(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109218825 B
(45)授权公告日 2020.12.11

(21)申请号 201811328492.1

(22)申请日 2018.11.09

(65)同一申请的已公布的文献号
申请公布号 CN 109218825 A

(43)申请公布日 2019.01.15

(73)专利权人 北京京航计算通讯研究所
地址 100074 北京市丰台区云岗北区西里一号院

(72)发明人 袁鹏 张卫 刘军 双世勇 欧阳文 尹严研 邓子超 马旭东 张巧霞 魏文宇 孙同飞

(74)专利代理机构 中国兵器工业集团公司专利中心 11011
代理人 周恒

(51)Int.Cl.
H04N 21/4408(2011.01)
H04L 29/06(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 108184134 A,2018.06.19
US 2018047011 A1,2018.02.15
CN 104113409 A,2014.10.22
魏振宇.基于TePA视频监控设备安全接入方法研究与实现.《中国优秀硕士学位论文全文数据库(信息科技辑)》.2017,

审查员 陈博

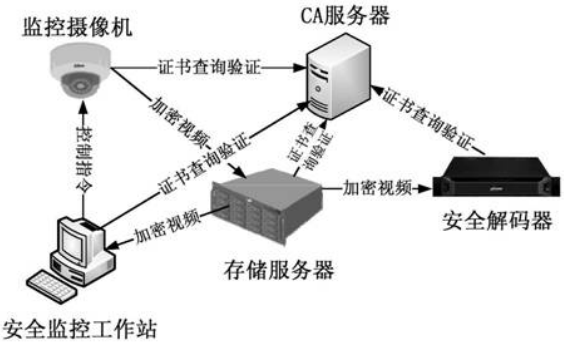
权利要求书3页 说明书12页 附图6页

(54)发明名称

一种视频加密系统

(57)摘要

本发明属于数据加密和视频安全相关技术领域,具体涉及一种视频加密系统,包括:双向认证模块、密钥协商模块、视频解密模块,安全解码器、安全监控工作站与存储服务器建立连接时,存储服务器将相关加固摄像机的视频密钥加密密钥和对应的版本号通过信令方式转发给安全解码器、安全监控工作站,转发过程执行1次密钥协商过程;设备认证,通过内置密码模块中公钥证书有效性的验证,可以对设备进行有效性验证,出现设备失控时,及时在CA服务器中将其吊销,即可阻断该设备再次入网。通过全程加密的加密方案,使得视频信息在各应用环节始终处于安全状态和严密监管之下,杜绝视频图像被非法窃取、伪造或变造的可能。



CN 109218825 B

1.一种视频加密系统,其特征在于,其应用于军队有视频加密需求的用户,所述视频加密系统包括:双向认证模块、密钥协商模块、视频加密模块;

其中,所述双向认证模块用于在存储服务器和加固摄像机之间进行双向认证,在加固摄像机首次或刷新会话通信协议注册到存储服务器时进行;通过双向认证,双方获取对方的公钥,即数字证书,公钥用于后续视频建立时的密钥协商过程,并协商消息认证密钥MAK,用于认证后续除了注册消息以外的信令;

所述密钥协商模块用于在存储服务器和加固摄像机之间进行密钥协商,用于首次建立视频加密通信之间的密钥协商、以及定时更换密钥时的自动密钥协商;包括安全监控工作站、安全解码器在内的设备需要使用视频数据时,由存储服务器转发加密视频,开始转发之前,也需要进行密钥协商,密钥协商后将视频密钥加密密钥VKEK通过信令的方式传送到最终的解密设备处;

所述视频加密模块用于在密钥协商成功后,再进行视频的加密、存储、转发和解密处理工作;

所述双向认证模块包括:双向认证存储服务器端模块和双向认证加固摄像机端模块;

所述双向认证过程中:

双向认证加固摄像机端模块用于向存储服务器发送注册请求,注册请求包括:加密算法类型域值范围和加固摄像机ID;

双向认证存储服务器端模块用于在收到双向认证加固摄像机端模块发送的注册请求后,对加密算法类型域值范围进行配置形成加密算法类型域值配置信息,并生成第一随机数R1,存储服务器将加密算法类型域值配置信息、第一随机数R1、存储服务器ID返回给加固摄像机;

双向认证加固摄像机端模块收到双向认证存储服务器端模块发送的内容后,还用于生成第二随机数R2,第二随机数R2、第一随机数R1、存储服务器ID经过运算合成后生成第一数字C1,第一数字C1利用加固摄像机的私钥进行签名,得到第一签名信息S1,双向认证加固摄像机端模块将第一随机数R1、第二随机数R2、存储服务器ID、第一签名信息S1和加固摄像机数字证书返回给存储服务器;

双向认证存储服务器端模块收到第一随机数R1、第二随机数R2、存储服务器ID、第一签名信息S1和加固摄像机数字证书后,还用于验证加固摄像机数字证书、第一随机数R1及第一签名信息S1,通过后存储服务器的内置密码模块生成密钥MAK,并利用加固摄像机数字证书对密钥MAK加密生成第二数字C2,存储服务器通过运算将第一随机数R1、第二随机数R2、加固摄像机ID生成第三数字C3,并将第二数字C2、第三数字C3加密后生成第二签名信息S2,最后存储服务器将第二数字C2、第三数字C3、第二签名信息S2和存储服务器数字证书返回给加固摄像机;

双向认证加固摄像机端模块收到第二数字C2、第三数字C3、第二签名信息S2和存储服务器数字证书后,还用于进行第二随机数R2、存储服务器数字证书的验证,验证通过后加固摄像机利用内置密码模块对第二数字C2进行解密获得密钥MAK,经过计算后得出正确的结果,则双方认证通过。

2.如权利要求1所述的视频加密系统,其特征在于,所述密钥协商模块包括:密钥协商存储服务器端模块和密钥协商加固摄像机端模块;

所述密钥协商过程中：

在双方认证通过后，所述密钥协商存储服务器端模块用于向加固摄像机发送视频请求信息，视频请求信息包括信令和经过哈希计算的密钥MAK；

所述密钥协商加固摄像机端模块接收视频请求信息后，用于验证密钥MAK，通过后，还用于分两种情况向存储服务器发送信息；

第一种情况：若加固摄像机不更新视频密钥加密密钥VKEK，则密钥协商加固摄像机端模块用存储服务器的公钥将视频密钥加密密钥VKEK加密生成视频密钥加密密钥密文EVKEK，再将视频密钥加密密钥密文EVKEK、视频密钥加密密钥版本号VKEVVersion放到SDP信道里发送给存储服务器；

第二种情况：若加固摄像机更新视频密钥加密密钥VKEK，则密钥协商加固摄像机端模块用存储服务器的公钥将视频密钥加密密钥VKEK加密生成视频密钥加密密钥密文EVKEK，再将视频密钥加密密钥密文EVKEK、更新后的视频密钥加密密钥版本号VKEVVersion、经过哈希计算的密钥MAK发给存储服务器；密钥协商存储服务器端模块收到信息后，对密钥MAK进行验证，验证通过后，经过计算获得正确结果，并反馈验证通过的信息给加固摄像机；密钥协商加固摄像机端模块获得验证通过的信息后，再将视频密钥加密密钥密文EVKEK、视频密钥加密密钥版本号VKEVVersion放到SDP信道里发送给存储服务器端；

所述密钥协商存储服务器端模块收到视频密钥加密密钥密文EVKEK、视频密钥加密密钥版本号VKEVVersion后，还用于对密钥MAK进行验证，验证通过后，验证通过后将验证回执返回给加固摄像机，密钥协商成功。

3.如权利要求2所述的视频加密系统，其特征在于，所述信令包含：视频请求类型、请求者、接收者、会话标识、当前时间和媒体要求SDP信道。

4.如权利要求3所述的视频加密系统，其特征在于，所述视频加密模块包括：加密加固摄像机端模块；所述加密加固摄像机端模块包括：读取单元、加固摄像机密码模块、加密单元、封装单元；

所述加密环节中：

所述读取单元用于读取待加密的视频数据；

加固摄像机密码模块用于随机生成引入初始量IV，并由引入初始量IV和视频加密密钥VEK通过对称算法计算后生成流密钥；

加密单元用于根据流密钥将待加密的视频数据进行加密，得到加密视频数据；

加密单元还用于采用对称算法，将视频密钥加密密钥VKEK对视频加密密钥VEK加密得到视频加密密钥密文EVEK；

封装单元用于将视频密钥加密密钥版本号VKEKVersion、视频加密密钥密文EVEK和引入初始量IV封装成安全参数集，安全参数集和加密视频数据拼接生成安全参数和视频密文封装包，即完成加密过程工作；加密加固摄像机端模块将安全参数和视频密文封装包发送给存储服务器。

