大修改量控制为, 将少量溢出像素的修改量控制为,以减少对嵌入载体视觉质量影响.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.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, EMD(*n*, *m*)模型的安全性增强策略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.

**3EMD(*n*, *m*)嵌入模型**

传统EMD方法[8,14-19]的基本出发点是选取特殊的基向量,通过基向量组合来构造出1为起始的连续正整数,通过对载体数据进行调整和不调整来嵌入秘密值, 而特殊的基向量一方面会降低密写的安全性, 而另一方面基向量难以选取和构造以达到嵌入策略所对应的最大嵌入容量[14, 16-17].

同以上文献[8,14-19]不同, 本文给出了EMD(*n*, *m*)嵌入模型,将*n*个载体数据的最多调整数量约束为*m*来嵌入秘密信息。

相对于传统EMD嵌入方法, EMD(*n*, *m*)嵌入模型剔除了传统EMD方法中的基向量,通过计算*n*个载体数据最多调整*m*个数据全部组合数来形成嵌密元素调整表, 然后选取与嵌密元素值相对应的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.EMD(*n*, *m*)模型始终保持*n*个载体数据中最多调整*m*个数据的最大嵌入容量并可通过调整*m*在图像视觉嵌入质量和嵌入容量上进行较好地折中,避免了文献[8,14-19]选取特殊的基向量所带来的容量受限, 由于在嵌入时调整量为,溢出像素的调整量为, 因而避免了文献[16-19]对嵌入掩体视觉质量产生较大影响.

记为载体向量任取*m*个数据进行调整的全部秘密信息组合数, 其具体计算方法如式(13)所示:

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

式(13)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.这里按进行调整是为了避免对载体修改量较大.

式(13)中, 当*m*=1时,，即对应为文献[8]传统EMD方法的嵌入容量; 当*m*=2时, , 当*n*=2时, 即对应为文献[14]EMD-2算法在*n*=2时的嵌入容量;当*n*>2时,大于文献[14]EMD-2算法的实际嵌入容量.而当*m*=*n*时,则对应为文献[15]给出的EMD-*n*算法的嵌入容量.

传统EMD方法是根据基向量的组合来调整出待嵌入的秘密值*d*, 而本文所给出的EMD(*n*, *m*)嵌入模型取消了基向量, 通过选取与嵌密元素值相对应的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.

记为维嵌密元素调整表, 其具体生成算法记为算法1:

第1步:初始化全0的维嵌密元素调整表;

第2步:初始化计数变量;

第3步: 将按3进制数进行表示, 并用长度为*n*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;

第4步:统计中的非零元素数量，若，则将嵌入到的第*k*行，置*k*=*k*+1;

第5步: 反复执行第3步和第4步, 直至*k*=.

算法1生成嵌密元素调整表的具体思路是不断地枚举范围内的候选整数*j*,将其转换为3进制数并通过1维向量进行存储,然后将元素映射为从而为每个3进制数字分配1个指定的调整量或0形成映射后的调整向量.中非零元素数量即对应为载体向量的调整元素数,因此算法1第4步通过筛选出来保证嵌密调整表中的任一行的总数量都小于*m*.

以EMD(3,3)为例, 由式(13)可计算出,因此可确定维嵌密元素调整表的规模为. 假设当前待枚举的,将其可表示为3位3进制数,则. 按算法1第3步可得中元素, 由于中非零元素数量, 故将作为中的1行. 表1是按算法1生成EMD(3,3)嵌密元素调整表, 其中第1列是为说明行号而增加的额外列.

表2 EMD(3,3)嵌密元素调整表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 行号 | 嵌密表元素 | | | |
| 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 |

表1中第1列对应EMD(3,3)嵌密元素调整表, 每一行中第2~4列元素则分别对应为中每个元素的调整量.

经典EMD模型都是根据载体像素调整位置的基向量元素的有效组合来嵌入秘密信息,因此经典的EMD模型都需要指定基向量,从而限制了秘密信息的表达范围.

而同经典的EMD模型不同,本文提出的EMD(*n*,*m*)模型中不存在基向量, 仅需通过选取嵌密调整表的第*d*行元素来对载体向量, 按式(14)进行调整以嵌入秘密信息*d*.

