(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 1 月 18 日 (18.01.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/010118 A1

(51) 国际专利分类号:
H04N 21/2347 (2011.01)

(21) 国际申请号: PCT/CN2016/089897

(22) 国际申请日: 2016 年 7 月 13 日 (13.07.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人:深圳大学(SHENZHEN UNIVERSITY) [CN/CN]; 中国广东省深圳市南山区南海大道3688号, Guangdong 518000 (CN)。

(72) 发明人:赵东宁(ZHAO, Dongning); 中国广东省深圳市南山区南海大道3688号, Guangdong 518000 (CN)。 张勇(ZHANG, Yong); 中国广东省深圳市南山区南海大道3688号, Guangdong 518000 (CN)。 张胜利(ZHANG, Shengli); 中国广东省深圳市南山区南海大道3688号, Guangdong 518000 (CN)。 徐勇(XU, Yong); 中国广东省深圳市南山区南海大道3688号, Guangdong 518000 (CN)。 陈剑勇(CHEN, Jianyong); 中国广东省深圳市南山区南海大道3688号, Guangdong 518000 (CN)。 李岩山(LI, Yanshan); 中国广东省深圳市南山区南海大道3688号, Guangdong 518000 (CN)。

(74) 代理人:深圳市恒申知识产权事务所(普通合伙) (HENSEN INTELLECTUAL PROPERTY FIRM); 中国广东省深圳市福田区南园路68号上步大厦10H, Guangdong 518000 (CN)。

(81) 指定国(除另有指明,要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明,要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,

(54) **Title:** DIGITAL VIDEO CONTENT SECURITY AUTHENTICATION METHOD AND SYSTEM THEREOF

(54) **发明名称**: 一种数字视频内容安全认证的方法及其系统

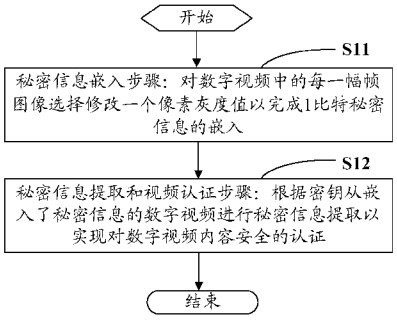

图 1

S11 SECRET INFORMATION EMBEDDING STEP: SELECTIVELY MODIFYING A PIXEL GREY-SCALE VALUE FOR EACH FRAME IMAGE IN A DIGITAL VIDEO, SO AS TO COMPLETE THE EMBEDDING OF ONE-BIT SECRET INFORMATION
S12 SECRET INFORMATION EXTRACTION AND VIDEO AUTHENTICATION STEP: EXTRACTING THE SECRET INFORMATION FROM THE DIGITAL VIDEO EMBEDDED WITH THE SECRET INFORMATION ACCORDING TO A KEY, SO AS TO REALIZE THE AUTHENTICATION ON DIGITAL VIDEO CONTENT SECURITY
AA START
BB END

(57) Abstract: Provided is a digital video content security authentication method. The method comprises: a secret information embedding step: selectively modifying a pixel grey-scale value for each frame image in a digital video, so as to complete the embedding of one-bit secret information; and a secret information extraction and video authentication step: extracting the secret information from the digital video embedded with the secret information according to a key, so as to realize the authentication on digital video content security. Also provided is a digital video content security authentication system. According to the technical solution provided in the present invention, the authentication security can be improved on the basis that the user experience is not affected.

(57) 摘要: 本发明提供一种数字视频内容安全认证的方法，其中，所述方法包括：秘密信息嵌入步骤：对数字视频中的每一幅帧图像选择修改一个像素灰度值以完成1比特秘密信息的嵌入；秘密信息提取和视频认证步骤：根据密钥从嵌入了秘密信息的数字视频进行秘密信息提取以实现对数字视频内容安全的认证。本发明还提供一种数字视频内容安全认证的系统。本发明提供的技术方案能在不影响用户体验的基础上提高认证的安全性。

WO 2018/010118 A1

[见续页]

CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

一种数字视频内容安全认证的方法及其系统

技术领域

本发明涉及多媒体内容安全技术领域，尤其涉及一种数字视频内容安全认证的方法及其系统。

背景技术

随着互联网、移动互联网和多媒体技术的飞速发展，数字视频的采集、处理和传播变得越来越便利，但数字视频内容所反映客观场景的真实性和完整性越来越受到学者、社会和政府的重视，对这些数字视频进行内容的安全认证和鉴别的重要性已不仅仅局限于多媒体内容安全问题，而且还关系到社会的和谐稳定、社会公信力、司法公正等社会问题。

然而，目前对数字视频的内容认证的方法大多对数字视频本身有一定的破坏，影响用户对数字视频的欣赏，且方法较为复杂，隐蔽性和脆弱性较差。

发明内容

有鉴于此，本发明的目的在于提供一种数字视频内容安全认证的方法及其系统，旨在解决现有技术中针对数字视频内容进行安全认证存在影响用户体验以及认证方法复杂且隐蔽性和脆弱性较差的问题。

本发明提出一种数字视频内容安全认证的方法，其特征在于，所述方法包括：

秘密信息嵌入步骤：对数字视频中的每一幅帧图像选择修改一个像素灰度值以完成 1 比特秘密信息的嵌入；

秘密信息提取和视频认证步骤：根据密钥从嵌入了秘密信息的数字视频进行秘密信息提取以实现对数字视频内容安全的认证。

优选的，所述秘密信息嵌入步骤具体包括：

依次按帧读取数字视频 V 中的每一幅帧图像 I(j)，其中，j=0，1，…，t-1，t 表示数字视频 V 的总帧数；

在读取到的数字视频 V 中任意获取一帧图像，确定该帧图像的大小并记为

m × n，其中，m 表示该帧图像的行数，n 表示该帧图像的列数，该帧图像中每一个像素都有一个坐标，左下角像素位置的坐标为(0，0)，右上角像素位置的坐标为(m-1，n-1);

将待嵌入的秘密信息转换为比特序列 w(i)，i=0,1,…,s-1，若所述秘密信息是一个字符串，则用 m_1 表示字符串的长度，作为密钥 key2，若所述秘密信息是一个二值图像，则对二值图像进行光栅扫描获得比特序列，比特序列大小 $s=m_1 \times n_1$，其中 m_1 和 n_1 分别表示二值图像的行数和列数，此时 m_1 和 n_1 作为密钥 key2;

设置 tt=0，ss=0;

读取比特序列中的比特信息 w(ss);

读取帧图像 I(tt)中所选取得到的选取图像块 B(tt)，该选取图像块 B(tt)的左下角位置坐标为(x，y)，右上角位置坐标为(x-1+half_m，y-1+half_n)，该选取图像块 B(tt)的大小为 half_m × half_n，其中，0 ⩽ x < half_m，0 ⩽ y < half_n，x=V_key mod half_m，y= V_key mod half_n，V_key=MD5(key1)，half_m=Trunc(m/2)，half_n= Trunc(n/2)，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数;

计算所述选取图像块 B(tt)中各像素点的灰度值均值 mean(tt);

