说 明 书

**面向三网融合的视频内容安全责任认定方法**

**所属技术领域：**

本发明属于计算机信息安全领域，针对三网融合新业态下，视频内容在开放网络传输，并在多个不可信主体间进行业务交互，当发生非法视频内容传播事件时，无法确定责任方而设计。本发明基于比特承诺、保密比较技术，设计了一种面向三网融合的视频内容安全责任认定方法，该方法具有良好的可实施性和安全性。

**背景技术：**

“三网融合”是指电信网、广播电视网和计算机通信网的相互渗透、互相兼容、并逐步整合成为全世界统一的信息通信网络，三大网络通过技术改造，能够提供包括语音、数据、图像等综合多媒体的通信业务。

传统的视频内容的审核都处于封闭环境中，安全性较高，责任认定容易。但在融合的过程中，网络的开放性和视频内容的多来源性、多样性，内容使用过程中多主体的不可信，攻击手段和方式的多元化等，使得视频内容的安全性面临新的形式和挑战。

在融合的过程中，对于电信网、广播电视网和计算机通信网上传输的视频内容，需要成立统一的监管部门对其进行审核监管，防止非法视频内容进入三网中传播。其审核分发一般过程为：三网中的内容提供商将自己的数字视频内容提交给统一的审核监管部门进行审核，审核通过后，内容提供商才可以选择网络运营商运营数字视频内容。在这个过程中，涉及多个业务流程和主体，当发生违反法律、法规和道德等内容传播时，无法追溯责任方。

分析上述过程，可知存在两方面的不安全因素导致无法确认责任方，其一：信道的不安全，数字视频内容在公开的网络传输，可能遭到恶意攻击者的篡改；其二：主体的不可信，即审核部门和内容提供商的不可信。审核部门可能对内容提供商发来的审核内容进行篡改，或可能因为把关不严导致非法的内容通过审核；内容提供商在收到审核通过的内容后，也有可能进行更改或替换。

通过查阅相关专利和文献资料，尚未发现面向三网融合环境，针对视频内容传播过程的安全责任认定方法。

**发明内容：**

为了克服上述三网融合环境下，视频内容在审核分发过程中，发生非法视频内容传播时的责任认定问题，本发明以MPEG压缩编码为研究对象，对视频内容进行时间维和空间维分割、采样，综合使用比特承诺和保密比较技术，提出了一种面向三网融合的视频内容安全责任认定方法。

本发明的特征在于：提出了一种视频内容关键信息采样方法，将视频在时间维，随机的选取若干关键帧，并按照帧序号划分为若干组；在空间维，对每个关键帧进行区域分割，分为中心区、边缘区和角落区，对不同的区域分配不同的采样率，对每个区域进一步细分到单元，对单元的亮度数据进行采样。将处于同一分组的关键帧采样信息进行级联后，进行比特承诺。在传输的过程中，接收方通过验证发送方所做的承诺，来判断视频是否被篡改过，以及定位篡改发生的区域。在发生纠纷时，在两方之间采用改进的可交换ElGamal加密算法对先前的比特承诺进行保密比较，从而在保护承诺的情况下，实现责任认定。

为了实现上述方法，本发明所采取关键技术方案如下：

1. **关键信息采样方案**

关键信息采样的核心思想是：将视频按照时间维和空间维进行分割、采样。对于一个视频自顶至下，分割为关键帧组、关键帧、区域（一个中心区、四个边缘区和四个角落区）和单元，最终每帧采样的数据就是一个单元所包含的亮度分量数据，如图1所示。

1. 关键帧组

将视频序列中的关键帧按照关键帧序号分成若干组，视频序列的分组数GSize、关键帧的数目IT与分组大小GT的关系为：GSize=IT/GT。若用Ic表示当前视频关键帧的序号，则当前帧所属的组号Gid=Ic/GT。

1. 帧间采样

帧间采样指对视频序列进行时间维的分割，选取部分关键帧。对关键帧的选取采用不同的间隔来增加其随机性，这样每个关键帧组包含的关键帧的数目也是随机的。在本发明中关键帧的选取是通过随机序列来实现的。

