

基于哈希的二维工程 CAD 图拓扑关系认证技术

马晓斌, 叶颖, 苏智勇

(南京理工大学自动化学院, 江苏 南京 210094)

摘 要: 针对二维工程 CAD 图拓扑关系完整性认证问题, 提出一种基于哈希的拓扑完整性认证算法。该算法首先提取图纸的拓扑关系生成拓扑图; 其次对图中的组件进行编码, 并提出一种局部拓扑量化模式(LTQP), 实现各组件拓扑特征的量化; 然后将组件按照其编码分成 5 类, 基于各组件的 LTQP 值, 利用离散余弦变换生成每类组件的哈希序列; 最后将每类组件的哈希序列进行合并, 得到完整的图纸哈希序列。实验结果表明, 该算法对旋转、缩放和平移等非恶意操作具有鲁棒性, 同时对恶意拓扑攻击具有脆弱性, 采用将组件分类来生成哈希序列的方式, 能够对受到拓扑攻击的组件的种类进行定位。

关 键 词: 工程 CAD 图; 拓扑认证; 局部拓扑量化模式; 离散余弦变换; 哈希
中图分类号: TP 391 **DOI:** 10.11996/JG.j.2095-302X.2017040476
文献标识码: A **文 章 编 号:** 2095-302X(2017)04-0476-07

Topology Authentication of 2D Engineering CAD Drawings Based on Hashing

MA Xiaobin, YE Ying, SU Zhiyong

(School of Automation, Nanjing University of Science and Technology, Nanjing Jiangsu 210094, China)

Abstract: Since it's difficult to authenticate the topological relation in the 2-dimensional engineering CAD drawing, a topological integrity authentication algorithm is proposed based on Hashing in this paper. Firstly, the algorithm extracts the topological relations of the drawings to generate the topology graph. Secondly, the components in the engineering CAD drawing are encoded, and the local topological quantization pattern (LTQP) is proposed to quantize the topological features of each component. Then, the components are divided into five categories according to their coding, and a Hash sequence is generated by discrete cosine transform based on the LTQP values. Finally, the Hash sequence of each category is combined to obtain the complete Hash sequence of the drawing. The experimental results show that the algorithm is robust to rotation, scaling and translation in engineering CAD drawings, and is vulnerable to the change of topological connection. By classifying the components to generate a Hash sequence, the algorithm can locate the type of components which is subjected to the topology attack.

Keywords: engineering CAD drawing; topology authentication; local topological quantization pattern; discrete cosine transform; Hashing

随着信息技术的发展, 工程计算机辅助设计 (computer aided design, CAD) 在建筑、工程建设、

石油化工等领域中获得了广泛地应用。随着工作效率的不断提升, 并行工程与协同工作成为工程

收稿日期: 2016-11-18; 定稿日期: 2016-12-21

基金项目: 国家自然科学基金项目(61300160)

第一作者: 马晓斌(1992-), 男, 江苏南通人, 硕士研究生。主要研究方向为计算机图形学。E-mail: 805070158@qq.com

通信作者: 苏智勇(1981-), 男, 江苏泰州人, 副教授, 博士。主要研究方向为计算机图形学、计算机视觉、图像与视频处理。E-mail: suzhiyong@njust.edu.cn

CAD 行业的发展方向。由此导致了不同人员和不同地点数据共享问题的出现,所以,工程 CAD 图在设计和传输的过程容易被有意或无意地修改。目前对于工程 CAD 图,亟需解决的问题是如何切实有效地认证图纸内容的完整性。

根据设计对象的不同,CAD 设计可以分成两大类^[1]:一类是产品 CAD,如机械 CAD 等;另一类是工程 CAD,如工厂 CAD 等,国外简称 AEC (architecture engineering construction)。这两种 CAD 技术领域的研究侧重点有所不同,主要差异体现在^[1]:产品 CAD 的设计重点在于精确表达出设计结果的几何形状和尺寸,注重细节的描述;工程 CAD 的设计重点在于本专业知识的描述和表达,以及专业元素之间目的连接关系,几何外形已经不是设计的重点。工程 CAD 中几何形体相对简单,模型数据主要是构件本身的工程信息和构件之间的拓扑关系描述。工程 CAD 建模则涉及大量工程约束,主要表现为组件之间的拓扑关系,拓扑关系在工程 CAD 中是至关重要和最为复杂的,也是 CAD 模型的核心所在。因此,如何对工程 CAD 图的拓扑完整性进行认证就显得至关重要。

