以心电信号作为密码的安全硬盘

摘要：

如今，在数据普遍信息化的今天，大容量硬盘的出现与普及使得我们能够更加方便的携带与储存信息。但同时，信息的安全与否显得尤为重要。

如今，信息盗窃案的频发与盗窃方法的层出不穷使得使用者对于硬盘的安全性产生了一定的质疑，这也同时警示了我们：提高硬盘安全性刻不容缓。

医学研究证明，人类的心电图模式都是独一无二的。如果我们能用心电图作为密码，并且启用指模保护系统作为辅助密码，这样就可以更有效地杜绝密码被盗用，从而阻止信息泄露悲剧的发生。

因此，我们设计了一款用心电图作为主要密码，指模作为辅助密码的硬盘，其工作原理主要基于心电信号处理系统，指模识别技术，配以先进的蓝牙无线传输技术，实现与电脑等产品的信息传输功能。严格保护用户电子文档的安全。

关键字：

心电图识别，指模识别，密码，信息安全

Abstract: Today, data universal message of today, the emergence and spread of large-capacity hard disk allows us to be more convenient to carry and store information. But at the same time the security of information is particularly important.

Today, frequent of information theft stream of users for the security of the hard disk questioned, at the same time warning us: To improve the hard disk security imperative.

Medical studies have shown that the human ECG patterns are unique. If we can use the ECG as a password and finger print protection system is enabled as an auxiliary password, so that you can more effectively eliminate the password to unauthorized use, thus preventing information leak tragedy.

Therefore, we designed an ECG as a password, fingerprint hard disk as a secondary password, and its working principle is mainly based on the ECG signal processing systems, fingerprint recognition technology with the advanced Bluetooth wireless technology to achieve with computer product information transfer capabilities. protect users of electronic documents safely.

Keywords： ECG to identify fingerprints to identify the password information security

目录

第一章 引言

1.1 研究背景

在信息化时代，信息安全是具有时代建设性意义的课题。在所有信息资源中，文件和档案是基础性资源,它们的信息安全问题是信息化时代信息安全大课题中必须优先解决的重要问题。同时,文档电子化所带来的新的文档信息安全问题也引起了各界的普遍关注。

1.2 研究现状

据有关权威部门统计数据显示，随着各行业在生产、管理上信息化程度日益增高，计算机泄密行为也呈上升趋势。而计算机泄密最大的特点就是较之一般侵占案件，其手段更隐蔽、危害也更大。一个恶意的机密泄露事件往往会给企业造成难以估量的后果：轻则需要投入巨额资金进行补救，重则会将一个企业置之死地。权威数据显示，几乎所有的中国企业对电子文档都没有任何防护措施，企业对于信息有保护措施的不到 3%。一些机密性的资料，电子文档轻易就可以的通过电子邮件和移动硬盘泄密到网络外部。

日前，Search Security 网站针对 358 名企业信息化负责人进行了一项关于企业信息安全的调查。调查的结果显示，目前企业机密泄露 30%~40%是由电子文件的泄露造成的，而《财富》排名前一千家的公司，每次电子文档泄露造成的损失约为 400 万元美金。

1.3 创意来源

这些惨痛的事实将信息安全的重要性放在我们面前。如何才能彻底的保护信息的安全，从根源消灭信息泄露的可能性呢？我们就这一问题进行了深入研究，大胆构思，设计了一款安全硬盘。

第二章 整体结构

1.1 核心创意

不知不觉间，硬盘已走过了 53 个年头，随着科技的发展，人们的需求不断加大，我们对于硬盘的储存容量的认识，已经从最初的 B，到现在的 GB，甚至更高端的 TB。但是，随着时代的发展与科技的进步，高科技手段的不断研发，即使人们对于信息安全的重视程度越来越高，硬盘也不可避免地成为用户信息的泄密者，而近期的“硬盘泄密门”更让大家惶恐不安。如何能用一种独特的保密手法将硬盘里的信息完好保存，将泄密的可能性降到最低呢？我们构思设计一种简便而且每个人都不同的密码。可是对于当今繁忙且快节奏的生活来说，单纯的数字字符密码容易被人们遗忘或记混甚至被不法分子盗窃，高深一点的虹膜识别技术也易被伪造。据科学研究证实，人类的心率跳动和脉搏永