5.如权利要求4所述的视频加密系统，其特征在于，所述视频加密模块包括：插入单元和存储单元；

所述存储环节中：

所述插入单元用于在接收到安全参数和视频密文封装包后，将视频密钥加密密钥版本

号VKEKVersion和视频密钥加密密钥密文EVKEK保存成VKEKVersion-EVKEK数据包，再把VKEKVersion-EVKEK数据包按接收的时间顺序插入到码流中；

所述存储单元用于将码流做本地存储，即完成存储过程工作。

6.如权利要求5所述的视频加密系统，其特征在于，所述视频加密模块包括：插入单元和转发单元；

所述转发环节中：

所述插入单元用于在接收到安全参数和视频密文封装包后，将视频密钥加密密钥版本号VKEKVersion和视频密钥加密密钥密文EVKEK保存成VKEKVersion-EVKEK数据包，再把VKEKVersion-EVKEK数据包按接收的时间顺序插入到码流中；

所述转发单元用于在收到接收方的码流转发请求后，用私钥将视频密钥加密密钥密文EVKEK进行解密，得到视频密钥加密密钥VKEK，加固摄像机利用接收方的公钥对视频密钥加密密钥VKEK重新加密后，获得新视频密钥加密密钥密文EVKEK2；然后将视频密钥加密密钥版本号VKEKVersion和新视频密钥加密密钥密文EVKEK2保存成VKEKVersion-EVKEK2数据包，再把VKEKVersion-EVKEK2数据包发送至接收方，即完成转发过程工作。

7.如权利要求6所述的视频加密系统，其特征在于，所述加固摄像机作为发送方；所述接收方为包括安全监控工作站、安全解码器在内的需要使用视频数据的设备。

8.如权利要求7所述的视频加密系统，其特征在于，所述视频加密模块包括：第一解密单元、解析单元、查找单元、第二解密单元、读取单元、运算单元、第三解密单元；

所述解密环节中：

接收方的第一解密单元用于接收到存储服务器发送的VKEKVersion-EVKEK2数据包后，利用本地私钥对新视频密钥加密密钥密文EVKEK2进行解密，得到视频密钥加密密钥原文vkek和对应的视频密钥加密密钥版本号VKEKVersion，并保存为VKEKVersion-vkek数据包存储到本地；

所述解析单元用于从收到的码流中解析出安全参数集，并从安全参数集中获取视频密钥加密密钥版本号VKEKVersion、视频加密密钥密文EVEK和引入初始量IV；

所述查找单元用于根据视频密钥加密密钥版本号VKEKVersion，从本地存储的VKEKVersion-vkek数据包中查找得到视频密钥加密密钥VKEK；

所述第二解密单元用于利用视频密钥加密密钥VKEK解密视频加密密钥密文EVEK得到视频加密密钥VEK；

所述读取单元用于读取待解密的加密视频数据；

所述运算单元用于采用分组加密算法，将视频加密密钥VEK和引入初始量IV生成流密钥；

所述第三解密单元用于根据流密钥将待解密的加密视频数据进行解密，得到解密后的视频数据，即完成解密过程工作。

一种视频加密系统

技术领域

[0001] 本发明属于数据加密和视频安全相关技术领域，具体涉及一种视频加密系统。

背景技术

[0002] 目前，网络视频监控技术的发展，其关注的重点在于系统功能的实现，主要包括视频图像的采集、存储和如何实现网络传输。而其安全则由于技术限制(实时视频大数据的加密瓶颈)和准备不足成为行业产品厂商的短板甚至是盲区，造成了目前的视频监控系统自身安全保障的缺失。

发明内容

[0003] (一)要解决的技术问题

[0004] 本发明要解决的技术问题是：如何提出一种视频数据“端模块到端模块”全程加密的加密方案，使得视频信息在各应用环节始终处于安全状态和严密监管之下，杜绝视频图像被非法窃取、伪造或变造的可能。

[0005] (二)技术方案

[0006] 为解决上述技术问题，本发明提供一种视频加密系统，其应用于军队有视频加密需求的用户，所述视频加密系统包括：双向认证模块、密钥协商模块、视频加密模块；

[0007] 其中，所述双向认证模块用于在存储服务器和加固摄像机之间进行双向认证，在加固摄像机首次或刷新会话通信协议注册到存储服务器时进行；通过双向认证，双方获取对方的公钥，即数字证书，公钥用于后续视频建立时的密钥协商过程，并协商消息认证密钥MAK，用于认证后续除了注册消息以外的信令；

[0008] 所述密钥协商模块用于在存储服务器和加固摄像机之间进行密钥协商，用于首次建立视频加密通信之间的密钥协商、以及定时更换密钥时的自动密钥协商；包括安全监控工作站、安全解码器在内的设备需要使用视频数据时，由存储服务器转发加密视频，开始转发之前，也需要进行密钥协商，密钥协商后将视频密钥加密密钥VKEK通过信令的方式传送到最终的解密设备处；

[0009] 所述视频加密模块用于在密钥协商成功后，再进行视频的加密、存储、转发和解密处理工作。

[0010] 其中，所述双向认证模块包括：双向认证存储服务器端模块和双向认证加固摄像机端模块；

[0011] 所述双向认证过程中：

[0012] 双向认证加固摄像机端模块用于向存储服务器发送注册请求，注册请求包括：加密算法类型域值范围和加固摄像机ID；

[0013] 双向认证存储服务器端模块用于在收到双向认证加固摄像机端模块发送的注册请求后，对加密算法类型域值范围进行配置形成加密算法类型域值配置信息，并生成第一随机数R1，存储服务器将加密算法类型域值配置信息、第一随机数R1、存储服务器ID返回给

加固摄像机；

[0014] 双向认证加固摄像机端模块收到双向认证存储服务器端模块发送的内容后，还用于生成第二随机数R2，第二随机数R2、第一随机数R1、存储服务器ID经过运算合成后生成第一数字C1，第一数字C1利用加固摄像机的私钥进行签名，得到第一签名信息S1，双向认证加固摄像机端模块将第一随机数R1、第二随机数R2、存储服务器ID、第一签名信息S1和加固摄像机数字证书返回给存储服务器；

[0015] 双向认证存储服务器端模块收到第一随机数R1、第二随机数R2、存储服务器ID、第一签名信息S1和加固摄像机数字证书后，还用于验证加固摄像机数字证书、第一随机数R1及第一签名信息S1，通过后存储服务器的内置密码模块生成密钥MAK，并利用加固摄像机数字证书对密钥MAK加密生成第二数字C2，存储服务器通过运算将第一随机数R1、第二随机数R2、加固摄像机ID生成第三数字C3，并将第二数字C2、第三数字C3加密后生成第二签名信息S2，最后存储服务器将第二数字C2、第三数字C3、第二签名信息S2和存储服务器数字证书返回给加固摄像机；

[0016] 双向认证加固摄像机端模块收到第二数字C2、第三数字C3、第二签名信息S2和存储服务器数字证书后，还用于进行第二随机数R2、存储服务器数字证书的验证，验证通过后加固摄像机利用内置密码模块对第二数字C2进行解密获得密钥MAK，经过计算后得出正确的结果，则双方认证通过。

[0017] 其中，所述密钥协商模块包括：密钥协商存储服务器端模块和密钥协商加固摄像机端模块；

[0018] 所述密钥协商过程中：

[0019] 在双方认证通过后，所述密钥协商存储服务器端模块用于向加固摄像机发送视频请求信息，视频请求信息包括信令和经过哈希计算的密钥MAK；

[0020] 所述密钥协商加固摄像机端模块接收视频请求信息后，用于验证密钥MAK，通过后，还用于分两种情况向存储服务器发送信息；

[0021] 第一种情况：若加固摄像机不更新视频密钥加密密钥VKEK，则密钥协商加固摄像机端模块用存储服务器的公钥将视频密钥加密密钥VKEK加密生成视频密钥加密密钥密文EVKEK，再将视频密钥加密密钥密文EVKEK、视频密钥加密密钥版本号VKEVVersion放到SDP信道里发送给存储服务器；

[0022] 第二种情况：若加固摄像机更新视频密钥加密密钥VKEK，则密钥协商加固摄像机端模块用存储服务器的公钥将视频密钥加密密钥VKEK加密生成视频密钥加密密钥密文EVKEK，再将视频密钥加密密钥密文EVKEK、更新后的视频密钥加密密钥版本号VKEVVersion、经过哈希计算的密钥MAK发给存储服务器；密钥协商存储服务器端模块收到信息后，对密钥MAK进行验证，验证通过后，经过计算获得正确结果，并反馈验证通过的信息给加固摄像机；密钥协商加固摄像机端模块获得验证通过的信息后，再将视频密钥加密密钥密文EVKEK、视频密钥加密密钥版本号VKEVVersion放到SDP信道里发送给存储服务器端；

