

学号 22151214548

西 安 电 子 科 技 大 学
专业学位硕士学位论文中期考核报告表

论文题目: 基于随机内容插入的可信存证关键技术研究

姓 名 孙恒康

学位类别 电子信息硕士

领 域 电子信息

校内导师 李风华

校外导师 郭云川

学 院 广州研究院

报告日期 2024 年 6 月 20 日

西安电子科技大学研究生院制

西安电子科技大学硕士学位论文中期考核报告要求

一、硕士生在完成学位论文开题报告后半年内，必须进行学位论文中期考核，会议由各学院自行组织，具体要求参照开题报告会要求执行。

二、中期考核结论分为两种：1. 通过，按专家意见修改后继续学位论文撰写工作；2. 不通过，重新考核。

三、在学位论文中期考核规定的时间期限内休学的硕士生，中期考核的时间期限相应顺延。

四、中期考核必须在规定时间内通过研究生学位管理系统申请，本表用 A3 纸张正反套印。

五、表格填写要求：正文字体宋体，字号小四，行间距固定值 20 磅。

选题来源：国家重点研发计划课题

一、学位论文研究目标及研究内容

（一）研究目标

设计一种针对不同模态的随机内容生成算法和对生成随机内容的插入算法，支持包括 txt 文本文件，json 结构化文件，图片文件。可以做到对不同模态的不同文件或相同模态的不同文件生成唯一的和原始存证信息相同模态的随机内容：并随机插入到原始存证信息的随机位置：头部、尾部、或者文件任意范围内。这样使得伪造生成具有相同语义且相同类型的散列值理论上不可能，可以有效避免有意伪造存证对象的情况发生，随机内容和随机插入规则也可以作为侵权的证据。在算法的基础上完成多模态随机内容生成和随机插入系统，包含客户端和服务端，作为对算法的检验和具体应用。

二）研究内容

1.研究场景

随着信息技术的飞速发展，人们在网络上产生的大量数据和操作记录需要进行审计和存证，以确保信息的完整性、可追溯性和安全性。然而，不同组织内部的防护条件差异巨大，有些防护能力较弱的组织无法保证内部的存证信息的安全，存证信息和审计信息有被修改和伪造的可能，因此当需要内部存证信息的时候，信息的可靠性就会大打折扣。

但是如果将需要存证的信息直接传输存放在可信的第三方也会带来诸多问题：当需要存证的信息涉及到商业机密或者个人的隐私数据的时候，将数据存储在第三方会带来数据泄露的风险；而且当需要存证的信息数据量巨大时候，网络传输会影响存证速度，拖慢业务的运行速度。所以常见的处理方法是将需要存证的数据生成认证校验码，只需要将认证校验码传输给第三方的存证系统，这样就能利用避免将信息保存在第三方的面临的数据泄露风险和效率低下的问题。

在单纯对原始存证信息生成认证校验码并向第三方机构发送认证校验码的基础上，还可以为校验码的生成引入新的随机性，即第三方存证中心根据用户提供的存证信息模态信息还其他数据信息（如文件名，文件大小，标题信息）生成和原始信息相同模态的唯一随机内容并将随机内容随机插入原始存证信息中。最后生成插入后的认证校验码。本文针对这一个业务流程中如何生成多模态随机信息和随机插入规则设计了适用于 txt 文本模态，json 结构化数据和图片信息的随机内容生成算法和插入规则算法，提高了存证信息的可信度。

本文提出了针对不同模态的存证信息生成相同模态的随机内容生成算法和将生成的随机内容随机嵌入到原始信息的插入算法。通过将随机内容随机插入到原始信息中然后在对插入后的信息进行认证校验码的生成。由于随机内容生成算

法和随机内容插入算法是根据不同的信息生成的，具唯一性，认证校验码具有机密性、完整性和不可否认性的特性，因此原始信息被伪造且伪造信息可以生成相同认证校验码理论上不可能，可以有效避免有意伪造存证信息的情况发生。