选取所述选取图像块 B(tt)中灰度值不小于所述灰度值均值 mean(tt)的像素点组成集合 H_set，计算集合 H_set 中的元素个数 H(tt)，并计算出集合 H_set 中灰度值最小的像素点对应的位置坐标(Hx，Hy)和对应的灰度值 H_v=p(Hx，Hy);

选取所述选取图像块 B(tt)中灰度值小于所述灰度值均值 mean(tt)的像素点组成集合 L_set，计算出集合 L_set 中灰度值最大的像素点对应的位置坐标(Lx，Ly)和对应的灰度值 L_v=p(Lx，Ly);

根据所述比特信息 w(ss)的值以及元素个数 H(tt)的奇偶性来完成 1 比特秘密信息的嵌入;

计算 ss = (ss+1) mod s，如果 tt+1 < t，则 tt = tt+1;

遍历数字视频 V 中的所有帧图像，依次嵌入秘密比特信息后，秘密信息嵌入过程终止，获取含秘密信息的数字视频 V′ 。

优选的，所述根据所述比特信息 w(ss)的值以及元素个数 H(tt)的奇偶性来完成 1 比特秘密信息的嵌入的步骤具体包括:

如果元素个数 H(tt)= half_m × half_n，则不对所述选取图像块做秘密信息嵌入操作;

否则，如果 w(ss)=0 且 H(tt)为偶数时，或者 w(ss)=1 且 H(tt)为奇数时，则不对所述选取图像块 B(tt)做任何操作即完成 1 比特秘密信息的嵌入;

否则，如果 w(ss)=0 且 H(tt)=1，则使得 p(Lx，Ly)= p(Hx，Hy);

否则，如果 w(ss)=0，H(tt)为奇数，且 H_v- mean(tt)⩽mean(tt)- L_v 时，则 p(Hx，Hy)= p(Lx，Ly);

否则，如果 w(ss)=0，H(tt)为奇数，且 H_v- mean(tt)＞mean(tt)- L_v 时，则 p(Lx，Ly)= p(Hx，Hy);

否则，如果 w(ss)=1，H(tt)为偶数，且 H_v- mean(tt)＞mean(tt)- L_v 时，则 p(Lx，Ly)= p(Hx，Hy);

否则，如果 w(ss)=1，H(tt)为偶数，且 H_v- mean(tt)⩽mean(tt)- L_v 时，则 p(Hx，Hy)= p(Lx，Ly)。

优选的，所述秘密信息提取和视频认证步骤具体包括:

依次按帧读取待认证的数字视频 V′ 中的每一幅帧图像 I′ (j)，其中，j=0，1，…，t′ -1，t′ 表示数字视频 V′ 的总帧数;

在读取到的数字视频 V′ 中任意获取一帧图像，确定该帧图像的大小并记为 m′ ×n′ ，其中，m′ 表示该帧图像的行数，n′ 表示该帧图像的列数，并依次确定该帧图像中每一个像素的位置坐标，左下角像素位置的坐标为(0，0)，右上角像素位置的坐标为(m′ -1，n′ -1);

设置 tt=0， w=“”;

读取帧图像 I′ (tt)中所选取得到的待认证图像块 B′ (tt)，该待认证图像块 B′ (tt)的左下角位置坐标为(x，y)，右上角位置坐标为(x-1+half_m′ ，y-1+half_n′)，该待认证图像块 B′ (tt)的大小为 half_m′ ×half_n′ ，其中，0⩽x＜half_m′ ，0⩽y＜half_n′ ，x=V_key mod half_m′ ，y= V_key mod half_n′ ，其中，V_key=MD5(key1)，half_m′ =Trunc(m′ /2)，half_n′ = Trunc(n′ /2)，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数;

计算所述待认证图像块 B′ (tt)中各像素点的灰度值均值 mean′ (tt);

选取所述待认证图像块 B′ (tt)中灰度值不小于所述灰度值均值 mean′ (tt)

的像素点组成集合 H′ _set，计算集合 H′ _set 中的元素个数 H′ (tt);

如果 H′ (tt)= half_m′ × half_n′ ，则不对该待认证图像块 B′ (tt)做提取操作;

否则，如果 H′ (tt)为偶数，则 w= w||" 0" ，这里 “||” 表示字符串拼接;

否则，如果 H′ (tt)为奇数，则 w= w||" 1" ，这里 “||” 表示字符串拼接;

如果 tt+1<t′ ，则 tt=tt+1;

遍历待认证的数字视频 V′ 中所有的帧图像，提取出秘密比特字符串 w;

根据密钥 key2 将提取的秘密比特字符串 w 通过表决模型进行比特串还原和秘密信息还原，再根据还原的秘密信息判断该数字视频的内容是否被篡改从而实现对数字视频内容安全的认证。

另一方面，本发明还提供一种数字视频内容安全认证的系统，所述系统包括:

秘密信息嵌入模块，用于对数字视频中的每一幅帧图像选择修改一个像素灰度值以完成 1 比特秘密信息的嵌入;

秘密信息提取和视频认证模块，用于根据密钥从嵌入了秘密信息的数字视频进行秘密信息提取以实现对数字视频内容安全的认证。

优选的，所述秘密信息嵌入模块具体用于:

依次按帧读取数字视频 V 中的每一幅帧图像 I(j)，其中，j=0，1，…，t-1，t 表示数字视频 V 的总帧数;

在读取到的数字视频 V 中任意获取一帧图像，确定该帧图像的大小并记为 m × n，其中，m 表示该帧图像的行数，n 表示该帧图像的列数，该帧图像中每一个像素都有一个坐标，左下角像素位置的坐标为(0，0)，右上角像素位置的坐标为(m-1，n-1);

将待嵌入的秘密信息转换为比特序列 w(i)，i=0,1,…,s-1，若所述秘密信息是一个字符串，则用 m_1 表示字符串的长度，作为密钥 key2，若所述秘密信息是一个二值图像，则对二值图像进行光栅扫描获得比特序列，比特序列大小 $s=m_1 \times n_1$，其中 m_1 和 n_1 分别表示二值图像的行数和列数，此时 m_1 和 n_1 作为密钥 key2;

设置 tt=0，ss=0;

读取比特序列中的比特信息 w(ss);

读取帧图像 I(tt)中所选取得到的选取图像块 B(tt)，该选取图像块 B(tt)的左下角位置坐标为(x，y)，右上角位置坐标为(x-1+half_m，y-1+half_n)，该选取图像块 B(tt)的大小为 half_m × half_n，其中，0≤x＜half_m，0≤y＜half_n，x=V_key mod half_m，y= V_key mod half_n，V_key=MD5(key1)，half_m=Trunc(m/2)，half_n= Trunc(n/2)，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数;

计算所述选取图像块 B(tt)中各像素点的灰度值均值 mean(tt);

选取所述选取图像块 B(tt)中灰度值不小于所述灰度值均值 mean(tt)的像素点组成集合 H_set，计算集合 H_set 中的元素个数 H(tt)，并计算出集合 H_set 中灰度值最小的像素点对应的位置坐标(Hx，Hy)和对应的灰度值 H_v=p(Hx，Hy);