[0023] 所述密钥协商存储服务器端模块收到视频密钥加密密钥密文EVKEK、视频密钥加密密钥版本号VKEVVersion后，还用于对密钥MAK进行验证，验证通过后，验证通过后将验证回执返回给加固摄像机，密钥协商成功。

[0024] 其中，所述信令包含：视频请求类型、请求者、接收者、会话标识、当前时间和媒体

要求SDP信道。

[0025] 其中，所述视频加密过程包括：加密环节、存储环节、转发环节、解密环节四部分，密钥协商成功后，才可进行视频的加密、存储、转发和解密处理工作。

[0026] 其中，所述视频加密模块包括：加密加固摄像机端模块；所述加密加固摄像机端模块包括：读取单元、加固摄像机密码模块、加密单元、封装单元；

[0027] 所述加密环节中：

[0028] 所述读取单元用于读取待加密的视频数据；

[0029] 加固摄像机密码模块用于随机生成引入初始量IV，并由引入初始量IV和视频加密密钥VEK通过对称算法计算后生成流密钥；

[0030] 加密单元用于根据流密钥将待加密的视频数据进行加密，得到加密视频数据；

[0031] 加密单元还用于采用对称算法，将视频密钥加密密钥VKEK对视频加密密钥VEK加密得到视频加密密钥密文EVEK；

[0032] 封装单元用于将视频密钥加密密钥版本号VKEKVersion、视频加密密钥密文EVEK和引入初始量IV封装成安全参数集，安全参数集和加密视频数据拼接生成安全参数和视频密文封装包，即完成加密过程工作；加密加固摄像机端模块将安全参数和视频密文封装包发送给存储服务器。

[0033] 其中，所述视频加密模块包括：插入单元和存储单元；

[0034] 所述存储环节中：

[0035] 所述插入单元用于在接收到安全参数和视频密文封装包后，将视频密钥加密密钥版本号VKEKVersion和视频密钥加密密钥密文EVKEK保存成VKEKVersion-EVKEK数据包，再把VKEKVersion-EVKEK数据包按接收的时间顺序插入到码流中；

[0036] 所述存储单元用于将码流做本地存储，即完成存储过程工作。

[0037] 其中，所述视频加密模块包括：插入单元和转发单元；

[0038] 所述转发环节中：

[0039] 所述插入单元用于在接收到安全参数和视频密文封装包后，将视频密钥加密密钥版本号VKEKVersion和视频密钥加密密钥密文EVKEK保存成VKEKVersion-EVKEK数据包，再把VKEKVersion-EVKEK数据包按接收的时间顺序插入到码流中；

[0040] 所述转发单元用于在收到接收方的码流转发请求后，用私钥将视频密钥加密密钥密文EVKEK进行解密，得到视频密钥加密密钥VKEK，加固摄像机利用接收方的公钥对视频密钥加密密钥VKEK重新加密后，获得新视频密钥加密密钥密文EVKEK2；然后将视频密钥加密密钥版本号VKEKVersion和新视频密钥加密密钥密文EVKEK2保存成VKEKVersion-EVKEK2数据包，再把VKEKVersion-EVKEK2数据包发送至接收方，即完成转发过程工作。

[0041] 其中，所述加固摄像机作为发送方；所述接收方为包括安全监控工作站、安全解码器在内的需要使用视频数据的设备。

[0042] 其中，所述视频加密模块包括：第一解密单元、解析单元、查找单元、第二解密单元、读取单元、运算单元、第三解密单元；

[0043] 所述解密环节中：

[0044] 接收方的第一解密单元用于接收到存储服务器发送的VKEKVersion-EVKEK2数据包后，利用本地私钥对新视频密钥加密密钥密文EVKEK2进行解密，得到视频密钥加密密钥

原文vkek和对应的视频密钥加密密钥版本号VKEKVersion，并保存为VKEKVersion-vkek数据包存储到本地；

[0045] 所述解析单元用于从收到的码流中解析出安全参数集，并从安全参数集中获取视频密钥加密密钥版本号VKEKVersion、视频加密密钥密文EVEK和引入初始量IV；

[0046] 所述查找单元用于根据视频密钥加密密钥版本号VKEKVersion，从本地存储的VKEKVersion-vkek数据包中查找得到视频密钥加密密钥VKEK；

[0047] 所述第二解密单元用于利用视频密钥加密密钥VKEK解密视频加密密钥密文EVEK得到视频加密密钥VEK；

[0048] 所述读取单元用于读取待解密的加密视频数据；

[0049] 所述运算单元用于采用分组加密算法，将视频加密密钥VEK和引入初始量IV生成流密钥；

[0050] 所述第三解密单元用于根据流密钥将待解密的加密视频数据进行解密，得到解密后的视频数据，即完成解密过程工作。

[0051] (三)有益效果

[0052] 与现有技术相比较，本发明提出一种视频数据“端模块到端模块”全程加密的加密方案，使得视频信息在各应用环节始终处于安全状态和严密监管之下，杜绝视频图像被非法窃取、伪造或变造的可能。

附图说明

[0053] 图1为本发明技术方案中加固监控系统图。

[0054] 图2为本发明技术方案中加固摄像机加密过程图。

[0055] 图3为本发明技术方案中数据终端模块解密过程图。

[0056] 图4为本发明技术方案中整个系统的主要工作流程图。

[0057] 图5为本发明技术方案中加固摄像机硬件组成图。

[0058] 图6为本发明技术方案中安全网络硬盘录像机NVR及解码器原理框图。

[0059] 图7为本发明技术方案中软件组成图。

[0060] 图8为本发明技术方案中认证协议流程图。

[0061] 图9为本发明技术方案原理图。

具体实施方式

[0062] 为使本发明的目的、内容、和优点更加清楚，下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述。

[0063] 为解决现有技术的问题，本发明提供一种视频加密方法，其应用于军队有视频加密需求的用户，如图1-图9所示，所述视频加密方法包括以下步骤：

[0064] 步骤1：双向认证；

[0065] 双向认证过程发生在存储服务器和加固摄像机之间，在加固摄像机首次或刷新会话通信协议注册到存储服务器时进行；通过双向认证，双方获取对方的公钥，即数字证书，公钥用于后续视频建立时的密钥协商过程，并协商消息认证密钥MAK，用于认证后续除了注册消息以外的信令；

[0066] 步骤2:密钥协商;

[0067] 密钥协商过程发生在存储服务器和加固摄像机之间,用于首次建立视频加密通信之间的密钥协商、以及定时更换密钥时的自动密钥协商;包括安全监控工作站、安全解码器在内的设备需要使用视频数据时,由存储服务器转发加密视频,开始转发之前,也需要进行密钥协商,密钥协商后将视频密钥加密密钥VKEK通过信令的方式传送到最终的解密设备处;

[0068] 步骤3:视频加密;

[0069] 视频加密过程包括加密过程、存储过程、转发过程、解密过程四部分,密钥协商成功后,再进行视频的加密、存储、转发和解密处理工作。

[0070] 其中,所述步骤1的双向认证过程包括如下步骤:

[0071] 步骤11:加固摄像机向存储服务器发送注册请求,注册请求包括:加密算法类型域值范围和加固摄像机ID;

[0072] 步骤12:存储服务器收到步骤11加固摄像机发送的注册请求后,对加密算法类型域值范围进行配置形成加密算法类型域值配置信息,并生成第一随机数R1,存储服务器将加密算法类型域值配置信息、第一随机数R1、存储服务器ID返回给加固摄像机;

[0073] 步骤13:加固摄像机收到步骤12存储服务器发送的内容后生成第二随机数R2,第二随机数R2、第一随机数R1、存储服务器ID经过运算合成后生成第一数字C1,第一数字C1利用加固摄像机的私钥进行签名,得到第一签名信息S1,加固摄像机将第一随机数R1、第二随机数R2、存储服务器ID、第一签名信息S1和加固摄像机数字证书返回给存储服务器;

[0074] 步骤14:存储服务器收到步骤13加固摄像机发送的内容后,验证加固摄像机数字证书、第一随机数R1及第一签名信息S1,通过后存储服务器的内置密码模块生成密钥MAK,并利用加固摄像机数字证书对密钥MAK加密生成第二数字C2,存储服务器通过运算将第一随机数R1、第二随机数R2、加固摄像机ID生成第三数字C3,并将第二数字C2、第三数字C3加密后生成第二签名信息S2,最后存储服务器将第二数字C2、第三数字C3、第二签名信息S2和存储服务器数字证书返回给加固摄像机;

