

基于绝句生成的构造式信息隐藏算法

秦川 王萌 司广文 姚恒

(上海理工大学光电信息与计算机工程学院 上海 200093)

摘要 目前利用文本生成进行秘密信息隐藏的研究中,生成文本的质量和嵌入率是主要存在的挑战.为此本文提出一种基于绝句生成的构造式信息隐藏算法.首先对绝句文本数据进行词向量的构建,然后利用机器翻译模型搭建新的绝句诗生成模型;在诗句生成阶段,需要向模型输入主题词、模板信息和押韵信息,通过输入信息的综合作用,生成第一行绝句诗;再利用现有可体现诗句主题的显著信息生成后续行的诗句.在利用绝句诗生成模型进行信息隐藏的过程中,对于相同的输入信息,模型可生成多首同一主题且符合模板要求的绝句诗;通过对主题词、模板信息、押韵信息以及诗句的不同选择,可有效实现秘密信息的隐藏.实验中使用了25000首绝句诗进行训练,结果表明本文算法的嵌入率可达到35%左右,与已报道的主流算法相比具有一定的优势,且本文所提出的模型生成的诗词语义通顺、主题明确.

关键词 文本生成;构造式信息隐藏;绝句;主题词;嵌入率

中图法分类号 TP309 DOI号 10.11897/SP.J.1016.2021.00773

Constructive Information Hiding with Chinese Quatrain Generation

QIN Chuan WANG Meng SI Guang-Wen YAO Heng

(School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093)

Abstract As one kind of the main media of information communication, the text is one of the common cover data in the field of information hiding, which has attracted extensive interests in the related research community. However, compared with digital image, video and other types of cover data, the redundancy of text is relatively lower and the space for data embedding is relatively limited. At present, the technique of text generation based on natural language processing becomes more and more popular, but its application in the field of information hiding is not satisfactory, which is still in the initial stage. In the current research of information hiding using text generation, the semantic quality of generated text and the embedding rate are the two main challenges. Therefore, in this paper, we propose a novel constructive information hiding method based on Chinese quatrain generation. First, word vectors are constructed for the quatrain text data, and at the same time, the information of keyword, pattern and rhyme for the quatrain poetry need to be determined and encoded, which then participate in the training of the quatrain generation model. Then, the quatrain generation model proposed in this paper is established through the Sequence to Sequence model, which is based on a bidirectional recurrent neural network with the attention mechanism. In the stage of quatrain generation, the first line of quatrain can be generated based on the input keywords and the combined effect of pattern information and rhyme information. Then, by selecting the words related to the keywords as the guidance information, the subsequent lines of the quatrain can be produced efficiently, which also ensures that the generated quatrain

has an unified theme and there are no obvious semantic deviations between the previous and latter lines. For the same input information, the model can generate multiple quatrains with the same theme and meet the requirements of the pattern. By choosing the different candidate quatrain lines and the information of keyword, pattern and rhyme, secret information can be hidden effectively. In the experiment, totally 25000 quatrains were used as the training data for the quatrain generation model. Experimental results show that, the hidden secret information can be extracted from the generated quatrain with no error, and the embedding rate of the proposed method can reach about 35%, which is significantly greater than some of reported information hiding methods based on text generation. We also utilized the same set of training data on our model with information hiding and the current typical poetry generation models without information hiding, and the trained results show that the performance indices of these models, such as perplexity and loss value, are close. Then, by comparing the 16 poetries randomly generated with each of these models, we can find that their performances of semantic quality for generated poetries are also equivalent. In addition, the computational complexity, security and robustness of the proposed method are discussed and the feasibility of practical application is also analyzed. Finally, future research directions of this work are given.

Keywords text generation; constructive information hiding; quatrains; keywords; embedding rate

1 引 言

信息隐藏是将秘密信息隐藏在公开的媒体信息中,使得除收发者外的其他人无法提取出隐藏的信息,甚至不知道有隐藏信息存在的技术.信息隐藏技术作为网络安全的重要研究方向,近年来取得了重大进展,在军事、法律、知识产权保护和隐私保护等领域都有应用^[1].通常秘密信息会被隐藏到各种多媒体载体当中,如图像^[2]、音频^[3]、视频^[4]以及文本等.文本作为使用最为广泛的载体之一,是人们日常沟通交流获取信息的主要媒介,在信息隐藏领域也得到了诸多的应用,具有很高的研究价值.但文本本身信息冗余度较低,因此如何使携带秘密信息的文本接近自然语言文本,并有较高的嵌入率,是文本信息隐藏算法亟待解决的问题^[5].随着信息隐藏技术的发展,通常信息隐藏方案可以划分为两类:载体修改式方案和构造式方案^[6].

目前基于文本的信息隐藏方案大部分属于载体修改式,即通过修改载体文本的格式或语法语义进行秘密信息的隐藏.根据修改方式的不同大致又可以将其分为两类.第一类为基于文本格式修改的信息隐藏方案.如通过细微地调整字符间距和行间距来隐藏秘密信息,由于人类视觉系统的特性,很难直接观察到文本的异常^[7].通过调整字符的属性,如磅

值、颜色、风格等,也能够隐藏秘密信息^[8-9].如文献^[9],通过控制 HTML 文本中字体的颜色来标记字符,从而映射不同的二进制码,达到秘密传输信息的目的.其它方法如文献^[10],通过文档中的不可见字符进行秘密信息的隐藏,在文本每一段结束时键入空白字符,如通过 SPACE 键和 TAB 键所生成的不可见字符的长度不同,来隐藏秘密信息.基于文本格式修改的信息隐藏方案不会改变文本的语义,但是对文本格式极为敏感,轻微的格式变化都会导致秘密信息无法正确提取.因此此类方案的鲁棒性不强,同时该类方案统计特征较为明显,容易被隐写分析算法检测出异常.第二类为基于文本语法语义修改的信息隐藏方案.该类方案主要涉及同义词替换方案和句式变换方案^[11-12].总体来说修改文本语法语义的方式,通过阅读感知很难发现这种细微的修改,因此隐蔽性较强.但由于对原始的文本进行了修改和调整,不可避免地会产生失真.在同义词替换方案中载体词汇暴露在文本当中,容易受到隐写分析算法的攻击^[13-14].同时考虑到载体文本的长度有限,可提供替换的词汇也有局限性,因此此类算法的嵌入率一般不高.

由于文本修改式信息隐藏算法存在以上的问题,基于文本生成的构造式信息隐藏算法应运而生,并成为当前的研究热点之一.此类算法是根据秘密信息驱动直接生成文本,没有对文本进行任何的修

改,因此更加隐蔽安全.文献[5]提出利用生成宋词进行秘密信息隐藏的构造式文本信息隐藏方案.文献[5]根据宋词的格式音律要求,选取不同的词汇组成新的宋词文本来隐藏秘密信息,引起了广泛关注.但文献[5]在生成宋词的过程中,没有深入考虑文本的语义要求,而是通过韵律规则等进行词语组合,生成的宋词相对缺乏中心思想,容易引起攻击者的怀疑,且该方案的嵌入率也较低.文献[15]在文献[5]的基础上进行了改进,在嵌入率方面有所提升,但生成文本的质量不高,主题思想不明确,词与词之间的语义匹配仍需要改进.文献[16]提出了基于马尔可夫链的宋词生成模型,所生成的宋词质量有所提高,但该方案的嵌入率较低.