目前,CAD 图的完整性验证技术主要分为数字水印技术与哈希技术两大类。数字水印^[2]是在 CAD 模型数据中嵌入信息,当 CAD 数据发生改变时,这些水印信息也会相应地发生一定程度的改变,从而能够将 CAD 数据的失真情况探测出来,鉴定出原始数据是否被篡改。哈希技术^[3]是在提取对象的不变特征后,通过某种映射关系将数据信息量大的对象映射为长度较小的比特序列,最后比较比特序列之间的距离校验 CAD 图的内容完整性。

基于数字水印的完整性认证技术主要应用于机械产品 CAD 图中几何信息的认证。1997 年 OHBUCHI 等^[4]首次提出三维模型水印技术,这标志着 CAD 数字水印技术的开端。起初发表的算法均是针对 CAD 图形的空域水印算法,主要包括 OHBUCHI 等^[4]提出的基于模型属性修改的水印算法以及 ICHIKAWA 等^[5]提出利用多边形网格中的表示冗余嵌入水印的若干算法。在工程图的数字水印技术方面,陈永府等^[6]提出一种非盲检测算法,通过采用微小扰动法,在工程图的编码冗余信息中嵌入水印,以抵御图元的增删等操作。彭飞等^[7]提出一种采用改进量化索引调制的二维 CAD 工程图小波域可逆水印算法,其对图形平移、

旋转、均匀缩放等攻击具有鲁棒性,但不能够抵抗实体增删的攻击。目前对于工程 CAD 图拓扑关系完整性认证的研究不多,SU 等^[8]基于半脆弱盲水印技术解决了管道等轴测图纸的拓扑完整性问题,对局部相似变换和缩放操作具有鲁棒性。

基于哈希的完整性认证主要针对机械产品 CAD 的几何信息。文献[9]用三维模型的鲁棒哈希算法将三维模型分割为子网格,并对其进行拉普拉斯-贝尔矩阵分解,并由此获得子网格的哈希值,该算法对高斯噪声、缩放、旋转等常见攻击具有鲁棒性。文献[10]基于三维模型的高比表面积作为特征,参考表面进行归一化处理,并通过二值化生成二进制的哈希值,该算法优点在于对拓扑的攻击具有鲁棒性。在机械产品 CAD 领域,文献[11]提出一种矢量数据哈希算法,其基于随机矩阵和高斯混合模型,利用 CAD 图中折线曲率作为哈希的特征值,算法具有唯一性、安全性和鲁棒性。

综上所述,目前对于 CAD 图完整性验证的研究主要针对机械产品 CAD 图的几何信息展开,而对于工程 CAD 拓扑关系完整性验证的工作比较匮乏。并且,基于数字水印技术的完整性验证技术,需要在模型中嵌入水印,这会对数据的原始信息造成或多或少的影响;哈希技术相对于数字水印技术,不用修改原始的模型数据,而是用哈希值表达工程 CAD 模型的内容特征。在工程 CAD 中引入哈希进行拓扑关系的完整性认证需要考虑哈希算法的选择、不变特征的提取等问题。其中最为困难的是如何提取工程 CAD 图的拓扑特征,因为得到的拓扑特征还需要同时满足鲁棒性、脆弱性和安全性的要求。

针对工程 CAD 图拓扑关系完整性认证问题,本文提出一种基于哈希的完整性认证技术。通过以工程 CAD 图中部件之间的拓扑连接关系为特征,采用 LTQP 算子量化拓扑特征,将组件进行分类,提取 LTQP 算子进行离散余弦变换(discrete cosine transform, DCT)生成工程 CAD 图的哈希序列,按照分类比实现对哈希序列最终拓扑关系的完整性认证。