选取所述选取图像块 B(tt)中灰度值小于所述灰度值均值 mean(tt)的像素点组成集合 L_set，计算出集合 L_set 中灰度值最大的像素点对应的位置坐标(Lx，Ly)和对应的灰度值 L_v=p(Lx，Ly);

根据所述比特信息 w(ss)的值以及元素个数 H(tt)的奇偶性来完成 1 比特秘密信息的嵌入;

计算 ss = (ss+1) mod s，如果 tt+1 < t，则 tt = tt+1;

遍历数字视频 V 中的所有帧图像，依次嵌入秘密比特信息后，秘密信息嵌入过程终止，获取含秘密信息的数字视频 V′ 。

优选的，所述秘密信息提取和视频认证模块具体用于:

依次按帧读取待认证的数字视频 V′ 中的每一幅帧图像 I′ (j)，其中，j=0，1，…，t′ -1，t′ 表示数字视频 V′ 的总帧数;

在读取到的数字视频 V′ 中任意获取一帧图像，确定该帧图像的大小并记为 m′ × n′ ，其中，m′ 表示该帧图像的行数，n′ 表示该帧图像的列数，并依次确定该帧图像中每一个像素的位置坐标，左下角像素位置的坐标为(0，0)，右上角像素位置的坐标为(m′ -1，n′ -1);

设置 tt=0， w= “” ;

读取帧图像 I′ (tt)中所选取得到的待认证图像块 B′ (tt)，该待认证图像块 B′ (tt)的左下角位置坐标为(x，y)，右上角位置坐标为(x-1+half_m′ ，y-1+half_n′)，该待认证图像块 B′ (tt)的大小为 half_m′ × half_n′ ，其中，0≤x＜half_m′ ，

$0 \leqslant y < half\_n'$，$x=V\_key \bmod half\_m'$，$y= V\_key \bmod half\_n'$，其中，$V\_key=MD5(key1)$，$half\_m' =Trunc(m'/2)$，$half\_n' = Trunc(n'/2)$，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数；

计算所述待认证图像块 B′(tt)中各像素点的灰度值均值 mean′(tt)；

选取所述待认证图像块 B′(tt)中灰度值不小于所述灰度值均值 mean′(tt)的像素点组成集合 H′_set，计算集合 H′_set 中的元素个数 H′(tt)；

如果 $H'(tt)= half\_m' \times half\_n'$，则不对该待认证图像块 B′(tt)做提取操作；

否则，如果 H′(tt)为偶数，则 w= w||" 0"，这里“||”表示字符串拼接；

否则，如果 H′(tt)为奇数，则 w= w||" 1"，这里“||”表示字符串拼接；

如果 tt+1<t′，则 tt=tt+1；

遍历待认证的数字视频 V′中所有的帧图像，提取出秘密比特字符串 w；

根据密钥 key2 将提取的秘密比特字符串 w 通过表决模型进行比特串还原和秘密信息还原，再根据还原的秘密信息判断该数字视频的内容是否被篡改从而实现对数字视频内容安全的认证。

本发明提供的技术方案充分利用数字视频作为载体，根据密钥和哈希函数在数字视频的帧图像中确定一个秘密图像块隐藏用于认证的秘密信息，该方法仅需要改动一个像素的灰度值即可完成 1 比特秘密信息的嵌入，难以被感知，不会影响用户的体验，而且安全性极高，并且对数字视频造成的失真也尽可能的小，还具有较好的脆弱性，从而可实现对数字视频内容的真实性和完整性进行安全认证。

附图说明

图 1 为本发明一实施方式中数字视频内容安全认证的方法流程图；

图 2 为本发明一实施方式中数字视频内容安全认证的系统 10 的内部结构示意图。

具体实施方式

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。

本发明具体实施方式提供了一种数字视频内容安全认证的方法，其中，所述方法主要包括如下步骤:

S11、秘密信息嵌入步骤：对数字视频中的每一幅帧图像选择修改一个像素灰度值以完成 1 比特秘密信息的嵌入;

S12、秘密信息提取和视频认证步骤：根据密钥从嵌入了秘密信息的数字视频进行秘密信息提取以实现对数字视频内容安全的认证。

本发明提供的一种数字视频内容安全认证的方法充分利用数字视频作为载体，根据密钥和哈希函数在数字视频的帧图像中确定一个秘密图像块隐藏用于认证的秘密信息，该方法仅需要改动一个像素的灰度值即可完成 1 比特秘密信息的嵌入，难以被感知，不会影响用户的体验，而且安全性极高，并且对数字视频造成的失真也尽可能的小，还具有较好的脆弱性，从而可实现对数字视频内容的真实性和完整性进行安全认证。

以下将对本发明所提供的一种数字视频内容安全认证的方法进行详细说明。

请参阅图 1，为本发明一实施方式中数字视频内容安全认证的方法流程图。

在步骤 S11 中，秘密信息嵌入步骤: 对数字视频中的每一幅帧图像选择修改一个像素灰度值以完成 1 比特秘密信息的嵌入。

在本实施方式中，秘密信息嵌入步骤 S11 具体包括 S1101- S1112 这 12 个子步骤，如下所示:

在子步骤 S1101 中，依次按帧读取数字视频 V 中的每一幅帧图像 I(j)，其中，j=0，1，…，t-1，t 表示数字视频 V 的总帧数;

在子步骤 S1102 中，在读取到的数字视频 V 中任意获取一帧图像，确定该帧图像的大小并记为 m × n，其中，m 表示该帧图像的行数，n 表示该帧图像的列数，该帧图像中每一个像素都有一个坐标，左下角像素位置的坐标为(0，0)，右上角像素位置的坐标为(m-1，n-1);

在子步骤 S1103 中，将待嵌入的秘密信息转换为比特序列 w(i)，i=0,1,…,s-1，若所述秘密信息是一个字符串，则用 m_1 表示字符串的长度，作为密钥 key2，若所述秘密信息是一个二值图像，则对二值图像进行光栅扫描获得比特序列，比特序列大小 $s=m_1 \times n_1$，其中 m_1 和 n_1 分别表示二值图像的行数和列数，此时 m_1 和

n_1作为密钥 key2;

在子步骤 S1104 中，设置 tt=0，ss=0;

在子步骤 S1105 中，读取比特序列中的比特信息 w(ss);

在子步骤 S1106 中，读取帧图像 I(tt)中所选取得到的选取图像块 B(tt)，该选取图像块 B(tt)的左下角位置坐标为(x，y)，右上角位置坐标为(x-1+half_m，y-1+half_n)，该选取图像块 B(tt)的大小为 half_m × half_n，其中，0⩽x＜half_m，0⩽y＜half_n，x=V_key mod half_m，y= V_key mod half_n，V_key=MD5(key1)，half_m=Trunc(m/2)，half_n= Trunc(n/2)，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数;

