一种基于前馈网络的分组密码体制

成 旭[1],赵学民[2]

(1.长安大学 信息工程学院,陕西 西安 710064;
2.郑州航空工业管理学院 计算机科学与应用系,河南 郑州 450015)

摘 要:研究了分组密码体制及前馈神经网络的特征,构造了一种分组密码体制的数学模型,并基于二层前馈网络具体实现了该分组密码体制。在此基础上进行了仿真,结果表明该分组密码体制是可行的;针对其安全性进行了大量的实验,说明此分组密码体制具有较高的安全性,具有很好的混乱特征和扩散特征,可以用于信息安全领域的加/解密过程。

关键词:分组密码;加密;解密;前馈神经网络

中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2007)01-0167-03

A Block Cipher Based on Feed-Forward Neural Network

CHENG Xu[1], ZHAO Xue-min[2]

(1. Department of Information Engineering, Chang'an University, Xi'an 710064, China;
2. Department of Computer Science & Application, Zhengzhou Institute of Aeronautical Industry Management, Zhengzhou 450015, China)

Abstract: Research the feature of block cipher cryptosystem and feed-forward neural network, the model of a block cipher is structured and realized based on two-layer feed-forward neural network in this paper. Simulations indicate that the block cipher is feasible. And through a large number of experiments, the block cipher presents high degree of security, confusion and diffusion. Therefore, the block cipher can be used in process of encryption and decryption.

Key words: block cipher; encryption; decryption; feed-forward neural network

0 引 言

密码技术是信息安全技术的核心,它主要由密码编码技术和密码分析技术两个分支组成[1]。20世纪90年代初,意大利的神经网络专家 Francesco E. Lauria 提出将神经网络用于密码学领域的设想,并进行了论述[2,3]。1994年杜生辉等提出用单层感知机构造分组密码[4],1998年章照止等提到用神经网络模型构造分组密码[5],2001年齐锐等提出一种基于神经网络的对称密码系统[6]等等。

文中在此基础上从前馈神经网络的特性出发,基于前馈网络构造了一种分组密码的数学模型,该模型具有很好的混乱特征和扩散特征;用一个两层前馈网络具体实现了该分组密码模型。

1 基于前馈网络的分组密码的数学模型

1.1 一种满足混乱规则的分组密码的数学模型

假设明文分组共 N 小块,即为:$\boldsymbol{M}=(m_0,m_1,\cdots,m_{N-1})$,相应的密文分组也为 N 小块,即:$\boldsymbol{C}=(c_0,c_1,\cdots,c_{N-1})$,其中,$m_i\in\{0,1,\cdots,N-1\}$,$c_i\in\{0,1,\cdots,N-1\}(i=0,1,\cdots,N-1)$。

加密函数为:$c_i=E_{\boldsymbol{K}_{E_i}}(m_i)\equiv(m_i+k_i)\bmod N$ (1)

其中,加密密钥为:$\boldsymbol{K}_E=(k_0,k_1,\cdots,k_{N-1})$,$k_i\in\{0,1,\cdots,N-1\}(i=0,1,\cdots,N-1)$。

相应的解密函数为:

$$m_i=D_{\boldsymbol{K}_{D_i}}(c_i)\equiv(c_i+N+(-k_i))\bmod N \quad (2)$$

其中,解密密钥与加密密钥互为相反数,即 $\boldsymbol{K}_D=(-k_0,-k_1,\cdots,-k_{N-1})$,$k_i\in\{0,1,\cdots,N-1\}(i=0,1,\cdots,N-1)$。

由于模运算是一种非线性运算,所以以上的加/解密函数能够表现出一定的混乱特征。但加/解密函数的扩散特征却太不明显。

1.2 一种满足扩散规则的分组密码的数学模型

假设明文分组共 N 小块,即为:$\boldsymbol{M}=(m_0,m_1,\cdots,m_{N-1})$,相应的密文分组也为 N 小块,即:$\boldsymbol{C}=(c_0,c_1,\cdots,c_{N-1})$,其中 $m_i\in\mathbf{Z}$,$c_i\in\mathbf{Z}(i=0,1,\cdots,N-1)$。