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

式(14)中,或对应为嵌入时发生溢出的处理情况, 即当产生上溢时,此时通过标记上溢情况; 当发生下溢时, 此时通过标记下溢情况, 与式(14)相对应的秘密信息*d*提取式如式(15)所示:

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

式(15)中,和分别对应为下溢和上溢嵌入标志, 此时可由反向调整直接确定的取值.

通过式(15)可提取出,从而得到嵌入的秘密信息*d*

经典的EMD模型是通过式(4)来提取出嵌入的*X*进制数*d*,安全性较低; 式(15)相对于式(4), 不仅需要嵌入后的载体向量,还需要嵌入前的载体向量和嵌密调整表,若未知,则无法提取出嵌入的秘密信息*d*,因此相对于式(4)具备更高的安全性.

式(13)~式(15)和的生成策略算法1即构成了本文所给出的EMD(*n*,*m*)模型的嵌入和提取策略.

当*m*=1时, EMD(*n*,*m*)模型和文献[8]具备同样的嵌入容量;当*m*=2和时, 即对应为文献[14]EMD-2在时的嵌入容量;当时,则对应为文献[16]EMD-*n*算法的嵌入容量.而对于其他情况, EMD(*n*,*m*)模型始终保持最大的嵌入容量,由于EMD(*n*,*m*)模型在嵌入时调整量为,溢出像素的调整量为, 因而避免了文献[16-18]对嵌入掩体视觉质量产生较大影响.EMD(*n*,*m*)模型可根据*m*的不同取值,在图像视觉嵌入质量和嵌入容量上进行较好地折中,在提取时和嵌入前的载体向量和嵌密调整表直接绑定,因此相对于传统的EMD嵌入方法具有更高的安全性.

**4基于EMD(*n*, *m*)的数字图像密写方法**

EMD(*n*, *m*)嵌入模型可直接应用到图像密写上, 当*n*=*m*时, EMD(*n*, *m*)密写方法可达到与文献[15]同等的嵌入率, 然而, EMD(*n*, *m*)密写方法的嵌密元素个数和最多可改变的嵌密元素个数固定, 因此据其得到嵌密元素调整表后, 可顺利提取出秘密信息. 为此, 本文将EMD(*n*, *m*)嵌入模型应用到图像密写上时增加相应的安全策略, 即动态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.

首先, 动态生成嵌密元素个数*n*和最多可改变的嵌密元素个数*m*. 具体生成方法为用户给定系统参数, 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(18)生成随机数, 抛弃前*IT*个随机数;

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

取式(1)连续生成的4个随机数和, 按式(2), 式(3)生成嵌密元素个数和最多可改变的嵌密元素个数:

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

式(2)和式(3)中, “”为向下取整函数.

其次, 置乱嵌密元素调整表, 按式(4)将第*i*行作为第行:

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

式(4)中同余参数*a*的具体生成规则为将按式(5)映射为, 将按式(6)映射为, 将和分别作为式(1)的系统参数和初始值, 将式(1)产生的随机数*R*按式(7)量化为, 反复执行式(18)直至和互质, 将作为*a*, 同余参数*b*的生成规则如式(8), 为消除暂态效应, 将式(1)迭代产生的前, 个随机数抛弃.

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

基于EMD(*n*, *m*)的数字图像密写方法具体嵌入算法记为算法2:

第1步: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, 记剩余秘密信息序列为, 初始化, 将***C***扫描为1维载体元素序列, 记的剩余序列为, 初始化, 记, 其中为剩余的长度,记为已嵌入秘密信息的载体元素序列, 初始化, 输入用户给的系统参数, , *IT*, *nmax*, 根据式(1)(2)(3)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(8)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,

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

第2步: 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*j*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.

第3步:置乱嵌密元素调整表为,

第3步: 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(9)确定当前截取的2进制位串序列的长度,按照式(10)从中截取长度为的比特位串,并按照式(11)对进行更新,按照式(12)将取出的个2进制位串序列转换为对应的10进制数*d*;

|  |  |
| --- | --- |
|  | (9) |
|  | (10) |
|  | (11) |
|  | (12) |

第4步: 按照式(13)从中取前*n*个元素作为并按照式(14)更新; 根据秘密信息*d*取的第*d*行, 按照式(15)将调整为,

|  |  |
| --- | --- |
|  | (13) |
|  | (14) |
|  | (15) |

按照式(16)将添加到中.