在子步骤 S1107 中，计算所述选取图像块 B(tt)中各像素点的灰度值均值 mean(tt)；在本实施方式中，$mean(tt)=\frac{1}{half\_m\times half\_n}\sum_{i=x}^{x-1+half\_m}\sum_{j=y}^{y-1+half\_n}p(i,j)$，其中 p(i，j)表示帧图像中(i，j)位置处的像素灰度值，若选取图像块 B(tt)是彩色图像，则将彩色图像该位置像素点的绿色值（即 G 值）作为灰度值计算;

在子步骤 S1108 中，选取所述选取图像块 B(tt)中灰度值不小于所述灰度值均值 mean(tt)的像素点组成集合 H_set，计算集合 H_set 中的元素个数 H(tt)，并计算出集合 H_set 中灰度值最小的像素点对应的位置坐标(Hx，Hy)和对应的灰度值 H_v=p(Hx，Hy)；在本实施方式中，如果不止一个像素点灰度值最小，则随机选取一个即可;

在子步骤 S1109 中，选取所述选取图像块 B(tt)中灰度值小于所述灰度值均值 mean(tt)的像素点组成集合 L_set，计算出集合 L_set 中灰度值最大的像素点对应的位置坐标(Lx，Ly)和对应的灰度值 L_v=p(Lx，Ly);

在子步骤 S1110 中，根据所述比特信息 w(ss)的值以及元素个数 H(tt)的奇偶性来完成 1 比特秘密信息的嵌入；在本实施方式中，子步骤 S1110 具体包括:

如果元素个数 H(tt)= half_m × half_n，则不对所述选取图像块做秘密信息嵌入操作;

否则，如果 w(ss)=0 且 H(tt)为偶数时，或者 w(ss)=1 且 H(tt)为奇数时，则不对所述选取图像块 B(tt)做任何操作即完成 1 比特秘密信息的嵌入;

否则，如果 w(ss)=0 且 H(tt)=1，则使得 p(Lx，Ly)= p(Hx，Hy);

否则，如果 w(ss)=0，H(tt)为奇数，且 H_v- mean(tt)≤mean(tt)- L_v 时，则 p(Hx，Hy)= p(Lx，Ly);

否则，如果 w(ss)=0，H(tt)为奇数，且 H_v- mean(tt)＞mean(tt)- L_v 时，则 p(Lx，Ly)= p(Hx，Hy);

否则，如果 w(ss)=1，H(tt)为偶数，且 H_v- mean(tt)＞mean(tt)- L_v 时，则 p(Lx，Ly)= p(Hx，Hy);

否则，如果 w(ss)=1，H(tt)为偶数，且 H_v- mean(tt)≤mean(tt)- L_v 时，则 p(Hx，Hy)= p(Lx，Ly)。

在子步骤 S1111 中，计算 ss = (ss+1) mod s，如果 tt+1＜t，则 tt = tt+1;

在子步骤 S1112 中，遍历数字视频 V 中的所有帧图像，依次嵌入秘密比特信息后，秘密信息嵌入过程终止，获取含秘密信息的数字视频 V′ 。

在步骤 S12 中，秘密信息提取和视频认证步骤：根据密钥从嵌入了秘密信息的数字视频进行秘密信息提取以实现对数字视频内容安全的认证。

在本实施方式中，秘密信息提取和视频认证步骤 S12 具体包括 S1201- S1212 这 12 个子步骤，如下所示：

在子步骤 S1201 中，依次按帧读取待认证的数字视频 V′ 中的每一幅帧图像 I′ (j)，其中，j=0，1，…，t′ -1，t′ 表示数字视频 V′ 的总帧数;

在子步骤 S1202 中，在读取到的数字视频 V′ 中任意获取一帧图像，确定该帧图像的大小并记为 m′ ×n′ ，其中，m′ 表示该帧图像的行数，n′ 表示该帧图像的列数，并依次确定该帧图像中每一个像素的位置坐标，左下角像素位置的坐标为(0，0)，右上角像素位置的坐标为(m′ -1，n′ -1);

在子步骤 S1203 中，设置 tt=0， w=“”；

在子步骤 S1204 中，读取帧图像 I′(tt)中所选取得到的待认证图像块 B′(tt)，该待认证图像块 B′ (tt)的左下角位置坐标为(x，y)，右上角位置坐标为(x-1+half_m′，y-1+half_n′)，该待认证图像块 B′(tt)的大小为 half_m′ × half_n′，其中，0≤x＜half_m′ ，0≤y＜half_n′ ，x=V_key mod half_m′ ，y= V_key mod half_n′ ，其中，V_key=MD5(key1)，half_m′ =Trunc(m′ /2)，half_n′ = Trunc(n′ /2)，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数;

在本实施方式中，根据秘钥 key1 和哈希函数（如 MD5）计算 V_key=MD5(key)

的值;

在子步骤 S1205 中，计算所述待认证图像块 B′ (tt)中各像素点的灰度值均值 mean′ (tt); 在本实施方式中，$mean'(tt)=\frac{1}{half\_m'\times half\_n'}\sum_{i=x}^{x-1+half\_m'}\sum_{j=y}^{y-1+half\_n'}p(i,j)$，其中 p(i，j)表示帧图像中(i，j)位置处的像素灰度值，若选取图像块 B(tt)是彩色图像，则将彩色图像该位置像素点的绿色值（即 G 值）作为灰度值计算;

在子步骤 S1206 中，选取所述待认证图像块 B′ (tt)中灰度值不小于所述灰度值均值 mean′ (tt)的像素点组成集合 H′ _set，计算集合 H′ _set 中的元素个数 H′ (tt);

在子步骤 S1207 中，如果 H′ (tt)= half_m′ × half_n′ ，则不对该待认证图像块 B′ (tt)做提取操作；在本实施方式中，此时如果 tt+1＜t′ ，则 tt=tt+1，并跳转至子步骤 S1204，否则，跳转至子步骤 S1211;

在子步骤 S1208 中，否则，如果 H′ (tt)为偶数，则 w= w||＂ 0＂ ，，这里“||”表示字符串拼接，如果 tt+1＜t′ ，则 tt=tt+1，并跳转至子步骤 S1204;

在子步骤 S1209 中，否则，如果 H′ (tt)为奇数，则 w= w||＂ 1＂ ，，这里“||”表示字符串拼接，如果 tt+1＜t′ ，则 tt=tt+1，并跳转至子步骤 S1204;

在子步骤 S1210 中，如果 tt+1<t′ ，则 tt=tt+1;

在子步骤 S1211 中，遍历待认证的数字视频 V′ 中所有的帧图像，提取出秘密比特字符串 w;

在子步骤 S1212 中，根据密钥 key2 将提取的秘密比特字符串 w 通过表决模型进行比特串还原和秘密信息还原，再根据还原的秘密信息判断该数字视频的内容是否被篡改从而实现对数字视频内容安全的认证。

本发明提供的一种数字视频内容安全认证的方法充分利用数字视频作为载体，根据密钥和哈希函数在数字视频的帧图像中确定一个秘密图像块隐藏用于认证的秘密信息，该方法仅需要改动一个像素的灰度值即可完成 1 比特秘密信息的嵌入，难以被感知，不会影响用户的体验，而且安全性极高，并且对数字视频造成的失真也尽可能的小，还具有较好的脆弱性，从而可实现对数字视频内容的真实性和完整性进行安全认证。