加密函数为:

$$c_i=E_{\boldsymbol{K}_{E_i}}(\boldsymbol{M})=\sum_{j=0}^{N-1}\boldsymbol{K}_{E_{i,j}}\times m_j \quad (3)$$

收稿日期:2006-04-05

作者简介:成 旭(1978-),男,河南信阳人,硕士研究生,研究方向为计算机网络与信息技术。

其中，$\boldsymbol{K}_E = \begin{bmatrix} k_{0,0} & k_{0,1} & \cdots & k_{0,N-1} \\ k_{1,0} & k_{1,1} & \cdots & k_{1,N-1} \\ \vdots & \vdots & \vdots & \vdots \\ k_{N-1,0} & k_{N-1,1} & \cdots & k_{N-1,N-1} \end{bmatrix}$ 为加密密钥，$k_{i,j} \in \mathbf{R}(i,j = 0,1,\cdots,N-1)$。相应的解密函数为：

$$m_i = D_{\boldsymbol{K}_{D_i}}(c_i) \equiv \sum_{j=0}^{N-1} \boldsymbol{K}_{E_{i,j}} \times c_j \tag{4}$$

其中，解密密钥与加密密钥互为逆矩阵，即 $\boldsymbol{K}_D = (\boldsymbol{K}_E)^{-1}$。

总体上说，这种加/解密函数的扩散特征还是比较明显的，但其混乱特征并不明显。

1.3 基于前馈网络的分组密码的模型

1.3.1 数学模型

C. E. Shannon 在他的经典论文[7]中提出，两种密码系统通过“乘积”的方式可以被组合在一起。根据这种理论，可以把 1.1 节和 1.2 节讨论的两种模型分别作为两个密码系统 T 和 R，各自用一层前馈神经网络来实现；通过“乘积”的方式就可以得到一种同时满足混乱规则和扩散规则的新密码系统(如图 1 所示)。

1.3.2 安全性分析

在第一层加密系统 T 中，由于各个神经元用到的传输函数是模运算，而模运算是一种非线性运算；在第二层加密系统 R 中，也用到了矩阵相乘的运算，所以该模型总体上能够表现出较好的混乱特征。

在第二层加密系统 R 中，由于明文对密文的扩散影响程度很高，密钥对密文的扩散影响程度也较高，所以该层总体上能够表现出很好的扩散特征。

当密码分析者采用穷举密钥空间攻击时，由于需要穷举加密密钥 K_1 和加密密钥 K_2 的密钥空间，而在理论上加密密钥有无穷种不同的选法，所以仅仅靠穷举密钥空间来得到明文在理论上是不可行的，即此分组密码体制是无条件安全的。

2 用于分组密码体制的两层前馈网络的具体实现

假设已经把原始明文变成加密过程所需要的数字形式，以便作为加密网络的输入向量。把原始的二进制明文分成一个分组序列，其中每个分组包含 N 个小块，每个小块由 M 位二进制位组成，且 $N \in [1,2^M]$，即每个明文分组包括 $M \times N$bit。M 和 N 的值由消息源和目的地双方共同约定。图 2 是图 1 所述模型的加密部分的具体实现，图 3 是图 1 所述模型的解密部分的具体实现。