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

第5步: 待秘密嵌入完成后按照式(17)将重构为秘密图像,

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

算法2第3步中置乱嵌密元素调整表的具体思路为: 根据用户密钥, , *IT*, *nmax*, ,将和代入式(1)求出若干连续随机数并将前*IT*个数抛弃后, 顺次取4个数并将前2个数代入式(2)(3)求得当前, ,将后2个数代入式(5)(6)(7)(8)求出,,将其代入式(4)置乱. 当用户密钥,,时,生成一组, ,对应的嵌密元素调整表如表2所示, 将其按照式(4)置乱后如表3所示.

表3EMD(3,3)嵌密元素置乱调整表

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

基于EMD(*n*, *m*)的数字图像密写方法提取算法记为算法4:

第1步: 输入原始的载体图像,和载密图像, , 以及用户密钥, , *IT*, *nmax*,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, 根据用户密钥按式(1)(2)(3)计算嵌密元素*n*和最多可改变嵌密元素个数*m*;

第2步: 根据*n*和*m*计算秘密信息组合数, 根据*n*及用户密钥生成置乱后的嵌密元素调整表, 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) |

第3步: 按式(17)由计算;

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

从嵌密元素调整表中搜索出对应的行号*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) |

即为提取到的秘密信息序列.

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, 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。

**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, 测试图像分辨率为的256色灰度图像Lena,Girl Man,Lake, 如图5-1所示,

|  |  |
| --- | --- |
| E:\extrem\STOGO\EMDimgFrom\Lena.bmp | E:\extrem\STOGO\EMDimgFrom\Women.bmp |
| a Lena | b Girl |
| E:\extrem\STOGO\EMDimgFrom\Man.bmp | E:\extrem\STOGO\EMDimgFrom\Lake.bmp |
| c Man | d Lake |
| 图5-1载体图像 | |



c. Man d. Lake

a. Lena b. Girl

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*lb*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个载体数据而嵌入1个2*n*+1进制的数, 其秘密信息嵌入率如式(18)所示,

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

EMD-2[14]算法在*n*个载体数据中最多将2个载体数据而嵌入1个10*n*-13进制的数, 其秘密信息嵌入率如式(19)所示,

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

EMD-*n*[15]算法在*n*个载体数据中将任意多个而嵌入1个进制的数, 其秘密信息嵌入率如式(20)所示,

|  |  |
| --- | --- |
|  | (20) |

文献17在*n*个载体数据中将任意多个而嵌入1个进制的数, 其秘密信息嵌入率如式(21)所示,

|  |  |
| --- | --- |
|  | (21) |

文献16的秘密信息嵌入率即是文献17中当*x*=2时的情况.

文献18算法对每个载体像素的调整方式数为*c*, 其秘密信息嵌入率如式(22)所示,

|  |  |
| --- | --- |
|  | (22) |

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) |

可知,EMD(*n*,*m*)模型秘密信息嵌入率在*n=*1时和文献8的秘密信息嵌入率相等,在*n=*2时大于文献14的秘密信息嵌入率, 在*n=m*时和文献15的秘密信息嵌入率相等, 在*n=m*同时*n*>3时大于文献16的秘密信息嵌入率,虽然文献17和文献18秘密信息嵌入率较高, 但对载体像素的修改太大, 因此视觉质量没有EMD(*n*,*m*)模型高.

**4.2**EMD(*n*,*m*)模型的正确嵌入和正确提取实验

为验证EMD(*n*,*m*)模型的可行性, 首先进行秘密信息嵌入实验, 分别在3组*n*值下进行实验, , 每组*n*下*m*取值范围为, 待嵌入的秘密信息为随机生成的01序列, 在一幅图像中嵌入秘密信息时, 将对所有像素进行嵌密. 由于的*n*,*m*不同取值导致一幅图像能携带的秘密信息数量不同, 而当图像分辨率和*n*,*m*值相同时将对应相同的秘密信息, 否则对应不同的秘密信息. 图5-2为*n*,*m*不同取值时可嵌入秘密信息对应的二值图像. 为方便描述图像信息, 将秘密信息二值图像命名为*s-n-m*, 其中*s*表示此图为秘密信息图, *n-m*对应为具体的值, 例如图a的s-3-1表示当*n=*3,*m=*1时的秘密信息图像.

