1、面向三网融合的视频内容安全责任认定方法，其特征包括：

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亮度分量数据。

1. 关键帧分组。将视频按照关键帧序号进行分组。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。
2. 帧间采样。从一个视频中选取若干关键帧，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。将每个关键帧分成三种类型的区域，分别为中心区(M)、边缘区(E)和角落区(C)。其中，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。
2. 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。“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。综上所述，一个四元组需要位数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。
3. 混沌序列表示采样点。Logistic映射的数学形式为：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。将Logistic混沌序列{Xk；k=0,1,2,3…}代入下面的阈值函数：



这样就可得到一个二值混沌序列，记为：。由步骤4)可知，一个采样点需要Tb位表示，将二值混沌序列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. 采样。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**

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用参数P对视频计算得：HG’= H’0||H’1||H’2||…||H’GSize。

g) 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。

1. **保密比较方案**

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。

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。

上述算法可交换证明，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。