(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 110427762 B
(45)授权公告日 2021.03.23

(21)申请号 201910664442.9

(22)申请日 2019.07.23

(65)同一申请的已公布的文献号
申请公布号 CN 110427762 A

(43)申请公布日 2019.11.08

(73)专利权人 湖南匡安网络技术有限公司
地址 410082 湖南省长沙市岳麓区麓山南路252号国家超级计算长沙中心1号楼
专利权人 湖南大学

(72)发明人 李肯立 刘俊 覃舒婕 杨志邦 徐晓阳 王远亮

(74)专利代理机构 武汉臻诚专利代理事务所(普通合伙) 42233
代理人 宋业斌

(51)Int.Cl.
G06F 21/60(2013.01)
H04L 9/00(2006.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 109218825 A,2019.01.15
CN 102469344 A,2012.05.23
EP 3193486 A1,2017.07.19
CN 101552666 A,2009.10.07
US 8522027 B2,2013.08.27
CN 108199824 A,2018.06.22
CN 109831295 A,2019.05.31
CN 109921905 A,2019.06.21
CN 1980451 A,2007.06.13
CN 108365947 A,2018.08.03
CN 102123392 A,2011.07.13
CN 109218018 A,2019.01.15
CN 108924594 A,2018.11.30

审查员 罗捷

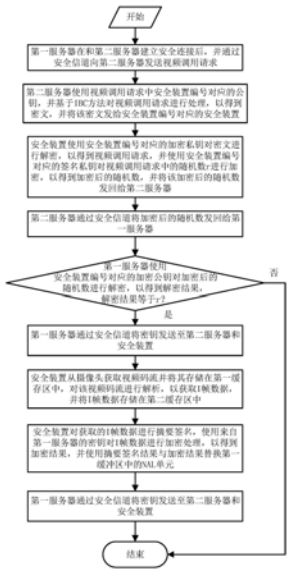
权利要求书5页 说明书13页 附图3页

(54)发明名称

一种实现电力监控系统视频安全传输的加密和解密方法

(57)摘要

本发明公开了一种实现电力监控系统视频安全传输的加密方法,包括:第一服务器在和第二服务器建立安全连接后,并通过安全信道向第二服务器发送视频调用请求,第二服务器使用视频调用请求中安全装置编号对应的公钥,并基于IBC方法对视频调用请求进行处理,以得到密文,并将该密文发给安全装置编号对应的安全装置,安全装置使用安全装置编号对应的加密私钥对密文进行解密,以得到视频调用请求,并使用安全装置编号对应的签名私钥对视频调用请求中的随机数进行加密,以得到加密后的随机数,并将该加密后的随机数发回给第二服务器。本发明能够针对视频监控系统的特征和安全威胁设计安全防护机制,从而确保视频监控系统的安全性和可靠性。



CN 110427762 B

1.一种实现电力监控系统视频安全传输的加密方法，是应用在包括通过网络彼此通信连接的第一局域网和第二局域网的电力监控系统中，其中第一局域网包括多个第一终端设备以及与其通信连接的第一服务器，所述第二局域网包括多个第二终端设备、多个安全装置、以及第二服务器，第二终端设备通过第二服务器与安全装置通信连接，其特征在于，所述加密方法包括以下步骤：

(1)第一服务器在和第二服务器建立安全连接后，并通过安全信道向第二服务器发送视频调用请求，该视频调用请求中包括该安全装置编号CID和随机产生的随机数r；

(2)第二服务器使用视频调用请求中安全装置编号CID对应的公钥Q_{CID}，并基于IBC方法对视频调用请求进行处理，以得到密文，并将该密文发给安全装置编号CID对应的安全装置；

(3)安全装置使用安全装置编号CID对应的加密私钥S_{CID}对密文进行解密，以得到视频调用请求，并使用安全装置编号CID对应的签名私钥S'_{CID}对视频调用请求中的随机数r进行加密，以得到加密后的随机数E(r)，并将该加密后的随机数E(r)发回给第二服务器；

(4)第二服务器通过安全信道将加密后的随机数E(r)发回给第一服务器；

(5)第一服务器使用安全装置编号CID对应的加密公钥Q'_{CID}对加密后的随机数E(r)进行解密，以得到解密结果r′，并判断r′是否和随机数r相等，如果是则进入步骤(6)，否则过程结束；

(6)第一服务器通过安全信道将密钥key_1发送至第二服务器和安全装置；

(7)安全装置从摄像头获取视频码流并将其存储在第一缓存区中，对该视频码流进行解析，以获取I帧数据，并将I帧数据存储在第二缓存区中；

(8)安全装置对获取的I帧数据进行摘要签名，使用来自第一服务器的密钥key_1对I帧数据进行加密处理，以得到加密结果，并使用摘要签名结果与加密结果替换第一缓冲区中的NAL单元；

(9)安全装置将第一缓冲区中的视频码流通过有线或者无线传输至第二局域网内的第二服务器上。

2.根据权利要求1所述的加密方法，其特征在于，步骤(7)包括以下子步骤：

(7-1)安全装置读取视频码流至第一缓存区，该视频码流包括多个NAL单元；

(7-2)安全装置设置计数器i＝1；

(7-3)安全装置判断i是否大于第一缓存区中视频码流中NAL单元的总数N，如果是则过程结束，否则转入步骤(7-4)；

(7-4)安全装置读取视频码流中的第i个NAL单元，并判断其是否是I帧，如果是则转入步骤(7-5)，否则转入步骤(7-6)；

(7-5)安全装置将该第i个NAL单元放入第二缓存区中；

(7-6)安全装置设置计数器i＝i+1，并返回步骤(7-3)。

3.根据权利要求2所述的加密方法，其特征在于，步骤(8)包括以下子步骤：

(8-1)安全装置对第二缓存区中NAL单元的RBSP数据使用SM3算法进行散列运算，以得到摘要，使用安全装置编号CID对应的签名私钥S'_{CID}对该摘要进行签名以得到签名值，并将签名值和安全装置编号CID构造成类型为SEI的NAL单元；

(8-2)安全装置将步骤(8-1)中构造的NAL单元插入第二缓冲区中的NAL单元前，以形成

更新后的第二缓冲区；

(8-3)安全装置同时将更新后的第二缓冲区中类型为I帧的NAL单元的RBSP数据按字节为单位进行编号，所有奇数号的RBSP数据组成奇队列，所有偶数号的RBSP数据组成偶队列；

(8-4)安全装置通过SM4加密算法、并使用来自第一服务器的密钥key_1对奇队列进行加密，以得到加密后的奇队列密文，将加密后的奇队列密文与偶队列进行异或运算，以得到偶队列密文；

(8-5)安全装置使用步骤(8-4)得到的奇队列密文和偶队列密文按编号进行重新组合，并使用重新组合的结果替换第二缓冲区中类型为I帧的NAL单元的RBSP数据；

(8-6)安全装置将更新后的第二缓冲区中类型为SEI的NAL单元和类型为I帧的NAL单元进行连接，并使用连接后的结果替换第一缓冲区中对应的NAL单元。

4.根据权利要求2所述的加密方法，其特征在于，进一步包括以下步骤：

(10)第二服务器根据混沌序列方程迭代生成两个混沌序列X、Y，并将其存入第一缓冲区中；

(11)第二服务器循环读取安全装置发来的视频码流，对该视频码流进行置乱加密处理，以得到置乱加密后的视频码流，并将该置乱加密后的视频码流存入第二缓冲区中；

(12)第二服务器循环读取第二缓冲区中置乱加密后的视频码流，对该视频码流进行扩散加密，以得到扩散加密后的视频码流；

(13)第二服务器将步骤(3)得到的扩散加密后的视频码流发送到第一局域网的第一服务器。

5.根据权利要求4所述的加密方法，其特征在于，步骤(11)包括以下子步骤：

(11-1)第二服务器设置计数器k＝1；

(11-2)第二服务器判断k是否大于视频码流中NAL单元的总数N，如果是则进入步骤(11-10)，否则转入步骤(11-3)；

(11-3)第二服务器以3个字节为单位将视频码流中的所有NAL单元分为n组，所有分组构成NAL单元序列P，其中$P=\{p_1,p_2,p_3,\ldots,p_n\}$，p表示分组；

(11-4)第二服务器从第一缓冲区中的混沌序列X中获取n个实数构成新的混沌序列Z，其中$Z=\{x_1,x_2,\ldots,x_n\}$，x表示混沌序列X中的实数；

(11-5)第二服务器将新的混沌序列Z中的实数x_α根据规则转换成整数值a_α，以得到比特置乱序列$A=\{a_1,a_2,\ldots,a_n\}$，其中$\alpha\in[1,n]$；

(11-6)第二服务器使用步骤(11-5)得到的比特置乱序列A对步骤(11-3)得到的NAL单元序列P进行比特置乱操作，以得到序列$P'=\{p'_1,p'_2,p'_3,\ldots,p'_n\}$；

(11-7)第二服务器将新的混沌序列Z中的元素按照从大到小的顺序进行排序，从而得到有序序列$X'=\{x'_1,x'_2,\ldots,x'_n\}$，并生成位置置乱序列$D=\{d_1,d_2,\ldots,d_n\}$，该位置置乱序列中的第z个元素$d_z$为有序序列X'中的第z个元素在混沌序列Z中的位置，且有$z\in[1,n]$；