|  |  |  |
| --- | --- | --- |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=2.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=3.bmp |
| a. s-3-1 | b. s-3-2 | c. s-3-3 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=3.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=2.bmp |
| d. s-4-1 | e. s-4-2 | f. s-4-3 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=4.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=4.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=3.bmp |
| g. s-4-4 | h. s-5-1 | i. s-5-2 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=2.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=5.bmp |
| j. s-5-3 | k. s-5-4 | l. s-5-5 |
| 图5-2秘密信息图像 | | |

首先验证正确嵌入, 按EMD(*n*,*m*)模型将图5-2对应的秘密信息序列分别嵌入图5-1对应的载体图像中得到的密写图像如图5-3所示, 为方便描述嵌密图像, 将其命名为*name-n-m*, 将4副载体图像分别用abcd表示,其中a表示Lena图像, b表示Girl图像, c表示Man图像, d表示Lake图像, *n-m*对应为具体的值. 例如a-4-2表示Lena图像在*n=*4, *m=*2时的嵌密图像.

|  |  |  |
| --- | --- | --- |
| E:\extrem\STOGO\EMDimgFrom\Lena.bmp | E:\extrem\STOGO\EMDimgFrom\Women.bmp | E:\extrem\STOGO\EMDimgFrom\Man.bmp |
| a. a-3-1 | b. b-3-1 | c. c-3-1 |
| E:\extrem\STOGO\EMDimgFrom\Lake.bmp | E:\extrem\STOGO\EMDimgFrom\Lena.bmp | E:\extrem\STOGO\EMDimgFrom\Women.bmp |
| d. d-3-1 | e. a-3-2 | f. b-3-2 |
| E:\extrem\STOGO\EMDimgFrom\Man.bmp | E:\extrem\STOGO\EMDimgFrom\Lake.bmp | E:\extrem\STOGO\EMDimgFrom\Lena.bmp |
| g. c-3-2 | h. d-3-2 | i. a-3-3 |
| E:\extrem\STOGO\EMDimgFrom\Women.bmp | E:\extrem\STOGO\EMDimgFrom\Man.bmp | E:\extrem\STOGO\EMDimgFrom\Lake.bmp |
| j. b-3-3 | k. c-3-3 | l. d-3-3 |
| 图5-3密写图像（48幅图像？会不会太多） | | |

其次验证正确提取, 根据不同*n*,*m*值利用图5-1中的载体图像和图5-3中的密写图像按照EMD(*n*,*m*)模型提取算法提取秘密信息, 并将提取出的秘密信息输出为二值图像, 如图5-4所示, 为方便描述提取出的秘密信息图像, 将其命名为,例如表示*n=*3, *m=*1时从图*a-*3-1中提取出的秘密信息二值图像.

|  |  |  |
| --- | --- | --- |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=2.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=3.bmp |
| a. s-a’-3-1 | b. s-b’-3-1 | c. s-c’-3-1 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=3.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=2.bmp |
| d. s-d’-3-1 | e. s-a’-3-2 | f. s-b’-3-2 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=4.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=4.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=3.bmp |
| g. s-c’-3-2 | h. s-d’-3-2 | i. s-a’-3-3 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=2.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=5.bmp |
| j. s-b’-3-3 | k. s-c’-3-3 | m. s-d’-3-3 |
| 图5-4提取出的秘密信息（48幅图像？） | | |

经计算, 图5-2中的秘密信息图像和图5-4中的所提取的秘密信息图像误码率均为0, 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**EMD(*n*,*m*)模型视觉质量验证及嵌入率对比实验

计算图5-3中的密写图像对应的PSNR值以验证EMD(*n*,*m*)模型嵌密后图像的视觉质量, 表5-1对应图5-3中图像的PSNR.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 表5-1 EMD(*n*,*m*)模型密写图像PSNR | | | | |
| *n*,*m* | 不同*n*,*m*下各图像的PSNR(单位dB) | | | |
| Lena | Girl | Man | Lake |
| 3,1 | 46.0296 | 46.0296 | 46.0296 | 46.0296 |
| 3,2 | 45.8632 | 45.8632 | 45.8632 | 45.8632 |
| 3,3 | 45.8282 | 45.8282 | 45.8282 | 45.8282 |
| 4,1 | 46.0501 | 46.0501 | 46.0501 | 46.0501 |
| 4,2 | 45.9101 | 45.9101 | 45.9101 | 45.9101 |
| 4,3 | 45.8398 | 45.8398 | 45.8398 | 45.8398 |
| 4,4 | 45.8140 | 45.8140 | 45.8140 | 45.8140 |
| 5,1 | 46.1031 | 46.1031 | 46.1031 | 46.1031 |
| 5,2 | 45.9546 | 45.9546 | 45.9546 | 45.9546 |
| 5,3 | 45.8722 | 45.8722 | 45.8722 | 45.8722 |
| 5,4 | 45.8362 | 45.8362 | 45.8362 | 45.8362 |
| 5,5 | 45.8196 | 45.8196 | 45.8196 | 45.8196 |