设采样的最大间隔用X位比特来表示，则最大间隔Rmax=2X，随机数序列为R={rj| rj =Random(Rmax)，j=0,1,2,3…}，其中Random(Rmax)用于生成不大于Rmax的自然数序列。当前第i个采样帧的序号Ic可表示为：

。

1. 帧内采样

帧内采样是对采样关键帧进行空间维的分割，提取关键帧内部单元亮度分量数据。空间维的分割分为区域划分和单元划分，如图2所示。

1. 区域划分

关键帧被划分成三种区域类型，分别为中心区(M)、边缘区(E)和角落区(C)，中心区只有一块，位于帧的中心位置；边缘区位于中心区的正上、正右、正下、正左方，共4块，并按照此顺序进行区内编号，分别为0,1,2,3；角落区位于四个角上，从左上角开始按顺时针方向进行区内编号，分别为0,1,2,3。对于不同的区，根据人眼关注度的不同，所分配的采样率是不同的，它们之间的采样比率为：M:E:C=4:3:1。

1. 单元划分

对于每个区域，划分为4个单元，单元编号从左上角顺时针方向编号为0,1,2,3，每个单元即为每一次采样的最小信息单元。由于人眼对亮度信息比较敏感，因此，只采样单元中亮度分量数据。

1. 采样点信息表示

采用四元组表示一次采样点信息，四元组形式为（帧序号间隔，区域类型，区域内序号，单元序号）。其中“帧序号间隔”表示此次采样的关键帧帧序号与上一关键帧采样序号的差值，其取值范围由采样间隔X所决定，对于第一次采样，帧序号间隔就是采样的帧序号。“区域类型”表示为中心区、边缘区、角落区之一，它们之间的采样比为4:3:1，共8个状态，因此可以用二进制的3位进行表示，具体参考表1中所示。“区域内序号”表示同种区域的顺序编号, 除中心区外，每个区域都有4个，所以可以用二进制的2位进行表示，对于中心区此编号不予区分。“单元序号”即采样的信息单元，每个分区有4个信息单元，所以其可以用二进制的2位进行表示。

表 1 二值序列所对应区域表

|  |  |
| --- | --- |
| 二值序列 | 表示区域 |
| 000 | 角落区 |
| 001 | 边缘区 |
| 010 | 边缘区 |
| 011 | 边缘区 |
| 100 | 中心区 |
| 101 | 中心区 |
| 110 | 中心区 |
| 111 | 中心区 |

1. 混沌序列产生二值序列

混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程。一类非常简单却被广泛研究的动力系统是Logistic映射。

1. Logistic映射的形式及特征

Logistic映射的数学形式：XK+1=µ XK (1- XK)；其中，混沌域为（0,1），0≤µ≤4称为分支参数，XK∈(0,1)。混沌动力系统的研究工作指出，当在3.5699456和4之间选取一个值，Logistic映射工作处于混沌态。也就是说，由初始条件X0在Logistic映射的作用下所产生的序列{Xk；k=0,1,2,3…}是非周期的，不收敛的并对初始值非常敏感的，如图3所示。

1. 将Logistic映射值转化为二值序列

将Logistic生成的混沌值序列{Xk；k=0,1,2,3…}代入下面的阈值函数：



这样就可以得到一个二值混沌序列，记为：。

1. 二值序列表示采样点

由（4）可知，一个采样点可以用一个四元组表示。整个四元组所需要的位数Tb=帧序号间隔位数+区域类型位数+区域内序号位数+单元序号位数，进一步，Tb=X+3+2+2  Tb=X+7。

由此可知，一个采样点需要Tb位进行表示。将步骤（5）中的二值混沌序列S进行分割成块，每块由Tb位构成，代表一个采样点坐标信息。

1. 关键帧组的采样信息级联

根据采样点坐标信息，对单元进行采样，获得每个采样点单元的数据信息，将处于同一关键帧组Gid的单元信息级联为关键帧组采样信息GSGid。以此类推，得到所有关键帧组的采样信息GS={GSGid; Gid=0,1,2,3…,GSize}。