1 基于局部二值模式的拓扑特征提取

工程 CAD 图的拓扑特征提取是生成哈希算法的核心所在。特征向量需要对改变工程 CAD 图的拓扑关系的恶意攻击具有较强的敏感性,同时在

常规的不影响拓扑关系的情况下,对组件几何信息进行编辑(旋转、平移等)操作具有一定的鲁棒性。

1.1 拓扑图构建

为了提取工程 CAD 图的拓扑特征,首先需要将图纸组件进行量化。工程 CAD 图中各组件具有标准的图形,这些图形均符合相关的国家和行业标准,因此,可以根据图形库和各行业的专业知识来预先对组件进行分类,并对组件进行统一编码以解决图形表达的异构性。本文以流程工厂 CAD 为例,将图纸中的组件编码位数定为 3 位,其中首位是图纸模型的基本元素,包括设备、管元件和建筑构件等基本构件,第 2、3 位为每一大类细分后的子项。例如,节流阀属于基本元素中元件的阀门类,元件编号为 1,阀门类的编号为 1,节流阀在阀门类的下属编码为 8,所以节流阀的编号为 118。

拓扑图用来描述组件间的连接关系,通过提取组件间的拓扑关系能够得到工程 CAD 图的拓扑图(图 1),其中图 1(b)结点中的数字代表组件的编码值,边代表组件之间拓扑相连。

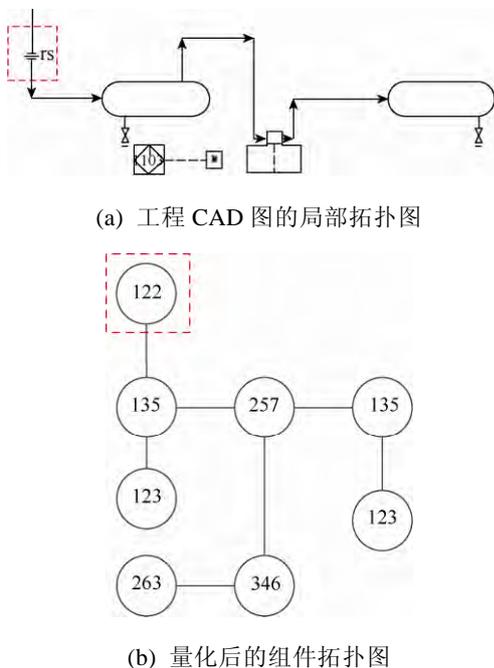


图 1 工程 CAD 图的局部及其量化后的拓扑图

1.2 基本 LBP 算子

LBP 算子是一种用来描述图像局部纹理特征的算子。其首先由 OJALA 和 HARWOOD^[12]提出,LBP 算子具有旋转不变性和灰度不变性等显著的

优点,可提取图像局部的纹理特征,因此常用于纹理分类、人脸识别等领域。

基本 LBP 算子^[13]是对图像中的每一个像素的 3×3 窗口进行操作,以该窗口的中心像素的灰度值为阈值,将中心像素与 8 邻域内的像素灰度值进行比较,其值大于中心像素则记为 1,否则为 0,如式(1)所示

$$s(x) = \begin{cases} 1, & x > 0 \\ 0, & x \leq 0 \end{cases} \quad (1)$$

由此得到一个 8 位二进制数,并将其转换成十进制数就可以得到该窗口的 LBP 值。基本 LBP 算子定义为

$$LBP(x_c, y_c) = \sum_{i=0}^7 s(g_i - g_c) \cdot 2^i \quad (2)$$

其中, g_c 为局部区域的中心像素的灰度值; g_i 为中心像素领域的第 i 个采样点的灰度值。

一个基本的 LBP 算子的计算原理如图 2 所示。图 2 是一个中心像素灰度值为 63 的 3×3 的窗口,中心像素与其 8 邻域像素灰度值作差的结果为 $(-19, 15, 29, 27, 19, 11, -2, -31)$,根据式(1)得到系数向量为 $(0, 1, 1, 1, 1, 1, 0, 0)$,处理得到一个 8 位的二进制数“01111100”,最后将这个二进制数转换成十进制数结果为 124,即中心点处像素的 LBP 值为 124。