随着深度学习在机器翻译方面的广泛应用,基于机器翻译模型进行诗词创作的技术日趋成熟.文献[17]提出使用循环神经网络(Recurrent Neural Network, RNN)不断将新生成的诗词压缩到历史向量中,从而生成新的诗词.文献[18]提出一种规划模型的诗词生成方案,通过预先规划诗词每一句的主题词,来辅助指导诗词的生成,确保了每一句话的语义信息.规划模型生成诗词的质量较高,但存在主题不明确的问题.文献[19]提出了基于工作记忆模型的诗词生成方案.工作记忆模型利用主题信息、历史信息和本地信息,确保生成诗词主题的灵活表达,同时所生成的诗词的质量高,在已报道的文献中处于较好的水平.高质量的诗词生成模型也引起了信息隐藏领域学者的高度关注.文献[20]利用规划模型,并通过挑选备选字的方式进行秘密信息的隐藏,获得了较高的嵌入率.但文献[20]通过备选词库的组合会有较大的损失,对生成诗词的质量影响较大,导致该方案所生成诗词的质量一般.且随着诗句的生成,由于没有主题信息的限制,可能会丢失主题信息.另一方面,文献[20]的秘密信息提取过程需要对模型所能生成的诗词进行遍历,导致提取算法效率较低,无法实现实时提取.

针对以上信息隐藏算法所存在问题,本文提出一种基于绝句生成的构造式信息隐藏算法,实现了秘密信息的实时隐藏和提取,且生成绝句诗质量高.绝句属于近体诗的一种形式,由四句组成,有严格的格律要求,常见的绝句有五言绝句和七言绝句.由于绝句文本的信息冗余低,如果强行进行字符的隐藏,必定会造成较高损失,使文本的可读性下降.如何使所隐藏的字符自然地出现在所生成的绝句诗词中是

需要解决的关键问题.为此本文提出了基于主题词的高质量绝句生成算法,确保主题词能够自然地出现在所生成的绝句诗词文本中.与文献[20]相比,本文算法无需设置内置词库来限制所生成的绝句诗词,从而能够使所生成诗词的损失降到更低,保证生成诗词的可读性.同时我们在训练模型过程中添加了字符的韵律信息,这样生成的诗句抑扬顿挫感强,能够达到自然押韵.在嵌入率方面,我们根据所生成绝句诗的主题词、模板、押韵信息以及备选诗句来进行秘密信息的隐藏,具有较高的嵌入率.实际上,利用本文提出的方案除诗句外还可以对宋词、元曲、对联、歌词等韵律和平仄要求高的文体进行文本生成,进而实现秘密信息的隐藏.需要注意的是,需对不同文体的文本分别进行训练,并采用相应的模板及韵律规则.

本文所提出的方案主要在三个方面有所贡献:一是在嵌入率方面有较大提升;二是生成诗词可读性强、韵律自然、主题明确;三是能够实现实时隐藏和提取,同时可对提取的秘密信息进行自我校验,判断文本是否遭受过篡改,安全性更高.相较于基于载体选择的信息隐藏算法,本文所提出的基于文本生成的构造式信息隐藏算法首先在安全性方面表现更好.因为构造式信息隐藏算法没有固定词库,而是通过计算来进行字词的选择和匹配,因此在没有相同训练数据的情况下,很难进行攻击和分析.其次,在生成文本质量方面,构造式信息隐藏算法更加注重字与字之间的搭配,因此生成文本的质量更高.

本文第2节介绍所提出算法的整体框架;第3节具体介绍所提出的基于主题词的绝句生成方法;第4节给出信息隐藏算法和提取算法;第5节为实验结果及分析比较;第6节给出全文的总结与进一步的工作.

2 算法整体框架

本文所提出方案的整体框架如图1所示.本文方案主要由三部分组成,分别为模型训练、隐藏过程和提取过程.

在模型训练过程中,需要对绝句诗进行预处理,然后根据本文提出算法进行训练,最终生成符合秘密信息隐藏要求的绝句生成模型.收发双方需要共享相关训练参数,确保双方生成的模型达到相同的效果.

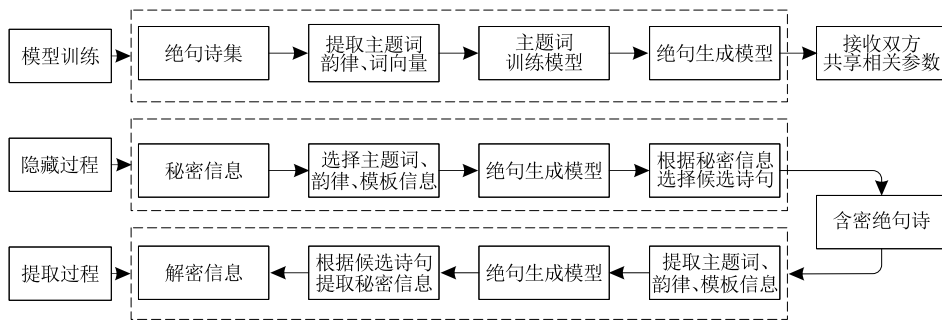


图 1 方案整体框架图

在隐藏过程中,首先根据秘密信息选择对应的主题词、韵律及模板信息;然后输入模型,生成候选的绝句句句;根据秘密信息选择候选诗句,生成含密绝句诗.在提取过程中,首先根据接收到的绝句诗提取出主题词、韵律和模板信息,然后按照隐藏过程中生成诗句的方法将相关信息输入模型生成候选诗句;接着根据候选诗句,对照接收到的诗句,提取秘密信息.以上为本文方案的整体框架,接下来进行详细介绍.

3 高质量绝句生成模型

本文绝句生成模型的基础是基于注意力机制的序列到序列模型(Sequence to Sequence, Seq2Seq)^[21], 因此我们在给出本文的生成模型之前首先对

Seq2Seq 模型及工作记忆模型进行相关介绍.

3.1 基于注意力机制的 Seq2Seq 模型

在 Seq2Seq 模型中,使用一个循环神经网络作为编码器,将完整的句子压缩为一个向量.使用另外一个 RNN 作为解码器,根据输入向量生成目标句子.但是当输入的句子过长时,这个中间向量难以存储足够的信息.同时中间向量作为一个整体,无法做到精准地解码,而注意力机制(Attention Mechanism)就是为了解决这个问题而设计^[22].注意力机制是将当前解码的重点放在当前所对应的字或者片段,而不是整个句子.众所周知,中国古诗词不仅在格式以及韵律上有着严格的要求,同时行与行之间的单个字或者词都有着紧密的关联.因此,基于注意力机制的 Seq2Seq 模型在中国古诗词生成过程中有着较好的表现,其生成诗句的基本流程如图 2 所示.