由表5-1可知,*n*,*m*值固定时,不同图像对应的PSNR相等, 这是因为实验中图像分辨率和*n*,*m*值相等时,对应的秘密信息相等, 所以对载体的调整位置和调整大小相等. *n*固定时,*m*值越小,图像视觉质量越好. 如*n*=3, *m=*1时,4幅密写图像的PSNR均为46.0296dB,大于*n*=3, *m=*2时4幅密写图像的PSNR45.8632dB,大于*n*=3, *m=*3时4幅密写图像的PSNR45.8282dB, 此规律和理论分析一致, 因为*n*固定时, *m*值越小,说明调整的像素个数越少, 密写图像的视觉质量越高. 而表5-1中的PSNR值均大于38dB,说明EMD(*n*,*m*)模型下图像的视觉质量较高, 不易引起察觉.

根据不同*n*,*m*下的秘密信息组合数*Vkind*计算其对应的秘密信息嵌入率ER,如表5-2.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 表5-2 EMD(*n*,*m*)模型秘密信息嵌入率 | | | | |
| *n*,*m* | 不同*n*,*m*下各图像的嵌入率(bit/每像素) | | | |
| Lena | Lena | Lena | Lena |
| 3,1 | 0.9358 | 0.9358 | 0.9358 | 0.9358 |
| 3,2 | 1.4160 | 1.4160 | 1.4160 | 1.4160 |
| 3,3 | 1.5850 | 1.5850 | 1.5850 | 1.5850 |
| 4,1 | 0.7925 | 0.7925 | 0.7925 | 0.7925 |
| 4,2 | 1.2611 | 1.2611 | 1.2611 | 1.2611 |
| 4,3 | 1.5056 | 1.5056 | 1.5056 | 1.5056 |
| 4,4 | 1.5850 | 1.5850 | 1.5850 | 1.5850 |
| 5,1 | 0.6919 | 0.6919 | 0.6919 | 0.6919 |
| 5,2 | 45.9546 | 45.9546 | 45.9546 | 45.9546 |
| 5,3 | 45.8722 | 45.8722 | 45.8722 | 45.8722 |
| 5,4 | 45.8362 | 45.8362 | 45.8362 | 45.8362 |
| 5,5 | 45.8196 | 45.8196 | 45.8196 | 45.8196 |











参考文献中不同密写算法的PSNR值和ER值如表5-3和表5-4所示, 对应参考文献下第1列为PSNR值,第2列为ER值. 因为相同的*n*,*m*值对应相同的秘密信息组合数, 所以图像分辨率及大小相同且*n*,*m*值相同时对应相同的秘密信息嵌入率及PSNR, 因此表5-3和表5-4只针对参考文献比较不同*n*,*m*下的秘密嵌入率及PSNR, 不针对不同图像进行对比.

表5-3对比了文献8, 文献14-16, 因为这4篇文献只有*n*在变化, 而文献17和文献18中每个像素的调整范围还可设置, 因此将文献17和文献18与前面的文献的分开对比.如表5-4.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 表5-3 参考文献PSNR及ER | | | | |
| *n* | 文献8 | | 文献14 | |
| 3 | 45.9948 | 0.9358 | 45.8697 | 1.3625 |
| 4 | 46.0488 | 0.7925 | 45.9170 | 1.1887 |
| 5 | 46.0936 | 0.6919 | 45.9601 | 1.0419 |
| *n* | 文献15 | | 文献16 | |
| 3 | 45.7943 | 1.5850 | 45.7060 | 1.6513 |
| 4 | 45.7343 | 1.5850 | 45.7032 | 1.4943 |
| 5 | 45.7938 | 1.5850 | 45.6543 | 1.3977 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 表5-4 参考文献PSNR及ER | | | | |
| *n* | 文献17 | | | |
| *x*=3 | | *x*=5 | |
| 3 | 45.6037 | 1.9924 | 45.3511 | 2.6648 |
| 4 | 45.6002 | 1.7472 | 45.3604 | 2.2493 |
| 5 | 45.5727 | 1.5989 | 45.3980 | 2.0000 |
| *n* | 文献18 | | | |
| *c*=3 | | *c*=5 | |
| 3 | 45.8122 | 1.5850 | 45.8122 | 1.5850 |
| 4 | 45.8108 | 1.5850 | 45.8108 | 1.5850 |
| 5 | 45.8117 | 1.5850 | 45.8117 | 1.5850 |