(11-8)对步骤(11-6)得到的序列$P'=\{p'_1,p'_2,p'_3,\ldots,p'_n\}$按照步骤(11-7)得到的位置置乱序列$D=\{d_1,d_2,\ldots,d_n\}$进行置乱，以得到序列$P''=\{p''_1,p''_2,p''_3,\ldots,p''_n\}$，其中$p''_z=p'_{dz}$；

(11-9)第二服务器线设置计数器k＝k+1，并返回步骤(11-1)；

(11-10)第二服务器将所有经过置乱加密的NAL单元进行组合，从而得到置乱加密后的

视频码流，并将其存入第二缓冲区中。

6.根据权利要求5所述的加密方法，其特征在于，步骤(12)包括以下子步骤：

(12-1)第二服务器设置计数器f＝1；

(12-2)第二服务器判断f是否大于第二缓冲区中所有NAL单元的总数N，如果是则过程结束，否则转入步骤(12-3)；

(12-3)第二服务器以3个字节为单位将第二缓冲区中的所有NAL单元分为n组，所有分组构成NAL单元序列Q″，其中Q″＝{q''_1,q''_2,...q''_n}，q″表示分组；

(12-4)第二服务器从第一缓冲中的混沌序列Y中获取n个实数构成新的混沌序列W，其中W＝{y_1,y_2,...,y_n}，y表示混沌序列Y中的实数；

(12-5)第二服务器将新的混沌序列W中的第β个实数y_β根据规则转换成参数序列k_β，以得到参数序列K＝{k_1,k_2,...,k_n}，其中β∈[1,n]；

(12-6)第二服务器计算新的混沌序列W的均值$\overline{W}$，根据该均值并使用阈值函数生成参数控制序列Q＝{q_1,q_2,q_3,...,q_n}；

(12-7)第二服务器使用步骤(12-5)得到的参数序列K和步骤(12-6)得到的参数控制序列Q对步骤(12-3)得到的NAL单元序列Q″进行扩散操作，以得到扩散加密序列Q″′，且Q″′＝{q'''_1,q'''_2,...,q'''_n}；

(12-8)第二服务器将扩散加密序列Q″′中的所有元素进行连接，以得到扩散后的NAL单元；

(12-9)第二服务器使用扩散后的NAL单元替换第二缓冲区中对应的NAL单元；

(12-10)第二服务器设置计数器z＝z+1，并返回步骤(12-1)。

7.一种与权利要求1至6中任意一项所述实现电力监控系统视频安全传输的加密方法对应的解密方法，其特征在于，包括以下步骤：

(1)第二终端设备向第二服务器发送加密结果查看请求；

(2)第二服务器在收到加密结果查看请求后，将密钥key_1和加密结果通过安全信道发给第二终端设备；

(3)第二终端设备设置计数器j＝1，

(4)第二终端设备判断j是否大于加密结果中NAL单元的总数N，如果是则进入步骤(8)，否则转入步骤(5)；

(5)第二终端设备读取视频码流中的第j个NAL单元，并判断其是否是为SEI类型，如果是则转入步骤(6)，否则转入步骤(7)；

(6)第二终端设备将该第j个NAL单元和第j+1个NAL单元放入第三缓存区中；

(7)第二终端设备设置计数器j＝j+2，并返回步骤(3)；

(8)第二终端设备使用步骤(2)中的密钥key_1对第三缓冲区的加密数据进行验证和解密处理，以得到解密结果。

8.根据权利要求7所述的解密方法，其特征在于，步骤(8)包括以下子步骤：

(8-1)第二终端设备根据安全装置编号CID获取对应的签名公钥Q'_{CID}，并使用公钥Q'_{CID}对SEI中携带的签名值进行解密，以得到摘要值B；

(8-2)第二终端设备将NAL单元的RBSP数据按字节为单位进行编号，所有奇数号的RBSP数据组成奇队列，所有偶数号的RBSP数据组成偶队列；

(8-3)第二终端设备通过SM4解密算法、并使用密钥key_1对奇队列进行解密密,以得到解密后的奇队列明文,将解密后的奇队列明文与偶队列进行异或运算,以得到偶队列明文,并将奇队列明文和偶队列明文发送到安全装置;

(8-4)第二终端设备使用步骤(8-3)得到的奇队列密文和偶队列密文按编号进行重新组合,并使用重新组合的结果替换步骤(8-2)中NAL单元的RBSP数据,以得到I帧明文;

(8-5)第二终端设备对步骤(8-4)得到的I帧明文使用SM3算法进行散列运算,以得到摘要B′,并判断摘要B′是否和步骤(8-1)中得到的摘要B相等,如果是则进入步骤(8-6),否则过程结束;

(8-6)第二终端设备使用该I帧明文替换I帧密文,以还原视频码流,并对该视频码流进行解码,以获得最终的监控视频。

9.根据权利要求7所述的解密方法,其特征在于,当所述加密方法包括步骤(10)至(13)时,所述解密方法进一步包括以下步骤:

(9)第一服务器根据混沌序列方程迭代生成两个混沌序列X、Y,并将其存入第一缓冲区中;

(10)第一服务器循环读取第二局域网发来的视频码流,对该视频码流进行扩散解密处理,以得到扩散加密前的视频码流,并将该扩散解密后的视频码流存入第二缓冲区中;

(11)第一服务器循环读取第二缓冲区中的经过扩散解密的视频码流,进行置乱解密处理,以得到置乱加密前的视频码流;

(12)第一服务器将置乱解密后的视频码流进行保存,等待第一局域网终端设备获取视频数据。

10.根据权利要求9所述的解密方法,其特征在于,

步骤(10)包括以下子步骤:

(10-1)第一服务器设置计数器count1=1;

(10-2)第一服务器判断count1是否大于第二缓冲区中所有NAL单元的总数N,如果是则进入步骤(10-8),否则转入步骤(10-3);

(10-3)第一服务器以3个字节为单位将第二缓冲区中的所有NAL单元分为n组,所有分组构成NAL单元序列Q″′,其中$Q''' = \{q'''_1, q'''_2, \ldots, q'''_n\}$,q″′表示分组;

(10-4)第一服务器从第一缓冲区中的混沌序列Y中获取n个实数构成新的混沌序列W,其中$W = \{y_1, y_2, \ldots, y_n\}$,y表示混沌序列Y中的实数;

(10-5)第一服务器将新的混沌序列W中的实数y_i根据规则转换成参数序列k_i,以得到参数序列$K = \{k_1, k_2, \ldots, k_n\}$;

(10-6)第一服务器计算新的混沌序列W的均值$\overline{W}$,根据该均值并使用阈值函数生成参数控制序列$Q = \{q_1, q_2, q_3, \ldots, q_n\}$;

(10-7)第一服务器使用步骤(10-5)得到的参数序列K和步骤(10-6)得到的参数控制序列Q对步骤(10-3)得到的NAL单元序列P″′进行扩散解密操作,以得到扩散解密序列P″;

(10-8)第一服务器将所有经过置乱加密的NAL单元进行组合,从而得到置乱加密后的视频码流,并将其存入第二缓冲区中;

步骤(11)包括以下子步骤:

(11-1)第一服务器设置计数器count3=1;

(11-2)第一服务器判断count3是否大于视频码流中NAL单元的总数N,如果是则进入步骤(11-10),否则转入步骤(11-3);

(11-3)第一务器以3个字节为单位将视频码流中的所有NAL单元分为n组,从而得到NAL单元序列P″,其中P″＝{p''_1,p''_2,p''_3,...,p''_n},P″表示分组;

(11-4)第一服务器从第一缓冲区中的混沌序列X中获取n个实数构成新的混沌序列Z,其中Z＝{x_1,x_2,...,x_n},x表示混沌序列X中的实数;

(11-5)第一服务器将新的混沌序列Z中的实数x_1根据规则转换成整数值a_1,以得到比特置乱序列A＝{a_1,a_2,...,a_n};

(11-6)第一服务器将新的混沌序列Z中的元素按照从大到小的顺序进行排序,从而得到有序序列X′＝{x'_1,x'_2,...,x'_n},并生成位置置乱序列D＝{d_1,d_2,...,d_n},该位置置乱序列中的第z个元素d_z为有序序列Z中的第z个元素在混沌序列X′中的位置,且有z∈[1,n];

(11-7)对步骤(11-3)得到的序列P″＝{p''_1,p''_2,p''_3,...,p''_n}按照步骤(11-6)得到的位置置乱序列D＝{d_1,d_2,...,d_n}进行位置置乱解密,以得到序列P′＝{p'_1,p'_2,p'_3,...,p'_n},其中p'_z＝p''_{dz};

(11-8)第一服务器使用步骤(11-5)得到的比特置乱序列A对步骤(11-7)得到的NAL单元序列P′进行比特置乱解密操作,以得到序列P＝{p_1,p_2,p_3,...,p_n}。

一种实现电力监控系统视频安全传输的加密和解密方法

技术领域

[0001] 本发明属于视频监控技术领域，更具体地，涉及一种实现电力监控系统视频安全传输的加密和解密方法。

背景技术

[0002] 随着对电力系统安防要求的不断提升，相应地对视频监控系统的需求量也越来越大，这些视频监控系统对发电厂、变电站等关键场所的实时运行情况进行监视和记录，维护了电力系统的稳定运行。