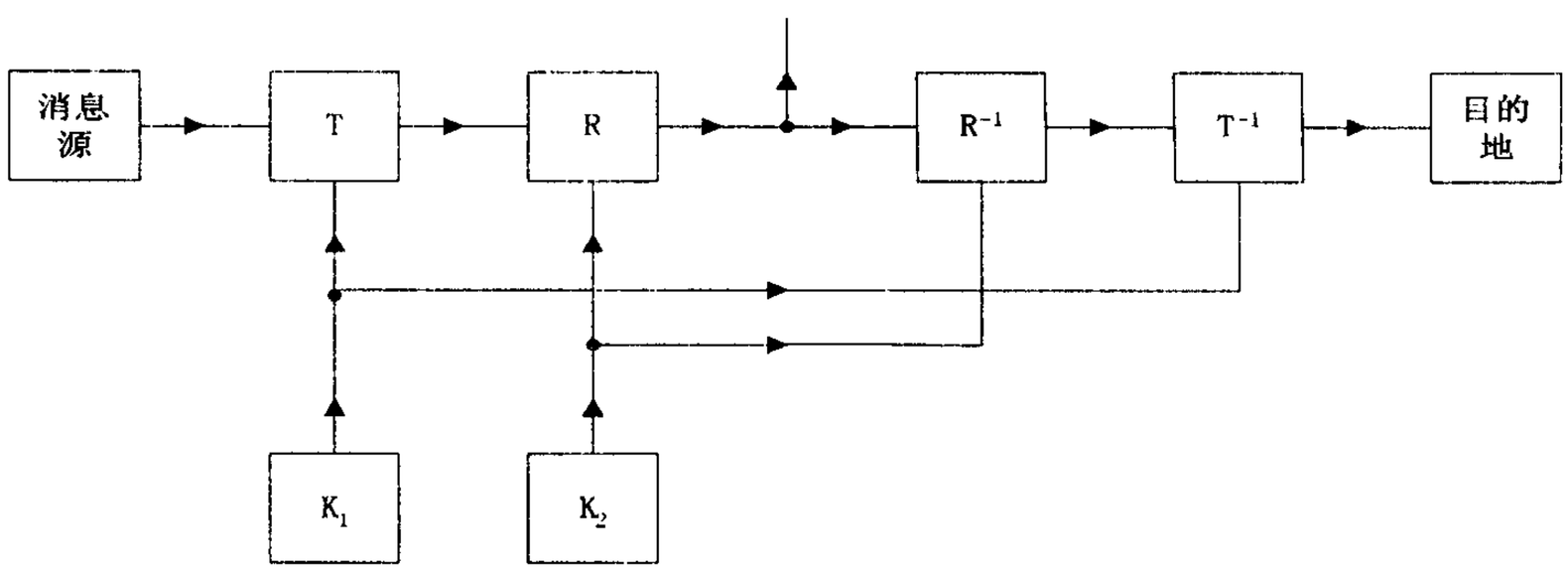

图 1 基于两层前馈网络的分组密码的模型

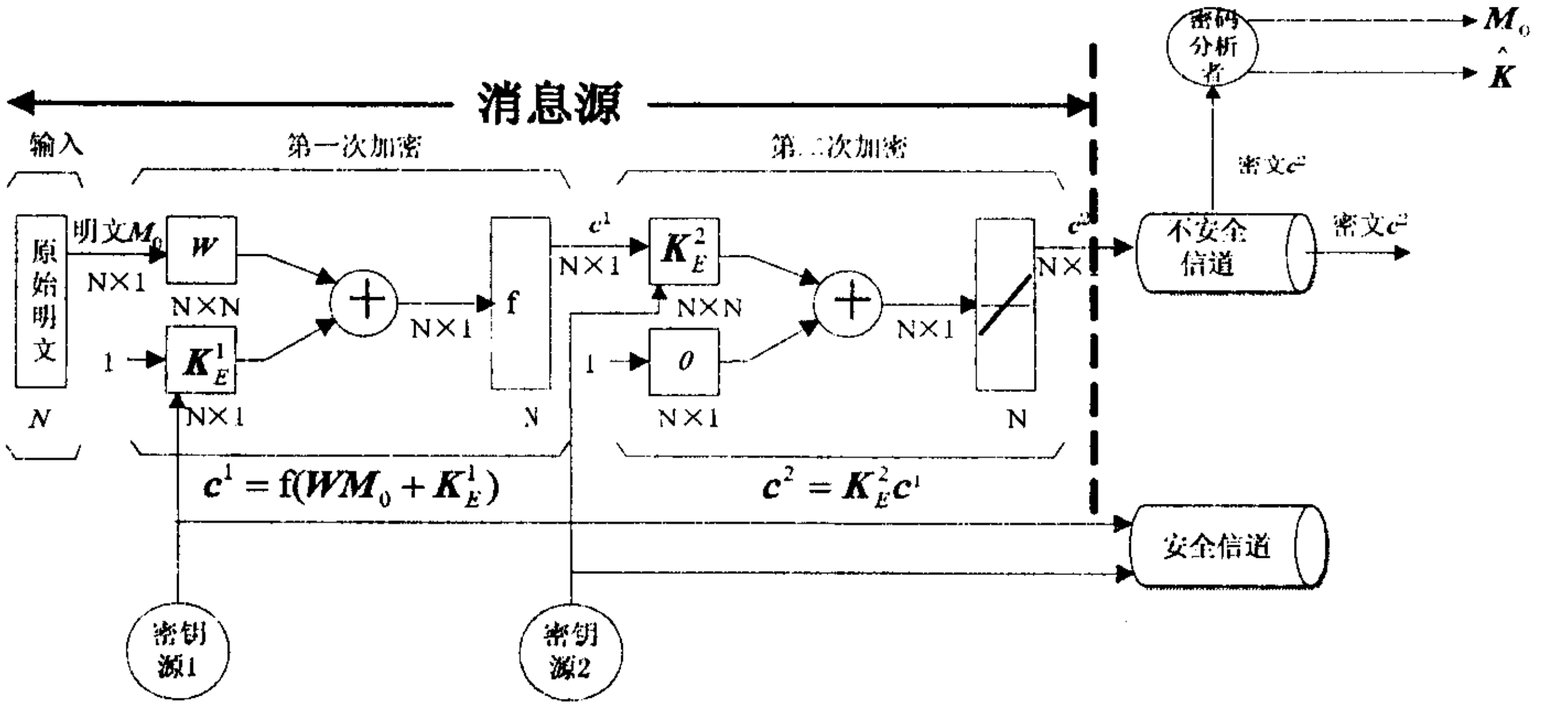

图 2 基于两层前馈网络的分组密码的具体实现——加密部分

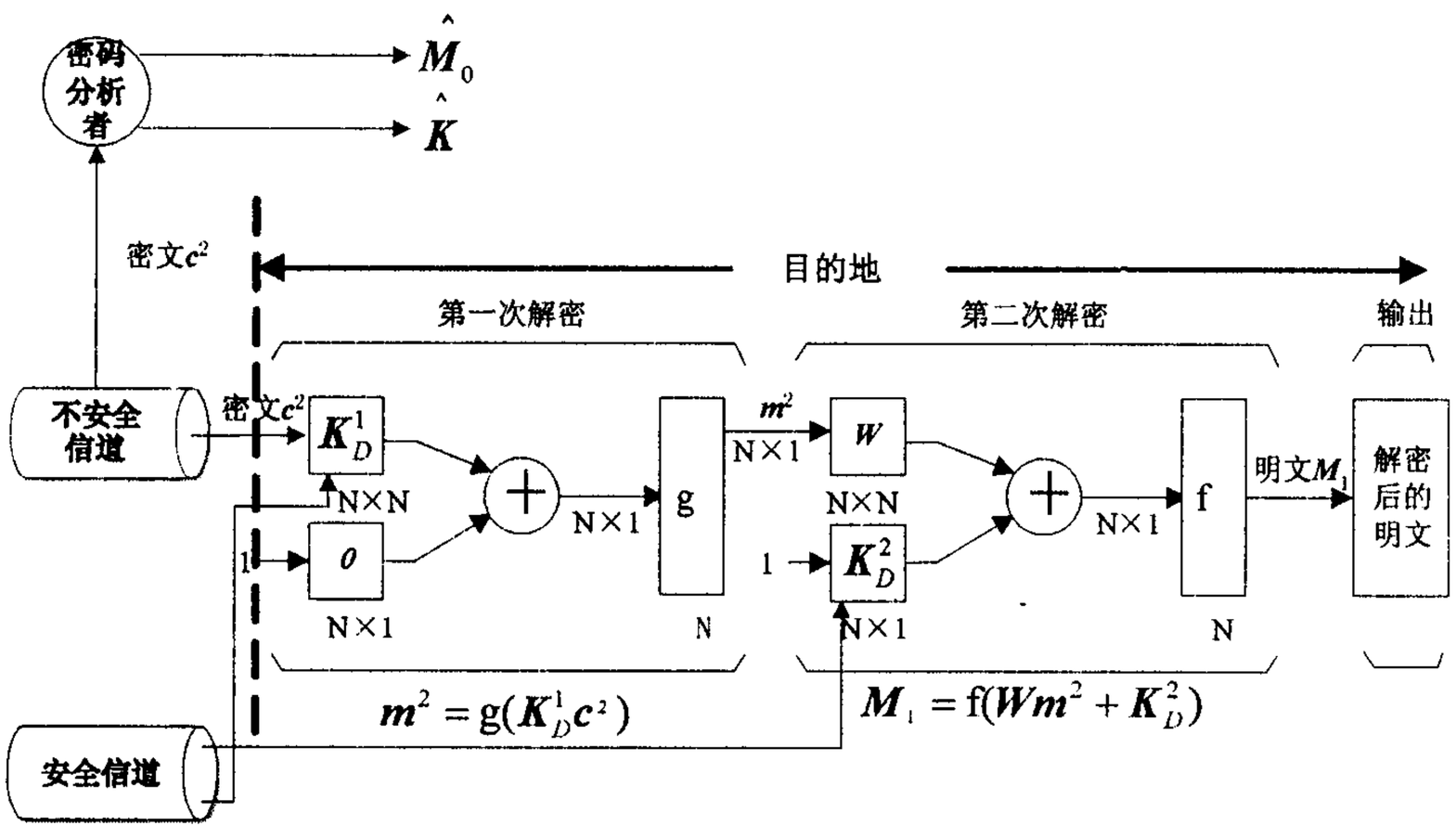

图 3 基于两层前馈网络的分组密码的具体实现——解密部分

3 用于分组密码体制的两层前馈网络的仿真

3.1 加/解密过程的仿真(实验一)

为验证该分组密码体制的性能，笔者参与进行了大量

的实验,下面以其中的一个实验为例,说明该分组密码体制的具体工作流程。在该实验中,假设 $M = 4, N = 16$ (即每个明文分组由 16 个小块组成),各小块内容的具体值如表 1 所示。