远不会重复，每个人的心率跳动和脉搏也都是独一无二的。因此，我们设想到利用每个人心电图微小的特异性来设计密码。下面主要阐述这款硬盘的设计原理、功能、以及辅助技术支持。

1.2 系统核心组成

以心电图作为密码的安全硬盘的首要目的是保护用户的信息安全。它使用先进的心电信号处理系统、加以辅助的指模识别认证系统，密码比对系统，提示报警系统，自动锁死系统、密码初始系统、以及自动杀毒系统、蓝牙无线传输系统及蓝牙加密系统 DES，微型电池电源和电源开关等。系统间相辅相成，大大的提高了硬盘的防盗性。

心电信号处理系统由输入装置、放大装置、控制电路组成。指模识别系统主要包括指纹输入装置，指纹图像读取装置，特征提取处理器组成。心电信号处理系统、指模识别系统的输入装置可合二为一，既减少了成本，又美化了外观。密码比对系统、自动锁死系统、自毁系统、为内部程序。提示报警系统由扬声器，示警灯组成。密码初始系统由密码初始设置系统和一根数据线组成。蓝牙无线传输系统由信号发射装置构成。

1.3 核心功能

1.3.1 初始化心电图和指纹

当用户拿到这款硬盘时，首先需要做的是设定密码初始值。首先先将随硬盘附赠的密码初始设置程序安装进一个安全的电脑内，并用数据线将硬盘与电脑连接。程序会自动启动硬盘。此时提示系统将会提示用户在输入装置上录入心电图范本以及指纹范本（心电图需要左右手各一只手指，产生电压差）。硬盘扬声器会长鸣“嘀”，提示用户心电图和指纹数据已录入密码比对系统中后，此硬盘的密码设置即已完成。随后，密码初始化程序会自动关闭硬盘。等待硬盘初始化。初始化的完成意味着硬盘“名花有主”，再也不会识别其他任何人的密码。这就为以后储存在硬盘中的文件的高安全性，打下了夯实基础。

1.3.2 存储拷贝及移除硬盘中文件

硬盘的主要功能还是易于储存和便于携带。该款安全硬盘不仅保留了普通硬盘的特征（即存储拷贝及移除），并在储存和拷贝的过程中添加安全保护的措施。当用户需要使用硬盘时，首先摁住开关一到两秒，并在提示系统提示后输入心电图和指纹数据。在密码比对系统确认与范本数据大致相同后，密码比对系统自动使硬盘开启无线蓝牙状态，可被电脑等设备搜寻到。用户随后可向硬盘内拷贝或删除文件。当文件写入硬盘时，硬盘会自动给执行杀毒系统，扫描文件并识别现有病毒库，且硬盘采用固态格式，防止文件内部程序隐藏躲避杀毒系统并盗取密码。在文件管理结束后，再次摁住开关一到两秒，硬盘关闭。此功能保证了只有用户本人才可以对硬盘中的文件进行管理，再没有别人可以私自窥觑到硬盘中文件，有效地保护了用户文件的私密性和机密性。

1.3.3 蓝牙传输及加密功能

蓝牙，具有低功耗、小体积、低成本的特点。它的即时性使得它不需要固定的基础设施，且易于安装和设置。您不需要电缆即可实现连接。但是，正是因为蓝牙的广泛性，使得蓝牙的传输变得易于被攻击、资料更易被盗。因此我们也想到了使用 DES 算法为蓝牙的传输通道进行保密，将用户的信息彻底保护起来，将“安全”进行到底。