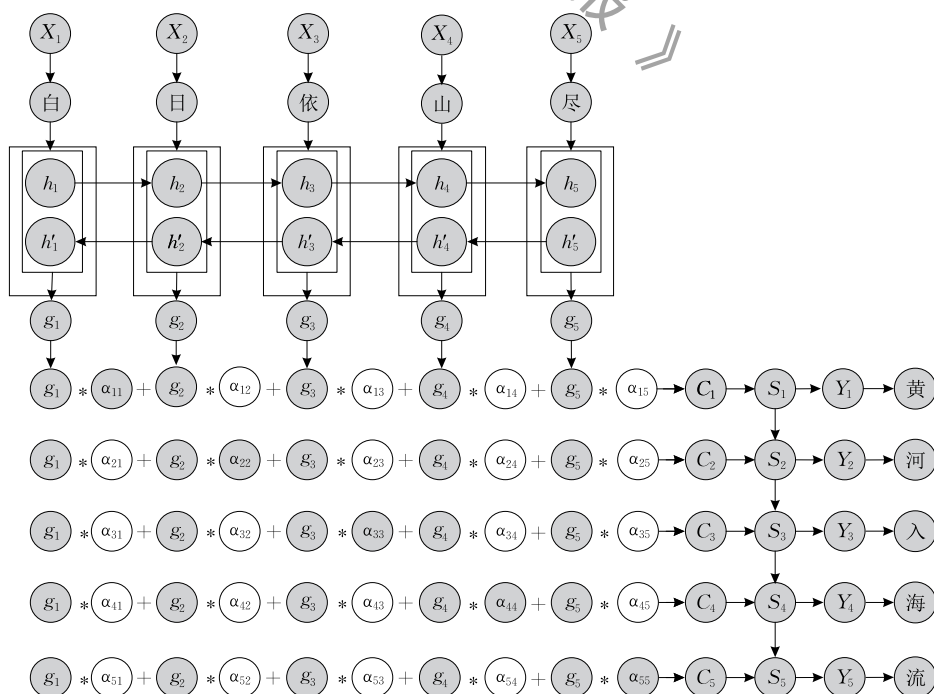


图 2 诗句生成基本流程

这里使用基于注意力机制的 Seq2Seq 模型,其中编码器以双向 LSTM(Long Short-Term Memory)为基础^[23]. 编码过程中,第一句诗词输入表示为 $X=(x_1, x_2, \dots, x_N)$, 输出结果表示为 $Y=(y_1, y_2, \dots, y_M)$, h_n 和 h'_n 分别代表编码过程中前向传播和反向传播的隐层状态, r_n 表示重置门, u_n 表示更新门, g_n 表示编码器在第 n 个字最终输出, 计算公式为

$$d_n = \tanh(U[h_{n-1} \cdot r_n] + Wx_n) \quad (1)$$

$$u_n = \sigma(U_u h_{n-1} + W_u x_n) \quad (2)$$

$$r_n = \sigma(U_r h_{n-1} + W_r x_n) \quad (3)$$

$$h_n = (1 - u_{n-1}) \cdot h_{n-1} + u_n \cdot d_n \quad (4)$$

$$g_n = [h_n, h'_n] \quad (5)$$

双曲正切函数 $\tanh(\cdot)$ 为激活函数,用以在神经元中引入非线性因素,使得神经网络可以逼近任意非线性函数. h'_n 的计算过程与 h_n 基本一致. 在注意力机制的作用下,解码器的第 t 步解码过程首先计算得出 α_{tn} , 其表示第 t 步查询状态下第 n 个字编码输出 g_n 与当前解码结果的相关程度,计算公式为

$$\alpha_{tn} = \frac{\exp(v_{t,n})}{\sum_{m=1}^N \exp(v_{t,m})} \quad (6)$$

$$v_{t,n} = \mathbf{v}_a^T \tanh(\mathbf{W}_a s_{t-1} + \mathbf{U}_a g_n) \quad (7)$$

其中, \mathbf{v}_a , \mathbf{W}_a , \mathbf{U}_a 是参数矩阵. 用 c_t 表示第 t 次解码的结果,代表了与解码结果最相关的原始信息,是 h_n 与 α_{tn} 加权平均,计算公式为

$$c_t = \sum_{n=1}^N \alpha_{tn} g_n \quad (8)$$

同时 c_t 在下次解码中会作为额外的信息输入到网络当中, s_t 是解码器在第 t 次解码时的状态.

3.2 工作记忆模型基本原理

在 Seq2Seq 古诗词生成的基础上,文献[19]提出了工作记忆模型. 该模型被划分为三个模块,分别为主题信息模块、历史信息模块、本地信息模块. 工作记忆模型生成诗词的过程如图 3 所示.

工作记忆模型的基础部分为门控循环单元(Gated Recurrent Unit, GRU)^[24]. 在生成过程中,工作记忆模型的输入分为两个阶段,其中第一个阶段的输入为主题词、模板信息和韵律信息;第二个阶段的输入是通过模型计算得到的,包括主题信息、历史信息和本地信息. 假设输出诗词由 n 句组成,表示为 $\{L_i\}_{i=1}^n$; 输入主题词共有 K 个,表示为 $\{W_k\}_{k=1}^K$; M_1 表示主题信息, M_2 表示历史信息, M_3 表示本地信息, $M = [M_1, M_2, M_3]$ 代表全部工作记忆信息. 主题

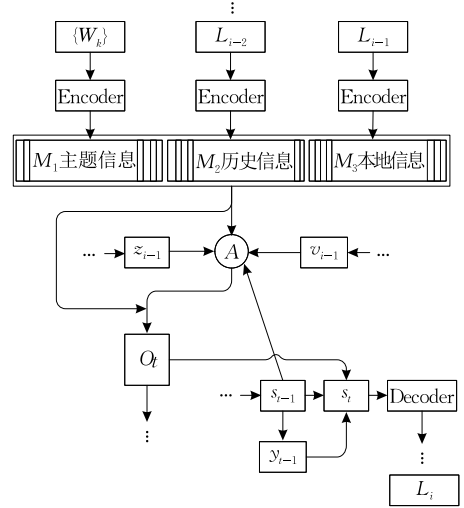


图 3 工作记忆模型诗词生成过程

词 W_k 被全部写入到主题信息 M_1 当中,并且在诗词生成的过程中保持不变,用来指导每一句诗词的生成,确保不偏离主题. 在生成第 i 句诗词 L_i 之前, L_{i-1} 的每一个字都会被写入本地信息 M_3 中. 与其它模型不同,这里并没有将 L_{i-2} 的全部信息写入到 M_2 ,而是从 L_{i-2} 当中选择最有代表意义的、最贴近主题的词或者字写入到历史信息中,这样可降低对主题的干扰. v_{i-1} 为全局追踪向量,记录已经生成的内容,为模型提供全局信息,随着诗句的生成不断更新. 为了保证生成诗词主题不偏离,设计了主题追踪机制,引入变量 z_{i-1} ,以更加明确的方式记录主题的使用信息. O_t 为信息的输出, s_t 为解码输出, β 表示投影参数, y_t 代表了第 t 次解码后词汇表中每个字符的概率信息,表达式为

$$s_t = \text{GRU}(s_{t-1}, [y_{t-1}, O_t, q_t, v_{t-1}]) \quad (9)$$

$$p(y_t | y_{1:t-1}, L_{1:t-1}, \mathbf{W}_{1:k}) = \text{softmax}(\beta s_t) \quad (10)$$

式(9)中 q_t 代表包含了平仄及押韵的韵律信息. 绝句诗词需要满足固定的格式和韵律,因此这里引入韵律分量,用来控制生成绝句诗词的格式和韵律. 在训练过程当中定义了 36 个音韵类别,训练的绝句诗词均为 5 言绝句或 7 言绝句. 工作记忆模型能够生成高质量的绝句诗词,但是所得到的诗词冗余很低,无法直接进行秘密信息的隐藏.

3.3 绝句生成模型

如何进行秘密信息的隐藏,同时保证生成诗词的质量,是需要解决的问题. 通过对工作记忆模型原理的分析,能够得出这样的结论:诗词生成的发起信息主要来源于“主题词”,生成诗词的第一行与主题词的关系最紧密. 假设:如果主题词能够出现在生成绝句诗的第一句中,且位置固定,那么就可以顺利地将秘密信息提取出来. 同时第一行诗词的生成,不依

赖于后序诗词,这样可以保证生成诗词的质量不受影响.基于以上分析与假设,我们提出了一种基于主题词的高质量绝句生成算法.首先鉴于 Seq2Seq 模型的诸多优点,文献[18-19,25]利用 Seq2Seq 模型,分别进行了古诗词生成算法的设计.虽然实施细节有所不同,但是大致可以划分为三个模块.本文以文献[25]为例进行介绍,第一个模块是由词生成诗句(Word-To-Line,WTL)的过程,第二个模块是由诗句生成诗句(Line-To-Line,LTL)的过程,第三个模块是由上下文生成诗句(Context-To-Line,CTL)的过程.图4是基于 Seq2Seq 诗词生成过程的示例.在诗词生成的过程当中,首先设置主题词为“秋雁”,然后通过 WTL 模块,生成第一句诗词;然后以第一句作为输入,经过 LTL 模块,生成第二句诗词;将第一、二句诗词作为输入,经过 CTL 模块生成第三句;最终由前三句诗词生成第四句诗词.三个模块的搭建都是以 Seq2Seq 模型为基础.