本发明具体实施方式还提供一种数字视频内容安全认证的系统 10，主要包

括:

秘密信息嵌入模块 11，用于对数字视频中的每一幅帧图像选择修改一个像素灰度值以完成 1 比特秘密信息的嵌入;

秘密信息提取和视频认证模块 12，用于根据密钥从嵌入了秘密信息的数字视频进行秘密信息提取以实现对数字视频内容安全的认证。

本发明提供的一种数字视频内容安全认证的系统 10，利用数字视频作为载体，根据密钥和哈希函数在数字视频的帧图像中确定一个秘密图像块隐藏用于认证的秘密信息，该方法仅需要改动一个像素的灰度值即可完成 1 比特秘密信息的嵌入，难以被感知，不会影响用户的体验，而且安全性极高，并且对数字视频造成的失真也尽可能的小，还具有较好的脆弱性，从而可实现对数字视频内容的真实性和完整性进行安全认证。

请参阅图 2，所示为本发明一实施方式中数字视频内容安全认证的系统 10 的结构示意图。

在本实施方式中，数字视频内容安全认证的系统 10，主要包括秘密信息嵌入模块 11、秘密信息提取和视频认证模块 12。

秘密信息嵌入模块 11，用于对数字视频中的每一幅帧图像选择修改一个像素灰度值以完成 1 比特秘密信息的嵌入。

在本实施方式中，所述秘密信息嵌入模块 11 具体用于:

依次按帧读取数字视频 V 中的每一幅帧图像 I(j)，其中，j=0，1，…，t-1，t 表示数字视频 V 的总帧数;

在读取到的数字视频 V 中任意获取一帧图像，确定该帧图像的大小并记为 m × n，其中，m 表示该帧图像的行数，n 表示该帧图像的列数，该帧图像中每一个像素都有一个坐标，左下角像素位置的坐标为(0，0)，右上角像素位置的坐标为(m-1，n-1);

将待嵌入的秘密信息转换为比特序列 w(i)，i=0,1,…,s-1，若所述秘密信息是一个字符串，则用 m_1 表示字符串的长度，作为密钥 key2，若所述秘密信息是一个二值图像，则对二值图像进行光栅扫描获得比特序列，比特序列大小 $s=m_1 \times n_1$，其中 m_1 和 n_1 分别表示二值图像的行数和列数，此时 m_1 和 n_1 作为密钥 key2;

设置 tt=0，ss=0;

读取比特序列中的比特信息 w(ss);

读取帧图像 I(tt)中所选取得到的选取图像块 B(tt)，该选取图像块 B(tt)的左下角位置坐标为(x，y)，右上角位置坐标为(x-1+half_m，y-1+half_n)，该选取图像块 B(tt)的大小为 half_m × half_n，其中，0≤x＜half_m，0≤y＜half_n，x=V_key mod half_m，y= V_key mod half_n，V_key=MD5(key1)，half_m=Trunc(m/2)，half_n= Trunc(n/2)，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数;

计算所述选取图像块 B(tt)中各像素点的灰度值均值 mean(tt);

选取所述选取图像块 B(tt)中灰度值不小于所述灰度值均值 mean(tt)的像素点组成集合 H_set，计算集合 H_set 中的元素个数 H(tt)，并计算出集合 H_set 中灰度值最小的像素点对应的位置坐标(Hx，Hy)和对应的灰度值 H_v=p(Hx，Hy);

选取所述选取图像块 B(tt)中灰度值小于所述灰度值均值 mean(tt)的像素点组成集合 L_set，计算出集合 L_set 中灰度值最大的像素点对应的位置坐标(Lx，Ly)和对应的灰度值 L_v=p(Lx，Ly);

根据所述比特信息 w(ss)的值以及元素个数 H(tt)的奇偶性来完成 1 比特秘密信息的嵌入;

计算 ss = (ss+1) mod s，如果 tt+1 < t，则 tt = tt+1;

遍历数字视频 V 中的所有帧图像，依次嵌入秘密比特信息后，秘密信息嵌入过程终止，获取含秘密信息的数字视频 V′ 。

在本实施方式中，秘密信息嵌入模块 11 的具体处理流程如前述的步骤 S11 所示，在此就不做重复描述。

秘密信息提取和视频认证模块 12，用于根据密钥从嵌入了秘密信息的数字视频进行秘密信息提取以实现对数字视频内容安全的认证。

在本实施方式中，所述秘密信息提取和视频认证模块 12 具体用于:

依次按帧读取待认证的数字视频 V′ 中的每一幅帧图像 I′ (j)，其中，j=0，1，…，t′ -1，t′ 表示数字视频 V′ 的总帧数;

在读取到的数字视频 V′ 中任意获取一帧图像，确定该帧图像的大小并记为 m′ × n′ ，其中，m′ 表示该帧图像的行数，n′ 表示该帧图像的列数，并依次确定该帧图像中每一个像素的位置坐标，左下角像素位置的坐标为(0，0)，右

上角像素位置的坐标为(m′ -1，n′ -1);

设置 tt=0， w=“”；

读取帧图像 I′(tt)中所选取得到的待认证图像块 B′(tt)，该待认证图像块 B′(tt)的左下角位置坐标为(x，y)，右上角位置坐标为(x-1+half_m′，y-1+half_n′)，该待认证图像块 B′(tt)的大小为 half_m′ ×half_n′ ，其中，0≤x＜half_m′ ，0≤y＜half_n′ ，x=V_key mod half_m′ ，y= V_key mod half_n′ ，其中，V_key=MD5(key1)，half_m′ =Trunc(m′ /2)，half_n′ = Trunc(n′ /2)，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数;

计算所述待认证图像块 B′ (tt)中各像素点的灰度值均值 mean′ (tt);

选取所述待认证图像块 B′ (tt)中灰度值不小于所述灰度值均值 mean′ (tt)的像素点组成集合 H′ _set，计算集合 H′ _set 中的元素个数 H′ (tt);

如果 H′ (tt)= half_m′ ×half_n′ ，则不对该待认证图像块 B′ (tt)做提取操作;

否则，如果 H′ (tt)为偶数，则 w= w||" 0" ，这里“||”表示字符串拼接;

否则，如果 H′ (tt)为奇数，则 w= w||" 1" ，这里“||”表示字符串拼接;

如果 tt+1<t′ ，则 tt=tt+1;

遍历待认证的数字视频 V′ 中所有的帧图像，提取出秘密比特字符串 w;

根据密钥 key2 将提取的秘密比特字符串 w 通过表决模型进行比特串还原和秘密信息还原，再根据还原的秘密信息判断该数字视频的内容是否被篡改从而实现对数字视频内容安全的认证。

在本实施方式中，秘密信息提取和视频认证模块 12 的具体处理流程如前述的步骤 S12 所示，在此就不做重复描述。

本发明提供的一种数字视频内容安全认证的系统 10，利用数字视频作为载体，根据密钥和哈希函数在数字视频的帧图像中确定一个秘密图像块隐藏用于认证的秘密信息，该方法仅需要改动一个像素的灰度值即可完成 1 比特秘密信息的嵌入，难以被感知，不会影响用户的体验，而且安全性极高，并且对数字视频造成的失真也尽可能的小，还具有较好的脆弱性，从而可实现对数字视频内容的真实性和完整性进行安全认证。