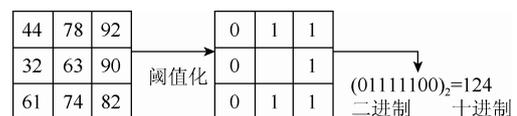


图 2 基本 LBP 算子示意图

1.3 LTQP 算子

基于 LBP 算子,本文提出了一种基于拓扑特征的 LTQP 算子。LTQP 算子是以工程 CAD 图中的组件编码值为阈值,并将其与有拓扑连接的组件编码值相比较而生成的。LTQP 算子定义为

$$LTQP(x) = \sum_{i=0}^n s(t_i - t_c) \cdot |t_i - t_c| \quad (3)$$

$$s(x) = \begin{cases} 1, & x \leq 0 \\ 2, & x > 0 \end{cases} \quad (4)$$

其中, t_c 为中心组件的编码值; t_i 是与 t_c 有拓扑连接的组件编码值; n 是与 t_c 拓扑连接的组件数。如果拓扑连接的组件编码值大于中心组件编码值,则记为 2,否则记为 1。求中心组件编码值与其拓扑连接的组件编码值差的绝对值,并将其绝对值

与阈值化后的值(1 或 2)相乘, 最后相加得到中心组件的 LTQP 值。

LTQP 算子的计算原理如图 3 所示。图 3 是一个中心组件编码值为 140 的拓扑图, 中心组件编码值与各拓扑连接组件的编码值的差的结果为 (8,-12,-15,136), 根据式 (4) 得到系数向量为 (2,1,1,2), 最后根据式(3)进行求和得到编码 140 的组件的 LTQP 算子值为 307。LTQP 算子采用 2 值编码的求和方式, 尽可能地保留了中心组件和拓扑连接组件之间的编码关系, 当组件发生改变时, LTQP 值也能够随之变化。

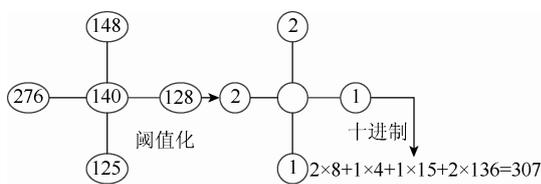


图 3 改进 LBP 算子示意图

2 哈希值的生成与校验

2.1 基于离散余弦变换的哈希值生成

本文算法通过对提取的各组件 LTQP 值按照组件编码进行分类, 并建立每类组件的 LTQP 值矩阵; 然后对每一类的矩阵进行 DCT 变换; 最后对变换后的系数进行处理, 生成每类矩阵的哈希序列。具体步骤如下:

(1) 计算工程 CAD 图中每个组件的 LTQP 算子值。

(2) 将工程 CAD 图中的组件按照其组件编码的首位数字分成 5 类(1-2,3-4,5-6,7-8,9)。

(3) 将每类中组件的 LTQP 值按其编码值的大小依次放入 $n \times n$ 的矩阵块中, n 通过式(5)来确定

$$(n-2)^2 < N \leq n^2, \quad n = 2k, \quad k = 1, 2, \dots \quad (5)$$

其中, N 为该类组件的总数; n^2 为最接近 N 的偶数平方值。该 $n \times n$ 的矩阵如式(6)

$$f(i, j) = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \quad (6)$$

其中, a_{ij} 为组件的 LTQP 算子值, 根据其组件编码值的大小按照行优先的方式依次排放入 $n \times n$ 的矩阵中, 若出现组件编码值相同时, 则根据拓扑连接的组件编码值的大小进行排列。当组件数不足 n^2 时, 用 0 补齐。

(4) 利用 DCT 变换将处理后的拓扑关系 LTQP 值从空间域变换到频率域。DCT 变换式^[14]为

$$F(u, v) = \begin{cases} \frac{2}{n} \left[\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f(i, j) \cos \frac{(2i+1)u\pi}{2n} \cos \frac{(2j+1)v\pi}{2n} \right] \\ \frac{1}{n} \left[\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f(i, j) \right], \quad u = v = 0 \end{cases} \quad (7)$$

其中, u 和 v 表示 DCT 变换后矩阵的位置; $F(u, v)$ 表示拓扑关系块的频率系数值; $f(i, j)$ 表示每个组件的 LTQP 算子值。当 u 和 v 不同时为 0, 表示变换域的高频部分, 也称为交流系数。当 $u=0$ 且 $v=0$ 时, $F(0,0)$ 表示变换域中的低频成分, 也称为直流系数, 其物理意义是 $n \times n$ 拓扑关系块中所有元素均值的 n 倍。

(5) 对 5 类矩阵块进行 DCT 变换后的频率系数进行处理。若矩阵块中 $n < 4$, 则将 $F(u, v)$ 用 0 补齐成 4×4 的矩阵块, 若 $n \geq 4$, 取 $F(u, v)$ 左上角 4×4 的小块。将这 5 个 4×4 小块中的频域系数分别按照行优先的方式组成长度为 16 的一维向量 A_i , $i=1, 2, \dots, 5$ 。