其二，为了解决在传输过程中可能存在带毒文件进入硬盘，破坏其内部程序，导致用户信息泄露。我们也设计了自动查毒程序。将危险扼杀在萌芽里。自动杀毒程序也会在与电脑安全连接时自动与电脑杀毒程序的病毒库同步。扫罗全部最新病毒。

1.3.4 自动锁死保护文件

自动锁死功能有两点用处：

一是针对硬盘丢失，或出现硬盘被盗等悲剧发生后，有不法分子企图解锁用户的安全硬盘，当不法分子输入其他人的心电图数据和指纹数据，被密码比对系统确认不是硬盘主人自主解锁硬盘，会通过提示示警系统播放：“密码错误，请重新输入。”在三次输入密码错误后，提示系统长鸣“嘀”声三分钟并执行自动锁死功能。在自动锁死后的 24 小时内,硬盘不接收并识别任何的心电图及指纹数据,就算是硬盘主人本人的正确“密码”也不可以。在 24 小时后，硬盘心电信号处理系统、加以辅助的指模识别认证系统只提供一次认证机会，如果再次输错，硬盘将进入更长的锁死时间。这就避免了由于硬盘丢失或被盗所导致用户信息泄露的问题。将安全硬盘的安全性提升至最大化，使用户安心放心。

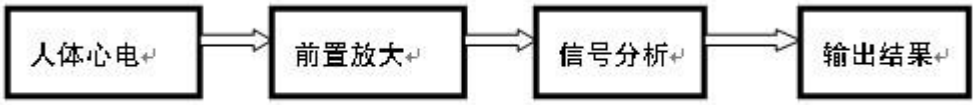
第二个用途主要针对保护企业老板，演艺明星，公务人员等需要随身携带机密文件的人员所设计的功能。据医学证明，人们在紧张时刻，身体肌肉紧绷,血管收缩,大脑耗氧量增加,于是心脏负荷增大,所以心电图加速，继而使得心电图较平静时差异较大。当遭遇绑匪等恶势力的威胁，逼迫用户启动硬盘，拷贝出绑匪所想要知道的商业机密、个人隐私，甚至是更加重要的信息时，用户心惊胆战输入密码后，密码比对系统会确认是硬盘主人使用硬盘，但由于心电图数据差别较大，密码比对系统自动认定用户处于不正常的状态下，此时该硬盘会将全部数据自动设置为隐藏，不产生任何提示，使私密不会外泄。如果在短时间内重复三次较大差异，硬盘则会直接执行自动锁死程序，将硬盘引入自动锁死状态。

第三章相关技术支持

1．心电信号处理系统

心电信号是一种由心肌收缩而产生并可提供心脏生理功能变化信息的生物电信号，有着易于检测和较好的直观性的特点。心电图则是记录心脏在每个心动周期中,由起搏点,心房,心室相继兴奋,伴随着生物电的变化,通过心电描记器从体表引出多种形式的电位变化的图形(简称 ECG) .心电图是心脏兴奋的发生,传播及恢复过程的客观指标。