分析上述采样过程，可知在该过程中，需要选取一组采样参数P(GT,X,X0,µ)，通过这组参数来控制视频序列的采样，最终输出所有关键帧组的采样信息GS。

1. **采样信息组比特承诺方案**

比特承诺允许一方提交一个数值而不用立即揭露该数值所表示的意义，他可以在某个时间以后才揭示意义。比特承诺具有不可否认性和机密性的特点。比特承诺协议可以采用哈希函数来实现。哈希函数可将任意长度的输入消息压缩为某一固定长度的消息摘要的函数，输出的消息也称为散列码。哈希函数的这种单向特性和输出数据长度固定的特征使得它可以生成文件或其他数据块的“数字指纹”，因此在数据完整性保护、数字签名等领域得到广泛应用。

发送方用A表示，接收方用B表示，明文数据为上一步采样参数P和采样信息GS，A和B各自产生一个公钥/私钥对，相互公开公钥，并妥善保管私钥。用E表示加密算法，D表示解密算法，A产生的公钥表示为pkA，对应的私钥为skA；B的公钥为pkB，私钥为skB。协议执行过程：

1. 承诺阶段
2. A采用哈希算法对每组采样信息GSGid进行哈希计算：HGid=Hash(GSGid)，将GSize组哈希结果进行级联：HG= H0||H1||H2||…||HGSize，其中“||”表示信息级联。
3. A使用B的公钥加密采样参数P(GT,X,X0,µ)得CP=EpkB(P)，用其私钥加密HG得CHG=EskA(HG)。
4. 将密文CHG发送给B，暂且保留密文CP。
5. B收到消息CHG，进行解密得HG=DpkA(CHG)，HG就是A对B的承诺，B不知道HG代表的信息，同时A也无法进行否认。
6. 揭示阶段
7. A将CP发送给B。B解密P=DskB(CP)。
8. B采用参数P对视频m计算得：HG’= H’0||H’1||H’2||…||H’GSize。
9. B验证HG中每个HGid是否与HG’中的H’Gid相等，若全部相等，则B相信A的承诺。
10. **保密比较方案**

保密比较是指参与比较的各方在不出示本方秘密数据的前提下验证各方数据是否相同。一般假设参与协议的各方都是半诚实参与者，所谓的半诚实参与者是指各参与者在计算过程中将严格地执行协议，不会进行串通，但也会保留计算的中间结果并试图推导出其他参与者的输入。

若一个加密方案满足等式：，则称该加密方案为可交换的加密方案。可交换加密算法可以实现两方之间的保密比较。

ElGamal算法可用于签名又可用于加密，其安全性依赖于计算有限域上离散对数的难度。当ElGamal用于加密时，首先需要选择一个素数p，三个随机数g、x和k，其中g和x都小于p，k与p-1互素,对明文M的加密算法为：



a和b是密文对，密文的长度是明文M的两倍,x为私钥，公开y,g和p。ElGamal加密算法不具有可交换性。本发明改进了ElGamal加密算法，使其满足可交换性。在保密比较的双方之间共享一个大素数p，相互保密g、x和k；由于保密比较不需要对密文进行解密，所以丢弃用于解密的密文a及其相关计算。设保密比较的双方为A和B，A拥有消息MA，B拥有消息MB，在不泄露MA和MB的情况下，验证MA和M B是否相同。改进的可交换保密比较算法执行过程如下：

1. A选择一个大素数p，并将p发送给B。
2. A产生随机数gA,xA,kA，其中gA,xA都小于p, kA与p-1互素。B也产生随机数gB,xB,kB，其中gB,xB都小于p, kB与p-1互素。A和B相互保密这些数据。
3. A做如下计算：

 (1)

 (2)

把式(1)代入（2）得：

 (3)