值得注意的是，上述实施例中，所包括的各个单元只是按照功能逻辑进行划

分的，但并不局限于上述的划分，只要能够实现相应的功能即可；另外，各功能单元的具体名称也只是为了便于相互区分，并不用于限制本发明的保护范围。

另外，本领域普通技术人员可以理解实现上述各实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，相应的程序可以存储于一计算机可读取存储介质中，所述的存储介质，如ROM/RAM、磁盘或光盘等。

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。

权 利 要 求 书

1. 一种数字视频内容安全认证的方法，其特征在于，所述方法包括:

秘密信息嵌入步骤: 对数字视频中的每一幅帧图像选择修改一个像素灰度值以完成 1 比特秘密信息的嵌入;

秘密信息提取和视频认证步骤: 根据密钥从嵌入了秘密信息的数字视频进行秘密信息提取以实现对数字视频内容安全的认证。

2. 如权利要求 1 所述的数字视频内容安全认证的方法，其特征在于，所述秘密信息嵌入步骤具体包括:

依次按帧读取数字视频 V 中的每一幅帧图像 I(j)，其中，j=0，1，…，t-1，t 表示数字视频 V 的总帧数;

在读取到的数字视频 V 中任意获取一帧图像，确定该帧图像的大小并记为 m × n，其中，m 表示该帧图像的行数，n 表示该帧图像的列数，该帧图像中每一个像素都有一个坐标，左下角像素位置的坐标为(0，0)，右上角像素位置的坐标为(m-1，n-1);

将待嵌入的秘密信息转换为比特序列 w(i)，i=0,1,…,s-1，若所述秘密信息是一个字符串，则用 m_1 表示字符串的长度，作为密钥 key2，若所述秘密信息是一个二值图像，则对二值图像进行光栅扫描获得比特序列，比特序列大小 $s=m_1 \times n_1$，其中 m_1 和 n_1 分别表示二值图像的行数和列数，此时 m_1 和 n_1 作为密钥 key2;

设置 tt=0，ss=0;

读取比特序列中的比特信息 w(ss);

读取帧图像 I(tt)中所选取得到的选取图像块 B(tt)，该选取图像块 B(tt)的左下角位置坐标为(x，y)，右上角位置坐标为(x-1+half_m，y-1+half_n)，该选取图像块 B(tt)的大小为 half_m × half_n，其中，0 ⩽ x < half_m，0 ⩽ y < half_n，x=V_key mod half_m，y= V_key mod half_n，V_key=MD5(key1)，half_m=Trunc(m/2)，half_n= Trunc(n/2)，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数;

计算所述选取图像块 B(tt)中各像素点的灰度值均值 mean(tt);

选取所述选取图像块 B(tt)中灰度值不小于所述灰度值均值 mean(tt)的像素点组成集合 H_set，计算集合 H_set 中的元素个数 H(tt)，并计算出集合 H_set 中灰度值最小的像素点对应的位置坐标(Hx，Hy)和对应的灰度值 H_v=p(Hx，Hy);

选取所述选取图像块 B(tt)中灰度值小于所述灰度值均值 mean(tt)的像素点组成集合 L_set，计算出集合 L_set 中灰度值最大的像素点对应的位置坐标(Lx，Ly)和对应的灰度值

L_v=p(Lx，Ly);

根据所述比特信息w(ss)的值以及元素个数H(tt)的奇偶性来完成1比特秘密信息的嵌入;

计算ss = (ss+1) mod s，如果tt+1 < t，则tt = tt+1;

遍历数字视频V中的所有帧图像，依次嵌入秘密比特信息后，秘密信息嵌入过程终止，获取含秘密信息的数字视频V′ 。

3. 如权利要求2所述的数字视频内容安全认证的方法，其特征在于，所述根据所述比特信息w(ss)的值以及元素个数H(tt)的奇偶性来完成1比特秘密信息的嵌入的步骤具体包括:

如果元素个数H(tt)= half_m × half_n，则不对所述选取图像块做秘密信息嵌入操作;

否则，如果w(ss)=0且H(tt)为偶数时，或者w(ss)=1且H(tt)为奇数时，则不对所述选取图像块B(tt)做任何操作即完成1比特秘密信息的嵌入;

否则，如果w(ss)=0且H(tt)=1，则使得p(Lx，Ly)= p(Hx，Hy);

否则，如果w(ss)=0，H(tt)为奇数，且H_v- mean(tt)⩽mean(tt)- L_v时，则p(Hx，Hy)= p(Lx，Ly);

否则，如果w(ss)=0，H(tt)为奇数，且H_v- mean(tt) > mean(tt)- L_v时，则p(Lx，Ly)= p(Hx，Hy);

否则，如果w(ss)=1，H(tt)为偶数，且H_v- mean(tt) > mean(tt)- L_v时，则p(Lx，Ly)= p(Hx，Hy);

否则，如果w(ss)=1，H(tt)为偶数，且H_v- mean(tt)⩽mean(tt)- L_v时，则p(Hx，Hy)= p(Lx，Ly)。

4. 如权利要求1所述的数字视频内容安全认证的方法，其特征在于，所述秘密信息提取和视频认证步骤具体包括:

依次按帧读取待认证的数字视频V′ 中的每一幅帧图像I′ (j)，其中，j=0，1，…，t′ -1，t′ 表示数字视频V′ 的总帧数;

在读取到的数字视频V′ 中任意获取一帧图像，确定该帧图像的大小并记为m′ × n′ ，其中，m′ 表示该帧图像的行数，n′ 表示该帧图像的列数，并依次确定该帧图像中每一个像素的位置坐标，左下角像素位置的坐标为(0，0)，右上角像素位置的坐标为(m′ -1，n′ -1);

设置tt=0， w=“”;

读取帧图像I′ (tt)中所选取得到的待认证图像块B′ (tt)，该待认证图像块B′ (tt)的左下角位置坐标为(x，y)，右上角位置坐标为(x-1+half_m′ ，y-1+half_n′)，该待认证图像块B′ (tt)的大小为half_m′ × half_n′ ，其中，0⩽x < half_m′ ，0⩽y < half_n′ ，x=V_key mod half_m′ ，y= V_key mod half_n′ ，其中，V_key=MD5(key1)，half_m′ =Trunc(m′ /2)，half_n′

= Trunc(n′ /2)，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数；

计算所述待认证图像块 B′ (tt)中各像素点的灰度值均值 mean′ (tt)；

选取所述待认证图像块 B′ (tt)中灰度值不小于所述灰度值均值 mean′ (tt)的像素点组成集合 H′ _set，计算集合 H′ _set 中的元素个数 H′ (tt)；