[0075] 步骤15:加固摄像机收到步骤14存储服务器发送的内容后,进行第二随机数R2、存储服务器数字证书的验证,验证通过后加固摄像机利用内置密码模块对第二数字C2进行解密获得密钥MAK,经过计算后得出正确的结果,则双方认证通过。

[0076] 其中,所述步骤2的密钥协商过程包括如下步骤:

[0077] 步骤21:双方认证通过后,存储服务器向加固摄像机发送视频请求信息,视频请求信息包括信令和经过哈希计算的密钥MAK;

[0078] 步骤22:加固摄像机接收步骤21存储服务器发送的内容后,验证密钥MAK,通过后,分两种情况向存储服务器发送信息;

[0079] 第一种情况:若加固摄像机不更新视频密钥加密密钥VKEK,则摄像机用存储服务器的公钥将视频密钥加密密钥VKEK加密生成视频密钥加密密钥密文EVKEK,再将视频密钥加密密钥密文EVKEK、视频密钥加密密钥版本号VKEVVersion放到SDP信道里发送给存储服务器;

[0080] 第二种情况:若加固摄像机更新视频密钥加密密钥VKEK,则加固摄像机用存储服务器的公钥将视频密钥加密密钥VKEK加密生成视频密钥加密密钥密文EVKEK,再将视频密

钥加密密钥密文EVKEK、更新后的视频密钥加密密钥版本号VKEVVersion、经过哈希计算的密钥MAK发给存储服务器;存储服务器收到信息后,对密钥MAK进行验证,验证通过后,经过计算获得正确结果,并反馈验证通过的信息给加固摄像机;加固摄像机获得验证通过的信息后,再将视频密钥加密密钥密文EVKEK、视频密钥加密密钥版本号VKEVVersion放到SDP信道里发送给存储服务器;

[0081] 步骤23:存储服务器收到步骤22中加固摄像机发送的内容后,对密钥MAK进行验证,验证通过后,验证通过后将验证回执返回给加固摄像机,密钥协商成功

[0082] 其中,所述步骤21中,所述信令包含:视频请求类型、请求者、接收者、会话标识、当前时间和媒体要求SDP信道。

[0083] 其中,所述步骤3的视频加密过程包括:加密环节、存储环节、转发环节、解密环节四部分,密钥协商成功后,才可进行视频的加密、存储、转发和解密处理工作。

[0084] 其中,所述加密环节包括:

[0085] 步骤311:读取待加密的视频数据;

[0086] 步骤312:加固摄像机内置密码模块随机生成引入初始量IV,引入初始量IV和视频加密密钥VEK通过对称算法计算后生成流密钥;

[0087] 步骤313:流密钥将待加密的视频数据进行加密,得到加密视频数据;

[0088] 步骤314:加固摄像机采用对称算法,将视频密钥加密密钥VKEK对视频加密密钥VEK加密得到视频加密密钥密文EVEK;

[0089] 步骤315:加固摄像机将视频密钥加密密钥版本号VKEKVersion、视频加密密钥密文EVEK和引入初始量IV封装成安全参数集,安全参数集和加密视频数据拼接生成安全参数和视频密文封装包,即完成加密过程工作;加固摄像机将安全参数和视频密文封装包发送给存储服务器。

[0090] 其中,所述存储环节包括:

[0091] 步骤321:存储服务器接收到步骤315加固摄像机发送的内容后,将视频密钥加密密钥版本号VKEKVersion和视频密钥加密密钥密文EVKEK保存成VKEKVersion-EVKEK数据包,再把VKEKVersion-EVKEK数据包按接收的时间顺序插入到码流中;

[0092] 步骤322:存储服务器将码流做本地存储,即完成存储过程工作。

[0093] 其中,所述转发环节包括:

[0094] 步骤331:存储服务器接收到步骤315加固摄像机发送的内容后,将视频密钥加密密钥版本号VKEKVersion和视频密钥加密密钥密文EVKEK保存成VKEKVersion-EVKEK数据包,再把VKEKVersion-EVKEK数据包按接收的时间顺序插入到码流中;

[0095] 步骤332:存储服务器收到接收方的码流转发请求后,用私钥将视频密钥加密密钥密文EVKEK进行解密,得到视频密钥加密密钥VKEK,加固摄像机利用接收方的公钥对视频密钥加密密钥VKEK重新加密后,获得新视频密钥加密密钥密文EVKEK2;然后将视频密钥加密密钥版本号VKEKVersion和新视频密钥加密密钥密文EVKEK2保存成VKEKVersion-EVKEK2数据包,再把VKEKVersion-EVKEK2数据包发送至接收方,即完成转发过程工作。

[0096] 其中,所述加固摄像机作为发送方;所述接收方为包括安全监控工作站、安全解码器在内的需要使用视频数据的设备。

[0097] 其中,所述解密环节包括:

[0098] 步骤341:接收方接收到存储服务器发送的内容后,利用本地私钥对新视频密钥加密密钥密文EVKEK2进行解密,得到视频密钥加密密钥原文vkek和对应的视频密钥加密密钥版本号VKEKVersion,并保存为VKEKVersion-vkek数据包存储到本地;

[0099] 步骤342:接收方从收到的码流中解析出安全参数集,并从安全参数集中获取视频密钥加密密钥版本号VKEKVersion、视频加密密钥密文EVEK和引入初始量IV;

[0100] 根据视频密钥加密密钥版本号VKEKVersion,从步骤341中本地存储的VKEKVersion-vkek数据包中查找得到视频密钥加密密钥VKEK;

[0101] 步骤343:利用视频密钥加密密钥VKEK解密视频加密密钥密文EVEK得到视频加密密钥VEK;

[0102] 步骤344:读取待解密的加密视频数据;

[0103] 步骤345:采用分组加密算法,将视频加密密钥VEK和引入初始量IV生成流密钥;

[0104] 步骤346:流密钥将待解密的加密视频数据进行解密,得到解密后的视频数据,即完成解密过程工作。

[0105] 此外,本发明还提供一种视频加密系统,其应用于军队有视频加密需求的用户,所述视频加密系统包括:双向认证模块、密钥协商模块、视频加密模块;

[0106] 其中,所述双向认证模块用于在存储服务器和加固摄像机之间进行双向认证,在加固摄像机首次或刷新会话通信协议注册到存储服务器时进行;通过双向认证,双方获取对方的公钥,即数字证书,公钥用于后续视频建立时的密钥协商过程,并协商消息认证密钥MAK,用于认证后续除了注册消息以外的信令;

[0107] 所述密钥协商模块用于在存储服务器和加固摄像机之间进行密钥协商,用于首次建立视频加密通信之间的密钥协商、以及定时更换密钥时的自动密钥协商;包括安全监控工作站、安全解码器在内的设备需要使用视频数据时,由存储服务器转发加密视频,开始转发之前,也需要进行密钥协商,密钥协商后将视频密钥加密密钥VKEK通过信令的方式传送到最终的解密设备处;

[0108] 所述视频加密模块用于在密钥协商成功后,再进行视频的加密、存储、转发和解密处理工作。

[0109] 其中,所述双向认证模块包括:双向认证存储服务器端模块和双向认证加固摄像机端模块;

[0110] 所述双向认证过程中:

[0111] 双向认证加固摄像机端模块用于向存储服务器发送注册请求,注册请求包括:加密算法类型域值范围和加固摄像机ID;

[0112] 双向认证存储服务器端模块用于在收到双向认证加固摄像机端模块发送的注册请求后,对加密算法类型域值范围进行配置形成加密算法类型域值配置信息,并生成第一随机数R1,存储服务器将加密算法类型域值配置信息、第一随机数R1、存储服务器ID返回给加固摄像机;

[0113] 双向认证加固摄像机端模块收到双向认证存储服务器端模块发送的内容后,还用于生成第二随机数R2,第二随机数R2、第一随机数R1、存储服务器ID经过运算合成后生成第一数字C1,第一数字C1利用加固摄像机的私钥进行签名,得到第一签名信息S1,双向认证加固摄像机端模块将第一随机数R1、第二随机数R2、存储服务器ID、第一签名信息S1和加固摄

像机数字证书返回给存储服务器；

[0114] 双向认证存储服务器端模块收到第一随机数R1、第二随机数R2、存储服务器ID、第一签名信息S1和加固摄像机数字证书后，还用于验证加固摄像机数字证书、第一随机数R1及第一签名信息S1，通过后存储服务器的内置密码模块生成密钥MAK，并利用加固摄像机数字证书对密钥MAK加密生成第二数字C2，存储服务器通过运算将第一随机数R1、第二随机数R2、加固摄像机ID生成第三数字C3，并将第二数字C2、第三数字C3加密后生成第二签名信息S2，最后存储服务器将第二数字C2、第三数字C3、第二签名信息S2和存储服务器数字证书返回给加固摄像机；