[0003] 视频监控系统的应用包括以下几个层次，第一层次是现场视频监控，其主要由前端摄像机、视频刻录器、视频显示器等组成，用于实现现场监控和监控视频存储等；第二层次是远程视频监控，由监控前端、控制台以及传输网络组成，用于支持适应无人值班的变电站、地市级监控中心等远程监控体系；第三层次是融入应急指挥系统，其实现各级监控视频与相应的应急指挥中心互联，以供应急指挥中心直接调用现场视频的图像。

[0004] 然而，现有视频监控系统本身却存在一定的安全性缺陷：一方面，高清摄像头等视频采集设备难以管理，这些设备容易被非法接入或替换，同时存在弱口令等问题；另一方面，监控中心在对下级电厂或变电站进行远程监控的过程中，传输的视频数据通常是采用明文传输，其容易被窃取、篡改甚至替换，使得上级不能得到安全可靠的监控视频数据，从而使得电网安全受到威胁；第三方面，黑客还会利用视频监控系统的安全隐患，注入恶意代码，并以监控系统的后端作为跳板攻击内网内的其他系统，从而带来更大的安全威胁。

发明内容

[0005] 针对现有技术的以上缺陷或改进需求，本发明提供了一种实现电力监控系统视频安全传输的加密和解密方法，其目的在于，能够针对视频监控系统的特征和安全威胁设计安全防护机制，从而确保视频监控系统的安全性和可靠性。

[0006] 为实现上述目的，按照本发明的一个方面，提供了一种实现电力监控系统视频安全传输的加密方法，是应用在包括通过网络彼此通信连接的第一局域网和第二局域网的电力监控系统中，其中第一局域网包括多个第一终端设备以及与其通信连接的第一服务器，所述第二局域网包括多个第二终端设备、多个安全装置、以及第二服务器，第二终端设备通过第二服务器与安全装置通信连接，所述加密方法包括以下步骤：

[0007] (1)第一服务器在和第二服务器建立安全连接后，并通过安全信道向第二服务器发送视频调用请求，该视频调用请求中包括该安全装置编号CID和随机产生的随机数r；

[0008] (2)第二服务器使用视频调用请求中安全装置编号CID对应的公钥Q_{CID}，并基于IBC方法对视频调用请求进行处理，以得到密文，并将该密文发给安全装置编号CID对应的安全装置；

[0009] (3)安全装置使用安全装置编号CID对应的加密私钥S_{CID}对密文进行解密，以得到视频调用请求，并使用安全装置编号CID对应的签名私钥S'_{CID}对视频调用请求中的随机数r

进行加密，以得到加密后的随机数E(r)，并将该加密后的随机数E(r)发回给第二服务器；

[0010] (4)第二服务器通过安全信道将加密后的随机数E(r)发回给第一服务器；

[0011] (5)第一服务器使用安全装置编号CID对应的加密公钥Q'_{CID}对加密后的随机数E(r)进行解密，以得到解密结果r′，并判断r′是否和随机数r相等，如果是则进入步骤(6)，否则过程结束；

[0012] (6)第一服务器通过安全信道将密钥key_1发送至第二服务器和安全装置；

[0013] (7)安全装置从摄像头获取视频码流并将其存储在第一缓存区中，对该视频码流进行解析，以获取I帧数据，并将I帧数据存储在第二缓存区中；

[0014] (8)安全装置对获取的I帧数据进行摘要签名，使用来自第一服务器的密钥key_1对I帧数据进行加密处理，以得到加密结果，并使用摘要签名结果与加密结果替换第一缓冲区中的NAL单元；

[0015] (9)安全装置将第一缓冲区中的视频码流通过有线或者无线传输至第二局域网内的第二服务器上。

[0016] 优选地，步骤(7)包括以下子步骤：

[0017] (7-1)安全装置读取视频码流至第一缓存区，该视频码流包括多个NAL单元；

[0018] (7-2)安全装置设置计数器i＝1；

[0019] (7-3)安全装置判断i是否大于第一缓存区中视频码流中NAL单元的总数N，如果是则过程结束，否则转入步骤(7-4)；

[0020] (7-4)安全装置读取视频码流中的第i个NAL单元，并判断其是否是I帧，如果是则转入步骤(7-5)，否则转入步骤(7-6)；

[0021] (7-5)安全装置将该第i个NAL单元放入第二缓存区中；

[0022] (7-6)安全装置设置计数器i＝i+1，并返回步骤(7-3)。

[0023] 优选地，步骤(8)包括以下子步骤：

[0024] (8-1)安全装置对第二缓存区中NAL单元的RBSP数据使用SM3算法进行散列运算，以得到摘要，使用安全装置编号CID对应的签名私钥S'_{CID}对该摘要进行签名以得到签名值，并将签名值和安全装置编号CID构造成类型为SEI的NAL单元；

[0025] (8-2)安全装置将步骤(8-1)中构造的NAL单元插入第二缓冲区中的NAL单元前，以形成更新后的第二缓冲区；

[0026] (8-3)安全装置同时将更新后的第二缓冲区中类型为I帧的NAL单元的RBSP数据按字节为单位进行编号，所有奇数号的RBSP数据组成奇队列，所有偶数号的RBSP数据组成偶队列；

[0027] (8-4)安全装置通过SM4加密算法、并使用来自第一服务器的密钥key_1对奇队列进行加密，以得到加密后的奇队列密文，将加密后的奇队列密文与偶队列进行异或运算，以得到偶队列密文；

[0028] (8-5)安全装置使用步骤(8-4)得到的奇队列密文和偶队列密文按编号进行重新组合，并使用重新组合的结果替换第二缓冲区中类型为I帧的NAL单元的RBSP数据；

[0029] (8-6)安全装置将更新后的第二缓冲区中类型为SEI的NAL单元和类型为I帧的NAL单元进行连接，并使用连接后的结果替换第一缓冲区中对应的NAL单元。

[0030] 优选地，进一步包括以下步骤：

[0031] (10)第二服务器根据混沌序列方程迭代生成两个混沌序列X、Y,并将其存入第一缓冲区中;

[0032] (11)第二服务器循环读取安全装置发来的视频码流,对该视频码流进行置乱加密处理,以得到置乱加密后的视频码流,并将该置乱加密后的视频码流存入第二缓冲区中;

[0033] (12)第二服务器循环读取第二缓冲区中置乱加密后的视频码流,对该视频码流进行扩散加密,以得到扩散加密后的视频码流。

[0034] (13)第二服务器将步骤(3)得到的扩散加密后的视频码流发送到第一局域网的第一服务器。

[0035] 优选地,步骤(11)包括以下子步骤:

[0036] (11-1)第二服务器设置计数器k=1;

[0037] (11-2)第二服务器判断k是否大于视频码流中NAL单元的总数N,如果是则进入步骤(11-10),否则转入步骤(11-3);

[0038] (11-3)第二服务器以3个字节为单位将视频码流中的所有NAL单元分为n组,所有分组构成NAL单元序列P,其中P=$\{p_1,p_2,p_3,\ldots,p_n\}$,p表示分组;

[0039] (11-4)第二服务器从第一缓冲区中的混沌序列X中获取n个实数构成新的混沌序列Z,其中Z=$\{x_1,x_2,\ldots,x_n\}$,x表示混沌序列X中的实数;

[0040] (11-5)第二服务器将新的混沌序列Z中的实数x_α根据规则转换成整数值a_α,以得到比特置乱序列A=$\{a_1,a_2,\ldots,a_n\}$,其中α∈[1,n];

[0041] (11-6)第二服务器使用步骤(11-5)得到的比特置乱序列A对步骤(11-3)得到的NAL单元序列P进行比特置乱操作,以得到序列P′=$\{p'_1,p'_2,p'_3,\ldots,p'_n\}$。

[0042] (11-7)第二服务器将新的混沌序列Z中的元素按照从大到小的顺序进行排序,从而得到有序序列X′=$\{x'_1,x'_2,\ldots,x'_n\}$,并生成位置置乱序列D=$\{d_1,d_2,\ldots,d_n\}$,该位置置乱序列中的第z个元素$d_z$为有序序列X′中的第z个元素在混沌序列Z中的位置,且有z∈[1,n];

[0043] (11-8)对步骤(11-6)得到的序列P′=$\{p'_1,p'_2,p'_3,\ldots,p'_n\}$按照步骤(11-7)得到的位置置乱序列D=$\{d_1,d_2,\ldots,d_n\}$进行置乱,以得到序列P″=$\{p''_1,p''_2,p''_3,\ldots,p''_n\}$,其中$p''_z=p'_{dz}$;。

[0044] (11-9)第二服务器线设置计数器k=k+1,并返回步骤(11-1);

[0045] (11-10)第二服务器将所有经过置乱加密的NAL单元进行组合,从而得到置乱加密后的视频码流,并将其存入第二缓冲区中。

[0046] 优选地,步骤(12)包括以下子步骤:

[0047] (12-1)第二服务器设置计数器f=1;

[0048] (12-2)第二服务器判断f是否大于第二缓冲区中所有NAL单元的总数N,如果是则过程结束,否则转入步骤(12-3);

[0049] (12-3)第二服务器以3个字节为单位将第二缓冲区中的所有NAL单元分为n组,所有分组构成NAL单元序列Q",其中Q"=$\{q''_1,q''_2,\ldots q''_n\}$,q″表示分组;