如果 H′ (tt)= half_m′ × half_n′ ，则不对该待认证图像块 B′ (tt)做提取操作；

否则，如果 H′ (tt)为偶数，则 w= w||" 0" ，这里“||”表示字符串拼接；

否则，如果 H′ (tt)为奇数，则 w= w||" 1" ，这里“||”表示字符串拼接；

如果 tt+1<t′ ，则 tt=tt+1；

遍历待认证的数字视频 V′ 中所有的帧图像，提取出秘密比特字符串 w；

根据密钥 key2 将提取的秘密比特字符串 w 通过表决模型进行比特串还原和秘密信息还原，再根据还原的秘密信息判断该数字视频的内容是否被篡改从而实现对数字视频内容安全的认证。

5. 一种数字视频内容安全认证的系统，其特征在于，所述系统包括：

秘密信息嵌入模块，用于对数字视频中的每一幅帧图像选择修改一个像素灰度值以完成 1 比特秘密信息的嵌入；

秘密信息提取和视频认证模块，用于根据密钥从嵌入了秘密信息的数字视频进行秘密信息提取以实现对数字视频内容安全的认证。

6.如权利要求 5 所述的数字视频内容安全认证的系统，其特征在于，所述秘密信息嵌入模块具体用于：

依次按帧读取数字视频 V 中的每一幅帧图像 I(j)，其中，j=0，1，…，t-1，t 表示数字视频 V 的总帧数；

在读取到的数字视频 V 中任意获取一帧图像，确定该帧图像的大小并记为 m × n，其中，m 表示该帧图像的行数，n 表示该帧图像的列数，该帧图像中每一个像素都有一个坐标，左下角像素位置的坐标为(0，0)，右上角像素位置的坐标为(m-1，n-1)；

将待嵌入的秘密信息转换为比特序列 w(i)，i=0,1,…,s-1，若所述秘密信息是一个字符串，则用 m_1 表示字符串的长度，作为密钥 key2，若所述秘密信息是一个二值图像，则对二值图像进行光栅扫描获得比特序列，比特序列大小 s=m_1 × n_1，其中 m_1 和 n_1 分别表示二值图像的行数和列数，此时 m_1 和 n_1 作为密钥 key2；

设置 tt=0，ss=0；

读取比特序列中的比特信息 w(ss)；

读取帧图像 I(tt)中所选取得到的选取图像块 B(tt)，该选取图像块 B(tt)的左下角位置坐

标为(x，y)，右上角位置坐标为(x-1+half_m，y-1+half_n)，该选取图像块 B(tt)的大小为 half_m × half_n，其中，0≤x＜half_m，0≤y＜half_n，x=V_key mod half_m，y= V_key mod half_n，V_key=MD5(key1)，half_m=Trunc(m/2)，half_n= Trunc(n/2)，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数；

计算所述选取图像块 B(tt)中各像素点的灰度值均值 mean(tt)；

选取所述选取图像块 B(tt)中灰度值不小于所述灰度值均值 mean(tt)的像素点组成集合 H_set，计算集合 H_set 中的元素个数 H(tt)，并计算出集合 H_set 中灰度值最小的像素点对应的位置坐标(Hx，Hy)和对应的灰度值 H_v=p(Hx，Hy)；

选取所述选取图像块 B(tt)中灰度值小于所述灰度值均值 mean(tt)的像素点组成集合 L_set，计算出集合 L_set 中灰度值最大的像素点对应的位置坐标(Lx，Ly)和对应的灰度值 L_v=p(Lx，Ly)；

根据所述比特信息 w(ss)的值以及元素个数 H(tt)的奇偶性来完成 1 比特秘密信息的嵌入；

计算 ss = (ss+1) mod s，如果 tt+1＜t，则 tt = tt+1；

遍历数字视频 V 中的所有帧图像，依次嵌入秘密比特信息后，秘密信息嵌入过程终止，获取含秘密信息的数字视频 V′ 。

7. 如权利要求 5 所述的数字视频内容安全认证的系统，其特征在于，所述秘密信息提取和视频认证模块具体用于：

依次按帧读取待认证的数字视频 V′ 中的每一幅帧图像 I′ (j)，其中，j=0，1，…，t′ -1，t′ 表示数字视频 V′ 的总帧数；

在读取到的数字视频 V′ 中任意获取一帧图像，确定该帧图像的大小并记为 m′ × n′ ，其中，m′ 表示该帧图像的行数，n′ 表示该帧图像的列数，并依次确定该帧图像中每一个像素的位置坐标，左下角像素位置的坐标为(0，0)，右上角像素位置的坐标为(m′ -1，n′ -1)；

设置 tt=0， w= “” ；

读取帧图像 I′ (tt)中所选取得到的待认证图像块 B′ (tt)，该待认证图像块 B′ (tt)的左下角位置坐标为(x，y)，右上角位置坐标为(x-1+half_m′ ，y-1+half_n′)，该待认证图像块 B′ (tt)的大小为 half_m′ × half_n′ ，其中，0≤x＜half_m′ ，0≤y＜half_n′ ，x=V_key mod half_m′ ，y= V_key mod half_n′ ，其中，V_key=MD5(key1)，half_m′ =Trunc(m′ /2)，half_n′ = Trunc(n′ /2)，key1 为密钥，MD5 为哈希函数，Trunc()为截尾取整函数，mod 为取模函数；

计算所述待认证图像块 B′ (tt)中各像素点的灰度值均值 mean′ (tt)；

选取所述待认证图像块 B′ (tt)中灰度值不小于所述灰度值均值 mean′ (tt)的像素点组成集合 H′ _set，计算集合 H′ _set 中的元素个数 H′ (tt)；

如果 H′(tt)= half_m′ × half_n′，则不对该待认证图像块 B′(tt)做提取操作;

否则，如果 H′(tt)为偶数，则 w= w||" 0"，这里“||”表示字符串拼接;

否则，如果 H′(tt)为奇数，则 w= w||" 1"，这里“||”表示字符串拼接;

如果 tt+1<t′，则 tt=tt+1;

遍历待认证的数字视频 V′中所有的帧图像，提取出秘密比特字符串 w;

根据密钥 key2 将提取的秘密比特字符串 w 通过表决模型进行比特串还原和秘密信息还原，再根据还原的秘密信息判断该数字视频的内容是否被篡改从而实现对数字视频内容安全的认证。

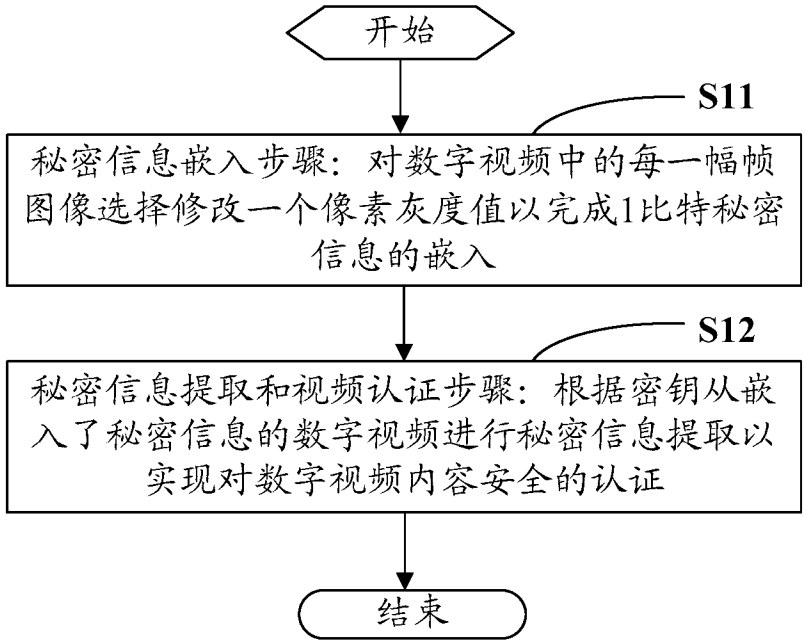
开始
S11
秘密信息嵌入步骤：对数字视频中的每一幅帧图像选择修改一个像素灰度值以完成1比特秘密信息的嵌入
S12
秘密信息提取和视频认证步骤：根据密钥从嵌入了秘密信息的数字视频进行秘密信息提取以实现对数字视频内容安全的认证
结束