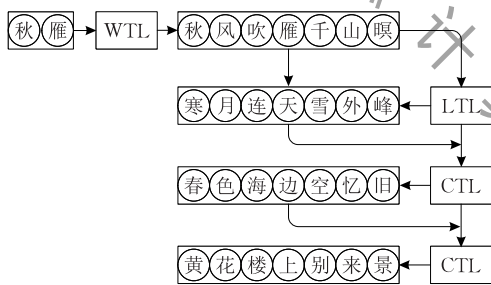


图4 基于 Seq2Seq 诗词生成过程

本文所提出算法重点是对工作记忆网络中 WTL 部分的改进,也就是由主题词到第一句诗词的生成过程.设主题词的个数为 1,在生成第一个字的解码过程中,通过式(9)可以得出 s_t 的解码状态为

$$s_{t=1} = GRU(s_0, [y_0, O_{t=0}, q_{t=0}, v_0]) \quad (11)$$

其中, s_0 为解码器初始状态, y_0 为起始信息对 $s_{t=1}$ 的作用.当 $O_{t=0}$ 时, O_t 的信息主要来源于主题词, v_0 在 $t=1$ 时没有记录信息.可以得出:第一行诗词的生成只和主题词相关.这样 $y_{t=1}$ 可由下式计算得到:

$$p(y_t | y_{1:t-1}, L_{1:t-1}, W_{1:k}) = \text{softmax}(\beta s_t) \quad (12)$$

此时可以得出, y_t 词汇表中每个字符的概率信息只与主题词和解码状态 $s_{t=1}$ 有关.基于上述理论分析,我们提出了基于主题词的绝句生成算法.通过调整训练阶段的参数及训练方法,能够保证主题词出现在生成绝句诗词的第一行的固定位置中.

下面以绝句《春晓》:“春眠不觉晓,处处闻啼鸟.夜来风雨声,花落知多少.”为例来介绍绝句的生成.绝句诗《春晓》的韵律及平仄信息符合绝句诗常用的

8个模板之一,其平仄及押韵的信息在图5中进行了标注.本文方案中 WTL 模块训练过程的主要思想和简要训练过程如图5所示.可以看出,在训练过程中平仄及音律信息也参与了编码计算,这对生成诗句质量的提高可起到帮助作用.模型在训练完成后不仅会注重字与字之间含义的匹配,且音律信息也会影响到候选字的选择,故生成文本的质量更高.由于本文方案生成的诗句还需隐藏秘密信息,所以对生成绝句的格式及音律等要求更加严格.因此我们在方案当中增加了音律惩戒因子,以使得生成的绝句诗符合模板的要求.在解码过程中,本文方案所使用绝句判定方法相较于其它文献更加精准,且可对汉语中的多音字进行区分辨别,从而确保提取秘密信息的准确性.接下来介绍本方案如何实现主题词自然地出现在预置的位置.

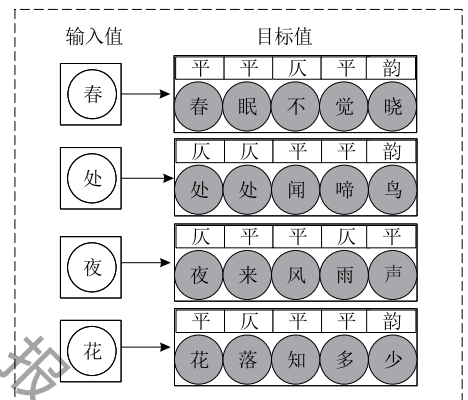


图5 WTL 模块训练过程

首先将输入的主题词设置为“春”,为保证主题词能够自然地隐藏到诗词当中,将“春眠不觉晓,处处闻啼鸟.夜来风雨声,花落知多少.”设置为目标值.可以看出,“春”在《春晓》当中位于首字的特殊位置.对其它的诗词也通过这样的方式进行训练.为了扩大训练样本,对其余的诗句也做同样的训练.从而使网络能够学习到主题词在诗词中的位置信息,确保模型在生成诗词的过程中,在给定主题词后,能够自动将主题词隐藏到固定的位置,同时保证生成诗词的质量不受影响.通过实验验证,当向模型输入主题词时,在预置的位置上经过计算后,词汇表 y_t 中所对应的主题词会以最低的损失出现在候选字当中.由此通过主题词的隐藏以及 y_t 中不同候选字的组合,经过损失计算生成不同的候选诗句,可实现大容量的秘密信息隐藏.实际上,主题词并非只能固定出现在诗句的首词或者首字,可根据需要调整训练

过程中输入主题词的位置,进而可生成主题词出现在首句任意位置的诗句。

4 信息隐藏和提取算法

4.1 信息隐藏

在进行信息隐藏前,我们把秘密信息分为 2 段,将主题词、绝句模板及韵律 3 个参数所对应的秘密信息称为第一段秘密信息,将候选诗句所对应的秘密信息称为第二段秘密信息. 信息隐藏算法具体可分为三步. 第一步:根据第一段秘密信息确定参

数;第二步:根据输入参数生成候选诗句;第三步:根据第二段秘密信息选取诗句. 秘密信息的隐藏过程如图 6 所示. 在第一步中,主要工作是根据分段后的秘密信息,确定要输入到模型中的参数. 参数分为三个部分:主题词(Keyword)、绝句模板(Pattern)、韵律(Rhyme). 其中 Keyword 根据训练数据确定,这里假设 Keyword 列表的大小为 K_{num} . 中国绝句诗词有非常严格的格式限制,常用的绝句模板共有 8 种,包括 5 言和 7 言各 4 种,因此这里 Pattern 的大小设置为 $P_{num}=8$. 韵律(Rhyme)控制方面,主要依据《词林正韵》,将韵律划分为 36 种,即 $R_{num}=36$.