(6) 利用 Logistic 方程作为混沌序列发生器进行加密, Logistic 方程^[15]如式(8)

$$x_{n+1} = \mu x_n (1 - x_n), \quad 3.5699 < \mu < 4, \quad 0 < x_n < 1 \quad (8)$$

利用该公式计算得到长度为 16 的一维向量 M , 将 M 中的对应位置的值与向量 A_i 中对应位置的值相乘, 得到 5 个加密后的向量 A'_i , 向量中的数据类型为浮点数。

(7) 对于向量 A'_i 中的每个分量, 本文算法对浮点数进行处理, 根据国际标准 IEEE 754 将浮点数用 32 位二进制数表示。设置 32 位的二进制密钥 K , 其中 16 位为 1, 另 16 位为 0, 1 代表有效位, 0 代表无效位。将向量 A'_i 中的二进制数用 32 位密钥 K 加密, 保留下密钥 K 中 1 对应的位置的数组成一个新的 16 位的二进制数。转换后每个矩阵块共有 $16 \times 16 = 256$ 位二进制哈希码, 将这些哈希码按照组件种类分类的顺序依次相连, 最后得到共 $256 \times 5 = 1280$ 位二进制数的哈希序列。

2.2 哈希值的校验

在拓扑校验阶段, 获得待检测图纸后对组件按相同规则编码并计算 LTQP 算子, 然后将组件分类, 对每类组件的 LTQP 算子进行 DCT 变换后得到待检测工程 CAD 图的哈希序列。将得到的 1280 位哈希序列按照每 256 位分隔, 得到 5 段哈希序

列, 每段序列对应 1 类组件。通过分别比对原始工程 CAD 图与待检测图纸的 5 个哈希序列, 计算哈希码间的汉明距离 dis_i

$$dis_i = \sum_{m=0}^{16 \times 16} |h_m - h'_m|, i = 1, 2, \dots, 5 \quad (9)$$

其中, h_m 和 h'_m 分别表示两张工程 CAD 图中对应类别组件的哈希码。设定阈值 T , 当 $dis_i > T$ 时, 则认为工程 CAD 图中第 i 类组件中的拓扑连接发生篡改。

3 实验与分析

以流程工厂 CAD 为例, 选择 3 类 PID 图进行实验。第 1~3 类图纸中组件数分别在 50、100、200 件左右。每类工程 CAD 图包含 20 张图纸, 对这些图纸进行几类常见的局部的缩放、旋转的非恶意操作以及增加、删除和替换等恶意拓扑攻击操作来检验算法的性能。本文算法中 Logistic 方程的初始值 $x_0=0.6$, $\mu=3.9625$, 密钥 K 取 32 位数中的奇数位置为 1。分别从算法的唯一性、安全性、鲁棒性和脆弱性来验证实验结果。

3.1 唯一性

具有相似拓扑关系的两张工程 CAD 图, 会生成不同的二值哈希序列。如果哈希序列之间的距离大于一定的阈值, 就认为这两张工程 CAD 图的拓扑连接关系不同。本文算法对 60 张工程 CAD 图纸进行实验, 得到 60 组哈希序列, 并对其进行匹配。利用组合式(10)得到 1 770 个结果, 匹配直方图如图 4 所示。

$$C_m^n = \frac{m!}{n!(m-n)!} m = 60, n = 2 \quad (10)$$

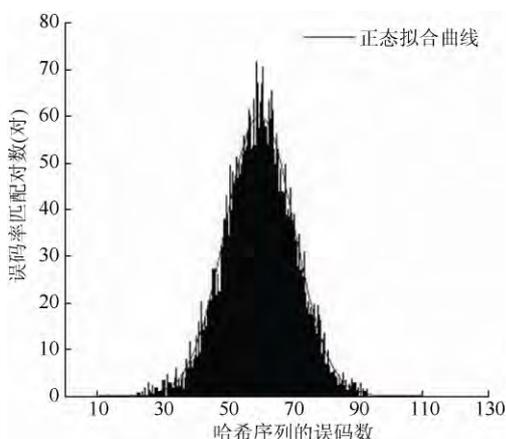


图 4 哈希序列匹配直方图

从图 4 可以看出, 该结果基本服从高斯分布, 高斯分布的方程^[16]为

$$P = \int_{-\infty}^T \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}} dx \quad (11)$$