[0115] 双向认证加固摄像机端模块收到第二数字C2、第三数字C3、第二签名信息S2和存储服务器数字证书后，还用于进行第二随机数R2、存储服务器数字证书的验证，验证通过后加固摄像机利用内置密码模块对第二数字C2进行解密获得密钥MAK，经过计算后得出正确的结果，则双方认证通过。

[0116] 其中，所述密钥协商模块包括：密钥协商存储服务器端模块和密钥协商加固摄像机端模块；

[0117] 所述密钥协商过程中：

[0118] 在双方认证通过后，所述密钥协商存储服务器端模块用于向加固摄像机发送视频请求信息，视频请求信息包括信令和经过哈希计算的密钥MAK；

[0119] 所述密钥协商加固摄像机端模块接收视频请求信息后，用于验证密钥MAK，通过后，还用于分两种情况向存储服务器发送信息；

[0120] 第一种情况：若加固摄像机不更新视频密钥加密密钥VKEK，则密钥协商加固摄像机端模块用存储服务器的公钥将视频密钥加密密钥VKEK加密生成视频密钥加密密钥密文EVKEK，再将视频密钥加密密钥密文EVKEK、视频密钥加密密钥版本号VKEVVersion放到SDP信道里发送给存储服务器；

[0121] 第二种情况：若加固摄像机更新视频密钥加密密钥VKEK，则密钥协商加固摄像机端模块用存储服务器的公钥将视频密钥加密密钥VKEK加密生成视频密钥加密密钥密文EVKEK，再将视频密钥加密密钥密文EVKEK、更新后的视频密钥加密密钥版本号VKEVVersion、经过哈希计算的密钥MAK发给存储服务器；密钥协商存储服务器端模块收到信息后，对密钥MAK进行验证，验证通过后，经过计算获得正确结果，并反馈验证通过的信息给加固摄像机；密钥协商加固摄像机端模块获得验证通过的信息后，再将视频密钥加密密钥密文EVKEK、视频密钥加密密钥版本号VKEVVersion放到SDP信道里发送给存储服务器端；

[0122] 所述密钥协商存储服务器端模块收到视频密钥加密密钥密文EVKEK、视频密钥加密密钥版本号VKEVVersion后，还用于对密钥MAK进行验证，验证通过后，验证通过后将验证回执返回给加固摄像机，密钥协商成功。

[0123] 其中，所述信令包含：视频请求类型、请求者、接收者、会话标识、当前时间和媒体要求SDP信道。

[0124] 其中，所述视频加密过程包括：加密环节、存储环节、转发环节、解密环节四部分，密钥协商成功后，才可进行视频的加密、存储、转发和解密处理工作。

[0125] 其中，所述视频加密模块包括：加密加固摄像机端模块；所述加密加固摄像机端模块包括：读取单元、加固摄像机密码模块、加密单元、封装单元；

[0126] 所述加密环节中：

[0127] 所述读取单元用于读取待加密的视频数据；

[0128] 加固摄像机密码模块用于随机生成引入初始量IV，并由引入初始量IV和视频加密密钥VEK通过对称算法计算后生成流密钥；

[0129] 加密单元用于根据流密钥将待加密的视频数据进行加密，得到加密视频数据；

[0130] 加密单元还用于采用对称算法，将视频密钥加密密钥VKEK对视频加密密钥VEK加密得到视频加密密钥密文EVEK；

[0131] 封装单元用于将视频密钥加密密钥版本号VKEKVersion、视频加密密钥密文EVEK和引入初始量IV封装成安全参数集，安全参数集和加密视频数据拼接生成安全参数和视频密文封装包，即完成加密过程工作；加密加固摄像机端模块将安全参数和视频密文封装包发送给存储服务器。

[0132] 其中，所述视频加密模块包括：插入单元和存储单元；

[0133] 所述存储环节中：

[0134] 所述插入单元用于在接收到安全参数和视频密文封装包后，将视频密钥加密密钥版本号VKEKVersion和视频密钥加密密钥密文EVKEK保存成VKEKVersion-EVKEK数据包，再把VKEKVersion-EVKEK数据包按接收的时间顺序插入到码流中；

[0135] 所述存储单元用于将码流做本地存储，即完成存储过程工作。

[0136] 其中，所述视频加密模块包括：插入单元和转发单元；

[0137] 所述转发环节中：

[0138] 所述插入单元用于在接收到安全参数和视频密文封装包后，将视频密钥加密密钥版本号VKEKVersion和视频密钥加密密钥密文EVKEK保存成VKEKVersion-EVKEK数据包，再把VKEKVersion-EVKEK数据包按接收的时间顺序插入到码流中；

[0139] 所述转发单元用于在收到接收方的码流转发请求后，用私钥将视频密钥加密密钥密文EVKEK进行解密，得到视频密钥加密密钥VKEK，加固摄像机利用接收方的公钥对视频密钥加密密钥VKEK重新加密后，获得新视频密钥加密密钥密文EVKEK2；然后将视频密钥加密密钥版本号VKEKVersion和新视频密钥加密密钥密文EVKEK2保存成VKEKVersion-EVKEK2数据包，再把VKEKVersion-EVKEK2数据包发送至接收方，即完成转发过程工作。

[0140] 其中，所述加固摄像机作为发送方；所述接收方为包括安全监控工作站、安全解码器在内的需要使用视频数据的设备。

[0141] 其中，所述视频加密模块包括：第一解密单元、解析单元、查找单元、第二解密单元、读取单元、运算单元、第三解密单元；

[0142] 所述解密环节中：

[0143] 接收方的第一解密单元用于接收到存储服务器发送的VKEKVersion-EVKEK2数据包后，利用本地私钥对新视频密钥加密密钥密文EVKEK2进行解密，得到视频密钥加密密钥原文vkek和对应的视频密钥加密密钥版本号VKEKVersion，并保存为VKEKVersion-vkek数据包存储到本地；

[0144] 所述解析单元用于从收到的码流中解析出安全参数集，并从安全参数集中获取视频密钥加密密钥版本号VKEKVersion、视频加密密钥密文EVEK和引入初始量IV；

[0145] 所述查找单元用于根据视频密钥加密密钥版本号VKEKVersion，从本地存储的

VKEKVersion-vkek数据包中查找得到视频密钥加密密钥VKEK；

[0146] 所述第二解密单元用于利用视频密钥加密密钥VKEK解密视频加密密钥密文EVEK得到视频加密密钥VEK；

[0147] 所述读取单元用于读取待解密的加密视频数据；

[0148] 所述运算单元用于采用分组加密算法，将视频加密密钥VEK和引入初始量IV生成流密钥；

[0149] 所述第三解密单元用于根据流密钥将待解密的加密视频数据进行解密，得到解密后的视频数据，即完成解密过程工作。

[0150] 综上，本发明涉及一种视频加密的加密方法及系统，属于数据加密和视频安全相关领域。为摆脱实时视频大数据的加密瓶颈，保障视频监控系统自身安全，本发明提供一种高清视频“端模块到端模块”的全程加密的加密方法及系统，包括步骤：密钥协商，存储服务器和加固摄像机建立视频连接时，进行密钥协商，协商成功后更换视频密钥加密密钥VKEK；加密传输，视频加密密钥VEK由交互的视频密钥加密密钥VKEK加密后也随码流一起传输，视频加密密钥VEK每1小时更新一次，在视频监控网络中传输时，视频数据以加密形态出现；密文存储，加密视频数据到达存储服务器后，由存储服务器直接以密文方式存入本地；加密转发，安全解码器、安全监控工作站与存储服务器建立连接时，存储服务器将相关加固摄像机的视频密钥加密密钥和对应的版本号通过信令方式转发给安全解码器、安全监控工作站，转发过程执行1次密钥协商过程；设备认证，通过内置密码模块中公钥证书有效性的验证，可以对设备进行有效性验证，出现设备失控时，及时在CA服务器中将其吊销，即可阻断该设备再次入网。

[0151] 实施例1

[0152] 本实施例中包括：

[0153] (1)密钥协商

[0154] 存储服务器和加固摄像机建立视频连接时，每24小时进行1次密钥协商，协商成功后更换视频密钥加密密钥。密钥协商基于公钥密码算法，在CA服务器的支撑下进行。

[0155] (2)加密传输

[0156] 密钥协商成功后，加固摄像机使用本地生成的视频加密密钥对视频数据进行加密，视频加密密钥VEK由交互的视频密钥加密密钥VKEK加密后也随码流一起传输，视频加密密钥VEK每1小时更新一次。在视频监控网络中传输时，视频数据以加密形态出现。