1.1 心电信号处理流程



图表 1 心电信号处理流程图

1.2 心电信号处理

(1)心电信号检测

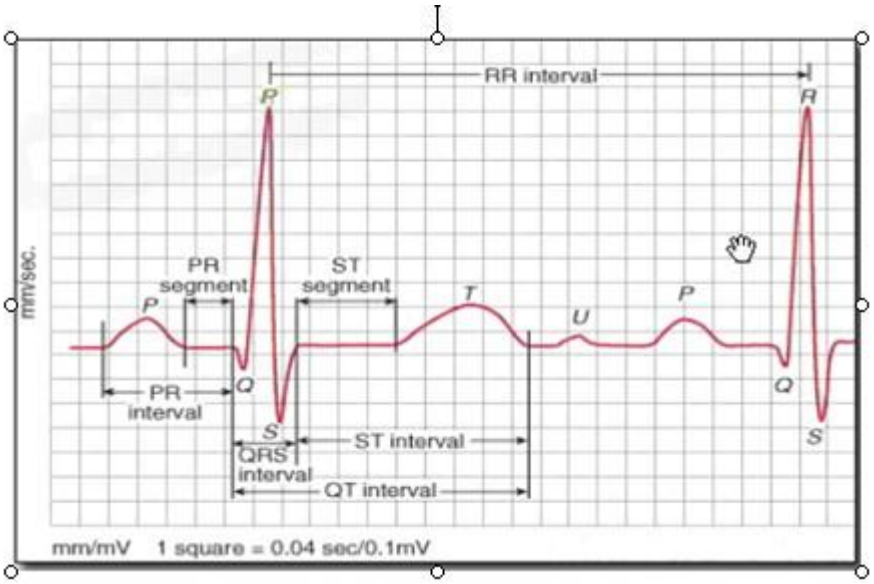
通过双极肢体导联方法左右手手指间形成的生物电位差将人体心电导入心电信号处理系统。当前绝大部分的心电信号检测方法主要分为两步：首先对心电信号进行滤波，滤除信号中的主要噪声（基漂、工频电、肌电、器械移位等），对 QRS 波群进行加强；然后采取一定的准则确定阈值，检出所需的信息。目前的手段多是应用小波变换，在时域上结合频域上对心电信号进行分析处理。信号处理的目的就是：准确的分析、诊断、编码压缩和量化、快速传递或存储、精确地重构（或恢复）。需要注意的是需要保证在相对平静的状态下导入心电信号，以保证心电的稳定性及相对一致性。

(2)心电信号预处理

通过前置放大机制将生物电放大化、抑制噪音和伪迹，并将生物电信号放大化送入后方的心电信号处理程序中。

1.3 信号分析

将放大后的心电信号通过一定的分析计算步骤得出心电的正常波动图，继而输出结果。通常方法是经验分析 EDS 方法。



图表 2 心电信号处理效果图

1.4 应用情况

该技术在我们的日常生活中已经有了比较完善的技术发展，主要应用于诊断心血管疾病等方面。

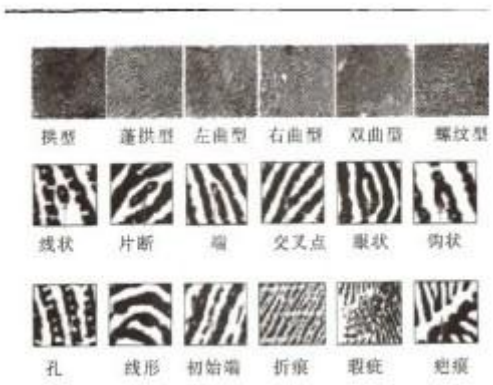
2．指纹认证识别系统

2.1 工作原理

指纹识别是在现有的硬盘系统上接入指纹采集芯片，在硬盘的主控程序中增加指纹识别处理模块，从而使其能够采集使用者的指纹，并加以识别，以达到对硬盘操作的访问控制及身份认证功能。我们提出了一种基于在移动 设备上的指纹识别系统，即可利用硬盘内置的指纹识别仪，进行个人指纹特征数据分析，随后将指纹图片发送至密码比对系统中，然后在比对系统对比最初存储的用户信息，进行身份识别。

2.2 指纹处理过程

指纹处理过程依次可分为 3 个阶段，依次是采集指纹图像、图像增强、预处理并形成模板和指纹对比。实际应用中 ，根据需求的不同，可以将人体的指纹特征分为：永久性特征 、非永久性特和生命特征。 永久性特征包括细节特征（ 中心点 、三角点 、端点、叉点、桥接点等）和辅助特征（纹型、纹密度 、纹曲率等元素 ）在人的一生中永远不会改变 ，在指前端的典型区域中最为明显，分布也最均匀。