经过拟合得到 $\mu = 70.3$, $\sigma = 10.6$ 。根据直方图, 取临界阈值 T 为 20, 根据式(11)计算拓扑关系的哈希序列的冲突率为 1.289×10^{-5} 。在 10^{-5} 的数量级, 表明 10 万张工程 CAD 图可能出现相同的哈希序列。因此, 当工程 CAD 图中某一类哈希序列的汉明距离大于 20 时, 认为该类的拓扑关系发生篡改, 可以保证拓扑关系特征的唯一性。

3.2 安全性

安全性是哈希算法的一个重要特性, 本文算法的安全性取决于密钥 K 以及混沌序列的应用。本文从两方面对算法的安全性进行了实验验证:

(1) 修改密钥 K 中有效位 1 的位置后, 将生成的哈希序列与原图纸的哈希序列比较, 哈希距离大于设定的阈值 20;

(2) 取 Logistic 方程的 μ 为 3.962 5 和 3.963 0, 分别对选取的 20 张工程 CAD 图纸进行哈希匹配, 计算得到的汉明距离均大于阈值 20。

因此, 在不能同时知道密钥 K 与 μ 的取值情况下无法得到正确的哈希序列, 所以本文提出的算法能够满足工程 CAD 图拓扑关系哈希算法的安全性要求。

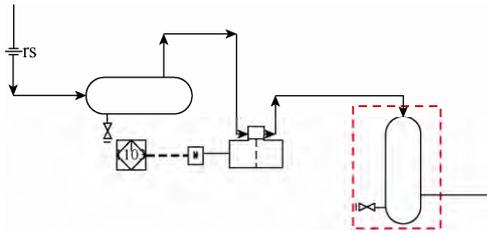
3.3 鲁棒性

本文算法通过提取工程 CAD 图的拓扑图后进行后续处理。在受到非恶意的几何操作之后, 其拓扑连接关系不会被破坏, 提取的拓扑图也将保持不变, 根据图纸中的拓扑图生成的 LTQP 算子也不会发生变化。在此基础上进行离散余弦变化后生成的哈希序列不会改变。因此算法对旋转、平移和缩放等保拓扑不变的几何操作具有鲁棒性。

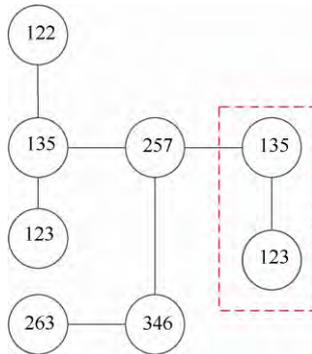
图 5 是对图 1(a)中的组件进行旋转、平移操作后对拓扑图结果影响的实例。

图 5 中的组件发生了几何位置的变化, 但其拓扑图未发生改变, 因此每个组件的 LQTP 算子值保持不变, 由其推导生成的哈希值结果也不会发生变化。

本文对 20 张实验图纸进行保拓扑关系不变的旋转、平移和缩放操作。测试结果显示本文算法误判率为 0, 由此证明本文算法对工程 CAD 图的保拓扑的几何操作具有鲁棒性。



(a) 将矩形框内的组件进行旋转后的 CAD 图



(b) 修改前后的拓扑连接图

图 5 对虚线框内组件进行旋转平移操作后的 CAD 图及生成的拓扑连接图

3.4 脆弱性

本文算法对组件常见的增加、删除和替换等拓扑恶意攻击具有脆弱性。

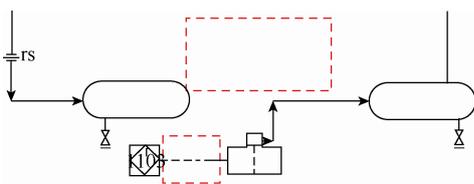
3.4.1 组件删除及组件间拓扑连接的删除

这种攻击是通过删除工程 CAD 图纸内的组件或组件之间的拓扑关系来实现的。当组件或其拓扑连接发生删除时, 相应组件的拓扑关系就将发生改变, 所生成的 LTQP 算子值也随之变化, 由此引起矩阵块的变化, 最终影响到 DCT 变换后生成的哈希值。通过计算哈希值之间的距离就可以判定图纸的拓扑关系发生了改变。图 6 为对图 1(a) 进行删除攻击后 LTQP 算子的影响实例。