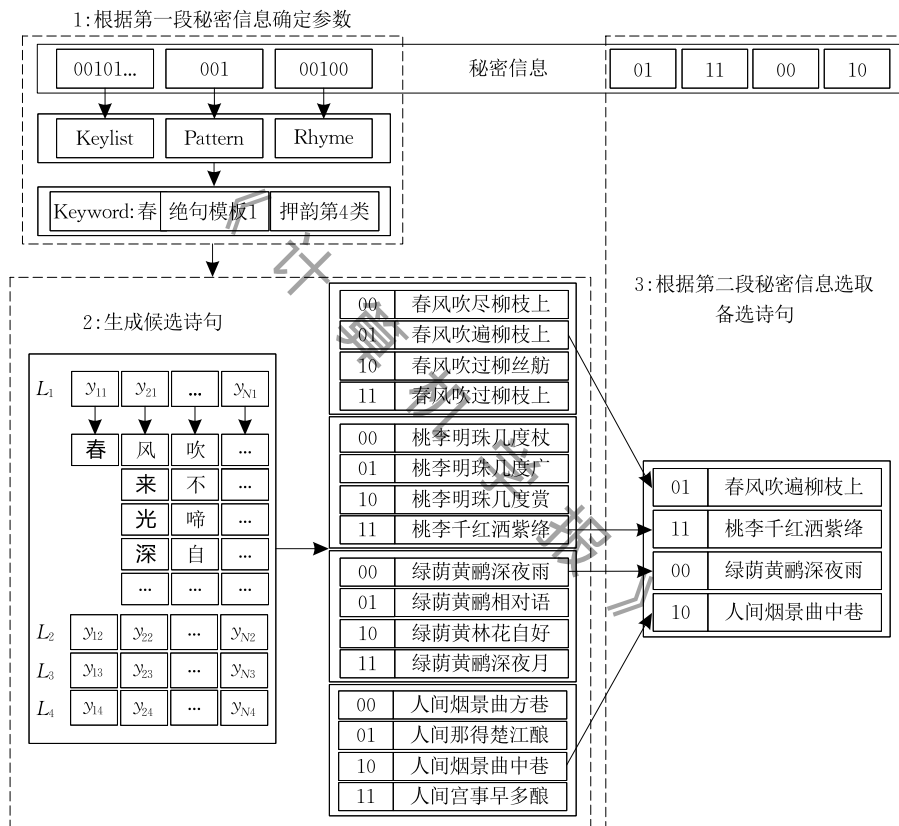


图 6 信息隐藏的流程图

在隐藏过程的第一步中,假设第一段秘密信息的长度为 D_1 比特,其计算公式为

$$\begin{aligned} D_1 &= \log_2(K_{num}) + \log_2(P_{num}) + \log_2(R_{num}) \\ &= \log_2(K_{num} \cdot P_{num} \cdot R_{num}) \end{aligned} \quad (13)$$

在第二步中,主要是根据秘密信息生成候选诗句. 假设 4 句绝句诗词的候选字集合分别为 L_1, L_2, L_3, L_4 . 设 $L_1 = \{y_{11}, y_{21}, \dots, y_{N1}\}$, N 为单句诗词的长度,可能的取值为 5 或者 7, y_{ij} 表示第 i 行的第 j 个位置的候选字列表,其所对应的概率列表称为候选字概率列表,列表长度为训练集中的字表大小.

在获取候选字概率列表后,如果直接以损失排序进行组合,那么所生成的诗句在语义上会有较大损失. 因此这里采用集束搜索算法(Beam-search)进行候选字的选择. Beam-search 算法是以较少的代价在相对受限的搜索空间找出近似最优解,且接近于整个搜索空间中的最优解. 图中所使用 $beam_{num}=4$,也就是说每一句诗可以有 4 句候选,且这 4 句候选语义上接近,归属于同一个主题. 同时在候选字选择的过程中,需要根据模板 Pattern 的“平仄”要求及韵律 Rhyme 要求,对候选字进行相应的惩罚,确保生成

的绝句诗符合模板的要求,同时保证秘密信息准确地提取。

在第三步中,主要工作是根据第二段秘密信息选取诗句,选取过程如图 6 所示. 首先将第二段秘密信息分割为四部分,然后根据秘密信息选取对应顺序的诗句. 在输入相同参数的情况下,所得到的候选诗句顺序相同,这样可确保能够正确提取秘密信息. 假设第二段秘密信息的长度为 D_2 比特,其计算公式为

$$D_2 = 4 \cdot \log_2(\text{beam}_{\text{num}}) \quad (14)$$

随着 beam_{num} 的增加,信息的嵌入率能得到较大的提升. 由式(13)和(14)可得到一首绝句诗隐藏秘密信息总长度 D 为

$$D = 4 \cdot \log_2(\text{beam}_{\text{num}}) + \log_2(K_{\text{num}} \cdot P_{\text{num}} \cdot R_{\text{num}}) \quad (15)$$

由式(15)可得出,本文所提出算法的信息嵌入率主

要与 4 个因素有关: beam_{num} 为候选诗句的个数,在一定范围内可自行设置; P_{num} 为固定值 8,即绝句诗模板有 8 种; R_{num} 为韵律种类,在本文算法中设为 36; K_{num} 为主题词的个数,可根据实际情况进行设置,在本方案中,主题词的个数不会影响提取算法的效率。

4.2 信息提取

本文提取算法的流程如图 7 所示. 提取算法基本上是隐藏算法的逆过程,可以分为三个步骤. 第一步:使用模板工具判定绝句诗的主题词 Keyword、模板类型 Pattern 及押韵情况 Rhyme,即第一段秘密信息. 在第一步中无法提取 beam_{num} 值, beam_{num} 是收发双方共同约定的参数;第二步:根据第一步中获取的参数,生成候选诗句;第三步:根据接收到的绝句诗,对照候选诗句,提取第二段秘密信息。

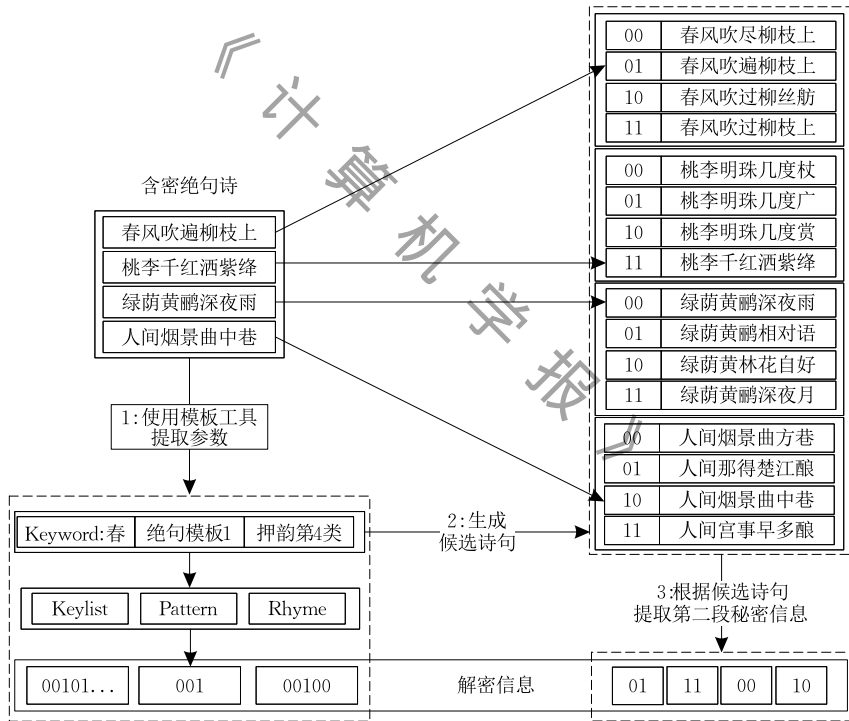


图 7 信息提取的流程图

具体来说,在第一步中,首先根据主题词的隐藏规则,查找主题词的位置并提取主题词,如“春”,再提取主题词所对应的秘密信息;然后对照平仄信息表,查找每一个字对应的平仄信息,确认模板 Pattern 类型并提取秘密信息;在押韵类型 Rhyme 判定过程中,对多音字进行区分,即一个汉字仅对应一种押韵类型,以保证 Rhyme 判定的结果唯一,再通过判定结果提取秘密信息. 通过以上步骤即可提取第一段秘密信息,同时获得生成绝句诗的参数信息. 在第二

步中,根据第一步中得到的参数信息,生成候选诗句,为第三步第二段秘密信息的提取做准备. 在第二步中,不需要对参数进行排列组合以及遍历所有可能的诗句,因为我们可以从含密绝句诗中获取所有参数信息,即本文提取算法更加灵活,且满足实时性要求. 在第三步中,我们根据生成的候选诗句,对照接收到的含密绝句诗,查找位置信息,即可完成对第二段秘密信息的提取. 通过将提取出的两段秘密信息进行级联,即可获得本文算法隐藏的全部秘密信息。