图表 3 指纹的典型区域特征

2.3 可行性分析

尽管指纹只是人体皮肤的一小部分，但用于识别的数据量相当大，对这些数据进行比对是需要进行大量运算的模糊匹配算法。利用现代电子集成制造技术生产的小型指纹图像读取设备和速度更快的计算机，提供了在微机上进行指纹比对运算的可能。另外，匹配算法可靠性也不断提高。至此，指纹识别技术已经非常简单实用。

2.4 发展情况

指纹识别技术已经成熟，其应用也日益普遍。除了用于刑事侦察之外，在民用方面也已非常广泛，如指纹门禁系统、指纹考勤系统、银行指纹储蓄系统、银行指纹保管箱、

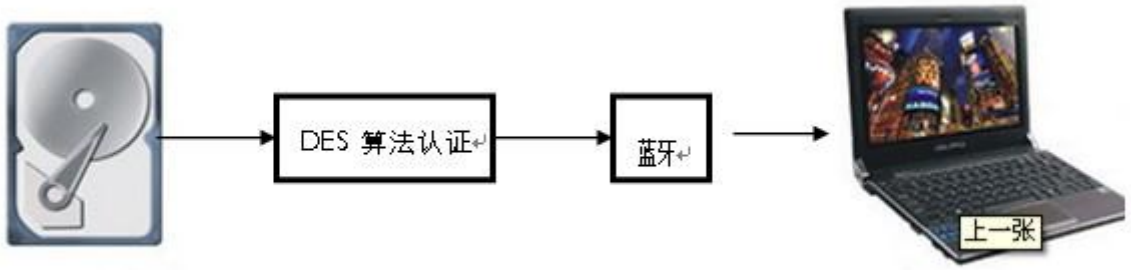
指纹医疗保险系统、计划生育指纹管理系统、幼儿接送指纹管理系统、指纹献血管理系统、证券交易指纹系统、指纹枪械管理系统、智能建筑指纹门禁管理系统、驾驶员指纹管理系统等。

3．蓝牙 DES 加密

3.1 概述

蓝牙是一种支持设备短距离通信（一般是 10m 之内）的无线电技术。能在包括移动电话、PDA、无线耳机、笔记本电脑、相关外设等众多设备之间进行无线信息交换。作为一种新技术，蓝牙的主要优点是：可以方便地建立无线连接来代替传统的有线电缆连接；移植性较强，可以应用到很多通信场合中，如 WA 它以低成本的近距离无线连接为基础，为固定与移动设备通信环境建立一个特别连接。P、GSM、DECT 等；安全性较高，且每一台蓝牙设备的地址全球唯一；功耗低、设计开发方便、成本较低。

3.2 蓝牙传输流程



图表 4 蓝牙传输流程图

3.3 蓝牙安全性

蓝牙采用的无线跳频技术使人们误认为蓝牙的安全机制已经解决。可是实际上，无线跳频技术对于窃听者和截取者不是一个技术障碍。目前的蓝牙芯片和设备并不具备数据的保密、数据的完整性和用户身份认证等安全措施。蓝牙技术在诞生之初，并没有考虑其安全性的问题。虽然现在已提供 128 位的芯片号作为设备的鉴权号，可是它在通信中可以被篡改和冒用。

3.4 蓝牙加密

我们进一步采用了分组加密算法为蓝牙传输“上保险”。

组加密算法 DES 算法综合运用了置换、代替、代数多种密码技术, 把信息分成 64 位大小的块, 使用 56 位密钥, 迭代轮数为 16 轮. 此算法有一个 64 比特的密钥作为参数, 在 DES 算法中, 将 64 位的初始密钥中的 8 个奇偶校验位剔除掉而留下真正的 56 位初始密钥. 原始信息被分成 64 位的固定长度数据块, 然后利用 56 位的加密密钥通过置换和组合方法生成 64 位的加密信息. 解密用的密钥与加密密钥相同, 只是解密步骤正好相反. DES 采用的加密方法, 一次加密一位或一个字节,形成密码流. 密码流具有自同步的