比较表5-1和表5-3, 表5-1和表5-4可知EMD (*n*,*m*)模型当*m*=1时, 其PSNR和文献8相近; 其嵌入率和文献8相同, 当*m>*1时, 其嵌入率大于文献8; 当*m*=2时, 其PSNR和文献14相近, 其嵌入率大于文献14; 当*m*=*n*时, 其PSNR大于文献15, 因为文献15对载体像素的修改不依赖于权值向量,所以对*n*个载体像素的修改数量可能取到离*n*较近的值, 而当*m*=*n*时, EMD(*n*,*m*) 模型对载体像素的修改数量可根据秘密信息对应的嵌密元素调整表行号随机取中的值, 当*m*=*n*时, EMD(*n*,*m*) 模型嵌入率和文献15相同; 当*m*=*n*时, EMD(*n*,*m*) 模型的PSNR大于文献16和文献17, 因为文献16和文献17对载体像素的调整范围分别为和, 而EMD(*n*,*m*)模型对载体像素的调整范围为, 当*n*相等时, 文献16的PSNR大于文献17的PSNR; 当*m*=*n*时, EMD(*n*,*m*)的嵌入率大于文献16中*n*>2时的情况, 小于文献17的嵌入率, 但是文献17是用较大的载体像素调整量换取的较大嵌入容量, 所以文献17的PSNR较之EMD(*n*,*m*) 模型的PSNR普遍较低; 当*m*=*n*时, EMD(*n*,*m*) 模型的PSNR和文献18当*c*=3时相近, 嵌入率和文献18当*c*=3时相同, 因为文献18当*c*=3时的像素调整范围为[-1,0,1], 最大嵌密元素数量为*n*, 嵌入的秘密信息进制数为3*n*, 和EMD(*n*,*m*),*m*=*n*时相同, 当文献18当*c*=5时, 像素调整范围为[-2,-1,0,1,2],因此其PSNR小于EMD(*n*,*m*) 模型*m*=*n*时的PSNR,其较高的嵌入率依旧是用较大的载体像素调整量换取的.

EMD(*n*,*m*)的秘密信息提取过程必须同时提供载体数据和密写数据, 因此安全性相对参考文献较高, 同时经过以上分析表明其能在实现和文献[15,16,17,18]相近或较高的视觉质量基础上实现最大嵌入容量, 实现和文献[8,14,15,16]相近或较高的嵌入率.



**4.3**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4组密钥下进行实验. 首先进行正确嵌入验证实验, 表5-5为模拟用户指定的4组密钥的详细信息.每组密钥对应的秘密信息二值图像如图5-5所示, 每组密钥对应的密写图像如图5-6所示, 为方便描述秘密信息, 将其命名为*s-index*, *s*表示此图是秘密信息图像, *index*表示第几组密钥.为方便描述密写图像, 将其命名为*name-index*,*name*其中*name*表示图像名称, *index*表示第几组密钥, 例如*a*-3表示Lena图像在第3组密钥下的密写图像.

|  |  |  |
| --- | --- | --- |
| 表5-5模拟用户指定的密钥 | | |
| 组别 | 密钥名称 | |
|  | *IT* |
| 1 | 3.2514822365454681 | 19808 |
| 2 | 3.0514653566487545 | 10000 |
| 3 | 3.9987412366954254 | 15034 |
| 4 | 3.9582136554725873 | 13156 |
| 组别 | 密钥名称 | |
|  |  |
| 1 | 0.2514822365455547 | 3 |
| 2 | 0.5489745623643663 | 4 |
| 3 | 0.1561967046719725 | 5 |
| 4 | 0.6570410236952914 | 6 |