5 实验结果及对比分析

下面从生成绝句诗的质量、嵌入率、算法复杂度及安全性和鲁棒性等方面进行实验分析与比较。

5.1 实验数据集及参数设置

本文实验中共用到绝句诗 25 000 首^[26], 其中训练数据 23 000 首, 测试数据为 1 000 首, 验证数据为 1 000 首. 实验中我们提取每一句诗词的前两个字作为主题词. 在训练过程中首先提取一首绝句诗中的 4 个主题词. 对于一首绝句诗, 随机选取 1 到 4 个主题词作为输入信息进行训练. 训练过程中模型的具体参数设置如下: 词向量长度为 256, 隐层网络为 512 层, 音律向量长度为 64, 全局追踪向量长度为 512, 主题追踪向量长度为 24. 每次训练输入的 batch 包含 64 首诗词, tanh 函数作为激活函数, 同时为了防止过拟合问题, dropout 的参数设置为 25%. 词向量使用 Word2vec 模型对整个语料库进行生成. 模型训练过程当中, 设置最低字频为 3, 也就是只使用出现频数大于 3 次的字. 经过筛选后, 整个字表的大小为 4540, 主题词的个数为 92 000. 整个模型使用 Tensorflow 框架搭建, 训练过程中使用 Nvidia RTX2060 显卡进

行计算.

5.2 生成诗词质量分析比较

文献[19]工作记忆模型生成诗词的质量较高, 并从流畅度、意境、连贯性、美学 4 个角度进行了分析. 因此本文算法生成诗词的质量主要与工作记忆模型生成诗词质量进行对比. PPL(perplexity)是自然语言处理领域中衡量语言模型性能的指标之一, 能够反映出一个模型训练的效果. PPL 的取值可以理解为在模型生成文本时, 当前待生成词有多少种合理的选择, 可选词的数量越少, 则认为模型越准确. 也就是说, PPL 越小模型拟合效果越好. 因此, 本文在实验比较中采用 PPL 值作为衡量生成诗句的流畅度、意境、连贯性和美学等方面的评价指标. 为了确保实验的公平性, 我们使用了相同的网络参数和语料库, 分别对绝句生成模型和工作记忆模型进行训练. 最终在训练集上达到了相近的水平. 本文模型在训练数据集上得到的 PPL 值为 4.02, 训练损失值为 1.391; 工作记忆模型在训练集上得到的 PPL 值为 4.53, 训练损失值为 1.538. 从理论上讲, 本文模型生成诗词的质量与工作记忆模型基本处于同一水平. 下面对两种模型生成诗词的质量进行展示和比较, 如图 8 所示.

文献[19]工作记忆模型	本文绝句生成模型	文献[19]工作记忆模型	本文绝句生成模型
Key:秋月, Pattern:0, Rhyme:25 秋风吹鬓老丝侵 江上吟诗空未寻 苍屋不知新月色 且云无数照人心	Key:秋月, Pattern:0, Rhyme:25 秋月自堪怜我老 孤灯寒雨过潇吟 停舟日后更相思 回首西山一片心	Key:风, Pattern:2, Rhyme:7 三十年来此地无 万山千里几时趋 天边风景消磨尽 清水芙蓉泛钓鱼	Key:风, Pattern:2, Rhyme:7 风絮飞花入画图 琴书却得与人无 江南万古今犹有 说尽英雄泪满渠
Key:西湖, Pattern:1, Rhyme:1 五湖无处觅西风 南去飞来未可穷 青鸟不知江路好 白头犹见月生中	Key:西湖, Pattern:1, Rhyme:1 西湖无限好相逢 东望斜阳欲断风 日暮江南春不到 十年憔悴一生空	Key:花, Pattern:3, Rhyme:3 何年花下重相见 共得天涯一片香 吹笛不成归路晚 忆君常遣使人望	Key:花, Pattern:3, Rhyme:3 花开三径流香去 从里幽人十月凉 梅底满山愁不到 风尘难向曲头长
Key:鸳鸯, Pattern:4, Rhyme:4 鸳鸯入画舫 丛竹映清爽 孤棹轻寒日 明朝醉别赏	Key:鸳鸯, Pattern:4, Rhyme:4 鸳鸯戢翼样 倒发紫罗幌 为客三千里 如今一夜相	Key:雪, Pattern:6, Rhyme:30 三年雪未落 栽竹渐深脚 数叶梅花在 西园柳絮各	Key:雪, Pattern:6, Rhyme:30 雪郎积翠幄 星聚泛银药 月色千年紫 日无一骑鹤
Key:野水, Pattern:5, Rhyme:10 野水碧山外 疏林拂石蟹 远云移积翠 行雁未全霏	Key:野水, Pattern:5, Rhyme:10 野水入秦塞 将军过汉代 何人求一树 九日泪痕彩	Key:红, Pattern:7, Rhyme:9 红药阶前草 青山柳色开 也知千载后 犹以陆名台	Key:红, Pattern:7, Rhyme:9 红雨青山外 孤舟野水开 东风吹客去 落月满江台
主题词为两个字组成		主题词为单字	

图 8 生成的绝句及质量对比

实验当中生成诗词的输入参数为随机选择, 接下来从生成诗词的质量及主题契合度两个方面进行分析. 第一方面: 生成诗词质量分析. 图 8 当中展示 16 首古诗词, 分别是本文绝句生成模型和文献[19]工作记忆模型生成的绝句诗. 通过阅读和对格律的分析, 本文算法所生成的绝句诗符合绝句模板的要

求且抑扬顿挫感强烈, 与工作记忆模型所生成诗词质量相当. 因为本文算法在训练过程中对韵律进行了编码, 因此与文献[17-18, 20, 25]仅考虑词向量的算法相比, 本文算法所生成诗词在韵律方面更加自然. 文献[5, 15-16]中的方法并没有生成新的词语, 而是从出现过的词语中根据规律进行选择, 因此所

生成的诗词在语义表达方面不够理想. 本次实验中所选取的绝句数量相对较少, 还可以扩大训练语料库, 再次提高生成绝句诗的质量. 第二方面: 主题词与主题的契合情况. 本文在实验中分别尝试不同的输入参数, 然后对所生成诗词的主题进行分析. 本文算法实验中主题词分别选取的是: 秋月、西湖、鸳鸯、野水、雪、红、风、花. 其中秋月、西湖、鸳鸯、野水为本文模型和文献[19]模型共有的主题词; 雪、红、风、花并不在本文模型的主题词列表当中. 但是可以看出, 这两种情况下本文方法的主题词与生成诗句主题均非常契合, 同时生成诗词的质量与文献[19]相当.

5.3 嵌入率分析与比较

嵌入率是衡量隐藏算法的重要指标. 文献[5, 15-16]以词组为基础进行秘密信息的隐藏, 随着候选词组的增加, 嵌入率能够不断提高; 文献[20]是以单个字为基础进行秘密信息的隐藏, 在嵌入率方面有突出的表现, 但是在候选字过多的情况下其生成诗词的质量一般, 很容易引起攻击者怀疑. 因此在保证生成诗词质量的条件下, 候选字的数量需要控制在一定范围内. 文献[27]是较早提出使用模板生成文本进行信息隐藏的方案之一, 其由两部分组成, 即词典和写作风格模板. 词典是(类型, 单词)对的列表, 其中类型可以是词性或者同义词集合; 风格模板是类型序列, 同时控制大小写、标点和空格等. 在本文方法中, 直观来看每一次输出的结果都是以整句诗的形式出现, 但本质上本文算法也是以字为单位进行选择的隐藏方法. 以上算法的嵌入率结果如图9所示.