B也做同样的计算得：

 (4)

bA1即是A对MA进行一次加密的密文，bB1即是B对MB进行一次加密的密文。

1. A将密文bA1发送给B，B将密文bB1发送给A。
2. A对收到的密文bB1进行二次加密：

 (5)

B对收到的密文bA1进行二次加密得：

 (6)

1. A和B交换二次加密结果,即A发送bA2给B，B发送bB2给A。
2. 则在A、B两端做验证：若bA2=bB2,则MA=MB，否则，MA≠MB。

上述改进的ElGamal加密算法可交换性证明如下：

把式(4)代入(5)得：

 (7)

根据mod运算的性质可得：

 (8)

把式(3)代入(6)得：

 (9)

根据mod运算的性质，可得：

 (10)

若MA=MB,则有式（8）同式（10），从而得证bA2=bB2，即该算法满足可交换性。在本发明中，在不暴露承诺的情况下，参与双方进行保密比较，从而确定责任方。

本发明对数据量大、冗余度高的视频内容，根据编码和人眼关注度的特征进行分割、采样，提取出最能代表视频内容特征的关键信息。将视频采样信息分成了若干组，对每个分组进行比特承诺。在视频传输过程中，在发送端，发送者使用其私钥加密承诺，使用接受者的公钥加密采样参数；在接收端，接受者用发送者的公钥解密承诺，用自己的私钥解密获取采样参数，这种方式有效的防止冒充攻击；同时，接受者通过对发送者承诺的验证，来判断视频是否在信道中发生篡改，以及对篡改发生区域进行定位。在发生责任纠纷时，双方不需要出示本方明文数据，只是进行简单的加密交换，就可以验证双方秘密数据是否相同，进一步分析保密比较结果，即可快速的确定责任方。

**附图说明：**

图1是视频分割采样示意图。

图2是关键帧分割示意图。

图3是不同参数的混沌序列。

图4是视频内容审核分发示意图。

**具体实施方式：**

本发明的实施例中部署了3个节点，分别为内容提供商(Content Provider,简称CP)、审核部门(Audit Provider,简称AP)和网络运营商(Network Operator,简称NO)，分别在这三个节点上部署视频内容安全责任认定系统。本实施例中计算机为“DELL计算机，Intel(R) Core(TM)i5-2400 CPU @ 3.10GHz 3.10GHz, 4.00GB内存，1T硬盘”。采用VC++编程实现。

**具体实施方案为：**

整个系统主要分为两大过程分别为视频内容的审核分发过程和发生纠纷时的责任认定过程。其中审核分发的过程为三网中的CP，将制作好的视频内容上传给统一的AP进行审核，审核通过后AP将内容返回给CP，CP再向三网中的NO分发视频内容，如图4所示。在发生纠纷时，需要AP和NO之间进行保密比较来确定责任方。具体实施过程如下：

1. **视频内容的审核分发过程**
2. CP端视频采样

CP端选择两组采样参数A(GT=100,X=3,x0=0.345,µ=3.65)和参数B(GT=200,X=4,x0=0.125, µ=3.80)，分别对视频m进行采样。其中A组采样结果用于发送给AP端进行信道防篡改验证，B组采样的结果用于从AP端发回视频的防篡改验证。以A组采样参数为例，介绍视频采样模块的处理过程如下：

1. 根据输入参数X=3，计算一个采样点二值序列位数Tb=X+7=3+7=10，即每个采样点需要10位进行表示。
2. 根据混沌初始值参数x0=0.345,µ=3.65，产生随机序列并进行二值化处理，得到二值序列S。
3. 对S按照Tb=10进行分块，每一块代表一个采样点，例如若混沌二值序列S：1011011110 0110100110…，其前10位表示了两个采样点信息，各二值段所映射的采样点信息如表2所示：

表 2 混沌序列映射采样点

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 101 | 101 | 11 | 10 | 011 | 010 | 01 | 10 |
| 帧序号为5 | 区域号为5 | 区内编号为3 | 单元号为2 | 帧序号间隔为3 | 区域号为2 | 区内号为1 | 单元号为2 |