2.具体研究内容

（1）不同模态的随机内容生成算法：针对 3 种不同的模态：txt 文本文件，json 结构化文件，图片文件，根据用户传入的文件模态类型和文件其他相关信息：文件名称，大小，标题信息等，生成和原始文件模态相同语义相近的随机内容。

（2）对 1 中生成的随机内容的随机插入算法：针对 3 种不同的模态：txt 文本文件，json 结构化文件，图片文件将对应随机内容按照随机的插入规则：包括但是不限于文件头部、尾部、数据任意节点，而且使原文件的语义不会发生明显变化。

（3）多模态随机内容生成和随机插入系统的设计与实现：包括一个客户端和服务端，基于上述研究内容 1 和 2 提出的算法，设计实现多模态随机内容生成和随机插入系统，验证所提出算法的可行性、可用性和高效性。并且要确保系统服务端能够正确处理大量用户的随机生成和插入规则请求，安全保存用户的认证及校验码和随机信息和随机规则。客户端能够正确向服务器传输文件特征，按照服务端返回的随机内容和随机插入规则完成对原始数据的改造，还要保证服务端和客户端的安全通信。

3. 总结

本研究首先提出多模态的随机内容生成和随机插入算法，然后针对特定的模态随机生成和插入中出现的问题：不同模态数据要生成随机的相同模态的随机数据，并且数据数据的插入规则要使得原始数据对随机数据的插入高效准确，且要保证数据的生成内容和插入规则完全随机。最后要使用可处理高并发请求的系统服务端和可以发送存证求情并可以在原始存证信息中插入随机内容的服务端来验证算法的生成效果和插入效果。用大量数据进行实验验证算法的性能和准确定。

二、目前已完成学位论文工作的内容

（一）文本内容

1. 修改式随机内容分析

修改式文本内容指的是在已有文本载体的基础上，对文本格式或者文本内容加以修改并嵌入信息。其中，基于文本格式的信息隐藏利用文本间距、字符属性以及字符在计算机中编码特征来隐藏信息；而基于文本内容的算法以自然语言处理技术为支撑，通过对文本语法和句法的分析，发掘出文本内容特征，构造合适的算法隐藏信息，该类算法可以划分成基于语法的修改和基于语义的修改。

文本都是由字、行和段等有规律的结构组成，因此可以利用字移编码和行移编码算法，在不可查的前提下，字移编码通过字符左移或右移微小的距离来嵌入信息，行移编码则通过行上移或下移微小的距离来嵌入信息。在该算法中行移编码嵌入容量小于字移编码，但字移编码隐蔽性较低。

除了文本间距，字符的属性如字体大小、样式和颜色等也可以用来隐藏秘密信息。针对英文文本富含很多空格这一特性，可以利用空格字符的字体大小来隐藏秘密信息，略微更改空格字符字体大小隐藏“1”，不修改隐藏“0”。对利用空格字符的方式可以进行一些改进，不仅利用空格字符的字体大小，还利用了空格字符的类型，其中字体类型可以编码 6 比特的秘密信息，字体大小编码 1 比特的秘密信息，从而提升了信息隐藏容量，但该算法受到字体类型种类的限制。

有些编码后的字符插入文本后不会被人眼感知，此类字符被称为“不可见字符”。利用这个特性，提出了基于 Unicode 编码的不可见字符嵌入算法，该算法将 Unicode 不可见字符编码两两组合表示成二进制序列，从而可以将秘密比特串翻译成不可见字符插入到文本每个句子的句号前，完成秘密信息隐藏。理论上利用不可见字符的嵌入秘密信息方法具有很大的容量，独立于文本文件的格式和排版，但一般的文本文件不允许存在过多空字符，因此限制了此类算法的应用

2. 生成式文本

基于马尔可夫模型的算法，这类算法将马尔可夫模型作为模拟生成文本的统计语言模型，在保证文本质量的基础上，依据不同的编码方式嵌入机密信息。马尔可夫链的两次近似使得该模型不能很好地替代统计语言模型，需要进一步优化所生成的隐写文本质量。该类算法在特殊的文本载体如诗歌上展现出较好的隐写效果，使得研究者们将研究重点转移到生成式隐写算法。