[0157] (3)密文存储

[0158] 加密视频数据到达存储服务器后，由存储服务器直接以密文方式存入本地。

[0159] 安全监控工作站调取历史数据查看时，存储服务器先用私钥解密出录像文件中保存的视频密钥加密密钥VKEK的原文，并用码流接收方的公钥对视频密钥加密密钥VKEK原文重新加密；录像文件保持加密形式发送给码流接收方；接收方用自己的私钥解密视频密钥加密密钥VKEK后，用视频密钥加密密钥VKEK解密视频加密密钥VEK，从而解密视频流用于播放。

[0160] (4)加密转发

[0161] 安全解码器和安全监控工作站不直接连接加固摄像机，通过存储服务器获得视频数据。安全解码器、安全监控工作站与存储服务器建立连接时，存储服务器将相关加固摄像

机的视频密钥加密密钥和对应的版本号通过信令方式转发给安全解码器、安全监控工作站，转发过程也要执行1次密钥协商过程，区别是视频加密密钥不是新生成的，是转发加固摄像机的。

[0162] (5)设备认证

[0163] 通过内置密码模块中公钥证书有效性的验证，可以对设备进行有效性验证。出现设备失控时，及时在CA服务器中将其吊销，即可阻断该设备再次入网。

[0164] 实施例2

[0165] 本实施例中，提供一种使用军队公共普通密码算法中的非对称密码算法、对称密码算法和杂凑密码算法的加密方法，算法采用满足军队公共普通密码标准的安全密码部件或密码产品实现。所述算法包括：

[0166] (1)非对称密码算法用于身份鉴别、数字签名、密钥协商等；

[0167] (2)对称密码算法用于视频数据的加密保护；

[0168] (3)杂凑密码算法用于对签名信息的完整性进行校验。

[0169] 该视频加密方法，其密钥管理包括：

[0170] (1)视频密钥加密密钥VKEK：密钥长度为16字节，通过平台的公普加密设备实时生成，每24小时更换一次，用后覆盖；

[0171] (2)视频加密密钥VEK：密钥长度为16字节，通过摄像头内置的公普加密设备实时生成，每小时更换1次，用后覆盖；

[0172] (3)发送方和接收方设备公钥：密钥长度为382比特，通过军队公用普通密码基础设施预先生成；

[0173] (4)发送方设备私钥：密钥长度为191比特，通过军队公用普通密码基础设施预先生成；

[0174] (5)接收方设备私钥：密钥长度为191比特，过军队公用普通密码基础设施预先生成。

[0175] 实施例3

[0176] 本实施例主要包括前端模块安全视频采集接入和后端模块服务中心管理两大部分。

[0177] 首先，利用前端模块的视频采集设备，包括高清安全网络摄像机，将视频数据采集并加密后，通过视频专网传输到后端模块管理中心。然后通过管理中心的视频管理主服务器、流媒体服务器、存储服务器、安全解码器、CA认证服务器及安全工作站等后端模块管理设备对视频数据进行安全的客户端模块浏览、集中存储、电视墙观看等具体应用。

[0178] 视频数据安全传输的关键节点体现在：

[0179] (1)实现前端模块视频加密，保护用户的重要及敏感图像不被非法窃取、篡改；

[0180] (2)安全认证管理，网络内所有安全设备采用数字证书实现身份认证，防止未经授权的设备侵入系统，同时采用数据完整性保护算法，对会话协议和控制协议进行保护，防止非法用户的协议攻击。

[0181] 其中，在各类摄像头中分别配置1块USB密码模块；在存储服务器、安全解码器及监控工作站上分别配置一套标准的PCIE密码卡。

[0182] 公普密码设备配置及密钥配置情况见下表：

[0183]

安装地点	设备名称	配套密码设备	密钥配置	功能描述
前端模块安装点	加固摄像机	USB接口密码模块	本机设备公私钥对、CA证书	前端模块采集设备对视频流进行签名及加密传输，对信令进行完整性校验及认证。
后端模块机房	CA认证服务器	标准PCIE密码卡或USB密码模块	全网公钥证书、CA公私钥对	数字证书查询验证
	视频管理主服务器			设备入网认证、域管理、远程登录管理。
	存储服务器	标准PCIE密码卡	本机设备公私钥对、CA证书	视频信息存储，视频流转发
指控中心	安全解码器	标准PCIE密码卡	全网KEK，本机设备公私钥对、CA证书	监控中心解码服务器，通过认证服务器认证接入视频加固管理平台，对视频进行存储、解码
	安全监控工作站	标准PCIE密码卡	全网KEK，本机设备公私钥对、CA证书	管理工作站，接入视频加固管理平台，对系统内设备进行配置、管理、状态监控、指挥调度，B/S、C/S架构。

[0184] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明技术原理的前提下，还可以做出若干改进和变形，这些改进和变形也应视为本发明的保护范围。

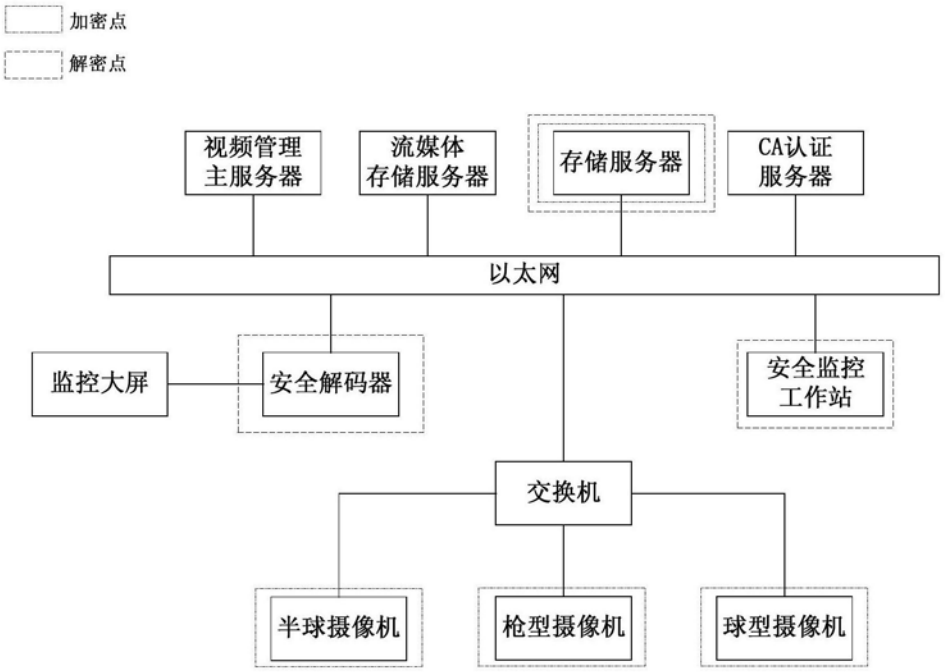

加密点
解密点
视频管理
主服务器
流媒体
存储服务器
存储服务器
CA认证
服务器
以太网
监控大屏
安全解码器
安全监控
工作站
交换机
半球摄像机
枪型摄像机
球型摄像机

图1

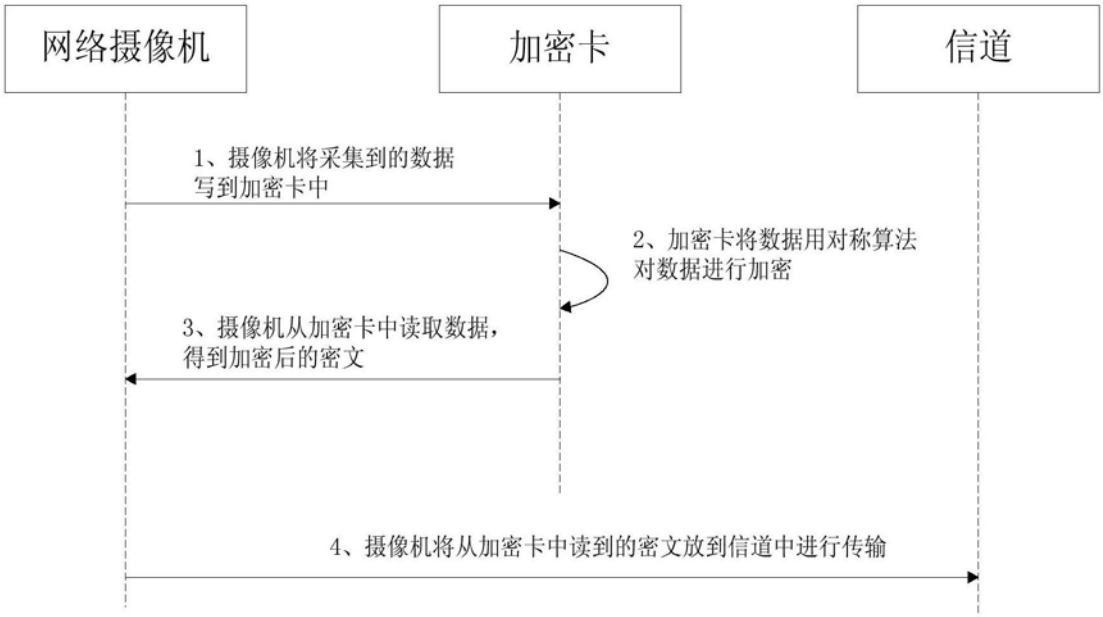

网络摄像机
加密卡
信道
1、摄像机将采集到的数据
写到加密卡中
2、加密卡将数据用对称算法
对数据进行加密
3、摄像机从加密卡中读取数据，
得到加密后的密文
4、摄像机将从加密卡中读到的密文放到信道中进行传输