表中描述了两个采样单元的信息，其中第一个采样单元用四元组表示为（101,101,11,10），其表示视频帧序列关键帧的第5帧的中心区单元号为2的区域；第二个采样单元用四元组表示为（011,010,01,10），代表该帧序号与前一个采样帧间隔为3，即帧序号为8，并且边缘区为1的单元号为2的单元。以此类推，获得视频序列所有采样点坐标。对视频m按照产生的采样点坐标进行单元采样，获取采样单元的亮度数据。根据采样点帧序号Ic和分组GT，计算每个采样点所属的分组Gid=Ic/GT。将采样数据按组Gid级联，得到采样信息组GS={GSGid; Gid=0,1,2,3…GSize}。实例中视频m有关键帧IT =657帧，GT=100，则GSize=IT/GT=6，则视频被分为0-6个关键帧组，其中帧组、帧区间及各组采样数如表3所示：

表 3 帧组、帧区间及采样数表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 组号 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 帧区间 | 0-99 | 100-199 | 200-299 | 300-399 | 400-499 | 500-599 | 600-657 |
| 采样数 | 14 | 10 | 15 | 13 | 8 | 14 | 7 |

1. 采样信息组比特承诺
2. 承诺阶段

CP端对上步中的A组采样参数提取的组采样信息GS采用MD5哈希算法进行比特承诺，将一个采样信息组映射为一个128位的大整数，即HGid=MD5(GSGid)，Gid∈[0,6]，计算结果级联得HG= H0||H1||H2||…||H6，HG就是CP要承诺的信息。CP加密采样参数A，得CA=EpkAP(A)；加密比特承诺值HG，得CHG=EskCP(HG)。CP将承诺密文CHG和视频m发送给AP。AP收到消息后，对承诺密文CHG进行解密得HG=DpkCP(CHG)，则HG就是CP对视频m的比特承诺。

1. 揭示阶段

CP将CA发送给AP，AP解密获得采样参数A=DskAP(CA)，并用这组参数对视频m进行步骤（1）中计算，得HG’= H’0||H’1||H’2||…||H’6。AP验证HG’中每个H’Gid是否与CP发送的HGid相同，若0-6组全部相同，则AP相信CP先前所做的承诺，从而证明视频m在传输信道中没有被篡改；若存在不等的，则信道传输中发生了恶意篡改，AP不接受CP所做的承诺，并向CP返回出错的组号Gid，通过组号可以进一步定位篡改发生的区域。

1. 审核返回。

AP对成功收到的视频m进行审核，审核通过后，选取一组采样参数C(GT=100,X=3, x0=0.12, µ=3.678)对视频m按照上述（1）采样方式计算，并按照步骤（2）的方式把承诺及视频发回给CP，CP通过对参数C的承诺进行验证，判断在信道上是否有篡改发生。如果没有，CP则需要进一步验证在AP端是否有篡改发生，通过本地B组参数对返回的视频进行采样和比特承诺，并将结果与本地保存的B组参数采样的比特承诺结果进行比对，若相等则表明在AP端没有发生修改，否则，AP端对视频进行了篡改。

1. 分发。视频在经审核返回CP后，CP确认审核过程中没有被篡改，就可以将视频m分发给NO进行运营。CP采用和AP进行视频传输的方式将视频m和参数A采样的比特承诺HG发送给NO。NO进行验证，确保视频在信道中没有被篡改。

在整个审核分发的过程中，发送方在发送视频内容时进行了比特承诺，接收方对收到的视频都进行了比特承诺验证，从而有效地确保视频内容的传输安全。同时，视频内容从AP返回CP时，CP进行了二次验证，即使用B组参数验证比特承诺，防止AP对视频内容进行修改，从而有效的保证视频内容在三网中的安全传输，为进一步做责任认定做好基础。

1. **发生纠纷时的责任认定过程**

当发生可疑视频在三网中传播，需要鉴别是CP进行了内容替换，还是AP审核把关出了问题时，AP和NO都不需要将本方视频内容的比特承诺数据出示给对方，而是采用保密比较验证比特承诺的方式，通过分析验证结果即可确定责任方。