特点. DES 算法已被广泛采用并被认为是非常可靠的, 并且 DES 至今仍被公认是较安全的, 所以研究在蓝牙技术中采用 DES 加密算法来进行加密, 是一件有意义的工作。

第四章 预计技术难点

4.1 心电密码采集准确性

此问题包括如运动后的心率加快等情况或极端条件下的判定情况，以及在测量心电信号时，产生的基线漂移问题。对于基线漂移问题，当今常采用的矫正基线的方法为基线拟合方法,即通过多点采样,去掉某些突变点,拟合出基线的波形,并与输入信号相减,以得到稳定的 ECG 波形,这种方法的缺点是处理的时间较长。但是安全硬盘的目标就是解密方便简单，需要我们以后进一步解决基线漂移的高速化的问题。此外，心电信号主要适用于医疗等方面，也没有将心电信号在极端条件下使用的情况发生。如何能削减心电信号处理系统的使用条件，现在还存在问题。

4.2 微小化

一个小小的硬盘，要包容进如此庞大的安全系统所要解决的问题是如何将所需元器件微小化的问题。就未来趋势，小巧便携才使我们追求的目标。

4.3 复杂性

安全硬盘虽在大部分方面充分替用户着想，为用户提供强大的安全保护措施，但是其所需要的内部比对密码程序等会极为复杂，至今仍无法妥善解决。

4.4 蓝牙加密化

目前，蓝牙技术广泛应用于各种电话系统、无线电缆、无线公文包、各类数字电子设备、电子商务等领域，把各种便携式电脑与蜂窝移动电话用无线电路连接起来，使计算机与通信更加密切结合 起来，使人们能随时随地进行数据信息的交换与传输。但是如果我们将蓝牙技术运用到机密文件的传输，就需要考虑其安全性。DES 算法虽能在一定程度上弥补蓝牙在安全的缺憾，但是，如何将 DES 算法移植进蓝牙技术中，还需要我们进一步的探究。

第五章 发展前景

随着人们对信息安全的不断重视，对隐私的保护不断加强。可以预见，随着硬盘的普及化的发展，人们对于硬盘可靠性的要求也会越来越高。作为以心电信号为密码的安全硬盘，它将硬盘里的信息完好保存，将泄密的可能性降到最低。一方面，最大化的满足人们对信息安全的要求，让人们“存的放心”；另一方面，保留了硬盘体积小，容量大等鲜明特点，让人们“用的舒心”。无论是企业使用，还是个人使用，安全硬盘都能满足用户的需求，更好的为人们的日常生活进行服务。

第六章 总结

当今社会，移动硬盘越来越被大众所接受。其容量大，体积小，传输速度快的优点也越来越受到大众的青睐。但是它的安全性却一直没能得到解决。而以心电信号作为密码的安全硬盘则在根本上彻底解决这个问题。科技的发展是以更好的服务大众作为目标的。虽然安全硬盘目前只是一个诞生在我们创意里的一个模型，目的是利用科技来实现信息安全，将文件机密化。我们期望在不久的将来，随着安全硬盘的诞生，信息安全必然会达到一个新的高度。但是由于专业知识的限制，我们的论文可能无法有力的阐述安全硬盘的原理，敬请专家以及读者给予指正。

参考文献

[1] 丁海斌.论信息化时代电子文档的信息安全 2003 年 5 月辽宁大学学报(哲学社会科学版) 2003 年.

[2] 郑之光, 杨红丽. 以 DES 为基础的蓝牙加密算法的研究与实现. 小型微型计算机系统 2010 年.

[3] 王鑫泉 ，王 灏. 指纹识别原理及其应用.[M] 北京：局解手术学杂志， 2006 年.

[4]康健楠，李昕，王秀清，张涛. 基于经验模态分析心电信号预处理研究.[M] 宗光华，李大寨译. 北京：计算机工程与应用， 2010 年.