在仿真过程中得到的最终密文 $\boldsymbol{C}$ 和解密后的明文 $\boldsymbol{M}_1$ 分别如下:

表 1　原始明文分组中各小块的具体值

小块的序号	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
各小块的值	10	1	11	3	0	14	9	13	12	8	3	10	6	5	15	1

$\boldsymbol{C}' = \{12775, 8424, 12185, 11756, 13508, 10888, 13231, 12291, 13491, 14325, 14897, 15416, 13245, 13394, 16257, 15627\}$

$\boldsymbol{M}'_1 = \{10,1,11,3,0,14,9,13,12,8,3,10,6,5,15,1\}$

通过将 $\boldsymbol{M}_1$ 和原始明文 $\boldsymbol{M}_0$ 进行比较,结果表明该分组密码体制能够正常工作。

3.2　安全性分析过程的仿真

1.3.2 节曾对该分组密码的安全性进行了理论上的分析,文中进行了大量的实验来观察这种分组密码的扩散效果,结果表明该分组密码体制确实具有很好的扩散特征。下面以其中的 4 个实验为例进行说明,参数设置与实验一相同。

(1) 实验二。

通过实验二来验证明文 $\boldsymbol{M}_0$ 对密文 $\boldsymbol{C}$ 的扩散影响程度。

改变作为加密网络输入向量的 N 个小块中的一个小块,而加密密钥 $\boldsymbol{K}_E^1$ 和 $\boldsymbol{K}_E^2$ 均不变,来观察生成的密文分组 $\boldsymbol{C}$。可以发现 N 个小块都发生了变化。