图2

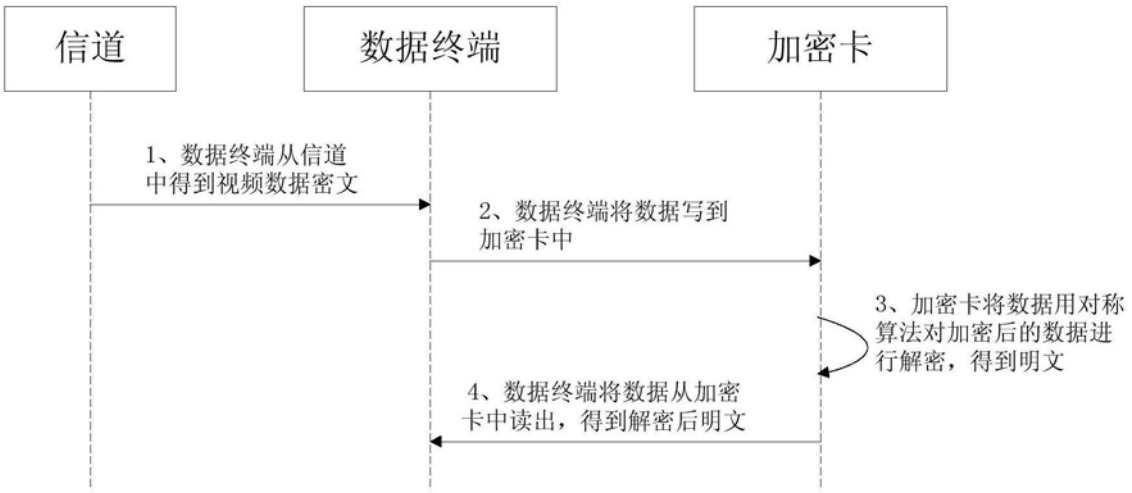

信道
数据终端
加密卡
1、数据终端从信道中得到视频数据密文
2、数据终端将数据写到加密卡中
3、加密卡将数据用对称算法对加密后的数据进行解密，得到明文
4、数据终端将数据从加密卡中读出，得到解密后明文

图3

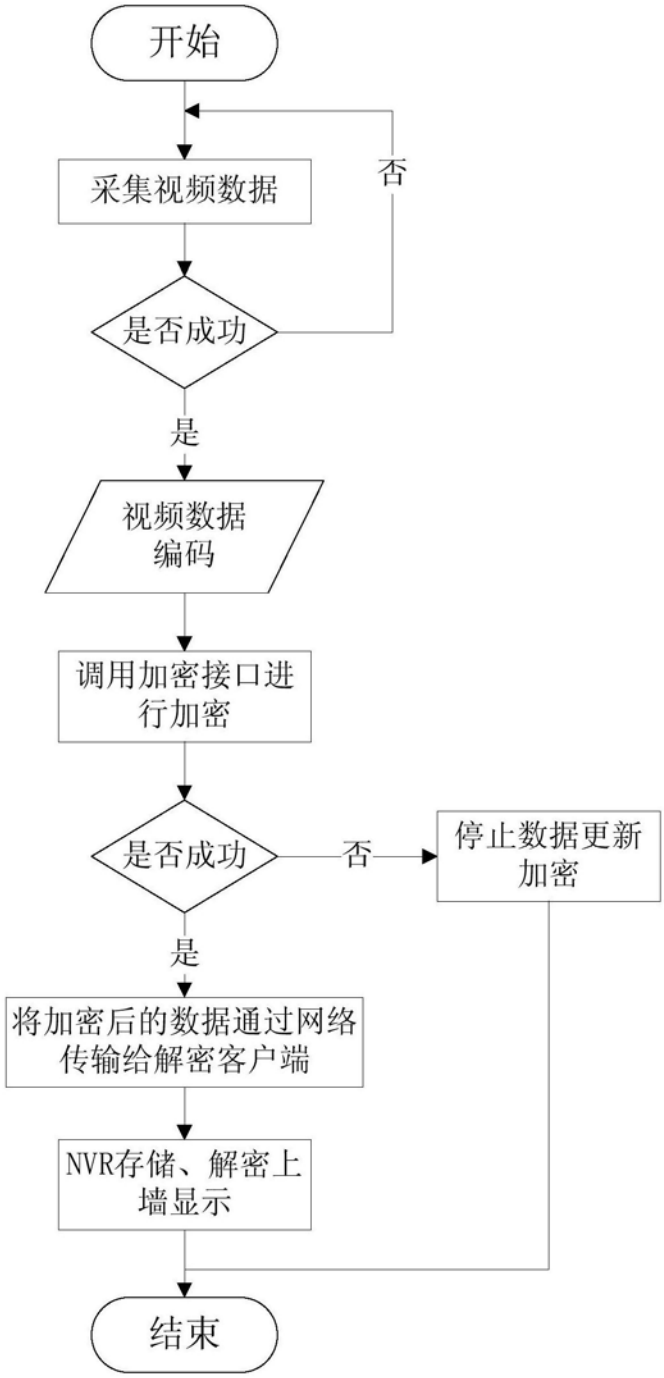

开始
采集视频数据
否
是否成功
是
视频数据
编码
调用加密接口进
行加密
是否成功
否
停止数据更新
加密
是
将加密后的数据通过网络
传输给解密客户端
NVR存储、解密上
墙显示
结束

图4

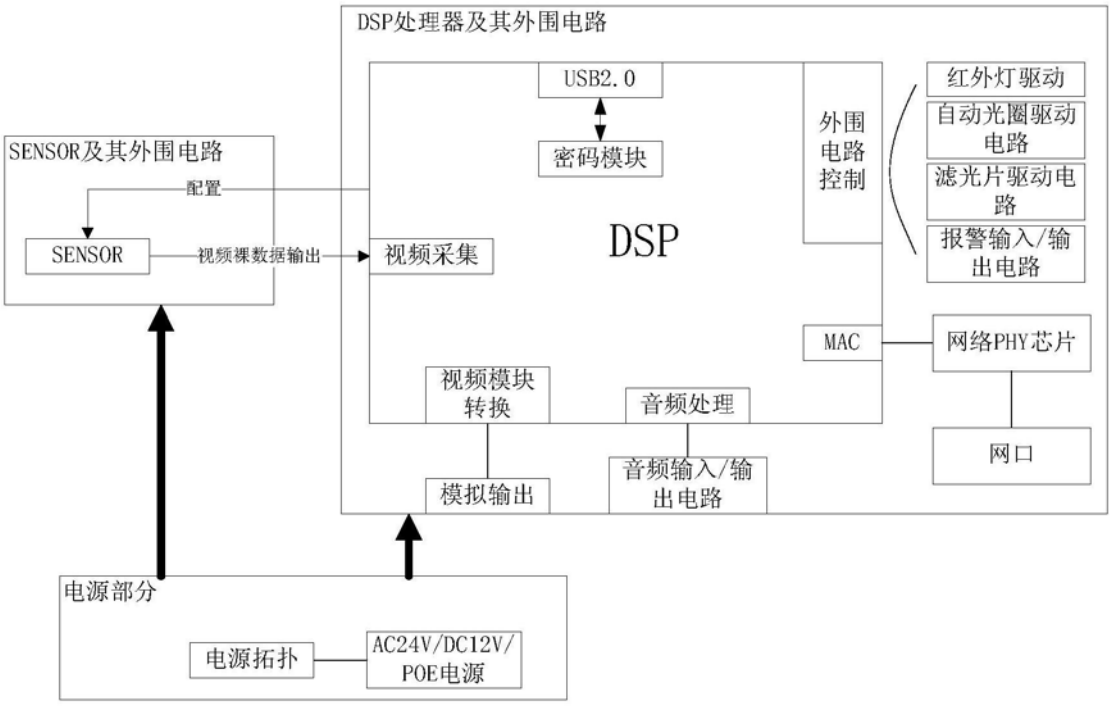

DSP处理器及其外围电路
USB2.0
密码模块
DSP
外围电路控制
红外灯驱动
自动光圈驱动电路
滤光片驱动电路
报警输入/输出电路
SENSOR及其外围电路
配置
SENSOR
视频裸数据输出
视频采集
MAC
网络PHY芯片
视频模块转换
音频处理
网口
模拟输出
音频输入/输出电路
电源部分
电源拓扑
AC24V/DC12V/POE电源