在“视频内容的审核分发过程”中AP和NO都拥有对视频m的A组参数采样比特承诺值HG，但是由于CP可能对视频m进行了替换，重新计算了HG，故需要验证其是否相等。假设NO端收到视频用m’表示，比特承诺值用HG’表示，则保密比较的目的是为了验证HG是否与HG’相等。具体的保密比较执行过程如下：

1. AP生成一个随机的大素数p，并把p发送给NO。
2. AP产生一组ElGamal密钥gAP,xAP,kAP;NO也产生一组密钥gNO,xNO,kNO。
3. AP端计算：；NO端计算：。AP和NO交换计算结果bAP1和bNO1。AP端对收到的密文数据bNO1进行加密得：；NO端对收到的AP数据进行加密得：。AP和NO再次交换计算结果bAP2和bNO2。
4. 在AP端和NO端分别有二次加密结果bAP2和bNO2。AP和NO两方都可验证bAP2和bNO2是否相等。若bAP2≠bNO2，则表明CP发生了内容替换，责任方为CP；若bAP2=bNO2，则说明视频内容没有变动，是AP审核不严造成的问题，责任方为AP。

为了评测本发明中视频内容采样和比特承诺方法的效率，选取了6段不同大小视频流进行采样和比特承诺，并与传统的哈希算法在计算时间上进行比对，其结果如表4所示。从比较结果中，可以看出对于较小的视频文件来说，其计算时间相差不大，但是随着文件的增大，本发明方法执行效率有较大改善。

表 4 性能测试表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 视频 | 大小（MB） | 参数(GT,X,X0,µ) | 采样承诺时间  (毫秒) | Hash时间  （毫秒） |
| 1 | 7.5 | (25,1,0.32,3.71) | 30 | 35 |
| 2 | 59.8 | (30, 2,0.46,3.84) | 263 | 294 |
| 3 | 144.3 | (50,3,0.41,3.97) | 487 | 718 |
| 4 | 687.8 | (100,4,0.67,3.88) | 2915 | 3571 |
| 5 | 973.7 | (200,5,0.66,3.92) | 4216 | 5652 |
| 6 | 1383.8 | (200,5,0.62,3.81) | 5952 | 8053 |

为了进一步检测本发明中采样和比特承诺方法对视频篡改检测的效果，在测试视频中，考虑到取材的广泛性和普遍性，分别从广告、新闻、电影和体育比赛中选取6段视频流，视频大小和采样参数各不相同，其检测结果如表5所示，表中篡改帧区域指的是对视频序列中关键帧序号区间，篡改结果对应的是检测篡改发生的组号。从表中可以看出，对于不同的视频，在不同的区域进行篡改，本发明中方法都能很好的检测出篡改情况，并且能够定位篡改发生的区域。

表 5 篡改检测结果

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 类型 | I帧数 | 参数(GT,X,X0,µ) | 篡改帧区域 | 结果 |
| 广告 | 160 | (20,1,0.62,3.81) | 40-45 | 2 |
| 新闻 | 2874 | (30, 2,0.76,3.64) | 1003-1018,2050-2062 | 33,68 |
| 体育 | 4011 | (60,3,0.21,3.77) | 无篡改 | 无 |
| 体育 | 6250 | (100,4,0.34,3.99) | 3003-3018,5055-5077 | 30,50 |
| 电影 | 7750 | (200,5,0.46,3.93) | 3205-3230 | 16 |
| 电影 | 8226 | (150,4,0.11,3.96) | 50-67,8007-8028 | 0,53 |

本发明对视频进行分割、采样，采用4:2:1的权重策略，重点突出了受关注区域，降低了算法复杂度，同时提高了检测精度。使用比特承诺方法，通过三网中不可信主体间验证承诺，不仅保证了视频内容传输的安全可靠，而且使发送者对发送视频内容具有不可否认性；在发生纠纷时，通过不可信主体间对先前所做的承诺进行保密比较，实现三网融合环境下的安全责任认定。