|  |  |
| --- | --- |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=2.bmp |
| a. s-1 | b. s-2 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=5.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=3.bmp |
| c. s-3 | d. s-4 |
| 图5-5每组密钥对应的秘密信息 | |

|  |  |  |
| --- | --- | --- |
| E:\extrem\STOGO\EMDimgFrom\Lena.bmp | E:\extrem\STOGO\EMDimgFrom\Women.bmp | E:\extrem\STOGO\EMDimgFrom\Man.bmp |
| a. a-1 | b. b-1 | c. c-1 |
| E:\extrem\STOGO\EMDimgFrom\Lake.bmp | E:\extrem\STOGO\EMDimgFrom\Lena.bmp | E:\extrem\STOGO\EMDimgFrom\Women.bmp |
| d. d-1 | e. a-2 | f. b-2 |
| E:\extrem\STOGO\EMDimgFrom\Man.bmp | E:\extrem\STOGO\EMDimgFrom\Lake.bmp | E:\extrem\STOGO\EMDimgFrom\Lena.bmp |
| g. c-2 | h. d-2 | i. a-3 |
| E:\extrem\STOGO\EMDimgFrom\Women.bmp | E:\extrem\STOGO\EMDimgFrom\Man.bmp | E:\extrem\STOGO\EMDimgFrom\Lake.bmp |
| j. b-3 | k. c-3 | l. d-3 |
| 图5-6不同密钥下的密写图像 | | |







其次验证加入安全性策略的EMD(*n*,*m*)算法的正确提取实验, 根据表5-2中嵌入秘密信息时的密钥以及图5-1中的载体图像和图5-6中的密写图像提取出的秘密信息图像如图5-7所示, 为方便描述秘密图像将其命名为,*s*表示此图为秘密信息图像,表示图像名称, *index*表示第几组密钥. 例如表示从图5-6中的图*c*-3中提取出的秘密信息.

|  |  |  |
| --- | --- | --- |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=2.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=3.bmp |
| a. s-a’-1 | b. s-b’-1 | c. s-c’-1 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=3.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=2.bmp |
| d. s-d’-1 | e. s-a’-2 | f. s-b’-2 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=4.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=4.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=3.bmp |
| g. s-c’-2 | h. s-d’-2 | i. s-a’-3 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=2.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=5.bmp |
| j. s-b’-3 | k. s-c’-3 | l. s-d’-3 |
| 图5-7正确密钥提取出的秘密信息 | | |



经计算, 图5-5中的秘密信息图像和图5-7中提取出的对应秘密信息图像误码率均为0, 因此加入安全性策略的EMD(*n*,*m*)算法可保证秘密信息的正确嵌入和正确提取.

**4.4**加入安全性策略的EMD(*n*,*m*)模型视觉质量验证实验

为验证图5-6中不同图像的视觉质量, 计算其PSNR值, 如表5-3所示,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 表5-3加入安全性策略的EMD(*n*,*m*)密写图像PSNR | | | | |
| 密钥 | 不同密钥下各图像的PSNR(单位dB) | | | |
| Lena | Girl | Man | Lake |
| 1 | 45.8632 | 45.8632 | 45.8632 | 45.8632 |
| 2 | 45.9370 | 45.9370 | 45.9370 | 45.9370 |
| 3 | 45.8879 | 45.8879 | 45.8879 | 45.8879 |
| 4 | 45.8908 | 45.8908 | 45.8908 | 45.8908 |



从表5-3可看出, 相同密钥下各图像的PSNR相等, 因为密钥相同时每组嵌密元素数量及最多可调整的嵌密元素数量,置乱后的嵌密元素调整表完全相同, 所以相同密钥下图像的调整幅度和调整位置相等; 其次, 不同密钥下图像的PSNR均在45.86之上, 可见加入安全性策略的EMD(*n*,*m*)密写嵌入视觉质量较高,不容易被察觉. 较之表5-1EMD(*n*,*m*)模型密写图像的PSNR, 加入安全性策略的EMD(*n*,*m*)密写PSNR整体较高, 因为其对嵌密元素的修改数量随机取中的值,而不是固定的值, 平均嵌密元素的修改数量相当于(1+*m*)/2, 例如第3组密钥, *n*=5,其PSNR=45.8908dB, 而表5-1中*n*=5, *m=*1时密写图像的PSNR=46.1031dB, *n*=5, *m=*2时密写图像的PSNR=45.9546dB, 均大于45.8908dB, *n*=5, *m=*4时密写图像的PSNR=46.8362dBdB, *n*=5, *m=*5时密写图像的PSNR=45.8196dB, 均小于45.8908dB, *n*=5, *m=*3时密写图像的PSNR=45.8722dB,接近于45.8908dB,实验数据证明加入安全性策略的EMD(*n*,*m*)模型和EMD(*n*,*m*)模型中*n*=(1+*m*)/2时的PSNR接近相等;