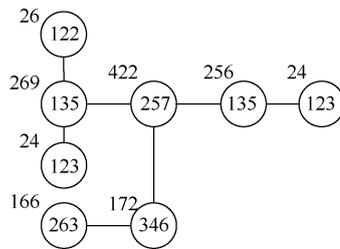
图 6 中组件编码左上角为该组件的 LTQP 算子值。以编号为 257 的组件为例, 当删除与其拓扑相连的组件 346 时, 其 LTQP 算子值从 422 改变为 134, 根据算子值生成的拓扑矩阵块也会发生改变, 哈希序列也随之发生改变。因此本文算法对删除操作具有脆弱性。

3.4.2 组件增加及组件间拓扑连接的增加

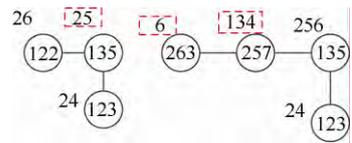
这种攻击是通过增加工程 CAD 图纸内的组件或组件之间的拓扑关系完成的。当增加组件或其拓扑连接时, 拓扑关系发生改变, 导致 LTQP 算子值变化, 最终影响到 DCT 变换后生成的哈希值。通过计算哈希序列之间的距离就可以判定图纸的拓扑关系发生了篡改。图 7 为对图 1(a) 进行增加攻击后 LTQP 算子的影响实例。



(a) 删除矩形框内的组件或拓扑连接后的 CAD 图

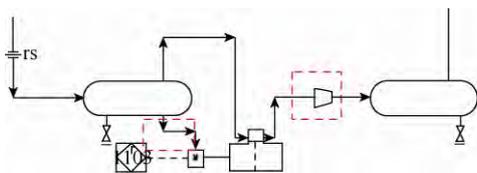


(b) 原工程 CAD 图的拓扑连接图

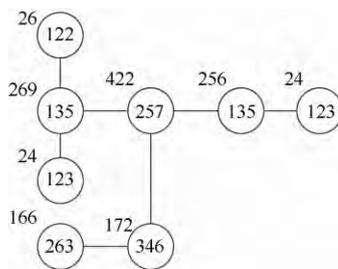


(c) 删除操作后得到的拓扑图

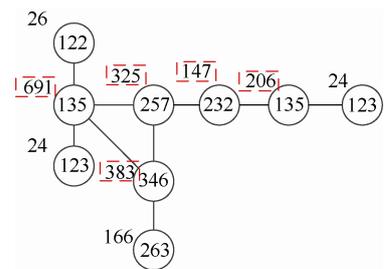
图 6 删除操作后的 CAD 图及删除前后的拓扑图



(a) 增加矩形框内的组件或拓扑连接后的 CAD 图



(b) 原工程 CAD 图的拓扑连接图



(c) 增加组件或拓扑关系得到的拓扑图

图 7 增加操作后的 CAD 图及增加前后的拓扑图

图 7 组件编码左上角为该组件的 LTQP 算子值。以编号为 257 的组件为例,当增加与其拓扑相连的组件 232 时,其 LTQP 算子值从 422 改变为 325,根据算子值生成的拓扑矩阵块也发生了改变,哈希序列也随之发生改变。因此本文算法对增加操作具有脆弱性。

3.4.3 组件替换

组件的替换可以看作是将原连接组件删除,然后加入并连接新的组件。因此,替换操作可认为是增加和删除攻击的组合。虽然该类攻击不会对提取的拓扑图的结构发生改变,但是拓扑连接的组件编码发生了变化,因此也会导致 LTQP 算子发生改变,从而引起哈希序列发生改变。

为了测试算法对于拓扑攻击的脆弱性,对工程 CAD 图纸进行 3 种攻击实验,其中第 1 组为组件删除;第 2 组为组件的增加;第 3 组用新的组件去替换原图纸的组件。利用本文算法对图纸进行拓扑连接的完整性认证,并测试算法的攻击定位能力,结果见表 1,其中 A 类图纸组件数为 50, B 类 100, C 类 200。

表 1 拓扑攻击实验结果(%)