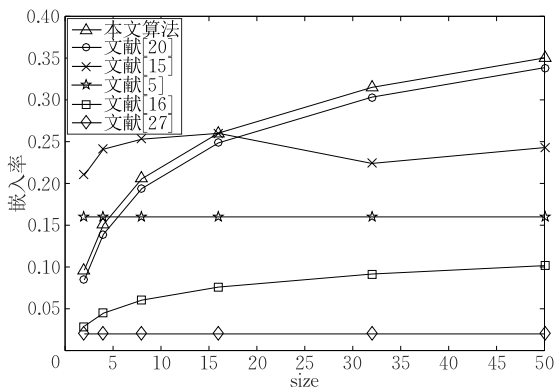


图9 不同方法嵌入率比较结果

在实验中, 字表的大小为 4540, 每一句诗的候选诗句理论上有着 4540^N 种选择, 这是一个相对较大的选择范围, 意味着本文方案有很高的嵌入率. 为了

保证生成诗句的质量, 本文采用 Beam-search 算法对候选字进行筛选. 该算法的选择过程是对候选字动态规划选择的过程, 因此总能从 4540^N 种诗句中选取到质量相对较好的诗句. 由式(15)可以得出, 本文算法的嵌入率主要与 $beam_{num}$, R_{num} , K_{num} , P_{num} 相关. 由于模板中的平仄信息可能与主题词 Keyword 的平仄信息冲突, 因此实验中没有在 P_{num} 中嵌入秘密信息. 同时本文将 $beam_{num}$ 转换为单字的嵌入表达方式, 以便与其它文献进行公平地比较, 其中备选列表的大小 $size$ 满足:

$$size^N = beam_{num} \quad (16)$$

一个汉字或标点符号在计算机中存储需要 16 比特, 最终得出嵌入率 ER (Embedding Rate) 的计算公式为

$$ER = \frac{4 \cdot N \cdot \log_2(size) + \log_2(K_{num} \cdot R_{num})}{4 \cdot (N+1) \cdot 16} \quad (17)$$

其中, N 的取值为 5 或者 7, 分别对应五言绝句和七言绝句. 实验中, 训练集主题词数量共有 92000 个, 我们选取其中的 40000 个用于生成绝句诗并隐藏信息, 即 $K_{num} = 40000$. 与其它方案进行对比之前, 对参数进行了统一, 确保实验在同一个标准下进行. 通过对图9的分析不难发现, 本文方法在嵌入率方面表现较好. 虽然文献[5]和文献[15]的方法在嵌入率方面也有较好的表现, 但是其生成诗词的质量不够理想. 文献[16]生成诗词的质量相对有所提高, 但是其方案嵌入率偏低. 文献[20]方法的嵌入率与本文方法比较接近, 但文献[20]信息提取算法的复杂程度要远高于其它算法.

5.4 算法复杂度分析与比较

本文隐藏算法和提取算法所用到的字典码本均属于预生成, 故这里主要对比隐藏算法及提取算法本身的复杂度. 本文隐藏算法中主要的操作包括选取主题词 Keyword、模板 Pattern 和韵律 Rhyme, 这些量均为固定值, 因此这一步的时间复杂度为 $O(1)$; 然后根据选择的这三个值来生成绝句诗, 该过程的算法复杂度主要集中在选字排序过程, 时间复杂度为 $O(size \cdot N)$, 其中 $size$ 为候选字的个数, N 为诗句的长度, 这样隐藏算法的时间复杂度为 $O(n^2)$. 提取过程中, 仅需根据主题词 Keyword 词典、韵律 Rhyme 词典获取索引, 然后再根据备选诗句获取索引, 以提取秘密信息, 时间复杂度为 $O(size \cdot N)$, 这样提取算法的复杂度为 $O(n^2)$. 其它文献的隐藏及提取算法复杂度如表1所示.

表 1 算法复杂度比较

算法	信息隐藏复杂度	信息提取复杂度
文献[5]	$O(1)$	$O(n)$
文献[15]	$O(1)$	$O(n)$
文献[16]	$O(n^2)$	$O(n)$
文献[20]	$O(n^2)$	$O(n^4)$
本文算法	$O(n^2)$	$O(n^2)$

在文献[5,15-16,20]中,只有文献[20]与本文方案的嵌入率相当,但是本文提取算法的效率要明显高于文献[20];但与其它文献相比,本文算法因为对生成诗词的质量要求更高,故算法复杂度也相对较高.文献[20]没有将生成诗词需要的输入信息隐藏到诗句中,需要根据现有的主题词词库和模板信息将所有可能出现的诗句遍历生成,然后才能提取秘密信息,其提取算法的时间复杂度为 $O(\text{size} \cdot N \cdot K_{\text{num}} \cdot P_{\text{num}})$,也就是 $O(n^4)$.而本文提取算法复杂度仅为 $O(n^2)$.所以从算法复杂度角度分析,相较于文献[20],本文方案更加灵活,能够实现实时的信息隐藏和提取,应用场合更加广泛.

5.5 安全性及鲁棒性分析

关于本文方案的安全性,攻击者如果想获取到秘密信息,或者通过大数据分析破解秘密信息,那么攻击算法需要做到以下几点:(1)分析提取生成绝句诗的主题词,包括主题词的字数和位置;(2)统计分析主题词所对应的二进制码;(3)分析生成诗句次序所对应的二进制码;(4)获取本方案的训练数据,并对训练数据进行分析;(5)即使训练数据被公开,攻击者需要达到与收发双方相同的模型损失值.因为损失值的不同意味着模型的拟合程度不同,即使使用相同的主题词所生成的诗句也可能不一致.

综上所述,攻击者想要获取本文方案的秘密信息非常困难.同时与其它文献对比,如文献[15]中基于宋词生成的方案,其所生成的宋词为词库组合而成,而词库是根据已有的宋词作品分词形成,并没有新的词语生成.这样攻击者很容易就可以获取词库中的大部分词组,进而进行分析.而本文方案所生成的文本是根据模型计算得到的,有新的词语和诗句生成,对攻击者而言分析的成本明显更高.

另外,本文方案生成的诗句在传输过程中,可能遭到恶意篡改或者攻击.如果是对文本格式的篡改,那么秘密信息的提取不受影响;如果是对文本内容进行篡改,被篡改部分的秘密信息将无法正确提取,但接收者能够定位被篡改的部分.假设在信息隐藏方案被公开的情况下,由于本文方案所生成文本的质量较高,隐蔽性较好,因此信息隐藏的行为被发现

的风险要低于其它文献方法,即本文的方案更加安全.在传输秘密信息的过程中,可以利用主题词和候选诗句来进行秘密信息的隐藏,这样就可以避免统计特征均匀分布的问题.同时可考虑将本文方案应用于多用户的场景,为了避免同一个秘密信息由相同的诗句来表达,可通过将多个主题词对应同一秘密信息来实现.

6 总 结

本文提出了一种基于绝句生成的构造式信息隐藏算法,实现了秘密信息的大容量隐藏,同时生成的绝句诗质量较好,且算法安全性高.训练过程中通过主题信息、历史信息和本地信息的综合作用生成高质量诗句,通过加入韵律向量来保证生成诗句的音律流畅自然.信息隐藏过程中向模型输入主题词、模板及押韵信息,模型经过计算生成候选诗句,而后隐藏秘密信息.信息提取过程中,主题词的自然隐藏保证了秘密信息能够实时准确提取.下一步的工作可以通过生成不同风格的古诗词,如宋词、对联等,来扩展隐藏秘密信息文本的种类,然后增加主题词的数量进一步提高生成文本的质量,提高嵌入率.

致 谢 在此,我们向对论文提出宝贵意见的审稿专家们表示衷心的感谢!