[0050] (12-4)第二服务器从第一缓冲中的混沌序列Y中获取n个实数构成新的混沌序列W,其中W=$\{y_1,y_2,\ldots,y_n\}$,y表示混沌序列Y中的实数;

[0051] (12-5)第二服务器将新的混沌序列W中的第β个实数y_β根据规则转换成参数序列

k_β,以得到参数序列K＝{k_1,k_2,...,k_n},其中β∈[1,n];

[0052] (12-6)第二服务器计算新的混沌序列W的均值W,根据该均值并使用阈值函数生成参数控制序列Q＝{q_1,q_2,q_3,...,q_n}。

[0053] (12-7)第二服务器使用步骤(12-5)得到的参数序列K和步骤(12-6)得到的参数控制序列Q对步骤(12-3)得到的NAL单元序列Q”进行扩散操作,以得到扩散加密序列Q”',且Q″′＝{q''_1,q''_2,...,q''_n};

[0054] (12-8)第二服务器将扩散加密序列Q”'中的所有元素进行连接,以得到扩散后的NAL单元;

[0055] (12-9)第二服务器使用扩散后的NAL单元替换第二缓冲区中对应的NAL单元。

[0056] (12-10)第二服务器设置计数器z＝z+1,并返回步骤(12-1)。

[0057] 按照本发明的另一方面,提供了一种与所述实现电力监控系统视频安全传输的加密方法对应的解密方法,包括以下步骤:

[0058] (1)第二终端设备向第二服务器发送加密结果查看请求;

[0059] (2)第二服务器在收到加密结果查看请求后,将密钥key_1和加密结果通过安全信道发给第二终端设备;

[0060] (3)第二终端设备设置计数器j＝1,

[0061] (4)第二终端设备判断j是否大于加密结果中NAL单元的总数N,如果是则进入步骤(8),否则转入步骤(5);

[0062] (5)第二终端设备读取视频码流中的第j个NAL单元,并判断其是否是为SEI类型,如果是则转入步骤(6),否则转入步骤(7);

[0063] (6)第二终端设备将该第j个NAL单元和第j+1个NAL单元放入第三缓存区中;

[0064] (7)第二终端设备设置计数器j＝j+2,并返回步骤(3);

[0065] (8)第二终端设备使用步骤(2)中的密钥key_1对第三缓冲区的加密数据进行验证和解密处理,以得到解密结果。

[0066] 优选地,步骤(8)包括以下子步骤:

[0067] (8-1)第二终端设备根据安全装置编号CID获取对应的签名公钥Q'_{CID},并使用公钥Q'_{CID}对SEI中携带的签名值进行解密,以得到摘要值B;

[0068] (8-2)第二终端设备将NAL单元的RBSP数据按字节为单位进行编号,所有奇数号的RBSP数据组成奇队列,所有偶数号的RBSP数据组成偶队列;

[0069] (8-3)第二终端设备通过SM4解密算法、并使用密钥key_1对奇队列进行解密密,以得到解密后的奇队列明文,将解密后的奇队列明文与偶队列进行异或运算,以得到偶队列明文,并将奇队列明文和偶队列明文发送到安全装置;

[0070] (8-4)第二终端设备使用步骤(8-3)得到的奇队列密文和偶队列密文按编号进行重新组合,并使用重新组合的结果替换步骤(8-2)中NAL单元的RBSP数据,以得到I帧明文;

[0071] (8-5)第二终端设备对步骤(8-4)得到的I帧明文使用SM3算法进行散列运算,以得到摘要B′,并判断摘要B′是否和步骤(8-1)中得到的摘要B相等,如果是则进入步骤(8-6),否则过程结束;

[0072] (8-6)第二终端设备使用该I帧明文替换I帧密文,以还原视频码流,并对该视频码流进行解码,以获得最终的监控视频。

[0073] 优选地，当所述加密方法包括步骤(10)至(13)时，所述解密方法进一步包括以下步骤：

[0074] (9)第一服务器根据混沌序列方程迭代生成两个混沌序列X、Y，并将其存入第一缓冲区中。

[0075] (10)第一服务器循环读取第二局域网发来的视频码流，对该视频码流进行扩散解密处理，以得到扩散加密前的视频码流，并将该扩散解密后的视频码流存入第二缓冲区中；

[0076] (11)第一服务器循环读取第二缓冲区中的经过扩散解密的视频码流，进行置乱解密处理，以得到置乱加密前的视频码流。

[0077] (12)第一服务器将置乱解密后的视频码流进行保存，等待第一局域网终端设备获取视频数据。

[0078] 优选地，步骤(10)包括以下子步骤：

[0079] (10-1)第一服务器设置计数器count1＝1；

[0080] (10-2)第一服务器判断count1是否大于第二缓冲区中所有NAL单元的总数N，如果是则进入步骤(10-8)，否则转入步骤(10-3)；

[0081] (10-3)第一服务器以3个字节为单位将第二缓冲区中的所有NAL单元分为n组，所有分组构成NAL单元序列Q″′，其中$Q''' = \{q'''_1, q'''_2, \ldots, q'''_n\}$，q″′表示分组；

[0082] (10-4)第一服务器从第一缓冲区中的混沌序列Y中获取n个实数构成新的混沌序列W，其中$W = \{y_1, y_2, \ldots, y_n\}$，y表示混沌序列Y中的实数；

[0083] (10-5)第一服务器将新的混沌序列W中的实数y_i根据规则转换成参数序列k_i，以得到参数序列$K = \{k_1, k_2, \ldots, k_n\}$。

[0084] (10-6)第一服务器计算新的混沌序列W的均值$\overline{W}$，根据该均值并使用阈值函数生成参数控制序列$Q = \{q_1, q_2, q_3, \ldots, q_n\}$。

[0085] (10-7)第一服务器使用步骤(10-5)得到的参数序列K和步骤(10-6)得到的参数控制序列Q对步骤(10-3)得到的NAL单元序列P″′进行扩散解密操作，以得到扩散解密序列P″；

[0086] (10-8)第一服务器将所有经过置乱加密的NAL单元进行组合，从而得到置乱加密后的视频码流，并将其存入第二缓冲区中；

[0087] 步骤(11)包括以下子步骤：

[0088] (11-1)第一服务器设置计数器count3＝1；

[0089] (11-2)第一服务器判断count3是否大于视频码流中NAL单元的总数N，如果是则进入步骤(11-10)，否则转入步骤(11-3)；

[0090] (11-3)第一务器以3个字节为单位将视频码流中的所有NAL单元分为n组，从而得到NAL单元序列P″，其中$P'' = \{p''_1, p''_2, p''_3, \ldots, p''_n\}$，P″表示分组；

[0091] (11-4)第一服务器从第一缓冲区中的混沌序列X中获取n个实数构成新的混沌序列Z，其中$Z = \{x_1, x_2, \ldots, x_n\}$，x表示混沌序列X中的实数；

[0092] (11-5)第一服务器将新的混沌序列Z中的实数x_i根据规则转换成整数值a_i，以得到比特置乱序列$A = \{a_1, a_2, \ldots, a_n\}$。具体的，所述转换规则为：

[0093] 取新的混沌序列Z中实数值x_i的小数点后8位构成$L_i = 0.l_0l_1l_2l_3l_4l_5l_6l_7$，计算$a_i = \left(\left(\overline{L_i} \times 10^8\right) \bmod 23 + 1\right)$，以使得$1 \leqslant a_i \leqslant 23$。

[0094] (11-6)第一服务器将新的混沌序列Z中的元素按照从大到小的顺序进行排序，从而得到有序序列$X'=\{x'_1,x'_2,...,x'_n\}$，并生成位置置乱序列$D=\{d_1,d_2,...,d_n\}$，该位置置乱序列中的第z个元素$d_z$为有序序列Z中的第z个元素在混沌序列X′中的位置，且有$z\in[1,n]$；

[0095] (11-7)对步骤(11-3)得到的序列$P''=\{p''_1,p''_2,p''_3,...,p''_n\}$按照步骤(11-6)得到的位置置乱序列$D=\{d_1,d_2,...,d_n\}$进行位置置乱解密，以得到序列$P'=\{p'_1,p'_2,p'_3,...,p'_n\}$，其中$p_z'=p''_{dz}$。

[0096] (11-8)第一服务器使用步骤(11-5)得到的比特置乱序列A对步骤(11-7)得到的NAL单元序列P′进行比特置乱解密操作，以得到序列$P=\{p_1,p_2,p_3,...,p_n\}$。

[0097] 总体而言，通过本发明所构思的以上技术方案与现有技术相比，能够取得下列有益效果：

[0098] 1、本发明通过设置安全装置，使得第一局域网在调用监控视频时首先需要完成双向安全认证，从而能够防止摄像头被替换，或者恶意用户访问摄像头，进而有效防止了窃取视频或篡改视频的发生。

[0099] 2、本发明对于第一局域网和厂站之间的远距离视频数据传输，使用了混沌序列生成密钥、对视频数据进行两次置乱和两次扩散的加密方案，对视频数据进行了重加密，为视频数据在长距离远程传输过程中的安全性提供了保障。