图5

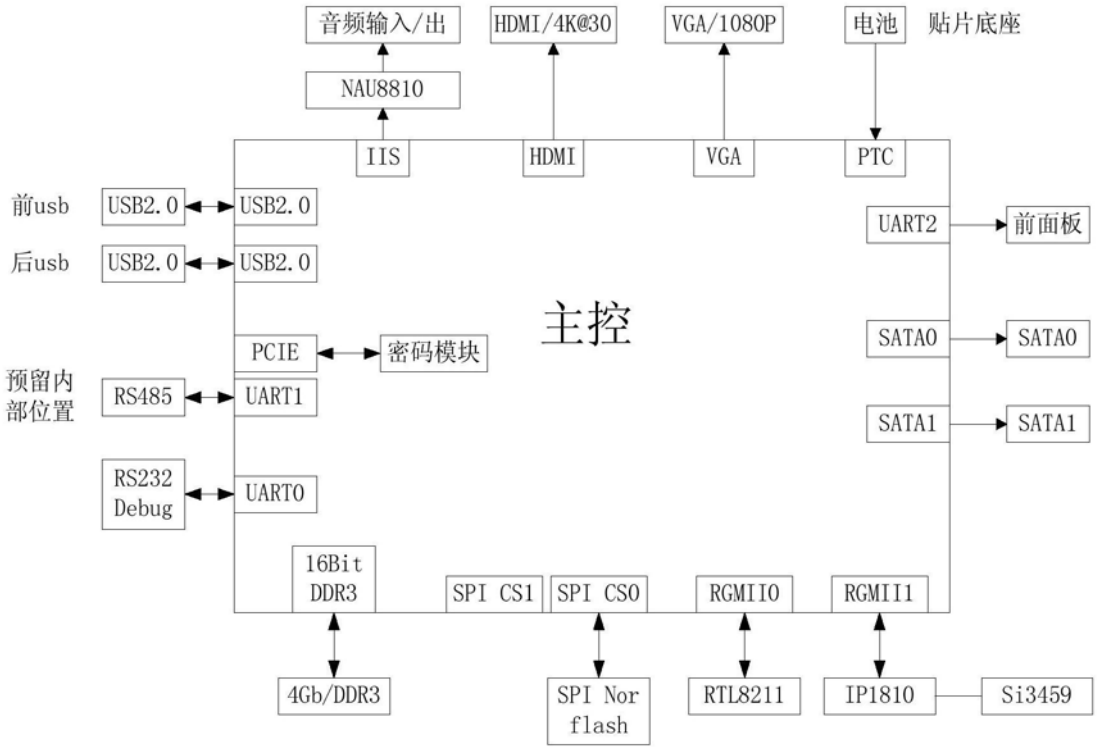

音频输入/出
HDMI/4K@30
VGA/1080P
电池
贴片底座
NAU8810
IIS
HDMI
VGA
PTC
前usb
USB2.0
USB2.0
UART2
前面板
后usb
USB2.0
USB2.0
主控
PCIE
密码模块
SATA0
SATA0
预留内部位置
RS485
UART1
SATA1
SATA1
RS232 Debug
UART0
16Bit DDR3
SPI CS1
SPI CS0
RGMII0
RGMII1
4Gb/DDR3
SPI Nor flash
RTL8211
IP1810
Si3459

图6

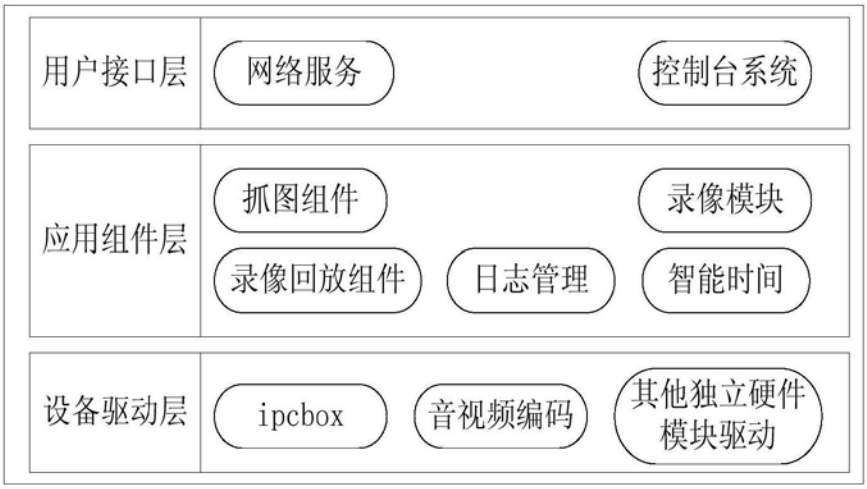

用户接口层
网络服务
控制台系统
应用组件层
抓图组件
录像模块
录像回放组件
日志管理
智能时间
设备驱动层
ipcbox
音视频编码
其他独立硬件
模块驱动

图7

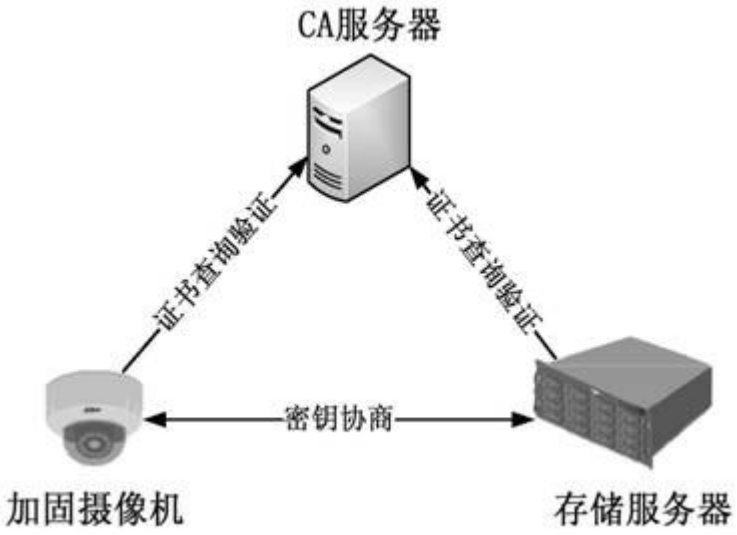

CA服务器
证书查询验证
证书查询验证
密钥协商
加固摄像机
存储服务器

图8

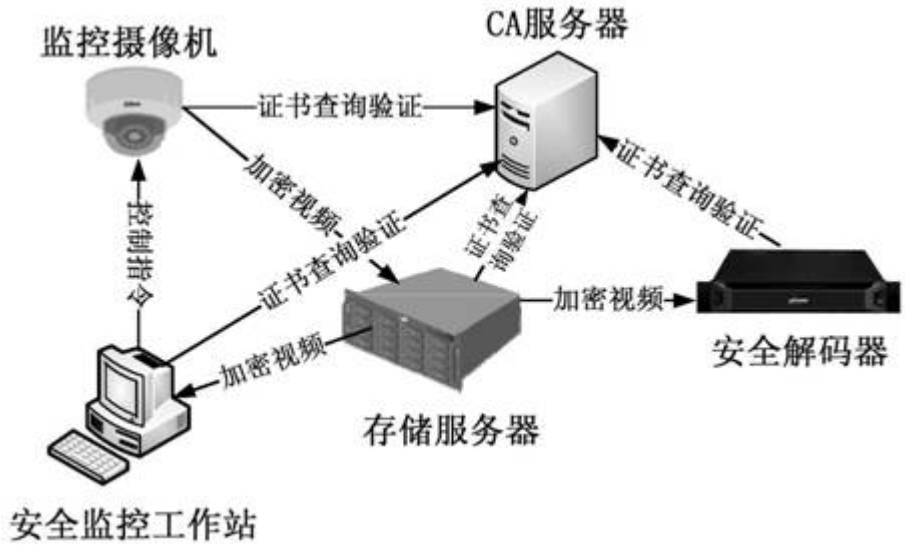

监控摄像机
CA服务器
证书查询验证
加密视频
证书查询验证
证书查询验证
证书查询验证
控制指令
证书查询验证
加密视频
加密视频
安全解码器
存储服务器
安全监控工作站

图9