参 考 文 献

- [1] Katzenbeisser S, Petitcolas F A P. Information Hiding Techniques for Steganography and Digital Watermarking. Massachusetts, USA: Artech House, 2000
- [2] Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge, UK: Cambridge University Press, 2009
- [3] Zamani M, Manaf A B A, Ahmad R B, et al. A secure audio steganography approach//Proceedings of the IEEE International Conference for Internet Technology and Secured Trans (ICITST). London, UK, 2009: 1-6
- [4] Mazurczyk W, Wendzel S, Zander S, et al. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures. New Jersey, USA: John Wiley and Sons, 2016
- [5] Yu Zhen-Shan, Huang Liu-Sheng, Chen Zhi-Li, et al. High embedding ratio text steganography by ci-poetry of the Song dynasty. Journal of Chinese Information Processing, 2009, 23(4): 55-62(in Chinese)
(于振山, 黄刘生, 陈志立等. 用宋词实现高嵌入率文本信息隐藏. 中文信息学报, 2009, 23(4): 55-62)

- [6] Zhang Xin-Peng, Qian Zhen-Xing, Li Sheng. Prospect of digital steganography research. *Journal of Applied Sciences*, 2016, 34(5): 475-489(in Chinese)
(张新鹏, 钱振兴, 李晟. 信息隐藏研究展望. *应用科学学报*, 2016, 34(5): 475-489)
- [7] Kim Y W, Moon K A, Oh I S. A text watermarking algorithm based on word classification and inter-word space statistics//*Proceedings of the 7th International Conference on Document Analysis and Recognition (ICDAR)*. Edinburgh, UK, 2003: 775-799
- [8] Ramakrishnan B K, Thandra P K, Srinivasula A V S M. Text steganography: A novel character-level embedding algorithm using font attribute. *Security and Communication Networks*, 2017, 9(18): 6066-6079
- [9] Lee C, Chen H. Data concealment scheme for HTML documents based on color code//*Proceedings of the 5th International Conference on Intelligent Information Hiding & Multimedia Signal Processing*. Kyoto, Japan, 2009: 632-635
- [10] Kumar R, Malik A, Singh S, et al. A space based reversible high capacity text steganography scheme using Font type and style//*Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA)*. Noida, India, 2016: 1090-1094
- [11] Su B, Ding X Y, Liu G S, et al. An information hiding method for text by substituted conception//*Proceedings of the 4th International Symposium on Information Science and Engineering*. Shanghai, China, 2012: 131-135
- [12] Xiang L Y, Li Y, Hao W. Reversible natural language watermarking using synonym substitution and arithmetic coding. *Computers Materials & Continua*, 2018, 55(3): 541-559
- [13] Yang Y, Chen Y W, Chen Y L. A novel universal steganalysis algorithm based on the IQM and the SRM. *Computer, Materials & Continua*, 2018, 56(2): 261-271
- [14] Xiang L Y, Yu J M, Yang C F, et al. A word-embedding-based steganalysis method for linguistic steganography via synonym substitution. *IEEE Access*, 2018, 6: 64131-64141
- [15] Liu Y C, Wang J, Wang Z B, et al. A technique of high embedding rate text steganography based on whole poetry of song dynasty//*Proceedings of the 2nd International Conference on Cloud Computing and Security*. Nanjing, China, 2016: 178-189
- [16] Luo Y B, Huang Y F, Li F F, et al. Text steganography based on ci-poetry generation using Markov chain model. *KSII Transactions on Internet and Information Systems*, 2016, 10(9): 4568-4584
- [17] Zhang X, Lapata M. Chinese poetry generation with recurrent neural networks//*Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*. Doha, Qatar, 2014: 670-680
- [18] Wang Z, He W, Wu H, et al. Chinese poetry generation with planning based neural network//*Proceedings of the 26th International Conference on Computational Linguistics*. Osaka, Japan, 2016: 1051-1060
- [19] Yi X, Sun M, Li R, et al. Chinese poetry generation with a working memory model//*Proceedings of the 27th International Joint Conference on Artificial Intelligence*. Stockholm, Sweden, 2018: 4553-4559
- [20] Luo Y, Huang Y. Text steganography with high embedding rate: using recurrent neural networks to generate Chinese classic poetry//*Proceedings of the 7th ACM Workshop on Information Hiding & Multimedia Security*. New York, USA, 2017: 99-104
- [21] Sutskever I, Vinyals O, Le Q V. Sequence to sequence learning with neural networks//*Proceedings of the Neural Information Processing Systems*. Montreal, Canada, 2014: 3104-3112
- [22] Vaswani A, Shazeer N, Parmar N, et al. Attention is all you need//*Proceedings of the 31st International Conference on Neural Information Processing Systems*. California, USA, 2017: 6000-6010
- [23] Hochreiter S, Schmidhuber J. Long short-term memory. *Neural Computation*, 1997, 9(8): 1735-1780
- [24] Cho K, Van M B, Bahdanau D, et al. On the properties of neural machine translation: Encoder-decoder approaches//*Proceedings of the Empirical Methods in Natural Language Processing*. Doha, Qatar, 2014: 103-111
- [25] Yi X, Li R, Sun M. Generating Chinese classical poems with RNN encoder-decoder//*Proceedings of the 16th China National Conference*. Nanjing, China, 2017: 211-223
- [26] Zhang J, Feng Y, et al. Flexible and creative Chinese poetry generation using neural memory//*Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics*. Vancouver, Canada, 2017: 1364-1373
- [27] Chapman M, Davida G. Hiding the hidden: A software system for concealing ciphertext in innocuous text//*Proceedings of the International Conference on Information and Communications Security*. Beijing, China, 1997: 335-345



QIN Chuan, Ph.D., professor, Ph.D. supervisor. His research interests include multimedia security and image processing.

WANG Meng, B.S.. Her research interests include information hiding and image processing.

SI Guang-Wen, M.S.. His research interests include information hiding and deep learning.

YAO Heng, Ph.D., associate professor. His research interests include multimedia forensics, information hiding, image processing and pattern recognition.

Background

The research of this work belongs to the field of information hiding, also named as data hiding. As we know, with the continuous improvement of computing power, the possibilities of traditional information hiding methods being detected and then being cracked are increasing. As a result, the technique of coverless information hiding appears. The characteristic of coverless information hiding is; cover data will not be modified, thus, the possibility of being noticed by the third party is obviously declining, and the risk of being cracked is also decreased greatly. At present, there are two main types of coverless information hiding methods; one is based on the cover selection strategy, and the other is based on the cover generation strategy, which can also be called as the constructive information hiding. However, two main challenges exist in the design of information hiding method based on text generation, one is the semantic quality of generated text, and the other is the embedding rate of secret information. Currently, these two problems have not been well solved, especially for these mantic quality of generated texts. This work focuses on constructive information hiding with Chinese quatrain generation, and the semantic quality of our generated quatrain poetry has better performance than that of the existing methods. In the procedure of quatrain

poetry generation, our method uses the Seq2Seq model, and pays more attention to the rhyme of quatrain poetry and the corresponding relationship with the theme, thus, the quatrain poetry generated by our model is more natural and smooth. In addition, the embedding rate of our method is also greater than that of some state-of-the-art methods.

This work is supported in part by the National Natural Science Foundation of China project “Reversible Data Hiding in Encrypted Images Based on Distributed Source Coding and Side-Information Optimization Mechanism” under Grant No. 61672354, which aims at embedding additional information into cipher data sent from the content owner on the data-hider side, recovering the original plaintext data on the receiver side, and realizing data labeling, management and tracking without revealing the plaintext content and sacrificing the privacy of content owner, and is also supported in part by the NSFC project “Noise Inconsistency Based Image Forensic Research Using High-Order Statistical Analysis and Local Homogeneity Constraints” under Grant No. 61702332, which focuses on using the high-order statistical-based noise estimation method as the entry point to study the new theories and methods of noise estimation and its forensic applications.