[0100] 3、本发明对于局域网内的视频传输，使用仅加密I帧数据的加密方案，在提供视频数据加密传输的同时，保证了现场监控的实时性要求。

附图说明

[0101] 图1是本发明所应用到的电力监控系统的示意图。

[0102] 图2是本发明实现电力监控系统视频安全传输的加密方法的流程图。

[0103] 图3是本发明实现电力监控系统视频安全传输的解密方法的流程图。

具体实施方式

[0104] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。此外，下面所描述的本发明各个实施方式中所涉及到的技术特征只要彼此之间未构成冲突就可以相互组合。

[0105] 图1是本发明所应用的电力监控系统的示意图，该电力监控系统包括通过网络彼此通信连接的第一局域网和第二局域网，其中第一局域网包括多个第一终端设备以及与其通信连接的第一服务器，所述第二局域网包括多个第二终端设备、多个安全装置、以及第二服务器，第二终端设备通过第二服务器与安全装置通信连接

[0106] 第一局域网远程查看下级厂站的监控视频时，首先需要与摄像头进行双向安全认证，双向认证由安全装置和两级服务器共同完成。安全装置由第一局域网统一发放并部署在下级厂站的监控设备后端，每一个安全装置都拥有唯一的身份标识CID、加密私钥S_{CID}和签名私钥S'_{CID}，上级厂站记录安全装置所连接的摄像设备的编号以及部署位置。第一局域网的密钥服务器生成系统主密钥MSK和系统公钥PK，对外公开PK，秘密保存MSK，并根据CID

秘密生成安全装置的加密私钥S_{CID}和签名私钥S'_{CID}，置入安全装置CID中，加密公钥Q_{CID}和签名公钥Q'_{CID}可由公开的公钥计算函数得到，则安全装置拥有两个公私钥对$\{Q_{CID},S_{CID}\}$和$\{Q'_{CID},S'_{CID}\}$。

[0107] 如图2所示，本发明提供了一种实现电力监控系统视频安全传输的加密方法，是应用在包括通过网络彼此通信连接的第一局域网和第二局域网的电力监控系统中，其中第一局域网包括多个第一终端设备以及与其通信连接的第一服务器，所述第二局域网包括多个第二终端设备、多个安全装置、以及第二服务器，第二终端设备通过第二服务器与安全装置通信连接，所述加密方法包括以下步骤：

[0108] (1)第一服务器在和第二服务器建立安全连接后，并通过安全信道向第二服务器发送视频调用请求，该视频调用请求中包括该安全装置编号CID和随机产生的随机数r；

[0109] (2)第二服务器使用视频调用请求中安全装置编号CID对应的公钥Q_{CID}，并基于标识的密码技术(Identify-based cryptography，简称IBC)方法对视频调用请求进行处理，以得到密文，并将该密文发给安全装置编号CID对应的安全装置；

[0110] (3)安全装置使用安全装置编号CID对应的加密私钥S_{CID}对密文进行解密，以得到视频调用请求，并使用安全装置编号CID对应的签名私钥S'_{CID}对视频调用请求中的随机数r进行加密，以得到加密后的随机数E(r)，并将该加密后的随机数E(r)发回给第二服务器；

[0111] (4)第二服务器通过安全信道将加密后的随机数E(r)发回给第一服务器；

[0112] (5)第一服务器使用安全装置编号CID对应的加密公钥Q'_{CID}对加密后的随机数E(r)进行解密，以得到解密结果r′，并判断r′是否和随机数r相等，如果是则进入步骤(6)，否则过程结束；

[0113] 通过本步骤的验证过程，完成了安全装置与第一局域网之间的双向认证，并且建立起了第一局域网-第二局域网、第二局域网-安全装置的两条安全信道。

[0114] (6)第一服务器通过安全信道将密钥key_1发送至第二服务器和安全装置；

[0115] (7)安全装置从摄像头获取视频码流并将其存储在第一缓存区中，对该视频码流进行解析，以获取I帧数据，并将I帧数据存储在第二缓存区中；

[0116] 在本步骤中，获取的视频码流是H.264或者H.265。

[0117] 具体而言，视频码流一般分为I、P、B三种帧，I帧是全帧压缩编码帧，描述了图像背景和运动主体的详情，P、B帧的编码通过I帧进行，我们通过对I帧数据加密以实现监控视频的加密。

[0118] 本步骤包括以下子步骤：

[0119] (7-1)安全装置读取视频码流至第一缓存区，该视频码流包括多个网络提取层(Network abstract layer，简称NAL)单元，每个NAL单元均通过其起始标识符0x000001或0x00000001定位；

[0120] (7-2)安全装置设置计数器i＝1；

[0121] (7-3)安全装置判断i是否大于第一缓存区中视频码流中NAL单元的总数N，如果是则过程结束，否则转入步骤(7-4)；

[0122] (7-4)安全装置读取视频码流中的第i个NAL单元，并判断其是否是I帧，如果是则转入步骤(7-5)，否则转入步骤(7-6)；

[0123] (7-5)安全装置将该第i个NAL单元放入第二缓存区中；

[0124] (7-6)安全装置设置计数器i＝i+1,并返回步骤(7-3)；

[0125] (8)安全装置对获取的I帧数据进行摘要签名,使用来自第一服务器的密钥key_1对I帧数据进行加密处理,以得到加密结果,并使用摘要签名结果与加密结果替换第一缓冲区中的NAL单元；

[0126] 本步骤包括以下子步骤：

[0127] (8-1)安全装置对第二缓存区中NAL单元的原始字节序列负荷(Raw byte sequence payload,简称RBSP)数据使用SM3算法进行散列运算,以得到摘要,使用安全装置编号CID对应的签名私钥S'_{CID}对该摘要进行签名以得到签名值,并将签名值和安全装置编号CID构造成类型为补充增强信息(Supplemental Enhancement Information,简称SEI)的NAL单元；

[0128] (8-2)安全装置将步骤(8-1)中构造的NAL单元插入第二缓冲区中的NAL单元前,以形成更新后的第二缓冲区；

[0129] (8-3)安全装置同时将更新后的第二缓冲区中类型为I帧的NAL单元的RBSP数据按字节为单位进行编号,所有奇数号的RBSP数据组成奇队列,所有偶数号的RBSP数据组成偶队列；

[0130] (8-4)安全装置通过SM4加密算法、并使用来自第一服务器的密钥key_1对奇队列进行加密,以得到加密后的奇队列密文,将加密后的奇队列密文与偶队列进行异或运算,以得到偶队列密文；

[0131] (8-5)安全装置使用步骤(8-4)得到的奇队列密文和偶队列密文按编号进行重新组合,并使用重新组合的结果替换第二缓冲区中类型为I帧的NAL单元的RBSP数据；

[0132] (8-6)安全装置将更新后的第二缓冲区中类型为SEI的NAL单元和类型为I帧的NAL单元进行连接,并使用连接后的结果替换第一缓冲区中对应的NAL单元。

[0133] (9)安全装置将第一缓冲区中的视频码流通过有线或者无线传输至第二局域网内的第二服务器上。

[0134] 如图3所示,本发明提供了与上述实现电力监控系统视频安全传输的加密方法在同一局域网内的解密方法,包括以下步骤：

[0135] (1)第二终端设备向第二服务器发送加密结果查看请求；

[0136] (2)第二服务器在收到加密结果查看请求后,将密钥key_1和加密结果通过安全信道发给第二终端设备；

[0137] (3)第二终端设备设置计数器j＝1,

[0138] (4)第二终端设备判断j是否大于加密结果中NAL单元的总数N,如果是则进入步骤(8),否则转入步骤(5)；

[0139] (5)第二终端设备读取视频码流中的第j个NAL单元,并判断其是否是为SEI类型,如果是则转入步骤(6),否则转入步骤(7)；

[0140] (6)第二终端设备将该第j个NAL单元和第j+1个NAL单元放入第三缓存区中；

[0141] (7)第二终端设备设置计数器j＝j+2,并返回步骤(3)；

[0142] (8)第二终端设备使用步骤(2)中的密钥key_1对第三缓冲区的加密数据进行验证和解密处理,以得到解密结果。

[0143] 本步骤包括以下子步骤：

[0144] (8-1)第二终端设备根据安全装置编号CID获取对应的签名公钥Q'_{CID},并使用公钥Q'_{CID}对SEI中携带的签名值进行解密,以得到摘要值B;

[0145] (8-2)第二终端设备将NAL单元的RBSP数据按字节为单位进行编号,所有奇数号的RBSP数据组成奇队列,所有偶数号的RBSP数据组成偶队列;

[0146] (8-3)第二终端设备通过SM4解密算法、并使用密钥key_1对奇队列进行解密密,以得到解密后的奇队列明文,将解密后的奇队列明文与偶队列进行异或运算,以得到偶队列明文,并将奇队列明文和偶队列明文发送到安全装置;

[0147] (8-4)第二终端设备使用步骤(8-3)得到的奇队列密文和偶队列密文按编号进行重新组合,并使用重新组合的结果替换步骤(8-2)中NAL单元的RBSP数据,以得到I帧明文;

[0148] (8-5)第二终端设备对步骤(8-4)得到的I帧明文使用SM3算法进行散列运算,以得到摘要B',并判断摘要B'是否和步骤(8-1)中得到的摘要B相等,如果是则进入步骤(8-6),否则过程结束;