**4.5**加入安全性策略的EMD(*n*,*m*)模型密钥敏感性验证实验

为验证加入安全性策略的EMD(*n*,*m*)模型的密钥敏感性, 在提取图5-3中密写图像携带的秘密信息时, 随机指定4组密钥, 并按照随机指定的密钥提取图5-3中的信息. 提取出的秘密信息如图5-8所示,为方便描述秘密图像将其命名为,表示此图为用随机密钥提取出的秘密信息图像, 表示图像名称, *index*表示第几组随机密钥. 表5-4即为4组随机密钥.



|  |  |  |
| --- | --- | --- |
| 表5-4 随机指定的密钥 | | |
| 组别 | 密钥名称 | |
|  | *IT* |
| 1 | 3.5436678900354681 | 9808 |
| 2 | 3.0897521688905645 | 6535 |
| 3 | 3.8362698090426854 | 5034 |
| 4 | 3.3279094678965245 | 3156 |
| 组别 | 密钥名称 | |
|  |  |
| 1 | 0.6893526006987547 | 4 |
| 2 | 0.6754753680452764 | 3 |
| 3 | 0.5679835211658990 | 2 |
| 4 | 0.5647035366789075 | 5 |

|  |  |  |
| --- | --- | --- |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=2.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=3 m=3.bmp |
| a. s’-a’-1 | b. s’-b’-1 | c. s’-c’-1 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=3.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=2.bmp |
| d. s’-d’-1 | e. s’-a’-2 | f. s’-b’-2 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=4 m=4.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=4.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=3.bmp |
| g. s’-c’-2 | h. s’-d’-2 | i. s’-a’-3 |
| E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=2.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=1.bmp | E:\extrem\STOGO\allimages\modelimgage\emb- n=5 m=5.bmp |
| j. s’-b’-3 | k. s’-c’-3 | l. s’-d’-3 |
| 图5-8 随机密钥提取出的秘密信息 | | |

经计算, 图5-5中的秘密信息图像和图5-8中提取出的秘密信息图像误码率均为100%, 因为若当*n*不一致时提取出的秘密信息数量首先和嵌入的秘密信息不一致, 其次不同密钥对应不同*n*,*m*,因此对应不同的秘密信息组合, 所以理论和实验同时证明加入安全性策略的EMD(*n*,*m*)算法敏感性较高.

**6结语**

EMD(*n*,*m*)模型将秘密信息表达范围提高到最大值, 且其提取秘密信息时需同时提供载体数据和密写数据使其具有较高安全性, EMD(*n*,*m*)模型对载体数据的最大修改量保持在, 因此其视觉质量均较高, 加入安全性策略的EMD(*n*,*m*)算法在随机生成嵌密元素数量和最多可调整的元素数量及置乱嵌密元素调整表的基础上进一步提高了安全性.



















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. Lie W N, Chang L C. Data hiding in images with adaptive numbers of least significant bits based on the human visual system[C]// International Conference on Image Processing, 1999. ICIP 99. Proceedings. IEEE, 1999:286-290 vol.1.
6. [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" \t "_blank), [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" \t "_blank), Reversible Data Hiding by Reduplicated Exploiting Modification Direction Method[C],// International Conference on Intelligent Information Hiding and Multimedia Signal Processing,2011
7. 廖琪男, 孙宪波, 潘瑞冬. n维超立方体模映射安全隐写算法[J]. 电子学报, 2016, 44(1):160-167.
8. [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" \t "_blank), [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" \t "_blank), [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" \t "_blank).Novel Magic Matrices Generation Method for Secret Messages Embedding[J].International Journal of Computer Sciences and Engineering Systems,2011,3(5):0973-4406.
9. Kieu T D, Chang C C. A steganographic scheme by fully exploiting modification directions[J]. Expert Systems with Applications, 2011, 38(8):10648-10657.