常见攻击	A 类图纸	B 类图纸	C 类图纸
删除组件	96.1	97.3	97.5
增加组件	96.9	97.8	97.4
替换组件	96.4	96.2	96.6

从表 1 可知,本文算法对组件的增删和替换等改变拓扑攻击的检测定位的成功率均在 96% 以上,证明算法能够满足工程 CAD 图拓扑连接的完整性认证的要求。分析漏检的原因有 3 个:

(1) LTQP 算子采用绝对值求和的计算方式,这会导致发生拓扑攻击后不同组件的 LTQP 算子的结果会出现相同的情况;

(2) 每类矩阵块 DCT 变换后进行归一化时舍弃了一些数据,这将导致计算误差;

(3) 将浮点数转换为二进制数时只保留了 16 位,可能会出现浮点数变化,但是所取相应位置的二进制没有改变从而导致漏检。

4 结 论

本文提出了基于 LBP 算子的特征提取的哈希算法来解决工程 CAD 图中拓扑关系的完整性认证问题。通过实验表明,该算法简单,提取的 LTQP 特征对常规的保拓扑的几何操作具有鲁棒性,对

影响拓扑关系的增加、删除和替换操作具有脆弱性,能够区分一般操作与恶意攻击;同时本文的算法还具有唯一性和安全性。提出了组件分类编码的思想,当组件中的拓扑关系发生改变时,可以通过对相应种类组件的哈希序列的比对,从而缩小校验的范围以实现拓扑攻击的定位。下一步工作是研究在受到恶意拓扑攻击后能够精确定位到拓扑关系发生改变的组件哈希算法。

参 考 文 献

- [1] 唐荣锡. CAD/CAM 技术[M]. 北京: 北京航空航天大学出版社, 1994: 2-8.
- [2] 潘志庚, 孙树森, 李黎. 三维模型数字水印综述[J]. 计算机辅助设计与图形学学报, 2006, 18(8): 1103-1110.
- [3] 郭亚宁. 基于哈希编码的文本拷贝检测算法优化与实现[D]. 济南: 山东大学, 2014.
- [4] OHBUCHI R, MASUDA H, AONO M. Water making three-dimensional polygonal models [C]//Proceedings of the Fifth ACM International Conference on Multimedia. New York: ACM Press, 1997: 261-272.
- [5] ICHIKAWA S, CHIYAMA H, AKABANE K. Redundancy in 3D polygon models and its application to digital signature [J]. Journal of WSCG, 2002, 10(1): 225-232.
- [6] 陈永府, 赵建军, 陈立平, 等. 工程图数字水印技术研究[J]. 图学学报, 2010, 31(6): 191-197.
- [7] 彭飞, 雷瑜洲, 孙星明. 2 维 CAD 工程图小波域可逆水印[J]. 中国图象图形学报, 2011, 16(7): 1134-1139.
- [8] SU Z, YANG X, LI U G, et al. Topology authentication for piping isometric drawings [J]. Computer-Aided Design, 2015, 66: 33-44.
- [9] TARMISSI K, HAMZA A B. Information-theoretic hashing of 3D objects using spectral graph theory [J]. Expert Systems with Applications, 2009, 36(5): 9409-9414.
- [10] LEE S H, KWON K R. Robust 3D mesh model hashing based on feature object [J]. Digital Signal Processing, 2012, 22(5): 744-759.
- [11] LEE S H, HWANG W J, KWON K R. Polyline curvatures based robust vector data hashing [J]. Multimedia Tools & Applications, 2014, 73(3): 1913-1942.
- [12] OJALA T, HARWOOD I. A comparative study of texture measures with classification based on feature distributions [J]. Pattern Recognition, 1996, 29(1): 51-59.
- [13] 宋克臣, 颜云辉, 陈文辉, 等. 局部二值模式方法研究与展望[J]. 自动化学报, 2013, 39(6): 730-744.
- [14] 张斌. 基于感知哈希与数字水印图像内容认证技术研究[D]. 北京: 北京邮电大学, 2011.
- [15] 潘欣裕, 赵鹤鸣. Logistic 混沌系统的熵特性研究[J]. 物理学报, 2012, 61(20): 200504-1-200504-7.
- [16] 张敏. 基于图像内容认证的感知哈希算法的研究[D]. 长沙: 湖南大学, 2010.