[0149] (8-6)第二终端设备使用该I帧明文替换I帧密文,以还原视频码流,并对该视频码流进行解码,以获得最终的监控视频。

[0150] 虽然安全装置对码流中的I帧数据进行了加密,在保证实时性的前提下保证了视频数据的安全性与完整性,但是由于P帧和B帧中会有帧内预测的宏块,仍存在安全隐患,所以对于发给远程的第一局域网的视频,第二服务器对H.264码流进行了视频重加密,确保在复杂的网络环境内视频数据的安全传输。

[0151] 作为进一步优选地,上述加密方法可进一步包括以下步骤(应该说明的是,以下步骤实现的是二次加密过程):

[0152] (1)第二服务器根据混沌序列方程迭代生成两个混沌序列X、Y,并将其存入第一缓冲区中。

[0153] (2)第二服务器循环读取安全装置发来的视频码流,对该视频码流进行置乱加密处理,以得到置乱加密后的视频码流,并将该置乱加密后的视频码流存入第二缓冲区中;

[0154] 本步骤包括以下子步骤:

[0155] (2-1)第二服务器设置计数器k=1;

[0156] (2-2)第二服务器判断k是否大于视频码流中NAL单元的总数N,如果是则进入步骤(2-10),否则转入步骤(2-3);

[0157] (2-3)第二服务器以3个字节为单位将视频码流中的所有NAL单元分为n组,所有分组构成NAL单元序列P,其中$P=\{p_1,p_2,p_3,\ldots,p_n\}$,p表示分组;

[0158] (2-4)第二服务器从第一缓冲区中的混沌序列X中获取n个实数构成新的混沌序列Z,其中$Z=\{x_1,x_2,\ldots,x_n\}$,x表示混沌序列X中的实数;

[0159] (2-5)第二服务器将新的混沌序列Z中的实数x_α根据规则转换成整数值a_α,以得到比特置乱序列$A=\{a_1,a_2,\ldots,a_n\}$,其中$\alpha\in[1,n]$。具体的,所述转换规则为:

[0160] 取新的混沌序列Z中实数值x_α的小数点后8位构成$L_\alpha=0.l_0l_1l_2l_3l_4l_5l_6l_7$,计算$a_\alpha=\left(\left(\overline{L}_\alpha\times10^8\right)\bmod 23+1\right)$,以使得$1\leqslant a_\alpha\leqslant23$。

[0161] (2-6)第二服务器使用步骤(2-5)得到的比特置乱序列A对步骤(2-3)得到的NAL单元序列P进行比特置乱操作,以得到序列$P'=\{p'_1,p'_2,p'_3,\ldots,p'_n\}$。

[0162] 本步骤包括以下子步骤：

[0163] (2-6-1)第二服务器设置计数器h＝1；

[0164] (2-6-2)第二服务器判断h是否大于NAL单元序列P的长度n，如果是则过程结束，否则转入步骤(2-6-3)；

[0165] (2-6-3)第二服务器获取NAL单元序列P中的第h个分组p_h以及比特置乱序列A中的第h个元素a_h，将p_h左移a_h位进行比特位置置乱，从而得到新的分组p'_h；

[0166] (2-6-4)第二服务器设置计数器h＝h+1，并返回步骤(2-6-1)；

[0167] (2-7)第二服务器将新的混沌序列Z中的元素按照从大到小的顺序进行排序，从而得到有序序列$X'=\{x'_1,x'_2,...,x'_n\}$，并生成位置置乱序列$D=\{d_1,d_2,...,d_n\}$，该位置置乱序列中的第z个元素$d_z$为有序序列X'中的第z个元素在混沌序列Z中的位置，且有$z\in[1,n]$；

[0168] (2-8)对步骤(2-6)得到的序列$P'=\{p'_1,p'_2,p'_3,...,p'_n\}$按照步骤(2-7)得到的位置置乱序列$D=\{d_1,d_2,...,d_n\}$进行置乱，以得到序列$P''=\{p''_1,p''_2,p''_3,...,p''_n\}$，其中$p''_z=p'_{dz}$；。

[0169] (2-9)第二服务器线设置计数器k＝k+1，并返回步骤(2-1)；

[0170] (2-10)第二服务器将所有经过置乱加密的NAL单元进行组合，从而得到置乱加密后的视频码流，并将其存入第二缓冲区中；

[0171] (3)第二服务器循环读取第二缓冲区中置乱加密后的视频码流，对该视频码流进行扩散加密，以得到扩散加密后的视频码流。

[0172] 本步骤包括以下子步骤：

[0173] (3-1)第二服务器设置计数器f＝1；

[0174] (3-2)第二服务器判断f是否大于第二缓冲区中所有NAL单元的总数N，如果是则过程结束，否则转入步骤(3-3)；

[0175] (3-3)第二服务器以3个字节为单位将第二缓冲区中的所有NAL单元分为n组，所有分组构成NAL单元序列Q”，其中$Q''=\{q''_1,q''_2,...q''_n\}$，q″表示分组；

[0176] (3-4)第二服务器从第一缓冲中的混沌序列Y中获取n个实数构成新的混沌序列W，其中$W=\{y_1,y_2,...,y_n\}$，y表示混沌序列Y中的实数；

[0177] (3-5)第二服务器将新的混沌序列W中的第β个实数y_β根据规则转换成参数序列k_β，以得到参数序列$K=\{k_1,k_2,...,k_n\}$，其中$\beta\in[1,n]$。

[0178] 具体的，所述转换规则为：

[0179] 将y_β的每一位转换成4比特的二进制数，将得到的多个二进制数连接，从而得到新的二进制数k_β。

[0180] (3-6)第二服务器计算新的混沌序列W的均值$\overline{W}$，根据该均值并使用阈值函数生成参数控制序列$Q=\{q_1,q_2,q_3,...,q_n\}$。

[0181] 具体的，所述阈值函数为，对于Q中的第δ个实数q_δ，其中$\delta\in[1,n]$：

[0182] $$\begin{cases} q_\delta = 0, y_\delta \le \overline{W} \\ q_\delta = 1, y_\delta > \overline{W} \end{cases}$$

[0183] (3-7)第二服务器使用步骤(3-5)得到的参数序列K和步骤(3-6)得到的参数控制

序列Q对步骤(3-3)得到的NAL单元序列Q”进行扩散操作，以得到扩散加密序列Q″′，且Q″′＝{q″′$_1$，q″′$_2$，...，q″′$_n$}；

[0184] 本步骤包括以下子步骤：

[0185] (3-7-1)第二服务器设置计数器g＝1；

[0186] (3-7-2)第二服务器判断g是否大于n，如果是则过程结束，否则转入步骤(3-7-3)；

[0187] (3-7-3)第二服务器获取NAL单元序列Q”中的第g个分组q″$_g$、参数序列K中的第g个元素k$_g$、以及参数控制序列Q中的第g个元素q$_g$；

[0188] (3-7-4)第二服务器根据k$_g$和q$_g$对q″$_g$进行扩散操作，以得到扩散后的分组q″′$_g$，本步骤具体为：

[0189] $$q_1'''=\begin{cases}k_1\oplus q_1'',q_1=0\\k_1\odot q_1'',q_1=1\end{cases}$$

[0190] $$q_g'''=\begin{cases}\left(\left(q_{g-1}''+k_g\right)\bmod 256\right)\oplus q_g'',q_g=0\\\left(\left(q_{g-1}''+k_g\right)\bmod 256\right)\odot q_g'',q_g=1\end{cases},\ g=2,...,n$$

[0191] (3-7-5)第二服务器设置计数器g＝g+1，并返回步骤(3-7-1)；

[0192] (3-8)第二服务器将扩散加密序列Q”’中的所有元素进行连接，以得到扩散后的NAL单元；

[0193] (3-9)第二服务器使用扩散后的NAL单元替换第二缓冲区中对应的NAL单元。

[0194] (3-10)第二服务器设置计数器f＝f+1，并返回步骤(3-1)；

[0195] (4)第二服务器将步骤(3)得到的扩散加密后的视频码流发送到第一局域网的第一服务器。

[0196] 作为进一步优选地，本发明提供了一种与上述描述的二次加密过程对应的二次解密过程，包括以下步骤：

[0197] (1)第一服务器根据混沌序列方程迭代生成两个混沌序列X、Y，并将其存入第一缓冲区中。

[0198] (2)第一服务器循环读取第二局域网发来的视频码流，对该视频码流进行扩散解密处理，以得到扩散加密前的视频码流，并将该扩散解密后的视频码流存入第二缓冲区中；

[0199] 本步骤包括以下子步骤：

[0200] (2-1)第一服务器设置计数器count1＝1；

[0201] (2-2)第一服务器判断count1是否大于第二缓冲区中所有NAL单元的总数N，如果是则进入步骤(2-8)，否则转入步骤(2-3)；

[0202] (2-3)第一服务器以3个字节为单位将第二缓冲区中的所有NAL单元分为n组，所有分组构成NAL单元序列Q″′，其中Q″′＝{q″′$_1$，q″′$_2$，...，q″′$_n$}，q″′表示分组；

[0203] (2-4)第一服务器从第一缓冲区中的混沌序列Y中获取n个实数构成新的混沌序列W，其中W＝{y$_1$，y$_2$，...，y$_n$}，y表示混沌序列Y中的实数；

[0204] (2-5)将新的混沌序列W中的第β个实数y$_\beta$根据规则转换成参数序列k$_\beta$，以得到参数序列K＝{k$_1$，k$_2$，...，k$_n$}，其中β∈[1，n]。