根据一些公共文本建立状态转移图，对每个分支使用二比特定长编码，使用美国数据加密标准（data encryption standard, DES）算法将秘密信息从字节流转变成比特流，再根据状态转移图选择单词，生成隐写文本。该算法没有考虑到状态转移图中词与词之间概率大小的不同，因此可以改进了编码方式，根据需要编码的位数 n ，将转移图中的状态按照概率分配码字，直至每个码都对应唯一的一个短句，该短句即为隐写文本。除此之外，还使用标识符代替了发送方自己设定的开头词语，增加了随机性。该算法考虑到了状态转移概率，提升了文本质量，但是牺牲了信息隐藏容量。为了提升隐写文本的质量，研究者们考虑一些特殊体裁的文本，在中文领域如诗和词。比如采用宋词这个体裁，用平仄过滤候选词语，将候选词语使用霍夫曼编码，根据编码值选择词语生成隐写文本。该算法提升了文本质量，但受体裁的限制，其实用性较差。还有的算法打破了上述算法的限制，提出了一种根据马尔可夫链模型和霍夫曼编码自动生成隐写文本的算法，将状态转移图中的条件概率进行霍夫曼编码，从而选择出合适的词语用以生成隐写文本。该算法提升了文本质量和信息隐藏容量，生成的文本也不受体裁的限制，具有普适性。

3. 文本式总结

文本隐写的评价指标与隐写相同，即不可感知性、安全性以及嵌入容量，三者越高越好。经过学习这两大类的文本生成方式。决定采用修改式的随机内容插入算法：一方面，现有的语言处理算法生成的载体文档与原始自然语言有明显的区别。这种差异很容易用肉眼分辨出来，现有的语言处理算法从句法、语义和统计特性上都不能满足实际应用的要求，而且我们现在用于输入的信息仅仅是文本的标志，摘要等少量有效信息，无法生成语义相近的文本。另一方面，自然语言本身的复杂性，使得构造一个合理有效的替换表成为一项困难的工作。即使有一个理想的替代表，该算法仍然是不够的安全性，因为替代表可以被黑客攻击。

（二）图像数据

图像数据和文本数据不同，图像数据有更大的信息容量，可以更加灵活的信息插入方式。本文选取了 png 图片作为图像数据的格式来进行随机内容的插入。并学习了基于 png 图像的内容插入技术：

png 图片是一种无损压缩的位图格式，也只有在不损压缩或者不压缩的图片（BMP）上实现 1sb 隐写。如果图像是 jpg 图片的话，就没法使用 1sb 隐写了，原因是 jpg 图片对像数进行了有损压缩，我们修改的信息就可能会在压缩的过程中被破坏。而 png 图片虽然也有压缩，但却是无损压缩，这样我们修改的信息也就能得到正确的表达，不至于丢失。png 图片中的图像像数一般是由 RGB 三原色（红绿蓝）组成，每一种颜色占用 8 位，取值范围为 $0x00 \sim 0xFF$ ，即有 256 种颜色，一共包含了 256 的 3 次方的颜色，即 16777216 种颜色。而人类的眼睛可以区分约 1000 万种不同的颜色，这就意味着人类的眼睛无法区分余下的颜色大约有 6777216 种。LSB 隐写就是修改 RGB 颜色分量的最低二进制位（LSB），而人类的眼睛不会注意到这前后的变化，每个像数可以携带 3 比特的信息。

我们可以将根据图像名称，时间戳等关键信息生成的 hash 值，利用 LSB 隐写术嵌入到原始图片中。为了达到使第三方无法修改或者剔除嵌入内容的目的。我采用了随机 LSB 算法嵌入：

