你的摄像头，安全吗？国密安全芯片，保护你的隐私！

1、 你的隐私安全吗？

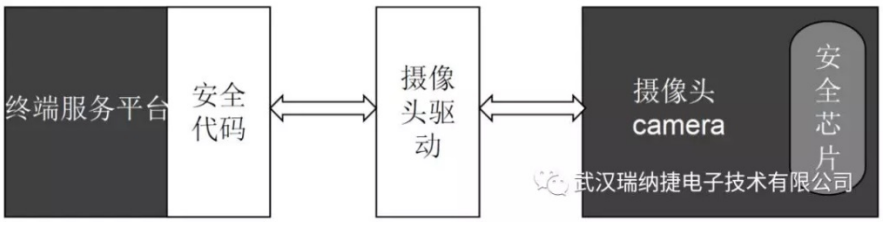
智能产品一直是近年以来的市场热点，基于智能产品的物联网，更是各大品牌竞相布局的阵地。作为其中重要组成部分的摄像头市场，更是有大量摄像制造商甚至贴牌厂商大量涌入。在市场上可以看到很多造型奇特的摄像头，其摄像头的画面清晰度也非常高，吸引了很多的家庭去使用，同时在使用的过程中也出现了很多的问题。其中，最大的问题就是安全问题，很多的摄像头在使用过程中并没有对摄像头及其操作者进行身份的认证，而导致生活隐私被暴露。

摄像头的安全使用，不仅仅限于家庭，还包括在金融行业（银行），重要场景（监狱，银行金库），工业等场景，应用于不同领域的摄像机必须使用不同的加密技术。对摄像头加密，可以保证未经授权的人无法篡改摄像头数据，同时也保证摄像头拍摄的内容需要授权才能访问。

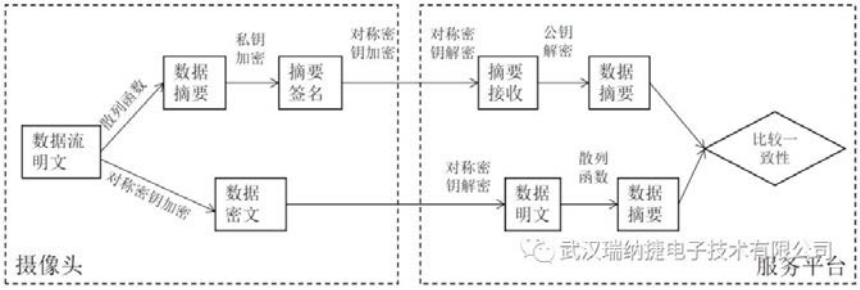
2、视频数据加解密原理

武汉瑞纳捷针对目前视频安防行业存在的普遍问题，推出一款基于高安全，低功耗的安全芯片----RJMU401；该安全芯片采用业内领先的低功耗高效率 32 位安全处理器 SC100 内核，内置 SM1/SM2/SM3/SM4/DES/RSA/AES 等多种加密算法，具备完备的安全防护，如频率检测、抗 SPA/DPA/EMA/DEMA 攻击、防篡改检测电路等措施，防止外部恶意攻击，保护芯片数据安全；该芯片已经取得国密型号认证；

那么该方案的实现原理是什么呢？



方案框架图



数据传输流程图

上述的框架图和数据流程图中，对于摄像头的加密安全使用包含了以下的技术：

1、 由于摄像头在使用过程中，会涉及很多不同的密钥。对于不同密钥，需要进行分类管理，也就是需要密钥安全管理系统（RCOS）。该密钥安全管理系统是由武汉瑞纳捷自主研发，能够满足金融级别的使用要求。

2、 身份认证技术。①外部身份认证：摄像头与终端服务平台必须要进行双端认证，鉴定彼此双方的身份。② 内部身份认证：摄像头与 RJMU401（加密芯片）之间的双端认证。

3、 图像加密：对于需要通过网络传输的图像加密，实现密文传输。只有通过了身份认证，同时也需知道密钥才能查看摄像头拍摄的内容。

3、方案的优点及安全保障

1、 采用国家密码局批准的 SM1、SM2、SM3、SM4 等高安全性密码算法，实现对信息数据的存储和传输加密，数据安全得到了全方位保障。

2、 纯硬件身份认证。该方案采用专用的加密芯片 RJMU401，实现身份认证，并以此为基础进行访问控制，充分保证了摄像头数据的安全性。

3、 多级认证体系，安全性能更高。

4、摄像头数据密文传输，防止在传输过程中数据被篡改。

4、安全芯片特点

一、32 位 ARM-SC100 安全处理器：

三级流水线架构，快速指令执行。超低功耗设计，有休眠和深度休眠模式。存储器保护单元（MPU），确保数据安全。Keil MDK 开发环境支持。自主研发的智能操作系统 COS。

二、超大的存储空间：

550KB 超大 Flash 存储空间，支持一卡多应用，随意升级和扩展应用。18KB 超大 SRAM 使数据处理畅通无阻。Flash 的擦写寿命 10 万次以上，读写一个 Page(256 字节)仅需 3ms。

三、完善的安全特性：

电压/频率/温度/光敏检测功能，防止恶意攻击破解芯片。硬件 CRC16/32 校验电路。硬件 32 位真随机数发生器。硬件防篡改检测电路。128 位唯一身份 ID。

四、强大的电气特性：

ESD 保护：4000V 以上。宽工作电压：1.62 to 5.5V。超低休眠功耗：10uA 以内。