[0205] 具体的，所述转换规则为：

[0206] 将y$_\beta$的每一位转换成4比特的二进制数，将得到的多个二进制数连接，从而得到新

的二进制数k_β。

[0207] (2-6)第一服务器计算新的混沌序列W的均值$\overline{W}$，根据该均值并使用阈值函数生成参数控制序列Q＝{q_1,q_2,q_3,...,q_n}。

[0208] 具体的，所述阈值函数为，对于Q中的第δ个实数q_δ，其中δ∈[1,n]：

[0209] $$\begin{cases} q_\delta = 0, y_\delta \le \overline{W} \\ q_\delta = 1, y_\delta > \overline{W} \end{cases}$$

[0210] (2-7)第一服务器使用步骤(2-5)得到的参数序列K和步骤(2-6)得到的参数控制序列Q对步骤(2-3)得到的NAL单元序列Q″′进行扩散解密操作，以得到扩散解密序列Q″；

[0211] 本步骤包括以下子步骤：

[0212] (2-7-1)第一服务器设置计数器count2＝1；

[0213] (2-7-2)第一服务器判断count2是否大于n，如果是则过程结束，否则转入步骤(3-7-3)；

[0214] (2-7-3)第一服务器获取NAL单元序列Q″′中的第count2个分组q''_{count2}、参数序列K中的第count2个元素k_{count2}、以及参数控制序列Q中的第count2个元素q_{count2}；

[0215] (2-7-4)第一服务器根据k_{count2}和q_{count2}对q''_{count2}进行扩散解密操作，以得到扩散解密后的分组q''_{count2}，本步骤具体为：

[0216] $$q_1'' = \begin{cases} k_1 \oplus p_1''', q_1 = 0 \\ k_1 \odot p_1''', q_1 = 1 \end{cases}$$

[0217] $$q_i'' = \begin{cases} ((q''_{count2-1} + k_{count2}) \bmod 256) \oplus q'''_{count2}, q_{count2} = 0 \\ ((q''_{count2-1} + k_{count2}) \bmod 256) \odot q'''_{count2}, q_{count2} = 1 \end{cases}, \quad count2 = 2,...,n$$

[0218] (2-7-5)第一服务器设置计数器count2＝count2+1，并返回步骤(2-7-1)；

[0219] (2-8)第一服务器将所有经过置乱加密的NAL单元进行组合，从而得到置乱加密后的视频码流，并将其存入第二缓冲区中；

[0220] (3)第一服务器循环读取第二缓冲区中的经过扩散解密的视频码流，进行置乱解密处理，以得到置乱加密前的视频码流。

[0221] 本步骤包括以下子步骤：

[0222] (3-1)第一服务器设置计数器count3＝1；

[0223] (3-2)第一服务器判断count3是否大于视频码流中NAL单元的总数N，如果是则进入步骤(3-10)，否则转入步骤(3-3)；

[0224] (3-3)第一务器以3个字节为单位将视频码流中的所有NAL单元分为n组，从而得到NAL单元序列P″，其中P″＝{p''_1,p''_2,p''_3,...,p''_n}，P″表示分组；

[0225] (3-4)第一服务器从第一缓冲区中的混沌序列X中获取n个实数构成新的混沌序列Z，其中Z＝{x_1,x_2,...,x_n}，x表示混沌序列X中的实数；

[0226] (3-5)第一服务器将新的混沌序列Z中的实数x_α根据规则转换成整数值a_α，以得到比特置乱序列A＝{a_1,a_2,...,a_n}，其中α∈[1,n]。具体的，所述转换规则为：

[0227] 取新的混沌序列Z中实数值x_α的小数点后8位构成L_α＝0.$l_0l_1l_2l_3l_4l_5l_6l_7$，计算$a_\alpha = \left((\overline{L}_\alpha \times 10^8) \bmod 23 + 1\right)$，以使得1≤$a_\alpha$≤23。

[0228] (3-6)第一服务器将新的混沌序列Z中的元素按照从大到小的顺序进行排序，从而得到有序序列$X'=\{x'_1,x'_2,...,x'_n\}$，并生成位置置乱序列$D=\{d_1,d_2,...,d_n\}$，该位置置乱序列中的第z个元素$d_z$为有序序列Z中的第z个元素在混沌序列X′中的位置，且有$z\in[1,n]$；

[0229] (3-7)对步骤(3-3)得到的序列$P''=\{p''_1,p''_2,p''_3,...,p''_n\}$按照步骤(3-6)得到的位置置乱序列$D=\{d_1,d_2,...,d_n\}$进行位置置乱解密，以得到序列$P'=\{p'_1,p'_2,p'_3,...,p'_n\}$，其中$p_z'=p''_{dz}$。

[0230] (3-8)第一服务器使用步骤(3-5)得到的比特置乱序列A对步骤(3-7)得到的NAL单元序列P′进行比特置乱解密操作，以得到序列$P=\{p_1,p_2,p_3,...,p_n\}$。

[0231] 本步骤包括以下子步骤：

[0232] (3-8-1)第一服务器设置计数器count4＝1；

[0233] (3-8-2)第一服务器判断count4是否大于NAL单元序列P的长度n，如果是则过程结束，否则转入步骤(3-8-3)；

[0234] (3-8-3)第一服务器获取NAL单元序列P′中的第count4个分组p'_{count4}以及比特置乱序列A中的第count4个元素a_{count4}，将p_{count4}右移a_{count4}位进行比特置乱解密，从而得到分组p_{count4}；

[0235] (3-8-4)第一服务器设置计数器count4＝count4+1，并返回步骤(3-8-1)；

[0236] (4)第一服务器将置乱解密后的视频码流进行保存，等待第一局域网终端设备获取视频数据。

[0237] 本领域的技术人员容易理解，以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

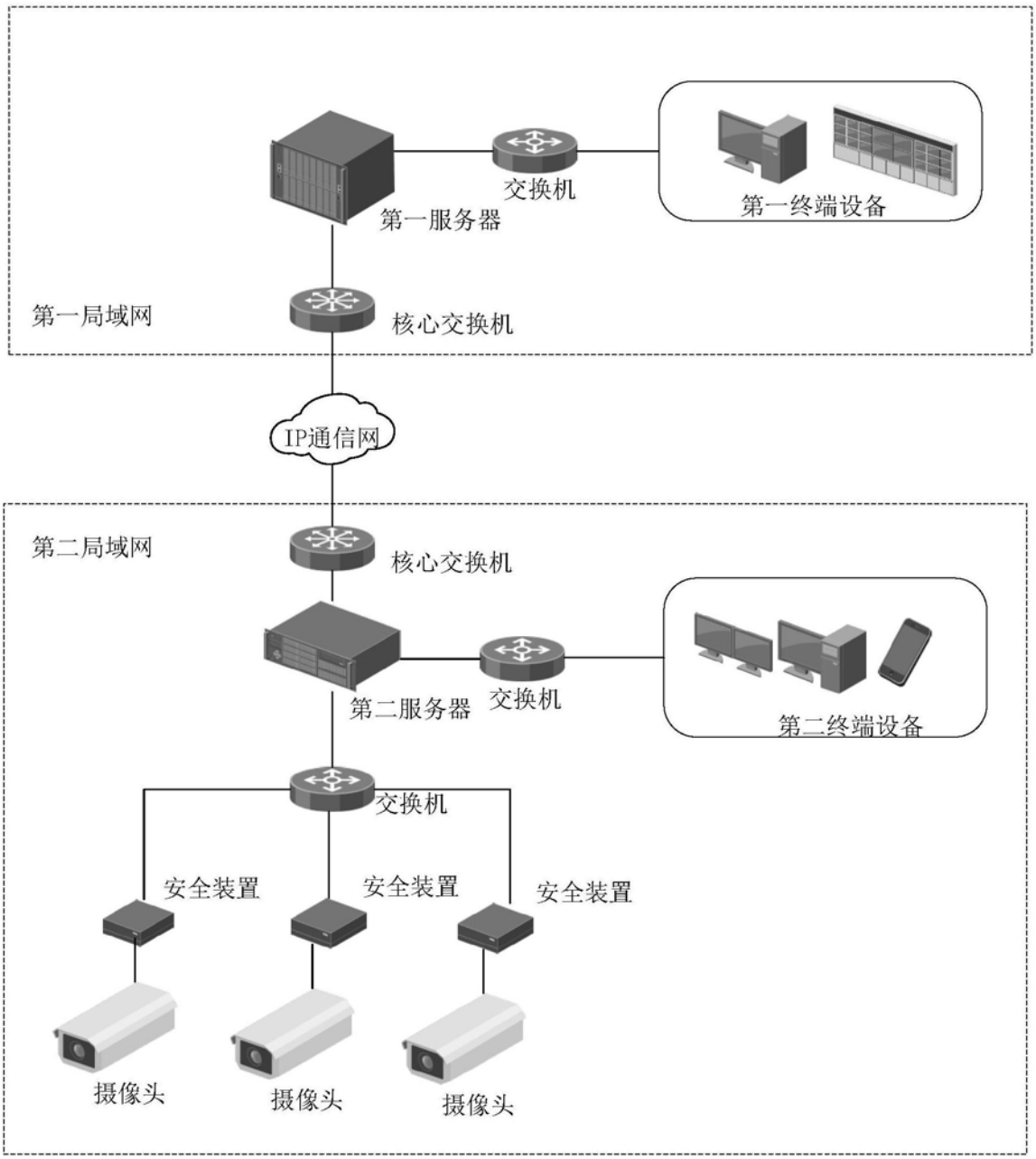

第一局域网
第一服务器
交换机
第一终端设备
核心交换机
IP通信网
第二局域网
核心交换机
第二服务器
交换机
第二终端设备
交换机
安全装置
安全装置
安全装置
摄像头
摄像头
摄像头