包含 N 个像素点的 256 色图像记作 N 维向量 $C^N = \{c_1, c_2, \dots, c_N\}$ ， $S^N = \{s_1, s_2, \dots, s_N\}$ 表示对应的载密图像，其中 c_i 和 s_i 都是取值于 $[0, 255]$ 的整数， $1 \leq i \leq N$ 。用 $M^L = \{m_1, m_2, \dots, m_L\}$ ， $L \leq N$ ，表示嵌入消息（一般为 hash 序列）； $m_i \in \{0, 1\}$ ， $1 \leq i \leq L$ 。用 k 表示隐写密钥，它取值于密钥空间 Key 。

首先利用隐写密钥 k 通过一个伪随机数发生器 G ，生成随机序列 y_1, y_2, \dots, y_L ，然后按如下方式产生消息的随机嵌入位置 x_i ， $1 \leq i \leq L$ 。

$$x_1 = y_1; x_i = x_{i-1} + y_i \quad 1 \leq i \leq L$$

最后把消息 $M = \{m_1, m_2, \dots, m_L\}$ ，嵌入到 $\{c_{x1}, c_{x2}, \dots, c_{xL}\}$ 的 LSB 位从而得到载密图像 S ，具体的嵌入过程是：若 C_{xi} 的 LSB 位与 m_i 相同，则不变，否则进行“LSB 替换”（即把 C_{xi} 的 LSB 位改成 m_i ）或按某种规则如通过“像素值 ± 1 ”实现消息嵌入，合法的接收者拥有隐写密钥 k ，所以可以从载密图像 S 读出嵌入消息。

我们把随机数发生器的输出定义为独立同分布的随机变量序列 Y_1, Y_2, \dots, Y_L ，其取值为 $[a+1, a+d]$ 之间的整数，其中 a 和 d 是两个整数，满足

$$P\{Y_i = a+i\} = p_i, \quad 1 \leq i \leq d, \quad \sum_{i=1}^d p_i = 1$$

随机数发生器的输出一般要服从均匀分布。否则，它在密码意义上是弱的，因为在这种情况下密码分析者容易恢复其种子或构造等价的发生器。通过以上的随机算法，期望达到的目的是将该图片的唯一的标识符 hash 值，均匀的嵌入在原始图片中且不被发现。

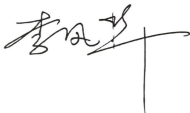



三、现阶段完成的工作与开题报告内容不相符的情况说明

研究内容：从生成和之前内容语义相近的随机内容后插入原始内容中，修改生成内容信息的唯一标志，将唯一标志隐写到原始内容中。因为信息输入有限，生成的随机内容和原始内容差距较大，利用有限的输入内容生成的散列值隐写到原始内容中可以很好的完成对随机内容的隐藏。

四、下一步工作计划及需要完成的研究内容和需要解决的关键技术

下一步工作计划及需要完成的研究内容是利用可靠隐写技术完成对随机内容的隐藏，以及防止被检测出隐写内容。主要的关键技术包括对于文本数据，利用修改式的方式插入随机内容，对于图片数据利用 Lsb 等图片隐写技术将随机内容插入。

五、已发表的与学位论文相关的学术论文、其他研究成果以及拟发表的研究成果
无

指导教师 评价 意见	<p>(重点写出该生的表现、计划完成情况、对后续工作情况的估计等。)</p> <p>计划按期完成，后续继续推进学位论文撰写</p> <div>校内指导教师签名：</div> <div>2024 年 7 月 25 日</div>
	<p>中期计划完成，继续完成学位论文</p> <div>校外指导教师签名：</div> <div>2024 年 7 月 25 日</div>
中期 总结 报告 评语 及 结论	<p>(中期考核结论分为两种：1. 通过，按专家意见修改后继续学位论文撰写工作；2. 不通过，重新考核。评语重点指出中期报告存在的问题并提出具体修改意见和建议。)</p> <p>通过，继续撰写学位论文</p> <div>组长签名：</div> <div>成员签名： </div> <div>2024 年 7 月 28 日</div>