(2) 实验三。

通过实验三来验证密文 $\boldsymbol{C}$ 对明文 $\boldsymbol{M}_1$ 的扩散影响程度。

改变作为解密网络输入向量的 N 个小块中的一个小块,而解密密钥 $\boldsymbol{K}_D^1$ 和 $\boldsymbol{K}_D^2$ 均不变,来观察解密后生成的明文分组 $\boldsymbol{M}_1$。可以发现 N 个小块都发生了变化。

(3) 实验四。

通过实验四来验证加密密钥 $\boldsymbol{K}_E^1$ 对密文 $\boldsymbol{C}$ 的扩散影响程度。

改变作为加密密钥 $\boldsymbol{K}_E^1$ 的 N 个阈值中的一个阈值,而明文 $\boldsymbol{M}_0$ 和加密密钥 $\boldsymbol{K}_E^2$ 均不变,来观察加密后生成的密文分组 $\boldsymbol{C}$。可以发现 N 个小块都发生了变化。

(4) 实验五。

通过实验五来验证加密密钥 $\boldsymbol{K}_E^2$ 对密文 $\boldsymbol{C}$ 的扩散影响程度。

改变作为加密密钥 $\boldsymbol{K}_E^2$ 的 N 阶连接权值矩阵中的一个元素,而明文 $\boldsymbol{M}_0$ 和加密密钥 $\boldsymbol{K}_E^1$ 均不变,来观察加密后生成的密文分组 $\boldsymbol{C}$。可以发现只有 1 个小块发生了变化。

综上所述,从总体上说,这种分组密码体制的扩散特征比较明显。

4　结　论

分组密码体制作为密码技术研究的热点,广泛用在数据的加密存储和保密传输上。文中建立了一种基于前馈网络的密码体制。理论分析和实验结果说明了该分组密码体制有很好的混乱特性和扩散特性,并且具有较高的安全性,可以用于信息安全领域的加/解密过程。

参考文献:

[1] 冯登国. 国内外密码学研究现状及发展趋势[J]. 通信学报, 2002,23(5):18－26.

[2] Lauria F E. On Neurocryptology[C]// Proceedings of the Third Italian Workshop on Parallel Architectures and Neural Networks. [s.l.]:[s.n.],1990:337－343.

[3] Lauria F E. Non－linguistic Neurocryptology and the Shannon theorem[C]// Marinaro M, Scarpetta G. Structures: from Physics to General Systems. Singapore: World Sc,1992:238－244.

[4] 杜生辉,阮传概. 用感知器构造分组密码[J]. 密码与信息, 1994(1):24－31.

[5] 章照止,杨义先,马晓敏. 信息理论密码学的新进展及研究问题[J]. 电子学报,1998(7): 9－18.

[6] 齐　锐,张大力,阎平凡. 基于神经网络的对称密码系统[J]. 清华大学学报:自然科学版, 2001,41(9):89－93.

[7] Shannon C E. Communication Theory of Secrecy Systems[J]. Bell System Technical Journal, 1949,28(4):656－715.

(上接第 157 页)

弱,在自动推理方面存在不足。从本体的初衷来说,构造本体的目的都是为了实现某种程度的知识共享和重用,所以将 UML 应用于本体的开发还是有现实意义和理论价值的。今后的研究工作将集中在本体模型的逻辑基础和自动推理方面,从而形成完善的本体建模方法。

参考文献:

[1] Berners－Lee T, Hendler J, O Lassila. The Semantic Web[J]. Scientific American, 2001, 284(5):34－43.

[2] Gruber T R. Towards principles for the design of ontologies used for knowledge sharing[J]. International Journal of Human－Computer Studies, 1995, 43(5):907－928.

[3] Booch G, Rumbaugh J, Jacobson I. UML 用户指南[M]. 邵维忠译. 北京:机械工业出版社,2001:5－18.

[4] W3C. OWL Web Ontology Language Guide W3C Candidate Recommendation[EB/OL]. 2003－08. http://www.w3.org/TR/owl－guide/.

[5] Horrocks I. Reasoning with Expressive Description Logics: Theory and Practice[M]. Manchester, UK: University of Manchester, 2002:41－72.