图1

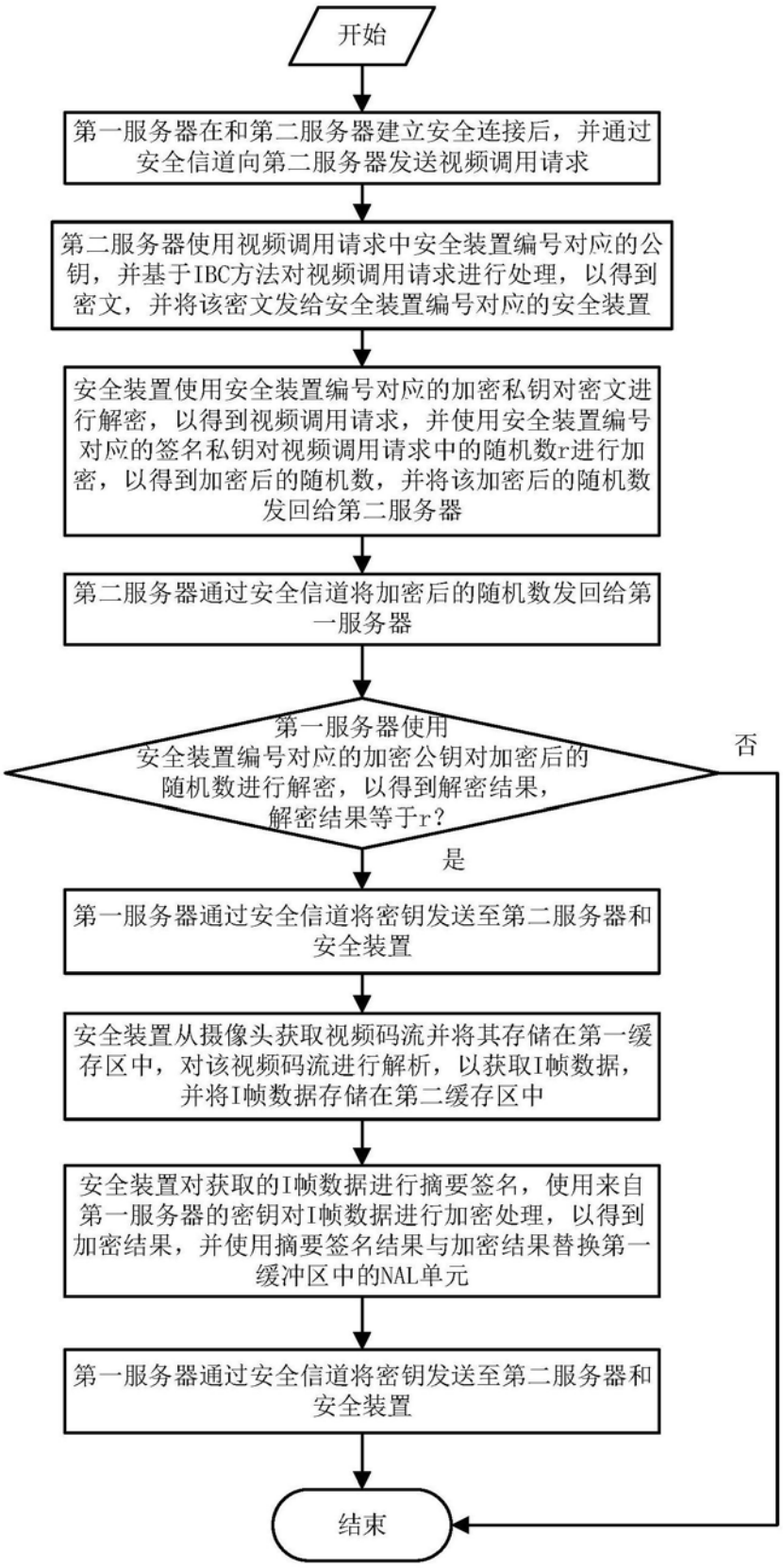

开始
第一服务器在和第二服务器建立安全连接后，并通过安全信道向第二服务器发送视频调用请求
第二服务器使用视频调用请求中安全装置编号对应的公钥，并基于IBC方法对视频调用请求进行处理，以得到密文，并将该密文发给安全装置编号对应的安全装置
安全装置使用安全装置编号对应的加密私钥对密文进行解密，以得到视频调用请求，并使用安全装置编号对应的签名私钥对视频调用请求中的随机数r进行加密，以得到加密后的随机数，并将该加密后的随机数发回给第二服务器
第二服务器通过安全信道将加密后的随机数发回给第一服务器
第一服务器使用安全装置编号对应的加密公钥对加密后的随机数进行解密，以得到解密结果，解密结果等于r？
否
是
第一服务器通过安全信道将密钥发送至第二服务器和安全装置
安全装置从摄像头获取视频码流并将其存储在第一缓存区中，对该视频码流进行解析，以获取I帧数据，并将I帧数据存储在第二缓存区中
安全装置对获取的I帧数据进行摘要签名，使用来自第一服务器的密钥对I帧数据进行加密处理，以得到加密结果，并使用摘要签名结果与加密结果替换第一缓冲区中的NAL单元
第一服务器通过安全信道将密钥发送至第二服务器和安全装置
结束

图2

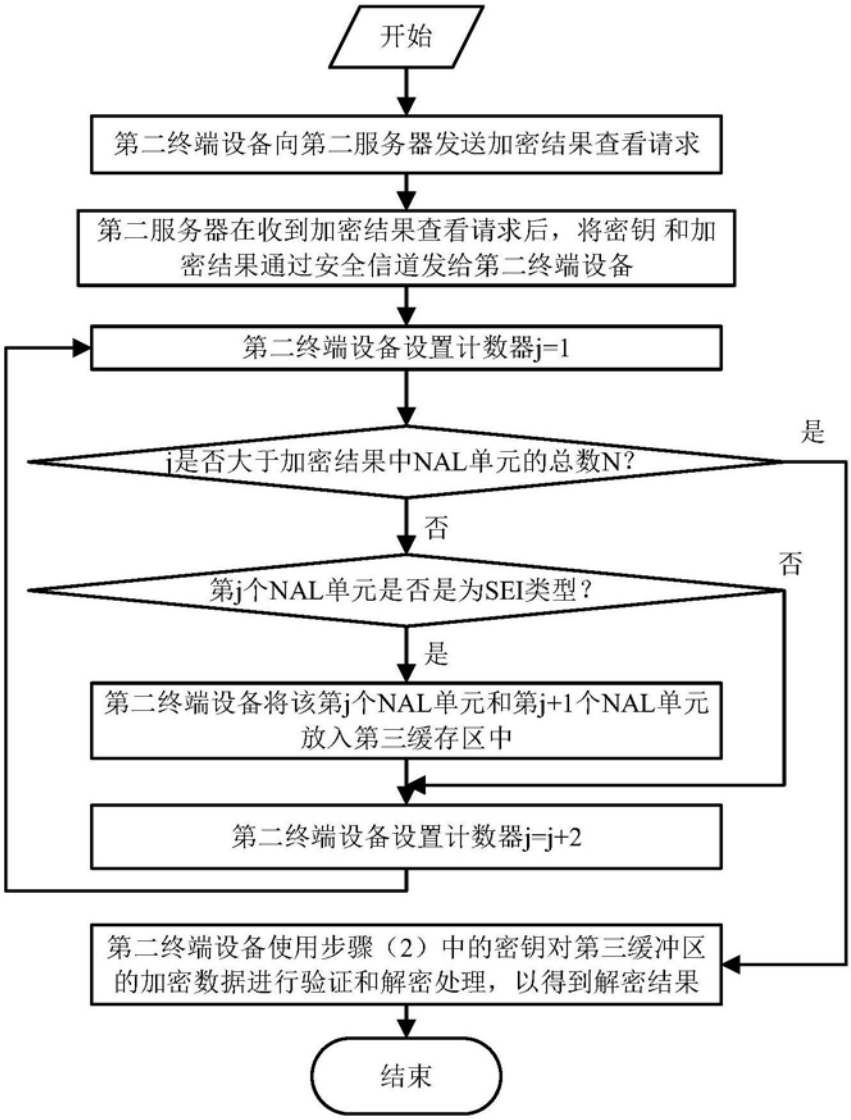

开始
第二终端设备向第二服务器发送加密结果查看请求
第二服务器在收到加密结果查看请求后，将密钥 和加密结果通过安全信道发给第二终端设备
第二终端设备设置计数器j=1
j是否大于加密结果中NAL单元的总数N?
是
否
第j个NAL单元是否是为SEI类型?
否
是
第二终端设备将该第j个NAL单元和第j+1个NAL单元放入第三缓存区中
第二终端设备设置计数器j=j+2
第二终端设备使用步骤（2）中的密钥对第三缓冲区的加密数据进行验证和解密处理，以得到解密结果
结束

图3