图 1

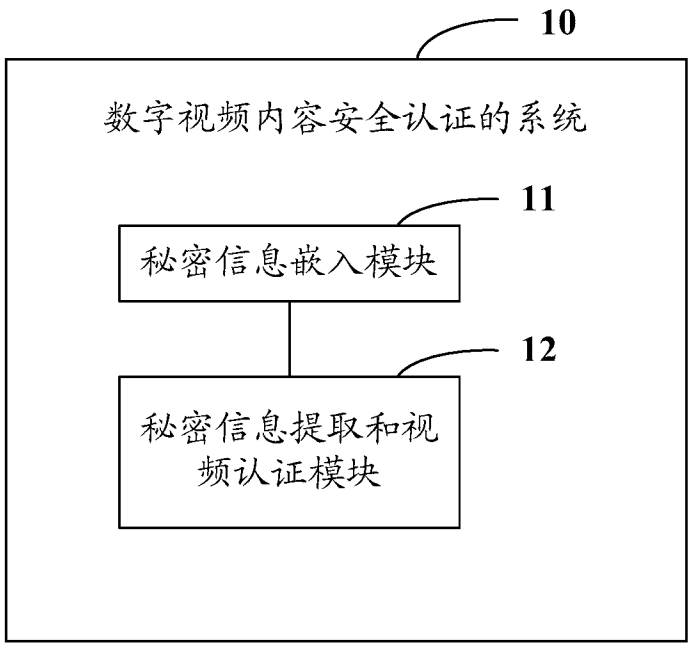
10
数字视频内容安全认证的系统
11
秘密信息嵌入模块
12
秘密信息提取和视频认证模块

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/089897

A. CLASSIFICATION OF SUBJECT MATTER

H04N 21/2347 (2011.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04N, G06T

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNABS, CNTXT, VEN, USTXT: watermark, cover, hide, secret, authentication, security, image, video, grey

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105592323 A (SHENZHEN UNIVERSITY) 18 May 2016 (18.05.2016) description, paragraphs [0054]-[0097], and figures 1-4	1-7
X	CN 103617589 A (XI'AN JIAOTONG UNIVERSITY) 05 March 2014 (05.03.2014) description, paragraphs [0068]-[0141], and figures 1-9	1-7
A	CN 105160694 A (SHENZHEN UNIVERSITY) 16 December 2015 (16.12.2015) the whole document	1-7
A	CN 103426141 A (SHENZHEN UNIVERSITY) 04 December 2013 (04.12.2013) the whole document	1-7
A	CN 103281178 A (SHENZHEN UNIVERSITY) 04 September 2013 (04.09.2013) the whole document	1-7
A	US 2006179318 A1 (NEC CORP.) 10 August 2006 (10.08.2006) the whole document	1-7
E	CN 106101746 A (SHENZHEN UNIVERSITY) 09 November 2016 (09.11.2016) claims 1-7	1-7

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 March 2017	11 April 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer SUN, Yifan Telephone No. (86-10) 62411522

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/089897

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105592323 A	18 May 2016	None	
CN 103617589 A	05 March 2014	CN 103617589 B	06 July 2016
CN 105160694 A	16 December 2015	None	
CN 103426141 A	04 December 2013	CN 103426141 B	10 August 2016
CN 103281178 A	04 September 2013	CN 103281178 B	20 January 2016
US 2006179318 A1	10 August 2006	JP 3630071 B2	16 March 2005
		US 7051207 B2	23 May 2006
		DE 60132128 D1	14 February 2008
		EP 1148704 B1	02 January 2008
		US 7469342 B2	23 December 2008
		DE 60132128 T2	18 December 2008
		JP 2001292297 A	19 October 2001
		EP 1148704 A3	31 March 2004
		US 2001028715 A1	11 October 2001
		EP 1148704 A2	24 October 2001
CN 106101746 A	09 November 2016	None	

国际检索报告

国际申请号
PCT/CN2016/089897

A. 主题的分类

H04N 21/2347(2011.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04N G06T

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNKI，CNABS，CNTXT，VEN，USTXT：水印，隐藏，秘密，认证，安全，图像，视频，灰度，watermark，cover，secret，authentication，security，image，video，grey

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 105592323 A (深圳大学) 2016年 5月 18日 (2016-05-18) 说明书第0054-0097段，图1-4	1-7
X	CN 103617589 A (西安交通大学) 2014年 3月 5日 (2014-03-05) 说明书第0068-0141段，图1-9	1-7
A	CN 105160694 A (深圳大学) 2015年 12月 16日 (2015-12-16) 全文	1-7
A	CN 103426141 A (深圳大学) 2013年 12月 4日 (2013-12-04) 全文	1-7
A	CN 103281178 A (深圳大学) 2013年 9月 4日 (2013-09-04) 全文	1-7
A	US 2006179318 A1 (NEC CORP) 2006年 8月 10日 (2006-08-10) 全文	1-7
E	CN 106101746 A (深圳大学) 2016年 11月 9日 (2016-11-09) 权利要求1-7	1-7

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 3月 24日	2017年 4月 11日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 孙一凡 电话号码 (86-10)62411522

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/089897

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	105592323	A	2016年 5月 18日	无			
CN	103617589	A	2014年 3月 5日	CN	103617589	B	2016年 7月 6日
CN	105160694	A	2015年 12月 16日	无			
CN	103426141	A	2013年 12月 4日	CN	103426141	B	2016年 8月 10日
CN	103281178	A	2013年 9月 4日	CN	103281178	B	2016年 1月 20日
US	2006179318	A1	2006年 8月 10日	JP	3630071	B2	2005年 3月 16日
				US	7051207	B2	2006年 5月 23日
				DE	60132128	D1	2008年 2月 14日
				EP	1148704	B1	2008年 1月 2日
				US	7469342	B2	2008年 12月 23日
				DE	60132128	T2	2008年 12月 18日
				JP	2001292297	A	2001年 10月 19日
				EP	1148704	A3	2004年 3月 31日
				US	2001028715	A1	2001年 10月 11日
				EP	1148704	A2	2001年 10月 24日
CN	106101746	A	2016年 11月 9日	无			